Akeron
Modern applications by business experts

Akeron & Akeron Lab

Information Security Incident Management Policy

Release date: 30 April 2024
Protection level: Public

Identification: AK 20

Date	Description of Changes	Rev. n°
30/04/2024	First issue for ISO 27001:2022	00
16/06/2024	Corrected typo, revised definitions	01
		02
		03

Akeron Lab S.r.l.
Via di Vorno 16, 55060 Capannori
t. +39 0683 1748200 | P.Iva 02215000460
info@akeron.com

Akeron S.r.l.
Via Farnesi 141, 55100 Lucca
t. +39 0583 15284 | P.Iva 01286330467
info@akeron.com

The Information Security Incident Management System encompasses all products and services offered by Akeron and is aimed at:

- Ensuring compliance with the requirements of ISO/IEC 27035-2:2023
- Ensuring compliance with mandatory requirements
- Reducing physical and/or monetary damage
- Reducing personal injury
- Reduce other business impacts(legal and regulatory impact, impact on service delivery, damage to the company's reputation, etc.).

The Corporate Information Security Incident Management Policy is part of the Integrated Management System, which covers:

DESIGN, DEVELOPMENT, SALE, CONFIGURATION AND SUPPORT OF MANAGEMENT AND PERFORMANCE MANAGEMENT SOFTWARE SOLUTIONS IN MANAGED MODE OR SAAS (SOFTWARE AS A SERVICE) ENVIRONMENTS IN COMPLIANCE WITH ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27035 GUIDELINES

The Policy applies to all Akeron personnel involved in the preparation, planning, detection, reporting, evaluation, decision making, response of Information Security incidents. This Policy is reviewed annually or when there are particular changes that affect the Policy.
This policy follows ISO 27035-2:2023, an extension applied to the Information Security Management System in accordance with ISO/IEC 27001:2022.

The importance of managing information security incidents for the organisation is linked to the creation of an environment that is aware of the importance of security and the related risks, through the direct commitment of business leaders to ensure that the objectives defined above are achieved.

The direct commitment of the company's managers is made evident by their involvement in the critical stages of the process and by the allocation of appropriate resources to achieve the stated objectives.

The company has drawn up an incident management plan, in addition to other documented information such as internal procedures and work instructions related to the Information Security Management System.
The security incident management process adopted by Akeron includes the following sub-processes, described in the following paragraphs:

- **Security event detection**: activity aimed at monitoring, analysing, tracking and classifying security events;
- **Security event management**: activity aimed at countering security breaches related to a given security event or incident, including damage assessment and restoration to the standard conditions

Akeron Lab S.r.l.
Via di Vorno 16, 55060 Capannori
t. +39 0683 1748200 | P.Iva 02215000460
info@akeron.com

Akeron S.r.l.
Via Farnesi 141, 55100 Lucca
t. +39 0583 15284 | P.Iva 01286330467
info@akeron.com

preceding the incident. Depending on the classification of the event (event, incident or false positive), the relevant management method is applied;

- **Post-accident analysis**: activity aimed at analysing the conditions that led to the accident in order to formulate an improvement plan act with the aim of reducing the risks of new accidents of similar nature;
- **Lesson learnt and continuous improvement**: activity aimed at continuous improvement of the entire Incident Management process.

Definitions	Description
Malevolent agent	An individual who, by exploiting the vulnerabilities inherent in an asset or by exploiting his or her knowledge arising from the organisational role he or she holds, intentionally or accidentally causes a breach of the security policies applied to the asset.
Post-incident analysis	Set of activities aimed at collecting and analysing evidence to establish the causes, context and manner of implementation of a security breach that can be classified as a security incident.
Criticalities	Set of adverse circumstances resulting from the concurrence of events that constitute a threat to the security of a given context.
Availability	Property of the information to be accessible and usable by authorised personnel, at the times, places and in the manner appropriate to the operational needs of the company.
Security Event	Any significant occurrence or event that takes place within a specific information asset or the company's information assets, detected by automated or non-automated means, which, due to its potential impact on the company's information assets, requires immediate action or response to ensure the protection, integrity and availability of information critical to the organisation.
Security Incident	Any event or set of events implying a breach of security policies causing damage to the company's information assets.
Integrity	Property of information to be present, correct and valid.
Monitoring of Security Events	Set of continuous, organised, controlled and documented activities aimed at detecting security events, also with the aid of automatic instruments.
Threats	Set of malicious events that may facilitate a breach of security policies and damage to the company's information assets.
Information assets	Set of capital goods, tangible and intangible, which are of significant value for the fulfilment of the company's mission. The information assets consist of the following types of resources: • Technological resources: systems, equipment, hardware and software infrastructures used as tools to support the company's processes; • Information: a set composed of an aggregation of elementary data, or other logically related information, functional to the performance of the company's processes;

Akeron Lab S.r.l.
Via di Vorno 16, 55060 Capannori
t. +39 0683 1748200 | P.Iva 02215000460
info@akeron.com

Akeron S.r.l.
Via Farnesi 141, 55100 Lucca
t. +39 0583 15284 | P.Iva 01286330467
info@akeron.com

	• Human resources: individuals inside or outside the organisation who, through their cognitive and professional assets, contribute to the performance of the company's processes within a predefined framework of skills and responsibilities; • Innovations, inventions, copyrights and patents: any element attributable to the organisation's scope of ownership that constitutes a source of advantage for the performance of the business mission and related processes.
Confidentiality	Characteristic of information to be knowable only to certain authorised parties.
Security breach	Action or set of intentional or accidental actions taken by a malicious agent that result in the circumvention or inhibition of security policies applied to a specific asset or information asset.
Vulnerability	Characteristic element of a given asset or information asset that could be exploited by malicious agents to make a breach of security policy and/or to damage the company's information assets.

For details of the various types of security incidents and how to report them, please refer to the dedicated Incident Management Procedure.
As described in detail in the procedure, the incident management process flow includes:

- planning and preparation
- detection
- reporting
- evaluation and decision-making
- response
- lessons learnt

Incident resolution is not only limited to restoring correct functionality, but is aimed at removing the causes, deepening the content of lessons learnt with a view to continuous improvement of the Information Security Incident Management process.

In the process of managing information security incidents and related activities, the Incident Response Team (hereafter IRT) is involved.

The IRT is the group responsible for the organisation's incident management capability, coordinated by the Incident Response Team Manager (hereafter IRT Manager).

- The **IRT** is responsible of:
  - Monitoring security events (during standard working hours) by ensuring the analysis and classification of events;
  - Collecting and evaluate all communications, verbal or written;
  - Tracking information gathered during event monitoring activities in an event sheet;
  - Supporting the IRT Manager in defining the treatment plan for non-pre-coded events;
  - Implementing treatment actions for pre-coded events, according to the relevant operational instructions approved by the IRT Manager and activating, where necessary, the Involved Functions responsible for systems management;

Akeron Lab S.r.l.
Via di Vorno 16, 55060 Capannori
t. +39 0683 1748200 | P.Iva 02215000460
info@akeron.com

Akeron S.r.l.
Via Farnesi 141, 55100 Lucca
t. +39 0583 15284 | P.Iva 01286330467
info@akeron.com

- Ensuring an adequate degree of effectiveness/efficiency of the systems for detecting, tracking and reporting security events;
- Evaluating and applying tuning actions to the platforms within its competence to deal with false positives;
- Defining, under the coordination of the IRT Manager, counter/containment actions for the treatment of events classified as occurrences or incidents;
- Collecting under the coordination of the IRT Manager the evidence and/or logfiles and apply changes to the platforms under its responsibility, involving the relevant functions if necessary;
- Dealing with events classified as Incidents, taking care of sending to the IRT Manager the incident report containing all relevant information for handling them;
- Supporting the IRT Manager in post-incident analysis activities, in collecting evidence useful for the definition of the causes, modes of implementation and damages suffered by ICT infrastructures;
- Coordinating the Involved Functions in the implementation of counter/containment measures for the handling of security incidents and events;
- Following security incidents, performing the following activities under the coordination and supervision of the IRT Manager:
  - Assessment of possible damage to the information assets and/or ICT assets affected by the incident;
  - Detection of damage, involving if necessary the Functions involved in the management of the ICT systems affected by the incident;
  - Drafting the incident report;
  - Drafting of the incident treatment and recovery plan.
- Formally closing the event sheets, updating the Incident Management Support Knowledge Base;
- Reporting to the IRT Manager, on a regular basis, on the management of security events, taking care to provide data on events, incidents and false positives during the reporting period.

- The **IRT Manager** is responsible for:
  - Defining operational instructions for the counteract/containment/processing of pre-coded events, involving, where necessary, the Involved Functions responsible for managing the systems;
  - Approving the strategy for counteracting and containing events and incidents, coordinating the IRT in subsequent treatment activities;
  - Supervising and coordinating the IRT's activities in the event of security incidents in defining the treatment and recovery plan, ascertaining the damage incurred, collecting evidence and drafting the incident report;
  - Formally approving the recovery plan drawn up by the IRT in the event of a security incident;
  - Assessing the degree of invasiveness of law enforcement/containment actions for incidents taken under management;
  - Coordinating the Involved Functions in the management of ICT systems affected by a security incident in the implementation of activities to restore them to standard conditions (prior to a security incident), with regard to the systems under the Functions' responsibility;
  - Notifying all parties involved (internal and external to the IRT) of the outcome of remedial actions;
  - Receiving event cards sent by the IRT;
  - Carrying out post-accident analysis in order to enable the proper implementation of the safety risk management improvement process, requesting the intervention of the IRT and external specialists if necessary;

Akeron Lab S.r.l.
Via di Vorno 16, 55060 Capannori
t. +39 0683 1748200 | P.Iva 02215000460
info@akeron.com

Akeron S.r.l.
Via Farnesi 141, 55100 Lucca
t. +39 0583 15284 | P.Iva 01286330467
info@akeron.com

- Receiving security status and incident management progress reports from the IRT;
- Defining and periodically reviewing the security incident handling and management process, in such a way as to ensure an adequate degree of effectiveness and efficiency of the process itself, in accordance with the set risk handling objectives;
- Conducting periodic review of the Incident Management procedure;
- Producing and sending to High Management and the Security Officer (CSO) reports on the event handling and security Incident Management process.
- Approving the recovery plan in case of security incidents;
- Managing reporting on security status and progress of incident management activities.

- The **Involved Functions** are responsible for:
  - Ensuring, within its area of responsibility, the implementation of measures to combat/contain security incidents and events, based on the instructions issued by the IRT;
  - Ensuring, within its area of competence and responsibility, the proper performance of the activities necessary to restore the standard service conditions following a security incident, based on the instructions given by the IRT;
  - Supporting the IRT in carrying out analyses of security incidents and events, following the requests made by the personnel in charge of this task;
  - Supporting the IRT Manager in carrying out post-accident analyses, following the requests made by the personnel in charge of this task.

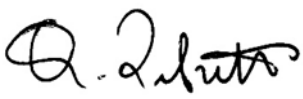
Company personnel help detect, analyse and respond to information security incidents.

Oversight of the information security incident management process is ensured by the monitoring defined in the appropriate internal company procedures, in addition to periodic IRT monitoring.

Depending on the incident category, the company may benefit from the collaboration of qualified vendors who can cooperate with the IRT in resolving information security incidents.
If necessary, therefore, the company can possibly turn to other organisations that can provide specific external support, such as forensic teams, legal advisers, etc.

Lucca, 30/04/2024

Signature for review and approval:



Akeron Lab S.r.l.
Via di Vorno 16, 55060 Capannori
t. +39 0683 1748200 | P.Iva 02215000460
info@akeron.com

Akeron S.r.l.
Via Farnesi 141, 55100 Lucca
t. +39 0583 15284 | P.Iva 01286330467
info@akeron.com