Guideline	Org.	Version	Page	Date	
Information security for contractors	IT	-	1/9	11	2021

Contents

1 Introduction and validity / scope

1.1 Introduction

This guideline defines rules for handling information and the use of information technology which suppliers, works contractors and service providers - hereinafter referred to as contractors - to Leopold Kostal GmbH & Co. KG and/or its affiliated companies (go to www.kostal.com) - hereinafter referred to as KOSTAL - must follow. The purpose of this guideline is to protect the confidentiality, integrity and availability of information, as well as the rights and interests of the customer, as well as all persons (natural and legal in definition) entering into a business relationship with and / or carrying out activities for KOSTAL.

1.2 Validity / scope

This guideline is intended for the board of directors of the contractor, its employees and those assisting in the performance of the tasks.

2 Maintaining the confidentiality of information / trade secrets

KOSTAL works exclusively with contractors who have undertaken to maintain the confidentiality of information and trade secrets within the framework of a confidentiality undertaking or a confidentiality agreement. In individual cases, if the information being transferred is subject to stricter security requirements, further special action may be demanded of contractors in order to take account of such requirements.

For example, the contractor shall be forbidden to process, store or release information received to third parties without KOSTAL's approval. An approval can be linked to comply with the following security requirements by the contractor or its sub-contractors.

3 Requirements for the contractor to maintain security of information

3.1 Basic principles

The contractor is required to implement an information security management system in accordance with the requirements of ISO 27001/27002 and to comply weith the legal requirements regarding data protection.

Depending on the form of the cooperation there are points of emphasis regarding the requirements covering the security measures to be implemented. The form of the cooperation may change in the course of the business relationship. In these circumstances the security measures to be implemented will also change. The following text sets out the minimum requirements for the contractor's information security management system.

3.2 Organising the security of information

Guidelines, processes and responsibilities must be defined, with which the security of information can be implemented and monitored.

This includes in particular:

- the establishment of an information security guideline.
- user guidelines setting out the rules for handling applications, systems and IT devices, as well as ways of using information technology.
- the description of processes for managing data-carriers, documents and information.
- the specification of roles and responsibilities in the field of information security.
- the duties of employees regarding confidentiality and the protection of trade secrets.
- the regular execution of training and awareness measures.

3.3 Controlling access

Actions must be implemented to ensure that personnel authorized to use the iinformation processing procedures can access only the personnel-related data and information/data requiring protection which are covered by their access authorization.

This includes in particular:

- the creation of authorization concepts for access to information, systems and applications requiring protection.
- the implementation of restrictions on access.
- preventing a concentration of functions and establishing a separation of functions.
- the implementation of a process for issuing authorizations.
- the regular checking of authorizations.
- recording the issue of authorizations and access to data.

3.4 Cryptography

The use of coding procedures to ensure the orderly and effective protection of confidentiality, authenticity or integrity of personnel-related data and inforfmation requiring protection.

This includes in particular:

- the encoding of directories, data-carriers and hard disks in PCs and laptops.
- the secure storage of data on mobile data-carriers. Data classified as confidential or secret must be encoded on mobile data-carriers.

3.5 Protecting buildings

Actions mustg be taken ro prevent unauthorized physical access to the organisation's information and information-processing facilities, as well as preventing their damage or deterioration.

This includes in particular:

- specifying secure areas.
- implementing access prevention.
- specifying personnel with access authorization.
- managing personnel-related access authorizations.
- rules for accompanying visitors and external personnel.
- monitoring areas outside opening hours.
- recording access by personnel.

3.6 Protecting operating equipment / information data

Appropriate action must be taken to prevent the loss, damage or theft or deterioration of operating equipment / information data and to prevent breaks in the production activities of the organisation.

This includes in particular:

- rules for the secure positioning of operating equipment.
- protecting operating equipment against over-voltage, power failures, fire and water.
- protecting information and information processing systems against theft.
- rules for the regular maintenance of operating equipment.
- implementing a process for the secure deletion, disposal and destruction of operating equipment.

3.7 Operating procedures and responsibilities

Measures must be taken to ensure the orderly and secure operation of systems and procedures for processing information.

This includes in particular:

- documenting operating procedures, in the form of operating manuals, for example.
- securing IT systems.
- the separate processing of production and test data.
- ensuring the separation of clients / separation of client data.

- Requirements covering a separation of functions must be implemented. Which functions cannot be linked and therefore must not be handled by one person at the same time must be specified, documented and justified. As a general principle operational functions must not be linked with monitoring functions.

3.8 Data security

Actions must be taken to ensure that information and data / personnel-related data requiring protection are protected against accidental destruction or loss.

This includes in particular:

- the creation of a data security concept.
- the regular execution of data protection measures.
- The data security media must be stored separately from the production systems.

3.9 Protection against malware by managing weaknesses and patches

The misuse of technical weak points must be prevented by the installation of current virus protection software and the implementing of patch management.

Regular checks must be carried out to detect possible weak points.

3.10 Protocolling and monitoring

Actions must be taken to ensure that checks can be made at a later stage to determine if and by whom (personnel-related) data in IT systems have been entered, modified or deleted.

These actions include in particular:

- the recording of access authorizations and access to data.
- regular checks on user authorizations.
- the recording of activities and regular evaluation of user and system activities

3.11 Network security management

Appropriate protection for the network must be implemented so that information and the infrastructure components are protected.

This includes in parrticular:

- the implementation of a network management system.

- the introduction of a user authentication system for external connections and connections between individual systems.
- ensuring the protection of diagnosis and configuration ports.
- Security gateways at transfer points / network limits.
- the isolation of sensitive systems.

3.12 Information transfer

Actions must be taken to ensure that personnel-related data and information and data requiring protection cannot be read, copied, modified or removed during electronic transfer or while they are transported or stored on data-carriers and that it is possible to check and discover at which points a transfer of personnel-related data and information and data requiring protection is possible by data transfer facilities. (This includes a description of the facilities used and transfer protocols, such as identification and authentication and encoding to the latest state of technology, automatic call-back, etc.)

This includes in particular:

- the secure transport and delivery of data / documents depending on the need to protect the data.
- the agreement of contracts for the protection of trade secrets with third parties and sub-suppliers.
- the recording of data transfers.
- the description of interfaces between systems and external data connections

3.13 Network separation

Groups of information services, clients, users and information systems should be separated from each other in networks.

This includes in particular:

- separating groups of information services, clients, users and information systems from each other.
- To reduce the risk that personnel-related data and information and data requiring protection are read on the network while they are being transferred between IT systems, these must be segmented.
- Direct connections by an Internet client via remote access (e.g., via VPN or RAS) to the company's network must be prevented by appropriate measures.

3.14 Obtaining, developing and maintaining systems

Actions and processes must be implemented to ensure that information security is an integral part of information systems over their entire lifetime.

This includes in particular:

- specifying security-specific rules and regulations covering the introduction of new information systems and the expansion of existing information systems.
- specifying rules for the development and alignment of software and systems.
- the development of guidelines for safe system development.
- monitoring external system development activities.
- the protection of test data.

3.15 Relationships with suppliers

Security measures to reduce the risks associated with the involvement of external parties should be agreed with sub-suppliers / sub-contrators and documented.

This includes in particular:

- the written addressing of security matters in contracts with sub-suppliers
- checking the security of sub-contractors

3.16 Managing information security incidents

Consistent and effective actions for the management of information security incidents (theft, system failure, data loss, etc.) must be implemented.

This includes in particular:

- the immediate reporting of information security incidents to the customer.
- the recording of security incidents.
- the implementing of processes for introducing action to prevent / prevent the recurrence of information security incidents.

3.17 Information security aspects of business continuity management/emergency management

System availability must be maintained in difficult situations such as crises or major damage. This must be ensured by an emergency management system. Requirements covering information security should be specified when planning the continuity of operations and recovery following an emergency.

This includes in particular:

- the creation of redundancies for critical components.
- assessing risks and planning actions to ensure continuation of the company's activities.
- the creation of emergency action plans.
- the regular execution of tests of the effectiveness of the emergency actions
- early information to the customer in the event of an emergency.

3.18 Compliance with legal and contractual requirements

Implement measures to prevent violations of legal, official or contractual obligations and any security requirements.

This includes in particular:

- the agreement of confidentiality obligations with employees and sub-suppliers.
- ensuring compliance with legal obligations within the framework of the cooperation.
- the return of all data, operating equipment and information data to the customer at the end of the contract.

3.19 Data protection requirements and data protection management

Protection in the private sphere, as well as the protection of personnel-related data should be ensured in accordance with relevant legislation, regulations and, if appropriate, the terms of a contract.

This includes in particular:

- the appointment of a data protection officer.
- the establishment of a data protection management system.
- the creation of procedure directories.
- the establishment of a management system for data protection in an emergency.
- the execution of regular checks / audits.
- compliance with legal requirements within the framework of contract data processing.
- the immediate reporting of data protection incidents to the customer.

3.20 Information security checks

Regular checks must be made to ensure that information processing is carried out in accordance with the defined securitry measures. The contractor must carry out regular checks in this regard.

The contractor will grant the customer the right to carry out regular checks at the contractor's premises.

4 Checking the implementation of security measures

KOSTAL reserves the right to check the implementation of the security requirements set out in Section 3.

The latest version of the VDA questionnaire and/or an individual assessment is used for the check. Alternatively, compliance with information security can be demonstrated with a TISAX assessment.