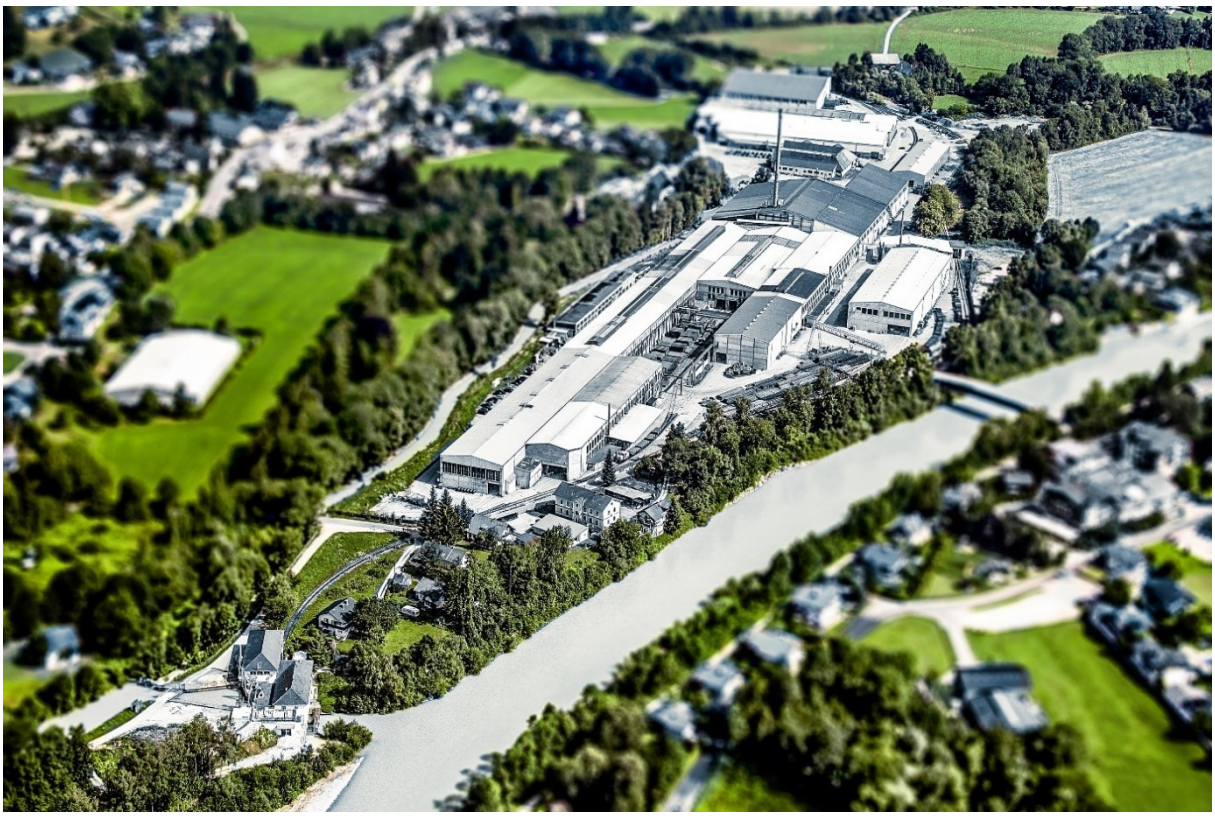
BINDING IT SECURITY REGULATIONS FOR SERVICE PROVIDERS

of Stahlwerk Annahütte Max Aicher GmbH & Co. KG



Stahlwerk Annahütte Max Aicher GmbH & Co. KG
Max-Aicher-Allee 1+2
83404 Ainring/Hammerau
www.annahuette.com
stahlwerk@annahuette.com

Formblatt 08-FB-IT-01-EN_Rev.01-07/20

1. Contents

2. Object

The local IT security regulations for service providers contain binding minimum requirements on the part of Stahlwerk Annahütte Max Aicher GmbH & Co. KG (also in short: "Customer") in respect to IT security at the contractor.
These IT security regulations are binding for entry and access to IT systems, services, data and applications in networks of Stahlwerk Annahütte by the contractor and his subcontractors. In individual cases, additional regulations relating to the order or systems may be supplemented by the customer.

3. Scope of validity, subcontractors and validations

The contractor shall ensure

- within his company and
- among his subcontractors

compliance with the local IT security regulations.
Whether and to the extent that the contractor may deploy subcontractors is oriented to the contractual agreements between the customer and contractor.
On request by the customer, the contractor shall demonstrate compliance with the IT security regulations and, if applicable, also the commitment on the part of his subcontractors.

4. General security regulations

4.1 Virus protection

The contractor must ensure that the latest version of a recognised secure antivirus system with a regularly updated virus signature database is installed on the hardware used by him and his subcontractors (e.g. Pcs, servers, gateways).

4.2 Patch management

The contractor and his subcontractors must ensure via a definite patch management process that updated security patches for the operating system software and applications are installed on the hardware used by him.

4.3 Network security

The contractor and his subcontractors must ensure that their networks as well as the IT systems are adequately protected against attacks and misuse according to the prior art, and likewise the confidentiality, availability and integrity of the IT systems, services, data and applications is ensured.

4.4 Physical access

It shall be guaranteed that the physical entry to IT systems and/or networks by the contractor is protected adequately and in accordance with the prior art.

4.5 Entry and access rights

If entry/access to the network is set up for a contractor or his subcontractors, the contractor shall observe the following regulations and commit his subcontractors to the same:

(1) Any employee of the contractor must log in with his user ID and secure passwords. User IDs and passwords must not be disclosed to third parties. If a joint user account is involved, which is used by several employees, the contractor must ensure that the access data are only known to the requisite group of persons.
(2) The customer hereby points out to the contractor that access and entries to the network are logged. The customer shall inform his employees and subcontractors about this.
(3) The contractor is obliged to inform the customer immediately when entry/access to the network is no longer necessary (e.g. completion of order, employee change, termination or other end to the order).

4.6 Retention and saving of passwords

All system and user passwords of the customer may only be saved by the contractor in a recognised secure password administration program in his IT systems and networks. The contractor shall thereby ensure that only authorised persons can access this information.

4.7 System services and user accounts

User accounts that are provided for the dial-in (remote maintenance) and/or support may only be used by the contractor for this purpose. Use as a system, service or administrator account is not permitted. The accounts are subject to the password policy and are therefore subject to a regular password change.

4.8 Data storage and portability

If a storage and/or portability of customer data, on IT systems or data carriers of the contractor or his subcontractors, is necessary, the contractor shall ensure that an adequate access protection is provided in respect to this data. This includes in all cases an encryption of the relevant data carrier according to the prior art (Bitlocker, etc.)

4.9 Cloud services etc.

The storage as well as transfer of data of the customer via public data repositories (cloud services) e.g. Microsoft OneDrive, DropBox etc. is not permitted under any circumstances.

4.10 On-site activities

In case of activities occurring on site at the customer and carried out using IT equipment of the customer, the following regulations must be observed and complied with.

(1) Before commencing work, the device must be checked by IT (quick check for antivirus protection and patch status.)
(2) Only network connections assigned by the customer may be used.
(3) The installation and operation of active components (modem, router, access points etc.) in the customer network is prohibited.
(4) Hardware and software may only be installed and/or modified on the end devices provided by SAH after consultation with IT.

5. Regulations for remote dial-in

The contractor may only use the remote access or dial-in assigned to him. A remote dial-in must be approved by the IT Department of Stahlwerk Annahütte. The following options/types are available to the contractor:

(1) SSL VPN
The customer shall provide an SSL VPN client. This shall be installed on the devices of the contractor.
(2) S2S connection
A fixed and permanent site-to-site connection via VPN is set up between the contractor and customer.

6. Working with administrator rights

The contractor and his subcontractors shall ensure that employees there with administration rights comply with the following regulations:

(1) The employees may only use the administration rights set up for the purpose of fulfilling the order for the said purpose exclusively. They are prohibited form communicating and/or transferring the assigned personal administration rights s well as the related user accounts and passwords.
(2) If the customer grants more extensive technical authorisations to the contractor on account of technical or organisational reasons, than are required for fulfilment of the order, the contractor and his subcontractors may nevertheless only use the authorisations that are absolutely needed for fulfilment of the order.
(3) Any unauthorised entry and access to IT systems, services, data and applications of the customer is prohibited, especially if such is outside the scope of the order.
(4) The bypassing or overriding of protection measures and encryption mechanisms is prohibited.
(5) When carrying out administrative tasks, a strict assurance of confidentiality, availability and integration must observed for the IT systems, services, data and applications.

7. General obligations

7.1 Duty of notification, blocked entry and access

The contractor is obliged to comply with the relevant safety regulations and laws and report all relevant errors, irregularities or security incidents as well as measures initiated for their rectification to the customer immediately.

If these security directives are not complied with, the customer reserves the right to block access by the contractor and/or his subcontractors to the network of Stahlwerk Annahütte without prior announcement, wholly or partially.

7.2 Use of the customer's information

(1) The contractor and his subcontractors are obliged to use the entry/access rights granted to them (IT systems, services, data and applications) only within the scope of fulfilling their contractual obligations.

(2) All information not publicly known but which becomes known as a result of the order as well as order-related copies, recordings and work results are the property of the customer and must be issued or returned to the same after the order is finished.

(3) The contractor and his subcontractors are obliged to treat all information disclosed to them in conjunction with the contractual fulfilment, their business and operational circumstances and all work results confidentially, and protect the aforementioned appropriately from becoming known to unauthorised parties as well as against non-contractual use, duplication, communication or disclosure. These obligations shall continue to apply after the end of the contractual relationship

(4) The contractor and his subcontractors are not permitted to appropriate business or operational, unpublished information, whatsoever the type, about the customer and/or his clients, suppliers or employees, to use such for their own purposes or to produce copies or recordings whatsoever the type, insofar as this is not necessary for the fulfilment of the order. Nor must such information, copies, recordings or work results be communicated or disclosed to third parties.

(5) Confidential information may only be communicated to subcontractors for whom the customer has granted his approval and who have been obligated to comply with the present security regulation.

7.3 Data secrecy

The contractor may only deploy personal who are committed to data secrecy (§ 5 BDSG Federal Data Protection Act), information security and, if applicable to other secrets (among others § 88 TKG Telecommunications Act) at the
customer. The obligations shall also continue to apply after the end of the activity.

7.4 Employee qualification

The contractor is obliged to only deploy employees, who are technically qualified to carry out the assigned tasks. The same applies for employees of subcontractors.

IT security regulations received, read and accepted:

Name of the contractor:

Place, date	Signature of contractor