Information security requirements for suppliers and business partners

TABLE OF CONTENTS

1 PRINCIPLES

1.1 INTRODUCTION

Information is a key asset of the Swoboda Group. Therefore, the protection and security of this information is of utmost importance to Swoboda. The primary corporate objective of effectively protecting central business processes, as well as the information assets and IT systems required for them, is achieved by establishing globally applicable security standards and integrating information security into internal processes.

Suppliers whose services (in the form of software, hardware or services for systems) are used at Swoboda must meet the minimum requirements described in the document regarding the quality of their work and compliance with information security measures.

1.2 GOALS

The aim of this document is to ensure the secure integration of service providers and suppliers into business operations. This includes describing the necessary information security regulations as a basis for contract design with third parties. These regulations aim to protect the confidentiality, availability, and integrity of the Swoboda Group's information, as well as its rights and interests regarding information assets.

1.3 SCOPE OF APPLICATION

The scope applies to affiliated companies and all other persons or entities, such as external partners or suppliers, who have access to information of the Swoboda Group. This includes not only electronically stored information but also documents and conversations.

1.4 DEFINITIONS AND DESIGNATIONS

Contractor	A contractor is the party that is commissioned by a client (Swoboda company) to carry out a specific business or service. The contractor assumes responsibility for the execution of the contract and must meet the conditions and requirements specified in the contract.
Client	A client is the party that commissions another party (the contractor) to carry out a business transaction or service as part of a contract.
Information owner (data owner)	The data owner (information owner) is responsible for a specific part of the data within an organization. He has full control over the data and ensures its protection and quality.

2 BASIC SECURITY REQUIREMENTS

External companies and their employees (contractors) who work for the Swoboda Group (client) commit to the following upon acceptance of the contract:

- Implementing appropriate security measures according to the current state of technology in relation to their services for the Swoboda Group. The basis for this includes: TISAX ISA Catalog, ISO 27001, EU GDPR, BSI IT-Grundschutz Compendium, and other relevant legal and industry-specific requirements.
- Maintaining confidentiality regarding internal information of the client and its employees. This obligation continues even after the termination of the contractual relationship.
- Proper handling and classification of digital and physical data and information according to the Swoboda Group's protection class concept.
- Not connecting external devices to the company network. Exceptions include approved VPN connections or the guest Wi-Fi.
- Sending, taking, or copying internal, confidential, and top secret documents only after approval by the internal data owner.
- Using smartphones, video cameras, or other image or audio recording devices only with prior permission from the internal contact person.

3 PERSONNEL

The Contractor shall ensure that

- a contact person responsible for information security is named to the client.
- only reliable and competent personnel are deployed for the fulfilment of the order and related services (e.g. administration of the client's IT systems, performance of internal maintenance work).
- its employees to take part in the annual IT security, information security and data protection training courses.
- the client must be informed immediately of any relevant personnel changes.
- the employees and, if applicable, subcontractors have been demonstrably made aware of their responsibilities and obligations with regard to information security and customer agreements, in particular the requirements of the client.

Anyone acting on behalf of the contractor who needs to have remote or local access to Swoboda Group systems must provide information about their identity. The contractor shall ensure that no access is misused in its name and shall assume full responsibility should this occur.

4 DEALING WITH INFORMATION VALUES

When storing, transferring, processing, archiving, destroying or deleting information and data carriers, the legal requirements must be taken into account and all protection objectives, such as confidentiality, availability, integrity, reliability, dependability and privacy, must be guaranteed at all times.

4.1 CLASSIFICATION AND LABELING OF INFORMATION VALUES

The classification of the information will be specified by the information owner (data owner) of the client on the basis of the following classification criteria and must be maintained throughout its entire life cycle and may only be changed after approval by the information owner of the client.

The following levels are defined for classifying information with regard to confidentiality requirements:

Top Secret
Unauthorized publication or disclosure of such information may result in major negative consequences or serious disruption to business activities. Access to top secret information must be limited to a small and specifically named number of individuals. Use this classification sparingly. The disclosure of the information may cause damage that threatens the existence of the company. Top secret information and documents must be marked with their classification level. Data on external media and storage devices with top secret content must be encrypted.

Confidential
This includes information whose publication could cause considerable damage to the future development of the company (competition, finances, legal situation). Personal data must be classified at least as confidential. Disclosure of the information could cause considerable damage and therefore this information must only be made accessible to a limited, authorized group of people. Confidential information and documents must be marked with their classification level. Confidential information that is passed on to parties outside Swoboda must be marked according to its classification level. Data on external media and data carriers with confidential content must be encrypted.

Internal
Information accessible to all employees, but not intended for the public. Forwarding only to internal employees. External parties may only access the information with the permission of the information owner. The use of company information in the public domain must be agreed in advance with the responsible departments. Disclosure of the information can cause minor to moderate damage. Internal information and documents must be marked with their classification level.

Public
Such information can be made available to the general public, so no protective measures are required. Disclosure of the information has no negative impact. It is recommended to mark

public information and public documents with their classification level. External disclosure of public information and documents requires the approval of the contracting authority.

4.2 PROCESSING OF PERSONAL DATA

Personal data may only be collected and processed on a legal basis. In the case of commissioned processing, corresponding contractual agreements must be made, which include detailed provisions on technical and organizational protective measures.

4.3 NEED-TO-KNOW PRINCIPLE AND LEAST-PRIVILEGE PRINCIPLE

In general, the granting of permissions and access to information must be based on the need-to-know principle and the least-privilege principle.

4.4 PROTECTION OF DATA STORAGES

Confidential, top secret, and personal information must be stored encrypted or kept on encrypted data storages.

Information that is no longer needed must be promptly and securely deleted from the data storages.

4.5 STORAGE OF INFORMATION IN EXTERNAL IT SERVICES (CLOUD)

The processing of the client's non-public information in external IT services (cloud) is permitted, provided that the contractor ensures that the external service offers an equivalent level of security.

4.6 TRANSFER OF INFORMATION VALUES

Internal, confidential, top secret and personal information must always be encrypted when transmitted via insecure networks (e.g. Internet, Wi-Fi).

Confidential, top secret and personal information should be encrypted when transmitted over secure networks (e.g. local, wired network) if technically possible.

4.7 PROVISION OF HARDWARE AND SOFTWARE

If hardware and software are provided to the contractor by the client, they may only be used for storing and processing the client's information. Information that is not related to the fulfilment of the task (e.g., private information or information from other clients) may not be stored or processed on the provided devices. The client reserves the right to terminate the provision at any time. The installation of third-party software on devices provided by Swoboda requires approval from the client. Disabling protective measures (e.g., changing system configurations, disabling malware protection or local firewall, installing software not approved by Swoboda, etc.) is not permitted.

4.8 RETURN AND DELETION

Devices and data storages provided by Swoboda that are no longer needed must be returned to the client immediately, but no later than at the end of the contract. Information stored on the contractor's data storages must be fully handed over to the client at the end of the contract and then securely deleted. Contractually defined and legal retention and deletion periods must be observed.

5 SECURITY OF IT SYSTEMS

5.1 IT SECURITY MEASURES

If the contractor's IT systems are used for the creation, transmission or storage of data for the client, the contractor ensures compliance with appropriate IT security measures for these systems according to the current state of technology, including:

- Access management, rights and role concepts, secure passwords
- Patch, capacity and vulnerability management
- Data backup
- Communication security
- System hardening
- Cryptography
- Malware protection
- Logging
- Documentation

5.2 ACCESS TO IT SYSTEMS

Access to IT systems and applications must be exclusively via personalized access data, i.e. a user ID and an individual password. Sharing personal access data with third parties is prohibited. Access data must be stored securely. Collective accounts are not permitted.

5.3 PASSWORD AND PIN SETTINGS

When using user accounts (standard users, technical users, privileged users, etc.) to log in to IT systems and applications or when encrypting files, the password complexity must be designed as follows:

- The password must contain at least 3 out of 4 of the character types upper case letters, lower case letters, numbers and special characters (e.g. !$%&).
- When using password managers, the master password must contain 4 of 4 character types (upper case letters, lower case letters, numbers and special characters (e.g. !$%&).
- The minimum password length must be 12 characters (also for Office documents, ZIP archives, etc.).
- The minimum password length for privileged accounts and service accounts must be at least 15 characters.

Passwords must not be easy to guess. The following rules apply in particular
at least organizationally:

- No use of easily identifiable data from the personal environment (e.g. name, date of birth, company name or cost center) or passwords that are used in the private environment
- No use of the user ID as part of the password.

- Avoidance of terms taken from dictionaries.
- Avoid cyclical passwords (e.g. word01, word02).
- Do not use keyboard sequences (e.g. asdfgh), number sequences (e.g. 123456) or alphabet sequences (e.g. abcdef).
- The number of the last passwords that may not be used (password history) must not be less than ten.

Passwords must be changed in the following cases:

- Default passwords/initial passwords of IT systems and applications.
- In the event of (suspected) knowledge of the password by an unauthorized third party.
- If a previous authorized user no longer needs the password for their tasks, provided the user account is not deactivated or deleted (e.g. for technical user accounts).
- Passwords from development, test, and integration environments when the IT system or application is put into operation.

5.4 MULTI-FACTOR AUTHENTICATION

Multi-factor authentication must be implemented for access to IT systems where confidential, top secret, or personal information is processed and/or stored, or where there is a high risk due to the compromise of the administrator or user account.

Multi-factor authentication is mandatory for VPN access.

6 SECURE SOFTWARE DEVELOPMENT

If the contractor develops or supplies software for the client, the contractor warrants that

- a secure test and development environment (e.g., access to source code, version control) is maintained.
- compliance with security guidelines and best practices for secure development (security and privacy by design / by default, principle of least privilege, segregation of duties) is ensured.
- security in the software development methodology (e.g., regular checks, code reviews) is implemented.
- the use of secure repositories.
- the client's company data, which is hosted by external service providers as part of software development projects, is stored, processed, and transported separately from the data of other customers of the service provider.
- software maintenance and support of the application are carried out exclusively via the secure remote access of the client.

7 DOCUMENTATION

The Contractor shall prepare detailed documentation (in particular in the design or development phases of applications and systems) and deliver it to the client. The contractor shall ensure that

- the entire development process, from the requirements and design phase through development and quality assurance to transfer to production and subsequent software maintenance, may only take place on the basis of a documented and approved specification.
- the documentation must be carried out in such a way that a technical expert can understand and further develop the program code with the help of the documentation.
- project, function, and interface documentation must be created in full and kept up to date.
- user and administrator documentation is produced to provide assistance with the use and administration of the application.

8 PHYSICAL AND ENVIRONMENTAL SECURITY

The contractor must ensure that unauthorized access to rooms, offices and facilities in which Swoboda Group information is processed is prevented. This also applies to production, delivery and loading areas through which unauthorized persons could gain access. The protection of offices is particularly important.

All provided information assets (e.g. documents, prototypes) and equipment made available must be handled properly in accordance with their classification and protected against access by third parties, loss, and theft.

The contractor is obliged to create policies that prescribe a tidy working environment and the activation of screen locks when not in use.

If the processing, storage, or retention of data is part of the contract content, the contractor ensures that measures for physical security and access protection are taken. These include, among others:

- Protection against fire and water
- Protection against or avoidance of extreme temperatures (air conditioning)
- Emergency power supply (UPS, emergency generator)
- Access protection and theft protection (electronic access control / locking system, alarm system, video surveillance)

9 REPORTING OBLIGATIONS

The contractor is obliged to immediately report to Swoboda any security incidents in its organization that are related to the contractual agreement and could potentially have a negative impact on material or immaterial assets of the Swoboda Group. These include, among others:

- Violation of laws, contractual regulations and requirements
- IT and information security incidents (e.g. industrial espionage, hacker attacks or security vulnerabilities in source code)
- Data protection incidents (e.g. disclosure of personal data)
- Other risks (e.g. vulnerabilities in IT systems)

In the event of an incident, the contractor shall provide resources upon request to mitigate, report, preserve evidence and remediate the incident, as well as the final corrective action report.

10 REVIEW OF IMPLEMENTATION

The contractor agrees, upon acceptance of the contract, to:

- Conduct or commission regular internal audits to a reasonable extent regarding compliance with and implementation of security measures.
- Allow the client, upon request, to conduct a reasonable review of compliance with and implementation of security measures through on-site audits or in the form of requested evidence (e.g., TISAX label, ISO27001 certificate) and to support this to the best of their ability, with on-site audits generally needing to be announced in advance.

11 CONTACT

For questions and to report security-related incidents, security or data protection incidents, and other risks, the following contacts are available:

Information Security Officer: informationsecurity@swoboda.com
Data Protection Officer: datenschutzbeauftragter@swoboda.com

12 DOCUMENT HISTORY

Date	Description	Employees
01.02.2025	First version	Information Security Officer