

- Guideline -

# Information security requirements for contractual partners

**Publisher: IT**

**Table of contents**

1	Aim and purpose.....	3
2	Scope of application .....	3
3	Audit law .....	3
4	IT security policy and standards.....	3
5	Information security information for contractual partners.....	3
6	Asset Management .....	4
7	User authentication.....	5
8	Password policy.....	5
9	Incident Management.....	6
10	Network security .....	6
11	Encryption of laptops and mobile storage capacities.....	7



12	Vulnerability Management.....	7
13	Change management.....	7
14	Backup .....	7
15	Client systems .....	8
16	Monitoring .....	8
17	Server Security .....	8
18	Mobile devices .....	9
19	Protection against malicious code .....	9
20	Access to data centers/ server rooms.....	9
21	Destruction of storage media.....	9
22	Final provisions.....	9
23	Change history .....	10

## 1 Aim and purpose

This document sets out WEBER-HYDRAULIK's expectations for protecting the confidentiality, integrity and availability of its data and assets.

Violation or disregard of these regulations may have legal consequences.

## 2 Scope of application

This guideline applies to contractual partners who provide deliveries and services for WEBER-HYDRAULIK on the basis of contractual regulations.

The regulations laid down in the guideline for action must be complied with. Deviations are only possible with the approval of the client.

## 3 Audit law

WEBER-HYDRAULIK is entitled to audit contractual partners on the basis of the guideline at least once a year.

## 4 IT security policy and standards

Contractual partners with access to WEBER-HYDRAULIK information must comply with its information security guidelines and the associated documents.

Furthermore, contractual partners must have suitable cyber risk governance processes in place to ensure the risk for the IT systems they use with regard to the confidentiality, availability and integrity requirements of WEBER-HYDRAULIK.

Guidelines and standards approved by the contractual partner's management must be in place to manage cyber risk. These must be demonstrably reviewed at least once a year.

## 5 Information security information for contractual partners

Within the framework of existing contractual and supply relationships, it is of the utmost importance that contractual partners comply with the security interests and information security requirements of WEBER-HYDRAULIK and its customers. For this reason, all scopes classified accordingly (such as design and development data and other correspondingly critical information) must be processed and protected in an appropriate manner.

TISAX (Trusted Information Security Assessment Exchange - [www.tisax.org](http://www.tisax.org)) and TPISR (Third Party Information Security Requirements - <https://www.aiag.org/supplychain-management/cybersecurity>) define industry standards for information protection and set out assessment requirements that must be guaranteed within the supply chain.

The contractual partner is required to actively ensure that its deliveries and services (this includes in particular data and critical information) have been classified accordingly and that a certified information security management system (e.g. ISO 27001) is operated. Contractual partners who provide deliveries and services in connection with the automotive business area of WEBER-HYDRAULIK must present a valid TISAX label upon request.

In accordance with the information security requirements of WEBER-HYDRAULIK, the contractual partner shall be obliged to secure all deliveries and services, as well as the entire related data stock of WEBER-HYDRAULIK, against unauthorized access, modification, destruction and other misuse in accordance with the state of the art. Furthermore, WEBER-HYDRAULIK data shall be strictly separated from data of other customers of the contractual partner.

If an identified, significant case of a breach of information security occurs, the WEBER-HYDRAULIK information security officer must be informed immediately.

Contact details:

**Ruth-Maria Gerlach**

[Data-Security@weber-hydraulik.com](mailto:Data-Security@weber-hydraulik.com) Phone:

+49 7161 / 65 393 30

Furthermore, the contractual partner must ensure that its subcontractors meet the described information security requirements by means of suitable contractual provisions.

## 6 Asset Management

The contractual partner shall treat information provided by WEBER-HYDRAULIK in accordance with the classification specified by WEBER-HYDRAULIK, but at least as confidential information.

Regular inventories of assets must be prepared and updated.

Strong encryption must be used for the transmission of information.

The forwarding and duplication of confidential documents as well as the utilization and communication of their contents is not permitted without the prior written consent of WEBER-HYDRAULIK.

WEBER-HYDRAULIK information may not be stored, printed, copied, passed on or processed in any other way outside the contractually agreed purpose.

Violations will be prosecuted accordingly.

## 7 User authentication

Access to the contractual partner's IT systems or to WEBER-HYDRAULIK data located there shall only be possible for securely identified (authenticated) users. For this purpose, the identity of a user must be securely established by means of suitable procedures.

Access controls must be implemented for information systems, networks and applications that

- check the identity of all users and
- restrict access to authorized users only.

Access controls must be based on a role-based access model. There must be differentiated access levels for end users and privileged access (e.g. system administrators).

The assignment process (assignment/modification/deletion) for privileged user IDs must be justified and documented. Privileged rights are only assigned after approval.

Access for information systems, network devices and applications must be checked regularly. If access is no longer required, it must be revoked.

## 8 Password policy

The following minimum requirements must be met when generating passwords:

- Password change: Change every 180 days
- Password complexity criteria:
  - Minimum length: 10 characters consisting of
    - at least 1 number
    - at least 1 special character
    - at least 1 capital letter
    - at least 1 lower case letter
- No reusability of the last 10 passwords
- The password can be changed again after one week at the earliest
- If a user enters an incorrect password five times in a row, the user account in question will be blocked

## 9 Incident Management

The contractual partner must have a documented process for the management of security incidents in order to recognize and deal with incidents.

Reported security incidents must be reviewed and then analyzed to determine their impact. All confirmed incidents must be classified, prioritized and logged. Every security incident must be reported to WEBER-HYDRAULIK.

Contact details of the information security officer:

**Ruth-Maria Gerlach**

[Data-Security@weber-hydraulik.com](mailto:Data-Security@weber-hydraulik.com) Phone:

+49 7161 / 65 393 30

Safety incidents must be handled by personnel trained in the handling and assessment of safety incidents. It must be ensured that suitable procedures for the identification, recording, procurement and preservation of information, its disclosure and duplication are not carried out without the prior written approval of WEBER-HYDRAULIK.

The contractual partner shall be obliged to cooperate with WEBER-HYDRAULIK in the processing of these reports.

## 10 Network security

The contractual partner must be able to demonstrate a suitable network security infrastructure. This includes, but is not limited to, detection/prevention systems (IDS/IPS) and other security controls that provide continuous security and have the ability to restrict unauthorized network traffic and detect and at least limit attacks, including their effects.

Remote access to the contractual partner's network must be approved and restricted to authorized personnel. Furthermore, remote access must be secured by secure access control protocols and suitable encryption.

Unused ports and protocols must be deactivated on servers in order to limit the attack surface.

Network connections used to transmit confidential and strictly confidential data must be encrypted.

The contractual partner must maintain a formal procedure for the approval, testing and documentation of the entire network.

## 11 Encryption of laptops and mobile storage media

Devices of the contractual partner on which WEBER-HYDRAULIK data is located must be appropriately encrypted and the implementation of the encryption must be continuously validated. A corresponding key management system must be in place.

Strong cryptography and security protocols (e.g. TLS, IPSEC, SSH, etc.) must be used to protect confidential information during transmission over open public networks.

Mass storage devices in mobile devices (laptops, tablets, smartphones) must be encrypted.

## 12 Vulnerability management

The contractual partner must immediately follow up information from technology providers and other sources regarding technical vulnerabilities of operating systems, applications and network devices. Vulnerabilities must be assessed immediately to ensure that appropriate measures are taken and to counter potential risks.

Furthermore, the contractual partner must operate a patch management system, apply available patches immediately and patch operating systems, applications and network devices in a uniform, standardized and prioritized manner. If a security patch cannot be applied promptly, measures must be taken to protect the respective system.

## 13 Change management

The security-relevant requirements for changes within the organization, business processes, information processing and systems must be continuously determined and implemented.

Changes with an impact on IT security must be planned and reviewed accordingly. A formal procedure for approving changes must be established.

## 14 Backup

All backup media must be secured during transportation and storage. Backup media that leave the contractual partner's premises must be protected against unauthorized access, misuse or falsification during transport.

Media should be cataloged so that a missing storage unit can be easily identified. Media must be labeled in such a way that they cannot be assigned to the respective customer by outsiders.

System and application backups must be designed in such a way that complete system recovery is ensured for a period of at least 30 days. Backup media must be located on separate systems. All confidential data must be destroyed within 30 days after termination of the contractual relationship. WEBER-HYDRAULIK data stored on backup media must be encrypted.

## 15 Client systems

The use of EDR/XDR and anti-spyware tools on the contractual partner's client systems is assumed.

All client systems that access confidential data must be physically secured, regardless of whether they are used or not. Received data and programs are automatically scanned for malware before they are executed. Furthermore, the entire data content of all systems is regularly scanned for malware. Data transmission through central gateways (e.g. e-mail, Internet, third-party networks) is checked with protection software (including encrypted connections).

Client systems that access confidential data from secure locations must have a password. A protected screen saver is required or account access must be blocked after 10 minutes of inactivity at the latest. Measures are defined to prevent protection software from being deactivated or modified by users.

## 16 Monitoring

The login to critical assets (server, network, etc.) must be protected against manipulation and unauthorized access. Event logs that record user activities, exceptions, errors and IT security events must be implemented and regularly reviewed. Activities of system administrators and system operators must be logged and the logs reviewed regularly. Logs must be kept for at least 3 months.

## 17 Server Security

All production servers must be located in a secure, access-controlled location. All systems must be hardened, including patching known vulnerabilities, prior to production deployment.

Guest, maintenance and standard accounts must be deactivated. Test accounts and user accounts are removed or revoked when they are no longer required.

Development and test systems must be separated from the production environment and the network. All ports and/or services on server operating systems and firewalls that are not required must be

must be deactivated. The operating system must be updated regularly. Unused software must not be installed. Access to directories must be restricted as part of a restrictive assignment of rights. All network traffic must be monitored for unusual activities/anomalies.

## 18 Mobile devices

To protect confidential information stored on mobile devices, the contractual partner must use strong encryption.

Personal data may only be stored on mobile devices with strong encryption. Appropriately documented guidelines, procedures and standards must be established.

## 19 Protection against malicious code

The contractual partner must have detection and prevention measures in place to protect against malicious software. Appropriate awareness must be created through user awareness training. Incoming and outgoing network traffic must be scanned and filtered in real time to detect and protect against malicious code (email, HTTP, FTP and other messaging). Unauthorized mobile code must be prevented from being executed.

## 20 Access to data centers/ server rooms

Any access to the security zones of the contractual partner requires access control (e.g. security guard, ID card reader, electronic lock, video surveillance). Access logs must be kept for at least 90 days. Access must be restricted to authorized personnel. The assigned rights must be checked regularly.

## 21 Destruction of storage media

The contractual partner must have procedures in place for the secure destruction of storage media. The destruction must be logged.

## 22 Final provisions

Deviations from the above requirements must be made in writing and acknowledged by WEBER-HYDRAULIK.

## 23 Change history

Rev.	Date	Processor	Changes
1	09.05.2022	Ruth-Maria Gerlach (ISB), Frank Bissinger	New creation
2			
3			
4			