Information Security Incident Management Policy

Diese Vorlage dient lediglich als Beispiel und beinhaltet nicht den kompletten Inhalt.

Für eine umfassende Beratung kontaktieren Sie uns gerne.

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

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 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 ISF 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 ISF Information Security Policy (ISP).

2 Roles and Responsibilities

The roles and responsibilities are defined in the Information Security Policy (ISP) of ISF. 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 ISF 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 ISF's Information Security Policy. With focus on incident response:

- Establishing and improving the information security culture across ISF.
- Facilitate the understanding of potential threats, vulnerabilities, and control techniques across ISF.
- Monitor information security trends internal and external to ISF 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.

Bereit, Ihr ISMS aufzubauen?

Lassen Sie uns gemeinsam starten!

Kontaktieren Sie uns jetzt für eine individuelle Beratung und Unterstützung.