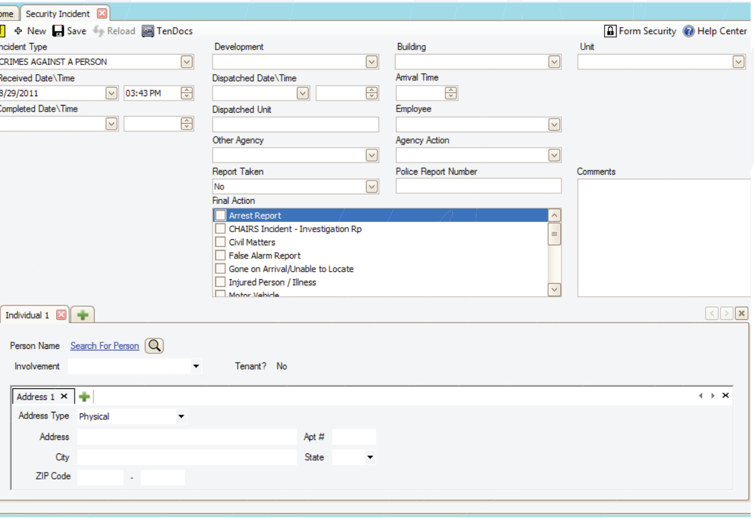
CHAPTER V

Compliance with Security Policies and Procedures



ncident Type: CRIMES AGAINST A PERSON

Received Date\Time: 3/29/2011 03:43 PM

Completed Date\Time:

Development:

Dispatched Date\Time:

Dispatched Unit:

Other Agency:

Report Taken: No

Final Action:

- □ Arrest Report
- □ CHAIRS Incident - Investigation Rp
- □ Civil Matters
- □ False Alarm Report
- □ Gone on Arrival/Unable to Locate
- □ Injured Person / Illness
- □ Motor Vehicle

Building:

Arrival Time:

Employee:

Agency Action:

Police Report Number:

Unit:

Comments:

Person Name: Search For Person

Involvement:

Tenant? No

Address Type: Physical

Address:

Apt #:

City:

State:

ZIP Code: -

Section B

SAFETY AND SECURITY INCIDENT REPORTING SYSTEM (SSIRS)

Promulgation 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**.**