Kuusakoski Recycling Information Security Principles for partners

Introduction

Information security principles defines the practical operating methods for executing information security. These principles apply to all partners that are in contract relationship to Kuusakoski. Information security principles are valid until further notice, and they are approved by Kuusakoski IT Manager.

Non-conformities

Every partner is obligated to report any threats and deviations related to information security to their Kuusakoski contact person. Any breaches of the information security or data protection legislation, information security and privacy policies and any guidelines issued based on them must always be reported to Kuusakoski contact person.

Any information security breach may result in cancellation of the cooperation. If a breach results in financial losses, compensation for the losses may be claimed. Any misuse of data or intentional breach of guidelines may lead to penal consequences.

The information security team and information management unit have an authorization and obligation provided by the highest level of management to monitor and control the information security and data protection of data systems and data processing and, if required, take action to investigate any problems and eliminate any risks identified. If required, incidents must be reported to the organization's management.

Partner personnel security

Personnel security means the management of information security threats resulting from the activities of the personnel and directed at the personnel. The aim is to have reliable partner network familiar with the information security guidelines and obligations set for them, at the beginning, during and at the end of their contractual relationship.

Principles:

- A review of information security and data protection guidelines are included in personnel induction. The partner ensures that employees are familiar with the Kuusakoski's information security requirements and practices.
- If required, information security training is arranged for employees to maintain their level of knowledge.
- Everyone is obligated to observe and report information security risks and deviations.
- Arrangements at the end of employment must be carried out so that the employee whose employment relationship ends, cannot have access to the company's data systems or facilities.

Physical information security

Physical information security means the protection of facilities, data tools, other devices that contain sensitive information and other material.

Principles:

- Any unauthorized access to the facilities of the company or its service provider, containing a data system environment or sensitive material, must be prevented by means of access control.
- Kuusakoski's partners are required to use an ID card at Kuusakoski's premises, unless the person is otherwise identified.
- IT hardware and archives containing important information must be placed, taking any water, heat, and fire risks into account. Any interruptions in the power supply must be taken into account, considering the criticality of hardware.

Security of Kuusakoski's IT services and data systems

The security of IT services and data systems covers data systems, IT services, support services, capacity services and software development partners. The aim is to have secure data systems and services that best correspond to business needs and partners that provide them and are committed to complying with activities in accordance with the Kuusakoski information security policy and to developing them.

Principles in Kuusakoski systems:

- Data systems and IT services are procured centrally by the Kuusakoski information management unit. Requirements for procurement include a functional and technical suitability for the company's IT service architecture.
- To deploy new software, it is required that the software has been tested and that its information security testing has been approved.
- IT service partners are required to sign non-disclosure agreements if company's secret information or personal data in accordance with the EU General Data Protection Regulation (GDPR) is processed in the specific service.
- IT service providers are required to comply with the information security and data protection legislation in their operations.

Hardware security

Hardware security covers terminal devices, servers, network devices and all other devices needed to process data. The hardware used must enable activities in accordance with the information security principles.

Principles:

- Hardware must be installed in accordance with approved standards, ensuring that the information security software required is installed and settings are defined in accordance with information security guidelines.
- Information owned by Kuusakoski will not be stored or transferred to external devices without Kuusakoski's written permission.

Telecommunications security

Telecommunications security means the uninterrupted and secure availability, protection and encryption of data connections, the authentication of users, secured data connections and the ability to monitor network traffic. Telecommunications security results in secure and reliable data transfer connections.

Principles:

- Company's networks and systems in which Kuusakoski's data is processed must be appropriately protected.
- Adequate measures must be taken to react to any deviations observed and any incidents related to Kuusakoski must be reported without delay.
- Email encryption is used for all confidential email messages.