INFORMATION SECURITY POLICY

Contents

1. Introduction

This document lays down Mandatum Group's (hereinafter Mandatum) information security policy (hereinafter Policy). Mandatum Group's subsidiaries are Mandatum Life Insurance Company Limited and Mandatum Asset Management Ltd and their subsidiaries. The Policy applies to all of Mandatum's employees and the representatives of stakeholders who process Mandatum's information in connection with their assignments. As far as the external stakeholders, such as subcontractors and service providers, are concerned, the requirements of this Policy are included, where applicable, to purchase agreements.

The Policy is a document that steers Mandatum's information security efforts. The Policy can be specified and supplemented by information security principles and guidelines that are brought to the attention of employees and material third parties. The principles and guidelines must not be in conflict with the Policy.

2. Purpose and objectives

The purpose of the Policy is to lay down the objectives, responsibilities and means of securing information at Mandatum. The objective of the Policy is to ensure that Mandatum's information, services, information systems and data communications systems are protected and secured in both normal and emergency conditions through administrative, technical and other means. Information security encompasses all of Mandatum's information and information processing, including archiving.

The objectives of information security at Mandatum are:

Customer focus

Customers' information is appropriately protected, and the services offered to customers are secure.

Business focus

Information security is part of developing high-quality services, digitalisation of services and data-driven business, as well as a positive customer experience.

Continuous improvement of information security

The continuous improvement of information security ensures that the level of information security is sufficient with regard to the nature and extent of the business, the threats on the information and information systems and the general technical development level. The information security meets the requirements and obligations set by legislation and authorities and corresponds with the level generally expected by external stakeholders from a financial institution.

3. Organisation and responsibilities

3.1 Board of Directors and CEO

The companies' Boards and CEOs are responsible for ensuring that Mandatum's information security is at a sufficient level and that sufficient resources are allocated to information security. The Boards of Mandatum Life Insurance Company Limited and

Mandatum Asset Management Ltd approve the information security policy annually and the Boards bear overall responsibility for compliance with the Policy.

3.2 Business Committee

The Business Committees of Mandatum Life Insurance Company Limited and Mandatum Asset Management Ltd handle, and the chairs of the Business Committees approve, the information security principles and strategy as presented by the Chief Information Security Officer.

3.3 Information Security and Cyber Risks Committee

The Information Security and Cyber Risks Committee ensures that operational risk management within the Group is arranged appropriately as it pertains to information security and cyber risks between business units, support units and steering functions is seamless.

3.4 Organisational units

Each organisational unit (hereinafter Unit) is responsible for the information security of its own organisation and the services it purchases in accordance with the information security policy, principles and guidelines. The Units are responsible for information security also in accordance with the internal control policy. The Units consult with Mandatum's information security team in matters that concern Mandatum's information security, for example, in projects and service purchases affecting information security.

3.4.1 HR Unit

The HR Unit is responsible for the security of personnel and premises, employment and induction processes and issuing guidelines to supervisors in the above matters.

3.4.2 Business Technologies Unit

The Business Technologies unit (hereinafter BT Unit) is responsible for the implementation of technical information security development projects, and for maintaining and monitoring the information security services that fall under its responsibility.

3.5 Information security team

The information security team is responsible for monitoring Mandatum's information security level (incl. cyber security) and handling information security deviations. In addition, the information security team highlights development needs related to information security and promotes measures to meet them.

The information security team supports the Units and issues them guidelines in matters related to information security.

The information security team carries out information security assessments and inspections as part of service procurement and the monitoring of information security levels.

3.5.1 Chief Information Security Officer (CISO)

The CISO is responsible for the operative management of the information security team and issues policies and statements in accordance with the information security policy and principles and approves the information security guidelines. The CISO is responsible for producing and maintaining the information security policies, principles and strategy and monitors their implementation.

The CISO is responsible for ensuring that the information security management system complies with the requirements of ISO 27001.

3.5.2 Cyber Security Manager

The Cyber Security Manager carries out information security monitoring in order to identify cyber threats and risks, and co-ordinates the processing of cyber-security-related deviations. The Cyber Security Manager participates in the information security projects of the business and other stakeholders and recommends good information security practices and approaches.

3.6 Personnel and those working on behalf of Mandatum

Each person employed by Mandatum or working on behalf of Mandatum has the obligation to comply with the information security policy, principles and guidelines and to ensure compliance with the information security and data protection obligations imposed by legislation at any given time and the obligations related to the insurance secrecy and other non-disclosure obligations.

3.6.1 Supervisors

Supervisors are responsible for ensuring that the employees complete the information security induction and training sessions targeted at personnel and that the employees are aware of the information security policy and principles and the information security guidelines that are essential for their tasks.

Supervisors are responsible for ensuring that each person working on behalf of Mandatum and having Mandatum's user credentials has a supervisor-level responsible person and that those working on behalf of Mandatum are aware of the information security policy and principles and the information security guidelines that are essential for their tasks.

Supervisors are also responsible for ensuring that each employee or person working on behalf of Mandatum is bound by the obligation of non-disclosure.

4. Measures

4.1 Assessing the level of information security

The level of information security must be continuously assessed in accordance with the agreed roles, taking into account Mandatum's key functions, resources and the processed information and the threats affecting them, the likelihood of the threats and the impact of the materialisation of the threats. Any shortcomings must be addressed, and sufficient measures must be carried out to manage the risks.

4.2 Management of information security risks

Sufficient technical and administrative measures must be in place to identify information security risks and deviations. Particular attention must be paid to information security risks affecting customers' information. The identified information security risks must be addressed and reported on regularly as part of operational risk management.

Information security is reported on regularly to the Information Security and Cyber Risks Committee, to the Risk Management Committee and to other stakeholders as part of quarterly risk management reporting.

4.3 Securing information

Information that is central to Mandatum's business must have owners, specified in accordance with the information management policy, who are responsible for securing the information, taking into account the confidentiality and significance of the information for business over the entire lifecycle of the information.

4.4 Securing services and information systems

Securing information systems

Internal and external information systems (including cloud services) must have designated persons in charge. The persons in charge of information systems under the BT Unit's responsibility are appointed by the head of the BT Unit. Similarly, the persons in charge of information systems under the responsibility of other Units are appointed by the head of each Unit.

The persons in charge of information systems are responsible for securing the information systems together with the information owners, taking into account the confidentiality of the information processed through the information systems and their significance for Mandatum's business.

Developing and purchasing services and information systems

When developing and purchasing services and information systems, the person in charge must take care, in a proactive manner, of identifying and addressing information security risks in relation to the significance of the service or information system for Mandatum's business and strategy and its impacts on Mandatum's information networks and IT infrastructure. Where required, the person in charge must consult with Mandatum's information security team and the BT Unit, and operate in accordance with other applicable policies, such as the purchasing, information security and outsourcing policies.

Traceability of information system events

When developing services and information systems, it must be ensured that a log entry is made on events that are significant in terms of business and particularly on the processing of personal data and that the events are traceable in accordance with the principles related to log entries.

Access control and user rights

Access to information systems must be controlled.

User rights to information and information systems must be granted and their use must be controlled in accordance with the user right principles. User rights must be determined based on work-related needs.

4.5 Securing digital business

Information security risks related to digital and data-driven business must be taken into account in developing and maintaining services, and they must be continuously assessed. In addition, sufficient measures must be carried out to minimise various disturbances and abuse situations.

4.6 Implementation of cyber security

Cyber security must always be taken into account. Special attention must be paid to identifying cyber threats and risks and addressing such observations without delay.

Measures to ensure cyber security must be sufficient and in line with good information security practices, and the implementation of the protective measures must strive for a layered security approach where possible.

4.7 Continuity management and preparing

Mandatum must have a continuity plan in place for different disturbances and emergency conditions. The continuity plan must have a designated owner who takes care of updating and testing the continuity plan.

4.7.1 Reporting on information security breaches

Means and a well-functioning process as well as instructions on how to proceed must be in place for reporting on information security breaches, taking into account the requirements set by legislation and authorities in terms of the obligation to report on information security breaches.

4.8 Ensuring information security awareness and competence

The information security awareness and competence of employees must be ensured through information security training and guidelines. The information security team is responsible for the content of the training.

The information security awareness and competence of third parties must be ensured through agreements and guidelines attached to them and, where possible, through training.

4.9 Meeting the requirements of ISO 27001 certification

Mandatum must fulfil the requirements set by ISO 27001 certification within the scope of the information security management system and commit to continuously improving the management system.

5. Communications

The information security policy, principles and guidelines are published on Mandatum's intranet. More information on applying the policy is available from Mandatum's information security team.

The information security team is primarily responsible for internal communications in information security matters. The head of the Data Governance Unit is the deputy.

Mandatum's communications policy is followed in external communications. In principle, matters concerning Mandatum's information security are not public, and external communications must always be preceded by a consultation with the CISO, an expert from the information security team or the head of the Data Governance Unit.

6. Monitoring and breaches

The CISO monitors compliance with the Policy and handles any breaches against the Policy together with supervisors and Mandatum's executive management. A breach of the Policy or guidelines drawn up on the basis of the Policy may lead to consequences under the Employment Contracts Act (55/2001).

The Units are responsible for complying with the Policy in their own units.

On the part of subcontractors and service providers, the responsibility for monitoring lies with Mandatum's representative steering the operations of the subcontractor or service provider.

Any other possible monitoring takes place as permitted by the agreements and under legislation.

In addition to this, each person employed by Mandatum or working on behalf of Mandatum has the obligation to monitor compliance with the Policy. Suspected breaches, abuses or shortcomings in information security must be reported to the CISO.

7. Deviations

Deviations from the Policy are possible where there is a strong business case, however, provided that the non-disclosure obligation laid down in legislation is not jeopardised. Deviations are reported to the CISO, who assesses the risks related to the deviation and issues instructions as required. If, based on the CISO's assessment, the deviation is significant, the decision on the deviation will be made by Mandatum's CEO.

8. Changes

The CISO prepares any changes to the Policy. The Boards of Mandatum Life Insurance Company Limited and Mandatum Asset Management Ltd approve the policy annually.