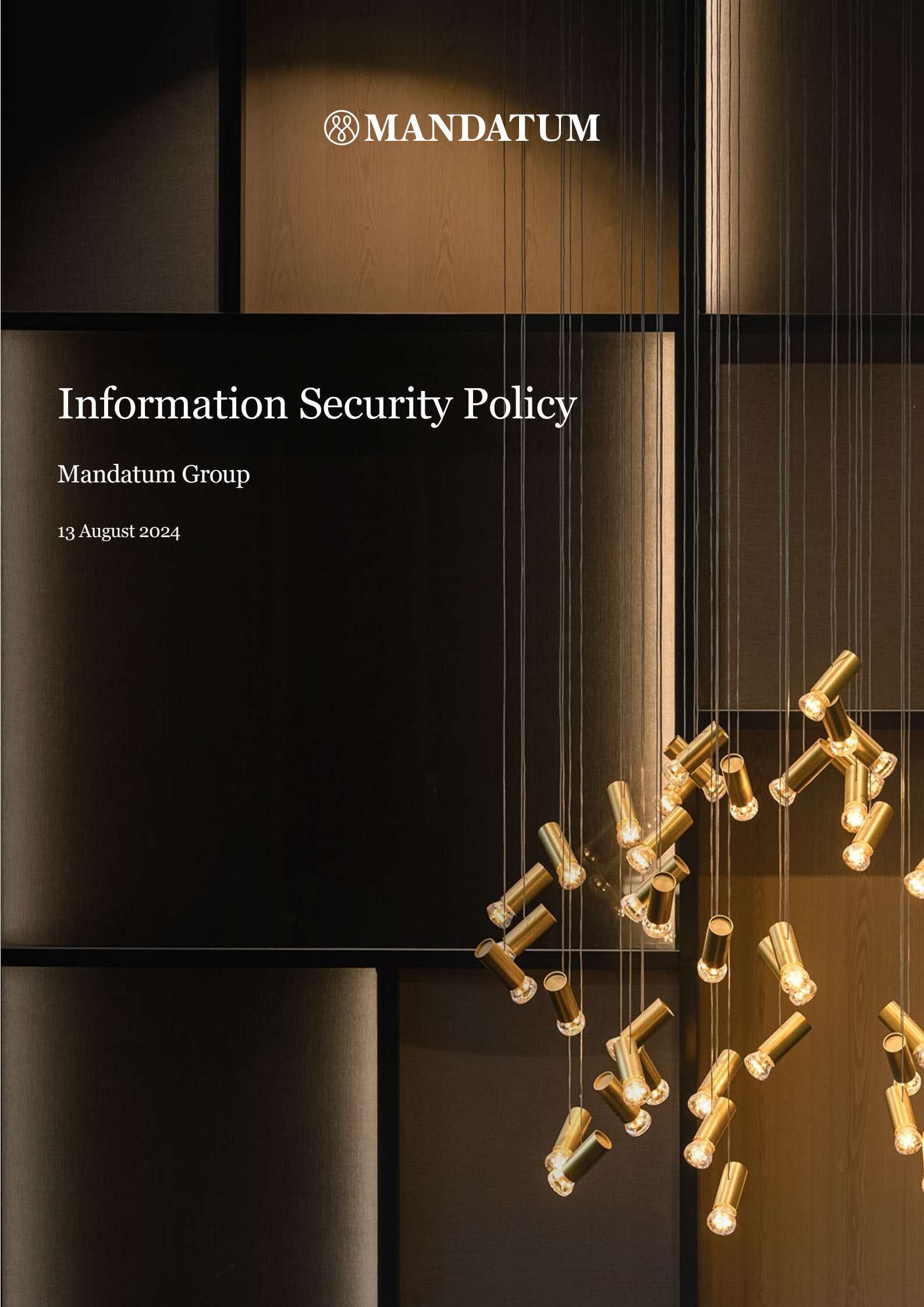
MANDATUM

Information Security Policy

Mandatum Group

13 August 2024



Contents

1 DEFINITIONS

"**BT Unit**" means the Business Technologies unit of Mandatum Group.

"**CISO**" means the Mandatum Group Chief Information Security Officer.

"**Cyber security**" refers to arrangements that aim to secure a digital and networked operating environment based on data processing technology.

"**HR Unit**" means the Human Resources unit of Mandatum Group.

"**Information security**" refers to arrangements that aim to ensure the availability, integrity, authenticity, and confidentiality of information. Availability means that the information is available at the desired time. Integrity refers to the consistency of the information with the original information (e.g., when transferring information). Authenticity means that data has not been corrupted after its creation and it comes from a trusted source i.e. it has not been created by an attacker or other impostor. Confidentiality means that the information is only available to the persons and entities for whom it is intended (e.g., job role, client or service provider contract).

"**Mandatum Group**" or "**Mandatum**" means Mandatum plc together with its subsidiaries (each a "**Group Company**").

"**Policy**" means this document.

2 INTRODUCTION

2.1 Background and Purpose

This document sets forth the information security policy of Mandatum Group (the "**Policy**"). The purpose of the Policy is to lay down the objectives, responsibilities and means of securing information at Mandatum. The Policy aims 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, covering whole life cycle from data creation to destruction.

The objectives of information security at Mandatum are:

Customer focus

Customer 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.

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. Such principles and guidelines must not be in conflict with the Policy.

2.2 Scope

This Policy applies to all Mandatum Group Companies and 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.

3 ORGANISATION AND RESPONSIBILITIES

3.1 Boards of Directors and CEOs

The Boards of Directors and CEOs of Mandatum Group Companies are responsible for ensuring that Mandatum's information security is at a high level and that sufficient resources are allocated to information security. The Board of Directors of Mandatum plc approves the Policy annually and bears ultimate responsibility for compliance with the Policy.

3.2 Information Security and Cyber Risks Committee

The Information Security and Cyber Risks Committee (ISCRC) ensures that operational risk management within Mandatum Group is arranged appropriately in the area of information security and cyber risks. The committee ensures that cooperation and flow of information pertaining to information security and cyber risks between business units, support units and steering functions is seamless.

The committee approves information security risk levels used in Mandatum Group's risk management.

The Information Security and Cyber Risk Committee handles, and the Chair of the ISCRC approves, information security principles and strategy as presented by the Group CISO.

3.3 First Line Functions

First line functions refer to business units and other support functions, such as HR and Business Technology, which are supporting businesses to achieve their goals.

Each organisational unit is responsible for the information security of its own organisation and the services it purchases in accordance with the Policy and the information security principles and guidelines as well as other policies of Mandatum Group in relation to information security, as applicable. The units shall consult with Mandatum's information security organisation in matters that concern Mandatum's information security, for example, in projects and service purchases affecting information security.

HR Unit

Mandatum Group's HR Unit is responsible for the security of personnel and premises, employment and induction processes and issuing guidelines to forepersons in the above matters.

Business Technologies Unit

The BT Unit is responsible for the implementation of Information Security Management System (ISMS) and technical information security development projects, and for maintaining and monitoring the information security services that fall under its responsibility.

The first and second lines of defence have their own information security roles. The roles in the BT unit are:

(a) Cyber Security Manager

The Cyber Security Manager carries out information security monitoring to identify cyber threats and cyber risks, and co-ordinates the processing of cybersecurity-related deviations. The Cyber Security Manager is responsible for developing cyber security and participates in the information security projects of the business and other stakeholders and recommends security best practices and implementation methods.

(b) Information Security Manager

The Information Security Manager carries out information security monitoring to identify information security threats and risks, and co-ordinates the processing of information security related deviations. The Information Security Manager is responsible for developing information security processes and participates in the information security projects of the business and other stakeholders and recommends security best practices and implementation methods.

3.4 Second Line Functions

Second line functions refer to the Group Risk Management and Group Compliance functions.

The Group Risk Management function is concerned with proper identification, assessment and management of risks throughout their lifecycle. The Group Risk Management function also supports business units in identification, assessment and management of risks. The information security and data risks of the Group Risk Management function, headed by the Group Chief Information Security Officer (CISO) is responsible for steering Mandatum's information security and business continuity planning, monitoring security level (including cyber security) and handling information security deviations. It executes information security assessments and inspections and highlights development needs related to information security and promotes their implementation.

At Mandatum, compliance risks are integrated as part of the operational risk framework defined in the Mandatum Group Risk Management Policy. As for data protection and the processing of Personal Data, the Group Compliance function is concerned with compliance risks inherent in them. The Group Compliance function is responsible for maintaining risk management framework for independent assessment of compliance risks with respect to data protection. The Group Data Protection Officer (DPO) is part of the function. Duties of the DPO are explained in detail in Mandatum Group's Data Protection Policy.

3.5 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 Policy and information security 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.

Forepersons

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

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

Forepersons 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 customer 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 management bodies, as applicable, as part of quarterly risk management reporting.

The key roles related to risk management are defined in the risk management policies of Mandatum Group. In addition to the above, this Policy applies to the management of information security risks.

4.3 Securing Information

Information that is central to Mandatum's business must have owners, specified in accordance with the Mandatum Group's internal Information Management Policy, who are responsible for securing the information, taking into account the confidentiality, integrity, availability 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 specialists and the BT Unit, and operate in accordance with other applicable policies, such as the purchasing, data protection 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 Log entry principles.

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.

4.8 Management of Data Security Breaches

There must be tools and a functioning process and operating instructions for managing and reporting data security breaches, taking into account the requirements set by legislation and authorities regarding the obligation to notify data security breaches.

4.9 Ensuring Information Security Awareness and Competence

The information security awareness and competence of employees must be ensured through guidelines and regular training. 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.

4.10 Meeting the Requirements of ISO 27001 Certification

Mandatum must fulfil the requirements set by ISO 27001:2022 certification within the scope of the information security management system and commit to continuously improving the management system.

5 COMMUNICATIONS

The Policy is published on Mandatum's website and intranet. Principles and guidelines supplementing the Policy are non-public and available for Mandatum's employees on Mandatum's intranet and/or brought to the attention of other parties as applicable. More information on applying the Policy is available from the CISO. The CISO is primarily responsible for internal communications in information security matters.

Mandatum's Disclosure 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 or an expert from the information security organisation.

6 MONITORING AND BREACHES

The CISO monitors compliance with the Policy and handles any breaches against the Policy together with forepersons 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 Finnish Employment Contracts Act (55/2001, as amended).

The Units are responsible for compliance 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 act in compliance with the Policy. Suspected breaches, abuses or shortcomings in information security must be reported to the CISO.

7 TIMELINESS AND REVISION OF THE POLICY

The contents of the Policy shall be reviewed when necessary, and at least annually, by the CISO. The CISO is responsible for preparing any updates or amendments to the Policy. The Policy is presented for the approval of the Board of Directors of Mandatum plc at least annually.

8 LANGUAGE OF THE POLICY

This Policy has been prepared in Finnish and English. In the event of any discrepancies, the Finnish version shall be decisive.

MANDATUM

Mandatum plc

Registered domicile and address:
Bulevardi 56, FI-00120 Helsinki, Finland

Business ID: 3355142-3

www.mandatum.fi