# Information Security Incident Management

## Table of Contents

## 1. Purpose

Annex A.16 is about management of information security incidents, events and weaknesses.

## 2. Scope

ISO 27001:2013 addresses the lifecycle clearly through A.16.1.1 to A.16.1.7 and it's an important part of the information security management system (ISMS) especially if you'd like to achieve ISO 27001 certification. Let's understand those requirements and what they mean in a bit more depth now.

## 3. Objectives

The objectives of this policy are:

- The objective in this Annex A area is to ensure a consistent and effective approach to the lifecycle of incidents, events, and weaknesses.

## 4. Governing laws and regulations

| Guidance | Section |
|---|---|
| ISO27001:2013 | A.16 (A16.1) |

## 5. Policy Statement

**16.0 outlines the requirements for managing information security incidents.**

organizations of all types and sizes should familiarize themselves with the best practices for preventing and responding to security incidents. Before we look at these individual requirements, it's important to understand what qualifies as information security incidents, and why incident management is important for your organization.

**16.1 Management of information security incidents, events, and weaknesses**

The objective of A.16.1 is to ensure your organization maintains a sound approach to managing and reporting information security incidents, such as breaches, unauthorized disclosure, destruction or loss of information, among others.

**16.1.1 Responsibilities & Procedures**

Prompt and effective action must be taken in the event of a security incident. To ensure this, management responsibilities and procedures should be established. When establishing management responsibilities and developing information security procedures, the following actions should be considered:

- Planning and preparing incident response.
- Monitoring, detecting, analyzing and reporting information security events.

- Logging incident management activities
- Handling forensic evidence
- Assessing and deciding on information security events and weaknesses
- Responding to a security incident, both internally and externally

It is important that all procedures ensure that information security incidents are handled by competent personnel, and that appropriate points of contact, both within and outside of the organization, are identified and established for the handling of information security issues.

Reporting procedures should include the following:

- Reporting forms that support the reporting action and log all necessary actions in the event of an information security event.
- Next steps to be followed in the event of an information security event.
- The formal disciplinary process to be followed in the case of employees who commit security breaches.
- An organized feedback process to ensure that parties concerned are updated on the progress and results of reported information security events.

All those responsible for information security incident management must be made aware of these processes, and all processes must be agreed upon with management.

**16.1.2 Reporting Information Security Events**

A good control here ensures that information security incidents and events can be reported through suitable management channels as soon as possible.

Employees and associated interested parties (e.g., suppliers) need to be made aware of their obligations to report security incidents and you should cover that off as part of your general awareness and training. To do this well they will need to have awareness of exactly what constitutes an information security weakness, event or incident so be clear about that, based on the simple example above. If an information security event occurs or is thought to have occurred, it must be reported immediately to the nominated information security administrator and that needs to be documented accordingly.

Some of the possible reasons for reporting a security incident include ineffective security controls, assumed breaches of information integrity or confidentiality, or availability issues e.g. not being able to access a service.

The auditor will want to see and will be sampling for evidence of awareness of what constitutes a weakness, event or incident amongst general staff, and the awareness of incident reporting procedures and responsibilities.

### 16.1.3 Reporting Information Security Weaknesses

This control simply builds on incidents and events but might be treated slightly differently once reported (see A.16.1.4) It is essential for employees to be aware of the fact that when discovering a security weakness, they must not attempt to prove that weakness, as testing it may be interpreted as a misuse of the system, whilst also risking damaging the system and its stored information, causing security incidents.

### 16.1.4 Assessment of & Decision on Information Security Events

Information security events require assessment before being classified as “incidents”. Established points of contact must evaluate information security events using an agreed-upon classification scale to assess the impact and extent of the event, and whether it qualifies as a security incident. The results of this assessment must be recorded for future reference and verification purposes. In summary, this process can be broken down into the following stages:

1. Identification, prioritization, and assessment
2. Containment
3. Investigation/ “root cause” analysis
4. Response
5. Follow up.

### 16.1.5 Response to Information Security Incidents

It is always good to assign owners, be clear on actions and timescales, and as with everything for ISO 27001, retain the information for audit purposes (also essential if you have other stakeholders and regulators to consider). The individual placed in charge of dealing with the security event will be responsible for restoring a normal level of security whilst also.

- collecting evidence as soon as possible after the occurrence.
- conducting an information security forensics analysis (grand term but at least being clear on root cause and related aspects or what happened and who was involved, why etc.)
- escalation, if required, for example to relevant regulators.
- ensuring that all involved response activities are properly logged for later analysis.
- communicating the existence of the information security incident or any relevant details to the leadership for them to be further communicated to various individuals or organizations on a need-to-know basis; and
- dealing with information security weaknesses found to cause or contribute to the incident.

### 16.1.6 Learning from Information Security Incidents

This is an important control, and your policy needs to demonstrate that knowledge gained from analyzing and resolving information security incidents will be used to help reduce the likelihood or

impact of any future incidents. As part of the commitment to continuous service improvement, you should ensure that you learn from the lessons of any security incident to therefore help evolve and adapt the ISMS to meet the changing landscape that is worked in.

Once an incident has been resolved, it should be placed into a status of review and learning, where the lead responder for that incident will discuss any changes required to the processes of the ISMS policies as a result. Any relevant recommendations should then be put to the ISMS Board for further discussion. Once the review and learning has been completed, updates have been made to the policies as required, the relevant staff must be notified and re-trained if required, and the cycle of information security awareness and education continues.

### 16.1.7 Collection of Evidence

Procedures are required for identifying, collecting, acquiring, and preserving information. This evidence can be used to decide on disciplinary and/or legal action, and internal procedures should take the following into account:

- Chain of custody
- Safety of evidence
- Safety of personnel
- Roles and responsibilities of personnel involved.
- Competency of personnel
- Documentation
- BBriefing

Whenever possible, the value of evidence should be strengthened with certification or other relevant supporting resources.

## 6. Non-Compliance

Non-Compliance is described by the standard as any situation in which there is a requirement that is not being fulfilled (i.e., not generating backup copies when needed, as established in the Backup Policy). Both a security event and a security incident can also be considered as non-compliance.

Properly defining security events, incidents and situations of non-compliance will allow your organization to strategically protect itself from security threats and possible regulatory and reputational risks.

## 7. Exceptions

Exception to this policy is to allow and not mention an incident in situation when the impact is low.

## 8. Revision History

| Version ID | Date of Change | Author | Rationale |
|---|---|---|---|
| | | | |

| | | | |
|---|---|---|---|
| | | | |
| | | | |
| | | | |