PREH GmbH

1. Purpose

The purpose of this document is to define information security regulations to be followed by partner companies when handling PREH information.

The guideline is addressed to the management and employees of the partner companies.

1. Target Group

Target Group	Note
Partner companies (service providers/suppliers) with access to information	until chapter 3.8
Partner companies (service providers/suppliers) with access to IT system of PREH	until chapter 4.3

3. General Requirements

3.1 Classification of information

If the classification is not known, then the classification of the information or data must be requested from the PREH contact. Information shall be protected throughout the life cycle according to its classification. The current classification of the information must be confirmed by the PREH contact person. The levels of classification are based on the VDA white paper "Harmonization of classification levels".

3.2 Labeling and handling of information

Classification	Requirements
confidential	Labeling: PREH is responsible for the definitions of the labeling. Storage: encrypted Transport: encrypted (e.g. TLS). Disposal: Dispose of documents in shredder, min. ISO21964 security level 4. Deletion of data on data carriers.
strictly confidential	Labeling: PREH is responsible for the definitions of labeling. Storage: encrypted Transport: end-to-end encryption. Disposal: Dispose of documents personally in shredder, min. ISO21964 security level 5. Secure deletion of data on data carriers.

3.3 Checking for Malware

The partner company must check the information regarding malware before delivery or transmission. This must be done using current test cycles and analysis options.

If malware is detected at the partner company, the contact person of PREH must be informed immediately. Furthermore, the effected data carrier may no longer be used.

3.4 Backup of informationen

Information is to be stored in such a way that central data backup can take place.

In case of non-central storage, the employee of the partner company is responsible for the data backup.

The data backups are to be protected like the normal information.

3.5 Clean Desk

The workplace is to be left “clean desk” after completion of the work. All PREH documents and information that are no longer required must be stored in a lockable container.

Unauthorized third parties must not have access to PREH documents or information.

3.6 Access rights to information and systems

Access rights to PREH information are to be assigned according to the need-to-know principle. These must be checked regularly and revised if necessary. Access to information must be adequately secured (e.g., strong authentication).

3.7 Exchange of informationen

All data carriers containing PREH information must be protected against loss, destruction, manipulation and unauthorized access. Data carriers that are no longer relevant must be destroyed according to standard procedures (see 3.2).

Data may only be exchanged via data exchange channels approved by PREH. For this purpose, the partner company must obtain information from its PREH contact person.

The partner companies must ensure that no unauthorized third parties can listen in on confidential information or gain access to it. When sending e-mails, the distribution list must be limited to the necessary extent.

3.8 Handling of information security incidents

Information security incidents affecting PREH's data or systems must be reported immediately to PREH's security organization security@preh.de and to PREH's contact person.

Examples of information security incidents include hacking, theft or loss of PREH information.

3.9 Data protection & legal and contractual requirements

The respective country-specific requirements and laws about data protection must be complied with by the partner companies.

The partner companies should maintain compliance management and implement legal and operational requirements in all cases.

Only licensed software is to be used. Software may only be installed by authorized personnel.

The contact person for the topic of information security is to be communicated to PREH's purchasing department.

Employees of the partner company are to be trained on the requirements of PREH. The "Security guideline for partner companies" can be included for this purpose.

4. Requirements for partner companies with direct access to the preh network

The following requirements must be met by partner companies that are assigned to one of the listed categories:

- Partner companies that have been provided with a client by PREH.
- Partner companies that have remote access (e.g. Citrix) or other VPN solutions with direct access to the PREH network.

It does not matter whether the employee of the partner company is located on its own premises or on the premises of PREH.

The provision, installation of hardware and software may only be performed by IT personnel of PREH. The change of settings is only allowed by IT personnel of PREH. The devices of PREH may only be opened by the specific IT personnel of PREH.

Only PREH data is to be used on PREH devices. The devices are to be handled properly and protected against loss.

4.1 Handling of login information and media

Login information and media (e.g., passwords, tokens) must not be disclosed to unauthorized persons. If compromise is suspected, the account password must be changed immediately.

Temporary passwords must be changed when logging in for the first time. When leaving the workplace, the client must be locked and tokens must be taken with it. Only passwords depending on the classification of the processed information may be used. International or national specifications and recommendations (e.g. NIST, BSI) should be taken into account for this purpose.

4.2 Access rights to information and systems

Access rights to PREH systems must be requested through the contact person. A list of partner company personnel who will be granted access to systems must be provided to the PREH contact upon request.

4.3 Access to the network

IT devices may only be connected to the VPN to PREH as long as it is necessary for work. Private internet use is not permitted.

The partner company undertakes to comply with the regulations of this security guideline.

Partner Company

Place, date

Signature

Name:

Function:

Signature

Name:

Function: