[organization logo]

[organization name]

**INCIDENT MANAGEMENT PROCEDURE**

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

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Dejan Kosutic | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc415652617)

[2. Reference documents 3](#_Toc415652618)

[3. Incident management 3](#_Toc415652619)

[3.1. Receipt and classification of incidents, weaknesses and events 3](#_Toc415652620)

[3.2. Treatment process for security weaknesses or events 4](#_Toc415652621)

[3.3. Treating minor incidents 4](#_Toc415652622)

[3.4. Treating major incidents 4](#_Toc415652623)

[3.5. Learning from incidents 4](#_Toc415652624)

[3.6. Disciplinary actions 4](#_Toc415652625)

[3.7. Collection of evidence 4](#_Toc415652626)

[4. Managing records kept on the basis of this document 4](#_Toc415652627)

[5. Validity and document management 5](#_Toc415652628)

[6. Appendix 5](#_Toc415652629)

# 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.

# Reference documents

* ISO/IEC 27001 standard, clauses A.7.2.3, 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
* Information Security Policy
* [List of Legal, Regulatory, Contractual and Other Requirements]

# Incident management

An information security incident is a "single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security" (ISO/IEC 27000:2009).

## Receipt and classification of incidents, weaknesses and events

Each employee, supplier or other third party who is in contact with information and/or systems of [organization name] must report any system weakness, incident or event which could lead to a possible incident in the following way:

1. all information and communication technology-related events must be reported to [job title of point of contact]
2. all other events must be reported to [job title of point of contact]

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

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

1. security weakness or event – no incident occurred, but the event related to a system, process or organization may trigger the occurrence of an incident in the near or further future
2. minor incident – an incident which cannot significantly impact confidentiality or integrity of information, and cannot cause long-term unavailability
3. major incident – an incident which can incur significant damage due to loss of confidentiality or integrity of information, or may cause an interruption in the availability of information and/or processes for an unacceptable period of time

## Treatment process for security weaknesses or events

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

## Treating minor incidents

If a minor incident was reported, the person who received the information must take the following steps:

1. take measures to contain the incident
2. analyze the cause of the incident
3. take corrective actions to eliminate the cause of the incident
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 – manual, electronic or automated (e.g. through help desk applications)].

## Treating major incidents

In the case of major incidents that could disrupt activities for an unacceptable period of time, an [Incident Response Plan as part of the Business Continuity Plan] is invoked.

## Learning from incidents

[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.

[job title] must analyze each incident recorded in the Incident Log (identifying type, relatedness, and cost of incident) and, if necessary, suggest preventive or corrective action.

## Disciplinary actions

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

## Collection of evidence

[job title] will define the rules on how to identify, collect and preserve evidence that will be accepted as evidence in legal and other proceedings.

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Record name*** | ***Storage location*** | ***Person responsible for storage*** | ***Controls for record protection*** | ***Retention time*** |
| Incident Log | Shared folder on the intranet | [job title] | Only [job title] has the right to edit the log | 3 years |
| Rules for identifying, collecting and preserving evidences | Shared folder on the intranet | [job title] | Only [job title] has the right to edit and publish the rules |  |

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

# 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.

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

* number of weaknesses or incidents which were not reported to authorized persons
* number of incidents which were not treated in the most adequate manner
* number of incidents which were not recorded in the Incident Log
* number of incidents for which evidence for legal action was inadequate
* number of violations of security rules where no disciplinary process was invoked

# Appendix

* Incident Log

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]