

Rev 0

# **Security Procedure: Incident Management Procedure**

This policy / procedure complies with the requirements of the ISO 27001:2013 International Standard

Annex A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7

## 1. PURPOSE

This document defines the policy and establishes the procedure for the identification, remediation, analysis, and prevention of security incidents relating to compromise or breach of protected information and related systems at [Company Name].

## 2. SCOPE

This policy applies security incidents affecting all [Company Name] owned and customer-owned information assets managed facilities, networks, systems, and technology assets that store, process or transmit information within the scope of the Information Security Management System (ISMS).

## 3. POLICY

It is the policy of [Company Name] that security incidents are defined, and that ongoing monitoring and detecting of security incidents leads to swift identification, containment, and resolution. Our goal is always protecting the confidentiality, integrity, and availability of all information within the scope of the ISMS as well as the systems and processes that store, process and transmit that information.

## 4. RESPONSIBILITIES (A.16.1.1)

Roles and responsibilities regarding specific access assignments are as follows.

- The **Senior Security Lead (insert other titles here and throughout as appropriate)** is responsible for:
  - maintaining and assuring that the incident management process is faithfully followed;
  - appropriate logs and records are maintained;
  - company management is notified and remains informed
  - law enforcement or regulatory agencies are notified and informed as required.

Rev 0

- timely resolution of individual incidents;
- collection of incident information and evidence to support ongoing continuous improvement and risk reduction.
- **Incident Managers** are assigned to manage assigned incidents from point of identification through resolution.
- Employees and system users are responsible for:
  - identifying and reporting security incidents immediately upon detection;
  - supporting the efforts of remediation, analysis, and prevention measures that they may be directly or indirectly affected by under the leadership of the Incident Manager.
- Adherence to this policy is a requirement of employment at [Company Name]. (See **HR Security Policy**).
- Awareness training for this policy is provided through the **Security Awareness Training** program.

## 5. PROCEDURES

### Identifying and reporting information security events and weaknesses (A.16.1.2, A.16.1.3)

Employees and contractors have a duty to be aware of the types of information security incidents and to report them immediately to the **Senior Security Lead**.

Information security incidents are any events that threaten the confidentiality, integrity, or availability (CIA) of in-scope information. Events that might constitute a security incident include:

- Penetration or compromise of a system by an unauthorized agent thereby granting unauthorized access to protected information.
- Unintentional human errors leading to a breach, such as sending an email containing unencrypted personally identifying information or clicking on a dangerous link in a phishing email.
- Loss or theft of information or a controlled asset.
- Intentional human actions such as sharing login credentials that grant unauthorized access to systems.

Rev 0

- Unauthorized physical entry of office or data center.
- Hardware failures impacting CIA.
- Software failures impacting CIA.

Employees and contractors also have a duty to be aware of potential weaknesses and vulnerabilities in systems or processes that might potentially be exploited and cause a security incident. Weaknesses should also be reported to the **Senior Security Lead**.

Examples of potential weaknesses or vulnerabilities include:

- Unlocked physical access points (doors, windows).
- Sensitive information left unattended (paper or electronic).
- Sharing of login credentials.
- Unlocked cabinets containing sensitive data.

## Assessment of and decision on information security events (A.16.1.4)

The **Senior Security Lead** takes the following actions when informed of a security event or a potential security weakness:

- The event is recorded in the **Security Incident Log** including time, date, reported by, description of the event or weakness, and the affected facilities, systems, or process.
- Assesses the reported event or weakness and decides whether it should be classified as a security incident based on the real or potential harm to CIA of in-scope protected information.
- For events/weaknesses classified as a security incident (see Response to information security incidents below):
  - Takes immediate remedial action directly or with the help of the **Organizational Controls Lead** and/or the **Technical Controls Lead**. Action will vary depending on circumstances, but its goal is always to immediately prevent further harm.

Rev 0

- Identifies an **Incident Manager** to take responsibility for causal analysis and preventive action. (Note, the **Senior Security Lead** may serve as the **Incident Manager**)
- Notifies law enforcement agencies, if merited by the severity of the incident, with company-management approval. (Reference the **Information Security Manual, Appendix A** for law enforcement contact information.)
- Notifies company management, and other interested parties (including customers) if the incident is externally or customer-facing.
- For events/weaknesses that are not classified as a security incident.
  - Takes any immediate remedial action necessary to resolve the event or reduce the weakness.
- Records actions taken in the **Security Incident Log**.

## Response to information security incidents (A.16.1.5, A.16.1.7)

When an event or weakness are identified as a security incident the **Incident Manager** assures that a complete understanding of the incident cause is established, and that appropriate corrective, preventive, and verification actions are in place, by taking the following steps:

- Collects information and evidence from various sources, as quickly after the incident as possible.
- Assures that the accuracy, integrity, protection, and chain-of-custody of collected evidence is assured by appropriate means.
- Logs all evidence including interview responses from involved or affected individuals.
- Conducts any security forensics analysis, as required.
- ensures that all response activities are properly logged for later analysis;
- communicates status of the investigation to company management.
- Documents factors/events that caused the incident.
- Directs actions to eliminate or reduce causes and to implement preventive changes to systems or processes.

Rev 0

- Verifies that implemented actions have been effective.
- Closes out the security incident in the **Security Incident Log**.

## Learning from information security incidents (A.16.1.6)

The **Senior Security Lead** will periodically analyze the types, volumes costs (if known) of security incidents in order to identify and evaluate trends, high-impact risks, and drive systemic improvement actions aimed at reducing risk levels and increasing the effectiveness of the ISMS.

Results of analyses are reviewed in Management Review meetings and resulting actions tracked in the Corrective Action system.

## 6. ACCESS CONTROL RECORDS

- Security Incident Log

## 7. REFERENCE DOCUMENTS

- HR Security Policy