Model job description

# Information Security Incident Manager

## Scope, purpose and nature of role

Managing the discovery, handling, resolution and learning points from information security incidents requires a professional, structured approach. The organization needs a [full or part-time] Incident Manager to take charge of investigating and resolving information security incidents as they occur, draw out the lessons from incidents and prepare the organization to cope more effectively with future incidents. Since information security incidents can affect any part of the organization, this will involve working with and coordinating colleagues in Information Security, Physical Security, Human Resources, Legal, IT, Privacy *etc*. plus, on occasions, external experts and authorities, as well as liaising with local management and keeping them informed if not involved in the incident resolution. The Incident Manager will form and lead *ad hoc* teams, prepare policies, procedures, status updates and post-incident reports and take charge confidently when the organization is in or is facing a crisis.

## Distinguishing characteristics of the ideal candidate

The following personal characteristics are high on our wish-list:

* A “rock” – stays cool, calm and collected under pressure, exuding an air of confidence;
* Decisive – able to make difficult decisions, prioritize and take appropriate action without prevaricating or unduly delaying, yet willing to be held to account for those decisions and actions, and willing to seek and accept advice from subject matter experts where necessary;
* A natural leader – someone who effortlessly commands authority and respect;
* Likes a challenge – responds positively under difficult circumstances, handles stress well;
* Supportive of team members and colleagues working under stress.

## Relevant qualifications, skills and experience

The following qualifications and experience are considered relevant and desirable for this role:

* **Information or IT security management:** CISSP, CISM, masters or undergraduate degree; at least 5 years’ work experience; some exposure to ISO/IEC 27001 and ITIL;
* **Incident/crisis management:** extensive experience as an incident management team member;
* **General:** at least 10 years’ cumulative employment record post school/academic studies including at least 5 years’ management, supervisory or team leader experience involving man-management, budgetary management, mentoring, relationship management *etc*.; competent at writing effective, professional business communications such as policies, procedures, contemporaneous status updates and management reports such as post-incident reviews.

Candidates must be willing to undergo background checks to verify their identity, character, qualifications, skills and experience.