CINIA'S SECURITY POLICY

The goal of security and risk management in Cinia is to protect people, assets, data, reputation and the environment against damage, criminal activity and accidents, so that Cinia's business and other goals can be fulfilled.

Cinia's secure services and operating models are key parts of Cinia's business image, social responsibility and the fulfilment of its business goals.

The security policy defines the goals, implementation principles and responsibilities for the company's security and risk management.

This policy applies to Cinia Ltd and its group companies.

Principles of corporate security and risk management

Cinia always acts in compliance with the legislation, guidelines issued by the company's Board of Directors, customer agreements, the risk management policy, good risk management practices and guidelines on Cinia's security activities.

All security-related responsibilities and tasks have been defined in writing.

Cinia's risk management is based on an annual calendar for the company's financial administration and other operations and guidelines on risk management issued by Cinia's executive team for each operating year.

According to the **annual calendar**,

- The Board of Directors issues guidelines on the implementation of risk management.
- The executive team arranges risk assessment workshops.
- The executive team issues guidelines and instructions concerning risk management.
- Responsible persons from each risk sector arrange risk workshops within their sectors.
- The security and risk management team discuss sector-specific risk assessments and action plans to control risks and compile an assessment of strategic risks.
- The company's CEO presents the assessment of strategic risks and the actions required to control them to the Board of Directors.
- The executive team regularly reviews the various areas of corporate security and decides on the need for internal and external audits and their implementation.

The executive team issues guidelines for the fulfilment of risk management for each operating year in April-June. The guidelines include at least the following:

- Goals and focus points of corporate security and risk management set for the operating year
- Revised annual calendar for risk management
- Responsible persons
- Personnel training
- Indicators, and
- Reporting.

Cinia's comprehensive risk management is based on security sector specific responsibilities defined by the executive team. Risk sectors and their responsible persons are:

- Business risks – Business Director
- Financing and financial risks – CFO
- Information security risks – Information Security Manager
- Personnel risks – Head of People Operations
- Facility risks – person responsible for the physical security of the premises
- Reputational risks – person responsible for external communication

Cinia offers induction to all people working in Cinia's premises regarding security guidelines and arranges regular security training that supports business activities. Cinia actively communicates security-related matters to its partners and personnel.

Maintenence and development of information security

The cyber operating environment is also Cinia's business environment. Because of this, cyber and information security is one of Cinia's security focus areas.

To maintain cyber and information security, Cinia has an information security policy that defines the aims, tasks, authorisations and responsibilities related to information security. The information security policy provides grounds for continuous development in line with customer demands and the standards in the sector and for maintaining necessary guidelines as well as reviews and training.

Roles and responsibilities

Cinia's **Board of Directors** is responsible to the company's shareholders for ensuring that Cinia has a functional risk management system. The Board of Directors defines the company's risk management policy in accordance with corporate governance guidelines. The Board of Directors monitors and supports the fulfilment of risk management within the company.

The company's **CEO** is responsible for ensuring that comprehensive risk management processes are planned and implemented efficiently. The CEO reports strategic risks to the Board of Directors.

- The company's **executive team** discusses and approves Group-level risk management goals, guidelines and resources, as well as matters presented to the Board of Directors, and actively monitors compliance with risk management guidelines.
- **The security and risk management team** acts as a preparatory body for the executive team and ensures a connection between risk management and business activities.
- **The security manager** is responsible for the guidance and monitoring of corporate security and risk management. The security manager is responsible for the execution and development of risk management processes and prepares matters to be handled by the security and risk management team.
- **The corporate security team** orchestrates the operation of various areas of corporate security. The team is managed by the security manager, and other members include the information security manager and experts, the person responsible for the security of the premises and the person responsible for personnel security.
- **The information security manager** is responsible for the maintenance of the information security policy and the management of information security activities and organisation, and reports to the security manager.

- **The person responsible for the physical security of the premises** is responsible for improving and organising the security of office and production facilities in cooperation with the person responsible for each location.
- **The head of people operations** is responsible for developing and managing personnel security. He also participates in the development of occupational safety and cooperation on occupational health and safety and is the person responsible as a member of the executive team.
- **The business directors** are responsible for the continuity and contingency plan for the business operations and the produced services.
- **Responsible personnel from the risk sectors** are responsible for conducting risk assessments in their sectors, maintaining and issuing guidelines, implementing risk management and reporting to the security manager.
- **The line management** is responsible for including comprehensive risk management during operational management and business processes, including stakeholder cooperation. Supervisors are responsible for ensuring that groups under their management work in compliance with security and risk management guidelines.
- **Every Cinia employee** undertakes to comply with all guidelines issued, take active part in security training and the continuous improvement of security, and report any information security deviations.

Strengthening the security policy

Members of the executive team of Cinia Group’s parent company confirmed this security policy on 14 May 2018. It replaces the previous policy approved on 15 August 2016.

The Board of Directors of the Group's parent company approved these guidelines on 23 May 2018.