[Organization logo]

[Organization name]

Commented [270011]: All fields in this document marked by square brackets [ ] must be filled in.

INCIDENT MANAGEMENT PROCEDURE

Commented [270012]: To learn more about this topic, read this article:

- How to handle incidents according to ISO 27001 https://advisera.com/27001academy/blog/2015/10/26/how-to-handle-incidents-according-to-iso-27001-a-16/

Code:	
Version:	
Date of version:	
Created by:	
Approved by:	
Confidentiality level:	

Commented [270013]: The document coding system should be in line with the organization's existing system for document coding; in case such a system is not in place, this line may be deleted.

Change history

Date	Version	Created by	Description of change
	0.1	27001Academy	Basic document outline

Table of contents

1. Purpose, scope and users

The purpose of this document is to ensure quick detection of security events and weaknesses, and quick reaction and response to security incidents.

This document is applied to the entire Information Security Management System (ISMS) scope, i.e. to all employees and other assets used within the ISMS scope, as well as to suppliers and other persons outside the organization who come into contact with systems and information within the ISMS scope.

Users of this document are all employees of [organization name], as well as all abovementioned persons.

Commented [270014]: Include the name of your organization.

2. Reference documents

- ISO/IEC 27001 standard, clauses 7.4, A.5.7, A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.4, and A.6.8
- Information Security Policy
- [List of Legal, Regulatory, Contractual and Other Requirements]

Commented [27A5]: You can find a template for this document in the ISO 27001Documentation Toolkit folder "05_General_Policies".

Commented [270016]: If you don't have this List, then list in these bullets the legislation and contracts that have requirements related to incident management.

3. Incident management

An information security incident is a "single or a series of unwanted or unexpected information

3.1. Receipt and classification of incidents, weaknesses and events

Each employee, supplier, or other third party who is in contact with information, systems, or

Commented [270017]: Include the name of your organization.

1.
2. all other events must be reported to [job title]

Commented [270018]: Include the job title of the person assigned as point of contact.

Commented [270019]: Include the job title of the person assigned as point of contact.

Incidents, threats, weaknesses, and events must be reported as soon as possible, by phone or in person.

Commented [2700110]:

The person who received the information must classify it in the following way:

a)

b)

c) major incident – an incident which can incur significant damage due to loss of confidentiality

3.2. Treatment process for security weaknesses or events

The person who received the information about a security threat, weakness, or event analyzes the information, establishes the cause, and, if necessary, suggests preventive and corrective action.

4. inform persons who were involved in the incident, as well as [job title], about the incident treatment process

The person who received information about a minor incident must log the incident [describe manner of recording it].

Commented [2700111]: E.g., manual, electronic, or automated (e.g., through help desk applications).

3.4. Treating major incidents

Commented [2700112]:

3.5. Learning from incidents

Commented [2700113]: Delete this item if control A.5.27 is marked as inapplicable in the Statement of Applicability.

[Job title] must review all minor incidents every three months, and enter recurring ones, or those which may turn into major incidents on the next occasion, in the Incident Log.

3.6. Disciplinary actions

Commented [2700114]: Delete this item if control A.6.4 is marked as inapplicable in the Statement of Applicability.

[Job title] must invoke a disciplinary process for each violation of security rules.

3.7. Collection of evidence

Commented [2700115]: Delete this item if control A.5.28 is marked as inapplicable in the Statement of Applicability.

4. Managing records kept on the basis of this document

Record name	*Storage location*	*Person*	*Controls for record*	*Retention*

		responsible for storage	*protection*	*time*
Incident Log	Shared folder on the intranet	[job title]	Only [job title] has the right to edit the log	3 years

Only [job title] can grant other employees access to the records.

5. Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once every six months.

Commented [2700116]: This is only a recommendation; adjust frequency as appropriate.

When evaluating the effectiveness and adequacy of this document, the following criteria must be considered:

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

6. Appendix

- [illegible]

[job title]
[name]

_____
[signature]

Commented [2700117]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.