

THE SECURITY INCIDENT INFORMATION MANAGEMENT HANDBOOK



THE HANDBOOK

The SIIM Handbook is intended to support users in establishing and developing effective information management for security event reporting and monitoring systems, both internally and externally, across organisations and the sector. It is structured around four objectives and seeks to make an important contribution in advancing practices related to security incident information management within non- governmental organisations.

Downloadable on our website www.redr.org.uk

GUIDANCE COVERING



Objective one: to inform immediate reaction and response to a security incident. The purpose is to ensure that information is sought and used to inform the immediate response to the incident.



Objective two: to implement lessons learned after a security incident for follow-up action and prevention. The purpose is to understand what happened with a view to planning and implementing any necessary changes and procedures that will help to treat the risk of similar future events, with a particular focus on prevention.



Objective three: to understand the NGO security context. The purpose is to improve contextual knowledge by using internal and external incident data. This will help inform strategic decisions, global communication and self-reflection among aid agencies.



Objective four: to inform strategic decision-making in an organisation. The purpose is to take stock of the changing nature of incidents, to understand the most challenging working environments, the organisation's overall exposure to risk, and to identify the best strategic responses.

TOOLS PROVIDED

Tool 1: SIIM self-assessment grid

Tool 2: Typology of incidents

Tool 3: Organisational or external incident

Tool 4: Incident reporting template

Tool 5: Incident analysis grids

Tool 6: How to conduct a factual debrief

Tool 7: Good practice in gender-sensitive incident reporting and complaints mechanisms for reporting sexual exploitation and abuse (SEA)

Tool 8: Action plan

Tool 9: SIIM systems

Tool 10: Incident storing

Tool 11: Technology to report and record incidents

Tool 12: Analysing data trends

Tool 13: Strategic-level questions for incident management

The SIIM project is a 21-month project funded by EU Humanitarian Aid. A collaboration between RedR, Insecurity Insight and EISF, it aims to increase sharing of security incident data across the humanitarian sector by building the capacity of organisations to accurately report and record security incidents.

