Table of contents

1 General provisions 2
2 Contractual regulation of relationships with external contractors 2
3 Protection of confidential information at meetings 3
4 Contracting partner's remote access 3
5 Termination of remote access 4
6 Physical access to information assets and information 4
7 Updating of security instructions for information security 4
8 Use of USB flash drives in process or production systems 4

1 GENERAL PROVISIONS

The purpose of the document is to define the procedures by the companies of the HSE Group, make sure that external interested parties (external contractors) ensure adequate protection of resources and provide the agreed level of services and information security. External contractors, consultants, and other individuals who are not regularly employed in the HSE Group are considered third parties or external contractors as per the definition of this policy.

All information obtained by the external contractor while working for the companies of the HSE Group is considered a confidential information, regardless of whether it is labelled as such or not. A confidential information also includes intangible knowledge that the external contractor acquires during its work, such as the organisation of processes and of physical security, and the like. The external contractor is obliged to protect all information obtained as confidential and may not disclose or use it in any other context without the explicit written permission of the responsible person of the HSE Group.

2 CONTRACTUAL REGULATION OF RELATIONSHIPS WITH EXTERNAL CONTRACTORS

The provisions on the acknowledgement of security requirements for external contractors, which are determined by security policies, are incorporated into a contract or added to the contract as an independent annex. The contract represents the legal basis for access by the external contractors to the organisation's data, i.e. information systems.

While cooperating with the contracting authority, external interested parties must be aware of its required security policies, which they confirm by signing a special document (information security statement). They are not permitted to access information and information assets until they sign the statement. They are also not permitted to have this access until suitable security and supervisory mechanisms have been implemented and the **required internal rules and the contract** that defines the conditions of access have entered into force.

The provisions oblige the external contractor:

- not to forward to unauthorised persons personal data, confidential informations and information obtained, accessed or learned in any other way during the implementation of contractual obligations,
- to protect information in such a way as to prevent unauthorised disclosure,
- not to use information in any way that is not determined in the contract,
- to make sure that their possible subcontractors are bound to protect confidential informations in the same manner as the external contractor itself,
- to observe that protection and non-disclosure also apply for all possible information or data that the external contractor received or became acquainted with before the conclusion of this contract.

As per the contract, security is implemented during the entire period of cooperation and for a certain period after the completion of cooperation with the external contractor. The contract concluded with the external contractor includes provisions referring to:

- the fact that all persons linked with the contractual implementation of services, including subcontractors, are aware of their obligations relating to the provision of suitable security,
- the method of reporting and informing about security incidents,

- the procedures for the protection of reresources for service implementation,
- the requirements relating to data protection,
- the management and accessibility of the list of contractors authorised for service implementation,
- the obligations referring to the installation and maintenance of the external contractor's software and hardware and required physical and logical supervisory mechanisms for accessing systems, services and information,
- the requirement that the external contractor protects the network from threats arising from external networks by means of equipment that ensures the highest possible security against malware and external intrusions into systems, services and data,
- the requirement that the external contractor will provide all data in connection with the provision of security of systems, services and information for service implementation based on a written request,
- the right to an audit review (the HSE Group reserves the right to examine the level of security provided by the external contractor by means of security checks of the external contractor's information system),
- the provisions determining the measures in the event of violations of obligations stipulated in the contract and the external contractors' responsibility or sanctions are also included in the contract,
- **the service continuity** is agreed on where necessary when ordering services from an external contractor if service has to be maintained in the event of unforeseen events, e.g. major breakdowns or accidents,
- contracts referring to personal data processing must include requirements in compliance with the General Data Protection Regulation,
- a non-disclosure agreement applies to all confidential informations or confidential data **as of their receipt,**
- external contractors may forward confidential information to third parties only on the basis of the prior written consent of the responsible person of the HSE Group.

3 PROTECTION OF CONFIDENTIAL INFORMATION AT MEETINGS

At meetings, we make sure that we know all the parties present and their roles before we start talking about confidential data. The task of the chairperson of the meeting is to initially introduce the attendees and explain the need for confidentiality to all the persons present.

Every attendee of the meeting is responsible for making sure that internal or confidential documents do not remain in the meeting room after the meeting ends "Put away paper documentation and clean the board."

4 CONTRACTING PARTNER'S REMOTE ACCESS

We give external contractors access exclusively to the information assets and systems that they absolutely need in the performance of contractual obligations, thereby preventing unauthorised access to other assets. To approve and implement a request for network access to external contractors, the service administrator prepares an application that must contain the prescribed information.

When accessing the network, the external contractors are authenticated with a unique identifier. All accesses of external contractors to the information system are recorded throughout the cooperation and are reviewed once every three months.

5 TERMINATION OF REMOTE ACCESS

The access of external contractors to the network is terminated immediately once the access to the information system is no longer needed or no later than when the contractual relationship between the HSE Group and the external contractor ceases to exist. The time of termination of the access of external contractors is reported to the information system administrator who approved the access.

Access to the network is also terminated in the event of a violation of security regulations and instructions.

If a violation of security regulations and instructions is suspected, access to the network is temporarily disabled until the actual state of the violation is established.

6 PHYSICAL ACCESS TO INFORMATION ASSETS AND INFORMATION

The equipment maintenance may only be performed by authorised external contractors with whom a contract is concluded with suitable provisions relating to information security. The access of external contractors to hardware is always supervised. Maintenance work is done at the location of the equipment. If this is not possible, the data carrier is removed from the equipment and stored safely. If the data cannot be removed or protected in another way, the maintenance procedure must be supervised.

7 UPDATING OF SECURITY INSTRUCTIONS FOR INFORMATION SECURITY

Information security instructions are revised once a year and adjusted if necessary to the new requirements of the HSE Group and standards. In the event of amendments, the revised security instructions are forwarded to the external contractors.

8 USE OF USB FLASH DRIVES IN PROCESS OR PRODUCTION SYSTEMS

Prior to the use of a USB flash drive in process or production systems, it is necessary to check the USB flash drive for malware on a dedicated computer. If malware is discovered on the USB flash drive, the latter must not be used.

Every check must be recorded on the form stored on the computer used for checking USB flash drives.