UNDSS | UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

PROTECTING THE PEOPLE WHO WORK FOR A BETTER WORLD

UNITED NATIONS SECURITY MANAGEMENT SYSTEM

SECURITY POLICY MANUAL

YOUR SAFETY, YOUR SECURITY, OUR PRIORITY

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
SECURITY POLICY MANUAL

CONTENTS[1]

[1]The chapters in blue are the policies which are in effect. The items in black are chapters yet to be developed. The blank chapters are no longer in existence.
*These are items supported by guidelines

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter II

UNITED NATIONS SECURITY MANAGEMENT SYSTEM

SECTION B

Framework of Accountability for the United Nations Security Management System

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 04 February 2011
Technical Review: 1 May 2017

I. Scope

1. The primary responsibility for the security and protection of personnel employed by United Nations system organizations, their spouses and other recognized dependants and property and the organizations' property rests with the host Government. This responsibility flows from every Government's normal and inherent function of maintaining order and protecting persons and property within its jurisdiction. In the case of international organizations and their officials, the Government is considered to have a special responsibility under the Charter of the United Nations or the Government's agreements with individual organizations.
2. Without prejudice to the above and while not abrogating the responsibility of the host Government for its obligations, the United Nations has a duty as an employer to reinforce and, where necessary, supplement the capacities of host Governments to fulfil their obligations in circumstances where United Nations personnel are working in areas that are subject to conditions of insecurity which require mitigation measures beyond those which the host Government can reasonably be expected to provide. This Framework of Accountability specifies the responsibilities and accountabilities of United Nations officials and personnel for such measures.
3. In this regard, the United Nations Security Management System (UNSMS), in seeking to establish and maintain operations in insecure and unstable environments, adopts the principle of "how to stay" as opposed to "when to leave" as a tenet of its security management approach.
4. In accepting responsibility and accountability for security management, it is recognized that fatalities and/or casualties may occur, even though appropriate efforts are being made and measures implemented to reduce to an acceptable level the risks to United Nations personnel, premises and assets.

II. Mission Statement of the United Nations Security Management System

5. The goal of the UNSMS is to enable the conduct of United Nations activities while ensuring the safety, security and well-being of personnel and the security of United Nations premises and assets**.**
6. To achieve this goal, all organizations shall maintain a robust and cohesive security management system and adhere to three principles:
   - Determination of acceptable risk
   - Provision of adequate and sustainable resources to manage the risk to personnel and their eligible dependants, premises and assets; and
   - Development and implementation of security policies and procedures.

III. Governance Mechanism

7. The governance of security management for the UNSMS as a whole is constituted as follows:

   a) The Inter-Agency Security Management Network (IASMN), consisting of the senior managers who have oversight of security functions within each member organization of the UNSMS, reviews existing and proposed policies, procedures and practices of the UNSMS and their implementation, and it provides recommendations on these to the High-Level Committee on Management (HLCM); and

   b) A comprehensive review of policies and resource-related issues pertaining to the entire UNSMS is a standing item on the agenda of the HLCM. The HLCM reviews the recommendations made by the IASMN and either decides on them directly or recommends their endorsement and implementation to the United Nations System Chief Executives Board for Coordination (CEB), which is chaired by the Secretary-General.

IV. Actors within the United Nations Security Management System

A. The Secretary-General

8. Under Article 97 of the Charter of the United Nations, the Secretary-General is the chief administrative officer of the Organization. The mandates promulgated by the principal organs are entrusted to him for their implementation under Article 98. The Secretary-General is thus accountable to the Member States for the proper running and administration of the Organization and implementation of its programmes, to include, in the context of this framework, the overall safety and security of United Nations personnel, premises and assets at headquarters and field locations. The Secretary-General can delegate authority to the various Under-Secretaries-General who are individually accountable to him.

B. The Under-Secretary-General for Safety and Security

9. The Under-Secretary-General for Safety and Security is appointed in writing by the Secretary-General to whom he/she reports and is accountable to. The Secretary-General delegates to the Under-Secretary-General for Safety and Security the authority to make executive decisions relevant to the direction and control of the UNSMS and the overall safety and security of United Nations personnel, premises and assets at both field and headquarters locations. The Under-Secretary-General for Safety and Security represents the Secretary-General on all security-related matters and serves as the Chairman of the IASMN. The responsibilities of the Under-Secretary-General for Safety and Security include:

   (a) Developing security policies, practices and procedures for the United Nations system worldwide.

   (b) Coordinating with the organizations of the United Nations system to ensure the implementation of, the compliance with and the support for security aspects of their activities.

   (c) Preparing reports of the Secretary-General on all security-related matters.

(d) Advising the Secretary-General on all matters related to security and safety of the United Nations system.

C. The Executive Group on Security

10. The members of the Executive Group on Security (EGS) are appointed by the CEB. When requested by the Under-Secretary-General for Safety and Security, the members of the EGS advise, reinforce and facilitate the rapid decision-making authority and accountability of the Under-Secretary-General for Safety and Security, in accordance with the EGS Terms of Reference. The members of the EGS have a responsibility to support the Under-Secretary-General in the discharge of his/her mandate related to the safety and security of all personnel employed by the organizations of the United Nations system and their recognized dependants, premises and assets.

D. Executive Heads of United Nations System Organizations[2]

11. Executive Heads of the United Nations Agencies, Funds and Programmes (AFP) are responsible and accountable to the Secretary-General for ensuring that the goal of the UNSMS is met within their respective organizations. Without prejudice to their accountability to their own governing and legislative bodies, Executive Heads of the United Nations specialized agencies, and of other organizations participating in the UNSMS, recognize the coordinating role and authority of the Secretary-General in matters related to the safety and security of United Nations personnel and commit themselves to ensuring that the goal of the UNSMS is met.

E. Senior Security Managers and/or Security Focal Points at Headquarters

12. The Executive Heads will appoint a Senior Security Manager and/or a Security Focal Point at their Headquarters to be responsible for coordinating the organization's response to safety and security matters and providing the Executive Head and all relevant actors with advice, guidance and technical assistance.

F. Designated Officials

13. In each country or designated area where the United Nations is present, the most senior United Nations official is normally appointed in writing by the Secretary-General as the Designated Official for Security and accredited to the host Government as such. The Designated Official[3] (DO) is accountable to the Secretary-General, through the Under-Secretary-General for Safety and Security, and is responsible for the security of United Nations personnel, premises and assets throughout the country or designated area. The Secretary-General delegates to the DO the requisite authority

[2] The term 'organizations' includes: the major organizational units of the Secretariat which have heads officially accountable to the Secretary-General; other bodies subsidiary or related to the United Nations, such as the United Nations Agencies, Funds and Programmes; and organizations participating in the United Nations security management system.

[3] Elected Executive Heads of Specialized Agencies appointed Designated Officials remain accountable to their respective governing bodies and carry out their DO functions based on specific bilateral arrangements agreed with the United Nations Department of Safety and Security.

to make decisions in exigent circumstances, including, but not limited to, the mandatory relocation or evacuation of personnel. This authority, and decisions taken pursuant to it, shall remain subject to the authority and review of the Under-Secretary-General for Safety and Security. The DO is responsible for ensuring that the goal of the UNSMS is met in his/her country or area.

G. Representatives of Organizations Participating in the United Nations Security Management System

14. Representatives of organizations of the United Nations system at the country level who participate in the UNSMS are accountable to the Secretary-General through their respective Executive Heads or to the Executive Heads of the United Nations specialized agencies, as appropriate, for all matters related to the security of their personnel at the duty station.

H. Security Management Team

15. The Security Management Team (SMT) will consist of the DO, who acts as chair, the head of each United Nations organization present at the duty station and the Chief Security Adviser (CSA)/Officer. The SMT advises the DO on all security-related matters.

16. In peacekeeping missions, where the Head of Mission serves as the DO, the SMT may also include Heads of components, offices or sections, as specified by the DO. Heads of military and police components of peacekeeping missions will always serve as members of the SMT.

17. Members of the SMT are responsible for supporting the DO in discharging his/her mandate related to the safety and security of all United Nations personnel, premises and assets.

I. Area Security Coordinators

18. Area Security Coordinators (ASCs) are staff members appointed in writing by the DO, in consultation with the SMT, in areas of larger countries which are separated from the capital, in terms of both distance and exposure in order to coordinate and control security arrangements applicable to all personnel, premises and assets in their areas of responsibility. ASCs are accountable to the DO for their security-related responsibilities, in accordance with their respective letters of appointment.

J. Chief Security Advisers/Security Advisers

19. The CSA/Security Adviser (SA) is a security professional appointed by the Under-Secretary-General for Safety and Security to advise the DO and the SMT in their security functions. The CSA/SA reports to the DO and maintains a technical line of communication to the United Nations Department of Safety and Security (UNDSS). In countries where a Deputy Security Adviser is authorized, these provisions also apply.

K. Chief Security Officers

20. In some countries where peacekeeping missions are deployed and the Head of Mission is appointed as the DO for that country or area, there may be no presence of security professionals appointed by the Under-Secretary-General for Safety and Security. Under these circumstances, the mission's Chief Security Officer will act as an SA and assume this level of accountability.

L. Country Security Focal Points

21. In the absence of a CSA/SA, the DO, in consultation with the UNDSS and the staff member's employing organization, will appoint an international staff member to act as Country Security Focal Point (CSFP) for the SMT. CSFPs are accountable to the DO, through their head of agency, for security-related matters, in accordance with their respective letters of appointment.

M. Other Security Personnel of the United Nations Department of Safety and Security

22. The UNDSS personnel, at headquarters and in the field, are responsible for assisting the DO, AFP and organizations of the United Nations system. It is accountable to the Under-Secretary-General according to the terms of the UNDSS internal framework for accountability.

N. Single-Agency Security Officers

23. Single-Agency Security Officers are security professionals hired by organizations of the UNSMS to advise their respective organizations and to be responsible for the security aspects of activities which are specific to their organizations. Single-Agency Security Officers are accountable to their respective organization and at the same time are responsible for supporting the DO under the coordination of the CSA/SA.

24. In the absence of the CSA/SA, Single-Agency Security Officers act as the CSA/SA ad interim for a specified period when required and requested. This will be confirmed in writing by the DO, following consultation with the relevant head of agency, and include the Terms of Reference of the CSA/SA for accountability purposes.

O. Local Security Assistants

25. The Local Security Assistant (LSA) is recruited at the country level by the UNDSS, AFP or missions led or supported by the Department of Peacekeeping Operations.

26. Under the immediate supervision of the respective security professional, the LSA provides assistance in the Security Risk Management (SRM) process and preparing, Minimum Operating Security Standards (MOSS), Residential Security Measures (RSMs) and contingency plans. The LSA monitors the implementation of security policies and procedures and all matters pertaining to the safety and security of personnel, premises and assets. It is important to note that the security professionals maintain responsibility and accountability for safety and security in accordance with the Framework of Accountability.

P. Wardens

27. Wardens are appointed in writing by the DO/ASC, in consultation with the SMT, to assist in the implementation of the security plan. Wardens are accountable to the DO/ASC for their security-related functions, irrespective of their employing organization.

Q. Personnel Employed by Organizations of the United Nations System

28. Personnel employed by the organizations of the United Nations system are accountable to their respective organizations. All such personnel, regardless of their rank or level, have the responsibility to abide by security policies, guidelines, directives, plans and procedures of the UNSMS and its organizations.

V. Conclusion

29. This Framework of Accountability provides clear guidance on how to enable the conduct of United Nations activities while ensuring the safety, security and well-being of personnel, premises and assets. This goal may be attained by ensuring that all actors of the UNSMS are empowered and provided with the necessary resources and training and a clear understanding of their roles and responsibilities.

30. The roles and responsibilities of all actors of the UNSMS for which they will be held accountable are attached as an annex.

ANNEX

Roles and Responsibilities of Actors within the United Nations Security Management System

A. The Secretary-General

1. Has overall responsibility for the safety and security of United Nations personnel, premises and assets at headquarters and field locations.

B. Under-Secretary-General for Safety and Security

1. Advises the Secretary-General on all matters related to the security and safety of personnel, premises and assets of the United Nations system;
2. Represents the Secretary-General on all security-related matters;
3. Leads and manages the Department of Safety and Security;
4. Chairs the Inter-Agency Security Management Network;
5. Prepares and publishes an internal framework for accountability documenting individual roles, responsibilities and accountabilities related to safety and security in his/her department;
6. Oversees the development of security policies, practices and procedures for the United Nations system worldwide;
7. Coordinates with the organizations of the United Nations system to ensure implementation, compliance and support for security aspects of their activities;
8. Prepares reports of the Secretary-General on all security-related matters; and
9. Directs the organizational response to crisis management as required.

C. The Executive Group on Security

1. When requested by the Under-Secretary-General for Safety and Security, or at the request of any Executive Group on Security (EGS) member, the EGS advises the Under-Secretary-General for Safety and Security in situations where a rapid decision is required to avoid loss of life or to resolve an impasse at the SMT level;
2. Meets as requested by the Under-Secretary-General for Safety and Security or confers with the Under-Secretary-General for Safety and Security by telephone or other means when the situation does not permit a meeting; and
3. Supports the Under-Secretary-General for Safety and Security in the implementation of his/her decision taken in consultation with the EGS.

D. Executive Heads of United Nations Organizations[4]

1. Implement the "no programme without security, no security without resources" strategy in all programmes;
2. Ensure that safety and security are core components of all programmes and activities, and that the SRM process considered and given due priority from the start of all planning processes;
3. Prepare and publishes an internal Framework of Accountability documenting individual roles, responsibilities and accountabilities related to safety and security for their organizations;
4. Ensure that all managers and personnel working for them not only support the Secretary-General, but also discharge their responsibilities to ensure compliance with the UNSMS;
5. Liaise closely with the Under-Secretary-General for Safety and Security to ensure a coherent, system-wide approach to security;
6. Have a collective responsibility to work together to implement and contribute to the development of the UNSMS;
7. Advocate in all available forums to ensure that Member States provide for the safety and security of all personnel, premises and assets of the United Nations system and that crimes against United Nations personnel, premises and assets will not be tolerated and the perpetrators brought to justice;
8. Have a "duty of care" to ensure that personnel employed by their organizations and their recognized dependants are not exposed to unacceptable risk and that all measures are taken to mitigate risks;
9. Appoint a Senior Security Manager and/or Security Focal Point at Headquarters;
10. Recognize and reward good performance in security management by including security in job descriptions and performance appraisals, and address cases of non-compliance at all levels in the organization; and
11. Address specific gender-related security concerns as required.

E. Senior Security Managers and/or Security Focal Points at Headquarters

1. Advise the Executive Head and senior management on security matters and keep them updated on security management issues;
2. Ensure that representatives of their organizations are aware that they must participate fully in the SMT as applicable;
3. Assist/support in the mobilization of resources to assist field offices in the implementation of security requirements;
4. Serve as members of the IASMN and other senior-level forums;

[4] The term 'organizations' includes: the major organizational units of the Secretariat which have heads officially accountable to the Secretary-General; other bodies subsidiary or related to the United Nations, such as the United Nations Agencies, Funds, and Programmes; and organizations participating in the United Nations Security Management System.

5. Work in close association with UNDSS and other members of the IASMN, as well as supports the Under-Secretary-General for Safety and Security in the discharge of his/her responsibilities;
6. Provide advice to representatives of their organizations for the implementation of security policies and procedures as applicable;
7. Ensure that all personnel of their organizations and their recognized dependants are aware of security training requirements, and facilitate the provision of security training and briefings;
8. Disseminate information and educational materials regarding security matters; and
9. Monitor and report on compliance with security policies, practices and procedures.

F. Designated Officials

1. Implement the arrangements detailed in United Nations security policies and procedures as well as develop and implement the required plans for the duty station with the aim of maintaining the security and safety of United Nations personnel, premises and assets;
2. Engage with the authorities of the host country to advocate full implementation of the host country's security responsibilities in respect of United Nations personnel, premises and assets;
3. Apply the SRM approach to all United Nations activities and operations;
4. Manage and direct all security activities at the duty station;
5. Recommend to the Under-Secretary-General for Safety and Security suitable nominations to act as Designated Official (DO) ad interim. Such appointees will be the head of a United Nations Agency, Fund, Programme or Organization;
6. Keep the Secretary-General informed, through the Under-Secretary-General for Safety and Security, of all developments in the country which have a bearing on the safety and security of the United Nations system;
7. In the event that operational matters affect safety and security, communicate this information to the Under-Secretary-General for Safety and Security;
8. Implement any arrangements decided by the Secretary-General in support of the host Government's measures for the safety and security of United Nations personnel, premises and assets, as well as maintaining liaison with the government of the host country on matters concerning the safety and security of United Nations personnel, premises and assets;
9. Collaborate on safety and security matters with intergovernmental and non-governmental organizations working as operational partners of the United Nations system in accordance with established guidelines;
10. Chair the SMT and submit minutes to UNDSS;
11. Keep the members of the SMT, as well as the senior officials of each organization at the duty stations (as applicable) fully apprised of all security-related information and measures being taken in the country;

12. Include in security arrangements at the duty station the staff members (and their recognized dependants) of intergovernmental and non-governmental organizations which have signed a memorandum of understanding;
13. Maintain a fully integrated operational communications system for security management;
14. In consultation with the SMT, appoint Area Security Coordinators (ASCs) and Wardens, verify that they are adequately trained and equipped and provide their parent agency with input for the individual's performance appraisal;
15. Prepare special arrangements, agreed on an inter-agency basis, for the evacuation of internationally-recruited personnel, and an internal relocation plan for locally-recruited personnel;
16. In an emergency where it has not been possible to communicate with the Under-Secretary-General for Safety and Security, use their best judgment in carrying out relocations/evacuations and report to the Secretary-General, through the Under-Secretary-General for Safety and Security, immediately thereafter;
17. Provide all United Nations personnel and their recognized dependants information on specific measures which they should take in relation to the security plan, and ensure that all such personnel receive adequate and appropriate security training;
18. Provide all requested reports to UNDSS, as outlined in the United Nations Security Management System *Security Policy Manual* or other directives from the Under-Secretary-General for Safety and Security;
19. Take appropriate action when advised of non-compliance with United Nations security policies, practices and procedures, including referral to the organization concerned, as well as report serious instances of non-compliance to the Under-Secretary-General for Safety and Security;
20. Address specific gender-related security concerns as required; and
21. If applicable, appoint, in consultation with the employing organization, a Country Security Focal Point and ensure that the Country Security Focal Point receives appropriate training to fulfil his/her responsibilities.

G. Representatives of Organizations Participating in the United Nations Security Management System

1. Implement appropriate actions to provide for the safety and security of their respective personnel and their recognized dependants at the duty station;
2. Ensure that safety and security is a core component of their respective programmes in the country and that appropriate funding is provided;
3. Consult with and assist the DO on all matters concerning security and the implementation and maintenance of the security plan, Minimum Operating Security Standards (MOSS) and RSMs;
4. Serve as a member of the SMT;
5. Advise the DO, CSA and their respective Security Focal Point at Headquarters on the particular concerns of their organizations regarding security;

6. Ensure full and complete compliance by their personnel and their recognized dependants with all security-related instructions;
7. Take action on instances of non-compliance of security policies, practices and procedures and advises the DO on actions taken;
8. Ensure that activities of their organization are conducted in a way that manages the risks to personnel, premises and assets;
9. On a regular basis, provide the DO with updated lists of all personnel and their recognized dependants in the country;
10. Routinely advise the DO regarding the whereabouts and the movement of their respective personnel and their recognized dependants, in accordance with procedures established at the duty station;
11. Report to the DO and their respective Security Focal Point at Headquarters all security-related incidents;
12. Report all recognized dependants residing at the duty station of internationally-recruited staff who are serving elsewhere so they are accorded the same provision for security as dependants of international staff serving at the duty station;
13. Ensure that arrangements are in place for intergovernmental and non-governmental organizations working as operational partners with the concerned United Nations agencies;
14. Ensure that movement of all personnel is undertaken in accordance with United Nations system rules and procedures;
15. Equip their respective personnel with required safety and security equipment as specified in MOSS and train personnel in its use;
16. Require that their respective personnel attend appropriate security awareness training and briefings;
17. Attend all security training for members of the SMT; and
18. Coordinate activities of agency security personnel, where applicable, with the DO.

H. Security Management Team

1. Collectively provides advice and support to the DO;
2. Meets on a regular basis to review the prevailing situation and ensures that security is being managed effectively at all locations throughout the country where personnel employed by the United Nations system are present;
3. Ensures that there are functioning and effective security and contingency plans which are maintained and implemented for all locations throughout the country where personnel employed by the United Nations system and their recognized dependants are present;
4. Ensures that lists of personnel and their recognized dependants are up-to-date;
5. Ensures that each ASC and Warden is trained, equipped and can carry out their responsibilities;

6. Establishes MOSS and RSMs, based on the SRM process, at all locations throughout the country where personnel employed by the United Nations system and their eligible dependants are present, including the monitoring of its implementation and compliance;
7. Ensures that resources are available to implement all measures which are approved;
8. Provides input on the performance appraisal of senior security officers employed in a country by the United Nations system where they have personnel operating, as appropriate; and
9. Addresses specific gender-related security concerns as required.

I. Area Security Coordinators

1. Act under the authority of the DO to coordinate and control the security arrangements for operations in their areas of responsibility;
2. Appoint Wardens for their areas of responsibility;
3. Develop and maintain area-specific security plans;
4. Maintain lists of personnel employed by the organizations of the United Nations system and their recognized dependants at their locations;
5. Coordinate the implementation of MOSS, based on the SRM process;
6. Keep the DO systematically informed regarding incidents or developments in their areas of responsibility which have a bearing on the security and safety of personnel employed by organizations of the United Nations system and their recognized dependants;
7. Convene meetings of the Area SMT; and
8. Manage the security clearance system for their areas of responsibility.

J. Chief Security Advisers/Security Advisers[5]

1. Serve as principal adviser to the DO and the SMT on all aspects of security management, crisis readiness and preparedness at their respective duty stations and in the execution of responsibilities with regard to the security of personnel employed by the organizations of the United Nations system and their eligible dependants, premises and assets;
2. Participate in and provide security inputs to operational planning;
3. Cooperate closely on security matters with representatives of organizations at the country level and all other officials of the United Nations system at the duty station to ensure the best possible security management;
4. Manage the security unit to include personnel, finance, budget and logistics;
5. Assist with security operations conducted by agencies as requested;

[5] The term 'Chief Security Adviser' or 'Security Adviser' applies to the senior security professional directly supporting the Designated Official. Where a Chief Security Adviser or Security Adviser is not present, this term is equivalent to the titles of Chief Security Officer and Chief of Security and Safety Services.

6. Establish and chair a Security Cell for duty stations where there are also Single-Agency Security Officers, in order to ensure that all security officers at the duty station are working together to further security management;
7. Prepare appropriate records of meetings of the Security Cell;
8. Develop contacts with national security agencies, with a view to obtaining the best possible protection for personnel employed by the organizations of the United Nations system and their recognized dependants and property;
9. Serve as a member of the SMT at the country level;
10. Undertake the SRM process for all locations in the country where personnel of the organizations of the United Nations system and their recognized dependants are present, and facilitates the implementation of recommended mitigating measures;
11. Prepare, maintain and update country-specific security plans, contingency plans and security lists of personnel employed by the organizations of the United Nations system and their recognized dependants;
12. Prepare and maintain current, feasible and implemental plans for relocation/evacuation to a safe area;
13. Maintain an effective and functioning security and emergency communications system;
14. Establish a system for briefing all personnel employed by the organizations of the United Nations system and their recognized dependants upon initial arrival, providing local security training as necessitated by changes in the security environment and ensuring such personnel are kept informed of matters affecting their security;
15. Maintain up-to-date instructions for personnel employed by the organizations of the United Nations system and their eligible dependants on precautions they should take in relation to the implementation of the security plan, including providing a comprehensive list of emergency supplies they should have on hand and providing guidance on their behaviour during emergencies, including natural disasters and political crises;
16. Report all cases in which personnel employed by the organizations of the United Nations system and/or their recognized dependants have been victims of crime;
17. Conduct security surveys of residential areas and premises;
18. Maintain an appropriate level of confidentiality regarding security matters;
19. Advise and assist the DO and the SMT in the development and implementation of MOSS and RSMs;
20. Maintain regular communication with their respective Regional Desks and submit all mandatory reports in a timely manner to UNDSS; and
21. Report to the DO and concerned representatives of organizations all instances of non-compliance with security policies, practices and procedures.

K. Country Security Focal Points (applicable in countries where there is no professional security staff assigned)

1. Manage day-to-day security-related matters supported by UNDSS;
2. Maintain up-to-date lists of personnel and their recognized dependants;
3. Prepare, maintain and update the country-specific security plan;
4. Submit all mandatory reports in a timely manner to UNDSS;
5. Immediately report all security-related incidents involving United Nations staff and their recognized dependants to the DO and UNDSS;
6. Assist the DO and SMT in the development and implementation of MOSS and RSMs, based on the SRM process;
7. Serve as a member of the SMT; and
8. Provide information on residential security to international staff.

L. Other Personnel of the United Nations Department of Safety and Security

1. Chief of Security and Safety Services/Sections

1. Provides for the security and safety of delegates, staff, visiting dignitaries and other visitors within the United Nations Headquarters and offices away from Headquarters;
2. Assists the CSA and participates in the work of the Security Cell for the development of security policies and procedures as appropriate;
3. Prepares, monitors and maintains safety and security standard operating procedures and systems; oversees emergency preparedness and crisis management, as well as conducts the SRM process;
4. Manages all human resources, finance, budget and logistical matters for his/her service/section;
5. Provides standardized and specialized training for staff and security personnel;
6. Provides personal protection for United Nations senior officials and dignitaries present and/or visiting his/her area of responsibility as required;
7. Advises and assists the DO and SMT in the development and implementation of relevant MOSS;
8. Coordinates with local authorities and local law enforcement agencies;
9. Cooperates closely with all other offices of the United Nations system at the duty station on security and safety matters to ensure the best possible security management; and
10. Retains day-to-day operational responsibility and reporting in accordance with the reporting lines established for the duty station;

2. Chief Security Officers for Peacekeeping Missions (where the Head of Mission is not the DO and a UNDSS Chief Security Adviser is present)

11. Manage the day-to-day operations of the security section and serves as the mission SA to the Head of Mission on all security-related matters;

12. Coordinate with the CSA and participates in the Security Cell for the development of security policies and procedures;
13. Contribute to the SRM process for all locations in the mission area where personnel are present and actively participates in the planning and evaluation of the effectiveness of the country security plans and other aspects of security operations;
14. Review and monitor activities related to the mission security programme and mission security plans. Identifies air and land evacuation requirements to be used in emergencies;
15. Maintain emergency communications by making periodic checks to determine if the system is operational and functioning properly;
16. Establishes a 24-hour emergency response system;
17. Maintain continuing awareness of prevailing local security conditions, identifying probable threats and advising mission and project personnel to follow appropriate preventative steps;
18. Provide personal protection for senior personnel or visiting VIPs as required;
19. Compile and maintain an updated staff list which includes all mission personnel, including visiting missions and consultants;
20. Monitor and evaluate office physical security measures, and conducts security surveys of installations and facilities;
21. Provide training and advice to mission personnel on RSMs, as well as determines the need for such resources;

3. Field Security Coordination Officers (responsible and accountable to the Chief Security Adviser/Security Adviser)

22. Implement all aspects of security management, crisis readiness and preparedness at the duty station;
23. Prepare, maintain and update country-specific security plans, contingency plans and security listings of personnel employed by organizations of the United Nations system and their recognized dependants;
24. Undertake the SRM process for all locations in the country/area where personnel employed by organizations of the United Nations system and their recognized dependants are present;
25. Establish contacts with national law enforcement agencies with a view to obtaining the best possible protection for personnel employed by the organizations of the United Nations system and their recognized dependants; and
26. Conduct security surveys of residences and premises.

M. Single-Agency Security Officers

1. Advise and assist the agency country representative or operations manager on their security responsibilities, including participation in operational planning, and provide security inputs, including information regarding compliance with United Nations security policies, practices and procedures;
2. Advise and assist the DO, ASC or CSA in the discharge of their responsibilities as required;

3. Participate as a member of the Security Cell established by the CSA/SA;
4. Advise the Security Cell on particular concerns of their organizations regarding security; and
5. Act as the CSA/SA ad interim during the absence of the CSA/SA for a given duty station, as appropriate and when required by his/her employing organization.

N. Local Security Assistants

1. Assist in monitoring the implementation of security policies and procedures;
2. Assist in supporting all matters pertaining to the safety and security of personnel, premises and assets;
3. Assist in developing security contingency plans and the country security plan;
4. Assist in the SRM process;
5. Assist in preparing MOSS and RSMs and monitoring compliance;
6. Assist in preparing contingency plans; and
7. Assist in conducting security training for United Nations personnel, locally-recruited guards and others as appropriate.

O. Wardens

1. Function as a channel of communication between the DO and personnel employed by the organizations of the United Nations system and their recognized dependants and visitors staying at hotels in their zones;
2. Regularly inform personnel regarding security arrangements and the residual security risks;
3. Undertake other security-related duties as assigned by the DO or the CSA/SA;
4. Ensures that recognized dependants left at the duty station by internationally recruited staff who are serving elsewhere are accorded the same provision for security as dependants of international staff serving at the duty station; and
5. Visit every family living in his/her area to ensure that they are aware of the security arrangements.

P. Personnel Employed by the Organizations of the United Nations System

1. Must familiarize themselves with information provided to them regarding the United Nations security management system at their location;
2. Obtain security clearance prior to traveling;
3. Attend security briefings and sign a document certifying that they have been briefed;
4. Know their Warden, CSA/SA, FSCO or CSFP;
5. Are appropriately equipped for service at the duty station;
6. Comply with all United Nations system security regulations and procedures at the duty station, both on and off duty;

7. Comport themselves in a manner which will not endanger their safety and security or that of others;
8. Report all security incidents in a timely manner;
9. Attend and complete security training relevant to their level and role; and
10. Complete the Basic Security in the Field CD-ROM and Advanced Security in the Field CD-ROM security learning programmes as appropriate.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter II

UNITED NATIONS SECURITY MANAGEMENT SYSTEM

SECTION C

Terms of Reference for the Executive Group on Security

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 5 May 2009
Technical Review: 1 May 2017

TERMS OF REFERENCE FOR THE EXECUTIVE GROUP ON SECURITY

A. Background

1. The Executive Group on Security (EGS) was established by the Chief Executive Board to facilitate the rapid decision-making capacity of the Under-Secretary-General for Safety and Security when there is an impasse or exigencies when life and limb are at stake which impacts the ability of the Designated Official (DO) or Security Management Team (SMT) to address rapidly developing or critical events which require a timely security decision.

2. The EGS may be called upon to serve the Under-Secretary-General for Safety and Security to advise and assist the Under-Secretary-General for Safety and Security, in rapidly resolving an impasse regarding the security of United Nations personnel and premises when there is no consensus within the SMT on the immediate course of action necessary at the duty station.

3. The EGS shall not meet or act as an appellate body.

B. Composition and Working Modalities

4. In addition to the Under-Secretary-General for Safety and Security, the EGS shall be composed of Executive Heads of organizations of the United Nations Security Management System (UNSMS) as follows:

(a) World Food Programme (WFP)/The Chair of the High-Level Committee on Management (HLCM);
(b) United Nations Development Programme (UNDP);
(c) Department of Peacekeeping Operations (DPKO)/Department of Field Support (DFS);
(d) Office for the Coordination of Humanitarian Affairs (OCHA);
(e) United Nations Children Fund (UNICEF);
(f) Up to two Executive Heads of United Nations organizations, ideally comprised of those with the largest operational footprint(s) and Offices away from Headquarters in the affected country.

5. Secretariat support to the EGS should be provided by Under-Secretary-General for Safety and Security.

C. Accountability of the Executive Group on Security

6. The purpose of the establishment of the EGS is to reinforce the decision-making authority and accountability of the Under-Secretary-General for Safety and Security as reflected in the Framework of Accountability (Section C).

7. The advisory role of the EGS should also be reflected in the Framework of Accountability. Within the context of the Terms of Reference of the EGS, members of the Group have an individual and collective responsibility to support the Under-Secretary-General for Safety and Security in the discharge of his/her mandate related to the safety and security of all personnel employed by the organizations of the United Nations system and their recognized dependants.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter II

UNITED NATIONS SECURITY MANAGEMENT SYSTEM

SECTION D

Inter-Agency Security Management Network (IASMN) Terms of Reference

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 21 October 2009
Technical Review: 1 May 2017

Inter-Agency Security Management Network
Terms of Reference

1. The Inter-Agency Security Management Network (IASMN) supports the High-Level Committee on Management (HLCM) in its comprehensive review of policies and resource-related issues pertaining to the entire United Nations Security Management System (UNSMS), which is a standing item on its agenda.

2. The IASMN will be chaired by the Under-Secretary-General for Safety and Security and a co-chair, who is elected among the members for a term of two years. It meets twice a year to review all existing and proposed policies, procedures and practices of the UNSMS, and it reports and makes recommendations on these to the HLCM. The Under-Secretary-General for Safety and Security or his/her designated representative should participate in these meetings.

3. The IASMN comprises the senior managers who have managerial oversight of the security function within the following bodies:

   (a) All organizations which are members of the Chief Executives Board;

   (b) Organizations that have concluded a memorandum of understanding with the United Nations for the purposes of participating in the UNSMS;

   (c) Any organization or department which has a specific mandate for management of the safety and security of United Nations staff, personnel and premises or which is directly involved in the coordination, delivery and support of United Nations activities in the field, especially during emergencies and in high-risk environments;

   (d) Any other organization invited by the Under-Secretary-General for Safety and Security, as the Chair, as observers; and

   (e) United Nations Staff Federations, as observers.

4. A Steering Group will be appointed in order to facilitate the work of the IASMN. The Steering Group will consider and propose the agenda for the IASMN meetings as well as the draft documents. The composition of the Steering Group will be reviewed and confirmed by the IASMN at its first meeting of the year.
5. Between annual meetings, the Under-Secretary-General for Safety and Security may convene working group meetings among interested organizations to discuss specific security issues. The reports of the working groups will be provided to the IASMN for review and endorsement.
6. The IASMN will monitor the implementation of United Nations security management policies, practices and procedures by all actors of the United Nations system, including the related programme budget. It will report and make recommendations thereon to the HLCM.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter II

UNITED NATIONS SECURITY MANAGEMENT SYSTEM

SECTION E

Relations with Host Countries on Security Issues

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 15 April 2012
Technical Update: 1 May 2017

A. Introduction

1. The primary responsibility for the security and protection of United Nations personnel, other individuals covered by the United Nations Security Management System (UNSMS) and the property of UNSMS organizations rests with the host Government. This responsibility flows from every Government's normal and inherent function to maintain order and to protect persons and property within its jurisdiction. In the case of the United Nations, the host Government has a special responsibility under the Charter of the United Nations and relevant agreements that the host Government may have with individual United Nations organizations.

2. Under Article 105 of its Charter, the United Nations is entitled to enjoy such privileges and immunities as are necessary for the fulfilment of its purposes. Likewise, United Nations officials are accorded with such privileges and immunities as are necessary for the independent exercises of their functions. United Nations entities and their staff, as well as some categories of non-staff personnel, enjoy similar privileges and immunities under the entities' respective constitutional instruments, international conventions and agreements with host Governments.

3. Within the territory of a State which is a party to the Conventions on the Privileges and Immunities of the United Nations and of the Specialized Agencies (together 'the Conventions'), United Nations staff members "shall be given, together with their spouse and relatives dependant on them, the same repatriation facilities in time of international crisis as diplomatic envoys"[1]. Bilateral agreements with host Governments may extend the same protections to certain categories of non-staff personnel. The Conventions further stipulate that the premises of the United Nations and United Nations entities are "inviolable" and that their property, wherever located and by whomsoever held, is immune from "any form of interference". For relevant provisions of the United Nations Charter and Conventions on the Privileges and Immunities of the United Nations and the Specialized Organizations, see Annex A.

4. References to legal instruments alone are not sufficient for ensuring host Government support in the protection of the United Nations. Therefore, while not abrogating the responsibility of the host Government for its obligations, the United Nations has a duty to reinforce and supplement the capacity of the host Government to fulfil these functions and to collaborate with the host Government to this end.

5. Security collaboration with host Governments is an integral part of the United Nations multi-dimensional strategy for the protection of United Nations personnel, property and operations.

[1] The Convention on the Privileges and Immunities of the United Nations, 1946 and the Convention on the Privileges and Immunities of the Specialized Agencies, 1947.

B. Purpose

6. The purpose of this policy is to outline the approach of the UNSMS for collaborating with host Governments as a strategic tool in security management. The policy aims to assist Designated Officials (DOs), the Security Management Team (SMT) and United Nations security professionals in enhancing collaboration with host country authorities as a key aspect of their responsibility to implement security risk management measures in collaboration with the host Governments.

7. The policy underlines the need for the DOs, the SMT and United Nations security professionals to review the host country's capacity to carry out its responsibilities for protecting the United Nations and to identify, reinforce and supplement any shortfalls in this capacity.

8. Nothing in this policy is meant to contravene UNSMS organizations' adherence to humanitarian principles as enshrined in international law.

C. Applicability and Scope

9. The policy is applicable to all the UNSMS organizations as well as all individuals defined in Chapter III of the *Security Policy Manual* (SPM) ("Applicability of the United Nations Security Management System"). All references to the United Nations herein refer to the United Nations and United Nations system organizations participating in the UNSMS.

10. The policy does not cover collaboration with de facto local authorities and/or "non-state actors" that may be in control of areas where no government authority is in place or functioning. Depending on the circumstances, it may be useful in such situations to apply the principles outlined in this policy even though non-state actors or de facto local authorities controlling areas are not host Governments.

D. Definitions

11. For the purposes of this policy, "host country" is defined as the country in which the United Nations is present and/or conducts its operations at the invitation of the Government.

12. "Host Government" refers to the Government of the host country in which the United Nations carries out its operation, activities and programmes.

E. Improving Security Collaboration with Host Governments

13. In promoting and enhancing the protection of United Nations personnel, property and operations, DOs, SMT members and United Nations security professionals must make timely efforts to collaborate with host Government authorities.

14. At the country or local level, the DOs, members of the SMT[2] and United Nations security professionals shall take appropriate measures to enhance collaboration between the United Nations and host Governments, particularly in the following areas:

(a) **Liaison.** The first priority for ensuring proper host Government support for the safety and security of the United Nations is for the DOs and the most senior security professional directly supporting the DOs[3] to maintain close liaison with the designated contacts in the Ministry of Foreign Affairs, the Ministry of Interior and security organs. This includes cooperating with relevant host Government authorities to establish mechanisms for effective sharing of security-related information (see also paragraph 14b below) for strengthening the analysis of security threats and risks with implications for staff security, and for ensuring that privileged information is handled with appropriate discretion. The DOs shall request the host Government designate focal points with whom the United Nations can cooperate on a regular basis on security matters that impact staff security.

(b) **Information Sharing and Strategic Communication**. Two-way information exchange is central to the cooperation between the United Nations and the host Government, and it is an integral part of the UNSMS. Emphasis should be placed on situational awareness, analysis of threats and vulnerabilities regarding United Nations personnel, premises and operations, and strategies for communication with the local population and other target audiences to promote understanding of the United Nations mandates and activities. There should be regular information exchange meetings between host Government focal points in the Ministry of Foreign Affairs, Ministry of Interior and other relevant security organs of the host Government and the DOs and the most senior security professional directly supporting the DOs.

(c) **Security Risk Management Measures**. Attention should be paid to host Government assistance with, and implementation of, security risk management measures, especially with regard to United Nations premises and the import and licensing of security-related equipment. The assessment of security risks faced by the United Nations in any country at any given time, and what is required to manage them, may differ significantly between the host Government and the United Nations. Exchange of information and regular consultations eliminate differences and enable mutually agreed prevention and mitigation measures. Collaboration with host Government

[2] For designated security areas within a country, these provisions apply to Area Security Coordinators and Area Security Management Teams.

[3] This is usually the Chief Security Adviser (CSA) or other Security Adviser (SA), or their officer-in-charge *ad interim*. Where a CSA or SA is not present, this term is equivalent to the titles of Chief Security Officer, Chief of Security and Safety Services, Country Security Focal Point (CSFP) or Local Security Assistant (if necessary in countries where no international professional security adviser has been assigned or is present).

authorities must include periodic assessments of access control to, and external physical security of all United Nations premises and concrete action on the implementation of security management measures. Collaboration should also focus on timely customs clearance and licensing of security-related equipment required for the safety and security of the United Nations in that country. The host Government must provide the required resources for the safety and security of United Nations personnel, property and operations. Part of ensuring the necessary level of protection for the United Nations should include regular coordination meetings with host Government authorities (both within the Ministry of Foreign Affairs and Ministry of Interior) by both the DOs and the most senior security professional directly supporting the DOs.

(d) **Crisis Management**. As part of security risk management, planning and preparedness for the management of security crises affecting the United Nations is an important aspect of collaborating with host Government authorities. To enable the Government to respond effectively in a crisis, the DOs shall request the host Government designate focal points with the authority to mobilize and coordinate support when a crisis affects the United Nations in the country. Central to collaboration on crisis management is host Government provision of emergency contacts, procedures and resources. It is also important to assess the capacity of host Government authorities to respond to events that can adversely affect the security of United Nations personnel, premises or operations. Part of this assessment shall include an annual crisis response exercise/drill.

(e) **Legal Aspects**. Collaboration with host Government authorities should aim to ensure that crimes committed against United Nations personnel are investigated and perpetrators identified and prosecuted according to the law. Each representative of the UNSMS organizations in-country must ensure that their respective personnel are aware of and respect national laws and customs. The DOs, in conjunction with the respective representative of the UNSMS organizations in-country, shall bring to the attention of the host Government as soon as possible any concerns regarding arrests, detention or harassment of United Nations personnel or any obstruction to freedom of movement of United Nations personnel.

(f) **Concerns for Specific Categories of Personnel**. Collaboration with host Government authorities should include gender-related security issues and the special circumstances of locally-recruited personnel. It is important to ensure that host Government counterparts understand the status of locally-recruited United Nations staff and non-staff personnel under international law.

F. Roles and Responsibilities

15. DOs, SMT members and United Nations security professionals are responsible for implementing this policy as part of their security management responsibilities. All managers of the UNSMS are also responsible for carrying out their security

management functions concerning collaboration with host Government authorities on security-related issues in line with this policy and other relevant policies, including the security risk management policy.

16. The DOs have the responsibility to liaise with host Government authorities or other relevant authorities in all aspects of security management on behalf of the United Nations and to consult, as necessary, with the Under-Secretary-General for Safety and Security in implementing this policy. The DOs are responsible for adapting this policy to the local context.
17. The DOs and heads of UNSMS organizations must ensure that appropriate financial resources are forecasted and allocated to carry out this policy.
18. Heads of UNSMS organizations are responsible for informing their respective personnel of the policy on host country matters with the aim to enhance collaboration with host Government authorities as part of the security risk management to protect United Nations personnel, property and operations.
19. Security Advisers shall support the DOs and SMT members in carrying out this policy and related measures and providing technical advice on whether all required security risk management measures related to this policy are in place and effective.

G. Requirements for Review and Reporting

20. The DOs and the SMT, supported by the security advisers, must carry out regular assessment and review of host Government collaboration on issues related to the security of the United Nations.

21. Where a host Government has not adequately addressed aspects of its responsibility to provide for the safety and security of United Nations personnel, property or operations (with special emphasis on the priority areas listed in paragraph 14 above), the DO must take timely action to seek host Government support to put in place the appropriate measures. If host Government support continues to be inadequate, the DO must report this to the Under-Secretary-General for Safety and Security to request strategic interventions at the appropriate level.

22. If any in-country actors within the UNSMS require clarification on their responsibilities regarding host Government collaboration or require additional technical or operational support, they must contact their respective headquarters in a timely manner.

H. Training Requirements

23. This policy shall be included in the mandatory security training for the DOs, SMT members, security professionals and managers in the United Nations system organizations who have responsibility for security management in line with the Framework of Accountability.

I. Final Provisions

24. This policy is to be distributed to all United Nations personnel.

25. This policy enters into effect on 15 April 2012.

26. *Field Security Handbook* (2006), Chapter IV, Section A, paragraphs 4.1 – 4.4 and *Field Security Handbook* (2006) Annex A are hereby abolished.

Annex A

RELEVANT EXTRACTS OF THE CHARTER OF THE UNITED NATIONS
Charter of the United Nations

Article 104

The Organization shall enjoy in the territory of each of its Members such legal capacity as may be necessary for the exercise of its functions and the fulfilment of its purposes.

Article 105

1 The Organization shall enjoy in the territory of each of its Members such privileges and immunities as are necessary for the fulfilment of its purposes.

2 Representatives of the Members of the United Nations and officials of the Organization shall similarly enjoy such privileges and immunities as are necessary for the independent exercise of their functions in connection with the Organization.

3 The General Assembly may make recommendations with a view to determining the details of the application of paragraphs 1 and 2 of this Article or may propose conventions to the Members of the United Nations for this purpose.

RELEVANT EXTRACTS OF THE CONVENTION ON THE PRIVILEGES AND IMMUNITIES OF THE UNITED NATIONS ADOPTED BY THE GENERAL ASSEMBLY ON 13 FEBRUARY 1946

Article V

OFFICIALS

Section 17

The Secretary-General will specify the categories of officials to which the provisions of this Article and Article VII shall apply. He shall submit these categories to the General Assembly. Thereafter these categories shall be communicated to the Governments of all Members. The names of the officials included in these categories shall from time to time be made known to the Governments of Members.

Section 18

Officials of the United Nations shall:

a) Be immune from legal process in respect of words spoken or written and

all acts performed by them in their official capacity;

b) Be exempt from taxation on the salaries and emoluments paid to them by the United Nations;

c) Be immune from national service obligations;

d) Be immune, together with their spouses and relatives dependent on them, from immigration restrictions and alien registration;

e) Be accorded the same privileges in respect of exchange facilities as are accorded to the officials of comparable ranks forming part of diplomatic missions to the Government concerned;

f) Be given, together with their spouses and relatives dependent on them, the same repatriation facilities in time of international crisis as diplomatic envoys;

g) Have the right to import free of duty their furniture and effects at the time of first taking up their post in the country in question.

Section 19

In addition to the immunities and privileges specified in Section 18, the Secretary-General and all Assistant Secretaries-General shall be accorded in respect of themselves, their spouses and minor children, the privileges and immunities, exemptions and facilities accorded to diplomatic envoys, in accordance with international law.

Section 20

Privileges and immunities are granted to officials in the interests of the United Nations and not for the personal benefit of the individuals themselves. The Secretary-General shall have the right and the duty to waive the immunity of any official in any case where, in his opinion, the immunity would impede the course of justice and can be waived without prejudice to the interests of the United Nations. In the case of the Secretary-General, the Security Council shall have the right to waive immunity.

Section 21

The United Nations shall co-operate at all times with the appropriate authorities of Members to facilitate the proper administration of justice, secure the observance of police regulations and prevent the occurrence of any abuse in connection with the privileges, immunities and facilities mentioned in this Article.

Article VI

EXPERTS ON MISSIONS FOR THE UNITED NATIONS

Section 22

Experts (other than officials coming within the scope of Article V) performing missions for the United Nations shall be accorded such privileges and immunities as are necessary for the independent exercise of their functions during the period of their missions, including the time spent on journeys in connection with their missions. In particular they shall be accorded:

a) Immunity from personal arrest or detention and from seizure of their personal baggage;

b) In respect of words spoken or written and acts done by them in the course of the performance of their mission, immunity from legal process of every kind. This immunity from legal process shall continue to be accorded notwithstanding that the persons concerned are no longer employed on missions for the United Nations;

c) Inviolability for all papers and documents;

d) For the purpose of their communications with the United Nations, the right to use codes and to receive papers or correspondence by courier or in sealed bags;

e) The same facilities in respect of currency or exchange restrictions as are accorded to representatives of foreign governments on temporary official missions; and

f) The same immunities and facilities in respect of their personal baggage as are accorded to diplomatic envoys.

Section 23

Privileges and immunities are granted to experts in the interests of the United Nations and not for the personal benefit of the individuals themselves. The Secretary-General shall have the right and the duty to waive the immunity of any expert in any case where, in his opinion, the immunity would impede the course of justice and it can be waived without prejudice to the interests of the United Nations.

Chapter II

UNITED NATIONS SECURITY MANAGEMENT SYSTEM

SECTION F

Role of the Department of Safety and Security

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 18 April 2016
Technical Review: 1 May 2017

United Nations ST/SGB/2013/5

Secretariat

5 August 2013

Secretary-General's bulletin

Organization of the Department of Safety and Security

The Secretary-General, pursuant to Secretary-General's bulletin ST/SGB/1997/5, entitled "Organization of the Secretariat of the United Nations", as amended by ST/SGB/2002/11, and pursuant to General Assembly resolution 59/276 on questions relating to the programme budget for the biennium 2004-2005, and for the purpose of establishing the organizational structure of the Department of Safety and Security, promulgates the following:

Section 1
General provision and definitions

1.1 The present bulletin shall apply in conjunction with Secretary-General's bulletin ST/SGB/1997/5, entitled "Organization of the Secretariat of the United Nations", as amended by ST/SGB/2002/11.

1.2 For the purposes of the present bulletin, the following definitions shall apply:

The "United Nations Security Management System" means the strengthened and unified United Nations security management system instituted by the Secretary-General pursuant to General Assembly resolution 59/276, section XI, paragraphs 4 and 16, adopted on 23 December 2004. The United Nations Security Management System is comprised of the United Nations Secretariat, offices away from Headquarters, regional commissions and international tribunals, as well as the agencies, funds and programmes of the United Nations system.

The "Inter-Agency Security Management Network" is a working group of the High-Level Committee on Management designed with the goal of enabling the effective and efficient conduct of United Nations activities while ensuring the security, safety and well-being of staff as a high priority.

Section 2
Functions and organization

2.1 The Department of Safety and Security:

13-41804 (E) 120813
1341804

(a) Strengthens the United Nations Security Management System by enabling the safest and most efficient conduct of the programmes and activities of the United Nations system and by providing leadership, operational support and oversight of the United Nations Security Management System;

(b) Provides leadership, strategic guidance and an integrated coordination framework to enable the conduct of United Nations activities while ensuring the safety, security and well-being of personnel and the security of United Nations premises and assets;

(c) Provides security expertise to all United Nations Security Management System entities to enable the planning and safe conduct of mandates, missions, activities and programmes of the United Nations system;

(d) Leads the concerted development, across the United Nations Security Management System entities, of standardized security policies and procedures through an integrated and interdependent organizational approach by working closely with the security services of all the United Nations Security Management System entities, under the umbrella of the Inter-Agency Security Management Network;

(e) Delivers integrated, efficient and coherent security support to United Nations field operations, drawing together standardized policy, field support and other critical elements, and links with other United Nations entities, including through its leadership, to address safety and security needs, particularly in the case of crisis or emergency;

(f) Ensures effective security risk management through the establishment of a coordinated security threat and risk assessment mechanism within the framework of a common system-wide methodology;

(g) Identifies and evaluates the security-related threats and risks faced by the United Nations civilian personnel when delivering their programmes as mandated by the General Assembly and the Security Council;

(h) Ensures a coherent, effective and timely response to all security-related threats and other emergencies;

(i) Leads and supports the cooperation and collaboration among United Nations Security Management System entities, including their headquarters and field offices, in the planning and implementation of measures aimed at improving staff security, training and awareness;

(j) Promotes and coordinates strategic and operational partnerships within the United Nations Secretariat and with other organizations in the United Nations system, regional organizations and other multilateral and bilateral institutions and Member States to ensure that appropriate security measures are an integral part of the planning for existing and newly mandated United Nations operations;

(k) Provides leadership, oversight, strategic guidance and technical support to the Security and Safety Services of all entities of the Secretariat in New York and to the Offices away from Headquarters, regional commissions and international tribunals, by agreement;

(l) Establishes, oversees and maintains the necessary capacity to ensure the systematic and coordinated management of the need for close protection throughout the United Nations Security Management System;

(m) Guides and promotes gender-sensitive approaches to the planning, design and implementation of policies and operational activities led by the Department and takes action to promote gender balance at all levels and ensure a gender-friendly work environment at Headquarters and in the field.

2.2 The Department of Safety and Security is composed of the Office of the Under-Secretary-General for Safety and Security, the Division of Headquarters Security and Safety Services, the Division of Regional Operations and the Field Support Service.

2.3 The Department is headed by the Under-Secretary-General for Safety and Security. In performing his/her functions, the Under-Secretary-General is supported by the Assistant Secretary-General. The Under-Secretary-General, the Assistant Secretary-General and the officials in charge of each organizational unit perform the specific functions set out in the present bulletin.

2.4 To ensure coherence and, where appropriate, coordination with non-United Nations partners, the Department maintains the following mechanisms:

(a) Strategic cooperation frameworks and regular communication with regional and subregional organizations and international institutions on security-related issues;

(b) Modalities for coordination and information-sharing for all safety and security-related matters;

(c) Regular strategic dialogue and exchange with United Nations partners through meetings of the Secretary-General's Policy Committee, the Executive Committee on Peace and Security and other relevant senior management forums.

Section 3
Under-Secretary-General for Safety and Security

3.1 The Under-Secretary-General for Safety and Security is accountable to the Secretary-General.

3.2 The Under-Secretary-General is responsible for all activities of the Department of Safety and Security. The core strategic functions of the Under-Secretary-General include:

(a) Advising the Secretary-General on all matters related to the security and safety of personnel, premises and assets of the United Nations;

(b) Representing or ensuring the representation of the Secretary-General on all security-related matters with governing bodies, agencies, funds and programmes of the United Nations common system and administrative advisory bodies;

(c) Preparing reports of the Secretary-General on all security-related matters;

(d) Maintaining close liaison with the host countries' authorities and Member States to strengthen and implement the host countries' primary responsibility for the safety and security of United Nations personnel, premises and assets;

(e) Leading and managing the Department of Safety and Security, and providing executive direction and control of the United Nations Security Management System and ensuring the overall safety and security of United Nations personnel, their eligible family members and United Nations premises and assets at headquarters locations and in the field;

(f) Coordinating with the organizations of the United Nations Security Management System to ensure implementation, compliance and support for security aspects of their activities;

(g) Convening and chairing meetings of the Inter-Agency Security Management Network and the Executive Group on Security;

(h) Overseeing the development of security policies, practices and procedures for the United Nations Security Management System worldwide;

(i) Providing oversight, strategic policy and operational guidance to the Designated Officials for Security appointed by the Secretary-General and other field representatives deployed by the United Nations Security Management System entities;

(j) Taking all necessary measures on behalf of the Secretary-General, in coordination with the United Nations Security Management System, to ensure that United Nations personnel are properly informed about, and operate in conformity with, existing policies, minimum operating security standards and relevant codes of conduct, are trained and duly authorized in the areas of safety and security.

Section 4
Assistant Secretary-General for Safety and Security

4.1 The Assistant Secretary-General for Safety and Security is accountable to the Under-Secretary-General for Safety and Security.

4.2 The core functions of the Assistant Secretary-General include:

(a) Supporting the Under-Secretary-General in the full range of his/her responsibilities, including assuming responsibility for all operational activities of the Department related to tasking, planning the optimum use of resources, expertise and experience, and overseeing and assisting the Department's senior leadership in the discharge of their functions;

(b) Maintaining liaison with Designated Officials, representatives of Member States, regional groups, host Government authorities and other senior leadership within the scope of the United Nations Security Management System, both at Headquarters and field locations;

(c) Supervising and overseeing the Executive Office in carrying out its delegated financial, personnel and general administrative responsibilities;

(d) Overseeing and strengthening the day-to-day, internal management of the Department, as well as representing the Department in the absence of the Under-Secretary-General;

(e) Supporting the Under-Secretary-General in the performance of his/her functions as executive head of the Department, including by coordinating the work of various units both at Headquarters and in the field and overseeing the preparation of reports to intergovernmental bodies;

(f) Overseeing the work of the Policy and Compliance Service, the Field Support Service and the Executive Office.

Section 5
Office of the Under-Secretary-General for Safety and Security

5.1 The Office of the Under-Secretary-General consists of the front office, the Policy and Compliance Service and the Executive Office.

5.2 The front office of the Under-Secretary-General provides support to the Under-Secretary-General and the Assistant Secretary-General in carrying out their functions, which include the coordination of the work of the various units at Headquarters and in the field and overseeing the preparation of reports to intergovernmental bodies.

Policy and Compliance Service

5.3 The Policy and Compliance Service is headed by a Chief, who is accountable to the Assistant Secretary-General. The Service consists of the Compliance, Evaluation and Monitoring Section and the Policy, Planning and Coordination Unit, each of which is headed by a Chief, who is accountable to the Chief of Service.

5.4 The Chief of the Service and the Chief of the Policy, Planning and Coordination Unit serve as the secretariat for the Inter-Agency Security Management Network and are accountable to the Assistant Secretary-General. The secretariat for the Inter-Agency Security Management Network provides inputs to the Under-Secretary-General.

5.5 The core functions of the Policy, Planning and Coordination Unit include:

(a) Reviewing and recommending policies and guidelines required for the United Nations Security Management System;

(b) Producing substantive policy documents and providing review of policy drafts prepared by other United Nations organizations on safety and security-related matters;

(c) Producing reports of a substantive nature to the legislative organs of the United Nations on behalf of the Department on safety and security-related matters;

(d) Enhancing the coordination and integration of, and compliance with, policies and procedures within the United Nations Security Management System.

5.6 The core functions of the Compliance, Evaluation and Monitoring Section include:

(a) Monitoring and evaluating the implementation of, and compliance with, security policy, procedures and guidelines of the United Nations Security Management System;

(b) Advising members of the United Nations Security Management System on compliance-related matters;

(c) Planning, coordinating and conducting inspections and compliance managerial reviews;

(d) Advising on the development of security compliance training in close collaboration with the Training and Development Section;

(e) Conducting strategic and thematic evaluations and promoting knowledge management, including lessons learned and best practices in safety and security-related matters.

Executive Office

5.7 The Executive Office is headed by an Executive Officer, who is accountable to the Under-Secretary-General.

5.8 The core functions of the Executive Office are set out in section 7 of Secretary-General's bulletin ST/SGB/1997/5.

5.9 The Executive Office undertakes inter- and intradepartmental coordination on issues relating to human resources, budgetary, logistics and general administrative matters, including at the inter-agency level, as they relate to the area of safety and security.

5.10 The Executive Office coordinates with the United Nations Development Programme, the Department of Field Support and the Department of Peacekeeping Operations on the administration and support provided to the Department of Safety and Security field offices and with the local administrations of the Offices away from Headquarters and the regional commissions to ensure consistency in the administrative practices of the local security and safety services.

Section 6
Division of Regional Operations

6.1 The Division of Regional Operations is headed by a Director, who is accountable to the Under-Secretary-General. The Division consists of the Threat and Risk Assessment Unit, the Peacekeeping Operations Support Section and the Regional Sections.

6.2 The Division of Regional Operations is responsible for the management of regional operations for safety and security and serves as the safety and security focal point for field duty stations, providing primary operational and technical support, including:

(a) Providing technical advice and guidance to Designated Officials for Security, Security Management Teams and Security Advisers according to existing policies and guidelines, best practices and lessons learned, and to assist them in the discharge of their functions and responsibilities for security;

(b) Effectively coordinating safety and security matters in the field with United Nations Security Management System entities, including agencies, funds and programmes;

(c) Coordinating with the Department of Peacekeeping Operations, the Department of Political Affairs and the Office for the Coordination of Humanitarian Affairs on the planning, implementation and review of safety and security programmes for peacekeeping, humanitarian and other special missions in the field;

(d) Ongoing monitoring and evaluation of the effectiveness, efficiency and coherence of existing security arrangements, procedures, modalities and practices in field duty stations;

(e) Coordinating contingency planning and crisis preparedness and timely response in field duty stations to security crises;

(f) Developing security requirements and arrangements for new missions as well as for special, regular and emergency operations;

(g) Programme and budget planning for regional operations to ensure the deployment of critical security resources to locations with the highest requirements, including the planning and administration of surge deployment.

6.3 The Division of Regional Operations is also responsible for management of the Communications Centre, which, for the purpose of timely information-sharing, is geographically co-located within the United Nations Operations and Crisis

Centre, a jointly staffed Secretariat-wide crisis and coordination centre. The core functions of the Communications Centre include:

(a) Maintaining round-the-clock emergency communications at Headquarters and with field duty stations on security matters;

(b) Organizing round-the-clock dispatch of official correspondence, including communiqués, security clearances and other official communications of the Department of Safety and Security and videoteleconferences between Headquarters and field duty stations;

(c) Providing operational support to the United Nations Operations and Crisis Centre, as well as with Regional Sections and the Peacekeeping Operations Support Section in crisis situations;

(d) Round-the-clock monitoring of open media sources to provide timely alerts on evolving events and developments that may impact on the safety and security of the United Nations system worldwide.

6.4 The Threat and Risk Assessment Unit is headed by a Chief, who is accountable to the Director of the Division. The core functions of the Threat and Risk Assessment Unit include:

(a) Identifying, in a timely manner, developing threats that may affect civilian personnel, assets and operations of the organizations of the United Nations system;

(b) Developing strategic, regional and country-specific security threat and risk assessments as required by the Department, Division and other actors of the United Nations Security Management System;

(c) Providing analytical and assessment support to other sections of the Division and field duty stations in the review of threat and risk assessments;

(d) Developing methodologies for security analysis and the training of security analysts in the field and methodological support and oversight over the outputs of security analysts in the field;

(e) Developing and distributing timely security threat information to all actors of the United Nations Security Management System at Headquarters and in the field;

(f) Developing security risk assessments for activities and travel conducted by Senior United Nations Officials, including development of Personal Security Risk Assessments.

6.5 The Peacekeeping Operations Support Section is headed by a Chief, who is accountable to the Director/Deputy Director of the Division. The core functions of the Peacekeeping Operations Support Section include:

(a) Providing effective security support to Integrated Operational Teams and other mission-focused work groups of the Department of Peacekeeping Operations;

(b) Coordinating security issues with the Department of Field Support;

(c) Ensuring that peacekeeping missions have complied with all United Nations security management policies and guidelines.

6.6 Each of the Regional Sections is headed by a Chief, who is accountable to the Director/Deputy Director of the Division. Both the Regional Sections and the Peacekeeping Operations Support Section are responsible for the day-to-day

management of security operations in the field in countries and areas under their responsibilities, including:

(a) Coordinating daily with Designated Officials for Security and Security Advisers in the field on all security-related issues affecting United Nations personnel, assets and operations;

(b) Reviewing and endorsing Security Risks Assessments, Security Plans, Minimum Operating Security Standards and Residential Security Measures, and ongoing review of security levels wherever United Nations operations occur;

(c) Ensuring adequate contingency planning in the field, identifying possible crisis scenarios, plans of action, response strategies, required resources and arrangements;

(d) Developing crisis response strategies and provision of crisis response assistance, technical advice and guidelines to the field in contingency situations resulting from safety and security accidents and incidents;

(e) Coordinating with the Department of Peacekeeping Operations, the Department of Political Affairs and the Office for the Coordination of Humanitarian Affairs in the planning, implementation and review of safety and security programmes for peacekeeping, humanitarian and other special missions in the field;

(f) Monitoring compliance with security policies, procedures and modalities and implementation of Minimum Operating Security Standards and Residential Security Measures at field duty stations and by security components of peacekeeping operations and other special missions in the field, in close coordination with the Compliance, Evaluation and Monitoring Section.

Section 7
Division of Headquarters Security and Safety Services

7.1 The Division of Headquarters Security and Safety Services is headed by a Director, who is accountable to the Under-Secretary-General.

7.2 The Division consists of the Protection Coordination Unit and the Security and Safety Services/Sections located at United Nations Headquarters in New York, the Offices away from Headquarters, the regional commissions and the international tribunals.

7.3 The Division of Headquarters Security and Safety Services is responsible for the strategic management of safety and security operations at the Security and Safety Services/Sections locations, providing primary operational and technical support, including:

(a) Providing technical advice and guidance to Directors General, Executive Secretaries and Registrars of the Security and Safety Services/Sections locations, and Chiefs of Security Advisers according to existing policies and guidelines, sharing best practices and lessons learned, assisting in the discharge of their functions and responsibilities for security;

(b) Providing the framework to ensure standardization, and the integration of, practices and procedures in the Security and Safety Services/Sections;

(c) Acting as the focal point for consultation and advice within the Secretariat and with specialized agencies of the United Nations system regarding all security and safety policy issues, in particular the provision of security and safety

operations at any United Nations system premises by providing policy direction and standards;

(d) Ongoing monitoring and evaluation of the effectiveness, efficiency and coherence of existing security arrangements, procedures, modalities and practices at the Security and Safety Services/Sections locations;

(e) Coordinating contingency planning and crisis preparedness and timely response at the Security and Safety Services/Sections locations;

(f) Advising on and coordinating security support for planning and implementing security arrangements for special events organized or sponsored by United Nations Security Management System organizations at locations and venues external from their headquarters;

(g) Closely collaborating with the Executive Office, acting as focal point for advice within the Division's responsibilities, on administrative matters such as budget and human resources issues as needed.

7.4 The Protection Coordination Unit is headed by a Chief, who is accountable to the Director of the Division. The core functions of the Protection Coordination Unit include:

(a) Developing a global repository of United Nations Security Management System policy and guidance to support the delivery of protective services while maintaining strategic oversight of all aspects of protective services operations within the United Nations system;

(b) Providing requisite guidance and oversight for global protective service operations for Senior United Nations Officials in a systematic and coordinated manner by identifying United Nations close protection assets to meet operational needs;

(c) Monitoring policy and guideline implementation and providing direction to resolve any failings by ensuring regular updating of an assignment and travel-tracking mechanisms of Senior United Nations Officials;

(d) Acting as the focal point for consultation and advice to other United Nations Security Management System entities, regarding all issues affecting the provision of protective services;

(e) Developing a strategic human resources platform from which the United Nations system can recruit protective services officers;

(f) In close consultation with the Division of Field Support Service, supporting the development and implementation of a robust training programme for officers delivering protective services within the United Nations system.

7.5 Each Security and Safety Service/Section at United Nations Headquarters in New York, the Offices away from Headquarters, the regional commissions and the international tribunals is headed by a Chief, who is accountable to the Director of the Division as well as the Director General/Executive Secretary or his/her designee.

7.6 The core functions of the Security and Safety Services/Sections include:

(a) In accordance with the policies and guidelines of the United Nations Security Risk Management process, professionally managing risk utilizing state-of-the-art practices to establish a safe and secure environment for representatives, United Nations personnel and visitors at the designated United Nations premises, enabling the implementation of programmes;

(b) Protecting organizational assets by continuous review of vulnerabilities and developing and implementing appropriate and cost-effective risk mitigation strategies utilizing human resources and innovative technologically based applications solutions;

(c) In the context of organizational enterprise risk management, developing and exercising scenario-specific emergency preparedness response plans for significant natural and man-made situations as part of crisis management and business continuity;

(d) Maintaining liaison with local law enforcement authorities to facilitate cooperation and adherence to the relevant requirements for protection of United Nations personnel and assets, in accordance with respective host country agreements at the various duty stations;

(e) Providing specialized services, including protective services to Senior United Nations Officials and visiting dignitaries, investigatory capability, risk assessment functionality, hostile surveillance detection, information security and medical response;

(f) Providing security managers and personnel to assist United Nations organizations holding special events and external conferences at locations and venues away from United Nations premises.

Section 8
Division of Field Support Service

8.1 The Division of Field Support Service is headed by a Chief, who is accountable to the Assistant Secretary-General. The Service consists of the Training and Development Section, the Critical Incident Stress Management Unit, the Aviation Risk Management Office and the Crisis Management Information Support Section.

8.2 The Training and Development Section is headed by a Chief, who is accountable to the Chief of the Service, and its core functions are as follows:

(a) Managing the development and implementation of a United Nations security knowledge transfer and training strategy for all target groups within the United Nations Security Management System;

(b) Based on competencies and the roles and responsibilities identified in the framework of accountability for the United Nations Security Management System, developing knowledge transfer and training objectives, standards and programmes of instruction for all actors in the United Nations Security Management System;

(c) Evaluating skill requirements and identifying training needs for effective security management;

(d) Delivering training, including core and specialist courses for the United Nations Security Management System based on the security training strategy as defined by the Inter-Agency Security Management Network's Working Group on Security Training;

(e) Evaluating, validating and reviewing security training policy and measuring its ongoing relevance against established standards and policies, to ensure it meets the needs of the United Nations Security Management System.

8.3 The Critical Incident Stress Management Unit is headed by a Chief, who is accountable to the Chief of the Service. The core functions of the Critical Incident Stress Management Unit include:

(a) Developing and implementing a comprehensive United Nations policy regarding the management of critical incident stress, including gender-specific requirements;

(b) Ensuring inter-agency coordination regarding critical incident stress management;

(c) Providing a rapid professional response to critical incidents involving personnel in the organizations of the United Nations Security Management System;

(d) Providing or facilitating the provision of critical incident stress management training for United Nations personnel in the organizations of the United Nations Security Management System;

(e) Maintaining a roster of stress counsellors available for deployment, as required;

(f) Researching, assessing and monitoring factors that may lead to stress-related problems in the field;

(g) Chairing the Inter-Agency Security Management Network's Working Group on Critical Incident Stress Management.

8.4 The Aviation Risk Management Office is headed by an Aviation Risk Management Officer, who is accountable to the Chief of the Service. The core functions of the Aviation Risk Management Office include:

(a) Providing advice to all actors in the United Nations Security Management System on the relative safety of commercial scheduled airlines;

(b) Developing a methodology and process to evaluate airlines, taking into consideration the unique circumstances and travel habits of the members of the United Nations common system;

(c) Developing a process to assess airlines, as requested by the United Nations Security Management System.

8.5 The Crisis Management Information Support Section is headed by a Chief, who is accountable to the Chief of the Service. The core function of the Crisis Management Information Support Section is managing systems, including an automated security clearance mechanism for the travel of United Nations system personnel and information management tools that provide security-related information to security professionals, security management teams and United Nations system personnel worldwide.

Section 9
Final provisions

9.1 The present bulletin shall enter into force on the date of its issuance.

9.2 The Secretary-General's bulletin of 1 June 1998, entitled "Organization of the Office of Central Support Services" (ST/SGB/1998/11, section 5, Security and Safety Service), is hereby abolished.

(*Signed*) **BAN** Ki-moon
Secretary-General

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter II

UNITED NATIONS SECURITY MANAGEMENT SYSTEM

SECTION G

Saving Lives Together

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 14 April 2014
Technical Review: 1 May 2017

A. Introduction

1. The Saving Lives Together framework (herein referred to as "the Framework")[1] was established by the Inter-Agency Standing Committee (IASC) to improve cooperation on security issues between the United Nations, non-governmental organizations (NGOs) and international non-governmental organizations (INGOs) that are implementing and/or operational partners of the United Nations. The Framework provides a collaborative approach to security management, particularly humanitarian operations in complex environments.

B. Purpose

2.The purposes of this policy are as follows:

(a) To reaffirm the commitment of all actors in the United Nations Security Management System (UNSMS) to security collaboration with relevant NGOs.

(b) To reaffirm the importance of the Saving Lives Together Framework and ensure support, within available resources, for the implementation of the Framework at all levels within the UNSMS.

(c) To outline the general approach of the UNSMS for using the Framework as a tool for collaborating with relevant NGOs.

(d) To assist Designated Officials (DOs), Security Management Teams (SMTs), United Nations security professionals and United Nations system organizations in their collaboration with relevant NGOs as a part of their security management responsibilities.

C. Applicability

3. The policy is applicable to all organizations and actors within the UNSMS.

4. Nothing in this policy contradicts the adherence to common humanitarian ground rules, including the need to maintain the neutrality and impartiality of humanitarian activities.

[1] Saving Lives Together "*A Framework for Improving Security Arrangements among IGOs, NGOs and the UN in the Field*", Rev. 2011. Since 2001, the United Nations Inter-Agency Standing Committee (IASC)[1] has examined best practices for security collaboration between the United Nations and non-United Nations organizations. Those best practices formed the basis for the Saving Lives Together framework, developed by the IASC. In 2006, the United Nations High-Level Committee on Management (HLCM) and the IASMN (in Vienna in May 2006) approved the Saving Lives Together framework (ref: CEB/2006/HLCM/12/CRP.2). In August 2011, the IASC endorsed a review of the Framework. In October 2011, participants in the Second Saving Lives Together Conference, held in Geneva, endorsed the revised Saving Lives Together Framework, followed by the IASMN's endorsement of the revised Framework in February 2012 at its 17th regular session. In October 2015, the United Nations Office for the Coordination of Humanitarian Affairs, the United Nations Department of Safety and Security and the United Nations Development Programme jointly issued a revised Saving Lives Together Framework. In October 2016, the HLCM approved revisions of the Programme Criticality Framework, followed by the endorsement of the Chief Executives Board for Coordination (CEB) in November 2016. The revised Framework, in line with the Secretary-General's decision (PC/2016/1), is a mandatory policy of the Organization in areas where security risk levels are "high" or above. The Designated Official is accountable for using the results of the Programme Criticality Assessment and for endorsing security risk management decisions taken at country-level, taking both the Programme Criticality and the results of the Security Risk Management process into consideration.

D. Scope

5. At the country or mission level, the DOs, Area Security Coordinators (ASCs), members of the SMT[2] and security professionals should take measures to enhance collaboration with relevant NGOs , in consultation with host Governments, in accordance with the staged approach to security collaboration as described in the IASC-endorsed Saving Lives Together framework (attached).[3]

6. The policy is to be implemented taking into account the specific context in which the UNSMS operates. Depending on the specific local context and the discretion of the DOs, the UNSMS collaboration with the NGOs may include other NGOs which are implementing partners of the United Nations.

E. Roles and Responsibilities

7. DOs, SMT members, ASCs and managers with security responsibilities in organizations in the UNSMS are responsible for implementing this policy and relevant operational guidelines as part of their security management responsibilities.

8. The DO is responsible for promoting the principles of the Framework and implementing measures identified in this policy while adapting the Framework's elements to the specific local context and available resources.

9. Security Advisers shall support the DOs and SMT members and provide technical advice in implementing this policy.

10. Executive Heads of UNSMS organizations are responsible for informing their respective personnel of this policy.

F. Requirement for Review and Reporting

11. The DO and the SMT, supported by security professionals, should regularly assess the capacity of the local UNSMS to support the implementation of this policy.

12. If any actors within the UNSMS, in-country or in a mission area, require clarification on their responsibilities regarding this policy or require additional technical or operational support they are to inform their respective headquarters in a timely manner.

G. Training and Compliance

13. This policy constitutes part of the mandatory training for DOs, SMT members, security professionals and managers in the UNSMS organizations who have security management responsibilities in line with the Framework of Accountability for the UNSMS.

14. All actors within the UNSMS should be made familiar with and are requested to abide by this policy.

[2] For designated security areas within a country or mission, these provisions also apply to ASCs and Area Security Management Teams.
[3] Saving Lives Together "*A Framework for Improving Security Arrangements among IGOs, NGOs and the UN in the Field*", Rev. 2015.

H. Final Provisions

15. This policy is to be distributed to all United Nations personnel.

16. This policy enters into force on 14 April 2014.

SAVING LIVES TOGETHER

"A Framework for improving Security Arrangements among International Non-Governmental Organizations/International Organizations and the United Nations"

October 2015

Objectives and Principles

Saving Lives Together, or SLT, is a series of recommendations aimed at enhancing security collaboration between the United Nations, International Non-Governmental Organizations and International Organizations ("SLT partner organizations"). It recognizes the collectively experienced security threats and the importance of collaboration to ensure the safe delivery of humanitarian and development assistance.

The objective of SLT is to enhance the ability of partner organizations to make informed decisions and implement effective security arrangements to improve the safety and security of personnel and operations.

To this end, SLT partner organizations commit to:

- Establish security coordination arrangements and forums;
- Share relevant security information;
- Cooperate on security training;
- Cooperate on operational and logistics arrangements, where feasible;
- Identify resource requirements for enhancing security coordination between the UN, INGOs and IOs, and advocate for funding; and
- Consult on common ground rules for humanitarian action.

It is recognized that SLT partner organizations perceive risks and assess vulnerabilities differently, accept different levels of risks, and implement security arrangements which they consider suitable for their organization and operational conditions.

In this context, SLT partner organizations accept that they remain fully accountable for the safety and security of their personnel in accordance with their 'duty of care' obligations as employing organizations. Accordingly, organizations that wish to cooperate under the SLT Framework are required to maintain internal security risk management procedures, contingency planning and adequate and reliable arrangements to respond to security emergencies. Implementation of SLT in the field will be achieved through the establishment of collaboration mechanisms at two levels: Regular and Enhanced. The arrangements associated with the two levels are designed to differentiate between "low/medium" and "high/very high" risk areas and the related security and operational conditions.

The SLT arrangements in the field will be supported by UN, INGO and IO headquarters security managers and through the SLT Oversight Committee. A feedback mechanism will be maintained for the resolution of coordination issues which may arise in the field.

Although Saving Lives Together is a voluntary engagement by the SLT partner organizations, the success and effectiveness of the initiative is dependent on the commitment of all participating organizations to work collectively towards the mutual goal of improving the security of personnel, operations and assets. Accordingly, organizations that wish to become SLT partner organizations must commit to the adoption of the principles, objectives and arrangements comprised in this framework.

Headquarters Support for SLT

UNDSS and OCHA will work with the headquarters of SLT partner organizations to achieve the following:

- Timely sharing of security incident reports and alerts;
- Timely responses to queries on SLT related issues;
- Supporting the resolution of security coordination problems which may arise in the field;
- Supporting the coordination of security incident response measures in the field;
- Sharing of contact information between security managers of SLT partner organizations;
- Collecting, compiling and cross-checking information for regular security reports and coordinate mutual assistance in maintaining relevant security incident databases;
- Making training events available to security managers of SLT partner organizations, when feasible;
- Organising workshops and conferences to enhance mutual knowledge and understanding of UN, INGO, and IO security collaboration;
- Exploring further areas of security cooperation between the UN, INGOs and IOs; seeking innovation and efficiencies in areas of security management.

To support the effective implementation of this framework with the required leadership and guidance, and to ensure monitoring and reporting, an SLT Oversight Committee has been established to:

- Provide strategic guidance for the implementation of the SLT Framework;
- Monitor the implementation of the SLT Framework;
- Review and approve INGO HQs' requests for admission to SLT partnership;
- Maintain a feedback mechanism for the resolution of coordination issues in the field;
- Identify and disseminate good practice to enhance security cooperation between the UNSMS, INGOs, and IOs;
- Report on the implementation of SLT to the IASC on an annual basis; UNDSS, on behalf of the SLT OC, will compile regular reports to reflect the status of SLT implementation globally, record new developments and initiatives, and publicise good practices;
- Monitor the application of the SLT Levels to ensure their coherence.

The SLT OC is co-chaired by UNDSS and a representative of an INGO SLT partner organization. UNDSS and OCHA will function as a Secretariat for the SLT OC.

SLT Partner Organizations

The SLT partnership comprises the following categories of organizations:

- United Nations Security Management System (UNSMS) Organizations;
- International Non-Governmental (INGOs)/ International Organizations (IOs) that are implementing or operational partners of United Nations Agencies, Funds and Programmes;

INGOs and IOs may request global SLT partnership status, which will be formalized through an exchange of letters of understanding (LOUs) between the headquarters of INGOs/IOs and UNDSS, upon review and agreement of the SLT OC. SLT partnership is conditional

to committing to implement the principles, objectives and arrangements comprised in this framework.

SLT Cooperation in the Field – Regular Level

The essential goal at the Regular Level of SLT implementation is to create dialogue and information sharing arrangements to ensure that all SLT partner organizations have adequate access to relevant security information.

Coordination Arrangements

- INGOs and IOs will nominate representatives to interface and engage with the UNSMS. Where feasible, INGOs and IOs will establish a security coordination platform or use a coordination entity to interface with the UNSMS through UNDSS;
- INGOs and IOs may opt to grant observer status to nominated UNSMS representatives to attend relevant portions of the INGO and IO security forum meetings;
- UNSMS may opt to grant observer status to INGO and IO representatives to attend the relevant portions of the United Nations' Security Cell and/or Security Management Team meetings.
- UNDSS will function as the focal point for SLT security cooperation on behalf of the UNSMS, in close cooperation with UN Agencies and OCHA;

Information Sharing

- Obtaining relevant, timely and accurate security information is a critical element of informed decision making, and it is therefore incumbent on all SLT partner organizations to commit to sharing relevant security information with each other.
- Security information shared under the SLT framework is for the sole purpose of enhancing the security of personnel, operations and assets, and must not be used for any other purposes. Participating organizations commit to ensuring confidentiality of shared information and the appropriate use of the information within their organization. Information received cannot be further distributed to third parties without the prior consent of the originating organization. All assessments and decisions made on the basis of shared security information remain the responsibility of the individual organizations making those assessments and decisions.
- It is recognised that SLT partner organizations may have limitations on what information they can share due to internal confidentiality requirements, restrictions applicable to information originating from third parties, obligations to protect the privacy of their personnel, and preserving the credibility and integrity of their organization. However, SLT partner organizations should make every effort to disclose relevant security information, especially when such information may be critical to mitigate an imminent risk of injury or death.
- Security information sharing comprises the following: incident reports; situation reports; security alerts; security procedures, risk mitigation and contingency measures, as well as lessons learnt related to security incidents.

Operational and Logistics Arrangements

- SLT partner organizations will share logistics to enhance security arrangements and respond to security incidents where feasible, e.g. UN Humanitarian Air Service (UNHAS);
- SLT partner organizations should seek to implement, where feasible, interoperable communications systems, advocate for the provision of frequencies, and assist each other in support and maintenance arrangements.

Security Training

- Recognising that UN, INGO and IO personnel operate in the same environment and that their security is often interlinked, it is advisable that security training is harmonised. Accordingly, SLT partner organizations will collaborate and consult on the development and delivery of security training, and offer participation or observer status at security training exercises, where feasible.
- In areas where the UNSMS establishes a Safe and Security Approaches to Field Environments (SSAFE) training, it will offer participation for INGO and IO personnel, if feasible.

SLT Implementation in the Field – Enhanced Level

When security conditions become more complex and challenging, information sharing and security coordination arrangements between SLT partner organizations should be enhanced concurrently. Accordingly, the goal of the Enhanced Level of cooperation is to achieve stronger and more effective information sharing, security coordination, and operational arrangements.

In areas with challenging security conditions, the elements of the Enhanced level SLT cooperation below should be considered and applied in addition to the Regular Level SLT components listed above.

Coordination Arrangements

Effective coordination mechanisms established and formalised:

- INGOs and IOs will establish a fully functioning security coordination platform to interface with the UNSMS;
- UNDSS will nominate a security focal point for SLT, providing a strong link with the INGO security coordination platform;

When required to provide additional capacity for security coordination with INGOs and IOs, and depending on capacity and availability of funding, UNDSS may establish a security support team.

Information Sharing

SLT partner organizations will:

- support the systematic sharing of security incident reports;
- establish regular security coordination meetings and briefings;
- share operational planning information, where relevant, in the interest of mutual security.
- UNDSS and the INGO security coordination platform will:
- cooperate closely and enhance information sharing to enhance situational awareness for all SLT partner organizations;
- cooperate on security analysis, risk assessments, and operational planning, where feasible.

UNSMS Security Information and Operations Centres (SIOC), where established, will function as a central node for coordination and information sharing between SLT partner organizations.

Operational and Logistics Arrangements

SLT partner organizations will:

- Collaborate on security arrangements for jointly conducted operations, where applicable;
- Identify security requirements to be included in Consolidated Appeals (CAP), Strategic Response Plans (SRP), or other joint funding appeals;
- Consult on security coordination with host country authorities and other local actors with a view to achieving a coordinated and/or common approach where appropriate;
- Consult on contracted security services, e.g. security escorts, with a view to achieving a coordinated and/or common approach, where appropriate.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter IV

SECURITY MANAGEMENT

SECTION A

Policy on Security Risk Management (SRM)

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 18 April 2016
Technical Review: 1 May 2017

A. Introduction

1. The Security Risk Management (SRM) process was launched by the United Nations Security Management System (UNSMS) in 2004 as a system–wide managerial tool to analyse and manage safety and security risks to United Nations personnel, assets and operations. It was last updated in 2009 with additional guidelines, training tools and templates.

2. In July 2010, the Inter-Agency Security Management Network (IASMN) formed a working group for broader enhancements of the SRM process. Reviews of the SRM process and the resulting recommendations and decisions indicated that the following areas could be further enhanced:

   (a) The reliability and validity of the assessment of security risks;

   (b) The context-specific SRM strategies;

   (c) Dynamic, responsive and flexible application of the SRM process, to changes in the situation and programming;

   (d) Structured decisions on risk management measures and acceptance of risks; and

   (e) Management and oversight of the implementation of approved SRM measures.

3. As a result, a revised SRM process has been developed and tested across the spectrum of security environments. It supports valid, context specific, and timely Security Risk Assessments and risk management decisions to ensure that programmes are delivered within an acceptable level of security risk. The revised SRM process supports security professionals and security decision-makers to effectively manage security risks.

B. Purpose

4. The purpose of this policy is to provide United Nations security decision makers, programme managers and security professionals with the concept, principles and applicability of the SRM process as defined by the UNSMS.

5. This policy must be read in conjunction with the UNSMS Security Risk Management Manual ("SRM Manual") which provides details of the theory, practices and procedures of the SRM process. The SRM Manual contains directions on how to carry out the SRM process and how to apply the SRM tools.

C. Scope and Applicability

6. This policy is applicable to all UNSMS organizations as well as all individuals defined in Chapter III of the *Security Policy Manual* (SPM) ("Applicability of the United Nations Security Management System"). All references to the United Nations herein refer to the United Nations and United Nations system organizations participating in the UNSMS.

D. Policy principles

7. The primary responsibility for the safety and security of the United Nations rests with the host Government.[1] In addition, all actors in the UNSMS have security management responsibilities and accountability in line with the Framework of Accountability for the UNSMS ("Framework of Accountability")[2] .

8. In cooperation and collaboration with relevant host Government entities, United Nations managers take security management decisions based on technical advice provided by United Nations security professionals.

9. The goal of UNSMS SRM is to enable programmes and operations of United Nations personnel, premises and assets.

10. Security Risk Management is essential to achieving the United Nations goals by decreasing the effect of threats. Security Risk Management offers a structured approach to identifying and assessing the threats to the United Nations, enabling identification of SRM measures to reduce the level of assessed risk and enhancing the decision-making process in line with the Framework of Accountability, UNSMS policies and guidelines. It allows managers to maximize programme opportunities and to allocate security-related resources in ways that enable programme delivery within acceptable levels of risk[3]. It is vital to achieving the planned and envisioned programme results for the UNSMS organizations, especially in complex and dangerous environments.

11. Security decisions must be in line with existing UNSMS policies and guidelines.

[1] For more details, refer to UNSMS *Security Policy Manual*, Chapter II, Section E ("Relations with Host Countries on Security Issues").
[2] For more details, refer to UNSMS *Security Policy Manual*, Chapter II, Section B ("Framework of Accountability for the United Nations Security Management System"), which outlines the roles and accountability of all actors with security management responsibilities in the United Nations Security Management System.
[3] For more details, please refer to the revised Programme Criticality Framework endorsed by the HLCM and the CEB in in 2016. This is the revision of the 2013 Programme Criticality Framework. In line with the Secretary-General's decision (PC/2016/1), the Programme Criticality Framework is a mandatory policy of the Organization in areas where security risk levels are "high" or above. The Designated Official is accountable for using the results of the Programme Criticality Assessment and for endorsing security risk management decisions taken at country-level, taking both the Programme Criticality and the results of the Security Risk Management process into consideration.

12. The UNSMS only has the remit for three areas of safety: road safety, fire safety and aviation safety. Thus, there are many other areas of safety not covered by the UNSMS (and, therefore, the SRM process), including medical issues, occupational health and safety, and structural engineering.

E. Security Risk Management concept

13. Any United Nations objective, from global strategic goals to local programme plans, may fail because of various obstacles. In the security context, obstacles are called threats. All managers must identify threats and evaluate how these threats may affect their objectives. In many of the places where we work, the effect of threats, if not managed, can be fatal to personnel and can result in cessation of programmes.

14. Security Risk Management is the process of identifying future harmful events ("threats") that may affect the achievement of United Nations objectives. It involves assessing the likelihood and impact of these threats to determine the assessed level of risk to the United Nations and identifying an appropriate response. Security Risk Management involves four key strategies: controlling, avoiding, transferring and accepting security risk. Security risks are controlled through prevention (lowering the likelihood) and mitigation (lowering the impact).

15. Risk is the combination of the likelihood of a threat being carried out and the subsequent impact to the United Nations. Security measures can either be used to prevent vulnerability from being exploited or mitigate the impact of exploitation, or both.[4] One way to think of risk management is that it is the systematic determination and implementation of timely and effective approaches for managing the effects of threats to the Organization. SRM is merely the management of security-related risks.

16. In the SRM process, likelihood and impact are assessed on a 1-5 scale and combined in a risk matrix as follows:

	Risk Matrix	Impact				
		Negligible	Minor	Moderate	Severe	Critical
LIKELIHOOD	Very Likely	Low	Medium	High	Very High	Unacceptable
	Likely	Low	Medium	High	High	Very High
	Moderately Likely	Low	Low	Medium	High	High
	Unlikely	Low	Low	Low	Medium	Medium
	Very Unlikely	Low	Low	Low	Low	Low

Figure 1: Risk Matrix

[4] When discussing the management of risks, the UNSMS has adopted the terms "prevention" and "mitigation"; taking measures to reduce likelihood is called "prevention"[4] while taking measures to reduce impact is called "mitigation".

F. The Security Risk Management process structured approach

17. The SRM process is a structured approach to evaluating security risks to ensure that a comprehensive threat and risk analysis leads to effective security decision-making and to the implementation of SRM measures. The SRM process endeavours to be

    (a) Objective, fact-based, logical and systematic,
    (b) Globally applicable in a consistent, de-politicized manner;
    (c) Reliable (achieve similar results when different people use it);
    (d) Valid (accurately represent the security environment on the ground), and
    (e) User-friendly without being over-simplistic. The SRM process is an ongoing process with nine steps:

    Step 1: Setting the Geographical Scope and Timeframe;
    Step 2: Situational Analysis;
    Step 3: Programme Assessment;
    Step 4: Threat Assessment (General and Specific);
    Step 5: Security Risk Assessment;
    Step 6: Security Risk Management Decisions;
    Step 7: Security Risk Management Implementation;
    Step 8: Acceptable Risk;
    Step 9: Follow up and Review.

18. Each step of the risk management process and how each step interacts with other steps is explained below in figure 2 below.

Figure 2: Security Risk Management Process Structured Approach

G. Roles and Responsibilities in the SRM Process

19. The Framework of Accountability identifies the following roles and responsibilities with regard to the implementation of the SRM process:

    (a) Security professionals are responsible for initiating, conducting and monitoring all phases of the SRM process;

    (b) Security decision makers are responsible for decisions made throughout the SRM process, including those associated with SRM measures and acceptable risk;

    (c) The Designated Official (DO) is the only decision maker who can approve SRM measures for an SRM Area. Where an Area Security Coordinator (ASC) is appointed, he or she will present the SRM recommendations for the Security Area to the DO for approval.

    (d) Any security decision maker can accept recommendations that follow an ad hoc SRM process, unless these recommendations would be less effective in reducing the risk than the requirement already approved by the DO. Such ad hoc recommendations would require DO approval.

20. Accountability for the conduct and quality of Programme Criticality Assessments lies with the Resident Coordinator or the Special Representative of the Secretary-General/Head of Mission, as applicable. The DO uses the results of the Programme Criticality Assessment and takes decisions on acceptable risk at the country level[5]. In situations of a very high residual risk, the final decision on acceptable risk lies with the Under-Secretary-General for Safety and Security.

21. The review of the SRM process, including recommended SRM measures and monitoring of the implementation of approved measures when necessary, must be a standing agenda item for all Security Management Team meetings.

H. Definitions

22. For the purpose of this policy, the definitions of key terms are as follows:

Security Risk Management	The systematic determination and implementation of timely and effective approaches for managing the effects of threats to the United Nations.

[5] Decision of the Secretary-General – 12 January 2016 Meeting of the Policy Committee.

Threat A potential cause of harm initiated by deliberate actions.

Hazard A potential cause of harm resulting from non-deliberate actions.

Risk The likelihood of a harmful event occurring and the impact of the event if it were to occur.
(Risk = Likelihood x Impact)

Conditions of Risks within the SRM Process:

- **Present Risk** The security risk based on the threats, and the security measures and procedures currently in place.
- **Projected Risk** The expected security risk if recommended security measures and procedures were to be in place.
- **Residual Risk** The security risk remaining after approved security measures and procedures have been implemented.
- **Risk Rating** A rating of the risk based on an assessment of the likelihood and impact from very low to unacceptable.

Likelihood A rating of the assessed potential for a harmful event to effect the Organization.

Impact A rating of the assessed potential harm that an event would have (if it were to occur) on the Organization.

Vulnerability A weakness that can allow a threat or hazard to cause harm.

Vulnerable Inadequate SRM measures and procedures meant to address a threat.

Capability The capacity or ability of threat actors to cause the threat event as described.

Intent The motivation or disposition of a threat actor to cause the threat event as described.

Event Description Clear description of a harmful event that the SRM process will examine (must include the effect on the Organization).

SRM Area Geographic scope defined for the application of the SRM process.

Programme Assessment A process by which the security professional formally

comprehends the programme requirements of the UNSMS organizations.

I. Training Requirement

23. All United Nations officials who have specific security responsibilities within the Framework of Accountability shall be cognizant of the SRM concept and process. Training on SRM shall be mandatory.

24. The United Nations Department of Safety and Security (UNDSS) shall develop a training specifically tailored for DOs, Security Management Team members, security professionals and managers of United Nations system organizations, and coordinate the delivery of such training courses.

J. Final Provisions

25. This policy is to be made available to all United Nations personnel.

26. This policy enters into force on 18 April 2016.

27. The UNSMS *Security Policy Manual* (SPM), Chapter IV, Section A: "Policy and Conceptual Overview of Security Risk Management" (April 2009), Chapter IV, Section B ("Security Level System") and Chapter IV, Section C ("Guidelines for Determining Acceptable Risk") are hereby abolished and replaced by the provisions of this policy.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter IV

SECURITY MANAGEMENT

SECTION D

Relocation, Evacuation and Alternate Work Modalities - Measures to Avoid Risk

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 8 April 2011
Technical Review: 1 May 2017

A. Introduction

1. The United Nations policy on Security Risk Management (SRM) categorizes decisions on how to manage risk as accept, control, avoid and/or transfer (see *Security Policy Manual (SPM)*, Chapter IV, "Policy on Security Risk Management", paragraph 14). As part of a broader security risk management strategy, the Designated Official (DO) may temporarily remove personnel and/or eligible family members from an area or situation of unacceptable risk as a means of managing that risk (i.e., avoiding the risk). This chapter lays out the parameters, as well as the roles and responsibilities of relevant actors, regarding the three basic options for avoiding risk used by the United Nations Security Management System:

   (a) Alternate Work Modalities (temporary closure of offices, "work-from-home" for personnel, "stay-at-home" instructions for eligible family members, etc.)

   (b) Relocation

   (c) Evacuation

B. Purpose

2. The purpose of this policy is to lay out the parameters of measures to avoid risk as part of SRM, including alternate work modalities, relocation and/or evacuation, and to clarify the roles and responsibilities of relevant United Nations Security Management System (UNSMS) actors in these decisions.

C. Application/Scope

3. The policy is applicable to all individuals covered by the UNSMS, as defined in Chapter III of the *Security Policy Manual* ("Applicability of United Nations Security Management System").

D. Conceptual Framework

4. The SRM process is the fundamental United Nations tool for managing risk. It assesses the level of risk of specific threats to the United Nations. Based on the SRM process, different security measures may be implemented to reduce the level of risk to acceptable levels and enable the United Nations to continue operations.

5. One security risk management option is to avoid risk by temporarily removing persons or assets from a situation of unacceptable residual risk by using alternate work modalities, relocation or evacuation (or their combination). Indeed, until proper measures to control and lower risks are put in place, avoiding risk is the only option when residual risks are deemed unacceptable (see "UNSMS Security Risk Management (SRM) Manual", page 48-49).

6. Any decision to avoid risk must take into consideration the impact of the removal of personnel and/or eligible family members on United Nations programmes and activities, including security and/or business continuity plans. Avoiding risk can be a cost-effective way to manage risk, and it is best suited for situations when resource limitations prevent the implementation of proper risk controls or when there has not been enough time to implement proper risk controls (for details on risk control, see "UNSMS Security Risk Management (SRM) Manual").

E. Alternate Work Modalities

7. For the purpose of this policy, "Alternate Work Modalities" are defined as measures that limit or totally remove the number of personnel or family members at a specific location(s), short of official relocation or evacuation, with the view to limit or remove their exposure to a sudden situation that creates unacceptable residual risk.

8. Alternate Work Modalities include, but are not limited to, temporarily limiting or removing the number of personnel at United Nations premises, ordering school-aged family members to stay out of school temporarily or creating "no-go" areas in urban areas where personnel and family members cannot visit at certain times.

9. Alternate Work Modalities are effective security risk management strategies for when there is no time to implement proper risk controls, if such controls are not cost-effective or if there is not enough information to determine what risk controls are needed.

10. Decisions on Alternate Work Modalities that involve temporarily closing offices or work-from-home arrangements must be made in accordance with United Nations Human Resources rules and regulations.

F. Evacuation and Relocation

11. Relocation is defined as the official movement of any personnel or eligible dependant from their normal place of assignment or place of work to another location within their country of assignment for the purpose of avoiding unacceptable risk. Relocation is a risk avoidance measure that can be applied to all personnel and eligible family members.

12. Evacuation is defined as the official movement of any personnel or eligible dependant from their place of assignment to a location outside of their country of assignment (safe haven country, home country or third country) for the purpose of avoiding unacceptable risk. Except in the situations outlined in paragraph 13 below, evacuation is a risk avoidance measure that can be applied only to internationally-recruited personnel and their eligible family members. The evacuation of eligible family members of internationally-recruited personnel is governed by the same eligibility conditions as for the payment of evacuation

allowances as per *Security Policy Manual*, Chapter VI, Section A ("Remuneration of United Nations System Staff and Eligible Family members on Relocation/Evacuation Status").

13. Locally-recruited personnel and/or their eligible family members may be evacuated from a duty station only in the most exceptional cases in which their security is endangered as a direct consequence of their employment by organizations of the United Nations common system. A decision in this regard can only be made by the Secretary-General, as recommended by the Under-Secretary-General for Safety and Security, based on a recommendation by the DO. Personnel and/or their eligible family members not covered by paragraph 12 above may also be assisted to leave the country by the organization, when possible and to the extent feasible and on a reimbursable basis.

14. The generic term "Family Restrictions" will be used to describe situations where the DO has placed restrictions on the presence of any or all eligible family members of United Nations internationally-recruited personnel for a given area. Similarly, the term "Personnel Restrictions" will be used to describe situations where the DO has placed restrictions on the presence of any or all United Nations personnel for a given area.

G. Roles and Responsibilities

15. The DO, in consultation with the Security Management Team (SMT) and based on the advice of the most senior security professional directly supporting the DO,[1] may institute planned or ad hoc Alternate Work Modalities for all or some United Nations personnel and eligible family members to address specific security problems in their area of responsibility in accordance with Section F above. Contingencies for Alternate Work Modalities should be included in the Security Plan and any ongoing Alternate Work Modality (such as "no-go" areas in a city) should be included in the country-specific Minimum Operating Security Standards.

16. Representatives of organizations participating in the United Nations Security Management System can also institute Alternate Work Modalities solely for their personnel in response to agency-specific risks. This derives from their responsibility and authority in the United Nations Framework of Accountability for Security. Representatives wishing to implement such measures should examine any possible negative impact these measures would have on security and/or business continuity plans. They should also consult with other members of

[1] This is usually the Chief Security Adviser (CSA) or a Security Adviser (SA), including their officer-in-charge *ad interim*. Where a CSA or SA is not present, this term is equivalent to the titles of Chief Security Officer, Chief of Security and Safety Services, Country Security Focal Point (CSFP) or Local Security Assistant (if necessary) in countries where no international professional security adviser has been assigned or is present.

the SMT to examine whether these decisions would have any negative impact on the security of other United Nations personnel in the country.

17. The DO, in consultation with the SMT, may recommend the relocation or evacuation of personnel and/or eligible family members when residual risks are deemed unacceptable. This recommendation is submitted through the Under-Secretary-General for Safety and Security to the Secretary-General. After assessing the situation, the Under-Secretary-General for Safety and Security makes a recommendation to the Secretary-General for approval of evacuation or relocation.

18. Upon the Secretary-General's approval of the recommendation, the Under-Secretary-General for Safety and Security distributes an "All Agency Communiqué" to the United Nations System announcing the details and parameters of the relocation and/or evacuation.

19. In the event that there is an impasse or life-threatening exigencies that impacts the ability of the DO and SMT to make timely risk avoidance decisions, the Under-Secretary-General for Safety and Security can take such decisions, including by consulting, as necessary, the Executive Group on Security to advise and assist in rapid decision-making.

20. In the event of a breakdown of communication, the DO is authorized to use his/her best judgment to implement relocation and/or evacuation and report on such action immediately thereafter to the Secretary-General, through the Under-Secretary-General for Safety and Security.

21. If the DO, in consultation with the SMT, recommends that relocation and/or evacuation are no longer needed in any circumstance or area, it is the Secretary-General, on the advice of the Under-Secretary-General for Safety and Security, who decides when and how personnel and eligible family members can return.

22. Decisions to relocate or evacuate personnel and/or family members are clearly decisions to control the number of personnel and family members as explained in paragraph 2(c) of Chapter V, Section A ("Security Clearance Procedures and the Travel Request Information Process (TRIP)"). Therefore, DOs must institute "manual" security clearance procedures[2] for all locations in relocation or evacuation status.

H. Process of Relocation and/or Evacuation

23. Authorized relocation and/or evacuation of personnel and/or family members requires the DO to take the following steps:

[2] See paragraph 18 of Chapter V ("Security Clearance Procedures and the Travel Request Information Process (TRIP)") for details on "manual" and "automatic" security clearance procedures.

(a) A decision, in consultation with the SMT, on which personnel and eligible family members must be relocated and/or evacuated. The decision as to who remains is based on the "Acceptable Risk Model" (see the UNSMS Security Risk Management (SRM) Manual) and associated mechanisms for determining Programme Criticality and personnel requirements for priority programmes. Personnel who are unable to carry out their assigned tasks effectively due to the security situation and level of residual risk should also be relocated/evacuated. The DO and SMT may determine who will be relocated or evacuated prior to any official authorization of relocation and/or evacuation, including as part of contingency planning or in anticipation of such authorization;

(b) Temporary concentration of all personnel and/or their eligible family members, as decided as per paragraph 23(a) above, in one or more concentration points. The DO and SMT may undertake this step prior to any official authorization of relocation and/or evacuation in anticipation of such authorization;

(c) Relocation of all personnel and/or their eligible family members, as decided as per paragraph 23(a) above, to alternative locations within the country (note: the temporary concentration and/or internal relocation of locally-recruited personnel and eligible family members is contingent on their desire to avail themselves of this option); and/or

(d) Evacuation outside the country of all internationally-recruited personnel and/or their eligible family members, as decided as per paragraph 23(a) above.

24. Relocation and evacuation movements are official travel, so the Travel Request Information Process (TRIP) must be updated regarding the movements of personnel and eligible family members.

25. Before the evacuation of any personnel or eligible family members, the DO must take all of the following actions:

(a) Notify the host Government and local authorities and request assistance as necessary;

(b) Notify the DO in the designated country of evacuation, as well as neighbouring countries and any other countries that may be affected, of the evacuation;

(c) Notify Area Security Coordinators and wardens to instruct all personnel and their eligible family members on actions to be taken;

(d) Brief Area Security Coordinators and wardens, as necessary, on further steps that may be required;

(e) Review financial arrangements, including for the payment of salary advances, allowances or other essential payments as necessary;

(f) Adjust lists of personnel and eligible family members to reflect the evacuation and/or relocation;

(g) Notify personnel in other parts of the country, unaffected by the evacuation and/or relocation, of these developments through the Area Security Coordinator; and

(h) Complete a checklist in respect of those who have been evacuated as per Annex A below, "Follow up after Evacuation of United Nations Personnel".

I. Return of Evacuated Personnel and Eligible Family members:

26. Any personnel evacuated may be authorized to return under two conditions:

(a) The Secretary-General, through the Under-Secretary-General for Safety and Security, authorizes the cancellation of the evacuation status on the recommendation of the DO, in consultation with the SMT, in accordance with paragraph 21 above; or

(b) The staff member is recommended to return to the duty station based on a Programme Criticality assessment, as outlined in paragraph 23(a) above, and is authorized to do so by the Secretary-General, through the Under-Secretary-General for Safety and Security).

27. The authorization to evacuate eligible family members means that eligible family members, as described in the evacuation authorization, are not authorized to be present until the Secretary-General, through the Under-Secretary-General for Safety and Security, cancels the evacuation status on the recommendation of the DO, in consultation with the SMT, in accordance with paragraph 21 above. Compliance is mandatory.

J. Final provisions:

28. Field Security Handbook (2006), Chapter V, Section E and G and Annexes I and J are hereby abolished.

Annex A: Checklist: Follow-up After Evacuation of United Nations Personnel

NAME OF STAFF MEMBER: _____
TITLE: _____
ORGANIZATION: _____
PROJECT / OFFICE: _____

1. Personal effects/household goods
   - Still remain at duty station? _____
   - Packed or unpacked, and whereabouts _____
   - Has staff member: _____
     a) Left packing instructions? _____
     b) Specified destination and full shipping address? _____
     c) Specified mode of shipment? _____
     d) Supplied packing list? _____
     e) Arranged insurance? _____
     f) Obtained export permit? _____
     g) Specified any items for disposal locally? _____
     h) Indicated preferred prices? _____
     i) Left instructions for transfer of any income from sales? _____
     j) Left details of any items still in shipment to the duty station? _____

2. Private Vehicles
   - Still at duty station? _____
   - Make, type and plate/chassis number _____
   - Whereabouts? _____
   - Has staff member: _____
     a) Specified destination and full shipping address? _____
     b) Specified mode of shipment? _____
     c) Arranged insurance? _____
     d) Obtained export permit? _____
     e) Specified that vehicle is to be sold locally? _____
     f) Indicated preferred price? _____
     g) Left instructions for transfer of any income from sales? _____

3) Rental, etc.
   - Has staff member: _____
     a) Surrendered his lease? _____
     b) Left written instructions for settlement of outstanding rental payments or for recovery of deposits from landlord? _____
     c) Left written instructions for payment/terminal payment of house servants? _____
     d) Left written instructions for payment of outstanding utilities/recovery of deposits for: _____

- gas? _____
- electricity? _____
- water? _____

e) left written instructions for payment of outstanding school fees? _____

4. Bank accounts

Has staff member:

a) Left bank accounts? _____
b) Left local currency? _____
c) Other financial items left? _____
d) Left transfer instructions with bank? _____
e) Left transfer instructions with Designated Official's office together with written authority for DO or his representative to handle account? _____

UNITED NATIONS SECURITY MANAGEMENT SYSTEM

Security Policy Manual

Chapter

IV

SECURITY MANAGEMENT

SECTION E

Security of United Nations Premises

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 8 November 2012
Technical Review: 1 May 2017

A. Introduction

1. The primary responsibility for the security and protection of United Nations personnel, eligible family members and organization property rests with the host Government. This responsibility flows from every Government's normal and inherent function of maintaining order and protecting persons and property within its jurisdiction. In the case of the United Nations, the Government has a special responsibility under the Charter of the United Nations and relevant agreements the host Government may have with individual United Nations organizations. The organizations of the United Nations Security Management System (UNSMS) rely on the host Government for the provision of adequate security.[1]

2. Without abrogating the responsibility of the host Government for its obligations, the United Nations has a duty as an employer to reinforce and supplement the capacity of the host Government to fulfil these functions in circumstances where United Nations personnel are subject to conditions of insecurity that require security measures beyond what the host Government can provide. This need for UNSMS organizations to reinforce and supplement what the host Government can provide for premises security is important when the whole or part of the United Nations premises is an "exclusive use area" of the United Nations in which the host Government has no authority.

3. The security of premises is a security risk management issue, but a specific policy focused on strengthening premises security is required for the following measures:

   (a) Premises are static locations that are more vulnerable to detailed, planned criminal, terrorist, civil unrest or other attacks or the impact of attacks on neighbouring buildings;

   (b) Premises concentrate personnel and/or assets within one location;

   (c) United Nations premises can be considered as desirable, even iconic, targets for various forms of violence, including terrorism, civil unrest and crime;

   (d) Most premises that the United Nations lease, rent or have provided by member states are not built with security and safety considerations;

   (e) Security for premises often requires large financial and capital investments in security construction and systems, including physical security, as well as long term planning;

   (f) Personnel expect United Nations premises to be places where they can feel safe and secure.

[1] In accordance with *Security Policy Manual*, Chapter II, Section E ("Relations with Host Countries on Security Issues"), paragraph 10, if de facto local authorities and/or "non-state actors" are in control of the areas where United Nations premises are located, depending on the circumstances, it may be useful to apply the principles outlined in this policy even though non-state actors or de facto local authorities controlling areas are not host Governments.

B. Purpose

4. The purpose of this policy is to establish the basic principles and requirements for efficient and effective management of security risks associated with United Nations premises.

C. Application/Scope

5. The policy is applicable to all UNSMS organizations as well as all individuals defined in Chapter III of the *Security Policy Manual* (SPM) ("Applicability of the United Nations Security Management System").

6. This policy is primarily intended for all categories of security personnel and others with responsibility for acquisition, operation and maintenance of United Nations premises.

7. This policy only covers the security aspects of premises management, including fire safety. This policy does not address occupational health or safety issues or safety aspects relating to premises design, construction, refurbishment and management, including the technical assessment of the risks from natural hazards.

8. This policy is applicable to all United Nations premises worldwide.

D. Premises Security

9. For purposes of this policy, the term "United Nations premises" means all categories of land and physical structures occupied by personnel of one or more organizations of the UNSMS, including structures such as buildings, offices, warehouses, stores, shops, dwellings, containers, prefabs and tents.[2]

10. This policy is that there must be a minimum standard for United Nations premises that is grounded on four important principles of premises security:

    (a) Security Risk Management;

    (b) Integrated Systems Approach;

    (c) "Four Ds" (Deter, Detect, Delay and Deny);

    (d) Concentric Layers of Security.

11. **Security Risk Management**. UNSMS officials will use the SRM process to determine appropriate situation-specific security procedures and measures for premises safety and security. Application of the SRM process for a specific

[2] When United Nations personnel are working in non-United Nations premises, such as government facilities, the provisions of *Security Policy Manual*, Chapter IV, Section N ("Policy for United Nations Minimum Operating Security Standards"), paragraph 6.3 shall apply.

United Nations premises will identify the actors with the intent and capability to carry out credible threats against the premises, with special emphasis on the threat actors that have the capability to exploit potential weaknesses in a premises' security system. The weaknesses are documented in a security survey for the premises and analysed within the vulnerability assessment of the SRM process for the specific premises. In this approach, not all United Nations premises will be protected in the same way or to the same extent, but all premises protection will be commensurate with the specific security situation the premises faces. United Nations security professionals are to work in close collaboration with host Government, facilities managers and other applicable parties in the applications of the SRM process to United Nations premises.

12. **Integrated Systems Approach**. Proper security and safety of United Nations premises require an approach that focuses on the total system and resulting management of it, rather than on the individual components of the system. The systems approach is an integration of physical,[3] procedural, technical and human aspects that create a self-reinforcing protection of the premises. The Integrated Systems Approach must also coordinate with areas of responsibility of the host Government outside of the premises.

13. **Four Ds**. Security systems for premises are based on the effective use of the following principles, for which the host Government is primarily responsible[4]:

    (a) Deter – physical and procedural security that attempts to prevent undesirable action against the premises by influencing attacker's decision-making (increase perception of effort or fear of failure);

    (b) Detect – measures to detect and assess planning, or actual attempts to plan, by threat actors to penetrate security perimeter or to test the effectiveness of the security system in place;

    (c) Delay – physical, technical, procedural or psychological barriers to restrict movement and to allow time for appropriate response[5] (by security or host Government forces);

    (d) Deny – the ability to oppose or negate the effects of an action against the premises, including denying access to information on the layout and contents of the premises. The premises security system must be designed to

[3] For the purposes of this policy, physical security entails the full range of construction, fixtures, equipment and related procedures that are integrated into the larger premises security system.

[4] It is the responsibility of UNSMS officials to review and assess host Government ability to apply the "Four Ds". If this assesment indicates that the host Government is lacking in any area, the UNSMS organization responsible for the premises must find means to compensate.

[5] With the appropriate resources, time and planning capabilities, any security system can be defeated. Therefore, the security system must also include an appropriate response by host Government or other security forces to neutralize the threat or an appropriate response by management to evacuate the premises.

deny identified threat actors the ability to carry out a successful harmful action against the premises.

14. **Concentric Layers of Security**. The integration of the principles outlined in the Four Ds above requires the concept of Concentric Layers of Security (Defence in Depth). Proper premises security requires a system designed with sufficient diversity and redundancy so that the strength of one particular component offsets the weakness of another. Components of the security system must be designed in sufficient number of layers to make it more difficult to defeat the whole system. All United Nations premises require at least two physical layers of security between personnel or valuable assets and the areas beyond direct United Nations control, including a system to only allow authorized persons, vehicles and other items to cross these layers (access control). The principle of Concentric Layers of Security also requires UNSMS officials responsible for the premises to coordinate with areas of responsibility of the host Government outside of the premises.

15. Access control systems, beginning at the perimeter and continuing through each layer of protection within the premises, channel personnel and vehicle access through designated control points for verification of identity, authority to enter and other security checks. Access control systems must provide for detection of and response to unauthorized entry attempts or other security breaches. Physical security measures on the perimeter of United Nations premises must be capable of confining attempted intrusions to the perimeter and limiting the risk to personnel associated with the threat of a direct or targeted attack or delaying attempted intrusions for sufficient time to enable a response that will limit the risk to personnel. Proper selection, supervision, management and training of guard forces used in the premises security system are also required.

16. The UNSMS organization responsible for the premises is to work in close collaboration with United Nations security professionals, host Governments, facilities managers and other responsible parties during all phases of design, construction, refurbishment and management of premises security systems to ensure that the technical, architectural and engineering elements of the premises are appropriate for the security threats and risk determined by the SRM process. This collaboration is essential to ensure that United Nations resources are used efficiently. When a UNSMS organization is considering occupying a new premises, United Nations security professionals must be involved in a security evaluation and assessment of the premises and, after acquisition of premises, must be involved in ongoing planning of security arrangements. Any assessments conducted by facilities managers to determine the risk from natural hazards are to be reviewed by security personnel to ensure security contingency response plans for natural-hazard events affecting the premises are compatible with the design and structural elements of the premises. Planning should also consider future changes in the threats the premises may face and the fact that threats may increase faster than premises upgrades can reasonably be made.

17. United Nations premises facing a substantial threat from direct, targeted violence must ensure full-time supervision to oversee the premises' security system (including coordination with the host Government) and to ensure its continual proper operation.

18. Premises security systems must also incorporate fire safety issues[6] and crisis contingency plans, including building evacuation plans and mass casualty plans.[7]

E. Roles and Responsibilities

19. In accordance with the "Framework of Accountability for the United Nations Security Management System"[8] (herein "Framework of Accountability"), the UNSMS is to reinforce and supplement the capacity of the host Government to fulfil its responsibilities for the security and safety of United Nations premises. The Framework of Accountability describes the responsibilities of security managers within the UNSMS in relation to premises security.

20. The Under-Secretary-General for Safety and Security is responsible for overseeing the development of this policy and coordinating its implementation with organizations of the UNSMS.

21. The Designated Official (DO), in consultation with the Security Management Team (SMT), is accountable for ensuring that the SRM process is applied to the United Nations premises in its respective duty stations/missions so that SRM measures recommended for the premises are cost-effective, relevant, implementable and sustainable. SRM measures will respond to the security risks identified and must be designed, implemented, supervised and maintained up-to-date to counter the capable threat actors identified. Special emphasis is placed on investments and procedures that address more than one security risk at the same time. All security arrangements at United Nations premises shall also comply with the current Minimum Operating Security Standards policy and the country-specific Minimum Operating Security Standards requirements.

22. The premises security system must be approved by the DO and implemented within an agreed timeframe according to its priority. Organizations of the UNSMS are responsible for providing adequate funding to meet the premises security needs of their respective agencies. The UNSMS cost-sharing mechanism should be applied to shared or common premises, as appropriate. Notwithstanding this, agencies, funds, programmes and organizations may implement additional SRM measures to their respective premises as they determine appropriate. If there are any significant problems with the proper application or implementation of

[6] See *Security Policy Manual*, Chapter VII, Section C ("Fire Safety").
[7] See *Security Policy Manual*, Chapter IV, Section N ("Policy for United Nations Minimum Operating Security Standards").
[8] See *Security Policy Manual*, Chapter II, Section B.

premises security systems by UNSMS organizations, the DO must contact the Under-Secretary-General for Safety and Security for support and/or intervention at the Headquarters level.

23. The DO and the most senior security professional directly supporting the DO[9], along with the designated representative (and security professional, as applicable) of the UNSMS organization managing the premises, shall establish and maintain contact with both national and local security authorities to confirm the responsibility of host Governments for premises protection and security and to ensure proper host country collaboration in the planning, developing and maintaining of the United Nations premises security system. If host Government support is insufficient, the DO must contact the Under-Secretary-General for Safety and Security for support and/or intervention at the Headquarters level.

24. If premises are purpose-built for use by an organization of the UNSMS, the security system for that premises, and the capital investment required, must be included in the earliest stages of planning.

25. The evaluation of premises for rent or purchase by an organization of the UNSMS must examine security consideration as early as possible and take into full account area-specific requirements, conditions and considerations.

26. Based on the outcome of the SRM process and prevailing conditions, a recommendation will be made by the DO, in consultation with the SMT, as to whether common premises, single-agency premises or a more diverse United Nations premises approach is appropriate to respond to the particular security threats and risks to the United Nations. Decisions on common premises must be guided by realistic assessments about the ability to create an appropriate premises security system for one location that will adequately protect a large number of staff despite the high-visibility and high value of the "target". Cost-saving should never be the primary decision-maker with regard to common premises.

27. United Nations security professionals are responsible for determining the security risks to United Nations premises through the SRM process and shall advise the DO, SMT and the UNSMS organization responsible for the premises. During the SRM process, security personnel shall engage with respective facilities managers to ensure that the required security response to non-security risks, such as natural hazards, are reflected in security plans and procedures. Security professionals should also consider occupational health and safety issues in the development of security contingency response plans.

[9] This is usually the Chief Security Adviser (CSA) or other Security Adviser (SA), or their officer-in-charge *ad interim*. Where a CSA or SA is not present, this term is equivalent to the titles of Chief Security Officer, Chief of Security and Safety Services, Country Security Focal Point (CSFP) or Local Security Assistant (if necessary in countries where no international professional security adviser has been assigned or is present).

28. While evaluating the security of premises and recommending appropriate security measures, United Nations security professionals should, when necessary, consult and/or engage necessary technical expertise[10] and applicable UNSMS guidelines and technical standards.

F. Additional Considerations

29. Existing Inter-Agency fora, such as the Inter-Agency Network for Facilities Managers, the United Nations Development Group Task Team on Common Premises and, at the country level, Operations Management Teams should network and integrate efforts of all United Nations premises stakeholders. The United Nations Department of Safety and Security and the UNSMS organizations Security Focal Points have to participate in the above to allow proper mainstreaming of safety and security in premises decisions.

30. Training for premises security planning and operation is to be developed and provided by the United Nations Department of Safety and Security and other appropriate UNSMS organizations to all relevant personnel.

31. The implementation of the present policy will be monitored and supported by the compliance, evaluation and monitoring processes of the United Nations Department of Safety and Security.

32. In accordance with the United Nations "Use of Force Policy", deadly force can never be used to defend property.

G. Final Provisions

33. This policy is meant to be shared with all United Nations personnel.

34. This policy enters into effect on 08 November 2012.

[10] Technical experts, if not available "in-house" may include, but are not limited to, qualified architects, engineers, design consultants, construction and blast engineers, counter-terrorism experts, law enforcement personnel, safety and security specialists and building management officials.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter IV

SECURITY MANAGEMENT

SECTION F

Special Events Organized or Sponsored by United Nations Security Management System Organizations

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 8 November 2012
Technical Review: 1 May 2017

A. Introduction

1. United Nations Security Management System (UNSMS) organizations sponsor and organize a large number of events and conferences each year. These events and conferences often gather large numbers of United Nations personnel and other participants in locations that are normally not under organizational control. These unique security challenges and the broad variations in size, scale and security requirements for these events necessitate a UNSMS policy. This policy should be read in conjunction with the *Security Management Operations Manual* (SMOM) guidelines entitled "Security Arrangements for Special Events Organized or Sponsored by United Nations Security Management System Organizations".

B. Purpose

2. The purpose of this policy is to ensure the proper management of security issues associated with special events organized or sponsored by UNSMS organizations.

C. Application/Scope

3. The policy is applicable to all organizations participating in the UNSMS.

D. Conceptual Framework

4. UNSMS organizations routinely coordinate and organize meetings and other similar events as part of their regular country program or normal work both within and outside their respective office facilities. These meetings are program activities that fall within the normal scope of the Program Assessment within the Security Risk Management process and are not the focus of the present policy.

5. Some events (herein "Special Events"), however, create unique security challenges because of their scope, size or public profile. To ensure that these unique security requirements are properly met, this policy outlines the key notifications and planning steps required.

E. Definitions

6. For the purposes of this policy, a "Special Event" is defined as any event, conference, meeting or special conference sponsored or organized by a UNSMS organization that meets all of the following criteria:

   (a) The event is held at a venue other than a UNSMS organization's premises;

   (b) Participants include both personnel and other individuals of the organizations[1] and third parties (i.e., government officials or private individuals) are participating in the event.

[1] As per *Security Policy Manual* Chapter III "Applicability of UN Security Management System"

(c) The UNSMS organization has concluded or intends to conclude a legal agreement with the host country with respect to the "Special Event".

F. Notification

7. The responsibility of each UNSMS organization is to notify the Designated Official (DO) and most senior security professional[2] of their programme activities; however, each organization shall make specific notification of any event that they are planning that would meet the criteria of a Special Event as per paragraph 6 above.

8. The most senior security professional directly supporting the DO will inform the headquarters of the United Nations Department of Safety and Security (UNDSS) of the above notification.

9. This notification is not a request for clearance for the conference to take place. It merely initiates the required process, including allowing the DO to determine whether the security situation permits the holding of the conference and assess whether adequate security measures can be implemented for the conference.

10. If a UNSMS organization is not sure if its event qualifies as a "Special Event" for the purposes of this policy, it should notify the most senior security professional directly supporting the DO, who will work with the headquarters of UNDSS to clarify the fact.

11. The above notifications should ideally come at least three months in advance of the planned start date of the Special Event.

G. Assessment

12. The most senior security professional directly supporting the DO, in coordination with other security professionals of the UNSMS organizations, will complete the Security Risk Management (SRM) process[3] for the proposed event and venue and make recommendations on the security risk management measures needed to bring the residual security risks to the conference to acceptable levels.

13. The decision about whether a Special Event should be held at any particular location at any particular time must be supported by the SRM process and a resultant security plan that shows the residual security risks to the event will be within acceptable levels. As guidance, Special Events should not normally be held in locations with high and very high residual risks because of the complexity involved in managing security risks to large events in such locations.

[2] This is usually the Chief Security Adviser, other Security Adviser, or most senior security professional directly supporting the DO.
[3] Please refer to *Security Policy Manual* Chapter IV, Section A: Policy on Security Risk Management which entered into force on 18 April 2016

H. Planning and Support

14. If the DO, in consultation with the Security Management Team and on the advice of UNDSS, provides clearance for the event to occur, the Department will coordinate with the most senior security professional directly supporting the DO to establish whether to provide additional specialized assistance is required for the event.

15. Should such additional specialized assistance be needed, an Event Security Coordinator (ESC) will be assigned. Either a security professional with relevant experience from the UNSMS organization sponsoring or organizing the event or UNDSS official(s) will be appointed. The costs of UNDSS personnel appointed to the event will be charged to the hosting organization. The designated ESC will visit the event venue, update the event's SRM process and security plan, update all applicable agreements with the host Government and establish any additional security requirements for the conference. The ESC will work in close collaboration with UNDSS.

16. The UNSMS organization sponsoring or organizing the event shall ensure the all applicable legal documents and agreements (for example, the Host Country Agreement) are established with the relevant government authority hosting the event. In addition, a more detailed operational-level written agreement between the host Government and the UNSMS organization may be required to clarify and confirm the understanding of both parties concerning the division of responsibilities and tasks outlined in the operational plan.

17. The UNSMS organization sponsoring or organizing the event shall request the host Government provide a senior officer to directly supervise and direct all host country security elements supporting the Special Event. This senior officer must work in close cooperation with representatives of UNDSS, where applicable.

18. More details on the above are found in the *Security Management Operations Manual* guidelines entitled "Security Arrangements for Special Events Organized or Sponsored by United Nations Security Management System Organizations".

I. Final Provisions

19. This policy is to be made available to all United Nations personnel.

20. This policy enters into effect on 08 November 2012.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter IV

SECURITY MANAGEMENT

SECTION G

Close Protection Operations

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 15 April 2012
Technical Review: 1 May 2017

A. Introduction

1. The primary responsibility for the security and protection of staff members rests with the host country. Senior United Nations officials can face an increased risk of security incidents due to their potentially higher visibility and the fact that they are often required to issue statements which may make them a focus of hostile entities. Protective Services are designed to enable the ongoing presence of the Senior United Nations Official facing an increased risk. Protective Services deliver a range of flexible options, of which close protection operations are used to manage the highest risk

B. Applicability

2. The policy is applicable to all security personnel and managers in United Nations Security Management System (UNSMS) organizations who are responsible for providing or coordinating protective services, including close protection.

3. Member State-provided close protection teams (e.g., police or military contingents) that are not employed on United Nations contracts are exempt from the provisions of this policy.

C. General Policy

4. Close protection operations are a viable method to manage risks to the security and dignity of United Nations officials. Close protection operations are defined as the 24/7 provision of multiple protection officers, armed, in concentric layers of defence around the protected person to prevent or minimize the effects, primarily through extraction from the area, of an attack intended to cause physical harm or embarrassment.

5. The UNSMS System provides a mechanism by which the need for close protection arrangements can be assessed and delivered where deemed necessary.

6. At the guidance of the General Assembly, close protection is provided on a permanent basis to the following:

   (a) The President of the General Assembly;

   (b) The Secretary-General;

   (c) The Deputy Secretary-General.

7. The deployment of close protection in all other circumstances will be based upon the Security Risk Management (SRM) process and generally for official business only. Further provisions in circumstances under which close protection may be deployed are provided in the *Manual of Guidance on Protective Services*.

8. The SRM process will be conducted according to the procedures outlined in *Security Policy Manual* (SPM), Chapter IV, Section A "Policy on Security Risk Management (SRM)".

9. Armed United Nations close protection officers shall be permitted access to all premises and vehicles of organizations of the UNSMS when required to do so as part of their official duties.

D. Notification and Assessment

10. The SRM process will be conducted upon the assignment or travel on official business of a Senior United Nations Official

11. A Senior United Nations Official is defined as an Executive Head of an organization participating in the UNSMS.

12. The United Nations Department of Safety and Security (UNDSS) will maintain a confidential, ongoing review of those Senior United Nations Officials identified as facing an elevated threat and will conduct the SRM process with consideration for these officials. The respective Security Focal Point will be informed of the inclusion of their Senior United Nations Official in this process and is responsible for notifying the UNDSS of the intended travel itinerary and programme. This notification commences the assessment process.

13. The SRM process for all other Senior United Nations Officials will be conducted upon request from the officials concerned.

14. The need for close protection for individuals not included in the definition of a Senior United Nations Official and for those whom the United Nations retains a duty of care, such as Goodwill Ambassadors and Messengers for Peace, will be assessed upon specific requests from the respective organizations.

15. In all circumstances, notification should be made in writing and email to the Under-Secretary-General for Safety and Security at least ten full working days prior to travel and must include details of the itinerary and programme. Where emergency travel is undertaken or changes to existing travel plans are made in transit, the UNDSS should be informed at the earliest opportunity.

E. Operational Planning

16. The most senior security professional directly supporting the Designated Official (DO)[1] in the location to be visited or assigned to is responsible for producing documents related to the following:

[1] This is usually the Chief Security Adviser or another Security Adviser, including their officer-in-charge *ad interim*. Where a Chief Security Adviser or Security Adviser is not present, this term is equivalent to the titles of Chief Security Officer, Chief of Security and Safety Services or the Local Security Assistant (if necessary for countries where no international professional security adviser has been assigned or is present).

(a) The SRM process;

(b) The Concept of Security;

(c) The Operational Plan.

17. Where the DO determines that no capability exists within the country to undergo the SRM process on the Senior United Nations Official, the Division of Regional Operations in the UNDSS may assign additional expertise to assist.

18. The Concept of Security is a broad overview of the security requirements for the operation, including arrival and departure protocols, during movement, at the accommodation and office or event location, and medical support. It includes the division of responsibility between the host country and United Nations, the chain of command for the operation and the intended providers for each requirement. It also outlines any additional assets not available in-country which the UNDSS must source. The Concept is designed to be shared with the headquarters of the UNDSS for information and the Security Focal Point of the Senior United Nations Official for approval, without risking breaches of confidentiality, and it should include a cost estimate.

19. The Operational Plan is a detailed schedule of the implementation of the Concept of Security, with timings and contingencies for each phase of the operation and emergency actions, communications schedules and contact details and linkage with the host country. The Plan is to be kept strictly confidential and would not normally be shared beyond the DO, the most senior security professional directly supporting the DO and any individuals assisting in the implementation of the Operational Plan.

20. Where no capability exists to prepare the Concept of Security and/or the Operational Plan, the UNDSS may assign additional experts to assist.

21. The decision to deploy a close protection team from the United Nations, either in support of host country resources or where these are unavailable, will form part of the SRM process, recommended by the senior most security professional to the Designated Official.

22. The DO will determine whether the recommendations on close protection are approved or revised.

F. Coordination and Resourcing

23. Where close protection is to be deployed, the most senior security professional directly supporting the DO will appoint an officer in country to act in the role of Close Protection Coordinator to implement the Operational Plan.

24. The Protection Coordination Unit of the UNDSS will facilitate the liaison between the Close Protection Coordinator and the Security Focal Point to the office of the Senior United Nations Official, on a confidential basis.

25. Funding for the close protection detail will be provided by the participating organization sponsoring the visit. In instances of contention, the Protection Coordination Unit will facilitate dialogue between the Security Focal Point to the office of the Senior United Nations Official and senior management within the UNDSS to obtain resolution.

G. Delivery and Review

26. United Nations Close Protection Officer training and refresher courses are required for any individual to function as a United Nations Close Protection Officer.[2]

27. The delivery of any close protection arrangements will be carried out in accordance with the *Manual of Guidance on Protective Services* and the United Nations Use of Force Policy as found in *Security Policy Manual* (SPM), Chapter IV, Section H.

28. The Protection Coordination Unit will conduct a Post Operational Review with input from the office of the Senior United Nations Official, the Close Protection Coordinator and the close protection provider to identify best practices and lessons learned.

H. Final provisions

29. This policy is meant to be distributed to all United Nations personnel.

30. This policy enters into force on 15 April 2012.

31. "United Nations Policy on Close Protection Operations" (08 October 2008) is hereby abolished.

[2] At its 14th Session in January 2011, the IASMN decided that all close protection officers must be fully certified to the UNDSS specified standard by 01 January 2015.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter IV

SECURITY MANAGEMENT

SECTION H

Use of Force Policy

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 8 April 2011
Technical Review: 1 May 2017

A. Introduction

1. The United Nations recognizes and respects the value and integrity of each and every human life. Deciding whether to utilize force when authorized in the conduct of official responsibilities is one of the most critical decisions made by a United Nations security official. It is a decision which must be made quickly and under difficult, often unpredictable and unique circumstances. Sound judgment and appropriate exercise of discretion will always be the foundation of decision-making in the broad range of possible use of force situations. The official will necessarily have to select what type of action, ranging from verbal warnings or instructions to the use of a force, including deadly force, is appropriate based on the nature of the threat to be negated and the specific circumstances of the incident.

2. While detailed policy guidance is provided in training and must serve as the basis for any official's decision on what type of force to use, if any, this is no substitute for good judgment that must be exercised at all times.[1] United Nations security officials are always to bear in mind that when the use of force is unavoidable, they will act with restraint, respecting and preserving human life and causing the minimum harm to people and property.

B. Purpose

3. The purpose of this policy is to provide United Nations security officials with guidelines and restrictions for the use of force (both Non-Deadly Force and Deadly Force). This policy is based on the highest standards of international guidelines and human rights law.[2]

C. Applicability

4. This policy applies to United Nations security officials at the Security Service, General Service, Field Service and Professional levels as well as other contracted security personnel responsible for the protection of United Nations personnel, visitors and assets.

[1] Detailed guidance on the implementation of the Use of Force Policy is set out in the United Nations Department of Safety and Security *Manual of Instruction on Use of Force Equipment including Firearms*. The full range of options in the use of force is covered in training.

[2] Reference is made to the Memorandum dated 21 June 2007 from the Asssitant Secretary-General of Legal Affairs to the Deputy Under-Secretary-General for Safety and Security. It is noted that specific host country use of force laws and policies may impact this United Nations policy. United Nations security officials responsible for the implementation of this policy should confer with their local legal counsel.

D. Definitions

5. Deadly Force means any force that creates a substantial risk of causing death or serious bodily injury.

6. Non-Deadly Force means any use of force other than that which is considered deadly force. This includes any physical effort used to control or restrain another, or to overcome the resistance of another.

7. Serious Bodily Injury means physical injury which creates a substantial risk of death, or which causes serious and protracted (i.e., long-term) disfigurement, protracted impairment of health or protracted loss or impairment of the function of any bodily organ.

8. Bodily Injury means any physical injury other than that which is considered serious bodily injury.

E. Essential Criteria for the Use of Force

9. The following essential criteria must be applied:
   (a) The force is reasonable, proportional to the threat offered and the minimum required to negate the threat;
   (b) The force is necessary, under all the circumstances known at the time, to negate the threat;
   (c) There is no other reasonable alternative available.

F. Criteria for the Use of Non-Deadly Force

10. Based on the three essential criteria above, a United Nations security official may use Non-Deadly Force**:**
    (a) In defence of him/herself, other United Nations personnel and/or others against imminent threat of bodily injury;
    (b) To maintain order and security within and/or restrict access to United Nations premises; and prevent damage to United Nations premises or property;
    (c) To detain[3] and/or prevent the escape of a person who constitutes a threat to order and security and/or who has committed a serious crime.

G. Criteria for the use of Deadly Force

11. Based on the three essential criteria in 9 above, a United Nations security official may only use Deadly Force:

[3] The right to detain is set out in ST/AI/309/Rev 2, dated 18 February 1997

(a) To defend him/herself, other United Nations personnel and/or others against an imminent threat of death or serious bodily injury and there is no other reasonable alternative available.

H. Additional Considerations

Decision to Use Force

12. As a first step in the use of force, security officials will audibly instruct the subject to comply. If, however, giving such an instruction would pose a risk to the security official or others, it need not be given. When a decision is made to use force the security official should act decisively and without hesitation, using force proportional to the threat and the minimum required to negate the threat. A United Nations security official is not required to place him/herself or others in unreasonable danger before acting.

Post Application of Force

13. Once force has been applied and the threat negated, the security official must:

    (a) Where feasible, arrange for appropriate medical aid to the person subjected to the use of force; and

    (b) Follow all relevant procedures, including reporting the incident to the supervisor, and cooperate with United Nations investigations.

14. A security official involved in the application of non-deadly or deadly force may be provided with stress and medical counselling as appropriate.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter IV

SECURITY MANAGEMENT

SECTION I

Armed Private Security Companies

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 8 November 2012
Technical Review: 1 May 2017

A. Introduction

1. The primary responsibility for the security and protection of United Nations personnel, their eligible family members and the premises and property of United Nations Security Management System (UNSMS) organizations rests with the host Government. In ensuring such safety and security, certain circumstances may arise where armed security services become necessary. When the host Government is unwilling or unable to provide such protection, as determined by the United Nations in consultation with the relevant authorities, armed security services will normally be provided by alternate Member States or the appropriate security entity within the United Nations system.

2. On an exceptional basis, to meet its obligations the UNSMS may use private companies to provide armed security services when threat conditions and programme need warrant it.

3. The fundamental principle guiding when to use armed security services from a private security company is that this may be considered only when there is no possible provision of adequate and appropriate armed security from the host government, alternate Member State(s) or internal United Nations system resources such as the Security and Safety Services or security officers recruited directly by a mission or through another UNSMS organization.

B. Purpose

4. In circumstances where a UNSMS organization determines that armed security services from a private security company are required, the engagement and use of such services will be governed by a clear accountability and responsibility framework and clear operational standards and oversight. Further details are stipulated in the accompanying "Guidelines on the Use of Armed Security Services from Private Security Companies".

5. The present policy describes the fundamental pillars of the decision-making framework, the assessment process and standards for such decisions.

C. Applicability

6. This policy is applicable to all security professionals and managers in the United Nations Security Management System in accordance with Security Policy Manual, Chapter II, Section B, entitled "The Framework of Accountability for the Security Management System".

7. This policy applies to the selection, contracting and management of any armed security services from private security companies by an organization participating in the UNSMS.

D. General Policy

8. The objective of armed security services from a private security company is to provide a visible deterrent to potential attackers and an armed response to repel any attack in a manner consistent with the United Nations "Use of Force Policy", respective host country legislation and international law.

9. Armed security services from a private security company may not be contracted, except on an exceptional basis and then only for the following purposes:

    a. To protect United Nations personnel, premises and property.

    b. To provide mobile protection for United Nations personnel and property.

10. The details of the services outlined in paragraph 9 above are contained in the accompanying "Guidelines on the Use of Armed Security Services from Private Security Companies".

11. The approval of the Under-Secretary-General for Safety and Security must be obtained prior to commencing the process of engaging a private security company.

E. Security Risk Management

12. The decision to use armed security services must be based upon a specific Security Risk Management Process (SRM).

13. The SRM will be conducted in accordance with *Security Policy Manual*, Chapter IV, Section A ("Policy on Security Risk Management")[1].

14. The SRM must be supported by further analysis and recommendations on the need for an armed security capability and on the most appropriate provider for that capability, as outlined in Section F.

15. Armed security services from private security companies will be considered on an exceptional basis only when the SRM and supporting analysis and recommendations have concluded that the fundamental principle guiding the use of armed security services from a private security company, outlined in paragraph 3, has been met.

F. Roles and Responsibilities

16. The responsible most senior security official identified by the Under-Secretary-General for Safety and Security, usually the Designated Official (DO) supported by the Security Management Team (SMT), must evaluate any potential negative impacts the contracting of armed security services from a private security

[1] The Policy on Security Risk Management entered into force on 18 April 2016.

company could have on the United Nations system and its programmes. The analysis of the potential negative impacts should encompass, *inter ali*a, the prevailing usage of private security companies in the area of operation as well as globally, host country and local community acceptance of armed security services from private security companies and the local history of negative impacts of incidents involving private security companies and their armed security services.[2]

17. When the DO and the SMT agree that the use of armed security services from a private security company is justified, a request for approval must be submitted to the Under-Secretary-General for Safety and Security for consideration. The Executive Heads of the affected agencies, funds and programmes or the head of Department for Secretariat-led field operations must be copied on this request.

18. The request for approval will include the related SRM, explanations of why armed security services cannot or should not be provided by the host government, alternate Member States or internal UNSMS resources and details of the assessment of the potential negative impacts of engaging armed security services from a private security company.

19. The Under-Secretary-General for Safety and Security shall reply in writing as to whether he/she approves the request for the use of armed security services provided by private security companies.

20. Where approval for the use of armed security services provided by private security companies is granted, at each contract renewal the full approval process must be implemented, including a new assessment of the primary options of host governments, alternate Member States or internal United Nations system resources for such provision.

G. Selection Criteria for the Armed Private Security Company

21. In cases where the Under-Secretary-General for Safety and Security has approved the use of armed security services from a private security company, companies bidding for the contract must meet the mandatory requirements for possible selection. The mandatory requirements are described in the "Guidelines on the Use of Armed Security Services from Private Security Companies".

22. The selection of armed security services from a private security company shall be undertaken in accordance with the applicable UNSMS organization's rules and regulations from those companies that meet the requirements stipulated in paragraph 21 above.

[2] For examples of the humanitarian considerations in this analysis, reference should be made to IASC Guidelines on the Use of Armed Escorts for Humanitarian Convoys, found at: *https://docs.unocha.org/sites/dms/Documents/Armed%20Escort%20Guidelines%20-%20Final.pdf*

H. Screening Requirements for the Personnel of the Armed Private Security Company Selected

23. The private security company wishing to provide armed security services to an organization participating in the UNSMS shall confirm to that organization, in writing, that the mandatory screening process for its personnel, as outlined in the "Guidelines for Armed Security Services from Private Security Companies" has been conducted and that only personnel who meet the mandatory requirements will be used to provide armed security services to the UNSMS organization in question.

I. Use of Force, Weapons Manual and Standard Operating Procedures

24. Any private security company wishing to provide armed security services to an organization participating in the UNSMS is required to develop and implement:

    a. Its own Use of Force Policy consistent with the applicable national laws of the state in which the services are to be provided and, to the extent consistent with the applicable national law, with the United Nations "Use of Force Policy" as found in Security Policy Manual, Chapter IV, Section H (which shall be made available to the private security company for reference). However, the Use of Force Policy of the private security company must be as or more restrictive than the "United Nations Use of Force Policy". The private security company's Use of Force Policy shall not be less restrictive than the "United Nations Use of Force Policy". In addition, the private security company's Use of Force Policy shall be consistent with the International Code of Conduct for Private Security Service Providers[3];

    b. Its own firearms management procedures and "Weapons Manual" consistent with the applicable national laws of the state in which the services are to be provided and, to the extent consistent with the applicable national law, with the "United Nations Department of Safety and Security Manual of Instruction on Use of Force Equipment, including Firearms" (which shall be made available to the private security company for reference). However, the private security company's Weapons Manual must be as or more restrictive than the "United Nations Department of Safety and Security Manual of Instruction on Use of Force Equipment, including Firearms". The private security company's Weapons Manual shall not be less restrictive than the "United Nations Department of Safety and Security Manual of Instruction on Use of Force Equipment, including Firearms". In addition, the private security company's firearms management procedures and Weapons Manual should also be consistent with the International Code of Conduct for Private Security Service Providers;

[3] See http://www.icoc-psp.org/

c. The necessary standard operating procedures for the implementation of the contract in consultation with the UNSMS organization involved.

J. Training Requirements to be met by the Private Security Company

25. The private security company is required to ensure that its personnel have the requisite skills and experience to perform the services in accordance with the contract and standard operating procedures (see paragraph 24(c) above).

26. Before commencing the provision of services to the UNSMS organization in question, the private security company must provide a written certification to that organization that each of the company's personnel has undergone the above training and demonstrated the necessary level of skill.

K. Management and Oversight

27. The day-to-day management of the contract is the function of the UNSMS organization that has engaged the private security company, and that organization shall provide a daily on-site inspection of the private security company.

28. In circumstances where a private security company is hired to provide armed security services to a common United Nations facility or a common United Nations operation, it is the responsibility of the most senior security professional directly supporting the DO[4] to:

    a. Ensure that the on-site inspection of the private security company is completed;

    b. Ensure that a monthly review of the performance of the private security company is also completed;

    c. The on-site inspections and the monthly review may be delegated to members of the Security Cell, but the most senior security professional directly supporting the DO will remain accountable for their completion.

29. The most senior security professional directly supporting the DO and an official of the contracting organization must immediately submit a joint report of any performance issues or concerns identified, along with recommended remedial action, to the DO and the Country Representative of the organization concerned for approval.

[4] For the purposes of this policy, this is the Chief Security Adviser, Security Adviser, Chief of Security and Safety Services, or their respective officer-in-charge *ad interim*.

L. Training and Compliance

30. This policy is to be part of the training for DOs, SMT members, security professionals and managers in UNSMS organizations who have responsibility and accountability for managing security for their organization.

M. Utilization of Common Security Funding for Armed Private Security Companies

31. In instances where armed security services from private security companies are funded through the local Common Security Budgets (CSB), a specific budget line indicating the amount for these services must be included in the local security cost shared budget.

N. Enforcement

32. United Nations personnel that fail to abide by the terms of this policy may be subject to administrative measures.

O. Final Provisions

33. This policy is to be made available to all United Nations personnel.

34. This policy enters into effect on 8 November 2012.

35. Annex O of the Field Security Handbook is hereby abolished.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM

Security Policy Manual

Chapter IV

SECURITY MANAGEMENT

SECTION J

Arming of Security Personnel

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 18 April 2016
Technical Review: 1 May 2017

A. Introduction

1. The primary responsibility for the security and protection of United Nations personnel and other individuals covered by the United Nations Security Management System (UNSMS) rests with the host Government. However, circumstances may arise where it may be mandated or otherwise necessary to supplement existing host Government capacity with, inter alia, armed United Nations peacekeepers, including United Nations guard units provided by Member States or private security services.[41] Under certain circumstances, when such options are not available, applicable, appropriate or sufficient, the arming of trained[42] security professionals may be considered in order to protect UNSMS personnel. In those instances, there are specific principles and procedures established in this policy that must be followed.

B. Purpose

2. The purpose of this policy is to outline the strict framework under which UNSMS security personnel, designated under paragraph 4 below, may be authorized to carry arms. Detailed provisions, including guidelines, procedures and standards, for arming such personnel are found in the United Nations Department of Safety and Security's (UNDSS) *Manual of Instruction on Use of Force Equipment, including Firearms* ("*Manual of Instruction*").[43] The *Manual of Instruction* shall be read in conjunction with this policy, but it shall not be interpreted as limiting or prejudicing this policy in any way.

C. Applicability

3. This policy is applicable to all organizations participating in the UNSMS.

4. This policy contains specific provisions applicable to the following categories of UNSMS security personnel:

    - UNSMS security personnel assigned under UNDSS/Division of Headquarters Security and Safety Services (DHSSS);[44]

    - All other UNSMS security personnel with specific protection

[41] See UNSMS *Security Policy Manual*, Chapter IV ("Security Management"), Section I ("Armed Private Security Companies").
[42] For the purpose of this policy, training refers to the specific training in use of firearms, including safety, technical qualification and unit tactics.
[43] The Terms of Reference for the Weapons Committee are found under Annex B of the UNDSS *Manual of Instruction of Use of Force Equipment, including Firearms*.
[44] This includes all UNSMS security personnel assigned globally under UNDSS Security and Safety Services (SSS).

functions, such as Close Protection Officers,[45] guard force managers, guards or security personnel performing escort operations; and

- All other UNSMS security personnel who do not normally have protection functions, who may be temporarily assigned protection functions under exceptional circumstances and in accordance with the strict provisions contained in this policy.

D. Principles

5. Arming of United Nations security personnel shall be subject to national and local laws and regulations, as applicable, as well as any existing agreements between the United Nations and the host Government, such as Status of Forces Agreements (SOFAs) or Status of Mission Agreements (SOMAs).

6. The Under-Secretary-General for Safety and Security may authorize the arming of UNSMS security personnel in a Designated Area, based on their specific functions, as outlined in paragraph 4 above. Such authorization constitutes a Security Risk Management (SRM) measure[46] and therefore, the security considerations for arming UNSMS security personnel shall be based upon the approved SRM process for the Designated Area when there are risks that cannot be mitigated by the host Government, United Nations guard units provided by Member States or private security services, or when such options are not available, applicable, appropriate or sufficient.

7. Arming of UNSMS security personnel shall be subject to a formal recommendation and authorization process, as detailed in this policy, as well as strict compliance and oversight mechanisms. Authorization shall only be granted to UNSMS security personnel who are trained and certified[47] to carry arms issued by UNSMS organizations.

7..1.1. With regard to the arming of DHSSS personnel in particular, it is recognized that Security Officers assigned under DHSSS are required to carry arms whenever on duty.[48] The roles and responsibilities of such personnel are detailed in the *Manual of Instruction*. The recommendation and authorization process for arming such personnel, along with the revocation process for such

[45] See UNSMS *Security Policy Manual*, Chapter IV ("Security Management"), Section G ("Close Protection Services").
[46] Please refer to UNSMS *Security Policy Manual* Chapter IV, Section A, Policy on Security Risk Manageement, which entered into force on 18 April 2016.
[47] In accordance with the *Manual of Instruction* and specific provisions contained in this policy (see footnotes 2 and 11 and section H "Training Framework").
[48] See Secretary-General's report A/56/848, paragraph 34(b) ("It is a standard requirement that all United Nations security officers carry firearms when on duty").

personnel once armed, shall continue to be governed by the *Manual of Instruction*.

7...1.2. With regard to other UNSMS security personnel, this policy distinguishes between the following two categories:

7...1.2.1. UNSMS security personnel whose primary role or responsibility is to perform a protection function, such as Close Protection Officers,[49] guard force managers or security personnel performing escort operations; such personnel may be armed in accordance with the Recommendation and Authorization Process found in this policy (see Section F, "Recommendation and Authorization Process"); and

7...1.2.2. UNSMS security personnel whose primary role or responsibility does not normally involve a protection function; such personnel may only be armed under exceptional circumstances in a Designated Area and only to the extent required to perform a specific protection function, including, but not limited to, circumstances where there is an imminent threat to life. Such personnel shall be assigned protection functions and armed in accordance with the Recommendation and Authorization Process found in this policy (see Section F, "Recommendation and Authorization Process"), if appropriately trained[50] and certified to carry a firearm for the period specified.

8. Given UNSMS organizations' accountability and responsibility for their personnel, in line with the *Framework of Accountability*,

- UNSMS organizations are required to promulgate their internal policies in line with this policy, the *Manual of Instruction* and the *Use of Force Policy,* qualifying if their security personnel are authorized to carry out protection functions or further restricting or barring them from carrying arms under any circumstances.

- UNSMS organizations may also determine that UNSMS security personnel authorized to carry a firearm do not carry their weapon when accompanying their personnel, entering their premises or utilizing their assets (e.g., vehicles and aircraft), particularly if doing so would violate their organization's policies, as identified above, or would harm an organization's ability to deliver its

[49] See UNSMS *Security Policy Manual*, Chapter IV ("Security Management"), Section G ("Close Protection Services").
[50] Training in use of firearms for this function includes safety, technical qualification and unit tactics.

programmes or fulfil its mandates.

E. Roles and Responsibilities

Under-Secretary-General for Safety and Security

9. Through this policy, the Under-Secretary-General for Safety and Security has authority to authorize the possession and use of arms for UNSMS security personnel, in order to strengthen the safety and security of UNSMS personnel.

10. In exercising this authority, the Under-Secretary-General for Safety and Security shall be responsible for authorising, in writing, inter alia, the following:

    - Specific Designated Areas, in which UNSMS security personnel, designated under paragraphs 7b above, may carry arms. Such personnel shall be personally identified, including their specific functions or titles, and the duration and circumstances of their authorization;

    - Specific types of standard or alternative weapons, weapon systems or ammunition that such personnel may carry, dependent upon their current training certification for the weapons indicated.

11. The Under-Secretary-General for Safety and Security shall be the final decision maker regarding all requests to arm UNSMS security personnel in a Designated Area, in accordance with this policy, the *Manual of Instruction* and relevant Standard Operating Procedures (SOPs).

UNDSS Weapons Committee

12. The UNDSS Weapons Committee shall report to the Under-Secretary-General for Safety and Security, through the Director of DHSSS as Chair of the Weapons Committee, and shall adhere to the provisions of this policy, the *Manual of Instruction* and relevant SOPs.[51] The Weapons Committee serves as a technical advisory body and is responsible for, *inter alia*, the following:[52]

    - Reviewing requests to authorize the arming of UNSMS security personnel based on their specific functions in a Designated Area as outlined in this policy and taking into consideration UNDSS' Division of Regional Operations (UNDSS/DRO) final request, including input from Security Focal Points (SFPs) of UNSMS

[51] Including, but not limited to, UNDSS Headquarters Standing Operating Procedure (SOP), "Requests to the Under-Secretary-General for Safety and Security to Approve the Carriage of Firearms," dated 18 March 2015.
[52] UNDSS *Manual of Instruction of Use of Force Equipment, including Firearms*, paragraphs 1.19-1.20.

organizations with a presence in the Designated Area and making appropriate recommendations to the Under-Secretary-General for Safety and Security to grant or deny such requests in accordance with the SRM process;

- Reviewing requests to add or remove standard or alternative weapons, weapon systems or ammunition in a Designated Area and making appropriate recommendations to the Under-Secretary-General for Safety and Security to grant or deny such requests in accordance with the SRM process;

- Conducting an annual review of weapons, weapon systems and ammunition as found under Annex D of the *Manual of Instruction*;

- Providing input on policies, procedures, guidelines and standards related to weapons, weapons systems and ammunition; and

- Monitoring trends and advances in protective weapons and weapon systems technology.

13. UNSMS organizations shall collectively designate a representative from the IASMN to the Weapons Committee when required.

UNDSS' Division of Regional Operations

14. UNDSS/DRO shall be responsible for the following:

- Communicating the DO initial request to arm UNSMS security personnel in a Designated Area to Security Focal Points (SFPs) of UNSMS organizations with a presence in the Designated Area for their input;

- Validating that the request is in line with the SRM process, including that there is no other alternative mitigation measure to provide protection functions.

- Validating that the staff assigned to the functions proposed to be armed are supported by UNDSS/DRO on the condition that the required United Nations training and certification for the type of weapons proposed is successfully completed.

- Reviewing the DO's initial request, taking into consideration the input of SFPs of relevant UNSMS organizations;

- Submitting a final, written request to authorize the arming of UNSMS security personnel to the Chair of the UNDSS Weapons Committee. Such personnel shall be identified by name with their specific functions or titles, the duration and circumstances for their authorization shall be indicated;

- Maintaining close oversight over all aspects of implementation and operations for armed security personnel, including any revocation instituted by the Chief Security Adviser/Security Adviser (CSA/SA) or Chief Security Officer (CSO) in the field.

- Establishing a fact-finding investigation in all instances of discharge of weapons for any reason other than at a recognized and approved range training area for certification and training purposes.

Designated Official for Security/Security Management Team (SMT)

15. Under the Framework of Accountability, the DO for Security, advised and supported by the SMT, is responsible for the safety and security of UNSMS personnel, premises and assets in the Designated Area.

16. In fulfilling this responsibility, the DO, advised and supported by the SMT, shall be responsible for, *inter alia*, the following:

    - Considering and balancing any negative consequences of arming UNSMS security personnel, including with respect to the delivery of United Nations programmes and fulfilment of United Nations mandates, and recording them in the SMT minutes;

    - Requesting to the Under-Secretary-General for Safety and Security in writing, the arming of UNSMS security personnel based on specific functions in a Designated Area, as outlined in this policy and as determined through the SRM process, where there is no alternative mitigation measure that can be employed immediately;

    - Approving and issuing a *Firearms Carry Standard Operating Procedure* and other relevant SOPs for the Designated Area based on this policy, the Use of Force policy and the *Manual of Instruction*; and

    - Ensuring adherence to international, national and local laws and regulations as well as any existing agreements between the United Nations and the host Government.

Chief of Security (UNDSS/DHSSS)

17. The roles and responsibilities of the Chief of Security (COS), UNDSS/DHSSS are detailed in the *Manual of Instruction*.

Chief Security Adviser/Security Adviser and Chief Security Officer for Peacekeeping Missions[53]

18. Under the Framework of Accountability, the CSA/SA or CSO for Peacekeeping Missions,[54] as applicable, is responsible for advising the DO and the SMT with respect to their security functions.[55]

19. In fulfilling this responsibility, the CSA/SA or CSO shall be responsible for, inter alia, the following:

- Recommending to the DO/SMT, in writing, the arming of UNSMS security personnel that should be armed, based on their specific required functions in a Designated Area, as defined under paragraph 7b of this policy, in accordance with the SRM process; such personnel shall be identified by name, their specific functions or titles and the duration of their authorization (maximum 3 months); and other mitigation alternatives;

- Developing and implementing a local *Firearms Carry Standard Operating Procedure* and other relevant SOPs;

- Ensuring all UNSMS security personnel, authorized to carry arms in the Designated Area have been appropriately trained and certified to carry and use such arms for the environment required;

- Conducting, where feasible, appropriate background checks for UNSMS security personnel prior to recommending the carriage of arms or attendance of training in the use of weapons;

- Ensuring appropriate mechanisms exist to manage and secure all approved weapons, weapon systems and ammunition;

- Ensuring that relevant UNSMS security personnel authorized by the USG, UNDSS to carry arms in a Designated Area are issued approved distinctive badges, insignia, markings or uniforms to be publicly

[53] May include UNDSS/DHSSS' Chief of Security (COS) when simultaneously serving as the Chief Security Adviser (CSA)/Security Adviser (SA) for a Designated Area.
[54] For the purposes of this policy, any reference to Chief Security Officer (CSO) applies solely in the context of non-integrated Peacekeeping Missions.
[55] May be supported by UNDSS/DHSSS' Chief of Security (COS) if he or she is not simultaneously serving as CSA/SA.

displayed or worn whenever armed while on official business, as required;

- Ensuring that UNSMS security personnel authorized to carry arms by the Under-Secretary-General for Safety and Security do not carry such arms whenever the specific security situation or function to be performed does not warrant the carriage of arms;

- Ensuring that UNSMS security personnel permitted to carry personal arms under international, national, and local laws and regulations, yet not authorized to do so by the Under-Secretary-General for Safety and Security, do not carry such arms whenever on official business, including when accompanying UNSMS personnel, entering UNSMS premises or utilising UNSMS assets (e.g., vehicles and aircraft); and

- Ensuring compliance with this policy, UNDSS *Manual of Instruction*, local *Firearms Carry Standard Operating Procedure* and other relevant SOPs, including through the development of oversight mechanisms and reporting any non-compliance immediately to UNDSS/DRO;

- Notifying Saving Lives Together partners at the field level when firearms authorization has been granted by the Under-Secretary-General for Safety and Security.

Armed UNSMS Security Personnel

20. Armed UNSMS security personnel shall be responsible for the following:

- Abiding by all UNSMS policies and those of their respective parent organization;[56]

- Exercising good judgment at all times and complying strictly with this policy and the terms of the authorization;

- Ensuring maintenance of training and proper certification for the types of weapons they are authorized to carry;

- Carrying distinctive badges, insignia, markings or uniforms to be publicly displayed or worn whenever armed while on official business, as required by their functions;

[56] The Framework of Accountability, paragraph 28, states: "Personnel employed by the organizations of the United Nations system are accountable to their respective organizations. All such personnel, regardless of the rank or level, have the responsibility to abide by security policies, guidelines, directives, plans and procedures of the United Nations security management system and their organizations."

- Refraining from carrying or retaining possession of weapons when off-duty and when not performing the protection function for which the authorization was issued; and

- Respecting and adhering to an individual UNSMS organization's requirement that armed UNSMS security personnel does not carry their arms when accompanying their personnel, entering their premises, or utilizing their assets (e.g., vehicles, aircraft), particularly if doing so would violate the organization's policies or harm the organization's ability to deliver its programmes or fulfil its mandates.

21. Security professionals who have an advisory and managerial role are expected to conduct themselves in a manner that is appropriate with their function even if they have been granted authorization by the USG, UNDSS to carry firearms. They are required to perform their primary advisory role at all times.

F. Recommendation and Authorization Process[57]

22. The CSA/SA or CSO shall submit an initial, written recommendation to the DO/SMT, which shall be based upon or include the following:

- SRM Process: The SRM process must be followed with respect to a Designated Area or a specific mission, whereby the types of threats and the level of risk facing United Nations personnel as well as existing and potential risk management measures are considered;

- Detailed assessment of existing or potential host Government capacity, along with, *inter alia*, armed United Nations peacekeepers, United Nations guard units or private security services, as applicable, to provide for the safety and security of United Nations personnel, premises and assets in a Designated Area or on the specific mission;

- Specific recommendation containing the following:

22...1. UNSMS security personnel, that should be armed, based on the required functions in a Designated Area such personnel shall be identified by name, their specific functions or titles and the duration of their authorization;

22...2. Types of weapons, weapon systems and ammunition that should be issued;

22...3. Geographical areas where such personnel should be armed;

[57] See Annex A ("Flowchart of the Recommendation and Authorization Process").

22...4. Duration that such personnel should be armed; and

22...5. Reasons why such personnel should be armed, in accordance with the SRM process.

- Detailed assessment of existing support mechanisms for procuring the recommended types of weapons, weapon systems and ammunition as well as training and certifying UNSMS security personnel, as required; and

- Detailed assessment of adherence to international, national, and local laws and regulations as well as any existing agreements between the United Nations and the host Government, including but not limited to, SOFAs or SOMAs.

23. The DO, advised and supported by the SMT, shall review the CSA/SA or CSO initial recommendation and, upon agreeing with or modifying its content, submit an initial request to authorize the arming of UNSMS security personnel to UNDSS/DRO. The SMT should be asked to detail the negative consequences of arming UNSMS security personnel, including on the delivery of United Nations programmes and fulfilment of United Nations mandates. The DO's request shall be in writing and shall include the final recommendation, all required assessments under paragraph 22 of this policy, and all dissenting views expressed within the SMT.

24. UNDSS/DRO shall communicate the DO's initial request to SFPs of UNSMS organizations with a presence in the Designated Area for their input. UNDSS/DRO shall subsequently review the DO's initial request, taking into consideration the input of SFPs of relevant UNSMS organizations. Upon agreeing with or modifying its content, UNDSS/DRO may submit a final, written request to authorize the arming of UNSMS security personnel to the Chair of the UNDSS Weapons Committee; such personnel shall be identified by their name, specific functions or titles and the duration of their authorization.

25. The UNDSS Weapons Committee shall review the final request to authorize the arming of UNSMS security personnel, recognised under the Framework of Accountability, based on their specific functions in a Designated Area and make appropriate recommendations to the Under-Secretary-General for Safety and Security to grant, modify or deny such a request. Similarly, it shall review a final request to add or remove standard or alternative weapons, weapon systems or ammunition in a Designated Area and make appropriate recommendations to the Under-Secretary-General for Safety and Security to grant, modify or deny such requests.

26. The Under-Secretary-General for Safety and Security shall respond to the final request in writing with the advice and support of the UNDSS Weapons Committee. The Under-Secretary-General for Safety and Security may authorize the request, with or without modification, or deny the request. The authorization

shall indicate the name of the personnel, the rationale and timeframe for the authorization.

27. The CSA/SA or CSO shall not issue any weapons, weapon systems and ammunition prior to obtaining written authorization from the Under-Secretary-General for Safety and Security. Any issuance of arms must be in accordance with the Under-Secretary-General for Safety and Security' written authorization and the *Manual of Instruction*.

G. Revocation and Suspension Authority

28. The Under-Secretary-General for Safety and Security shall maintain the right to permanently revoke or modify, in writing, a previously granted authorization at any time with the advice and support of the UNDSS Weapons Committee.

29. UNDSS/DHSSS, UNDSS/DRO or UNSMS Security Focal Points may recommend to UNDSS Weapons Committee, in writing, that a previously granted authorization be permanently revoked or modified. The underlying reasons for revocation or modification must be included in the recommendation. Such a recommendation may be initiated at the headquarters level (i.e., by UNDSS/DHSSS or UNDSS/DRO, as applicable) or field level (i.e., by the CSA/SA, CSO or COS, as applicable, through the DO). The UNDSS Weapons Committee shall subsequently make appropriate recommendations to the Under-Secretary-General for Safety and Security to permanently revoke or modify the previously granted authorization.

30. UNDSS/DHSSS and UNDSS/DRO shall maintain the right to temporarily suspend a previously granted authorization for individual UNSMS security personnel. Such a suspension may be initiated at the headquarters level (i.e., by UNDSS/DHSSS or UNDSS/DRO, as applicable) or field level (i.e., by the CSA/SA, CSO or COS, as applicable).

H. Training Framework

31. UNDSS shall maintain a Joint Working Group on Firearms Training, which shall develop the required training standards, competencies and training courses for the various weapons, weapon systems and ammunition employed by the United Nations. UNDSS shall coordinate the delivery of such training courses.

32. Firearms training for security personnel performing protection functions, as indicated in paragraph 7b, shall include safety, technical qualification and unit tactics.

I. Use of Force

33. The use of force shall be governed by the UNSMS Use of Force Policy.[58]

[58] See UNSMS *Security Policy Manual*, Chapter IV ("Security Management"), Section H ("Use of Force Policy").

34. Any discharge of firearm[59] (other than during an approved training session) must be reported immediately to the CSA/CSO, including the time, date and location of the incident and any relevant details. A written report must follow as soon as feasible but no later than 24 hours after the incident.

35. In the event of an investigation into an alleged incident involving UNSMS security personnel and the possession or use of arms (i.e., weapons, weapon systems or ammunition authorized under this policy), the failure of such personnel to abide by the provisions of this policy or other UNSMS policies may warrant administrative or disciplinary action.

36. Investigations will be guided by ST/AI/371/Amend. 1 Disciplinary Measures and Procedures; or respective organizations policies and instructions; and policies of the UNSMS.

J. Final Provisions

37. This policy shall be made available to all UNSMS organizations and to all individuals covered under the UNSMS.[60]

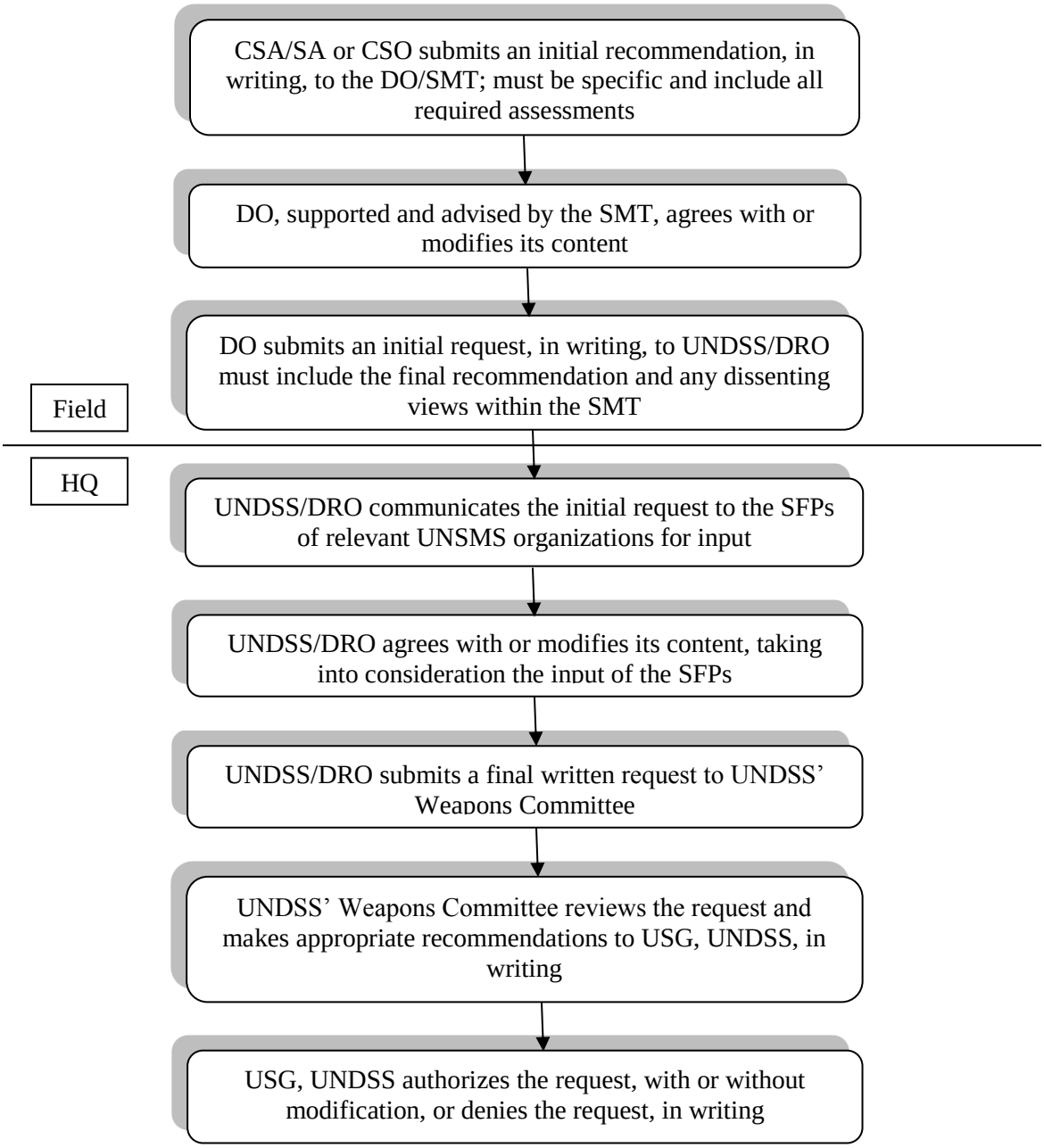
38. This policy enters into force on 18 April 2016.

39. The IASMN and UNSMS organizations will ensure that the *Manual of Instruction, Use of Force Policy* and relevant Standing Operating Procedures (SOPs) are revised in line with this policy and the UNSMS Security Policy Manual (SPM).

[59] See the *Manual of Instruction on Use of Force Equipment, including Firearms* for further guidance.
[60] See UNSMS *Security Policy Manual*, Chapter III ("Applicability of the United Nations Security Management System").

Annex A

Flowchart of the Recommendation and Authorization Process[61]



[61] See the *Manual of Instruction on Use of Force Equipment, including Firearms* for the Recommendation and Authorization Process applicable to UNSMS security personnel assigned under UNDSS/DHSSS.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter IV

SECURITY MANAGEMENT

SECTION K

Unarmed Private Security Services

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 18 April 2016
Technical Review: 1 May 2017

A. Introduction

1. The primary responsibility for the security and protection of personnel employed by the United Nations system organizations, their spouses and other recognized dependants and property, and of the organizations' property rests with the host Government. This responsibility flows from every government's normal and inherent function of maintaining order and protecting persons and property within its jurisdiction. In the case of international organizations and their officials, the Government is considered to have a special responsibility under the Charter of the United Nations or the host Government's agreements with the individual organizations.

2. Without prejudice to the responsibility of the host Government for ensuring safety and security, certain circumstances may arise where it is necessary for the United Nations Security Management System (UNSMS) to supplement the capacity of the Host Government. The UNSMS may use commercial (private) security services for specific security functions, to complement existing UNSMS capacities or to deliver security services in a cost-effective manner without endangering or compromising the security of UNSMS personnel and visitors.[1]

3. The use of armed private security services on an exceptional basis is regulated by the UNSMS policy on Armed Private Security Companies,[2] adopted in 2012. The present policy regulates the use of unarmed private security services (UPSS) providers to ensure a consistent approach, common standards and guidelines for the contracting and management of such services.

4. The fundamental principle of this policy is that the use of UPSS[3] will be governed by a clear accountability framework, common operational standards and the highest degree of oversight in line with United Nations procurement rules, international standards and human rights laws.

B. Purpose

5. This policy provides a list of the services for which UPSS providers may be contracted. It clearly identifies roles and responsibilities with regard to their engagement, management and oversight, including contract termination.

6. Further details are provided in the accompanying 'Guidelines on the Use of Unarmed Security Services from Private Security Companies,' which describes in more detail the decision-making framework, the assessment process and standards for the hiring and management of such companies.

[1] General Assembly Resolution 59/289, "Outsourcing practices," dated 29 April 2005.
[2] *Security Policy Manual*, Chapter IV, Section I ("Armed Private Security Companies")
[3] "Unarmed security services" are outlined in paragraph 11 of this policy and provided in more detail at paragraph 8 of the "Guidelines on the Use of Unarmed Security Services from Private Security Companies".

C. Applicability

7. This policy is applicable to all persons and organizations of the UNSMS in accordance with the *Security Policy Manual* (SPM), Chapter II, Section B, entitled 'The Framework of Accountability for the Security Management System'.

8. This policy applies to the selection, contracting and management of any UPSS from private security companies by any organization participating in the UNSMS.

D. General Policy

9. The UNSMS often establishes physical security systems in order to protect life, maintain order and deter terrorist and criminal attacks against personnel, premises, property and assets of UNSMS members.

10. The representative responsible for the organization's country operation must notify the Designated Official (DO) of the reason for engaging UPSS in the designated area.

11. UPSS duties may include the following:

    (a) Entry control procedures management, screening, perimeter patrolling, escorts, counter-hostile surveillance, mail screening, responding to alarms and training[4]

    (b) Security advisory and assessments services

    (c) Site and specialist technical surveys

    (d) Installation, maintenance and operation of security technology (e.g., close circuit television, tracking systems and communications)

    (e) Safety, fire, traffic and medical services

    (f) Residential guard services

    (g) Other services as defined in the contract and in accordance with this policy.

12. Further details on the services outlined in paragraph 11 above are contained in the accompanying 'Guidelines on the Use of Unarmed Security Services from Private Security Companies'.

13. By definition, members of private security companies who deliver UPSS shall not, at any time, carry firearms. Their equipment shall be limited to non-lethal equipment and their reactions governed by the criteria on the use of non-deadly

[4] Such as Safe and Secure Approach to Field Environments (SSAFE) training

force, identified in the UNSMS Use of Force Policy,[5] applicable host country legislation and international law.

E. Security Risk Management (SRM)

14. The decision to use UPSS must be supported by the SRM process. The SRM process must evaluate any potential negative impacts that the contracting of services from a UPSSs could have on the United Nations system and its programmes.

15. The SRM process will be conducted in accordance with the *Security Policy Manual* (SPM), Chapter IV, Section A: "Policy on Security Risk Management (SRM)."

16. The SRM process must be supported by specific analysis and recommendations on the requirement for an unarmed security capability.

F. Roles and Responsibility

17. When the use of UPSSs is determined by the respective organization's Representative based on the SRM process as outlined in paragraphs 14–16, the DO, Division of Regional Operations (DRO) and United Nations Department of Safety and Security (UNDSS) will be informed. The latter will be informed by the DO or through the Security Focal Point (SFP) of the organization concerned. Records of these decisions are to be retained in a central repository by the DRO. The "Guidelines on the Use of Unarmed Security Services from Private Security Companies" will outline applicable procurement processes and regulations, including circumstances where immediate emergencies are addressed, in the short-term, in a flexible and practical manner.

G. Authority

18. When contracted by a UNSMS organization, the UPSS provider is performing security risk management functions for the UNSMS at a given location or locations. In accordance with the Framework of Accountability,[6] United Nations personnel are expected to abide by requests made by the UPSS provider in the conduct of their contracted duties, which forms part of the authorized security policies, guidelines, directives, plans and procedures of the UNSMS.

H. Selection Criteria for the UPSS Providers

19. Where the DO and/or the relevant organization Representative have approved the use of UPSSs, companies bidding for the contract must meet mandatory requirements for consideration of their bid. The mandatory requirements are

[5] *Security Policy Manual*, Chapter IV, Section H ("Use of Force Policy").
[6] *Security Policy Manual*, Chapter II, Section B, paragraph 28

described in the 'Guidelines on the Use of Unarmed Security Services from Private Security Companies' and in the applicable procurement regulations.

I. Screening Requirements for the Personnel of UPSS Providers

20. Any UPSS provider wishing to provide unarmed security services to an organization participating in the UNSMS shall confirm to that organization, in writing, that the mandatory screening process for its personnel, as outlined in the 'Guidelines for Unarmed Security Services from Private Security Companies' has been conducted and that only personnel who meet the mandatory requirements will be used to provide unarmed security services to the UNSMS organization in question.

J. Use of Force, Non-Lethal Means and Standard Operating Procedures

21. Any UPSS provider wishing to provide services to an organization participating in the UNSMS is required to develop and implement its own Use of Force Policy that complies with the criteria on the use of non-deadly force included in the UNSMS Use of Force Policy[7] and that is consistent with the International Code of Conduct for Private Security Service Providers.[8]

K. Training Requirements to be met by UPSS Providers

22. The UPSS provider is required to ensure that its personnel have the requisite skills and experience to perform the services required in accordance with the contract and the standard operating procedures.

23. Before commencing the provision of services to the UNSMS organization in question, the UPSS provider must provide a written certification that each of the company's personnel to be employed in the contract has undergone the training required in the contract and demonstrated the necessary level of associated skill.

L. Management and Oversight

24. As part of the contract execution, the Contracting Officer shall appoint, in writing, a Contracting Officer's Representative (COR). The COR is responsible for the day-to-day oversight of the UPSS provider. The COR shall represent the Contracting Officer in any discussions on contract performance with the UPSS provider as outlined in the Scope of Work and contract.

25. In the case of a single UNSMS organization, that organization shall manage the contract of the UPSS provider.

[7] *Security Policy Manual*, Chapter IV, Section H ("Use of Force Policy"), paragraph 10.
[8] See http://icoc-psp.org/.

26. In the case of a common UNSMS facility,[9] the senior security professional shall be appointed as the COR.

27. The COR must immediately submit a joint report to the Contracting Officer regarding any performance issues or concerns identified along with recommended remedial action.

M. Training and Compliance

28. This policy is to be part of the training for the DOs, Security Management Team (SMT) members, security professionals and managers in UNSMS organizations who have responsibility and accountability for managing security for their organization.

N. Utilization of Common Security Funding for Unarmed Private Security Companies

29. In instances where UPSS providers are funded through local cost-shared security budgets (LCSSB), a specific budget line indicating the amount for these services must be included in that local security cost-shared budget.

O. Final Provisions

30. This policy is to be made available to all UNSMS personnel.

31. This policy enters into effect on 18 April 2016.

[9] *Security Policy Manual*, Chapter IV, Section E: ”Security of United Nations Premises”.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM

Security Policy Manual

Chapter

IV SECURITY MANAGEMENT

SECTION M

Gender Considerations in Security Management

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 18 April 2016
Technical Review: 1 May 2017

Introduction

1. In a global security environment that remains complex and dynamic, United Nations personnel[1] continue to work with significant security challenges, including challenges and risks that are gender-based. Gender refers to the attributes, opportunities and relationships associated with being male or female, including lesbian, gay, bisexual, transgendered and inter sexed (LGBTI) individuals. Gender is context-specific and variable, it determines what is expected, allowed and valued in given contexts. Gender identity is a person's basic sense of being a man, woman, or another gender, which may not be the same as one's gender assigned at birth. These attributes, opportunities and relationships are socially constructed and are learned through socialization processes. Like people all around the world, United Nations personnel are at risk of violence or other security-related threats and risks based on their gender or their sexual orientation and gender identity. As such, United Nations personnel, particularly women and individuals who are LGBTI are at risk of being subject to gender-based security incidents. The occurrence of gender-based security incidents has highlighted the importance of gender sensitivity, responsiveness and inclusion in Security Risk Management (SRM) in all environments in which the United Nations operates.

2. The United Nations has been at the forefront advocating for mainstreaming gender into all its policies and programmes, which includes the efforts to seek gender sensitivity and responsiveness in all aspects of the United Nations Security Management System (UNSMS) and process. While there have been achievements in this aspect, consistent efforts, however, are required. This shall include as a priority the development of a specific gender policy statement of the UNSMS to promote the understanding of gender-based security risks and to reaffirm the United Nations commitment to make the UNSMS more gender-sensitive and gender-responsive.

3. The need for a UNSMS policy on Gender Considerations in Security Management was recognized by the UNSMS organizations, and the decision to develop this policy was made in May 2015 through the UNSMS Inter-Agency Security Management Network (IASMN) forum. In developing this policy, the UNSMS has undertaken to ensure that the process be guided by the principles as manifested in the Convention on the Elimination of all Forms of Discrimination against Women (CEDAW) (1979), the Beijing Declarations and Platform for Action (1995), the Economic and Social Council (ECOSOC) Resolution on Mainstreaming the Gender Perspective into All Policies and Programmes in the United Nations System (1997), the United Nations System-Wide Policy on Gender Equality and the Empowerment of Women (2006) and the associated United Nations System-Wide Action Plan (SWAP) (2012).

[1] For the purposes of this policy, 'personnel' refers to United Nations personnel and eligible family members as outlined in UNSMS *Security Policy Manual*, Chapter III ("Applicability of United Nations Security Management System").

A. Purpose

4. The purpose of this policy is to raise awareness and address security related threats, risks and vulnerabilities of all United Nations personnel, especially those most vulnerable. The policy is also intended to reaffirm the United Nations commitment to ensuring its security management system is more gender-sensitive and gender-responsive and provides appropriate and effective responses, management and mitigation measures. Finally, the policy provides tools that will ensure the United Nations commitments are best fulfilled at various levels at the Headquarters and in the field.

5. This policy should be read in conjunction with *the Security Management Operations Manual* (SMOM) "Guidelines on Gender Considerations in Security Management".

B. Applicability

6. This policy is applicable to all UNSMS organizations as well as all individuals[2] defined in the UNSMS *Security Policy Manual* (SPM), Chapter III ("Applicability of United Nations Security Management System").

C. Scope

7. This policy intends to promote gender considerations and their inclusion in United Nations security management.

8. At the country or mission level, the Designated Official (DO) and Area Security Coordinator should take measures to enhance discussion with host Governments on matters determined by this policy to enable the right of all members of the UNSMS to a security management system that provides an appropriate gender-sensitive response. While this policy provides internal guidance for the United Nations, discussions with host Governments on gender considerations at the country or mission level are strongly encouraged. The United Nations will benefit from the host Governments' support when dealing with gender-related security incidents in a local context.

9. The policy recognizes the specific context in which the UNSMS operates. The UNSMS commits to communicate to all United Nations personnel host Governments' approaches (or attitudes) to gender, whilst implementing this policy and ensuring consistency with the values contained in the Charter of the United Nations.

[2] All individuals covered by the UNSMS include United Nations system personnel, United Nations Volunteers, individually deployed military and police personnel in missions led by the Department of Peacekeeping Operations or the Department of Political Affairs, consultants, individual contractors, experts on mission and other officials with a direct contractual agreement with an organization of the United Nations system. The term does not refer to military members of national contingents or members of formed police units when deployed with their contingent.

D. Policy

General Principles

10. The UNSMS commits to promoting the understanding by all United Nations security personnel of gender-specific risks for different groups of individuals, as well as the need for gender-sensitivity and gender-responsiveness in all aspects of the security management process in order to effectively prevent, mitigate and resolve gender-related security incidents. For those with security management responsibilities, their understanding of gender perspective is particularly important as this will ensure the inclusion of gender considerations at all levels, including at the policy, strategic and operational levels, both in the field and at the Headquarters.

11. The UNSMS commits to implementing ECOSOC Resolution on Mainstreaming the Gender Perspective into All Policies and Programmes in the United Nations System (1997). This will be a particular focus of the United Nations Security Risk Management (SRM) process to ensure that specific gender-based threats, risks and vulnerabilities are considered.

12. The UNSMS commits to aligning itself with the United Nations System-Wide Action Plan (SWAP) for Implementation of the United Nations Policy on Gender Equality and the Empowerment of Women. The UNSMS will ensure that appropriate prevention and mitigation measures to respond to gender-based security risks are identified and implemented.

13. The UNSMS commits to putting in place an appropriate response mechanism relative to the security and safety of United Nations personnel affected by gender-based security incidents and adheres to the core principles: Safe Environment, Confidentiality and Consent, Respect and Non-Discrimination.

14. The UNSMS commits to ensuring access to training and resources designed to promote gender-related security awareness and visibility and to ensure that those responding to such incidents have the capacity to respond appropriately.

15. The UNSMS commits to determining and allocating sufficient resources identified as mitigation measures for gender inclusion in security management.

Policy Requirements

16. All UNSMS security policies shall be reviewed to ensure that gender considerations are sufficiently reflected in all security policies, guidelines and procedures. The IASMN will ensure that all UNSMS policies are reviewed by gender focal points and/or gender experts from UN Women.

17. All organizations of the UNSMS shall apply effectively gender sensitive and gender responsive approaches throughout the SRM process. In that regard, the

DO and the Security Management Team (SMT), supported by the Chief Security Adviser (CSA), Security Adviser (SA) and Chief Security Officer (CSO) in collaboration with the Security Cell, will ensure that:

17.1 There shall be routine analysis of gender-based security threats and risks in each SRM area.

17.2 All gender-based threats, risks and vulnerabilities are considered and included in the SRM process, in particular when doing risk analysis, identifying specific risk management measures for gender-related security incidents, managing stress and reporting gender-related security incidents.

17.3 Every effort has to be made to ensure that gender-sensitivity and gender-responsiveness are applied in a country or area's security plans and procedures, including contingency plans for emergency/crisis situation.

17.4 Security Risk Management measures, including for residences, are reviewed on a regular basis with a gender perspective.

17.5 Gender-related security incidents may be reported and recorded through the UNSMS Safety and Security Incident Reporting System (SSIRS), only after the consent of the personnel has been obtained.

18. All organizations of the UNSMS will ensure that an appropriate response mechanism that is gender-responsive and gender-sensitive is established and maintained to support personnel affected by gender-related security incidents. This includes guidance for the UNSMS on immediate response.

19. In relation to training:

19.1 The IASMN Security Training Working Group will undertake regular review and evaluation of the UNSMS security training programmes to ensure they are gender-sensitive and gender-responsive.

19.2 The United Nations 'I Know Gender' training course (and/or another organizations' equivalent gender training) is mandatory for UNSMS security personnel.

19.3 UNDSS will develop a gender in security training programme to be delivered to United Nations personnel through a variety of training modalities.

20. All organizations of the UNSMS shall pursue every possible means to ensure that the United Nations personnel are fully briefed and aware of the risks that they may face, including those that are gender-related, and the availability of appropriate gender-sensitive support if there is a security incident.

20.1 UNDSS will create a gender section on the UNSMIN website where gender-related resources will be maintained. A specific section on gender will also be included in the UNDSS Travel Advisory.

20.2 All mandatory security briefings in country should be reviewed to incorporate gender-specific threats and address appropriate gender-related risk management measures as per the SRM process.

21. The UNSMS shall undertake regular evaluation and improvement of processes in place to support this policy.

E. Roles and Responsibilities

22. Executive Heads of the UNSMS organizations are responsible for informing their respective personnel of this policy and ensuring that all necessary actions are taken within their organizations so that the measures identified are actioned and appropriate resources are allocated.

23. DOs and SMTs are responsible for promoting the implementation of this policy and ensuring that expertise at the country level is utilized.

24. CSAs, SAs and CSOs, with the support from the Security Cell, are responsible for including gender-sensitivity and gender-responsiveness into the SRM process and all security plans and guidelines, including contingency plans.

25. UNDSS will ensure the SRM process will factor in gender-based threats, risks and vulnerabilities and that appropriate mitigation measures are identified and implemented.

F. Training

26. This policy shall become part of the mandatory training for DOs, SMT members and security personnel, as well as managers in the UNSMS organizations who have security management responsibilities and accountabilities as defined in the Framework of Accountability for the UNSMS.

G. Final Provisions

27. This policy is to be distributed to all United Nations personnel who are responsible to be familiar with, commit to and abide by this policy.

28. This policy enters into force on 18 April 2016.

29. This policy shall be reviewed every two years by the IASMN.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter IV

SECURITY MANAGEMENT

SECTION N

Policy for United Nations Minimum Operating Security Standards (MOSS)

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 20 April 2009
Technical Review: 1 May 2017

Introduction

1. Minimum Operating Security Standards (MOSS) is the primary mechanism for managing and mitigating security risks to the personnel, property and assets of the organizations of the United Nations. MOSS encompasses a range of measures designed to reduce the level of risk, as identified in the Security Risk Management (SRM) process[1], to an acceptable and manageable level. These measures are listed under categories which include: telecommunications, documentation, coordination mechanisms, medical, equipment, vehicles, premises, training and residential security measures.

2. A single MOSS system applies throughout the United Nations Security Management System (UNSMS). No distinction is made between Headquarters, the field or missions for the purposes of Security Risk Management. The Residential Security Measures (RSMs) will remain separate from MOSS.

3. In order to mitigate risks identified in the SRM process, MOSS must be applied and maintained at all duty stations.

4. Experience in the development and application of MOSS in the United Nations since 2002 has identified a need for the MOSS system to be kept as simple as possible, with the flexibility and capacity to allow adaptation to differing scenarios and rapidly changing circumstances.

Minimum Operating Security Standards

5. Each country and/or duty station, regardless of security risk level, type of operation or security environment, is to develop and maintain a Country MOSS based on the mandatory Global MOSS provided in Appendix 1.

6. Measures contained in the Country MOSS must be commensurate with the results of the SRM process applicable to the country or location. The measures should be presented to the Security Management Team (SMT) with an explanation of their rationale and then approved as laid down in paragraph 16 below.

7. The SRM process must clearly demonstrate that the MOSS measures proposed will reduce the risk to United Nations personnel in-country to an acceptable and manageable level.

8. Mitigation measures selected must be logical, realistic, cost-effective and capable of being implemented within the context of the operation or country.

[1] Please refer to *Security Policy Manual* Chapter IV, Section A on "Security Risk Management Policy" and SRM Manual of 11 December 2015.

9. Where the SRM process indicates that the security environment could change, the Country MOSS must include provisions for timely enhancement of MOSS as part of the SRM measures.

Responsibilities and Standards

10. As outlined in the Framework of Accountability, responsibility for implementing MOSS rests with the heads of United Nations organizations in-country.

11. Where a United Nations organization does not have a permanent presence in the country, the head of the organization should take measures to ensure that missions and staff visiting the country are briefed in advance on the MOSS requirements applicable. The Designated Official (DO) and the Security Adviser or Country Security Focal Point should provide assistance to enable such staff to comply, including the loan of equipment from a pool maintained for such visits, where appropriate. Costs of MOSS measures will be covered by the sending organization.

12. It is the responsibility of the Executive Head of each organization to take action with Member States for the appropriation of required resources for security; the Executive Head of each organization is also responsible for the allocation of appropriate resources for security within his/her organization.

13. The United Nations World Food Programme is the focal point for security telecommunications issues and in its capacity advises the Security Management Network on policy and implementation of security telecommunications standards and services.

14. The United Nations Medical Directors (UNMD) provides technical guidance to the UNSMS on the minimum medical standards to be included in MOSS.

15. Additional expert technical advice should be sought, if necessary, where the SRM process indicates a need for mitigation measures outside the normal competence of the United Nations safety and security staff.

16. The approval process for each Country MOSS will be in line with the SRM process as follows:

    (a) The MOSS will be approved by the DO at a formal SMT meeting. This will be a part of the SMT minutes;

    (b) The approved Country MOSS will be sent to the United Nations Department of Safety and Security (UNDSS) through the appropriate regional desk for review;

    (c) UNDSS will circulate it to the respective headquarters of all IASMN member organizations, and it will endorse the Country MOSS Table if no objections are received within one month.

17. Once endorsed, the Country MOSS is binding on all IASMN members with a presence in that country (including missions and visitors), at both the headquarters and field level. Oversight and compliance of MOSS will be provided by UNDSS.

Appendix 1 to MOSS Policy

UNITED NATIONS MINIMUM OPERATING SECURITY STANDARDS (MOSS)

Country MOSS must justify, through the rigorous application of the Security Risk Management process, the inclusion or exclusion of each of the items listed below

While the intention is to maintain flexibility and management discretion, common sense will dictate those measures (such as vehicle safety equipment and fire precautions) which should be mandatory in all locations regardless of the prevailing security situation

1. TELECOMMUNICATIONS

1.1. Emergency Communications System

(a) Where the Security Risk Management (SRM) process indicates a need, establish an **Emergency Communications System (ECS)** throughout the country and in its operational locations, in order to:

(i) Provide communications between the Designated Official (DO), Security Adviser (SA), Security Management Team (SMT), Wardens and United Nations medical personnel within the capital.

(ii) Provide communications between the Area Security Coordinator (ASC) and DO/SA and United Nations medical personnel.

(iii) Provide communications between the ASC and the Area SA and SMT within the area.

(iv) Enable communications between the DO/SMT/SA and relevant United Nations offices outside the country (including UNDSS).

(b) **Mobile satellite telephones** should be provided to all Crisis Coordination Centres (CCCs), DOs and Chief Security Advisers (CSA)/SAs and Agency Security Officers as well as for other key managers as decided by the SMT.

(c) The ECS is to be tested and practiced at regular intervals.

(d) The ECS network should be capable of operating 24 hour/7 days per week (24/7) should need arise.

1.2. Radio Communications

(a) When VHF/UHF communications are employed (in accordance with need identified in the SRM process), a **Security channel** for DO, SA and SMT members, and where applicable ASC, ASMT members, United Nations medical personnel and wardens, must be incorporated into radio networks.

(b) All United Nations vehicles are to be equipped with VHF/UHF radios. In addition, "Field Vehicles" (those which travel into the countryside or move between urban areas) are to have a second radio system, usually HF or an alternative communication system (e.g., satellite phone).

(c) Standard Operating Procedures for regular radio checks at residences and while moving are to be established.

(d) All international personnel, drivers, wardens and national personnel deemed "essential" are to be issued with handheld VHF/UHF radios. Radio checks are to be conducted routinely.

(e) All personnel who work regularly outside office premises are to be trained to operate all forms of telecommunications equipment provided for Field Vehicles.

2. SECURITY INFORMATION AND STRUCTURE

2.1. **Documentation**. Each country, and each duty station in the country, will have the following documentation:

(a) Items related to the SRM process.

(b) *Security Policy Manual* (SPM).

(c) *Security Management Operations Manual* (SMOM).

(d) Country/Area-specific Security Plan.

(e) Country/Area-specific MOSS.

(f) Security Standard Operating Procedures.

(g) Relevant Country Maps.

(h) Country PEP (post-exposure prophylaxis) Protocol.

2.2. **Warden Systems**

(a) Established and operational.

(b) Exercised regularly.

2.3. **Crisis Management Plans and Building Emergency/Evacuation Plan**

(a) Established for all United Nations offices and facilities.

(b) Exercised every six months (or more frequently if SRM process so indicates).

2.4. **SMT Meetings:** To be conducted and documented as per the United Nations *Security Policy Manual* (SPM).

2.5. **Security Clearance and Travel Notification**: System in place for approving security clearances into the country, recording travel notifications and tracking personnel movements inside the country.

2.6. **Incident Reporting:** System to ensure that all security incidents in country are reported using "SSIRS".

2.7. A common-system **CCC** is to be established in the capital and all United Nations locations in country which have an ASC.

3. MEDICAL

3.1. Response to Medical Emergencies

(a) **Casualty Evacuation Plans.** All duty stations are to have a "CASEVAC Plan" which includes rescue, immediate medical attention, identification or procurement of appropriate means of transportation, and location of appropriate primary health care facilities. [CASEVAC**:** the process for the rescue and movement of injured or sick personnel from the place or incident site at which injury occurs, or a person becomes ill, to a primary care medical facility inside the country.]

(b) **Medical Evacuation Plans.** All Duty Stations are to have a "MEDEVAC Plan" which includes the medical and administrative procedures necessary for evacuation of sick or injured personnel from the country, including the authority for authorization of evacuation and use of an air ambulance service where necessary. [MEDEVAC: the process for movement of injured or sick personnel from the primary care medical facility to a hospital, advanced care facility or place of recuperation outside the country in which the injury or illness occurred. It may also refer to the repatriation or reassignment of a staff member from a duty station which is deemed by the medical authorities to be potentially damaging to the staff member's health for reasons of climate, altitude or other environmental factors.]

(c) Each country is to have a **MASS CASUALTY PLAN** appropriate to the risks in-country and the response capacity of the local emergency services.

(d) Register of locally available medical facilities, emergency response services, and contact numbers to be maintained up-to-date and made available in ECS and to all duty personnel.

(e) Based on the country/duty station security situation an appropriate number of United Nations personnel will be trained in Basic First Aid.

(f) Each country is to have a medical plan and PEP protocol.

3.2. Medical Equipment

(a) All vehicles to carry Vehicle First Aid kits (specifications as per Security Technical Standards Manual).

(b) **Emergency Trauma Bags** (ETBs) distributed according to number of trained United Nations staff.

(c) One Basic First Aid kit per building (or per floor in buildings with more than 50 personnel).

(d) **PEP Kits** (which must be replaced by their due expiry dates) will be distributed through the country PEP kit protocol (which is to be attached to the country security plan as an annex and available in all radio rooms and duty personnel folders).

4. EQUIPMENT and SUPPLIES

4.1. **Emergency power supply** available for charging and operation of **common-systems** communications equipment, office external security lighting and other essential equipment. Adequate reserve stocks of fuel to be maintained.

4.2. **Emergency food, water, medical, sanitary and shelter supplies** (in non-perishable form) to be stocked in preparation for use in concentration points, bunkers, safe rooms and storm shelters as appropriate for the country and situation.

4.3. All personnel to prepare **individual emergency bags**, maximum weight 15 kg (33 lbs) and containing essential documents, clothing, hygiene and medical supplies, ready for rapid evacuation or relocation.

5. UNITED NATIONS VEHICLES

5.1. All United Nations Vehicles

(a) Must be operated by properly licensed operators.

(b) Must be appropriately registered with the host Government and properly maintained.

(c) Must be identified, where appropriate, with United Nations logos/flags/decals as determined by prevailing local conditions.

5.2. Non-United Nations Vehicles. Where United Nations staff travel in non-United Nations vehicles which are not MOSS compliant, every effort should be made to ensure that the United Nations personnel are MOSS compliant (i.e., equipped with communications equipment, etc.).

5.3. United Nations Vehicle Equipment

5.3.1. All vehicles (regardless of location)

(a) First aid kit.
(b) Fire extinguisher
(c) Spare wheel, jack and appropriate tools.
(d) Reflector triangles, battery-powered lantern and seat belts.

5.3.2 All Field Vehicles (according to country situation):

(a) 5 metre rope, strong enough to pull another field vehicle.
(b) Shovel, hand-axe or machete.
(c) Fire-lighting materials.
(d) High visibility sheet/flag,
(e) GPS-based tracking system for curfew, movement restriction and convoy monitoring.
(f) Adequate drinking water, food and necessities (including blankets/sleeping bags) to support all occupants for 24 hours (according to climatic conditions).

6. OFFICES, PREMISES AND FACILITIES PROTECTION

6.1. All United Nations Managed Buildings

(a) All buildings occupied by the United Nations are to be compliant, where feasible, with international building, safety and fire regulations or the applicable laws of the host country as appropriate (including construction for resistance to earthquakes or other natural hazards, according to local conditions).

(b) Appropriate access control measures based on size and location of premises.

(c) Separate entrances for personnel and visitors, where feasible and appropriate, in compliance with established standards (if/where applicable).

(d) Secured parking for authorized vehicles where appropriate.

(e) Alternate/emergency exits from buildings and from compounds.

(f) Security and/or guard force trained on appropriate surveillance and reconnaissance detection and reporting protocols.

6.2. **Premises with Additional Risks**. Premises that are assessed to be at high-risk from terrorism are to have:

(a) Stand-off distance as estimated/advised by a qualified expert (taking scale of likely threat, surroundings/approaches, construction, etc. into account)

(b) Structural reinforcement and blast walls as required/advised by a qualified expert.

(c) Shatter resistant film on windows and frame catchers.

(d) Bunkers/reinforced rooms.

(e) Surveillance and access control systems.

6.3. **United Nations Personnel Working in Government (or other non-United Nations Facilities)**

(a) To the extent practical, the DO and concerned head of organization should request MOSS-compliant conditions, to United Nations standards, for personnel working in non-United Nations premises.

(b) Where this is not fully possible, the SA should be asked to assess the premises to see if the security measures in place provide an equivalent level of protection from the risks identified in the SRM process as that provided in United Nations-managed premises.

(c) Where a MOSS-equivalent level of protection is not achieved, the DO and head of organization concerned should consider, and negotiate with the host government authorities, alternate means of enhancing mitigation, such as:

(i) Allowing physical modifications to the workspace actually occupied by the United Nations personnel.

(ii) Re-allocating the workspace used by the United Nations personnel (for example, to ensure that they are as far as possible from external walls or likely terrorist approaches).

(iii) Adjusting work patterns to limit the exposure of United Nations personnel within the government premises.

7. SECURITY TRAINING AND BRIEFINGS

7.1. **All New United Nations Personnel and their Recognized Dependants, as applicable, briefed on/provided with:**

(a) Country-specific security orientation briefing;

(b) Summary/Extract of country security plan and Evacuation Plan;

(c) Relevant Country/Area-specific Security Plan, SOPs and policies;

(d) Compliance with all United Nations security policies;

(e) Copy of current MOSS and RSMs applicable to the duty station;

(f) Briefing and written handout on medical arrangements available in-country and how to access them or call for emergency medical assistance;

(g) A copy of the Country PEP Protocol, which should specify PEP custodian arrangements, location of PEP kits and the procedure for obtaining assistance in the event of possible exposure to HIV/AIDS .

7.3. **Training:**

(a) All United Nations personnel to complete Basic Security for United Nations Personnel (BSUNP) and/r Advanced Security in The Field (ASITF) online or by CD-ROM, as required for the duty station.

(b) All personnel to receive cultural sensitivity briefings appropriate to country before or on arrival.

8. RESIDENTIAL SECURITY MEASURES

(a) Residential Security Measures (RSMs) will be approved as a separate requirement, in accordance with RSM procedures as updated from time to time.

(b) RSMs must take account of the relevant conclusions of the SRM process with respect to the local law and order situation.

9. ADDITIONAL MEASURES

9.1. Depending on the security environment and the SRM process, the DO and SMT may have to consider special measures. Examples of these are:

(a) **Personal Protective Equipment** (helmets, body armour, etc.). To be stocked adequately for all personnel needs as indicated by the Security Risk Assessment and SOPs establishing conditions for issue, carriage in vehicles and mandatory wearing.

(b) **Armoured Vehicles.** In addition to providing a means of evacuating personnel under fire in extremis, armoured vehicles are an option where access is needed to areas which are marginally under the "acceptable risk" threshold and where there is potential for resumption of conflict or fluidity of nearby conflict areas.

.

EXAMPLE COUNTRY MOSS FORMAT (for ILLUSTRATIVE PURPOSES/SUGGESTION ONLY)

United Nations Minimum Operating Security Standards

[COUNTRY NAME]

[Date]

(Required standards/mitigation measures are linked to security risks as identified in the SRM process)

1. TELECOMMUNICATIONS				
No.	**Item**	**Standard Requirement**	**Country Specific Requirements, Equipment & Procedures**	**Remarks**
1.1	Emergency Communications System	**Emergency Communications System (ECS) to be established** throughout [Country], as well as in [Cities], to provide for communication links between the: • DO, CSA, SMT, Wardens and UN medical personnel; • ASC and DO/CSA and UN medical personnel; • ASC and the FSCO, ASMT; • DO/SMT/CSA and relevant UN Offices outside the country (including DSS).	a. Mobile satellite telephones to be provided to: CCCs, DO, ASCs, CSA, DSA, FSCOs, Agency Security Officers, as well as other key managers; b. BGAN and/or VSAT provided to at least two offices in main operational hubs; c. The ECS network operating 24 hours/7 days per week in [City] and all main operational hubs inside [Country]; d. The ECS is to be tested and exercised monthly; e. ECS technical support, as required;	Requirements are mandatory
1.2	Radio Communications	VHF/HF communications employed to cover the entire territory of [Country], a **Security channel** for DO, SA and SMT members, and where applicable ASC, ASMT members, UN medical personnel and wardens, to be incorporated into radio networks.	a. All staff in [Country] to be issued with handheld VHF radios; b. All UN vehicles are to be equipped with VHF radios; c. UN Vehicles used for field missions to have a second radio system, usually HF or an alternative communication system (e.g. satellite phone); d. Radios provided to drivers of rented/non-UN vehicles; e. Radio Rooms established in all main operational hubs; f. Back-up radio system in bunkers/safe rooms; additional back-up system in secondary concentration point (where applicable). g. VHF base stations installed in all agency field offices; h. Repeater systems established for coverage of larger urban/rural areas; where appropriate; i. SOPs for regular radio checks at residences and while moving are to be established; j. All staff to be trained to operate all forms of telecommunications equipment; k. Radio checks in field locations to be conducted daily.	Requirements are mandatory Exemptions require the approval of the DO (e.g., community embedded staff in remote areas as per Section 9.7) based on alternative mitigation measures recommended in the SRM process.

2. SECURITY INFORMATION AND STRUCTURE				
No.	**Item**	**Standard Requirement**	**Country Specific Requirements, Equipment & Procedures**	**Remarks**
2.1	Documentation	a. Country/Area-specific Security Risk Management process b. United Nations Security Management System *Security Policy Manual* (SPM) c. *Security Management Operations Manual* (SMOM) d. Country/Area-specific Security Plan e. Country MOSS f. Security Standard Operating Procedures g. Relevant country maps h. Country PEP Protocol i. Security SOP booklet	As per standard requirement to be available at the DO's office, agency offices, and each duty station, in addition: j. Mine area maps (provided by UNMAS); k. Maps/lists displaying permissible/non-permissible roads/areas; l. Maps displaying areas where armoured or vehicles with ballistic blankets fitted have to be used; m. Cell phone coverage map (maintained by FAO)	Requirements are mandatory
2.2	Warden System	Warden system for national and international staff established and functional in all duty stations. Note: zone warden systems to be implemented in case international staff is authorized to reside in private residences.	a. Warden system for international staff to ensure emergency response coordination and staff concentration among UN (and NGO) compounds in a duty station - established and operational in all duty stations where more than one office and/or approved staff accommodation are located; b. Agency based warden system for national staff; c. Warden meetings monthly; exercise every 3 months, training every 6 months.	Requirement is mandatory Country-wide arrangements are presently implemented from Nairobi.
2.3	Staff Ceiling	Requirement for areas with high or very high residual risk.	a. Staff ceilings for international staff (assigned and on mission) to be established for all duty stations; b. Staff ceilings to be reviewed monthly (standing item on ASMT agenda).	ASMT recommends staff ceilings, SMT approves.
2.4	Building Emergency/ Evacuation Plan	Established for all UN offices and facilities	a. Building emergency/evacuation plans exercised every 6 months	Requirement is mandatory
2.5	SMT and ASMT Meetings	To be conducted and documented as per *UN Security Policy Handbook*.	SMT and SMT Working Group Meetings alternate weekly (DO determines participation - attendance is mandatory) – ASMT meetings weekly	Requirement is mandatory
	Security Clearance Procedures	System in place for approving security clearances into country, recording travel notifications, and tracking personnel movements inside the country.	a. Full ISECT implementation for external and internal travel, including Phase V areas b. ISECT profiles for all staff (agencies responsible that ISECT profiles are updated)	Requirement is mandatory
2.6	Incident Reporting	a. All security incidents are reported using "SSIRS"	*b.* Other reports as per the *Security Policy Manual* (SPM) c. Agency FSAs report incidents simultaneously to parent agency and CSA	Requirement is mandatory
2.7	Crisis Coordination	a. Established for all UN offices and facilities;	b. CCCs established in [City] and all main operational hubs; c. Exercised every six months (or more frequently if SRM process so	Establishment of SIOC by

	Centre (CCC)		indicates) - crisis management exercises only if no actual crisis occurred – otherwise prepare “lessons learned”.	[planned date].

United Nations Minimum Operating Security Standards – [Country]

3. MEDICAL SUPPORT				
No.	**Item**	**Standard Requirement**	**Country Specific Requirements, Equipment & Procedures**	**Remarks**
3.1	Response to Medical Emergencies	a. Casualty Evacuation Plans: immediate medical attention, identification or procurement of appropriate means of transportation, and location of appropriate primary health care facilities (inside the country). b. Medical Evacuation Plans: medical and administrative procedures necessary for evacuation of sick or injured personnel from the country, including the authority for authorization of evacuation and use of an air ambulance service where necessary. c. Establish and maintain area–specific casualty and medical evacuation plans; d. Establish and maintain Mass Casualty; e. Register of locally available medical facilities, emergency response services, and contact numbers to be maintained up to date and made available in ECS (classified as per UN PKO medical standards); f. All staff to be trained in Basic First Aid; g. Security staff and appropriate number of other staff trained and certified in trauma and mass casualty incident response; h. Establish medical plan and PEP Protocol;	i. Adequate number of stress counsellors dedicated to [Country] based staff; j. Adequate number of paramedics under supervision of a UN physician; k. UN medical officer to supervise stabilisation centres trained and certified in Advanced Trauma Life Support (ATLS) and Pre-hospital Trauma Life Support (PHTLS) or equivalent; l. Adequate air rescue capacity, minimum one pressurised aircraft with ALS on stand-by at all times;	Response times to be reduced - objectives to be accomplished before end of 2009: • CASEVAC - trauma stabilization by paramedic max. 1 hour after incident; • Air MEDEVAC and admission to Level II hospital max. 3 hours after incident; Note: Quarterly report to DSS on progress
3.2	Medical Equipment	a. All vehicles to carry Vehicle First Aid kits (specifications as per *Security Technical Standards Manual*). b. Emergency Trauma Bags (ETBs) distributed according to number of trained UN staff. c. One Basic First Aid kit per building (or per floor in buildings with more than 50 personnel). d. PEP Kits (which must be replaced by their due expiry dates) will be distributed through the country PEP Kit protocol (which is to be attached to the country security plan as an annex, and available in all radio rooms and duty personnel folders)	First aid kits, trauma bags, PEP kits as per requirement, in addition: e. Establish stabilization centres with ATLS and PHTLS capacity in all operational hubs (5 by September 2009 – all hubs by December 2009) f. Ambulances (or ambulance type vehicles with ability to fit stretchers) in main operational hubs; g. Establish UN dispensaries in selected locations (SMT decision); h. Support local hospitals to increase MCI and response capacity (e.g. ambulances) i. PEP kits stocked in UN dispensaries + 2 PEP kits per custodian (usually FSCO/FSA)	Note: Quarterly report to DSS on progress

CONTINUED FOR ALL MEASURES IN THE BASELIN

UNITED NATIONS SECURITY MANAGEMENT SYSTEM

Security Policy Manual

Chapter IV

SECURITY MANAGEMENT

SECTION O

Residential Security Measures (RSMs)

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 23 November 2015
Technical Review: 1 May 2017

A. Introduction

1. The primary responsibility for the security and protection of United Nations personnel and other individuals covered by the United Nations Security Management System (UNSMS) rests with the host Government. At times, however, governments may be unable to provide the necessary protection when there is a partial or total breakdown of law and order resulting in increased criminal activity.

2. Under such exceptional circumstances, Residential Security Measures (RSMs) may be approved to enhance residential security. RSMs may include residential security advice and training, procedures and restrictions, and the installation of security enhancements in or around residences ("cost-based elements").

3. United Nations personnel and other individuals covered under the UNSMS have a shared responsibility for ensuring their safety and security, in conjunction with the Organization, regardless of whether RSMs are approved. Therefore, it is incumbent upon all such personnel and other individuals covered under the UNSMS to ensure that they understand their threat environment and basic residential security principles and, in response, implement all practical and appropriate measures to enhance their residential security, commensurate with their threat environment, at all times.

4. RSMs are distinct from Minimum Operating Security Standards (MOSS). RSMs do not constitute a set of baseline measures to be applied uniformly across all duty stations. They may vary across duty stations depending upon the residential security risk environment. Once approved for a duty station, the implementation of RSMs shall be mandatory.

B. Applicability

5. This policy is applicable to all internationally-recruited or internationally-deployed individuals covered under the *UNSMS Security Policy Manual*, Chapter III ("Applicability of the United Nations Security Management System"). These individuals shall herein be referred to as "personnel."[1]

6. This policy is also applicable to eligible family members of personnel residing with such personnel at the duty station or installed at an Administrative Place of Assignment (APA) by the respective parent organization where RSMs have been approved.[2]

C. Purpose

7. RSMs are intended to protect personnel from physical harm or injury at their residence as a result of increased criminal activity at the duty station. RSMs are not

[1] This policy shall not apply to personnel required to live in a specific residence provided by their respective parent organization (e.g., guesthouse or compound at a high-risk duty station).

[2] The Special Operations Approach (SOA) for non-family duty stations provides for the designation of an Administrative Place of Assignment (APA), which is considered as the official duty station for eligible United Nations staff members for administrative purposes. The SOA is being phased out gradually and is expected to be fully discontinued as of 1 July 2016.

intended to safeguard property.

8. RSMs do not constitute an entitlement or allowance and shall not include cost-based elements that specific entitlements or allowances are intended to cover.[3]

D. Basis for RSMs

9. The Security Risk Management (SRM) constitutes the basis upon which RSMs are recommended and approved. The SRM process must be conducted in accordance with the *UNSMS Security Policy Manual* (SPM), Chapter IV ("Security Management: Security Planning"), Section A ("Policy on Security Risk Management (SRM)"). The SRM process must reasonably justify the existence of a "partial or total breakdown of law and order resulting in increased criminal activity," and, therefore, the need for RSMs at the duty station. Whenever possible, the SRM process shall include information on the following:
    (a) Nature, location and frequency of crimes or attacks, or the threat of crimes or attacks, targeting the residences of members of the international community at the duty station; and
    (b) Effectiveness of RSMs implemented by local authorities.

10. The SRM process may be supplemented by information relating to residential security at the duty station, including the following:
    (a) RSMs commonly implemented by other members of the international community for similarly-situated personnel or eligible family members;[4] and
    (b) Underlying cause(s) of a partial or total breakdown of law and order resulting in increased criminal activity at the duty station, including intolerance or hostility towards identifiable individuals or groups at the duty station.

E. Roles and Responsibilities for Determining RSMs

11. The Designated Official (DO), in consultation with the Security Management Team (SMT), shall determine what RSMs, if any, will be recommended for the duty station based upon the SRM process and any supplementary information. As noted in Section A ("Introduction"), RSMs may include residential security advice and training, procedures and restrictions, and cost-based elements. The following shall apply when recommending cost-based elements:
    (a) The DO, in consultation with the SMT shall reasonably justify any recommended cost-based elements based upon the SRM process and any supplementary information;
    (b) The DO/SMT shall not recommend any cost-based elements commonly

[3] For details on specific allowances and entitlements applicable in the UN Common System, please refer to the website of the International Civil Service Commission (www.icsc.un.org).

[4] Commonly implemented RSMs may change over time. Therefore, the Designated Official (DO)/Security Management Team (SMT) should take into account the local context when identifying such RSMs.

installed by owners or lessors of residential properties at the duty station;[5] and

(c) The DO, in consultation with the SMT, shall determine a financial cap (i.e., maximum amount) for each cost-based element. When determining such a cap, the DO/SMT shall first consider a common services approach, seeking economies of scale, common standards of performance and quality of service. One-time installation costs and recurrent costs (i.e., for operation or maintenance, as applicable) shall be identified separately.

12. The following procedures shall be followed by the DO when proposing RSMs and financial caps to the United Nations Department of Safety and Security (UNDSS) and by UNDSS when subsequently evaluating the DO's proposal:

(a) The DO's proposal, consisting of the SRM measures as part of the SRM process, and any supplementary information as well as recommendations for RSMs and financial caps, shall be submitted to UNDSS's Division of Regional Operations (DRO);

(b) Within fifteen (15) calendar days of the receipt of the DO's proposal, UNDSS/DRO shall:

(i) Evaluate the DO's proposal, in consultation with the relevant Chief Security Adviser (CSA)/Security Adviser (SA) or Country Security Focal Point (CSFP) in the field; and

(ii) Share the evaluation and the DO's proposal, including the outcome of the SRM process and any supplementary information, with the Headquarter Security Focal Points (SFPs) of respective parent organizations.

(c) Within fifteen (15) calendar days of the receipt of UNDSS/DRO's evaluation, the Headquarter SFPs of respective parent organizations shall provide input to UNDSS/DRO. If no input is provided, consensus shall be implied;

(d) Within five (5) calendar days of the receipt of input, UNDSS/DRO shall seek to establish consensus on the DO's proposal, in consultation with the Headquarter SFPs of respective parent organizations:

(i) If consensus is established, UNDSS/DRO shall notify the DO of any approved RSMs and financial caps;

(ii) If consensus is not established, a Residential Security Measures Review Group (RSMRG) shall be convened in accordance with the RSMRG's Terms of Reference;[6]

(b) Once approved, RSMs and financial caps for the duty station can only be modified through the submission of a new proposal by the DO, together with the most recent SRM process documents and any supplementary information.

F. Roles and Responsibilities for Implementing RSMs

13. Parent organizations at the duty station shall ensure that their respective personnel

[5] Commonly implemented RSMs may change over time. Therefore, the DO/SMT should take into account the local context when identifying such RSMs.

[6] The RSM Review Group's Terms of Reference are found in Annex A to this policy.

attend a security briefing upon their initial arrival at the duty station.[7] UNDSS/DRO shall ensure that the content of the security briefing includes sufficient residential security advice so as to inform personnel of the residential security environment and any approved RSMs.[8]

14. Parent organizations shall inform their respective personnel of their individual responsibility to implement RSMs, in accordance with this policy.

15. Parent organizations shall hold their respective personnel accountable for any default, fraud or deceit with regard to RSMs.[9]

16. With regard to cost-based elements, parent organizations shall notify personnel of the financial and implementation modalities under which such elements may be obtained.
    (a) In cases where parent organizations determine that the length of deployment does not justify obtaining a residence at the duty station, parent organizations shall ensure, whenever feasible, that personnel are provided with or directed to accommodation where RSMs, as applicable to the duty station, have been fully implemented.

17. Personnel are required to abide by the security policies and guidelines of the UNSMS and their respective parent organization, including with regard to RSMs.[10]

18. Personnel shall notify their respective parent organization of any delay or difficulty in implementing RSMs at their residence.

19. Personnel who change their residence within the duty station may be eligible for RSMs at their new residence depending on the circumstances for the change. Such circumstances shall be reviewed by their respective parent organization on a case-by-case basis.

20. Personnel may supplement RSMs at their own expense to fit their particular circumstances.

[7] The Framework of Accountability, Annex, Section G, paragraph 16 mandates representatives of United Nations Security Management System (UNSMS) organizations to require their respective personnel to "attend appropriate security awareness training and briefings."

[8] The Framework of Accountability, Annex, Section J, paragraph 14 mandates Chief Security Advisers/Security Advisers to establish a "system for briefing all personnel employed by the organizations of the United Nations system and their recognized dependants upon initial arrival, providing local security training as necessitated by changes in the security environment and ensuring such personnel are kept informed of matters affecting their security."

[9] The Framework of Accountability, paragraph 28 states: "Personnel employed by the organizations of the United Nations system are accountable to their respective organizations."

[10] The Framework of Accountability, paragraph 28 states: "Personnel employed by the organizations of the United Nations system are accountable to their respective organizations. All such personnel, regardless of the rank or level, have the responsibility to abide by security policies, guidelines, directives, plans and procedures of the United Nations security management system and their organizations."

G. Roles and Responsibilities for Compliance and Oversight

22. In addition to their roles and responsibilities noted in Section E ("Roles and Responsibilities in Determining RSMs"), the DO/SMT shall establish compliance mechanisms for the duty station to verify that RSMs have been properly implemented.[11] The DO/SMT shall designate the relevant Chief Security Adviser (CSA)/Security Adviser (SA)[12] to implement such mechanisms, which shall, whenever feasible, include an on-site visit to the residence.[13]

23. UNDSS shall submit an annual report to the IASMN identifying duty stations where RSMs have been proposed, approved or implemented over the past year and any related observations and trends.

H. Final Provisions

24. This policy shall be made available to all UNSMS organizations and to all individuals covered under the UNSMS *Security Policy Manual* (SPM), Chapter III ("Applicability of the United Nations Security Management System").

25. This policy shall be supplemented by Residential Security Measures (RSM) Guidelines in the UNSMS *Security Management Operations Manual* (SMOM). These guidelines are intended to complement this policy and, therefore, shall not be interpreted as limiting or prejudicing this policy in any way. These guidelines shall be made available to all UNSMS organizations and to all individuals covered under the UNSMS *Security Policy Manual* (SPM), Chapter III ("Applicability of the United Nations Security Management System").

26. This policy shall enter into force on 23 November 2015 and, upon entry into force, shall supersede Chapter V, Section H of the United Nations *Field Security Handbook* (2006), paragraphs 5.54-5.63 ("Security of Residences of Internationally-recruited Staff members (aka MORSS)"), in addition to all previous communiqués, memoranda, and other communications related to RSMs.

---

[11] The Framework of Accountability, Annex, Section H, para. 6 delegates the responsibility for "monitoring implementation and compliance" of residential security measures to the Security Management Team (SMT).

[12] In duty stations where no Chief Security Adviser (CSA)/Security Advisers (SA) is present, the Designated Official (DO)/Security Management Team (SMT) shall designate a representative from UNSMS organizations present at the duty station to implement such mechanisms.

[13] The Framework of Accountability, Annex, Section J, paragraph 17 requires Chief Security Advisers (CSAs)/Security Advisers (SAs) to conduct "security surveys of residential areas and premises" while paragraph 21 requires them to report "all instances of non-compliance with security policies, practices and procedures" to the Designated Official (DO) and concerned representatives of UNSMS organizations. Similarly, the *Framework of Accountability*, Annex, Section L, paragraph 26 requires Field Security Coordination Officers (FSCO) to conduct "security surveys of residential areas and premises." Furthermore, the *Framework of Accountability*, Annex, Section N, paragraph 5, requires Local Security Assistants (LSAs) to assist in "monitoring compliance" with respect to residential security measures. Finally, the *Framework of Accountability*, Annex, Section G, paragraph 6 mandates representatives of UNSMS organizations to ensure "full and complete compliance by their personnel and their recognized dependants with all security-related instructions" while paragraph 7 requires them to act on "instances of non-compliance of security policies, practices and procedures" and advise the DO on "actions taken."

Annex A

Terms of Reference for the Residential Security Measures Review Group (RSMRG)

1. The Residential Security Measures Review Group (RSMRG) is intended to resolve an impasse between the United Nations Department of Safety and Security's Division of Regional Operations (UNDSS/DRO) and Headquarter Security Focal Points (SFPs) of respective parent organizations with regard to what RSMs, if any, shall be approved for a duty station based upon the proposal submitted by the Designated Official (DO).

2. The RSMRG shall convene whenever consensus cannot be established between UNDSS/DRO and Headquarter SFPs of respective parent organizations with regard to the DO's proposal. The RSMRG shall meet no later than forty-five (45) calendar days after UNDSS/DRO's initial receipt of the DO's proposal.

3. The RSMRG shall include the following members:
   (a) The Director or Deputy Director of UNDSS/DRO, as Chair of the RSMRG, with the relevant UNDSS/DRO Desk Officers present;
   (b) A maximum of three Headquarter SFPs of United Nations Security Management System (UNSMS) organizations with a presence at the duty station, including the UNSMS organization with the greatest number of personnel at the duty station; and
   (c) Three Headquarter SFPs nominated by the Inter-Agency Security Management Network (IASMN) to serve on the RSMRG on an annual basis.

4. The RSMRG shall require a quorum of five (5) members, with at least one (1) member identified under paragraph c(i), c(ii), and c(iii) of this Annex, respectively, in attendance.

5. The RSMRG shall evaluate the DO's proposal in an effort to establish consensus.
   (a) If consensus is established, the Director or Deputy Director of UNDSS/DRO, as Chair of the RSMRG, shall notify the DO and Headquarter SFPs of respective parent organizations of any approved RSMs and financial caps.
   (b) If consensus cannot be established within forty-five (45) calendar days after UNDSS/DRO's initial receipt of the DO's proposal, the Under-Secretary-General for Safety and Security shall take the final decision, either upholding the DO's proposal or incorporating any amendments.

6. The Director or Deputy Director of UNDSS/DRO, as Chair of the RSMRG, shall ensure that a written summary of the RSMRG's deliberations and related outcome is provided to the DO and Headquarter SFPs of respective parent organizations.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter IV

SECURITY MANAGEMENT

SECTION T

Arrest and Detention

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 15 April 2012
Technical Review: 1 May 2017

A. Introduction

1. It is important to have clarity on the role that United Nations security officials play when individuals covered by the United Nations Security Management System (UNSMS) are arrested or detained by authorities of a Government. Clarity on the key legal and procedural issues surrounding arrest and detention enhances the ability of the UNSMS to ensure the safety and welfare of individuals affected.

B. Purpose

2. The purpose of this policy is to establish roles and responsibilities for officials in the UNSMS upon receiving information about the arrest or detention of any individual covered by the provisions of this policy. It is not intended to replace or contravene other administrative issuances of UNSMS organizations regarding arrest and detention.[1]

C. Applicability

3. The policy is applicable to all organizations and all individuals covered by the UNSMS, as defined in Chapter III of the *Security Policy* Manual (SPM) ("Applicability of United Nations Security Management System").

D. Conceptual Framework

4. Organizations participating in the UNSMS should follow standard procedures for responding to any incident of arrest and detention of an individual covered in paragraph 3 above.

5. The entities comprising the UNSMS are in some cases subject to different legal regimes governing their status, privileges and immunities and those enjoyed by their personnel. Therefore, it would be inappropriate for security officials to make determinations on the legal status of the person under arrest or detention. The relevant member organization of the UNSMS will provide, in accordance with its legal status and applicable legal instruments, guidance to the relevant security officials with respect to the arrest or detention of individuals for whom it has security responsibility.

6. The overall responsibilities of actors of the UNSMS at the duty station[2] in regard to incidents of arrest and detention of individuals covered by the provisions of this policy are to the following:

   (a) Ensure the applicable organization's headquarters is informed of the situation;

   (b) Immediately report the incident to the Under-Secretary-General for Safety and Security. This responsibility includes gathering all relevant information

[1] In the United Nations Secretariat, this would be ST/AI/299.
[2] This includes the Designated Official and/or the applicable UNSMS organization Representative.

about the incident, including from national authorities and from access to the detained person;

(c) When deemed appropriate, such as when there are concerns for the safety and/or welfare of the individual arrested or detained, request access as soon as possible to the detained person by an official of the United Nations and, if feasible, a medical physician. When such access is not granted, there should be systematic follow-up to request it until it is granted.

E. Duties and Responsibilities

7. When an individual covered by the UNSMS, as per paragraph 3 above,[3] has been arrested or detained by authorities of a Government, actors of the UNSMS at the duty station[4] shall immediately report the incident by the fastest means of communication available to the employing organization headquarters and the Under-Secretary-General for Safety and Security as soon as possible.

8. The Designated Official (DO) or the applicable UNSMS organization Representative at the location where the arrest or detention has taken place shall immediately contact the Foreign Ministry or relevant government office and request:

   (a) All relevant information about the arrest or detention; and

   (b) When there are concerns for the safety and/or welfare of the individuals arrested or detained, the Government's cooperation in arranging as a matter of urgency that representatives of the United Nations accompanied, if feasible, by a medical physician of their choice be given access to the individual arrested or detained. If necessary and applicable, the most senior security professional directly supporting the DO[5] shall use contacts at his or her level to assist the DO in seeking the Government's cooperation in this regard.

9. The report to the Under-Secretary-General for Safety and Security shall convey all information readily available, including the following:

   (a) The name and nationality of the person arrested or detained, his/her employment status with and official functions for the UNSMS organization concerned; for family members, the family relationship must be given. In the case of children, the age(s) should be given;

   (b) The time, place and other circumstances of the arrest or detention;

[3] In case of doubt concerning whether a person is included or not, the DO's report shall include information on the person's status.
[4] This includes the DO and/or the applicable UNSMS organization Representative.
[5] This is usually the Chief Security Adviser or another Security Adviser, including their officer-in-charge *ad interim*. Where a CSA or SA is not present, this term is equivalent to the titles of Chief Security Officer, Chief of Security and Safety Services or Local Security Assistant (if necessary in countries where no international professional security adviser has been assigned or is present).

(c) The legal expression or term used by the applicable local law to describe the arrest or detention;

(d) The legal grounds for the arrest or detention, including any charges against the person concerned;

(e) The name of the governmental agency, such as a court or administrative authority, under whose authority the measure is taken;

(f) Whether a representative of the United Nations has been or will be given access to the person arrested or detained. In the affirmative, any request or other reaction from the person concerned also shall be conveyed;

(g) Whether consular protection and/or legal counsel is planned to be availed to the person arrested or detained. In the affirmative, the identity of these services shall be conveyed; and

(h) An assessment of the welfare or safety of the arrested or detained individual, including any reports of mistreatment.

10. If information on some of the items listed above is not available without delay, the available information should be forwarded immediately and the missing items shall be communicated in a supplementary report or reports as soon as possible. Additional information relevant to the case shall also be reported as soon as possible. This will ensure that there is accurate and up-to-date information available centrally on the arrested or detained individual(s).

11. The employing organization will be responsible for communications with the immediate family members and staff representatives concerned. The employing organization shall also determine what further action may be required, including, as appropriate, the involvement of the Secretary-General and the Office of Legal Affairs.

12. The present procedures shall also be applied, as appropriate, with respect to detention carried out by persons other than authorities of the host Government.

F. Final provisions:

13. This policy is meant to be made available to all United Nations personnel.

14. This policy enters into force on 15 April 2012.

15. Field Security Handbook (2006), Chapter VI, Section F, paragraphs 6.18-6.26 and Annexes M and N are hereby abolished.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter IV

SECURITY MANAGEMENT

SECTION U

Hostage Incident Management

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 15 April 2012
Technical Review: 31 August 2016

A. Introduction

1. As the organizations of the United Nations Security Management System (UNSMS) are increasingly called upon to operate in insecure areas, the risk of United Nations personnel or their families becoming the victims of a hostage incident has increased as well. This policy provides actors within the UNSMS with an overview of how the United Nations manages a hostage situation.

2. This policy must be read in conjunction with UNSMS "Guidelines on Hostage Incident Management" available for Designated Officials (DOs), members of a Security Management Team (SMT) and Security Officials within the organizations of the UNSMS.

B. Purpose

3. The purpose of this policy is to outline the UNSMS strategy and approach to managing the risk from hostage-taking.

C. Application/Scope

4. The policy is applicable to all individuals covered by the UNSMS, as defined in Chapter III of the *Security Policy Manual* (SPM) ("Applicability of United Nations Security Management System"). These individuals include the categories of "United Nations Personnel" and "Other Individuals Covered" (the latter of which includes eligible family members).

5. The UNSMS hostage incident management processes may be applied to secure the release of individuals not covered by paragraph 4 above in *extremis* situations.

D. Conceptual Framework

6. The policy of the organizations of the UNSMS with regard to hostage-taking of personnel and other individuals covered is based on the existing norms of international law as reflected in the 1979 International Convention against the Taking of Hostages which, *inter alia*, provides that the taking of hostages is an offence of grave concern to the international community, that any person committing an offence of taking hostages shall either be prosecuted or extradited, and that States shall make such offences punishable by appropriate penalties which take into account the grave nature of these offences.

7. The policy of the UNSMS regarding hostage-taking is also based on the relevant decisions of its principal organs adopted in furtherance to the aforementioned norms of international law and, in particular, on Security Council resolution 579 (1985) by which the Council unequivocally condemned hostage-taking, called for the immediate release of all hostages wherever and by whomever they were being held, and affirmed the obligation of all States in whose territory hostages were held to urgently take all appropriate measures to secure their safe release and to prevent the commission of acts of hostage-taking in the future.

8. For the purposes of the present policy, hostage-taking is defined as the seizure or detention with a threat to kill, injure or to continue to detain individuals (hostages) in order to compel a third party, namely a State, an organization of the UNSMS, a natural or juridical person or group of persons, to do or to abstain from doing any act as an explicit or implicit condition for the release of the hostages.

E. Hostage Incident Management Policy

9. Should individuals covered by the UNSMS be taken hostage, the organization shall make every effort to secure their speedy and safe release. To achieve this goal, the organization may establish contact or start a dialogue with the hostage-takers if it is determined that this would promote the speedy and safe release of the hostages. Such contact or dialogue should be aimed at trying to convince the hostage-takers of the inhumanity, illegality and futility of their actions as a means of attaining their objectives.

10. The Organization shall neither pay ransom[92] nor make any substantial concessions to hostage-takers to secure the release of hostages, nor shall it intervene with the Member State concerned to make concessions in exchange for hostages because this would encourage potential hostage-takers, and thus increase the danger that other staff members might face in the future.

F. Planning and Prevention

11. Good security planning and coordination will greatly reduce the risk of United Nations personnel and other individuals covered becoming hostages and assist adherence to and compliance with this policy. To assist DOs in this effort, a simple hostage risk assessment methodology has been included in the UNSMS "Guidelines on Hostage Incident Management". Assessments should be undertaken before, during and after the conclusion of an incident. This is essential in the development of strategy, tactics and security.

12. Every hostage situation is different. There are no strict rules of behaviour; however, there are techniques which can be used by personnel to minimize the effects of a detention in the unlikely event they are taken hostage. Information on how to survive as a hostage is contained in Annex A below. This information should be made available to all United Nations personnel in the context of a security training programme at those duty stations where there is a threat of hostage-taking.

G. Responsibilities of Member States

13. Notwithstanding the provisions of the present procedures, the Government of the State in which the hostage-taking has occurred, or, if applicable, the Government of the State where the hostages are held by the offenders, has the primary responsibility

[92] Ransom is defined as the money or other consideration paid for the release of a hostage.

under international law to take all measures it considers appropriate to ease the situation of the hostages, in particular to secure their release and, after their release, to facilitate, when relevant, their departure. Any request for United Nations assistance in mediating an agreement to secure the release of hostages, made either by a Member State or an organization involved in the hostage incident, must be forwarded to the Under-Secretary-General for Safety and Security for approval.

H. Decision-Making Authority

14. The Under-Secretary-General for Safety and Security is directly accountable and reports to the Secretary-General. He/she is responsible for developing security policies, practices and procedures for the UNSMS to ensure implementation, compliance and support for security aspects of their activities. In the event of a hostage-taking, the Under-Secretary-General for Safety and Security will take the necessary policy decisions and ensure a coherent response by the Organization.

15. Should United Nations personnel, or other individuals covered, be taken hostage, it is the responsibility of the DO, who, in accordance with the Framework of Accountability of the United Nations Security Management System, is the key person in the security arrangements at the duty station, to take all necessary actions on behalf of the Organization to secure the speedy and safe release of the hostage(s). Such actions should be taken by the DO in consultation with the SMT and the United Nations Department of Safety and Security. In those instances where the issues involved are so sensitive as to cause damage to other United Nations personnel or have an impact on United Nations operations inside or outside that particular duty station, the DO should not proceed with any decisions which might have significant implications for the Organization and its personnel without obtaining the concurrence of the Under-Secretary-General for Safety and Security. Throughout the hostage incident, the DO should consult with the senior official of each organization at the duty station which has personnel being held hostage.

I. Hostage Incident Management

16. The UNSMS will manage the risk posed by hostage-taking, as well as hostage incidents themselves, in accordance with the "Guidelines on Hostage Incident Management" available for DOs, members of a SMT and Security Officials with the organizations of the UNSMS.

17. Coordinated planning and a unified response by the United Nations, host Governments and any other national representatives of the hostages is critical to prevent negotiations being compromised by differing interests and is crucial to securing the release of the hostage(s).

J. Lessons Learned Report

18. After the incident is over, a review and evaluation of the Hostage Incident Management Plan and the manner in which personnel responded should be conducted. The lessons learned not only enable the DO to make improvements to the local plan, but also can help other duty stations in reviewing or preparing their plans. UNSMS "Guidelines on Hostage Incident Management" provide methods for conducting and reporting on this evaluation.

19. A copy of the evaluation report prepared by the DO must be forwarded to the Under-Secretary-General for Safety and Security not later than 30 days after the termination of the incident. The United Nations Department of Safety and Security will consolidate the key lessons learned and share them with Senior Security Managers/Security Focal Points at the Headquarters of organizations participating in the UNSMS, as appropriate.

K. Enforcement

20. In the event of an investigation into a hostage incident, findings that any United Nations personnel failed to abide by the terms of this policy may lead to administrative or disciplinary proceedings.

L. Final Provisions

21. This policy is meant to be distributed to all United Nations personnel.

22. This policy enters into force on 15 April 2012.

23. *Field Security Handbook* (2006), Chapter VI, Section H, paragraphs 6.29-6.47 and "Hostage Incident Management Guidelines" (June 2006) are hereby abolished.

Annex A

Surviving as a Hostage

1. Every hostage or kidnap situation is different. There are no strict rules of behaviour; however, there are steps which can be taken to minimize the effects of detention.

2. If you are taken hostage or kidnapped, there are a number of options which could enhance your ability to cope and to see the incident through to a successful release. The following techniques have been successfully employed by persons taken hostage:

   (a) At the time of your seizure, do not fight back or attempt to aggravate the hostage-takers. You may be injured if you attempt to resist armed individuals. There is a possibility that you will be blindfolded and drugged;

   (b) Be prepared to explain everything you have on your person;

   (c) Immediately after you have been taken, pause, take a deep breath and try to relax. Fear of death or injury is a normal reaction to this situation. **Recognizing your reactions may help you adapt more effectively**;

   (d) Do not be a hero; do not talk back or act "tough". **Accept your situation**. Any action on your part could result in a violent reaction from your captors;

   (e) The first 15 to 45 minutes of a hostage situation are the most dangerous. Follow the instructions of your captors. Your captors are in a highly emotional state, regardless of whether they are psychologically unstable or caught in an untenable situation. They are in a fight or flight reactive state and could strike out. **Your job is to survive**. After the initial shock wears off, your captors are able to better recognize their position;

   (f) **Keep a low profile**. Avoid appearing to study your abductors, although, to the extent possible, you should make mental notes about their mannerisms, clothes and apparent rank structure. This may help investigators after your release;

   (g) Be cooperative and obey hostage-takers' demands without appearing either servile or antagonistic. Be conscious of your body language as well as your speech. Do not say or do anything to arouse the hostility or suspicions of your captors. **Do not be argumentative. Act neutral and be a good listener to your captors**. Do not speak unless spoken to, and then only when necessary. Be cautious about making suggestions to your captors, as you may be held responsible if something you suggest goes wrong;

   (h) Anticipate isolation and possible efforts by the hostage-takers to disorient you, including unverifiable stories by your captors or frequent movements to different locations;

(i) Try to keep cool by focusing your mind on pleasant scenes or memories or prayers. Create games and amusement in your mind. Try to recall the plots of movies or books. This will keep you **mentally active**;

(j) Ask for anything you need or want (medicines, books, and paper). All they can say is no;

(k) **Build rapport** with your captors. Find areas of mutual interest which emphasize personal rather than political interests. An excellent topic of discussion is family and children. If you speak their language, use it -- it will enhance communications and rapport;

(l) **Exercise daily**. Develop a daily physical fitness programme and stick to it;

(m) As a result of the hostage situation, you may have difficulty retaining fluids and may experience a loss of appetite and weight. Try to drink water and eat even if you are not hungry. It is important to maintain strength;

(n) Do not make threats against hostage-takers or give any indication that you would testify against them. If hostage-takers are attempting to conceal their identities, give no indication that you recognize them;

(o) Try to think of persuasive reasons why hostage-takers should not harm you. Encourage them to let authorities know your whereabouts and condition. Suggest ways in which you may benefit your captors in negotiations that would free you. It is important that your abductors view you as a person worthy of compassion and mercy. Never beg, plead or cry. You must gain your captors' respect as well as sympathy;

(p) If you end up serving as negotiator between hostage-takers and authorities, make sure the messages are conveyed accurately. Be prepared to speak on the radio or telephone;

(q) If there is a rescue attempt by force, drop quickly to the floor and seek cover. Keep your hands on your head. When appropriate, identify yourself;

(r) Escape only if you are sure you will be successful. If you are caught, your captors may use violence to teach you and possibly others a lesson;

(s) If possible, stay well-groomed and clean;

(t) At every opportunity, emphasize that, as a United Nations employee, you are neutral and not involved in politics; and

(u) **Be patient**

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter IV

SECURITY MANAGEMENT

SECTION Y

Improvised Explosive Devices (IEDs)

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 8 November 2012
Technical Review: 1 May 2017

A. Introduction

1. The use of Improvised Explosive Devices (IEDs) has increased by threat actors in many areas where the United Nations has operations. The United Nations has been the target of IEDs, including Person-Borne and Vehicle-Borne IEDs to devastating effect, and it can be expected that the United Nations will be targeted again by such weapons. An IED is a uniquely dangerous weapon due to its versatility, adaptability and method of employment.

2. Nevertheless, United Nations system entities are required to implement programmes and activities in areas where IEDs are currently employed or may be employed in the future, including where IEDs deliberately or indirectly threaten United Nations personnel, property and programmes. Some United Nations entities have been requested to engage in the removal of IEDs still operational with little policy guidance about the security risks this might entail. For these reasons, there is a clear need for a policy on the United Nations' approach to managing the security risk posed by IEDs.[1]

B. Purpose

3. The purpose of this policy is to outline the United Nations Security Management System (UNSMS) approach to managing the security risk posed by IEDs that directly or indirectly threaten United Nations personnel, property or programmes and to delineate the roles, responsibilities and limitations within the United Nations system for the management of these security risks[2].

C. Application/Scope

4. This policy is applicable to all UNSMS entities (herein "United Nations entities"), including all individuals defined in Chapter III of the *Security Policy Manual* (SPM) ("Applicability of Security Arrangements") (herein "United Nations personnel"). This policy does not cover members of formed military or police units when deployed with their contingent or unit in United Nations missions.

5. The scope of this policy is confined to IEDs that directly or indirectly threaten United Nations personnel, property or programmes. This policy does not address the United Nations' approach to, and management of, the effect of IEDs on others, including civilian populations.

6. Details on specific IED security risk management measures and related technical procedures will be covered in separate UNSMS standards and procedures.

[1] On 13 July 2010, the Secretary-General's Policy Committee decided that "DSS will, in consultation with DPKO, DPA and all other relevant UN agencies, coordinate and facilitate the development of a comprehensive policy on the UN's approach to Improvised Explosive Devices (IEDs) that are part of active hostilities and target UN personnel and facilities."
[2] Please refer to *Security Policy Manual* Chapter IV, Section A, Policy on Security Risk Management.

D. IED Definitions

7. For the purposes of this policy, an IED is defined as an explosive device fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to kill, injure, damage, harass or distract. IEDs are often made from commercially available products and/or military munitions, are simple in design and are usually cheap in labour and cost to produce.

8. IEDs are highly versatile weapons due to the multiple methods available for their construction, delivery and initiation. This versatility allows them to be rapidly adapted to achieve different effects against varying targets, defeat the tactics and counter-measures employed by opponents and/or changes in the supply of raw material for their construction. The versatility and adaptability of IEDs, combined with their simplicity and low cost in manufacture, have made them a preferred weapons choice of certain threat actors who have used them to either attack larger and better equipped security forces (often with an indiscriminate impact on the civilian population) or to target civilians directly (including the United Nations).

9. United Nations entities working in complex threat environments have long been confronted with various types of weapons, including explosive weapons. In most cases, the United Nations has dealt with explosive weapons that were abandoned or unexploded ordnance, including "explosive remnants of war" (ERW) that have ceased to have value for those who deployed them. However, explosive weapons, including IEDs, that are not remnants are considered "operational" (see below) and of some value to those who deploy or use them.

E. Remnant and Operational IEDs

10. For the purpose of this policy, IEDs are categorized as either a "Remnant IED" or an "Operational IED".

11. For the purpose of this policy, a "Remnant IED" is defined as an IED that has been declared so through the official procedures governing such decisions within the United Nations system, involving the Resident Coordinator/Humanitarian Coordinator, in consultation with the United Nations Country Team and mine-action advice, if necessary. Such decision-making processes will consider the political, humanitarian, legal and other issues of the context in which the IEDs are found.

12. For the purpose of this policy, an "Operational IED" is defined as an IED that has **not** been officially declared a Remnant IED by the process described in paragraph 11 above. If there is any doubt as to whether an IED has been officially declared a Remnant IED, it shall be assumed to be an Operational IED by default.

13. Various United Nations entities have a mandate and clear policies and guidelines for dealing with explosive remnants, for example the International Mine Action

Standards (IMAS) that include safety principles for dealing with these explosive hazards.[3] These safety principles, as well as advice from mine action advisers, are the basis of the United Nations strategy for lowering the risk posed by Remnant IEDs.

F. Managing the Security Risk posed by IEDs

14. IEDs can create a significant safety and security risk to the United Nations if not addressed. The security risk posed by IEDs that deliberately or indirectly threatens United Nations personnel, property or programmes will be managed through existing Security Risk Management policy[4] and manual. The strategy of the United Nations for managing the security risk from IED threats is one of both **prevention** and **mitigation**, and can include any prevention and/or mitigation measure except activities prohibited in paragraph 16 below.

15. **Prevention** entails physical, procedural and training measures intended to lower the likelihood of an IED incident occurring and affecting the United Nations. Prevention measures available to United Nations entities, include, but are not limited to, information exchange and management, travel planning, security-awareness programmes and electronic countermeasures. **Mitigation** entails physical, procedural and training measures intended to lower the impact of an IED incident once it has occurred. Mitigation measures available to United Nations entities, include, but are not limited to, defensive measures such as blast/ballistic protection and stand-off distance and crisis response plans and preparations for rapid medical attention. Approved IED security risk management measures will be included in the country-specific Minimum Operating Security Standards (MOSS).

16. United Nations entities and/or personnel covered by the provisions of this policy, as laid out in paragraph 4 above, cannot directly engage in, support or fund activities primarily meant to disarm, remove or destroy an Operational IED. This provision is founded on the understanding that interference with the active weapons systems of threat actors may create the intention and perceived justification for violent action against the United Nations. This provision is further reinforced in situations of armed conflict by the humanitarian principle of neutrality, as enshrined in international humanitarian law and other provisions of international law. This policy should not preclude United Nations personnel from conducting capacity development of national security authorities for the protection of civilians.

17. Nevertheless, nothing in this policy is meant to contravene the provisions of the United Nations "Use of Force Policy" (see *Security Policy Manual* (SPM), Chapter IV, Section H) as it may apply to defensive actions that may be deemed necessary in

[3] See, for example, IMAS 10.10 – 10.70, "Mine Action Safety and Occupational Health" at http://www.mineactionstandards.org/international-standards/imas-in-english/list-of-imas/.

[4] Please refer to the Security Policy Manual, Chapter IV, Section A on "Policy on Security Risk Management" which entered into froce on 18 Aptil 2016 and Security Risk Management Manual of 11 December 2015..

emergency situations meant to negate an imminent threat to the United Nations from an IED.

18. The primary responsibility for the management of IEDs, especially Operational IEDs, rests with the host Government or any other authority in control, including occupying powers or foreign forces operating in support of the authorities. Managing the security risk from Operational IEDs that directly target the United Nations may require the assistance of the host country, United Nations peacekeeping mission police/military assets and/or other international military/police forces, including to engage in activities prohibited to United Nations personnel as per paragraph 16 above.

19. If after prevention and mitigation measures are implemented the residual security risk from IEDs is deemed unacceptable,[5] then the only option is to avoid the risk by temporarily removing United Nations personnel or assets from the danger as per *Security Policy Manual* (SPM), Chapter IV, Section D ("Relocation, Evacuation and Alternate Work Modalities – Measures to Avoid Risk").

G. Roles and Responsibilities

20. In the management of the security risks posed by IEDs, officials of the UNSMS in-country, including the Designated Official (DO), members of the Security Management Team, and UNSMS Advisers, must fulfil their responsibilities as per the Framework of Accountability[6] for security and all other existing security management policies, including those governing Security Risk Management, with special reference to Section F above.

21. DOs have special responsibility to liaise with host country or other applicable authorities in relation to IEDs on behalf of the United Nations and to consult, as necessary, with the Under-Secretary-General for Safety and Security in implementing a workable IED security risk management plan.

22. Heads of United Nations entities are responsible for informing their respective personnel of the threats and risks posed by IEDs and for properly implementing the Security Risk Management measures included in this policy (and approved by the DO) to lower the risk to their personnel, property and programmes.

23. DOs and heads of United Nations entities are to ensure that appropriate financial resources are forecasted and allocated to implement the approved IED security risk management measures.

[5] See *Security Policy Manual*, Chapter IV, Section C ("Guidelines for Determining Acceptable Risk").
[6] See *Security Policy Manual*, Chapter II, Section B ("Framework of Accountability for the United Nations Security Management System").

24. United Nations Security Advisers shall advise on whether all required and approved IED security risk measures and procedures are in place and effective, including, but not limited to, physical protection, access control, training, contingency/crisis plans and information management and analysis.

25. All United Nations personnel shall be familiar with and abide by all United Nations IED risk management measures and procedures established in-country. Personnel covered by the provisions of this policy have a special responsibility to refrain from any activities outlined in paragraph 16 above and to report to their respective headquarters any attempts to force or persuade them to do so.

H. Enforcement

26. In the event of an investigation into an IED-related incident, findings that any United Nations personnel failed to abide by the terms of this policy may lead to administrative or disciplinary proceedings.

I. Final Provisions

27. This policy is meant to be made available to all United Nations personnel.

28. This policy enters into effect on 8 November 2012.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter V

COMPLIANCE WITH SECURITY POLICIES AND PROCEDURES

SECTION A

Security Clearance Procedures and the Travel Request Information Process (TRIP)

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 8 April 2011
Technical Review: 1 May 2017

A. Introduction

24. In accordance with the Framework of Accountability for the United Nations Security Management System (UNSMS), the Secretary-General delegates to the Designated Official (DO), through the Under-Secretary-General for Safety and Security, the requisite authority to take security-related decisions. Based on the DO's authority and responsibility for the security and safety of all United Nations system personnel and their eligible family members at a duty station, it is mandatory that DOs manage security clearance procedures for their area of responsibility and issue security clearances for external and internal travel. To assist with this responsibility, the Department of Safety and Security (UNDSS) supports a web-based system called "Travel Request Information Process" (TRIP).

25. Security clearance procedures are required so that the DO and other officials of the UNSMS in-country can:

    (a) Effectively monitor the location and number of United Nations system personnel and eligible family members and include them in the country security plan;

    (b) Provide important security information to United Nations system personnel and eligible family members on official travel, including locating all registered individuals in the event of a crisis or emergency, and;

    (c) Control the number of United Nations system personnel and eligible family members where the security plan requires it.

B. Purpose

26. The purpose of this policy is to ensure that all United Nations system personnel and related individuals (as explained in Section C below) on official travel on behalf of the Organization obtain security clearance before travelling and to outline the relevant roles and responsibilities regarding security clearances.

C. Application/Scope

27. The policy is applicable to all individuals covered by the UNSMS, as defined in Chapter III of the *Security Policy Manual* (SPM) ("Applicability of United Nations Security Management System"), who are on official travel for the Organization. Individuals covered by the provisions of this policy are herein referred to as "personnel" and "traveller" interchangeably.

D. Security Clearance – Official Travel

28. It is mandatory for United Nations system personnel and eligible family members to obtain security clearance for all official travel, regardless of location, and they cannot commence official travel without obtaining it (except as laid out in Section G below). The TRIP web-based system provides for "automatic" clearance response when the Security Plan allows (See Section E, paragraph 17 below). Other technological refinements that will facilitate requests for security clearance are supported and encouraged.

29. Organizations of the UNSMS shall make all necessary effort so that their personnel (and eligible family members) receive security clearance prior to all official travel. Organizations must also make all necessary effort so that all their travellers are well

acquainted with existing or potential security problems in the areas that they intend to visit.

30. It is critical that all travellers understand their responsibility for their security while on official travel, such as obtaining a security clearance prior to all official travel, obtaining destination-specific security information and advice prior to travelling and obtaining a security briefing from the appropriate security official upon arrival at their destination.

31. For the purpose of this policy, official travel includes official home leave or other entitlement travel where the cost of travel is borne by organizations of the United Nations system. This applies regardless of whether official travel is undertaken by air, sea, land or any combination thereof.

32. . Based on the Security Risk Management (SRM) process, security clearance authority for the SRM areas in which security risk level is unacceptable is not delegated and will be granted only by the Under-Secretary-General for Safety and Security on behalf of the Secretary-General.

33. The DO is responsible and accountable for his/her decision when providing security clearance for official travel to, through and within his/her area of responsibility, including when security clearances are issued automatically (see Section E below).

34. The DO has the authority to grant, deny or ask for more information on a security clearance request where delegation exists.

35. The DO may further delegate his/her authority to grant security clearance on his/her behalf. This delegation must be in writing and the DO remains ultimately accountable for all security clearances provided. For this purpose, authority may be delegated to:

    (a) The most senior security professional directly supporting the DO[1];
    (b) An Area Security Coordinator, who is responsible and accountable for security within his/her area of responsibility as designated by the DO, in consultation with the Security Management Team.

E. Security Clearance Procedures

36. This procedure applies to all personnel and eligible family members who are required to travel on official business to any location. The individual must submit a security clearance request in TRIP to the DO at the duty station to be visited. If the mission consists of more than one person, it is the responsibility of the mission team leader to request security clearance. For all official travel with his/her eligible family members, a staff member is considered the "mission team leader". Organizations may request security clearance on behalf of an individual, including consultants, experts on mission or other related personnel or eligible family members.

[1] This is usually the Chief Security Adviser or other Security Adviser, including their officer-in-charge *ad interim*. Where a Chief Security Adviser or Security Adviser is not present, this term is equivalent to the titles of Chief Security Officer, Chief of Security and Safety Services, Country Security Focal Point (CSFP) or Local Security Assistant (if necessary) in countries where no international professional security adviser has been assigned or is present.

37. The request for security clearance made in TRIP will include, at a minimum, the following information:

    (a) Name'
    (b) Nationality;
    (c) United Nations Laissez-Passer (UNLP) or national passport number, issue and expiry date;
    (d) Agency/organization;
    (e) Mission/travel purpose;
    (f) Specific dates of the mission;
    (g) Where the individual is staying while at the duty station.

38. A prerequisite for official travel by United Nations system personnel, with the exception of appointment travel, is successful completion of all required training, including "Basic Security in the Field" (BSITF) training for all official travel and "Advanced Security in the Field" (ASITF) for official travel to any field location.[2] Organizations of the UNSMS shall ensure that their personnel have completed these training courses as required. BSITF and ASITF certificates are valid for three years, at which point staff members must recertify.

39. Official travel within countries or other areas of responsibility also requires security clearance. TRIP ensures that internal security clearance requests are transmitted to the relevant person responsible (for example, the Area Security Coordinator), who processes the security clearance in accordance with his/her delegated authority in paragraph 12(b) above. DOs may create an "operational radius" whereby one security clearance applies to all official travel (see Section F below).

40. If the security plan for a certain location requires security clearance solely to track traveller numbers and movement, DOs have the option of setting "automatic" clearances in TRIP. When set to automatic, TRIP provides an immediate security clearance response when travellers create a TRIP entry for proposed official travel.

41. When the security plan requires control over the number of personnel or eligible family members in a specific location, DOs can set the TRIP system so that all official travel into a specific area has to be cleared manually. Manual security clearance procedures can be established at any location regardless of the security risk level, if the DO requires it, and it is highly recommended that all areas with high or very high residual security risk have manual security clearance procedures.

42. For official travel to areas requiring manual security clearance, TRIP entries must be submitted seven days before the start of travel to ensure sufficient time for the traveller to receive official approval. Locations requiring manual security clearance will be listed in the Travel Advisory issued by the UNDSS.

F. Security Clearances and Operational Radius

43. DOs can designate an Operational Radius, in which personnel routinely reside and operate and in which they can travel without obtaining further security clearance. Personnel

[2] For the purpose of this policy, "field location" is any location not designated as an "H" duty station under the mobility and hardship scheme established by the International Civil Service Commission (ICSC).

moving throughout this Operational Radius must be able to communicate with the United Nations radio room, communications centre or other source of assistance.

44. A cross-border Operational Radius may also be established. In this situation, the Under-Secretary-General for Safety and Security grants to one DO the authority, accountability and responsibility for an area on the other side of the border of that DO's country.[3]

45. An SRM process, in line with the SRM policy and manual[4], must justify the establishment of an Operational Radius as a security risk management measure. There must be clear justification showing that the area designated as the Operational Radius (including cross-border) contains similar threats and risks, as well as the requirement of one common set of security measures.

G. Exceptional Measures

46. In exceptional and compelling cases where insufficient time is available to comply with this policy, such as immediate medical evacuation or other life-threatening situations, the traveller must inform the DO or delegate, by the fastest means available, and complete the TRIP clearance process as soon as possible.

47. For the purposes of a "no notice" inspection or investigation by an agency or organization of the United Nations system, the Under-Secretary-General for Safety and Security may grant security clearances that are not submitted through TRIP in advance. The Department of Safety and Security will normally inform the DO and other concerned individuals of such official travel and, upon arrival in the country, the TRIP clearance will be processed.

48. If the security situation worsens, the DO must advise, through TRIP, all individuals with security clearance (and their employing organization via the Security Focal Point) whether the security clearance will be rescinded or if travel can take place as initially authorized.

H. Personal Travel

49. Personal travel, including for annual leave, is not official travel and does not require security clearance. However, all United Nations system personnel and/or eligible family members going on personal travel are strongly encouraged to register personal travel in TRIP, designating travel as such. Travellers completing a TRIP entry for personal travel will receive an acknowledgement along with essential security information. In the event of a crisis or emergency, it may also be possible for the local UNSMS to provide security support to United Nations system personnel and eligible family members who have registered personal travel in TRIP. Any such assistance is subject to the capacity of the UNSMS to provide such support at the time of the crisis or emergency.

I. Compliance with Security-Related Decisions

50. Personnel who refuse to comply with the security-related instructions of the DO may be informed by the DO, in writing and with a copy provided to the Security Focal Point at the

[3] A cross-border operational radius may be required when staff are residing in one country and traveling to work in a neighboring country on a daily basis.
[4] Please refer to *Security Policy Manual* Chapter IV, Section A on "Policy on Security Risk Management" which entered into force on 18 April 2016.

headquarters of their employing organization, that their security clearance has been revoked.

51. The DO will provide to the Department of Safety and Security, with a copy to the Security Focal Point at the Headquarters of the employing organization, the information and names of personnel refusing to comply with security clearance procedures and instructions.

J. Final Provisions

52. Chapter VI, Section A and Section B paragraph 6.2 of the Field Security Handbook (2006) and its Annex H are hereby abolished.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM

Security Policy Manual

Chapter V

COMPLIANCE WITH SECURITY POLICIES AND PROCEDURES

SECTION B

Safety and Security Incident Recording System (SSIRS)

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 17 April 2015
Technical Review: 1 May 2017

A. Introduction

1. The diversity and multitude of threat environments in which the United Nations Security Management System (UNSMS) operates requires mechanisms to help understand those threats and to allow senior managers the requisite information to assess and mitigate them. Knowledge of the type, location and impact of incidents that intentionally, or accidentally, harm United Nations personnel, programmes, premises and assets provides the foundation of this understanding and guides appropriate responses.

2. The Safety and Security Incident Recording System (SSIRS) is a tool intended to collect information on incidents that affect the UNSMS in order to inform of threats and incidents to contribute to situational awareness that supports effective response, including mitigation requirements and the review of operating modalities in accordance with security risk management practices.

3. SSIRS enables users to
   (a) **Register:** acknowledge that an incident occurred and alert others of this occurrence;
   (b) **Record:** store data;
   (c) **Query to support analysis**: contextualize information for security managers to interrogate and analyse;
   (d) **Disseminate:** distribute information products.

B. Purpose

4. The purpose of this policy is to define the type of incidents that are required to be recorded by SSIRS, by providing taxonomy of incidents, detail accountability for recording these incidents and instructions on the recording and endorsing processes.

C. Applicability

5. This policy is applicable to all personnel employed by the organizations of the UNSMS that have a security function within the UNSMS *Security Policy Manual* (SPM), Chapter II, Section B ("Framework of Accountability for the United Nations Security Management System"). In particular, this policy applies to all UNSMS actors as described within the Framework of Accountability, including personnel employed by the organizations of the UNSMS that have the responsibility to "report all security incidents in a timely manner."

6. This policy refers to the use of the Safety and Security Incident Recording System only. It does not alter or define responses to incidents. Standard Operating Procedures (SOPs) for appropriate incident management response, in addition to both UNSMS and organizational policies and guidelines, will outline the appropriate incident response in these cases.

D. Accountability for Security Incident Reporting

7. In accordance with the Framework of Accountability, all personnel employed by the organizations of the United Nations system are required to "report all security incidents in a timely manner".

8. Additionally, the Framework of Accountability requires the Designated Official (DO) to keep members of the Security Management Team (SMT), as well as senior officials of each organization at the duty station, as applicable, fully apprised of all security-related information and measures being taken in the country.

E. Use of the Safety and Security Incident Recording System

Requirements and Restrictions

9. SSIRS is primarily used to record incidents that harmed or had the capability and/or intent to harm United Nations personnel, programmes, activities, premises, facilities and assets only.

10. Reporting is mandatory for any incident involving or impacting United Nations personnel, programmes, activities, premises, facilities and assets.

11. SSIRS can be used to record incidents that do not involve or impact the United Nations. Use of SSIRS for non-United Nations impact incidents is at the discretion of the most senior security professional in each country. However, data related to non-United Nations impact incidents included in SSIRS cannot be used for any official purpose by any United Nations entity. It is for the exclusive use of the country inputting this data based on its own SOPs. Because this data is not verified or endorsed according to rules and standards set in the SSIRS policy or manual, this data is not to be used for any purpose except for those defined by individual country SOPs.

Responsibility for Using SSIRS

12. The most senior security professional is the person responsible for advising the DO within a designated area and is the person accountable for recording incidents in SSIRS. The most senior security professional will most likely be the Chief Security Adviser/Security Adviser, Chief Security Officer, Field Security Coordination Officer, Agency Security Officer or Country Security Focal Point, but can include others. The most senior security professional can only be security personnel recognized in the Framework of Accountability.

13. Accountability for ensuring that incidents are reported cannot be delegated; however, responsibility for data entry in SSIRS may be delegated. In consultation with the DO and the SMT, the most senior security professional determines the need and assigns rights to eligible persons (anyone with a role within the UNSMS) to enter and endorse incident data in SSIRS.

14. The United Nations Department of Safety and Security (UNDSS) Division of Regional Operations (DRO) will provide oversight on the daily implementation and use of SSIRS and review data entry in accordance with this policy.

15. To help ensure compliance in recording all incidents, SSIRS will automatically send an email showing all incidents recorded in the system for the past week to each Designated

Area's most senior security professional, DO/Area Security Coordinator (ASC) and relevant DRO Desk Officer, and will request them to verify that the data in respect of their area is complete.

F. Incident Recording Processes

16. The inclusion of an incident in SSIRS is a two-step process:

    (a) **Step 1: Entering incident data**: all relevant data regarding an incident, including who or what was impacted, when and where the incident occurred and how it happened is input into the SSIRS user interface. All data is in draft form and resides only on a local server until the incident data is endorsed;
    (b) **Step 2: Endorsing incident data:** all incident data entered into SSIRS (step 1) is reviewed for completeness and accuracy by the most senior security professional or his/her designate. Once reviewed, the most senior security professional/designate includes the SSIRS record in the global SSIRS data set by endorsing it.

Entering Incident Data

17. As described in paragraph 7 above, personnel employed by the organizations of the United Nations system are required to report incidents to UNSMS personnel who will then ensure the incident is recorded in SSIRS. Eligible persons with authority as delegated by the most senior security professional in a country are the only persons authorized to enter incident data directly into SSIRS.

    (a) Incidents involving only one organization

18. Individual organizations can input incidents involving or affecting their own personnel, programmes, activities, premises, facilities and assets into SSIRS as agreed to by the most senior security professional, in consultation with the DO and SMT, as outlined in paragraph 13 above.

    (a) Incidents involving multiple organizations

19. Incidents can be recorded by multiple organizations but must be reviewed and consolidated manually by the most senior security professional; alternatively, the most senior security professional may choose to enter data on incidents involving multiple organizations. This decision may be taken on a case-by-case basis and shall be made locally by the most senior security professional in consultation with the DO and SMT.

    (a) Other recording requirements

20. Incidents must be recorded in the designated area in which they occur. If a most senior security professional or other personnel of a UNSMS organization is informed of an incident that occurred outside his/her designated area, incident details must be relayed to the most senior security professional of the designated area in which the incident occurred.

21. All incidents must be recorded within seven days of the most senior security professional's knowledge of occurrence. If the incident is only drawn to the attention of the most senior security professional thereafter, it should still be recorded to ensure that all incidents are captured in the SSIRS system. In cases when multiple incidents occur within a given event, each incident will be recorded separately and then linked in the SSIRS.

22. If a country's most senior security professional decides to use SSIRS for the purpose of recording non-United Nations impact incidents, the SMT must agree on an SOP for recording and endorsing requirements. Once the SOP is adopted, the most senior security professional should request the capability to add non-United Nations impact incidents from UNDSS, Crisis Management Information Support Section (CMISS).

Endorsing Incident Data

23. The most senior security professional is responsible for ensuring the quality of incident data recorded by endorsing the record of the incident.

24. Endorsement of an incident is necessary for the incident to be included in the SSIRS dataset. Without endorsement, incident data will not be included in SSIRS.

25. The endorsement function can be delegated by the most senior security professional, but this must be delegated to a security professional (a UNSMS personnel who accepts responsibility and accountability for security management as per the Framework of Accountability).

26. The delegated entry and endorsement functions should ideally not reside with the same person.

27. Endorsement procedures for cases when incidents' details are unclear or there are discrepancies in details will be addressed through the UNSMS, as appropriate, for the designated area. Before endorsing a report, however, the onus is on the most senior security professional to ensure that the data entry is clear and accurate in accordance with this policy and guidelines.

Incident Response

28. SSIRS is primarily a recording mechanism. It does not replace SOPs within UNSMS organizations for reporting incidents nor does it trigger a response to an incident. In many cases, a SSIRS incident record might be created after an incident has received a response.

29. UNSMS organizations will have established critical incident management and response plans according to their own internal security management guidelines.

G. Disclaimer

30. Information in SSIRS is confidential and subject to all United Nations rules, regulations and procedures regarding information handling. It is to be used by UNSMS entities only. Any other use requires UNDSS permission.

H. Final Provisions

31. This policy shall be made available to all UNSMS organizations and to all individuals covered under UNSMS *Security Policy Manual*, Chapter III ("Applicability of United Nations Security Management System").

32. This policy enters into force on 17 April 2015.

33. *Field Security Handbook* (2006), Chapter VI, Section E, paragraphs 6.16-6.17 are hereby abolished**.**

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter V

COMPLIANCE WITH SECURITY POLICIES AND PROCEDURES

SECTION C

Security Training and Certification

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

8 November 2012
Technical Review: 1 May 2017

A. Introduction

1. To fulfil respective security-related responsibilities as detailed in the Framework of Accountability for the United Nations Security Management System, United Nations personnel at all levels requires proper training. Security-related training offers one of the most cost-effective ways to lower risks[1] to United Nations personnel, premises and assets. The Framework of Accountability clearly states that "all actors of the UNSMS are empowered by providing them with the necessary resources, training and a clear understanding of their responsibilities".[2]

2. The responsibility of the United Nations Department of Safety and Security (UNDSS) for security training across the whole United Nations Security Management System (UNSMS) is mandated by the General Assembly.[3] The UNSMS must have sustainable, coherent and targeted security learning programmes, including harmonized and regulated content for all security-related courses. Security training raises security awareness, promotes security culture and consciousness, improves security preparedness and creates the capacity to respond effectively to emerging threats towards the United Nations.

3. The goal of security training within the UNSMS is to enhance Security Risk Management effectiveness and cooperation between security personnel, managers with security responsibilities and all other personnel. Standardized training systems are an important tool in reaching this goal. At the same time, training must be delivered in a timely, cost-effective manner using the most appropriate means of delivery.

B. Purpose

4. This policy sets out the goals and parameters for UNSMS-wide security training. It identifies roles and responsibilities in the development and delivery of training materials, methodologies and learning programmes.

C. Applicability

5. The policy is applicable to all UNSMS organizations as well as all individuals defined in Chapter III of the *Security Policy Manual* ("Applicability of Security Arrangements").

D. Conceptual Framework

6. Specific objectives of security training are to develop and enhance the skills and knowledge of United Nations personnel to:

   a. Enhance the security preparedness of managers with security responsibilities within the UNSMS.

[1] Please refer to *Security Policy Manual* , Chapter IV, Section A (Security Risk Management Policy)
[2] *Security Policy Manual*, Chapter II, Section B ("Framework of Accountability for the United Nations Security Management System", paragraph 29).

[3] A/59/365 as of 11 October 2004, noted by A/RES/59/276 as of 17 January 2005.

b. Enhance the competencies, skills, knowledge, values and behaviour of all security personnel in the UNSMS.

c. Enhance security awareness for all United Nations personnel to assist them in acting in a manner that will not endanger their safety and security and to improve their understanding of their role in their own safety and security.

d. Enhance the security awareness training for eligible family members of United Nations personnel, especially at duty stations where they may be affected by the threats identified in the Security Risk Management process.

7. The strategy of security training within the UNSMS is to support effective United Nations operations worldwide by providing cost-effective security training to three categories of United Nations personnel: security managers,[4] security personnel and all other United Nations personnel.[5]

8. Security training within the UNSMS is either "core security training" or "specialized security training". Core security training ensures that United Nations personnel at all levels are familiar with their security responsibilities, how to fulfil those responsibilities and the range of support available to them. Specialized security training shall be designed to equip United Nations personnel with the specific knowledge and expertise they need to discharge their security responsibilities in a professional, consistent and accountable manner.

9. Recognizing that UNSMS organizations have their own professionally qualified trainers and learning managers, the UNDSS shall establish, through the Inter-Agency Security Management Network's "Security Training Working Group", a mechanism for certification on security learning programmes, to allow the greatest outreach for these learning products. Learning partnerships between UNDSS and UNSMS organizations ensures the best use of resources and training materials.

E. Training for United Nations Personnel

10. There are two core, self-administered online security learning programmes for all United Nations personnel: one basic programme and one advanced programme.

11. All United Nations personnel must successfully complete the basic security learning programme.

12. United Nations personnel assigned to, or visiting on official travel, any field location[6] must successfully complete the advanced security learning programme.

13. The certificates for the basic and advanced security learning programmes are valid for three years, after which the individual must re-certify.

[4] For the purposes of this policy, "security manager" refers to the Designated Official and Representatives of UNSMS organizations who are members of the Security Management Team in-country or are assigned as Area Security Coordinators or members of respective Area Security Management Teams.

[5] To include United Nations personnel who perform functions within a Warden System.

[6] For the purpose of this policy, "field location" is any location not designated as an "H" (Headquarters) duty station under the mobility and hardship scheme established by the International Civil Service Commission (ICSC).

14. It is the responsibility of all United Nations personnel to ensure that they have completed these training courses as required and of their respective organizations to ensure that these courses are made available.

15. In addition to the above, United Nations personnel must attend the required security briefings conducted by security personnel at each duty station and successfully complete other specialized security training where required at designated locations.

16. United Nations personnel who perform functions within a Warden System must successfully complete security training for those functions.

F. Training for United Nations Security Personnel

17. The security training curriculum provides progressive and comprehensive training at basic, intermediate and advanced stages and establishes an important career development channel for security personnel.

18. All security personnel with functional security responsibilities are to receive core training, specialist training or specific training relevant to their functional tasking, and this training should meet standards of content and methodology that are agreed upon through the Security Training Working Group. Additional career development courses are available on the UNDSS and UNSMS organization Learning Management Systems.

19. Core security training and learning programmes are designed to equip security personnel with the appropriate knowledge, skills and attitudes (behaviour) to fulfil their assigned functions to an agreed standard of competency. They will also enhance interoperability between UNSMS organizations and facilitate upwards mobility and career movement (i.e., "cross fertilization") of security personnel between UNDSS and other UNSMS organizations.

20. Specialized security training for security personnel shall depend on requirements to fulfil specific functions, including, but not limited to, courses on: hostage incident management, security analysis process and practice and close protection.

G. Training for United Nations Managers with Security Responsibilities

21. Security training is mandatory for security managers. Designated Officials are required to complete a Designated Official induction security orientation course prior to their assumption of duty at their respective country of assignment.

22. It is mandatory for Designated Officials, all members of Security Management Teams and Area Security Coordinators to complete training specific to their security functions. At a minimum, Designated Officials and Security Management Team members must complete the UNDSS online Security Management Team training module and maintain a record of certification.[7]

[7] Face-to-face Security Management Team training may also be conducted by qualified learning managers on a case-by-case basis.

H. Development of Training Materials and Delivery of Training Programmes

23. UNDSS is responsible for the following security training-related activities:

    a. Continuous review of training materials to ensure that they reflect approved security policies and procedures, best practices, lessons learned and requirements for objectivity.

    b. Through the Security Training Working Group, establish and oversee security-related qualification and certification standards and practices for learning managers and trainers across the UNSMS.

    c. With the support of the United Nations Department for General Assembly and Conference Management, develop security-related training materials in the official languages of the United Nations, as appropriate.

    d. Develop and maintain, in consultation with the Inter-Agency Security Management Network, the official listing of mandatory security training requirements.

24. UNDSS may provide security training through the following modalities:

    a. Distance learning initiatives.

    b. The Department's website and Learning Management System.

    c. Mobile training teams.

    d. A network of regional security training focal points, certified trainers and learning managers from UNSMS organizations.

    e. Outsourcing, where appropriate, to Member States, other UNSMS organizations or commercial vendors.

I. Management of Security Training Programmes

25. To ensure the relevance and efficiency of security training throughout the UNSMS, UNDSS will periodically assess training needs. All UNSMS organizations shall share training materials with other organizations within the system, either bilaterally or through the Security Training Working Group. This collaboration will help to ensure that training materials and activities meet requirements and may provide a basis for prioritization, cost efficiencies and the avoidance of duplication.

26. As part of its system-wide responsibility for security training, UNDSS shall establish and maintain a database to record training-related information regarding the number of United Nations personnel who have successfully completed security training.

27. UNDSS will catalogue its Learning Programmes, providing details of specific aims, learning objectives, key learning points, suggested methodologies for delivery and detailed lesson plans. Learning programmes will be available for use by qualified learning managers and certified trainers in any UNSMS organization. UNDSS will also cooperate closely, through the Security Training Working Group, with the

Learning Development Centres of other UNSMS organizations to develop learning best practices.

J. Roles and Responsibilities

28. In accordance with *Security Policy Manual*, Chapter II, Section B ("Framework of Accountability for the United Nations Security Management System"), the following are the responsibilities of various actors of the UNSMS in regards to security training:

    a. Senior Security Managers and/or Security Focal Points at Headquarters of UNSMS organizations shall ensure that all personnel of their organization, and their recognized eligible family members, are aware of security training requirements and facilitate the provision of security and safety training and briefings.

    b. Representatives of organizations participating in the UNSMS shall attend all security training as members of the Security Management Team.

    c. Chief Security Advisers/Security Advisers shall establish a system for briefing all personnel employed by the organizations of the UNSMS and their eligible family members upon initial arrival and provide local security training as necessitated by the security environment.

    d. Chief of Security and Safety Services/Sections shall provide standardized induction and specialist training for United Nations staff and security personnel.

    e. Chief Security Officers for Peacekeeping Missions (where the Head of Mission is not the Designated Official and where a UNDSS Chief Security Adviser is present) shall provide security training to mission personnel.

    f. Local Security Assistants shall assist in conducting security training for United Nation personnel, locally-recruited guards and others (including security guards from contracted companies) as appropriate.

    g. Personnel employed by the organizations of the UNSMS shall attend and complete security training relevant to their level and role and complete the required security training as outlined in paragraphs 10–16 above.

29. In accordance with *Security Policy Manual*, Chapter VII, Section D, *Road Safety*, UNSMS organizations in-country are responsible for road safety information and awareness campaigns for their personnel and for providing, in consultation and coordination with UNDSS, safe-driving training for drivers.

K. Final Provisions

30. This policy is to be made available to all United Nations personnel.

31. This policy enters into effect on 08 November 2012.

32. *Field Security Handbook*, Chapter II, paragraphs 2.5 (e), (f) and (j) are hereby abolished.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter V

COMPLIANCE WITH SECURITY POLICIES AND PROCEDURES

SECTION G

Boards of Inquiry

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 8 November 2012
Technical Review: 1 May 2017

A. Introduction

1. Using Boards of Inquiry as an analytical as well as a managerial tool to review investigation reports and record the facts of serious incidents is a well-established administrative practice in many organizations, including within the United Nations. Boards of Inquiry have proven to be useful in identifying gaps or deficiencies in procedures and policies and in strengthening internal controls to avoid recurrence and to improve managerial accountability. Recommendations of Boards of Inquiry can provide managers with a proposed course of action.

2. There is a corresponding need for a similar mechanism within the United Nations Security Management System (UNSMS) to review critical security and safety incidents involving the personnel and property of its member organizations. This mechanism would support the Framework of Accountability for the United Nations Security Management System and identify lessons learned to strengthen Security Risk Management (SRM) policy[1] and procedures and address operational gaps in SRM.

B. Purpose

3. The purpose of this policy is to establish a common framework within the UNSMS for convening and executing a Board of Inquiry (herein referred to as "a Board") following the investigation of a critical security incident that involves member organizations.

C. Application/Scope

4. The policy is applicable to all member organizations of the UNSMS and all their personnel (herein "United Nations personnel") as defined in Chapter III of the *Security Policy Manual* (SPM) ("Applicability of United Nations Security Management System").

D. Conceptual Framework

5. A Board of Inquiry is neither an investigative nor a judicial process and does not make recommendations on questions of compensation, legal liability or disciplinary action. A Board of Inquiry is convened after the investigators of the affected organizations have completed their investigation of the incident in accordance with their applicable legal framework. In appropriate cases, organizations affected will consider coordinating their pre-Board investigations with the view to gain maximum efficiency and preservation of evidence.

6. A Board of Inquiry is an analytical and managerial tool to review investigation reports and record the facts of critical security incidents involving organizations of the UNSMS, including whether the occurrence took place as a result of the acts

[1] Please refer to Security Policy Manual, Chapter IV, Section A, Policy on Security Risk Management, which entered into effect on 18 April 2016.

or omissions of any individual(s). The purpose of a Board of Inquiry is to identify gaps or deficiencies in SRM policy, procedures or operations, to SRM controls (lessons learned) and to improve accountability for SRM.

7. For the purpose of this policy, a "critical security incident" is defined as a significant occurrence caused by hostile action that results in death or serious injury of multiple personnel, generally of more than one UNSMS organization.

8. A Board of Inquiry is not appropriate in matters principally involving allegations of misconduct by any United Nations personnel. Such matters are to be handled by the relevant UNSMS organization in accordance with its internal policies and procedures.

9. Nothing in this policy inhibits the requirement for investigations, which might exist in certain cases, in accordance with other sources of policy and/or guidance of UNSMS organizations and national legislation.

E. Convening a Board of Inquiry

10. The Under-Secretary-General for Safety and Security will consult with the Executive Head(s) of the UNSMS organizations involved in an incident to determine together whether they consider that a Board of Inquiry is warranted. Where it is determined that such an inquiry is warranted, the Under-Secretary-General for Safety and Security shall proceed to convene the Board of Inquiry for that purpose.

11. The Board shall be established, and its members appointed, with a Convening Order signed by the Under-Secretary-General for Safety and Security after consultation with the Executive Head(s) of the UNSMS organization(s) involved in the incident, as per paragraph 10 above.[2] When necessary, the Under-Secretary-General for Safety and Security can consult the Executive Group on Security[3] before issuing a Convening Order.

12. The Terms of Reference of the Board constitutes an integral part of the Convening Order. The Terms of Reference is the framework within which the Board operates and defines the facts and issues the Board is to address. The Terms of Reference shall be as specific as possible and must provide a clear limit to the Board's scope of review. In particular, the Terms of Reference shall always specify that Board members are prohibited from making recommendations regarding compensation, disciplinary action or legal liability.[4] The Convening Order, including the composition of the Board, and the Terms of Reference shall be determined by the Under-Secretary-General for Safety and Security in consultation with the UNSMS organizations affected.

[2] Annex A provides a template for the Convening Order.
[3] See *Security Policy Manual*, Chapter II, Section C, "Terms of Reference for the Executive Group on Security".
[4] Annex B provides a template for developing Terms of Reference.

F. Composition of a Board of Inquiry

13. A Board of Inquiry shall comprise at least four (4) members, including a Chairperson. Due consideration shall be given to geographic and gender representation. A Board should generally not comprise more than six (6) members, including the Chairperson.

14. The Chairperson of the Board, whose name shall be identified in the Convening Order, shall be an individual with present or past United Nations system senior management experience, considering the provisions of paragraph 18 below.

15. At least one member of the Board shall be appointed from individuals recommended by the UNSMS organizations involved in the incident, considering the provisions of paragraph 17 below.

16. At least one member of the Board shall have practical and policy knowledge and experience of the UNSMS, considering the provisions of paragraph 17 below.

17. No person shall be appointed as a member of the Board if he or she

    (a) Has a perceived or actual conflict of interest with either the individuals or components involved in the incident under review;

    (b) Is from a unit or office that had the responsibility for security management of the location or office involved in the incident under review; or

    (c) Has taken part in the investigation of the occurrence, is a material witness, is an accused person, is a suspect from that investigation or is likely to have a role in reviewing the findings of the Board.

18. All Board members shall serve on the Board in their individual capacity and shall be independent for the purpose of this duty. Managers or supervisors of Board Members shall ensure that no undue pressure is exerted on them in the context of the Board's proceedings.

19. Depending on the nature of the occurrence, the Board may require expert advice in a related area. Subject experts shall be arranged by a Board Support Officer (see paragraph 22 below) with due regard to excluding conflict of interest with either the individuals or organizational components under review. Such experts shall not be considered Board members.

G. Support to the Board

20. The Board of Inquiry shall be supported by a Board Support Officer and a Secretary.

21. The Board Support Officer shall be responsible for all matters with regard to coordinating the convening process and ensuring the efficient functioning of the Board.

22. The Board Support Officer shall be appointed from the United Nations Department of Safety and Security or from one of the UNSMS organizations involved in the incident.

23. The Board Support Officer fulfils the following functions:

    (a) Draft the Convening Orders listing the names of the Board Chairperson and members and preparing, when necessary in consultation with the United Nations Office of Legal Affairs, incident-specific Terms of Reference for approval by the Under-Secretary-General for Safety and Security;

    (b) Administer the "Undertaking of Confidentiality" in accordance with the approved format;[5]

    (c) Provide administrative and logistical advice and support to Board members throughout the Board's proceedings;

    (d) Review the Board's draft report for quality control and format compliance;

    (e) Coordinate the review of the Board's report by the United Nations Office of Legal Affairs;

    (f) Submit the Board's report package and all annexes for approval by the Under-Secretary-General for Safety and Security;

    (g) Maintain all records related to the Board's review.

24. The Board Support Officer shall not be considered a Board Member.

25. A Secretary shall be appointed from the United Nations Department of Safety and Security or from one of the UNSMS organizations involved in the incident to serve the Board by providing day-to-day administrative assistance to its members, including the following:

    (a) Set up the initial briefings for the Board members;

    (b) Advise on Board procedures and arrange expert advice on applicable United Nations rules and regulations;

    (c) Arrange interviews with individuals who may have relevant information to provide;

    (d) Assemble relevant documentation from different sources;

[5]See Annex D.

(e) Prepare and participate in on-site visits;

(f) Keep minutes of interviews and deliberations;

(g) Draft the report for review by the Board members, the Board Support Officer, the United Nations Office of Legal Affairs and, in appropriate cases, other relevant offices;

(h) Obtain signatures of Board members, and of those who were formally interviewed by the Board, on the report case file documents; and

(i) Compile the report case file.

26. The Secretary shall not be considered a Board Member. However he/she shall be one of the signatories to the final report.

H. Proceedings of a Board of Inquiry

27. In its inquiry, a Board of Inquiry shall be responsible for the following:

(a) Receive the Convening Order and Terms of Reference;

(b) Receive a procedural briefing from the Board Support Officer and a legal briefing from the United Nations Office of Legal Affairs;

(c) Obtain all available investigation reports and other relevant source materials regarding the occurrence, including, *inter alia*: Security Incident Report(s), Military or Police Report(s), UNSMS organization investigation reports, technical assessments (including threat assessments and security risk assessments of the SRM process), witness statements, expert opinions, medical reports and evaluations and any other documents required by the Board to conduct its deliberations;

(d) Collect any relevant additional statements from any individual involved or affected by the incident, and conduct any necessary additional site visits, interviews, or further inquiries;

(e) Seek explanations or clarifications of technical or specialized reports or other information of a technical or specialized nature from experts or specialists, should it be deemed necessary by the Board to enable it to address all relevant issues;

(f) Establish facts from the whole body of available information presented and review the circumstances of the occurrence in a comprehensive manner; and

(g) Within the deadline specified in the Convening Order, present a written report to the Under-Secretary-General for Safety and Security, setting forth

in a clear, logical and objective manner the Board's findings, conclusions and recommendations.

28. United Nations personnel, as described in paragraph 4 above, have a duty to assist the Board of Inquiry by providing information they may have related to the incident. Any other person, including local citizens and local police or military officers, may be requested to make a statement to the Board or answer its questions, but are under no obligation to do so.

29. Due consideration shall be given to all individuals who were affected by or witnessed the incident – especially minors, particularly in sensitive cases – to protect them from unnecessary repeat interviews that could be intimidating.

30. Principles of fairness and due process shall apply to all aspects of the Board's proceedings. Any person interviewed can suggest the names of others who may have information relevant to the inquiry. The Board shall not be bound by any individual's suggestion, if it deems it irrelevant based on the analysis of previously collected information. Where the Board decides not to interview any person who has been suggested by another, it shall make an explicit statement to that effect in the "Deliberations" part of the report and give the reasons for its decision.

31. If necessary, persons who have previously provided information to an investigation may be questioned again by the Board to clarify any ambiguities in their statements and to indicate to what extent, if any, they have knowledge of relevant facts not previously mentioned in their statements.

32. If an individual, including non-United Nations personnel, provides information to the Board but refuses to make or sign a statement, the Board shall record that fact.

33. Individuals shall be interviewed in the language they naturally use, resorting to interpretation when necessary. In such cases, the "Undertaking of Confidentiality" shall be administered to the interpreter in accordance with the format attached herewith as Annex D.

34. Individuals providing information to the Board shall be questioned by the Board without the presence of other persons.

35. The Board shall question a minor in the presence of a parent, guardian or, if neither are available, an adult of the minor's choosing. Where possible, there should be present an appropriate officer from the United Nations system with experience dealing with children, ideally, a Child Protection Officer.

36. When United Nations personnel are called to provide information to the Board, the attestation at the beginning of the standard form statement (Annex E) shall be read to him/her in the language that the personnel naturally use. Following that, the individual shall sign the form and date it before proceeding to answer any questions. A thumb impression may be used in lieu of a signature.

37. All individuals interviewed by the Board shall be informed of the subject matter of the inquiry and the reasons why he or she has been called for an interview. The Board shall then ask the person to state any information he/she is aware of regarding the occurrence. Following that, the Board members may ask questions. Additional practical advice on interviews is contained in the Guidelines for Board members on the Conduct of Inquiries. (Annex F)

38. While the interview progresses, a record shall be taken of the information provided by the individual in the form of a statement. Translation into a working language of the United Nations shall be provided, if necessary.

39. Following the interview, the individual shall be familiarized with the transcript and asked if he/she wishes to amend anything. Once he/she is satisfied with the statement, he/she shall be asked to sign and date the statement. A thumb impression may be used in lieu of a signature. In the case of a third party providing information, the reference to administrative and/or disciplinary action shall be removed from the attestation text. The Board Chairperson shall also sign the statement.

I. Deliberations

40. The Board shall consider carefully all information and findings of fact it has collected.

41. Board Members shall consider which of the facts it has established, single or in combination with others, triggered the unfolding of events, resulting in the occurrence. No assumptions shall be made. At the same time, reasonable inference is admissible and shall be practiced.

42. While formulating their recommendations, Board Members shall focus them at the cause(s) of the occurrence in question. Board members shall be prohibited from making recommendations regarding compensation, disciplinary action or legal liability.

J. Timelines

43. The process to initiate and convene a Board of Inquiry shall be in accordance with the provisions of paragraph 10 and 11 above within two weeks of the results of the investigation of the incident being presented to the Under-Secretary-General for Safety and Security. All efforts shall be made to finalize the Board's report within the timelines stipulated in the Convening Order, preferably within six weeks.[6]

44. In the event that the Board cannot submit the report within the specified timeline, the Chairperson of the Board shall submit a written request for an extension to the

[6]Annex C provides a format outline for a Board report.

Under-Secretary-General for Safety and Security, stating the reason for not meeting the timeline.

K. Dissemination of a Board's Report

45. Board reports are to be treated as confidential documents. Access to a Board report and its annexes shall be provided in their entirety to the Executive Head of the affected UNSMS organization. Access to a Board report and its annexes shall be provided in their entirety or in part on a need-to-know basis to other officials of UNSMS organizations that require them for their deliberations. Special consideration shall be given to the protection of interests of individuals who provided information to the Board.

46. A copy of the Board report with all annexes shall be retained by the Department of Safety and Security for three calendar years, following which it shall be archived.

47. All Board reports that have implications in relation to issues of alleged misconduct or breach of discipline by United Nations personnel shall be forwarded to the appropriate office of the UNSMS organization concerned for review and follow-up.

48. Board reports shall, in principle, not be made available to parties other than the membership of the UNSMS. However, the Under-Secretary-General for Safety and Security shall, in consultation with the concerned organizations, have the discretion to make reports available to Member States, particularly in cases that involve the personnel of that country. Such reports may be redacted as appropriate.

49. When a Board report is shared with a Member State, it shall be accompanied by a *Note Verbale* that includes the following sentence: "This report is an internal document of the United Nations and is being made available for official use only; it is not to be made public in any form, either in whole or in part."

50. Board reports shall not be shared with other third party entities (e.g., families of victims). Upon request, and in consultation with the concerned organization(s), a summary factual account of the occurrence based on a Board report may be shared with such entities. Such factual accounts shall not contain any extraneous details, analysis, conclusions or recommendations usually found in a Board report. Requests of this nature must be approved in writing by the Under-Secretary-General for Safety and Security.

51. In deciding whether to make a report or a factual account of the occurrence available to an non-UNSMS entity, the Under-Secretary-General for Safety and Security shall seek the advice of the Office of Legal Affairs and, where relevant, other offices, on a case-by-case basis, especially in cases that might impact the privileges and immunities of the organizations and/or cases where issues of confidentiality arise.

L. Follow-Up Action and Lessons Learned

52. The United Nations Department of Safety and Security will collate all agreed-upon recommendations contained within the Board's report to address SRM-related operational, management and/or policy gaps or deficiencies. It is the responsibility of each UNSMS organization to implement agreed-upon recommendations applicable to them.

53. The United Nations Department of Safety and Security will also collect and analyse lessons learned and present to the Inter-Agency Security Management Network recommendations for reviewing UNSMS policies, procedures and measures based on this analysis.

M. Final Provisions

54. This policy is to be made available to all United Nations personnel.

55. This policy enters into effect on 08 November 2012.

Annex A

Board of Inquiry
Convening Order

Date: _____

To: [distribution]

From: [Under-Secretary-General for Safety and Security]
[Executive Head of Organization #1]
[Executive Head of Organization #2]

Subject: Board of Inquiry for [incident]

1. In accordance with United Nations *Security Policy Manual* (SPM), Chapter V, Section G, a Board of Inquiry is hereby convened to consider and prepare a report on the [brief description of occurrence] which took place on the [date] at [time] hours at [place].

2. The Terms of Reference of this Board are attached.

3. An initial legal briefing shall be provided to the Board on its responsibilities immediately prior to commencement of its deliberations. Copies of the investigation report and other relevant documentation will be forwarded to the Board members prior to the initial briefing. Attendance at the initial briefing and any subsequent briefings/meetings is mandatory.

4. Composition:

Name Title
Chairperson
Member
Member
Member

5. The Chairperson shall submit the final report, reviewed and finalized by [date].

Distribution:
Chairperson, Members of the Board
Legal Officer
Board Support Officer

Annex B

Terms of Reference of Board of Inquiry for [brief description of occurrence] which took place on the [date] at [time] hours at [place]

[Attention: the following Terms of Reference is generic and represents the most typical issues confronted by a Board of Inquiry. The Board Support Officer, in consultation with the appropriate Legal Advisers, shall prepare incident-specific Terms of Reference depending on the circumstances of each incident.]

The mandate of the Board of Inquiry shall be as follows:

(a) Obtain all investigation reports and other relevant source materials regarding the occurrence, including, *inter alia*: Security Incident Report(s), Military Police Report(s), technical assessments (including threat assessments and security risk assessments of the Security Risk Management process), witness statements, expert opinions, medical reports and evaluations and any other documents required by the Board to conduct its deliberations;

(b) Collect any relevant additional statements from any individual involved or affected by the incident, and conduct any necessary additional site visits, interviews, or further inquiries;

(c) Seek explanations or clarifications of technical or specialized reports a technical or specialized nature from experts or specialists, should it be deemed necessary by the Board to enable it to address all relevant issues;

(d) Establish facts from the whole body of available information presented and review the circumstances of the occurrence in a comprehensive manner;

(e) Within the deadline specified in the convening order, present a written report to the Under-Secretary-General for Safety and Security, setting forth in a clear, logical, concise and objective manner the Board's findings, conclusions and recommendations.

The Board shall establish the following facts:

(a) Date, time and place of occurrence;

(b) Factual and comprehensive account of the occurrence and the events leading thereto;

(c) Identification of United Nations and non-United Nations investigators, if applicable. Full names of all individuals involved in the occurrence, their nationalities, statuses and United Nations ID/index numbers;

(d) When, how and by whom were the United Nations Security Management System structures informed of the occurrence;

(e) What standing procedures, if any, were implemented following the notification of the occurrence? When, and by whom;

(f) When, how and by whom was the search and rescue operation/MEDEVAC carried out (if relevant);

(g) By whom and for how long was the occurrence site preserved;

(h) Who maintained custody of the chain of evidence during investigation(s);

(i) Have the remains of all of the victims been identified? How were the remains identified (if relevant);

(j) Whether or not any court action (prosecution or lawsuit) has been initiated;

(k) Residual security risk, SRM and Minimum Operating Security Standards (MOSS) in force at the time and place of the occurrence;

(l) Were the affected United Nations personnel briefed about security threats in the area;

(m) What precautionary measures, if any, and by whom have been put in place to anticipate the occurrence or mitigate its effects;

(n) The roles of each of the United Nations personnel involved in the incident;

(o) Identification (to the extent possible) of attackers.

The Board shall provide its judgment on the following:

(a) What caused the occurrence?

(b) Were relevant United Nations Security Management System SRM procedures, rules and regulations adequate? Were they followed properly?

(c) Did the occurrence take place as a result of the acts or omissions of any individual(s)?

(d) Did the death or injury occur in the course of a performance of official duties on behalf of their organization, or was the death or injury otherwise connected to the performance of such official duties?

The Board shall, based upon its conclusions, provide its recommendations concerning any actions, steps or measures that it considers should be taken by United Nations Security Management System organizations to properly manage security risks from potential future incidents and avoid future casualties in such incidents (e.g., compliance with previous Board recommendations and/or lessons-learned exercises, additional security precautions or administrative actions such as amending policies, rules, instructions or procedures, etc.).

For ease of reference the following outline format of a Board report is provided:

A. CONSTITUTION
B. DESCRIPTION OF OCCURRENCE
C. FINDINGS OF FACT
D. DELIBERATIONS
E. RECOMMENDATIONS
F. OBSERVATIONS
G. SIGNATURES
H. ANNEXES

Annex C

Format of Board of Inquiry Report

The Board shall prepare a report in the following format:

A. Constitution shall cite the convening order, its date, the period during which the Board conducted its proceedings, as well as the venue thereof;

B. Description of occurrence shall contain a factual description of the occurrence under review. It shall not include any extraneous information, analysis, conclusions and/or recommendations;

C. Findings of Fact shall respond to all issues cited in the Terms of Reference;

D. Deliberations shall contain an account of how the findings of fact related to the occurrence were assessed by the Board and shall specify the reasons relied upon by the Board in reaching the conclusions and recommendations in the case;

E. Conclusions shall generally follow the issues cited in the Terms of Reference. At a minimum, the Board shall be expected to reach a conclusion on the following:

(a) Cause(s) of the occurrence;

(b) Whether the occurrence took place as a result of acts or omissions of any individual(s) or non-compliance with existing UNSMS policies[7];

(c) Whether the death or injury occurred in the course of performance of official duties on behalf of an organization or was otherwise connected to the performance of such official duties.

F. Recommendations shall be specific and feasible with the focus on possible policy and operational measures with the aim to address the cause(s) of the occurrence and improve management accountability. Board members are prohibited from making recommendations regarding compensation, disciplinary action or legal liability.

G. Observations shall be an optional section of the report, reserved for additional matters not covered by the Terms of Reference, but believed by Board members to be significant and relevant to the subject matter of the inquiry.

H. Signatures shall be affixed by Board members only upon the review of the draft report by the Legal Adviser. A dissenting member shall not be obliged to put his/her signature on the report, but shall explain the abstention in a separate document addressed to the Under-Secretary-General for Safety and Security, which shall become an integral part of the case file.

[7] As contained in the *Security Policy Manual*

I. Annexes shall contain documents relevant to the subject matter of the inquiry, which have been considered by Board members in the course of the proceedings.

Annex D

UNDERTAKING OF CONFIDENTIALITY

I, the undersigned, undertake that, in the performance of my duties as a Chairperson /Member/Secretary (underline as appropriate) of [name] United Nations Security Management System Board of Inquiry, shall exercise the utmost discretion in all matters relating to the Board proceedings, and I shall not, at any time, use for private advantage or communicate any information relating to the Board proceedings to any person or institution, within or outside the United Nations, without the authorization of the Under-Secretary-General for Safety and Security.

I undertake that all evidence, files, statements, maps, drawings, photographs, discs, plans, reports, recommendations, estimates, documents and any other data or information compiled or received by me as a result of my association with the Board of Inquiry shall be treated as confidential, shall be delivered only to the Board Support Officer and shall not be retained by me in any form. I shall ensure that I have returned all documents and other information and materials to the Board Support Office after completion and submission of the Board of Inquiry Report.

Print name: _____

Signature: _____

Date: _____

Annex E

Statement to United Nations Security Management System Board of Inquiry [Reference No. _____]

The Statement of: _____
Name of Individual

Index No. (If UN personnel): _____

Position of UN personnel: _____

Address and Occupation _____
(If non-UNSMS individual) _____
_____

I do solemnly, sincerely, and truly declare and affirm that the information I give to this Board of Inquiry shall be the truth, the whole truth and nothing but the truth.

Signed: _____

Date: _____

1.
2.
Etc.

Attestation of Individual Providing Information
I have reviewed my above statement. I have been told that I may amend it or add anything I wish. The statement is true. I make it of my own free will, knowing that if I have wilfully stated in it anything that I know to be false, or do not believe to be true, I may be liable to administrative and/or disciplinary action.

_____ _____
Signature of Individual Date

_____ _____
Signature of Chairperson Date

Annex F

Guidelines for Board Members on the Conduct of Inquiries[8]

A. General

1. When the United Nations Security Management System Board of Inquiry (herein "the Board") is convened by the Under-Secretary-General for Safety and Security and the Executive Head(s) of the United Nations Security Management System organizations involved in the incident, it will receive, along with a Convening Order, its Terms of Reference, together with the report of the preliminary investigation and other document files assembled by the Board Support Officer. The Board will also receive initial briefings by the Board Support Officer and the United Nations Office of Legal Affairs.

2. When the Board members have been able to peruse the documents, they shall meet and determine the internal procedure by which they will operate, in particular deciding which persons shall be called for interviews. Minutes of the meetings shall be kept throughout the proceedings and should include a record of times, names and places relevant to the occurrence in question.

B. Interviews

3. Before starting interviews, the Board, at its preliminary meeting, should decide what issues on the Terms of Reference it will need to address with particular persons. While it will be, from time to time, inevitable that a person is called back more than once, the process of re-interviewing individuals should be avoided as much as possible.

4. The Board members should decide, in advance of each interview, the member who will lead it. At the beginning of the interview, this person should explain the mandate of the Board to the interviewee, introduce the Board members and request the Secretary to administer the attestation. After the interviewee has signed it, he/she should be requested to state, initially, what he/she knew about the occurrence in question. The interviewers should be careful not to ask "leading questions" (i.e., questions which suggest an answer). For instance, "Tell us what happened from your perspective in this incident" is usually much better than: "Is it right that there were three attackers?" In other words, the information should be the interviewee's and not the Board's.

5. When the interviewee has finished with the narration and the leading interviewer has completed her/his initial questioning, he/she will request other Members to ask questions, as they think appropriate. Finally, the interviewee shall be asked

[8]This Annex is directly based on United Nations Department of Peacekeeping Operations and Department of Field Support "Standard Operating Procedure – Boards of Inquiry", Annex III.

whether he/she wishes the Board to hear the information of any other particular persons or review any other lines of inquiry.

6. The above may seem simple, but it is not. The art of questioning is not easily acquired. While leading questions should not be asked initially, this does not mean that the Board should accept vague and unhelpful answers. The Board should obtain clear answers as much as possible. However, there is a fine line that must be drawn between pressing an interviewee for a clear answer and harassing him/her. Clearly, the latter is unacceptable.

C. Information

7. The Board should acquire the best information. It should note that original documents are better than copies, if they are available. Documents should always be identified by numbers and referred to in statements. Care and accuracy should be applied at all times.

8. Similarly, it is always preferable to hear what Mr. B actually says, rather than hear Mr. A's account of what Mr. B has supposedly said. This is always the case when it comes to deciding the truth of what actually happened, although there may be occasions when hearing what an individual has said before might be important to test that individual's consistency. Inconsistency sometimes indicates unreliable information.

D. Deliberations

9. The Board should arrive at conclusions based on information that it has considered carefully and found credible. No assumptions should be made. If the facts are simply not there, the Board must say so. At the same time, reasonable inference is admissible and should be practiced.

10. In determining the cause(s) of an occurrence, Board members should consider which of the facts it has established, single or in combination with others, triggered the unfolding of events, resulting in the occurrence. Conversely, a cause can be a deficiency that, if corrected, eliminated or avoided, could have prevented the occurrence. A cause may be an act, an omission, a condition or a circumstance and it either starts or sustains the accident sequence. A cause may be an element of human or mechanical performance. An environmental condition may be a cause if it was not foreseeable or avoidable.

11. One of the conclusions Boards are usually expected to make is whether or not the death or injury of a United Nations personnel occurred in the course of performance of official duties on behalf of their organization, or was the death or injury otherwise connected to the performance of such official duties? Unfortunately, organizations do not have a clear, unambiguous and precise definition of "official duty". For the purpose of Board proceedings, the following should be kept in mind. Absent information to the contrary, it is generally assumed that the official duty of United Nations personnel is usually limited by

official working hours. Traveling to or from work (but not deviations from the usual route for shopping, restaurants, clubs, etc.) would clearly be in connection with official duty. However, the real issue facing a Board is to make a sensible judgment on whether the occurrence is "in connection with official duty". The Board should arrive at a conclusion in this regard on the basis of assessment of the specific circumstances of the occurrence. Very often the issue facing a Board is to make a sensible judgment on whether the involvement of the person in occurrence was "service related". Board members will need to examine the specific circumstances of the occurrence to determine this. "Non-service related" activities would be ones where the participants were at liberty to decline participating therein.

E. Writing a Report

12. The report of a Board should be based on evidence derived from the Investigation Report, as well as facts obtained by the Board throughout its proceedings. It should cover all points of the Board's Terms of Reference.

13. The section "Constitution" should cite the convening order, its date, the period during which the Board conducted its proceedings, as well as the venue thereof.

14. Under the title "Description of Occurrence" the Board should provide a purely factual description of the occurrence under review. It should not include any extraneous information, analysis, conclusions and/or recommendations.

15. In the section "Finding of Fact" the Board should respond to all issues cited in the Terms of Reference. The objective of this paragraph is to present a clear statement of all relevant facts. The Board can choose to present them in either chronological order, starting with what is considered to be the first significant event, or follow the order of questions in the Terms of Reference. The most important factor is that all issues are fully addressed. The Board should avoid expressing its opinions and conclusions on the cause(s) of the occurrence in this section unless they form an essential part of the description of the accident. Adjectives "adequate", "appropriate", "inadequate", etc. should be saved for the section "Conclusions".

16. The following section, "Deliberations" is a "bridge" between the "Findings of Fact" and the two following sections. In this section, the Board should analyse all findings of fact and explain how it arrived at conclusions on the causes of the occurrences and the recommendations it wishes to make to avoid any repetition of the event, cited in the preceding section. The Board should describe each aspect that was considered and explain its significance. The reasoning of the Board should be based on its members' best judgment or expert opinion and should be explained in detail, as well as be supported by references to interview statements, documents or other exhibits. If there is conflicting information, the Board should state why it is not prepared to accept the information that it does not use. While determining whether personnel involved in an occurrence were performing official duties on behalf of their organization or the occurrence was otherwise

connected to the performance of such official duties, the Board should specify the facts and explain the reasons relied upon in reaching such a conclusion. In cases where the Board is of the opinion that rules and regulations were violated, the report should be specific as to what rule was violated and in what respect. If the Board concludes that the occurrence was caused by internal malfunctioning of the Organization, it should clarify where the procedures were inadequate and in what respect.

17. The "Conclusions" section of the report should generally follow the issues cited in the Terms of Reference. However, should the Board arrive at conclusions other than those requested in the Terms of Reference, they could also be included in the report.

18. "Recommendations" should be specific, feasible and directed at the elimination of the cause(s) of the occurrence in question. An important aspect to bear in mind is that Board Members are prohibited from recommending administrative or disciplinary action. Likewise, the recommendations regarding compensation or legal liability should never be made by the Board. These are matters outside the purview of a Board and should be addressed by the individual's organization.

19. "Observations": This is an optional section of the report. If, during the course of its deliberations, the Board's attention is drawn to additional matters of significance, not covered by the Terms of Reference but relevant to the subject matter of the inquiry, the Board can point them out in this section of the report.

20. "Signatures": Board members should initial the draft before submitting it for review by the Board Support Officer and the appropriate Legal Advisers. Once the report is finalized with due regard to the Board Support Officer's and the appropriate Legal Adviser's comments and recommendations, the Board members should sign it with their full signatures. A dissenting member is not obliged to put his/her signature on the report, but should explain the abstention in a separate document addressed to the Convening Authorities, which becomes an integral part of the case file.

21. "Annexes" The following documents should typically be annexed to a Board report:

    I. Convening order and Terms of Reference;

    II. Investigation report with original attachments, including photos;

    III. List of persons present or involved in the occurrence, giving names, United Nations ID/index numbers, positions (if civilian); addresses and occupations (if non-United Nations);

    IV. Statements and attestations by those providing information;

    V. Maps or sketches of the scene of the occurrence;

VI. Medical reports and technical inspection reports;

VII. Claims, local police reports, pending proceedings or actual decisions of local courts;

VIII. Detailed descriptions of property destroyed or damaged, with attachments of available damage/discrepancy reports; and

IX. Any additional relevant documents, statements, photos, etc.

F. Finalizing the Report

22. Members of the Board remain the sole authors of their report. As such, they are under no obligation to follow the recommendations of Legal Advisers made after reviewing the draft report. However, they should realize that the Under-Secretary-General for Safety and Security's position on the report will be greatly influenced by the opinions of Legal Advisers communicated in a memorandum attached to the report. Thus, the recommendations of Legal Advisers should be treated with the utmost respect and attention.

G. After the Inquiry

23. Board Members should consider whatever information they became privy to during the Board proceedings as strictly confidential, and should not share it with any other individual(s), other than those directly involved with the Board.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter VI

ADMINISTRATIVE AND LOGISTIC SUPPORT

SECTION A

Remuneration of United Nations System Staff and Eligible Family Members on Relocation/Evacuation Status

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 8 April 2011
Technical Review: 1 May 2017

REMUNERATION OF UNITED NATIONS SYSTEM STAFF AND ELIGIBLE FAMILY MEMBERS ON RELOCATION/EVACUATION[1] STATUS

Note: The following provisions are designed to assist organizations in the administration of Evacuation Allowances. These provisions are not an exhaustive listing; clearly, a certain degree of judgment and flexibility will be required to deal with the various situations that might arise. These should be handled on the basis of consultation among organizations.

Alternate Work Modality

1. Administrative measures related to Alternate Work Modalities (AWM)[2] that involve temporarily closing offices or the work status of a staff member will be implemented by each organization in line with its rules and regulations. The measures include, but are not limited to, working from home or an alternate work place within the duty station and Special Leave with Pay. If staff members and their eligible family members are instructed to move into a hotel within the duty station for security reasons, Daily Subsistence Allowance (DSA) at the rate applicable at the duty station (or an ad hoc DSA rate recommended by the Security Management Team and approved by the headquarters of the lead agency) will be payable in respect to the staff member and half of that amount for each eligible family member for up to 30 days.

Relocation

2. In case of relocation, the applicable DSA rate (or an ad hoc DSA rate recommended by the Security Management Team and approved by the headquarters of the lead agency) is payable in respect to the staff member and half of that amount for each eligible family member for up to 30 days.

Additional measures for locally recruited staff

3. In case of relocation of locally-recruited staff, irrespective of the DSA payment mentioned above, the Designated Official (DO) may recommend to the Security Management Team (SMT) that a decision be taken by representatives of organizations participating in the United Nations Security Management System (UNSMS) to provide an advance[3] of three months' salary to be paid to locally recruited staff members and, if necessary, transportation costs for themselves and their eligible family members. In the most exceptional cases where locally recruited personnel and/or their eligible family members are evacuated, Security Evacuation Allowance will be payable as per the provisions below.

---

1 Relocation is within the country of duty station; evacuation is outside. Security Evacuation Allowance is payable for evacuation. In relocation cases, DSA applies.

2 UNSMS *Security Policy Manual*, Chapter IV, Section D "Relocation, Evacuation and Alternate Work Modalities – Measures to Avoid Risk", paragraph 7.

3 This is an advance and not an additional salary of three months.

Security Evacuation Allowance

4. SEA is payable for eligible internationally recruited staff members and their eligible family members.[4]

a. In respect to the staff member:

- US $200 per day during the first 30 days and US $150 per day from the 31st day until the staff member returns to the duty station, or until the staff member is reassigned to another location, or until six months have elapsed following evacuation, whichever is soonest.

b. In respect to each eligible family member residing at the duty station:

- US $100 for the spouse and each dependant child during the first 30 days and US $75 per day from the 31st day until the staff member returns to the duty station, or is reassigned to another location, or until six months have elapsed following evacuation, whichever is soonest.

c. If the staff member is authorized to return to the duty station and some or all eligible family members are not authorized to return or unable to return due to specific 'Family Restrictions' that may be in force for security purposes, or if the staff member is sent on mission (and receives relevant DSA), the first eligible family member will be entitled to the higher rate of evacuation allowance (US $200 or US $150 as applicable).

5. Additionally, for the purpose of facilitating a small shipment of personal effects (and incidentals including terminal expenses); a lump sum of US $500 will be provided at the time of evacuation to eligible staff members who were installed at the duty station. This is a one-time payment for the staff member and all of his/her eligible family members even if they are evacuated at different times.

6. Loss and damage to personal effects that remain at the duty station will be compensated in accordance with established administrative guidelines. Staff members should be reminded of their responsibility to submit to the officer in charge who has been designated to manage organization-specific matters, a list of their valued and itemized personal effects, which will be used by the respective compensation committees of the organization to determine compensation in the event of loss or damage to personal effects.

Provisions applicable in respect to eligible internationally recruited staff members

7. Internationally recruited staff members eligible for both security evacuation allowance and security evacuation travel are those who travelled and were installed at the duty station at the organization's expense, as well as those who were internationally recruited at the duty station.

8. If the staff member is evacuated to the destination authorized by the Under-Secretary General for Safety and Security (USG DSS), the security evacuation allowance will be paid at the rates specified in paragraph 4(a) above.

[4] Rates agreed as per CEB/2009HLCM/HR/46/Rev.1.

9. If the staff member is outside the duty station at the time of evacuation, he/she will normally be entitled to the security evacuation allowance only as of the expected date of return to the duty station (*i.e.* upon expiration of any period of authorized home leave, annual leave, sick leave, or official mission).

10. If the staff member does not join his/her eligible family members immediately following evacuation (*e.g.* is sent on mission), he/she will be entitled to the security evacuation allowance only on the date of his/her actual arrival at the place of home leave or any other location.

Travel to the country of home leave or country of the staff member's choice

11. The cost of travel due to security evacuations will be based on the destination authorized by the USG, UNDSS. The staff member may choose to travel to a) the destination authorized by the USG, UNDSS, b) the country of home leave or c) the country of his or her choice. If the staff member and/or eligible family members choose to travel to the country of home leave or to the country of his or her choice instead of the authorized destination, the travel may be reimbursed up to cost of the authorized destination or it may be processed under the home leave entitlement. During the period of evacuation status in the home country, security evacuation allowance will be paid in respect to the staff member and each eligible family member at the rates specified in paragraph 4 above.

12. When security evacuation is authorized to the country of home leave and where a staff member and/or eligible family members cannot return to the home country due to 'Personnel Restrictions'[5] for security purposes or for political reasons, evacuation to a country of the staff member's choice may be authorized. When the reason for requesting travel to a country of the staff member's choice is solely for the personal convenience of the staff member, travel expenses to be borne by the Organization will not exceed the costs that would have been payable to the home country.

Provisions applicable in respect to eligible family members

13. For the purpose of determining eligibility for payment of security evacuation allowances and travel entitlements, eligible family members shall be those recognized family members of an internationally recruited staff member who travelled and were installed at the duty station at the Organization's expense and/or reside at the duty station with the staff member:

(a) **If the eligible family members are evacuated to the destination authorized by the USG, UNDSS,** security evacuation allowance will be paid at the rates specified in paragraph 4 (b) above;

(b) **If the eligible family members are evacuated to the destination authorized by the USG, UNDSS, but not the staff member,** the first eligible family member will be paid at the higher rate of security evacuation allowance;

(c) **If the staff member is authorized to return to the duty station and some or all eligible family members are unable to return due to specific 'Family**

[5] UNSMS Security Policy Manual, Chapter IV, Section D "Relocation, Evacuation and Alternate Work Modalities – Measures to Avoid Risk", paragraph 14.

Restrictions' that may be in force for security purposes, the first eligible family member who remains outside the duty station will be paid at the higher rate of security evacuation allowance;

(d) **If the staff member is sent on a mission** (and receives the relevant DSA), then the first eligible family member is paid at the higher rate of security evacuation allowance;

(e) **If the eligible family members are outside the duty station at the time of evacuation**, the allowance will be payable:

(i) effective the date they are joined by the staff member in the country of evacuation; or

(ii) on the expected date of return to the duty station, (when the staff member remains at the duty station);

(f) **In the case of a dependant child studying at a location (other than the staff member's official duty station) when 'Family Restrictions' for security purposes have been declared**, travel at the Organization's expense will normally be authorized on the basis of education grant or home leave travel. Security evacuation allowance will not be payable in this instance;

(g) **In the case of a dependant child on a visit at the staff member's duty station when 'Family Restrictions' for security purposes have been declared**, the travel at the Organization's expense will be authorized under the education grant and/or home leave travel. Security evacuation allowance will not be payable;

(h) **In the case of a dependant child studying at the staff member's duty station when 'Family Restrictions' for security purposes have been declared**, the following shall apply: when the child needs to attend a second school due to the declaration of 'Family Restrictions' for security purposes, additional education grant for attending the second school may be authorized for the same period, provided that the staff member can demonstrate that s/he has made every reasonable effort to obtain reimbursement of advance school fees from the school at the duty station from which the child was evacuated/relocated. Under these circumstances, security evacuation/relocation allowance is applicable but the lump sum for board element of the education grant will not be payable;

(i) Security evacuation allowances shall be paid for a maximum period of six months. In the event that evacuation remains in place beyond six months, the security evacuation allowance in respect to family members will cease to be paid as from the seventh month. Applicability of Extended Monthly Security Evacuation Allowance EMSEA) depends on the staff member's assigned date to the duty station in light of the decision by the GA Resolution 65/248.[6]

Emoluments applicable during evacuation

14. When evacuation has officially been declared by the USG, UNDSS for a duty station, he or she has the authority to order the relocation/evacuation of internationally recruited staff and their eligible family members to an authorized destination. If the cost of travel to the

[6] Extended Monthly Security Evacuation Allowance (EMSEA) will gradually phase out as per the GA Resolution 65/248. See also A/65/30 *Report of the International Civil Service Commission for the year 2010*, paragraph 243.

home country from the duty station is lower than that to the destination authorized by the USG, UNDSS, direct travel to the home country may be authorized whenever logistically possible.

15. During the period of evacuation to the destination authorized by the USG, UNDSS, staff members will continue to be paid their net base salary plus post adjustment, mobility hardship allowance applicable at the official duty station,[7] and the rental subsidy of the official duty station plus the security evacuation allowance (in respect to the staff member and each eligible family member).

16. If staff members and/or their eligible family members are not authorized to return to the duty station within 30 days following the evacuation, each respective organization will decide with regard to:

a. reassignment, temporary or otherwise, of the staff member together, as applicable, with his/her eligible family members;

b. travel to the home country.

Reimbursement of Rental Payment and Rental Deposit/Advance

17. Reimbursement of rental fee and/or rental deposit may be considered by the Organization in respect to evacuated staff who will not return to the duty station, if a well-documented request includes copies of the lease (which should normally contain the standard diplomatic clause) and correspondence between the staff member and the landlord showing that the staff member took the necessary action to terminate the lease and obtain reimbursement.

Extended Monthly Security Evacuation Allowance (EMSEA) [8]

18. An Extended Monthly Security Evacuation Allowance (EMSEA) shall be payable in respect to eligible family members of staff members of organizations that apply EMSEA after completion of the six month period mentioned in paragraph 13(i) above in the following cases:

(a) If the staff member is authorized to return to the duty station and some or all eligible family members are unable to return due to specific 'Family Restrictions' that may be in force for security purposes;

(b) If some or all eligible family members of a newly recruited staff member are unable to travel to the duty station due to specific "Family Restrictions" that may be in force for security purposes (in this case, the EMSEA will be payable from the first day on duty);

[7] The "official duty station" may be the Administrative Place of Assignment (APA) for staff members in Special Operations Area.

[8] Extended Monthly Security Evacuation Allowance (EMSEA) will gradually phase out as per the GA Resolution 65/248. See also A/65/30 *Report of the International Civil Service Commission for the year 2010*, paragraph 243.

(c) In cases where staff members have been reassigned to another duty station and some or all eligible family members are unable to travel to the duty station due to specific 'Family Restrictions' that may be in force for security purposes;

(d) When both the staff member and his/her eligible family members have been on evacuation status for more than six months, and no other arrangements have been made to place the staff member.

19. The amount of EMSEA is determined by applying the rental threshold percentage of the salary (net salary plus post adjustment) of a single staff member at the P-4 step VI level. The post adjustment and relevant threshold percentage used shall be that of the duty station where the family is located. In no case shall the amount be higher than that applicable in the staff member's country of home leave or for evacuated staff members of the previous duty station if the latter is maintained as actual family residence. The amount shall be set at one of two levels as follows:

(a) When paid on behalf of the spouse (who, for the purposes of EMSEA does not have to be a dependant), the EMSEA will be the rental subsidy threshold amount at the single rate of the actual residence of the spouse, as defined above;

(b) When paid on behalf of a spouse plus one or more dependant children, the amount in a) above is increased by 30% regardless of the number of dependants. Dependant children in respect to whom an education grant is paid are not taken into account for the determination of EMSEA payments.

20. In the application of the EMSEA, no additional travel entitlements shall be payable. However, regular travel entitlements (such as home leave, family, visit travel, education grant travel), remain payable. Furthermore, there is no obligation for the organization to provide any additional financial, administrative or legal assistance towards those family members.

21. The EMSEA shall not apply to staff members on mission service, i.e., those in receipt of base salary, post adjustment and other elements of remuneration of the duty station of origin, plus DSA or MSA of the mission area.

United Nations Volunteers (UNVs)

22. In the event of 'Personnel Restrictions' for security purposes, arrangements for UNVs are administered by UNDP or the United Nations.

Consultants

23. Provisions for evacuation for internationally recruited consultants will be incorporated into the initial contractual arrangements. Options for local or international consultants while 'Personnel Restrictions' for security purposes are in force are listed below.

a. Should there be 'Personnel Restrictions' for security purposes in an area where a consultant is operating, the consultancy contract will not be terminated if it is determined that the services to be provided by the consultant can be accomplished outside of the duty station location. The consultant's travel costs will be covered up to the location from where recruitment took place or any other location

mutually agreed from where the services can be provided as per the original terms.

b. Should there be 'Personnel Restrictions' for security purposes in an area where a consultant is operating, the consultancy contract will be terminated in accordance with the contractual termination clause if it is determined that the services to be provided by the consultant cannot be accomplished outside of the duty station location.

c. If circumstances permit, the consultant agrees and sound operational reasons exist, the consultancy contract may be suspended. The consultant's travel costs will then be covered up to the location from where recruitment took place. Once the 'Personnel Restrictions' for security purposes are lifted, the return of the consultant will be authorized and the related travel costs will be covered. The contract will be reactivated under the original terms and arrangements.

24. In situations where it is expected that 'Personnel Restrictions' for security purposes will be of a maximum duration of seven days, the consultant may be evacuated/relocated to the destination authorized by the USG, UNDSS. The applicable DSA in case of relocation or travel costs and security evacuation allowance in case of evacuation will be covered up to seven days (at the rate applicable to staff members) by the relevant organization. If the lifting of the 'Personnel Restrictions' for security purposes does not take place within the seven days period, options 23 a, b or c above apply.

Focal points on Administrative and Staff Welfare Issues

25. For administrative questions staff members should contact their respective agency's human resources focal point, and for staff welfare issues, the staff welfare focal point.

Overview of Security Evacuation Allowances

Area of Evacuation	Applicable Security Evacuation Allowance rate/staff member alone	Eligible family members
Outside the duty station country (safe haven, home country, third country)	US$ 200 per day for up to 30 days; thereafter US$ 150 per day (from the second through the sixth month)	For family normally residing at the duty station: US$ 100 per day for up to 30 days. Thereafter US$ 75 per day.
Shipping Entitlements and terminal expenses	A single lump-sum payment of US$ 500 is made to the staff member when he/she, or his/her family, is evacuated (i.e., it is not necessary that the staff member himself/herself is actually evacuated). The amount is the same regardless of the number of dependants. Terminal expenses are included in the lump-sum payment	
Relocation within country of duty station	DSA of location applies.	50% of applicable DSA per each eligible family member.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM

Security Policy Manual

Chapter VI

ADMINISTRATIVE AND LOGISTICS SUPPORT FOR SECURITY OPERATIONS

SECTION G

Management of Stress and Critical Incidents Stress (MSCIS)

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 23 November 2015
Technical Review: 1 May 2017

Introduction

1. The primary goal of the United Nations Security Management System (UNSMS) is to enable the conduct of United Nations activities while ensuring the safety, security and well-being of personnel.[1] The conditions under which UNSMS personnel operate in the field have changed drastically over the years, particularly in light of the United Nations' shift to a "stay and deliver" approach to operating in high-risk environments. This has substantially increased the number of individuals exposed to stress and critical incident[2] stress. While many individuals who experience stress or critical incident stress are able to resume their daily activities with minimal or no disruption, some may encounter difficulty resuming such activities due to psychological, somatic or social reactions linked to such exposure.

2. This policy governs the coordination and provision of psycho-social services by Counsellors,[3] contracted or employed by UNSMS organizations, to those who are at risk of experiencing or experiencing stress or critical incident stress. The coordination and provision of such services shall be in accordance with the following principles:

   (a) The management of stress and critical incident stress shall be conducted in accordance with the principles of immediacy, proximity and availability of high-quality professional services, which are embodied in the Management of Critical Incident Stress Framework (MCISF) (see Annex A, "Management of Critical Incident Stress Framework (MCISF)").

   (b) The management of critical incident stress has three distinct phases:

      (i) Pre-incident Preparedness;

      (ii) Incident Response;

      (iii) Post-incident Recovery.

A. Applicability

3. This policy is applicable to all individuals covered under Chapter III of the UNSMS' *Security Policy Manual* (SPM) ("Applicability of the United Nations Security Management System").

B. Structure

4. The United Nations Department of Safety and Security's (UNDSS) Critical Incident Stress Management Unit (CISMU) shall serve as the central body responsible for ensuring the adequate and timely coordination and provision of psycho-social services. In coordinating the provision of such services, CISMU shall take into

[1] The UNSMS' Framework of Accountability, Section II, paragraph 5 states: "The goal of the UNSMS is to enable the conduct of United Nations activities while ensuring the safety, security and well-being of personnel and the security of United Nations premises and assets."

[2] For purposes of this policy, a "critical incident" is "any sudden event or situation that involves actual, threatened, witnessed or perceived death, serious injury, or threat to the physical or psychological integrity of an individual or group" (Source: Diagnostic Statistical Manual IV).

[3] For purposes of this policy, a "Counsellor" shall include Staff Counsellors, Stress Counsellors and Staff Welfare Officers appropriately trained and certified in the provision of psycho-social services and contracted or employed by a UNSMS organization to provide such services.

account the respective capacity of each UNSMS organization to coordinate and provide such services to their respective personnel.

5. Such services shall be provided primarily at the field level through the establishment of a Critical Incident Stress Intervention Cell (CISIC), with coordination and support provided at the headquarter level, in accordance with the following structure:
   (a) Headquarter level
      (i) UNDSS/CISMU
         a. Chief of CISMU
         b. Regional Counsellors;

      (ii) Staff Counselling/Welfare Units or Sections of UNSMS organizations[4]
         a. Chiefs/Heads of Sections/Units[5]
         b. Staff Counsellors/Staff Welfare Officers[6];

      (iii) Psycho-social Crisis Coordination Centre (PCCC)
         a. The PCCC is a sub-group of the Crisis Coordination Centre (CCC) that is dedicated to coordinating the provision of psycho-social services to UNSMS personnel and their eligible family members in a crisis setting.[7] The Chief of CISMU shall determine when to activate the PCCC in a crisis setting. Upon activation, the PCCC shall operate twenty-four (24) hours per day and seven (7) days per week, whereby daily communication between relevant stakeholders listed under Section C ("Structure") shall be required;

      (iv) Critical Incident Stress Working Group (CISWG)[8];

   (b) Field level
      (i) Critical Incident Stress Management Cell (CISIC);
      (ii) UNDSS;
         a. CISMU-Field Counsellors;

[4] Excluding UNDSS, UNSMS organizations may maintain their own respective Staff Counselling/Welfare Units, at the headquarter level, under various titles.
[5] UNSMS organizations may employ their own respective Chiefs/Heads of their respective Staff Counselling/Welfare Units Counsellors, at the headquarter level, under various titles.
[6] UNSMS organizations employ their own Counsellors, at the headquarter level, dedicated to the provision of psycho-social services to their respective personnel, under various titles, including, but not limited to, "Staff Counsellor" or "Staff Welfare Officer".
[7] For the purposes of this policy, a crisis is any event that requires a United Nations system-wide coordinated response.
[8] The CISWG is a multi-disciplinary IASMN working group, chaired by the Chief of CISMU. CISWG members are nominated by their respective IASMN Security Focal Points (SFPs). Such members include Counsellors, Medical Officers, Human Resources Officers or Security Officers. The Office of the Ombudsman is represented as an Observer. The members meet throughout the year, either via Video Teleconference (VTC) or via formal meetings and reports on their progress to the IASMN. The CISWG draws upon lessons learned, promotes the identification of best practices and develops and promotes policies and guidelines to enhance the management of critical incident stress, with the aim of improving the psycho-social well-being of UNSMS personnel and their eligible family members.

(iii) Department of Peacekeeping Operations (DPKO) – Department of Field Support (DFS), Department of Political Affairs (DPA)

a. Staff Counsellors;

(iv) Staff Counselling/Welfare Units or Sections of UNSMS organizations[9]

a. Regional Staff Counsellors/Staff Counsellors/Staff Welfare Officers[10].

6. In order to ensure the adequate and timely provision of psycho-social services, coordination with the following partners may be required:
   (a) Emergency Preparedness and Support Team (EPST)[11];
   (b) United Nations Medical Emergency Response Team (UNMERT)[12];
   (c) Representatives of UNSMS organizations;
   (d) UNSMS security professionals
      (i) Inter-Agency Security Management Network (IASMN)
      (ii) UNDSS/Division of Regional Operations (DRO)
      (iii) UNDSS/Division of Headquarters Security and Safety Services (DHSSS)
      (iv) Designated Official (DO)/Security Management Team (SMT)
      (v) Chief Security Advisers (CSAs)/Security Advisers (SAs), Chief Security Officers (CSOs), Single-Agency Security Officers (S-ASOs) or Country Security Focal Points (CSFPs);
   (e) UNSMS network of Peer Helpers, Peer Support Volunteers and Family Focal Points ("PH/PSV/FFP")[13].

C. Roles and Responsibilities of CISMU

7. CISMU shall be responsible for the following:

   (a) Developing standardized methods and procedures for managing stress and critical incident stress, needs assessment and data gathering tools, recording and reporting templates for all relevant stakeholders listed under Section C ("Structure");

[9] Excluding UNDSS, UNSMS organizations may maintain their own respective Staff Counselling/Welfare Units, at the field level, under various titles.

[10] UNSMS organizations employ their own Counsellors, at the field level, dedicated to the provision of psycho-social services to their respective personnel, under various titles, including, but not limited to, "Regional Staff Counsellor," "Staff Counsellor" or "Staff Welfare Officer". Such Counsellors may also operate independently of the CISIC.

[11] Established in 2010, EPST coordinates and provides essential human resources support to United Nations personnel and their eligible family members during all phases of incidents related to malicious acts, natural disasters and other emergency incidents. It is housed under the Department of Management (DM)/Office of Human Resources Management (OHRM). More information is available at http://un-epst.org.

[12] Established in 2009, UNMERT is composed of over thirty (30) volunteer, emergency-trained medical professionals within the UN system who are ready to deploy globally at short notice to support mass casualty incidents (MCIs) affecting United Nations personnel. The UNMERT is managed by a Coordinator attached to MSD at UNHQ. It is deployed within the first twenty-four (24) to forty-eight (48) hours of MCI and works closely with United Nations medical and security personnel in the field to identify, triage and provide emergency medical treatment for United Nations personnel and their eligible family members immediately following a MCI and to facilitate medical evacuation.

[13] Integrated into the crisis management response structure to ensure managerial preparedness and enhance human resources crisis response during the aftermath of a MCI by providing comprehensive and compassionate support to survivors and surviving families of personnel.

(b) Developing mandatory certification and training courses for relevant UNSMS Counsellors, including guidance on how to establish a CISIC and maintain a functional network of PH/PSV/FFP;
(c) Developing mandatory joint training courses for relevant UNSMS Counsellors, human resources, medical and security professionals, focusing on joint planning and coordination in the field and ways to coordinate with the CISIC at the duty station;
(d) Developing mandatory training courses for UNSMS personnel[14] on managing stress and critical incident stress (e.g., preparation for deployment, emotional first-aid, burnout), including the development of "refresher" training courses;
(e) Developing mandatory certification and training courses for External Mental Health Professionals ("EMHP") and identifying EMHP in the field[15];
(f) Maintaining regular communication with relevant stakeholders listed under Section C ("Structure"), including the CISWG and IASMN.

D. The Management of Critical Incident Stress: Three Phases

Pre-incident Preparedness

8. CISMU shall be responsible for the following:

(a) Ensuring the capacity to respond to a critical incident through the establishment of a CISIC at a given duty station. In particular, CISMU shall (1) ensure the capacity to rapidly mobilize and deploy CISMU Regional or Field Counsellors, DPKO-DFS and/or DPA Staff Counsellors, PH/PSV/FFP and EMHP, in coordination with the CISWG as well as other relevant UNSMS Counsellors and UNSMS security professionals; and (2) immediately relay any request for psycho-social services to all relevant UNSMS organizations so that a consensus can be reached as to whether such services shall be funded by one or more select UNSMS organizations or, alternatively, through the local, cost-shared security budget.
    (i) At a minimum, a CISIC shall consist of one UNSMS Counsellor and a functional network of PH/PSV/FFP. A CISIC should also consist of EMHP, whenever possible.
    (ii) At high-risk duty stations, CISMU shall regularly assess the need to establish a standing CISIC,[16] in consultation with the Designated Official (DO)/Security Management Team (SMT), based on the psycho-social needs of UNSMS personnel and their eligible family members.
        a. Ensuring that an updated and approved psycho-social contingency plan exists, in consultation with all relevant stakeholders listed under Section C ("Structure")

[14] While not mandatory, eligible family members of UNSMS personnel should be strongly encouraged to attend any relevant training courses provided to UNSMS personnel.
[15] EMHP are externally trained and certified mental health professionals licensed to practice in their respective countries that may be trained, certified and/or employed by UNSMS organizations in order to play a role in the management of critical incident stress at the field level.
[16] The definition of a "high risk" duty station shall be in accordance with the UNSMS *Security Policy Manual*, Chapter IV (Security Management), *Guidelines to Determining Acceptable Risk*.

b. Ensuring the capacity to maintain regular communication and coordination with all relevant stakeholders listed under Section C ("Structure"), including through formal briefings, based on up-to-date Terms of Reference (TORs). Such communication and coordination shall be sufficient to assess and address the psycho-social needs of UNSMS personnel and their eligible family members.

c. In a crisis setting, the PCCC shall be responsible for implementing paragraphs 1-2 under Section E(a)(i) of this policy.

(b) Chiefs/Heads of Staff Counselling/Welfare Units or Sections of UNSMS organizations[17] shall be responsible for the following:

(i) Establishing and implementing their respective Pre-incident Preparedness plans.

(ii) Sharing their respective Pre-incident Preparedness plans with CISMU.

(iii) Seeking support from CISMU whenever internal resources are insufficient or unavailable.

(c) The DO/SMT shall be responsible for the following:

(i) Ensuring the availability of safety- and security-related resources required to implement any approved security contingency plan for the duty station, including the provision of psycho-social services, as required.[18]

(d) CSAs/SAs, CSOs, S-ASOs or CSFPs shall be responsible for the following:

(i) Including the provision of psycho-social services in any security contingency plan for high-risk and safe haven[19] duty stations, in coordination with all relevant stakeholders listed under Section C ("Structure").[20]

Incident Response

9. UNDSS/DRO shall be responsible for the following:

(a) Informing CISMU of any critical incident occurring at a duty station that may endanger the well-being of UNSMS personnel or their eligible family members in a timely manner, thereby triggering an incident response.

[17] Excluding UNDSS.

[18] The Framework of Accountability, Annex, Section H, paragraph 7 mandates the SMT to ensure "that resources are available to implement all measures which are approved."

[19] A "safe haven" duty station is identified as part of the country-specific security plan.

[20] The Framework of Accountability, Annex, Section J, paragraph 11 mandates CSAs/SAs to prepare, maintain and update "the country-specific security plan, contingency plans and security lists of personnel employed by the organizations of the United Nations system and their recognized dependants;" Annex, Section L, paragraph 13 mandates CSOs to contribute "to security risk assessments for all locations in the mission area where personnel are present, and actively participates in the planning and evaluation of the effectiveness of the country security plans and other aspects of security operations;" Annex, Section M, paragraph 1 mandates S-ASOs to advise and assist "the agency country representative or operations manager on his/her security responsibilities, including participation in operational planning, and provides security inputs, including information regarding compliance with United Nations security policies, practices and procedures;" Annex, Section K, paragraph 1 mandates CSFPs to manage "day-to-day security-related matters supported by UNDSS."

(b) Maintaining regular communication with CISMU regarding any changes in the prevailing environment at the duty station and serving as a liaison between CISMU and UNSMS security professionals in the field.

10. Upon receiving notification from UNDSS/DRO, CISMU shall be responsible for the following:
    (a) Rapidly assessing the needs of UNSMS personnel and their eligible family members and mapping locally-available resources, including EMHP.
    (b) Establishing or expanding a CISIC at the duty station in a timely manner, if necessary.
    (c) Coordinating the appropriate incident response through regular communication with all relevant stakeholders listed under Section C ("Structure"), including, but not limited to, the following:
        (i) Mobilizing the deployment of CISMU Regional or Field Counsellors, DPKO-DFS and/or DPA Staff Counsellors, PH/PSV/FFP and EMHP, in coordination with other relevant UNSMS Counsellors and UNSMS security professionals, in order to ensure delivery of appropriate services to all individuals referenced in Section B ("Applicability").
        (ii) Activating any updated and approved psycho-social contingency plan, if necessary. Prior to activing any psycho-social contingency plan, such a plan shall first be adapted by CISMU, in consultation with all relevant stakeholders as listed under Section C ("Structure"), to the local context, including the prevailing security environment at the duty station, in a manner that ensures the well-being of UNSMS personnel and their eligible family members.
            a. Maintaining regular communication with all relevant stakeholders listed under Section C ("Structure") so as to remain aware and rapidly react to any changes to the prevailing environment at the duty station, with the goal of ensuring the well-being of UNSMS personnel and their eligible family members.
            b. *In a crisis setting*, the PCCC shall be responsible for implementing paragraphs 1-5 under Section E(b)(ii) of this policy.

11. The DO/SMT shall be responsible for the following:
    (a) Ensuring the implementation of the approved security plan for the duty station, including the provision of psycho-social services, as required, with the aim of maintaining the well-being of UNSMS personnel and their eligible family members.[21]

12. Representatives of UNSMS organizations shall be responsible for the following:
    (a) Ensuring that their respective personnel, deployed to the duty station as part of the incident response, attend a security briefing[22] upon their initial arrival;[23]

[21] The Framework of Accountability, Annex, Section G, paragraph 1 mandates the DO to implement "the arrangements detailed in UN security policies and procedures as well as developing and implementing the required plans for the duty station with the aim of maintaining the security and safety of United Nations personnel, premises and assets".
[22] The Framework of Accountability, Annex, Section J, paragraph 14 mandates CSAs/SAs to establish a "system for briefing all personnel employed by the organizations of the United Nations system and their

(b) Ensuring that all activities of UNSMS personnel, deployed to the duty station as part of the incident response, are conducted in a way that manages the security risks to such personnel.[24]

13. If established or expanded, the CISIC shall be responsible for the following:
    (a) Re-assessing the needs of UNSMS personnel and their eligible family members at the duty station and clarifying strategies for carrying out the incident response with all relevant stakeholders listed under Section C ("Structure") and locally-available resources, including EMHP;
    (b) Providing psycho-social services to UNSMS personnel and their eligible family members as necessitated by the prevailing environment at the duty station, referring individuals to the most appropriate offices, if applicable (e.g., other UNSMS Counsellors, UNMERT, EPST and/or a UNDSS Field Office).
        (i) All relevant stakeholders listed under Section C ("Structure") shall encourage the use of psycho-social services by UNSMS personnel and their eligible family members; ensure equal access to such services and work to counter any stigmatization associated with the use of such services.
        (ii) The CISIC shall gather relevant data on various aspects of the incident response, in coordination with all relevant stakeholders listed under Section C ("Structure").
            a. Maintaining regular communication and coordination with all relevant stakeholders listed under Section C ("Structure") so as to inform such stakeholders of any changes to the prevailing environment at the duty station and coordinate any shift in approach or allocation of resources, with the goal of ensuring the well-being of UNSMS personnel and their eligible family members.
            b. In a crisis setting, the PCCC shall be responsible for implementing paragraphs 1-3 under Section E(b)(v) of this policy. The PCCC shall also be responsible for ensuring the rotation of CISMU Regional and Field Counsellors, in coordination with the CISWG and other UNSMS Counsellors, in order to avoid burnout.

14. Chiefs/Heads of Staff Counselling/Welfare Units or Sections of UNSMS organizations[25] shall be responsible for the following:
    (a) Rapidly assessing the needs of their respective personnel and their eligible family members;
    (b) Activating their respective Incident Response phase.

---

recognized dependants upon initial arrival, providing local security training as necessitated by changes in the security environment and ensuring such personnel are kept informed of matters affecting their security".

[23] The Framework of Accountability, Annex, Section G, paragraph 16 mandates representatives of United Nations Security Management System (UNSMS) organizations to require their respective personnel to "attend appropriate security awareness training and briefings".

[24] The Framework of Accountability, Annex, Section G, paragraph 8 mandates representatives of United Nations Security Management System (UNSMS) organizations to ensure "that activities of their organization are conducted in a way that manages the risks to personnel, premises and assets".

[25] Excluding UNDSS.

(i) Informing CISMU of their respective Incident Response and requesting CISMU's support whenever internal resources become insufficient or unavailable.

(ii) Coordinating their respective Incident Response phase with relevant, internal offices.

Post-incident Recovery

(a) If established or expanded, the CISIC shall be responsible for the following:

(i) Maintaining contact with and establishing adequate support mechanisms for impacted UNSMS personnel or eligible family members;

(ii) Maintaining regular communication and coordination with all relevant stakeholders listed under Section C ("Structure") so as to inform such stakeholders of psycho-social status of any UNSMS personnel or eligible family members and their ability to resume daily activities;

(iii) Submitting a written report to CISMU-HQ, including any relevant data, detailing their activities and observations at the duty station, including best practices and lessons learned, no later than twenty-one (21) calendar days after the Incident Response phase has concluded.

(b) CISMU shall be responsible for the following:

(i) Ensuring any necessary follow-up with impacted UNSMS personnel or eligible family or, alternatively, referring such individuals to UNSMS organizations with the ability to provide immediate and adequate psycho-social services;

(ii) Compiling and circulating all relevant reports received from the CISIC and other relevant stakeholders listed under Section C ("Structure") to relevant parties, respecting the confidential or classified nature of any information contained therein.

(c) Chiefs/Heads of Staff Counselling/Welfare Units or Sections of UNSMS organizations[26] shall be responsible for the following:

(i) Implementing their respective Post-Incident Recovery phase, whereby continued access to counselling services for all respective personnel impacted by a given critical incident shall be ensured;

(ii) Coordinating their respective Post-Incident Recovery phase with relevant, internal offices.

E. Final Provisions

15. This policy shall be made available to all UNSMS organizations and to all individuals covered under UNSMS *Security Policy Manual* (SPM) Chapter III ("Applicability of United Nations Security Management System").

16. This policy enters into force on 23 November 2015.

17. This policy hereby supersedes all previous UNDSS communiqués, memoranda and other communications related to the management of critical incident stress in the field.

[26] Excluding UNDSS.

Annex A

Management of Critical Incident Stress Framework (MCISF)

1. The Management of Critical Incident Stress Framework (MCISF) envisions an integrated and coordinated continuum of care that provides for the basic psycho-social needs of UNSMS personnel and their eligible family members. This multi-layered approach includes the local community resources in order to grant full access to all available United Nations resources, with all individuals involved in the management of stress and critical incident stress providing valuable feedback on their preparedness, response and recovery efforts.

2. The MCISF adopts a holistic approach, encompassing all three phases required in managing critical incident stress (i.e., Pre-Incident Preparedness, Incident Response and Post-Incident Recovery), taking into account the whole person and the systems to which he or she belongs: family, work and society. Psycho-social services must be provided with the highest degree of cultural awareness and sensitivity towards the needs of the individual and his or her local context. Such services focus on factors supporting human health and well-being, rather than those causing disease. The goal is to recognize and treat stress reactions on an as needed basis while recognizing that not all symptoms are pathological.

3. The management of critical incident stress begins well before the occurrence of a critical incident, primarily through the implementation of adequate preventative measures, and continues during and after the critical incident itself. Such services aim to mobilize the individual's intrinsic coping mechanisms, which are inherent to every human being. In this regard, an assessment is made to determine if a higher level of psycho-social intervention is necessary, with the ultimate goal of allowing the individual to resume his or her daily activities with no disruption.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter VII

PROVISIONS ON SAFETY MATTERS

SECTION B

Air Travel Policy

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 17 October 2011
Technical Review: 1 May 2017

A. Introduction

1. United Nations Security Management System (UNSMS) personnel serve in some of the most challenging environments in the world, often working in difficult conditions while conducting their duties under the mandates, programmes and activities of their respective organization.

2. Air transport is a preferred – and often the only – mode of transport available for reaching duty stations around the globe. Each duty station may pose different risks with regard to aviation. This policy accounts for these differences and provides consistent and up-to-date aviation information for UNSMS personnel.

3. The expertise of the International Civil Aviation Organization (ICAO) is relied upon to address issues that may challenge or pose additional risks to a flight.

4. For the purposes of this policy, responsibilities, aviation risks and aviation safety must be considered within the context of the safety and well-being of UNSMS personnel supporting the mandates, programmes and activities of their respective organization and in accordance with the policies, procedures, standards and other arrangements of the UNSMS.

B. Applicability

5. The policy is applicable to all UNSMS organizations and all individuals covered by the UNSMS, as defined in Chapter III of the *Security Policy Manual* ("Applicability of the United Nations Security Management System"). Such individuals shall herein be referred to as "personnel".

6. This policy applies to all personnel on official travel and using

   (a) Commercial Air (Transport) Operators
      (i) Scheduled
      (ii) Non-Scheduled;
   (b) United Nations Contracted Chartered Services;
   (c) Donated Flights.

7. This policy does <u>not</u> apply to medical evacuation flights.

C. Definitions

Relating to the UNSMS

8. **Air Travel Focal Point (ATFP)**. Assigned individual(s), acting as the representative(s) of their UNSMS organization, who is (are) primarily responsible

for responding to questions relating to air travel in accordance with the policy and guidelines of his or her organization.[1]

9. **Security Professional**. Under the Framework of Accountability for the UNSMS, the most senior security professional directly supporting the Designated Official (DO), who can be an agency-assigned professional.

10. **Air Travel Operational Guidelines**.[2] Guidelines developed by each UNSMS organization. These operational guidelines offer specific guidance regarding definitions, procedures, authorizations and requirements expected in the planning of air travel as it relates specifically to their organization.

11. **Manager with Signature Authority**. The manager entrusted by his or her UNSMS organization with the authority to weigh the risks associated with air travel against those associated with the delivery of his or her organization's programme(s), in accordance with the Framework of Accountability for the UNSMS.

12. **Aviation Risk Management Office (ARMO)**. An office within the United Nations Department of Safety and Security (UNDSS) that takes a broad, holistic approach to air transport and aviation, with a focus on aviation risks faced by personnel.

13. **Risk Management Tool (RMT)**. A structured, holistic and subjective risk assessment process model aligned with the Security Risk Management (SRM) process and used to identify threats and assess specific risks that may affect personnel and programmes.[3]

14. **Official Travel (or Official Business Travel)**. Official travel is defined as travel authorized and paid for, or provided by, the parent organization of the personnel.

    (a) Official travel covers all travel, undertaken in any of the circumstances set out below:
        (i) Initial appointment;
        (ii) Official business (including for training purposes);
        (iii) Change of official duty station;
        (iv) Separation from service;
        (v) Medical,[4] safety or security reasons;

[1] ATFP Terms of Reference (TORs) are included as Annex A to this policy.
[2] See Air Travel Operational Guidelines in the *Security Management Operations Manual* (SMOM), which provide a template for each UNSMS organization to develop its own Air Travel Operational Guidelines in accordance with this policy.
[3] The Risk Management Tool (RMT) and associated processes should only be conducted by security professionals and authorized ATFPs having demonstrated proficiency in the UNSMS security risk management (SRM) process.
[4] This policy is not applicable to medical evacuation flights.

(vi) Home leave;
(vii) Family visit;
(viii) Education grant travel;
(ix) Repatriation of eligible family members;
(x) Rest and Recuperation (R&R) travel (including all cases where those eligible for R&R decide to deviate and travel to a location other than the authorized R&R location).

(b) In addition, any authorized travel that is undertaken at no cost to the parent organization may also be considered official travel when undertaken for official business, including for training purposes.

Relating to Aviation

15. **Air Charter Agreement**. Air charter agreements refer to a contractual arrangement between an air operator and an organization employing its aircraft, crew and other necessary personnel for the sole purpose of providing short-term or long-term air transport services.

16. **Commercial Air (Transport) Operator**. An operator, with a valid Air Operator Certificate (AOC) issued by the State of the operator,[5] which, for remuneration or hire, provides scheduled or non-scheduled[6] air transport services to the public for the carriage of passengers.

17. **Donated Flight**. Air transport offered and provided by an air operator, whether publicly-owned (i.e., by the State or government) or privately-owned (i.e., by a corporation or person), to benefit personnel in support of humanitarian service, joint mandate and/or other purposes at no cost to the relevant UNSMS organization.

18. **United Nations Aviation Standards (AVSTADS)**. Established common aviation standards for chartered humanitarian and peacekeeping air transport operations to facilitate interoperability and that are applicable to UNSMS organizations involved in the provision of air charter agreements.

[5] Normally under the direction of a civil aviation authority or equivalent body.

6 Non-scheduled air transport, commonly referred to as an "Air Taxi," does not include passenger charter operators for the purposes of establishing contracted chartered services procured or administrated by air charter agreements. These air operations are covered in paragraph 29 under Section H ("Personnel Travel Facilitated by United Nations Contracted Air Charter Agreements").

Relating to Procedures

19. **Donated Flight RMT**. A formal process[7] initiated by the ATFP or security professional for the assessment of a donated flight for use in operational planning.

20. **United Nations Contracted Chartered Services**. Air charter agreements, procured under paragraph 15, for use to support United Nations mandated activities are governed by the United Nations Aviation Standards for Peacekeeping and Humanitarian Air Transport Operations (AVSTADS).[8]

D. Purpose

21. The purpose of this policy is to provide clear guidance on air travel in order to enable the mandates, programmes and activities of UNSMS organizations while ensuring the safety and security of personnel. This policy directs authorized users[9] towards available risk-based information and guidance relating to the use of air transport, thereby enabling informed decision-making by the Manager with Signature Authority.

E. Requirements for UNSMS Organizations

22. Each UNSMS organization is required to provide UNDSS with their official Air Travel Operational Guidelines. UNDSS will maintain a template that UNSMS members may use for this purpose. Key elements should, at a minimum, include the following:

    (a) Contact details of the ATFP and alternates;
    (b) Organization's insurance guidance relating to air travel, including the maximum number of personnel permitted to travel on one aircraft;
    (c) Organization's requirements for identifying the appropriate Manager with Signature Authority.

23. Each UNSMS organization shall assign at least one Air Travel Focal Point (ATFP)[10] who shall act as its representative and who shall be responsible for responding to questions relating to air travel in accordance with his or her organization's Air Travel Operational Guidelines.

[7] A Donated Flight RMT template and associated processes for use are accessible to ATFPs and security professionals via the United Nations Security Management Information Network (UNSMIN) website, maintained by UNDSS.
[8] All UNSMS organizations requiring the use of charter flights in order to meet specific mission requirements can contact the World Food Programme (WFP) Air Transport Unit or the Department of Field Support (DFS) Air Transport Section (ATS) to request assistance.
[9] Authorized users include the Air Travel Focal Point (ATFP) and security professionals as defined in paragraphs 8 and 9, respectively, under Section C "Definitions".
[10] Requirements for ATFPs and alternates are included in this policy and detailed in the Air Travel Operational Guidelines.

24. ATFPs shall have access to a dedicated United Nations website providing information (e.g., ICAO's categorizations, supplemental information) regarding the suitability of Commercial Air (Transport) Operators for use by personnel. Additionally, ATFPs shall have access to relevant risk management information, in addition to ARMO's support, training and Frequently Asked Questions (FAQs).

F. Requirements for Travelers/Passengers

25. All personnel are expected to comply with their respective organization's Air Travel Operational Guidelines.

26. All personnel are expected to comply with the safety requirements and briefings provided by crew members with regard to air operations.

27. All personnel are expected to comply with UNSMS policies, including the requirement to undergo relevant security training[11] and obtain a security clearance through the Travel Request Information Processing (TRIP)[12] system.

G. Personnel Travel on Commercial Air (Transport) Operators

28. Commercial Air (Transport) Operators are categorized using ICAO's methodology, which filters air operators into one of three categories: Unrestricted Use, Conditional Use, or Restricted Use. The categorization of any air operator shall only be used for internal purposes and shall not be made available to any individual or organization not covered by the UNSMS (see Section B, "Applicability"). The three categories and their implications for use by personnel are further explained below:

    (a) Unrestricted Use. The air operator meets established safety criteria and is considered suitable for use by personnel on official travel;

    (b) Conditional Use. The air operator is considered suitable for use by personnel on official travel when an Unrestricted Use air operator is not available. A risk assessment using the RMT, as per the framework established by UNDSS for specific circumstances (e.g., date, city pair and number of travellers), may be conducted to support decision-making for the use of these air operators;

    Supplemental information shall be provided to clarify the Conditional Use categorization and enable the UNSMS-assigned Air Travel Focal Point and/or security professional[13] to provide advice regarding suitability for use;

[11] See *Security Policy Manual*, Chapter V, Section C ("Security Training and Certification").
[12] See *Security Policy Manual*, Chapter V, Section A ("Security Clearance Procedures and the Travel Request Information Process (TRIP)").
[13] As defined in this policy.

(c) Restricted Use: The decision to use air operators categorized as 'Restricted Use' shall be made by the Manager with Signature Authority (see Section C, "Definitions") after conducting a risk assessment using the RMT, as per the framework established by UNDSS for specific circumstances (e.g., date, city pair and number of travellers).

H. Personnel Travel Facilitated by United Nations Contracted Air Charter Agreements

29. Air operators chartered under a United Nations contract (i.e., air charter agreement) are expected to adhere to the standards and procedures established in the AVSTADS (see paragraph 20). Commercial Air (Transport) Operators categorized as 'Unrestricted Use' for official United Nations travel may also be considered if charter services are offered.[14]

I. Personnel Travel Facilitated by Donated Flights

30. Donated Flights may include the use of publicly-owned (i.e., by the State or government) or privately-owned (i.e., by a corporation or person) aircraft.

31. The approval for the use of donated aircraft rests with the Representatives of UNSMS organizations at the country level,[15] in line with programme criticality. Authorization shall be granted after a Donated Flight risk assessment, using the RMT, has been conducted, whereby the assessment does not indicate Very High Risk.[16]

32. Should the Donated Flight risk assessment indicate Very High Risk, approval for use by the Under-Secretary-General for Safety and Security (USG, UNDSS) shall be required.[17]

33. In a crisis setting, whereby immediate deployment is required, approval may be granted by USG, UNDSS in lieu of a Donated Flight risk assessment.

34. The Donated Flight RMT form and instructions shall be made available to security professionals and authorized ATFPs.[18]

[14] Air charter services represent a procurement function, whereby the entire aircraft and all seats are designated for the sole use of the contracting organization. Personnel or UNSMS organizations requiring aircraft to be contracted under a charter agreement (i.e., one-time basis, short-term, long-term) may contact the World Food Programme (WFP) Air Transport Unit or Department of Field Support (DFS) Air Transport Section for assistance and guidance.

[15] See *Security Policy Manual*, Chapter II, "Framework of Accountability," Annex, Section G, paragraph 5, which mandates Representatives of UNSMS organizations advise "the Designated Official, Chief Security Adviser and their respective Security Focal Point at Headquarters on the particular concerns of their organization regarding security."

[16] The delegation of signature authorization must be stated in the relevant UNSMS organization's Air Travel Operational Guidelines.

[17] The USG, UNDSS may delegate this responsibility at his or her discretion.

J. Training and Compliance

35. Personnel shall be familiar with and abide by this policy. Personnel shall immediately report any non-compliance with this policy to their respective parent organization.

36. Training shall be provided by UNDSS to the Air Travel Focal Point (ATFP) and security professionals.

K. Final Provisions

37. This policy shall be made available to all UNSMS organizations and personnel.

38. This policy enters into force on 17 April 2015.

39. This policy supersedes the "Commercial Passenger Air Travel Guidelines, Final Revised Version" approved by the IASMN in May 2006 and all prior memoranda, circulars, communiqués and standard operating procedures issued by UNDSS relating to Personnel Air Travel.

[18] As defined in paragraph 13, Section C "Definitions", of this policy. This risk assessment represents the established UNDSS process for the use of donated aircraft, in compliance with the Malicious Acts Insurance Policy (MAIP).

ANNEX A

UNITED NATIONS AIR TRAVEL FOCAL POINT TERMS OF REFERENCE

I. INTRODUCTION

1. The role of the Air Travel Focal Point (ATFP) was established by the Inter-Agency Security Management Network (IASMN) in April 2005 to ensure harmonization and better coordination of aviation risk management efforts by the United Nations Security Management System (UNSMS) and implementation of aviation risk management initiatives aimed at enhancing safety for travelling personnel. The structure proposed by the IASMN envisioned air travel focal points, assigned by the UNSMS organization, responsible for interacting with the United Nations Department of Safety and Security's (UNDSS) Aviation Risk Management Office (ARMO).

2. The function of the ATFP is to act as his or her organization's representative to ARMO and facilitate communication between his or her organization's respective personnel and ARMO in order to enable the transfer of information relating to relevant policies, guidelines, standards and other arrangements and to address relevant queries from such personnel.

3. For issues that are unique and not clearly defined, the ATFP has direct access to ARMO and its secure website for assistance. Information, including training and Frequently Asked Questions (FAQs), is available to help the ATFP understand and address the most common issues related to air travel. These FAQs are updated as required.

4. The assistance provided by ARMO is focused on supporting the ATFP, who, in turn, guides the appropriate signatory authorities.[19] Should a unique situation arise with a specific air operator, the Risk Management Tool (RMT) may be conducted.[20]

II. COMPOSITION

5. Each UNSMS organization shall identify at least one staff member to serve as that organization's ATFP. The ATFP shall liaise with ARMO, which shall support the ATFP and his or her organization.

[19] The manager who approves the mode of travel must first compare the information provided to him or her with his or her organization's Air Travel Operational Guidelines. Authorized managers should weigh the requirements of the field or mission with information provided prior to approving flights on air operators categorized as 'Conditional Use' or 'Restricted Use'.

[20] Refer to United Nations Personnel Air Travel Policy for definition.

III. RESPONSIBILITIES

6. The ATFP shall:

(a) Serve as his or her organization's focal point for the implementation of the Air Travel Policy and his or her organization's Air Travel Operational Guidelines;

(b) Assist in populating his or her organization's Air Travel Operational Guidelines with required information, updated in line with UNDSS policies and recommendations and with a copy of such guidelines provided to UNDSS on an annual basis;

(c) Have access to risk management information as well as information and training by ARMO, including FAQs for common air travel questions and safety matters;

(d) Reference information provided by ICAO relating to the suitability of Commercial Air (Transport) Operators when advising authorized managers within their organization (see Section G, "Personnel Travel on Commercial Air (Travel) Operators");

(e) Compare the categorizations, suitability for use and any additional information received from ARMO with his or her organization's Air Travel Operational Guidelines and share such information with the appropriate Manager with Signature Authority;

(f) Conduct or request a risk assessment, using the RMT, for air operators categorized as 'Conditional Use' or 'Restricted Use', as authorized. The RMT is intended to ensure consideration of specific circumstances (e.g., date, city pair and number of travellers) and provide a risk assessment for the appropriate Manager with Signature Authority;

(g) Request a Donated Flight risk assessment, using the RMT, from ARMO, if applicable, and follow guidance from ARMO (see Section I, "Personnel Travel Facilitated by Donated Flights");

(h) Notify ARMO of relevant air travel concerns relating to air operations that may directly affect their duty station(s) (e.g., new air operator activity, air operator business news and reports from passengers);

(i) Advise and undertake activities that enhance interoperability between UNDSS, the ATFP and his or her organization on air travel matters; and

(j) Represent his or her organization at meetings related to air travel safety, risk management and use and suitability of air operators for official travel, as required.

IV. COMMUNICATION and COORDINATION

7. In order to adequately address questions regarding the suitability and use of air operators, ARMO shall communicate directly with the appropriate ATFP to ensure relevant information flows to the appropriate individual(s) within his or her organization.

8. Communication with ARMO shall be facilitated through one of the following channels:

   (a) ATFP, as assigned by his or her organization;
   (b) Security professional.

UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter VII

PROVISIONS ON SAFETY MATTERS

SECTION C

Fire Safety

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 15 April 2012
Technical Update: 1 May 2017

A. Introduction

1. Fire is a serious threat to the personnel and property of any organization, including the United Nations. Fires cause numerous injuries, deaths and losses of assets in organizations each year. Fire is a potential hazard in all United Nations premises because an outbreak of fire would jeopardize life, property and the delivery of programmes and projects.

2. While the primary responsibility for the safety and security of United Nations personnel rests with the host country, all United Nations organizations are responsible and accountable for providing adequate measures to prevent fires and protect personnel members and others at United Nations facilities against fire. Individually, all United Nations personnel are responsible and accountable for compliance with fire safety standards and taking reasonable efforts to prevent fires.

3. Losses from fires are preventable by applying basic fire prevention principles and being prepared for emergencies. Within the United Nations, fire prevention is the primary strategy for fire safety; however, mitigation measures for rapid detection, raising the alarm, containment and suppression must also be put in place, in addition to reliable measures to rapidly evacuate personnel and others who may be present on United Nations premises.

4. This strategy requires the highest level of systematic planning and preparedness at the managerial level, including proper procedures and continuous training. Effective management practices require the development and implementation of policies and procedures to protect personnel and property by preventing and/or dealing with fires and preparing for emergencies.

B. Purpose

5. This policy sets out the key elements of fire safety that all United Nations Security Management System (UNSMS) organizations shall follow to minimize the risk[1] from fire to personnel, to other occupants of United Nations premises, including visitors, and also to the premises itself and the property contained therein.

6. This policy must be read in conjunction with the "United Nations Fire Safety Guidelines".

C. Applicability

7. The policy is applicable to all organizations participating in the UNSMS and their personnel (herein referred to as "United Nations personnel") as defined in Chapter III of the Security Policy Manual ("Applicability of United Nations Security Management System").

[1] Please also refer to *Security Policy Manual* Chapter IV, Section A on Security Risk Mangement Policy.

8. This policy has special application for United Nations personnel and managers who are responsible for the implementation of and adherence to fire safety policy, procedures and programmes on United Nations premises.

9. As per *Security Policy Manual* (SPM), Chapter IV, Section E ("Security of United Nations Premises"), United Nations premises are defined as all categories of land and physical areas that are utilized or occupied by the organizations of the United Nations Security Management System, including structures such as buildings, offices, warehouses, stores, shops, dwellings, containers, prefabs and tents.

10. For government facilities hosting United Nations personnel, this policy shall be applied in accordance with the provisions of the *Security Policy Manual* (SPM), Chapter IV, Section N ("Minimum Operating Security Standards"), Appendix 1, paragraph 6.3.

D. Conceptual Overview

11. United Nations system organizations confront many challenges in achieving adequate and acceptable fire safety coverage. Major obstacles include the following:

    (a) United Nations organizations are often located in spaces which pose fire safety hazards and over which the United Nations has no proprietary right to enforce or make significant structural changes;

    (b) Limited or non-existent fire safety regulations resulting in buildings available to United Nations having minimal fire safety features;

    (c) Inadequate infrastructure to support fire safety systems and provide the necessary resources to fight fires.

12. There are three key elements to overcoming these challenges:

    (a) Using risk management principles, United Nations system organizations shall combine fire prevention and mitigation strategies and measures to protect United Nations personnel and facilities;

    (b) Make adequate provisions within each relevant budget for fire safety requirements;

    (c) Collaborate with host country authorities, including local fire services and, wherever possible, building owners.

E. Fire Safety Policy

13. The strategy of the United Nations for managing the risks from fire hazards is one of both prevention and mitigation.[2] Prevention entails measures intended to lower the likelihood of a fire occurring, such as compliance with applicable fire codes, fire safety rules for building occupants, regular housekeeping, fire safety inspections and training of personnel. Mitigation entails measures intended to lower the impact of a fire once it has occurred, including fire detection and alarm systems, fire suppression systems, fire and smoke compartmentalization, training on the use of fire suppression equipment, fire safety and evacuation planning, emergency evacuation drills, functioning evacuation routes (including alternates) and exits and medical emergency procedures.

14. The principal risk management tool is the Fire Safety Plan. All United Nations premises must have a written Fire Safety Plan that is compliant with the provisions of and template in the "United Nations Fire Safety Guidelines". The Fire Safety Plan is part of the larger Security Risk Management (SRM) Plan and describes actions required of those with key responsibilities in the prevention and mitigation of fire risks, as well as the responsibilities of United Nations personnel and visitors.

15. The existence of a Fire Safety Plan will be verified by all United Nations Department of Safety and Security (UNDSS) compliance missions.

16. The "United Nations Fire Safety Guidelines" provide baseline guidance and standards. Where host country fire prevention codes, rules and regulations provide more detailed technically-acceptable guidance and direction, they take precedence over United Nations guidelines. The highest standards, whether they are host country standards or United Nations guidelines, must always take precedence.

17. Where host country fire prevention codes, rules and regulations are absent or inadequate, reference should be made to the United Nations Fire Safety Guidelines. If more comprehensive guidance is required than is contained in the United Nations guidelines, reference should be made to a fire code that is internationally recognized and that is most applicable to the geographical location, for example the International Fire Code. More detailed guidance is found in the United Nations Fire Safety Guidelines.[3]

18. In those countries where the host country has an established fire safety structure, including fire safety professionals, codes, rules and regulations, United Nations personnel charged with fire safety responsibilities are to consult with host country fire safety professionals and fire safety authorities to ensure that implementation of any provision of United Nations Fire Safety Guidelines is consistent and compatible with the applicable host country codes.

[2] Security Policy Manual, Chapter IV, A ("Policy on Security Risk Management"), paragraph 14.
[3] See United Nations Fire Safety Guidelines, 2011, Part V, subheading "Fire Codes".

19. The provisions in the United Nations Fire Safety Guidelines are meant to be used, where applicable, for assessing, establishing and implementing fire safety programs in United Nations premises.

20. In addition to observing all host country fire safety requirements in all United Nations premises, United Nations personnel tasked with fire safety will ensure that fire safety policies and programmes are established in accordance with "United Nations Fire Safety Guidelines" and are in place.

21. Fire Safety Plans shall be regularly reviewed and updated to address any changes in the structure of buildings, functions, contents and any other matters which may have a bearing on fire safety.

22. Fire prevention and mitigation, including standards set out in local or international fire codes, must be factored into the design of United Nations premises and/or in the acquisition of existing premises for United Nations use.

F. Roles and Responsibilities

23. Internationally, the proven and most important element of effective fire safety in any domain requiring fire safety protection is a positive fire safety culture. A positive fire safety culture is primarily achieved and maintained by raising awareness among personnel, applying appropriate fire safety rules and regulations and defining associated responsibilities and accountability. Responsibilities and accountability for safety and security, which includes fire safety, are clearly articulated in the "Framework of Accountability for the United Nations Security Management System".[4]

24. Negligence and disregard for appropriate safety measures, including fire safety, at any level of responsibility is likely to directly add risk to lives, assets and programme delivery. Regardless of where personnel are located, each UNSMS organization has a duty of care to provide appropriate fire safety measures to lower the risk from fire to an acceptable level.

25. The following establishes the specific responsibilities for fire safety, primarily at the country level, within the UNSMS (see Annex A for schematic).

Under-Secretary-General for Safety and Security

26. The Under-Secretary-General for Safety and Security has the delegated authority from the Secretary-General to make executive decisions regarding the safety and security of United Nations personnel, premises and assets and is therefore responsible for fire safety within the United Nations.

[4] United Nations Security Management System , *Security Policy Manual*, Section B ("Framework of Accountability for the United Nations Security Management System" February 2011.

27. The Under-Secretary-General for Safety and Security is responsible for developing fire safety policies, practices and procedures for the United Nations system worldwide and coordinating with organizations of the United Nations system to ensure implementation, compliance and support for fire safety aspects of their activities.

Designated Official

28. The Designated Official (DO) is responsible for ensuring the establishment, monitoring and annual review of all Fire Safety Plans within his/her area of responsibility.

Chief Security Adviser (CSA)/Security Adviser (SA)/Country Security Focal Point (CSFP)

29. The most senior security professional directly supporting the DO[5] is responsible for monitoring and annual reviews of the Fire Safety Plans within his/her area of responsibility and performs the following duties in this role:

    (a) Coordinates closely with representatives or organizations in his/her area of responsibility to ensure that each United Nations organization and integrated premises (if applicable) is aware of their requirement to have a functioning Fire Safety Focal Point;

    (b) Ensures each UNSMS organization within his/her area of responsibility has a current Fire Safety Plan;

    (c) Informs and regularly updates all UNSMS organizations on host country legislation relating to fire safety;

    (d) Monitors compliance with this policy, the United Nations Fire Safety Guidelines and applicable host country legislation relating to fire safety;

    (e) In consultation with Security Focal Points and facilities management, provides advice to the DO on the acquisition of new premises;

    (f) Provides an annual report to the DO and Security Management Team (SMT) regarding the current state of Fire Safety Plans of UNSMS organizations in his/her area of responsibility.

[5] This is usually the Chief Security Adviser or another Security Adviser, including their officer-in-charge *ad interim*. Where a Chief Security Adviser or Security Adviser is not present, this term is equivalent to the titles of Chief Security Officer, Chief of Security and Safety Services, Country Security Focal Point or Local Security Assistant (if necessary, in countries where no international professional security adviser has been assigned or is present).

Representative of Organization (country-level)

30. The country-level representative of organizations participating in the UNSMS:

    (a) Implements appropriate actions to provide for the safety and security of their respective personnel at the duty station;

    (b) Ensures that fire safety is a core component of their respective security programmes in the country and that appropriate funding is provided;

    (c) Appoints an existing staff member as Fire Safety Focal Point;

    (d) Ensures that their personnel are familiar with all fire safety-related instructions;

    (e) Takes action on instances of non-compliance with fire safety policies, practices and procedures;

    (f) Reviews, approves and ensures that the organization's Fire Safety Plan is properly implemented.

Fire Safety Focal Point (country-level)

31. Each UNSMS organization shall appoint an existing staff member with the responsibilities of a Fire Safety Focal Point in each country where they have a presence.

32. The Fire Safety Focal Point is responsible for coordinating fire safety for the organization in-country in accordance with "United Nations Fire Safety Guidelines" and in collaboration with Chief Security Adviser/Security Adviser/Country Security Focal Point,:

    (a) Coordinates fire safety issues with facilities managers/owners, host country authorities and organization management;

    (b) Coordinates fire safety inspections, fire safety risk assessments and recommends remedial fire safety measures;

    (c) Prepares the Fire Safety Plan and Emergency Evacuation Plan;

    (d) Nominates and trains fire wardens as part of the Fire Safety Plan;

    (e) Ensures that a competent certified entity conducts periodic maintenance of fire safety and firefighting systems, where available;

    (f) Rehearses building evacuation plans through regular drills, as required by United Nations Minimum Operating Security Standards (MOSS);

    (g) Briefs and trains personnel on fire safety;

(h) Monitors adherence to fire safety policy;

(i) Advises management on all aspects of fire safety;

(j) In the event of a fire or an emergency evacuation, provides supervision and coordination in accordance with the Fire Safety Plan and Emergency Evacuation Plan.

33. In the absence of a competent local capacity, a qualified and certified fire safety entity may be engaged to carry out specific tasks listed in paragraph 31 above, however, the country-level representative of the UNSMS organization retains responsibility and accountability for those functions.

United Nations Personnel

34. United Nations personnel are responsible at all times for compliance with any fire safety regulations and procedures established at their duty station both on and off duty.

G. Training Requirements

35. All United Nations personnel shall attend briefings and be familiar with fire safety and evacuation procedures in their workplace.

36. All United Nations personnel who have a specific role under the Fire Safety Plan for their organization must be adequately trained in their responsibilities and participate in fire safety and evacuation drills. Training will normally be delivered by, or under the direction of, the Fire Safety Focal Point.

37. Fire Safety Focal Points shall receive fire safety training as and when provided by the United Nations Department of Safety and Security. Fire safety focal points are to be guided in the performance of their duties by the United Nations Fire Safety Guidelines.

H. Enforcement

38. For the purpose of this policy, a fire safety violation is defined as an act or omission that compromises or may compromise fire safety at United Nations premises. Fire safety violations identified during fire safety inspections or as a result of an investigation must be remedied as soon as possible. In the event of an investigation into a fire incident, findings that any United Nations personnel have failed to abide by the terms of this policy may lead to administrative or disciplinary proceedings.

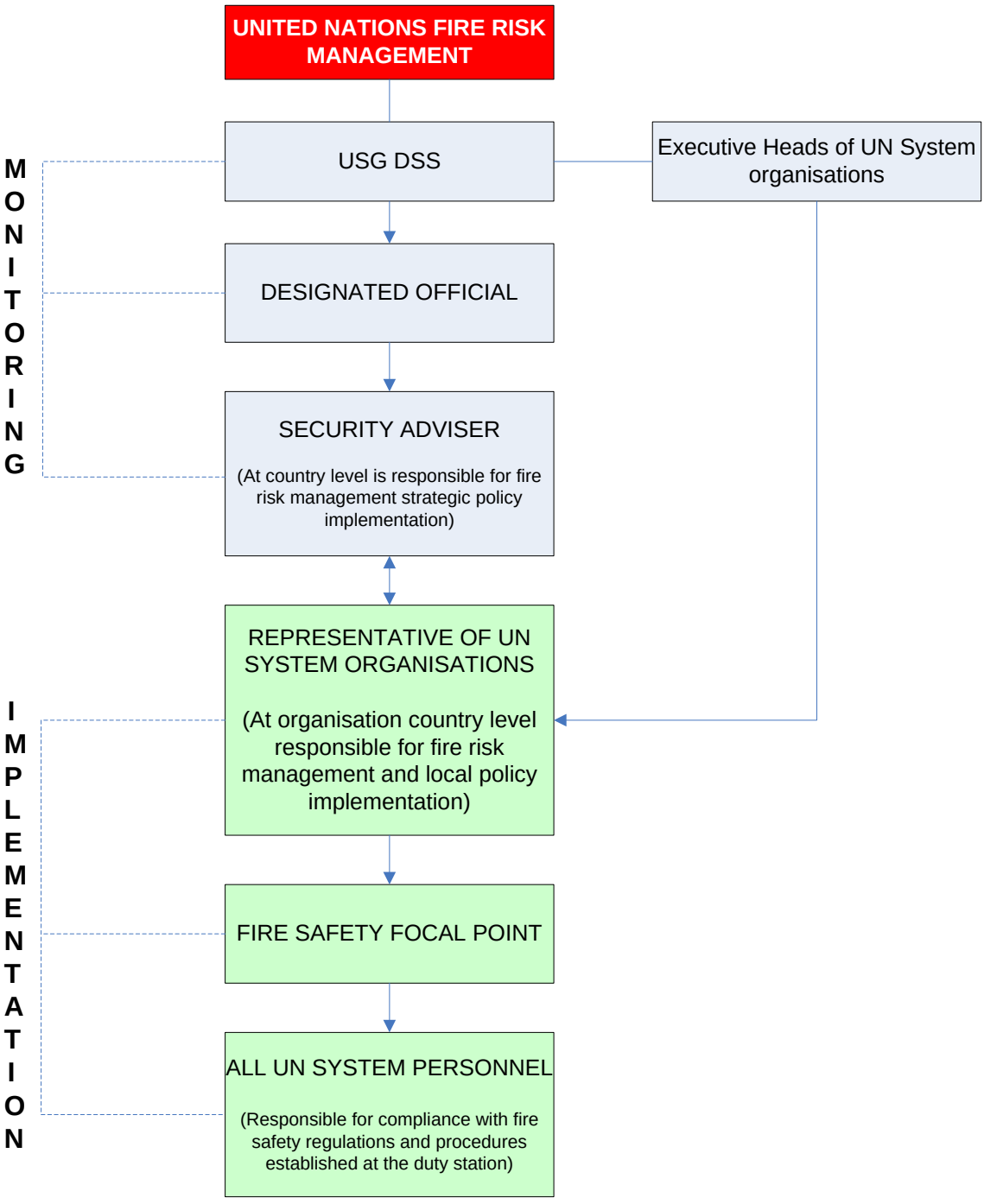
I. Final Provisions:

39. This policy is meant to be made available to all United Nations personnel.

40. This policy enters into force on 15 April 2012.

Annex A

United Nations Fire Safety Responsibility and Accountability



UNITED NATIONS SECURITY MANAGEMENT SYSTEM
Security Policy Manual

Chapter VII

PROVISIONS ON SAFETY MATTERS

SECTION D

Road Safety

.

UNITED NATIONS DEPARTMENT OF SAFETY AND SECURITY

UNDSS

Date: 31 October 2011
Technical Review: 1 May 2017

A. Introduction

1. Road and vehicle-related accidents are a common cause of injury and death among United Nations personnel. Poor road safety practices are not only a danger to drivers, passengers and other road users, they impede the ability of organizations to implement their programmes. Further, unsafe driving practices and road traffic accidents involving United Nations vehicles can generate resentment within the local population towards the United Nations, potentially creating further security incidents.

B. Purpose

2. The purpose of this policy is to promote the safe operation of United Nations vehicles[1] world-wide, to ensure road safety and to describe the roles and responsibilities of relevant United Nations Security Management System (UNSMS) actors in improving awareness and compliance with requirements and provisions for road safety.

C. Applicability

3. The policy is applicable to all individuals covered by the UNSMS, as defined in Chapter III of the *Security Policy Manual* (SPM) ("Applicability of the United Nations Security Management System") and to all non-United Nations personnel who are passengers in United Nations vehicles. For the purpose of this policy, the term "driver" applies to any person who operates a United Nations vehicle.

D. Conceptual Framework

4. Global road safety has been a subject of attention by staff, managers and even Member States, who have repeatedly registered their concern at the burden of injury and death resulting from road traffic accidents. United Nations personnel have an obligation to promote road safety by their own behaviour as drivers and road users. The policy sets out safe practices for operating and driving United Nations vehicles.

5. The strategy of the United Nations for managing the risk from road safety hazards is one of both prevention and mitigation, as discussed in the *Security Policy Manual* (SPM), Chapter IV, "Policy on Security Risk Management (SRM)", paragraph 14. Prevention entails measures intended to lower the likelihood of a road traffic accident occurring, such as driver training, driver regulations and safety-awareness programs. Mitigation entails measures intended to lower the impact of a road traffic accident once it has occurred, including the use of seatbelts and plans and preparations for medical attention, including first aid training drivers and other personnel.

6. Because of the large number of United Nations vehicles engaged in numerous road missions daily, there is a need for a global policy that sets out detailed requirements for the management of risks from road safety hazards.

[1] For the purpose of this policy, "United Nations vehicle" means a wheeled, ground transport motor vehicle (either owned, leased or rented) operated by any member organization of the UNSMS.

7. The current policy shall be read in conjunction with the latest policies on the use of United Nations road transport and materials produced for any on-going road-safety campaigns, including those of the United Nations Department of Safety and Security (UNDSS).

E. Requirements for United Nations System Organizations

8. United Nations system organizations are responsible for ensuring compliance with the provisions of this policy for each location where they manage vehicles. Each United Nations system organization has a responsibility for ensuring the safety of its personnel and property and should disseminate policies and take other appropriate measures accordingly. Nothing in the provisions of this policy restricts United Nations organizations from implementing stricter measures for road safety or determines the non-safety-related vehicle policies that United Nations organizations have in place for driving authorization, use of vehicles, etc.

9. United Nations system organizations are responsible for initiating, in all locations where they manage vehicles, road safety information and awareness campaigns for their personnel, including the rules and regulations for road safety, United Nations statistics (and, where available, national statistics) on road traffic accidents, and for providing, in consultation and coordination with the UNDSS, safe-driving training for drivers that reinforces the notions of "safety first" and "defensive driving".

10. United Nations organizations shall ensure that vehicles are properly managed and maintained in roadworthy condition, including according to local legislation.

11. United Nations organizations shall ensure the widest distribution of this policy to all personnel and the basic provision thereof in every United Nations vehicle.

12. In addition to the provisions of Section J below, United Nations system organizations are strongly encouraged to implement programs to reward drivers who demonstrate a safe driving record.

13. Designated Officials (DOs) are responsible for implementing first aid and medical response plans and preparations (including for adequate training and equipment) for their area of responsibility so that United Nations personnel injured in a road traffic accident can receive adequate medical response as soon as possible (in accordance with applicable medical guidelines). Casualty Evacuation and Medical Evacuation plans are also required and shall be included, along with other road safety requirements, as part of the country security plan, as per Chapter IV, Sections M and R of the *Security Policy Manual* (SPM).

F. Requirements for United Nations Vehicles

14. United Nations vehicles shall be in compliance with the Minimum Operating Security Standards (MOSS) set out in the *Security Policy Manual* (SPM), Chapter IV, Section N, Appendix 1, and paragraphs 5.1 – 5.3.2.[2]

15. In addition to the MOSS requirements, all United Nations vehicles must be equipped with properly functioning, standard safety features, including, but not limited to, seat belts for all driver and passenger seats, headlights, brake lights, signal lights, tires (including spares), special signalling for breakdowns (reflective vests, flares, etc.) and primary and emergency brakes.

16. United Nations system organizations should also consider the procurement of official vehicles with tested and proven safety features including, but not limited to, "Daytime Running Lights (DRL)", "Anti-Lock Braking Systems (ABS)", airbags and systems to alert maximum safe speeds.

17. United Nations vehicles shall be used for official purposes only, unless otherwise authorized.

G. Requirements for Drivers

18. In order to lower the risks from road safety hazards, all persons operating a United Nations vehicle shall:

    (a) Check, before departure and upon return, that the vehicle is in a roadworthy condition, has not been tampered with and that it contains all necessary functioning equipment required by MOSS and other requirements as per Section F above;

    (b) Immediately report all defects in the vehicle and/or its safety-related equipment to the United Nations official responsible for vehicle and transport management in their respective organization;

    (c) Use all safety-related equipment, including that outlined in Section F above, in the proper and prescribed manner;

    (d) Be duly authorized by their respective United Nations system organization to operate the vehicle at the duty station, poses a valid driving licence recognized by the United Nations and/or the host country, possess all required certification not covered by standard driving licences (e.g., for heavy or special use vehicles), and pass any required practical and written driving and road safety tests;

    (e) Be competent to operate the vehicle safely in all local conditions (including snow, ice and sandstorms), to invoke defensive driving techniques as necessary and to use radio/communications equipment properly;

[2] Any safety issues related specifically to armoured vehicles will be dealt with in separate documents on armoured vehicles standards.

(f) Be medically cleared for driving by the United Nations and/or local authorities, including an approved eyesight test at least biennially, and be equipped with the prescribed methods for correcting vision (eye glasses, contact lenses, etc.);

(g) Drive with due care at all times, maintaining the highest level of consideration towards passengers, other road users and pedestrians, including by obeying all national codes, driving regulations and speed limits;

(h) Adjust the speed of the vehicle according to local driving conditions (e.g., low visibility, rain, snow, etc.) to ensure a safe speed at all times and a safe distance from other vehicles on the road;

(i) Wear their seatbelt and advise passengers to also wear seat-belts;

(j) Not operate the vehicle, in any situation or in any circumstance, under the influence of any substance that may impair their ability to operate the vehicle, including, but not limited to, alcohol, drugs, narcotics, psychotropic, chemical substances and medicines;

(k) Not operate the vehicle knowing that his/her ability to do so safely has been impaired, affected or influenced by illness, fatigue or injury;

(l) Abstain from activities that would interfere with, or distract from, their exercising full control over the vehicle, including, but not limited to, consuming food/beverages or smoking while the vehicle is in motion;

(m) Refrain from operating radios, mobile cellular phones[3] or other communications devices while the vehicle is in motion, except where necessary as a security requirement and there are no other options;

(n) Use other safety equipment as a vehicle may require, such as wearing helmets while operating motorcycles, mopeds, etc.;

(o) Strictly adhere to any local security instructions regarding travel;

(p) Ensure that no firearms are brought into or are transported in the vehicle, unless expressly permitted by the United Nations;

(q) Report any request, order or pressure by anyone for the driver to violate the provisions of this policy.

H. Requirements for Passengers

19. In order to lower the risk from road safety hazards, all passengers of a United Nations vehicle shall

(a) Wear seat belts at all times while in the vehicle and not occupy a seat that is not fitted with a properly functioning seatbelt. In a security crisis situation, the number of passengers may exceed the number of seatbelts available;

(b) Use other safety equipment as the vehicle may require, such as wearing helmets while a passenger on motorcycles, mopeds, etc.;

[3] This provision includes speaking, texting or other uses.

(c) Not request, order or otherwise pressure the driver of the vehicle to violate any of the requirements as laid out in Section G above, including by conducting any required communication checks during the movement to release the driver of this obligation;

(d) Not smoke or consume alcoholic beverages in the vehicle;

(e) Strictly adhere to other security instructions regarding travel;

(f) Report any observed dangerous or unsafe driving by United Nations drivers to the appropriate United Nations official in charge of managing the vehicle fleet and the applicable United Nations security official (passengers have the right to refuse transportation in United Nations vehicles if they have a reasonable belief that the vehicle is not roadworthy or that the driver is not in a condition to operate the vehicle safely).

I. Response in the Event of a Road Traffic Accident

20. When a United Nations vehicle is involved in a road traffic accident, the United Nations driver (or other occupants if the driver is incapacitated) shall

(a) Remain at the accident scene until directed otherwise by local authorities, unless his/her personal safety, or the safety of the occupants, is manifestly endangered or local United Nations security protocols determine another course of action;

(b) If there are any persons injured, call for medical aid and take all necessary action to render the accident site safe, including rendering first aid to injured persons as he/she is qualified to administer. United Nations vehicles may be used to transport injured persons to medical assistance only under the direct request of medically-trained personnel;

(c) Report the accident as soon as possible to the United Nations official in charge of managing the vehicle fleet and the applicable United Nations security official. Local police authorities must also be informed as soon as practically feasible. United Nations security officials are responsible for liaising with the police authorities handling the case;

(d) Gather as much information as possible to assist the United Nations investigation of the incident;

(e) Not admit any personal liability or any liability on the part of the United Nations;

21. The driver must report road traffic accidents involving the vehicle. The accident report shall be submitted in accordance with existing guidelines.

J. Enforcement

22. In the event of an investigation into a road traffic accident, findings that any occupants of a vehicle have failed to abide by the terms of this policy may lead to administrative or disciplinary proceedings.

K. Final Provisions

23. This policy is meant to be distributed to all United Nations personnel.

24. This policy enters into force on 31 October 2011.