CINIA'S INFORMATION SECURITY POLICY

Cinia's business activities are based on the trust shown by its customers, partners and employees in the company's ability to see to the safe use and management of data material and the information security of the company's services. Cinia's information security policy defines how Cinia, in its activities, ensures the confidentiality, integrity, availability, non-repudiation and accuracy of data material compliant with requirements.

This information security policy supplements and specifies Cinia's previously released security policy and privacy policy.

This information security policy applies to Cinia Ltd and its subsidiaries ("Cinia"). All Cinia employees and any leased employees are obligated to familiarize this document and comply with it when working at Cinia and outside the workplace.

Goal of the information security policy

The goal of this information security policy is to protect any data held by Cinia against intentional and unintentional threats that may damage business activities or lower trust in the company's activities. This information security policy defines the principles, procedures and responsibilities that apply to the maintenance and development of information security at Cinia. This information security policy provides the basis of lower- level regulations and guidelines on information security.

Furthermore, this information security policy specifies the principles of corporate security defined in Cinia's security policy and comprises an integral part of Cinia's privacy policy on the managing of personal data. Information security risks are assessed, and the actions required to maintain them at an acceptable level are defined in accordance with the annual risk management calendar.

Principles of the information security policy

Cinia produces its services in a digital environment ("cyber environment"). As a result, information security management emphasises actions related to the maintenance of digital security. The monitoring of constant technological development and any resulting changes in continuously changing digital threats forms a central part of the company's information security practices.

Cinia is a telecommunications company defined in the legislation. It is governed by obligations set for the information security and preparedness of telecom companies and any official regulations issued under these obligations. Obligations for information security have also been defined in the privacy protection legislation.

In its service agreements, Cinia is committed to fulfil certain information security requirements that it has defined together with its customers. A significant number of Cinia's customers are companies and agencies that maintain the infrastructure critical to the whole society. As a result, the maintenance of information security at Cinia also focuses on broad social responsibilities.

At Cinia, data of the company or its customers can only be processed by those who need this data in their work or who have permissions to access this data. The use of data is monitored, for example, by means of access control and logs.

In maintaining its information security, Cinia uses operating models based on the ISO/IEC 27001 standard it has adapted to its operating environment and documented.

Maintenance of information security

Key responsibilities and processes have been defined in order to maintain information security in service production and other activities. In order to maintain information security in accordance with goals set:

- The parent company's executive team confirms company-level responsibilities, tasks and resources.
- The member of the executive team in charge of security prepares company-level decisions for the parent company's executive team.
- The risk and security manager monitors the development of the risk environment, maintains the company's information security management system, leads and coordinates daily information security maintenance tasks and prepares proposals for any additional activities required.
- Cinia's Cyber Security Operations Center is responsible of monitoring production and office networks and services round the clock. Cyber Security Operations Center leads and coordinates investigation of cyber security incidents.
- Business directors are responsible for continuity management and for ensuring that information security is in compliance with requirements regarding the services they produce or have procured from third parties.
- Superiors are responsible for complying with information security practices in their units and teams.
- Every Cinia employee must familiarize and follow information security guidelines governing employees.

Owners of data systems are responsible for the information security of their systems by carrying out and documenting software updates and reconfigurations, managing the access control required and keeping certificates in the integrated production environment up to date. System and integration changes are planned and carried out in accordance with the change management process following the principles of information security.

Cinia's Cyber Security Operations Center monitors and maintains cyber security of system environments of the company and its customers round the clock by collecting security and event logs and monitoring incidents and anomalies. Cinia's other resources support the Cyber Security Operations Center in technical analysis of incidents and ensuring business continuity.

Cinia's information security practices have been documented. Information security documents related to services are maintained together with service descriptions, while other information security documents are maintained in the intranet. Responsibilities for maintaining documents have been defined and published.

With regard to information security management, Cinia maintains internal documents of at least the following:

- Assessment and management of information security risks
- Access management and granted access rights
- System register and systems
- Remote use of systems
- Classification of data material and encryption practices
- Safe use of terminal devices
- Service continuity management

Information security training is arranged regularly for all Cinia employees, and this training is documented. New Cinia employees receive induction regarding the company's information security practices and guidelines as part of an induction programme arranged by the HR management and the superior of each employee.
All information security incidents, attacks and vulnerabilities, as well as any suspicions of these, are reported using official reporting tools or methods. Information security violations targeted at personal data and any suspicions of these

are reported in accordance with privacy protection guidelines. The Cyber Security Operations Centre releases regular reports on the status of information security to the parent company's executive team.

The parent company's executive team, together with the member of the executive team in charge of security, annually audit corporate security and information security maintenance processes.

Confirming the information security policy

Cinia's executive team has confirmed this information security policy on 20th of August 2018 and the updated policy on 18th of November 2019 and 7th of May 2020.

The Board of Directors of the Group's parent company approved these updated guidelines on the 28th of May 2020.