Information Security Standard for External Companies

Table of contents

1 Purpose

Information is one of the most important assets of the Eberspächer Group of Companies ("Eberspächer Group"). Due to the strategic importance that information holds for the Eberspächer Group, the security of such information is a key aspect of the Cooperation with external parties. The regulations described in this document aim to protect the confidentiality, availability and integrity of information within the Eberspächer Group, as well as the Group's rights to and interest in information assets.

This standard describes specific requirements and regulations for ensuring that the information assets of the Eberspächer Group (referred to below also as: "Eberspächer" or "Customer") are handled in a secure manner. It is aimed at the management teams at external companies. These includes suppliers, service providers and other partners (referred to below also as: "Contractor"), the employees thereof and at all third parties involved in the fulfilment of contractually agreed services.

2 Scope

This document is a mandatory requirement for all indicated contractors of the Eberspächer Group.

The regulations as described must be applied for all information assets of the Eberspächer Group. In addition to information saved electronically, documents, discussions and prototypes are also regarded as information assets.

3 Definitions/terms/abbreviations

Contractor	Suppliers, service providers and partners providing contractually agreed services on behalf of an Eberspächer Group company.
Information Managers	Information Managers are responsible for classifying information, defining the permitted group of recipients and authorizing access (e.g. assignment/approval of privileges).
NDA	Non-Disclosure Agreement
Level of Security	Protection in accordance with the NDA(s) and recognised standards (e.g. Annex A of ISO/IEC 27001)

4 Handling information assets

4.1 Classification and identification of information assets

Confidentiality must be maintained during the disclosure, transmission, safekeeping, storage, destruction and deletion of information and information storage media. The confidentiality of information is specified by the Customer's Information Manager according to the table below.

The classification of information must be maintained throughout the life cycle of the information and is allowed to be changed by the Information Manager only following approval.

Confidentiality	Description
Public	Information intended for use by the general public. **Read access:** No restriction **Write access:** Following approval **Delete access:** Following approval **Use in public:** After approval by the client
Internal	Information intended for internal use (customer's employees and authorized contractors). Restrictions as for "Public", except: **Reading access:** Only internal employees of the contractor who need access to the information according to the need-to-know principle; external employees and partners according to the signed NDA. **Public use:** Forbidden **Protective measures:** Effective access security and transport encryption. **Disposal:** Secure destruction of the information in accordance with the state of the art. **Physical security:** Compliance with the specifications in chapter 4.5.
Confidential	Information intended for use only by defined groups of people. Restrictions as for "Internal", except: **Access:** Only defined groups of persons within the scope of the cooperation. Disclosure to third parties only with appropriate security level or clearance by the customer.

Strictly confidential	Information intended for use only by defined individuals. Restrictions as for "Confidential", except: **Reading access:** Only defined individuals in the context of collaboration. **Protective measures:** Consistent secure encryption of data during transmission (end-to-end) and storage. If encryption is not possible, information must be protected by comparably effective measures.

"Strictly confidential" information must be explicitly marked as such (e.g. confidentiality flag) and treated with special care.

In the absence of any other agreement with the Information Manager, information entrusted to the Contractor must be treated as *confidential*.

4.2 Data protection

Personal data are allowed to be collected and processed only if there is a legal reason for doing so. In case of processing by order, contractual regulations that set out more detailed provisions, for technical and organizational protective measures for example, must be agreed accordingly.

4.3 Protection of confidentiality, availability and integrity

4.3.1 Access protection

The Contractor is under an obligation to employ suitable measures to protect the information entrusted to it by the Customer against unauthorized access (read, write, delete). This includes encrypting non-public information for transmission over public networks.

Access to the Customer's information assets must be restricted according to the **"need-to-know"** principle, meaning that access to certain information is granted only to those persons who need it to accomplish the tasks assigned to them. The Contractor is allowed to access information only for the purposes of accomplishing the assigned tasks. Authorized persons must also be committed to maintain confidentiality.

4.3.2 Handling of identification / authentication means

Personal identification / authentication means (e.g. passwords, PINs, access cards) that serve to access the Customer's information must never be disclosed. They must be kept in a safe place at all times.

Any passwords used to access the Customer's information must comprise at least eight characters (twelve characters for accounts with administrative privileges) and characters from at least three of the following categories:

- upper case letters (A-Z*)
- lower case letters (a-z*)
- numerals (0-9)
- special characters
- characters categorized as part of the alphabet, but which are neither upper nor lower case letters. Including in particular characters of the Asian languages.

*Including in particular diacritical, Greek and Cyrillic characters.

Any PINs used to access the Customer's information must comprise at least six characters.

The use of commonplace character and number sequences (e.g. 123456, abcd, 000000, etc.) and readily guessable character sequences (e.g. names, years, personnel numbers, natural language words, etc) in passwords or PINs is not permitted. The same passwords and PINs must not be used for different IT services and applications.

Passwords and PINs for access to information and customer systems must be changed regularly, but at the latest after six months. Alternatively, compensatory measures (e.g., 2FA) must be defined and used. Expired identification means must not be reused and have to differ from their predecessor by at least three characters.

4.3.3 Protection of information availability

The Contractor must employ suitable measures (e.g. regular backups) to protect the availability of the Customer's information assets. The permanent loss of the Customer's information or information storage media must be communicated immediately as an information security incident.

4.3.4 Disclosure and exchange of information

The disclosure/exchange ("disclosure") of non-public information of the customer within the meaning of chapter 4.1 is subject to the provisions of the concluded NDA or must be additionally regulated therein, if applicable.

The processing of the customer's nom-public information in external IT services (cloud) is permitted, provided that it is ensured by the contractor that the external service offers an equivalent level of security.

Insofar as an information asset is not explicitly identified during exchange, the classification must be communicated to the recipient.

I	**NOTE**
For the processing of personal data, the requirements in 4.2 also apply.	

4.4 Protection of software and hardware

4.4.1 Provision

Insofar as the software or hardware required to accomplish tasks is provisioned by the Customer, this must be used as priority for saving and processing the Customer's information.

Information not related to fulfilling tasks (e.g. private information, information from other customers) must not be stored or processed on provisioned devices.

The Contractor is responsible for ensuring that the software and hardware provisioned for the purpose of accomplishing the tasks assigned to it is used in a proper manner. The Customer reserves the right to stop provisioning at any time.

4.4.2 Installation and change

The installation of third party software on devices provisioned by Eberspächer is subject to the Customer's approval. In the absence of any agreement to the contrary, deactivating protective measures (e.g. anti-virus software) and making changes to the operating system configuration on provisioned devices is forbidden.

Firmware and software updates provisioned by the Customer must be installed without delay.

Third-party devices (e.g. laptops, smartphones) may only be connected to the Customer's network upon written agreement.

4.4.3 Protection of data storage media

When using mobile data storage media, it is important to ensure that only the most essential information is saved and information no longer required is permanently deleted.

Confidential and strictly confidential information must essentially be stored on encrypted data storage media. Exceptions must be approved by the Customer beforehand.

4.4.4 Return and deletion

Devices and data storage media provisioned by Eberspächer and no longer required must be returned to the Customer immediately, no later than at the end of the contract.

At the end of the contract, all information stored on the Contractor's data storage media must be delivered to the Customer and then permanently deleted. Contractually defined and statutory retention and deletion periods must be observed.

4.5 Physical security

All 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.

Devices and information provided are allowed to leave the Customer's premises only with the Customer's consent.

On leaving the workplace, devices in operation must be protected against unauthorized access (e.g. password-protected screen lock).

It must be ensured that devices on which the Customer's non-public information is processed are setup in such a way that the information cannot be seen by unauthorized third parties. This applies both inside and outside business premises.

The loss of any information assets and devices belonging to the Customer must be notified immediately. This also applies in the event of a short-term loss if access by unauthorised persons cannot be excluded.

I	NOTE
Site-specific regulations concerning physical security (e.g. special protected zones, ban on photography) are shown locally and must be observed accordingly.	

4.6 Reporting obligations

The Contractor is obliged to communicate to the Customer immediately any events and risks relevant to information security that concern the information that has been provided by the Customer.

Including:

- **Infringement of laws, contractual regulations and specifications**
- **Information security incidents** (e.g. suspicion of malware, breach due to theft)
- **Data protection incidents** (e.g. disclosure of personal data)
- **Identified risks** (e.g. weaknesses in IT systems)

*	TIP
Contact addresses for reporting events and incidents concerning information security and data protection that are relevant to third-party companies can be found in Chapter 4.10 of this document.	

The Contractor is obliged to record and analyze reportable incidents within its area of responsibility and to employ suitable measures to rectify such incidents.

The Contractor is also obliged to report immediately any privileges no longer required (e.g. for IT systems or access controls).

4.7 Intellectual property rights

The Contractor must safeguard intellectual property rights as part of accomplishing the tasks assigned to it. These include, but are not limited to, copyrights, image rights, Eberspächer IP or licenses.

Granted software licenses can be used only for the agreed purpose and in compliance with the license agreement of the manufacturer. Under current legislation, the use of unlicensed software is forbidden.

4.8 Compliance with specifications

The Contractor must guarantee compliance with the described specifications concerning information security. Within the Contractor's organization, clear responsibilities for compliance with and implementation of the described specifications must be assigned for this purpose. In particular, the Contractor's employees are obliged to comply with the information security specifications.

In addition to the specifications set out in this document, statutory requirements for data and information protection must be observed as part of accomplishing the assigned tasks.

All information security specifications in this directive are also binding for sub-contractors that have access to the Customer's information. The Contractor is responsible for ensuring that sub-contractors are aware and comply with the specifications.

Non-compliance with or breach of the agreed regulations is reviewed in accordance with operational and statutory regulations and punished accordingly.

4.9 Review

The Contractor is obliged to review compliance with the relevant requirements and specifications concerning information security within its organization on a regular basis. Moreover, any sub-contractors must also be subjected to regular reviews.

In addition, the Eberspächer Group reserves the right to review compliance with the requirements and specifications concerning information security at the Contractor. The Contractor is obliged to assist with such reviews by providing self-assessments and suitable documentary evidence.

4.10 Contact

The following contacts are available to answer technical questions and to report security-relevant events, incidents and changes:

Information security contact person: informationsecurity@eberspaecher.com

Data protection contact person: datenschutz@eberspaecher.com