Information Security Incident Management Policy

This template serves only as an example and does not contain the complete content.

Please contact us for comprehensive advice.

Policy-Owner	<name>
Approval	<name>
State	Draft | Review | Approved
Version	x.x
Valid from	<datum>
Classification	-CLASSIFICATION-

Table of contents

Farblegende Mustervorlage:

Anzupassen an unternehmensspezifische Begrifflichkeiten

Anzupassen anhand der Unternehmensvorgaben (z.B. private Nutzung erlaubt/verboten)

1 General

1.1 Objective

The objective this policy is to define binding rules for the management of information security incidents. The incident management shall follow industry standards, legal and contractual requirements. The following shall be achieved:

- Information security events are detected and efficiently dealt with, deciding when they should be classified as information security incidents.
- Identified information security incidents are assessed and responded to in the most appropriate and efficient manner and within the predetermined time frame.
- The adverse impact(s) of information security incidents on the organization and involved parties and their operations are minimized by appropriate controls as part of incident response.
- Information security vulnerabilities involved with or discovered during the incident are assessed and dealt with appropriately to prevent or reduce incidents. This assessment can be done either by the CDC or other teams within the organization and involved parties, depending on duty distribution.
- Lessons are learnt quickly from information security incidents, related vulnerabilities and their management. This feedback mechanism is intended to increase the chances of preventing future information security incidents from occurring, improve the implementation and use of information security controls, and improve the overall information security incident management plan.

The procedure described includes incidents relating to digital and physical assets, as well as related terms such as cyber security incident response or security incident response.

1.2 Target group

The rules defined in this policy are binding for all employees of the CLIENT including all subsidiaries, locations and affiliated companies worldwide, who are involved into the tasks of incident response (identification, analysis, prioritization, handling, …).

1.3 Violations of rules

Violations of, or disregard of the ruled defined in this policy may be sanctioned. Details are described in the CLIENT Information Security Policy (ISP).

2 Roles and Responsibilities

The roles and responsibilities are defined in the Information Security Policy (ISP) of CLIENT. Beside the roles defined in the ISP the following roles exist within the scope of this policy. Information security is a joint task, even if the responsibilities are assigned to individual roles. Everyone involved should always keep a holistic view.

2.1 Cyber Defence Center (CDC)

The Cyber Defence Center has the primary responsibility for managing all phases of security events, incidents, and breaches.

For CLIENT a CDC organizational structure (at least a virtual team) shall be defined and documented. The structure can be derived from the ENISA (European Union Agency for Cybersecurity) CSIRT (equal to CDC) maturity framework and good practices.

Figure 1: ENISA Example of a small CDC structure

"Smaller [CDCs] of up to five to seven people are mostly organised as one unit run by a unit manager. In this case, staff roles may be based on the NIST NICE framework's Cyber Defence Incident Responder work roles (PR-CIR-001) (36)."

NICE Cybersecurity Workforce Framework Work Roles

2.2 Chief Information Security Officer

Responsibilities of the Chief Information Security Officer (CISO) are described in CLIENT's Information Security Policy. With focus on incident response:

- Establishing and improving the information security culture across CLIENT.
- Facilitate the understanding of potential threats, vulnerabilities, and control techniques across CLIENT.
- Monitor information security trends internal and external to CLIENT and keep the Managing Director informed of information security related issues and activities affecting the organisation.
- Sponsor the Cyber Defence Center and ensure appropriate resources for incident response.

2.3 Data Protection Officer

With focus on incident response the Data Protection Officer (DPO) is responsible for the following:

- Classification of incidents as a personal data breach
- Determines if any reporting obligations arise from a personal data breach and associated laws (i.e. employees, customers, data subjects, data protection authorities)
- Owns legal assessment on global data protection laws and regulations (final decision on the interpretation of data protection laws and regulations)
- Coordination with data protection authorities
- Documentation of personal data breaches according to applicable law
- Ensures proper data protection training (including written guidance) for all stakeholders involved in incident response

2.4 IT Operations

- Provides impact assessment and proposed recovery approaches.
- Support includes, but not limited to:
  - CDC's chosen mitigation and recovery actions,
  - Attribution of assets within the environment,
  - Technical continuity activity,
  - Execution of response actions, as directed
- Strengthening/amending global security policies based on weaknesses identified during an incident.

4.1 Type of incidents

Confidentiality

Information leaks may have immediate effects on an organization, and may make information irretrievably available to unauthorized attackers and/or criminals.

One shall hence “close the doors” (= stop the leak, fill the breach) and prevent future breaches by identifying the place where it happened and its cause.

Integrity

Integrity incidents (unduly modified information) shall be detected and corrected before the information is published and/or used.

Prevention is necessary by identifying the cause.

Availability

Unavailability of information (unreachable, unusable, wiped or disappeared information) could create effects in relation with the SLA and the RPO. The information shall be found and recovered before the business effect is unacceptable.

Example: a financial report that has to be submitted to the fiscal authorities by a certain point in time cannot be transmitted in a timely manner.

Access control

Unauthorized access leads to system compromise, theft of resources, and information breach.

Future occurrences shall be prevented by identifying underlying exposures and causes and, where applicable, review of access control permissions (authorization, authentication, roles, privileges, network access, etc.)

Vulnerabilities

A technical, people or procedural vulnerability, such as an incorrect allocation of access rights, may allow for successful exploitation.

Examples of vulnerabilities include:

- Unpatched server, machine or outdated software
- Insufficient protection of assets (information, equipment, rooms) with regards to the criticality.

Technical failure

Technical failures render the ICT or physical device inoperative or unusable. It creates either a vulnerability or potential breach of the SLA and the RTO.

Theft or loss of equipment

Theft and loss of equipment, principally those containing information, shall be considered as availability and/or confidentiality incidents.

This template serves only as an example and does not contain the complete content.

Please contact us for comprehensive advice.

5 Incident response process

The process for handling security incidents at CLIENT consists of the following phases (based on ISO 27035)

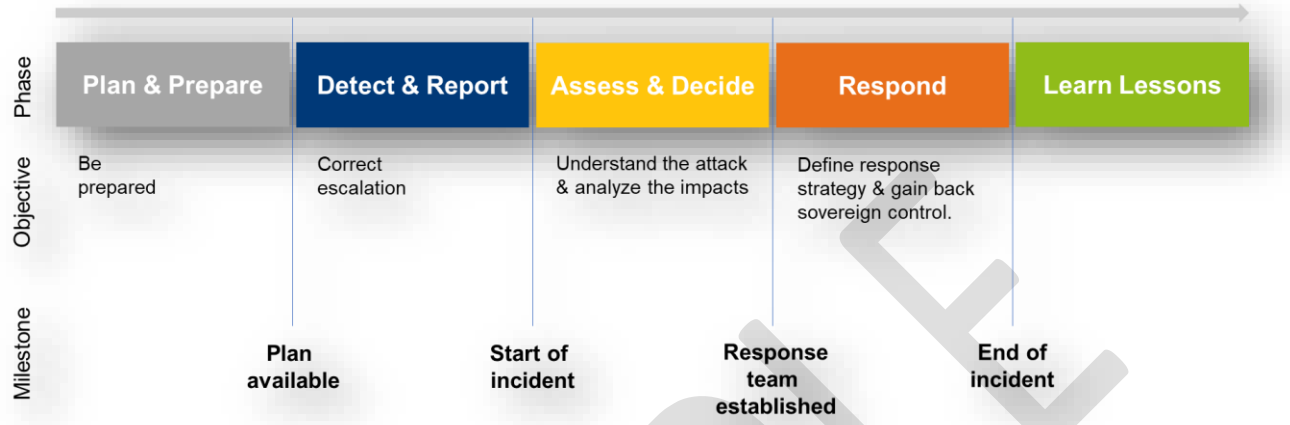


Figure 3: Incident response process

5.1 Plan and prepare

The preparation phase describes the steps taken to ensure preparedness for an incident. Steady-state time is an ideal for team members to further develop their skills, test new tools and techniques, and exercise the response capability to improve enterprise-wide adoption. The prepare phase is driven by incident response best practices, and the following objectives shall be fulfilled:

- Drive process improvements for the incident response capability, including the revision of processes, development of partnerships, and integration of new detection and response technology.
- Conduct incident response exercises to test established processes and the capabilities of personnel responsible for carrying out incident response.
- Drive enterprise-wide adoption of incident response processes by facilitating workshops and socialization sessions.
- Maintain contact lists, response plans, asset data bases.
- Attend specialized trainings and acquire certifications as necessary.
- Develop and document an information security incident management plan.
- Establish a Cyber Defence Center.
- Establish relationships and connections with internal and external organizations.
- Determine technical and other support (including organizational and operational support).
- Plan and provide information security incident management awareness and skills training for all roles.
- Test information security incident management plans and runbooks.

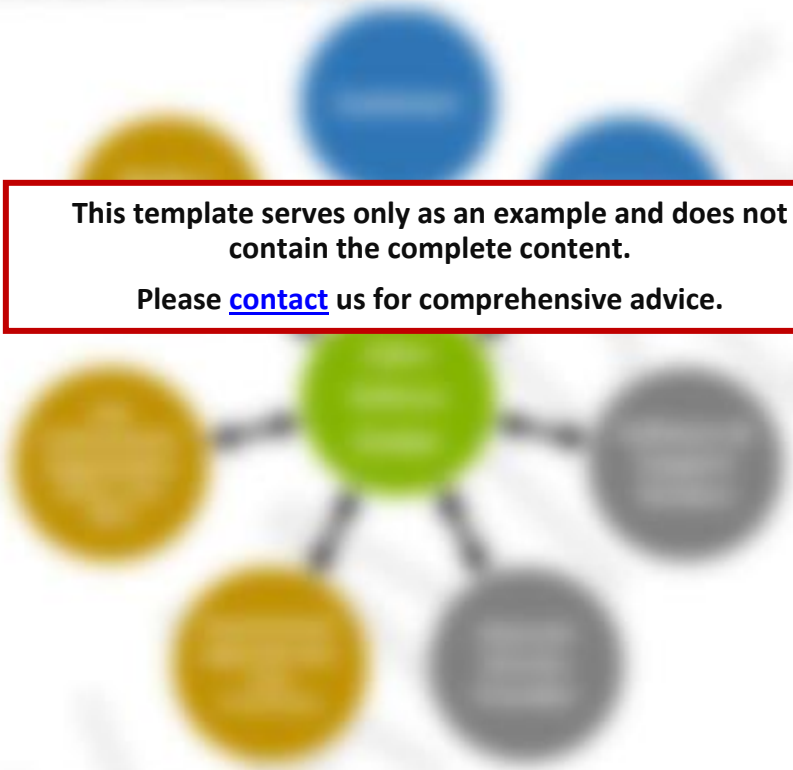
Security incident runbooks (structure in appendix: Runbook template) shall be created for the threats to be identified via threat intelligence activities and risk management. These are currently the scenarios:

- Phishing
- Malware

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

[illegible]

[illegible]



[illegible]

5.2 [illegible]

[illegible]

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

Ready to set up your ISMS?

Let's get started together!

Contact us now for individual advice and support.