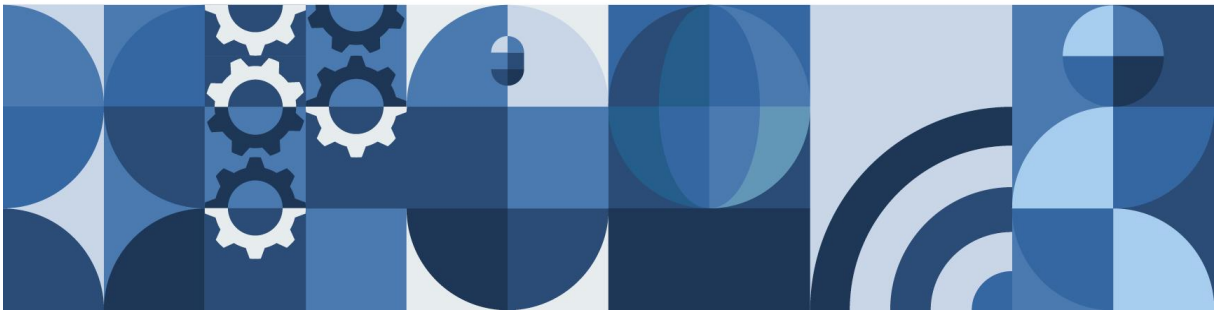
VOSS

IT & DIGITALIZATION



Information security requirements for external third parties

Version:	1.2
Date of the version:	21.01.2025
Confidentiality level:	INTERNAL / BUSINESS

Table of contents

1. INTRODUCTION 3

1.1. PURPOSE 3
1.2. SCOPE OF APPLICATION 3

2. GENERAL INFORMATION 4

3. INFORMATION SECURITY REQUIREMENTS 4

3.1. INFORMATION SECURITY GUIDELINES 4
3.2. DEALING WITH INFORMATION 4
3.3. IDENTITY MANAGEMENT 4
3.4. REMOTE WORK 4
3.5. PERSONAL SAFETY & TRAINING 4
3.6. SUBCONTRACTOR 5
3.7. ASSET MANAGEMENT 5
3.8. ENDPOINT PROTECTION 5
3.9. CRYPTOGRAPHY 5
3.10. SECURITY INCIDENTS & CONTINUITY 5
3.11. DATA BACKUP 6
3.12. PHYSICAL SECURITY 6

4. ADDITIONAL REQUIREMENTS FOR CONTRACTORS WORKING IN THE VOSS INFRASTRUCTURE 7

1. Introduction

1.1. Purpose

This guideline describes the minimum requirements for information security that must be observed by contractors of the client - the VOSS Group - when handling VOSS information and/or IT devices (e.g. computers, notebooks). The aim is to ensure confidentiality, integrity and availability of information and thus support the security of our business processes.

Contractors within the meaning of this regulation are subcontractors and suppliers of services and products.

In certain cases, customers of VOSS may, for their part, demand stricter information protection requirements that must also be met by affected/involved contractors.

1.2. Scope of application

These instructions apply to all contractors who process sensitive information for VOSS in accordance with contractual agreements or who receive such information from VOSS. Subsidiaries and branches of VOSS, as well as companies in which VOSS holds a shareholding, are excluded from this definition.

Deviations from these guidelines that reduce the level of safety are only permitted on a temporary basis and after consultation with the responsible bodies and the client VOSS and require justification.

Requirements in tenders or contracts apply independently of the requirements of this guideline for the contractor.

2. General information

To maintain information security, rules for cooperation and communication between VOSS and contractors are essential, especially if company confidential information is to be shared in the course of the business relationship.

VOSS has therefore voluntarily committed itself to operating its own information security management system (ISMS) in accordance with the information security standards of ISO 27001 / VDA ISA (TISAX).

3. Information security requirements

The Contractor has implemented the following information security requirements in its company:

3.1. Information security guidelines

The contractor has defined regulations on information security in its company and these have been approved by the management. These regulations have been published to the employees.

3.2. Dealing with information

Information must be classified according to its sensitivity and protected accordingly. Access to sensitive information must be controlled and documented. All employees who handle information are aware of the sensitivity classification and the rules derived from it.

3.3. Identity management

The registration, deregistration and allocation of user access (e.g. accounts, passwords) is a formal process and is documented. The handling of passwords and accesses is defined, and employees are obliged to comply with these requirements.

Access rights are assigned according to the need-to-know principle. The granting of privileged rights is restrictive. It is ensured that users can only access the information covered by their access authorization. It is ensured that the login procedures are carried out securely and are state-of-the-art.

3.4. Remote work

Security measures for working outside the company and measures to protect information accessed remotely have been implemented.

3.5. Personal safety & training

Confidentiality obligations are defined in contractual agreements between the contractor and its employees and contractors/subcontractors. Employees with access to sensitive information and/or areas/premises of VOSS have been checked.

Employees receive regular training on information security, IT security and data privacy.

3.6. Subcontractor

VOSS's consent is required for the commissioning of subcontractors by the Contractor if they are involved in any processes relevant to VOSS. If the commissioning of subcontractors is contractually regulated and VOSS has approved the commissioning, the Contractor must ensure that the information security level described here is also guaranteed at the subcontractor through contractual agreements and checks.

3.7. Asset management

All hardware and software components must be managed through a formal process over their entire life cycle. This includes procurement, maintenance and operation, decommissioning and disposal. Only licensed hardware and software are used to perform tasks.

The contractor should ensure that the software packages used for operating systems and applications originate from secure sources. The regular updating of the systems and applications used is ensured via a controlled process.

Measures have been implemented to prevent the unauthorized reading, copying, modification or deletion of data carriers (e.g. in notebooks, servers, external hard drives, USB sticks, etc.). There are rules and procedures for safe handling, disposal and transportation.

3.8. Endpoint protection

The Contractor shall ensure that the systems and hardware components operated by it are protected against malware, manipulation or data leakage in accordance with the state-of-the-art and are continuously monitored.

3.9. Cryptography

Sensitive data is encrypted both during transmission and storage.

3.10. Security incidents & continuity

Procedures for detecting, reporting and handling security incidents must be defined. Plans for maintaining business operations in the event of a security incident must be implemented.

Responsibilities and procedures for the detection, reporting and handling of security incidents are defined. Plans are also implemented to maintain business operations in the event of a security incident.

All reports of information security incidents involving VOSS data must be submitted to the following office as soon as possible: **informationsecurity@voss.net**

3.11. Data backup

The Contractor shall ensure that information is protected against loss at all times and can be restored within a reasonable period of time.

3.12. Physical security

Measures are in place to secure physical access to sensitive areas, information and systems. Identification of employees and external parties is possible (e.g. using employee ID cards or similar). It is regulated and ensured that only authorized personnel can access these areas.

4. Additional requirements for contractors working in the VOSS infrastructure

A contractor works in the VOSS infrastructure if:

- clients (physical or virtual end devices) are provided by VOSS, or
- the connection is made via remote access solutions with access to the VOSS internal company network (e.g. VPN), or
- the contractor is connected directly to the internal company network (e.g. IPSec tunnel).

The following requirements apply to these contractors:

- Regulations of the respective VOSS subsidiary(s) regarding the bringing of non-VOSS IT equipment onto the company premises or into security areas must be observed.
- The equipment provided must be handled properly and protected against loss or unauthorized modification.
- The manufacturer's instructions for protecting the devices must be observed.
- Devices provided by VOSS (e.g. notebooks) may only be taken off the factory premises after approval has been granted.
- Contractors may only carry out or initiate the provision or installation of hardware and software via the VOSS department responsible for them.
- Opening the IT device and making changes to the hardware (e.g. installation/removal of hard disks, memory modules) as well as manual changes to the security settings (e.g. browser settings) is only permitted for the responsible departments at VOSS.
- The use or subsequent modification of the programs provided by VOSS is only permitted if this has been approved by the responsible authorities.
- No data from other customers who do not belong to the VOSS Group are to be processed on the IT devices provided.