# Caverion Information Security Policy

## Caverion Guidelines

Internal

# Contents

# SUMMARY

- The objective of information security management is to ensure faultless operation of business functions.
- Information security management is an activity within the corporate governance framework which provides direction for security activities and ensures that objectives are achievable.
- Caverion's management demonstrates commitment to continuous information security management improvements by approval of this information security policy and regular management review meetings.
- This information security policy applies to Caverion globally, but also takes into consideration the applicable local legislation and procedures in every operating country.
- This policy applies to all Caverion employees, externals and anyone who processes information that Caverion owns or is responsible for.
- Caverion Group IT is responsible for planning, executing and monitoring the information security management system (ISMS) across Caverion.
- All Caverion employees must be familiar with the information security policy and guidelines and comply with them.
- The required controls to ensure the right level of information security are designed to consider that the required costs are reasonable compared to the potential impact of the security incidents.
- Information security controls are based on the risk management process.

# 1 Purpose and Objective

Information is an asset that requires protection in a similar way as physical buildings, machinery, and other physical assets. All information, applications, systems, and IT services used in Caverion need to be appropriately protected against information security risks to ensure confidentiality, integrity, and availability and compliance with regulations.

The objective of information security management is to ensure faultless operation of business functions by protecting information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction. The main three principles in verifying information security are confidentiality, integrity and availability of information and information systems:

- Confidentiality requires necessary level of secrecy enforced in the entire lifecycle of handling the information and preventing unauthorised disclosure of information.
- Integrity means assurance of accuracy and reliability of information and information systems and prevention of intentional or accidental unauthorised modification.
- Availability requires reliability and timely access to information and information systems. Systems must be able to recover from disruptions in a secure manner and provide an acceptable level of performance.

Information security management is an activity within the corporate governance framework which provides direction for security activities and ensures that objectives are achievable. Information security management relies on effective situational awareness and implementing security policies, procedures, and guidelines to ensure proper level of confidentiality, integrity, and availability accordingly. Information security management is based on regular information security risk assessments.

Caverion’s management demonstrates commitment to continuous information security management improvements by approval of this information security policy and regular management review meetings.

# 2 Scope

This information security policy applies to Caverion globally, but also takes into consideration the applicable local legislation and procedures in every operating country. Business divisions may prepare more restrictive information security policies for countries within the division.

Caverion information security management system (ISMS) covers all information and information systems and all processing of information, regardless of the format it is presented. This policy is including information security measures to comply with the General data protection requirements (GDPR) for secure personal data processing.

This policy applies to all Caverion employees, externals and anyone who processes information that Caverion owns or is responsible for. The policy addresses all aspects of information lifecycle, from creation to deletion.

# 3 Roles and Responsibilities

Group management has the overall accountability of information security to Caverion employees, customers, shareholders, authorities, and other interested parties. Group management must ensure that necessary resources and funding are available and that the information security management system is integrated in the business divisions, business units and group functions.

Caverion Group IT is responsible for planning, executing and monitoring the information security management system (ISMS) across Caverion. ISMS is including, but not limited to information security risk management, development, control implementation, documentation and awareness enhancement.

The acceptable levels of information security risk, and the baseline controls are accepted by the ISMS steering council in the management review meetings.

Caverion Information Security Council is responsible for supporting ISMS by evaluating information security materials, participating risks assessments and preparing improvement proposals for information security controls. Controls are prepared taking into consideration risk assessment results and changes in business or compliance requirements.

Group Information Security Officer is responsible for running the information security management system. The system is including but not limited to information security policy and guidelines, risk management, information security council, security awareness, monitoring, reporting to management and continuous improvement.

Caverion Group IT is responsible for implementing the required security controls for all IT services it is providing. Group IT has the overall responsibility for the security requirements of new technologies and fulfilling the requirements in common infrastructure and application development projects. Group IT shall report regularly to business and process owners of information security observations and measures taken.

The Group IT management team decides on the information security controls based on the information security council's proposals. Individual businesses division or business unit may not accept security risks affecting the entire company or choose not to implement the mandatory information security controls. The mandatory set of controls is defined in this Policy and the supporting documentation. Business divisions are responsible for information security management of their locally managed IT services, e.g. payroll system, and devices in line with this Policy and in compliance to local legislation.

Global process owner is accountable for decisions regarding information security in their processes, for example security classification and access rights management decisions.

All Caverion employees must be familiar with the information security policy and guidelines and comply with them. Each Caverion employee, contractor, consultant, and service provider is responsible for information security in their own work.

Line managers are responsible for verifying that new and existing employees have read this policy, follow it and have completed information security training.

Users, administrators, and contractors are required to report any information security weaknesses, abuse or any suspected exploitation of information security weaknesses to their superior or security management who needs to act as defined separately.

# 4 Controls

The required controls to ensure the right level of information security are designed to consider that the required costs are reasonable compared to the potential impact of the security incidents.

## 4.1 General mandatory information security controls

All information in Caverion must be classified according to its criticality to Caverion business. The information classification defines how information must be handled during the whole lifecycle and requirements for the security controls to provide adequate protection. The owner of the information is responsible for the classification. The main categories of information security classification are public, internal, confidential, and secret.

Information security controls are based on a risk management process. Information security risks are assessed annually, in case of significant changes, and during new information system development. Information security risk management is aligned with the corporate risk management process.

Access to Caverion information systems should be arranged thorough Caverion identity and access management system (IAM) where feasible. Exceptions must be agreed with Group IT.

Connections to corporate network are only allowed with devices accepted by Caverion Group IT.

Non-Caverion devices are only allowed to connect to Caverion IT services by the Group IT approved secure internet connection.

External users' access to Caverion network is possible only by separate procedures defined by Group IT.

Users may only use applications that are accepted by Group IT.

Group IT monitors and filters network traffic with automatic methods, taking into account legislation and other compliance requirements. It is Group IT's responsibility to verify corporate systems' security and continuity, and in order to do that Group IT has the obligation to intervene and investigate identified misconducts.

Group IT must be able to identify security breaches coming from external or internal sources. In order to succeed in that objective, there must be adequate technical capabilities to monitor the IT environment, recognize anomalies, and have information security incident management procedures in place.

Group IT monitors network traffic to identify anomalies to secure legitimate information transmissions and to take actions removing undesired components from the network. Monitoring will be conducted through automatic systems, and manual investigation takes place only when breaches are identified and reported, adhering to strict procedures in access management and NDAs.

All relevant security logs must be collected to a centralised log collection system, and they are analysed automatically in order to find anomalies.

Caverion's information systems are prioritised according to business impact.
The most important information systems must be evaluated against information security vulnerabilities in design and development phases and before deployment. Reassessments must be conducted after the deployment annually and when major changes are done to the information systems.

Group IT's information security officer prepares and updates an annual information security awareness training, which is mandatory for every employee in Caverion.

Caverion partners must comply with the information security requirements specified by Caverion. These are agreed on in an information security appendix to a service contract. Caverion reserves the right to conduct security audits to ensure sufficient level of information security.

Caverion uses cryptographic solutions where feasible to protect the confidentiality, authenticity and integrity of information. Requirements may come from e.g. customers, legislation, or authorities.

# 5 Communication

Caverion Group IT is responsible for information security related communications both within the corporation and with external parties.

# 6 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Information Security Policy is reviewed every second year as a standard. Necessary changes may be made on a need basis. Other information security documentation will be reviewed annually. Necessary changes may be made on a need basis.

This information security policy is approved by the President and CEO of Caverion Group.

| | | |
|---|---|---|
| Date issued | 11.12.2020 | |
| Approved by | President and CEO of Caverion Group | |
| Document type | Ways of Working (IT) | |
| Document owner | Group Information Security Officer | |
| | | |
| Version | Date | Remarks |
| 1.0 (original) | 07.06.2013 | |
| 1.1 | 08.12.2016 | |
| 1.2 | 15.08.2017 | Compliance upates |
| 1.3 | 15.11.2018 | Bi-annual review and updates |
| 1.4 | 11.12.2020 | Bi-annual review and updates |