Supplementary requirements for the supply of information and communication technology components in equipment and pay-per-use manufacturing services

As of 9 March 2026

The provisions set out in this document supplement the regulations in the document "Minimum IT security standards for external partners".
Insofar as individual provisions of this document go beyond or contradict the requirements of the "Minimum IT Security Standards for External Partners", the provisions of this document shall take precedence.
The obligation to comply with the "Minimum IT Security Standards for External Partners" remains unaffected and must be complied with in full in any case.

The processor/contractor (AN) is obliged to provide the client (AG) with all services and products in the areas of information technology (IT), operational technology (OT), telecommunications, automation, digitalisation, software, hardware, network and security technology, as well as all related consulting , support , service and other services, to fully comply with all applicable legal, regulatory and normative requirements vis-à-vis the client (CL).

1 Compliance with industry standards

In particular, the Contractor shall ensure that the requirements of the NIS2 Directive and the IEC 62443 series of standards, as amended, are bindingly complied with. Security requirements must be taken into account as early as the conception and design phase (security by design and security by default) and effectively maintained throughout the entire life cycle of the service. Upon request, the Contractor must immediately provide the Client with suitable and comprehensible evidence of compliance with these requirements.

2 Secure design (security by design / security by default)

The Contractor shall ensure that security requirements are taken into account in a binding manner as early as the conception and design phase of the service provided.
In particular, the following principles must be observed:

- Minimisation of the attack surface
- Separation of zones, systems and functions
- Principle of minimum rights assignment ("least privilege")
- Avoidance of unnecessary interfaces, services and communication paths

The architecture must be suitable for permanently ensuring the confidentiality, integrity, availability and traceability of the client's systems and data.

3 Secure implementation

The implementation of services and components in the automation environment must be carried out in accordance with the state of the art and taking into account recognised secure development and implementation practices.
In particular, it must be ensured that:

- Standard and default configurations are checked and securely hardened
- unnecessary services, user accounts and interfaces are deactivated
- Security-related configurations are documented and implemented in a traceable manner

Unauthorised changes to system configurations or security mechanisms are not permitted and require prior approval by the client.

4 Secure operation

The operation of the systems and components used must be controlled, traceable and in compliance with the defined security requirements.
The contractor must ensure that:

- Access to systems and components is logged and traceable
- security-related events are detected and reported
- Operating and safety parameters are checked regularly

Operation must not enable the circumvention of existing security, monitoring or protection mechanisms of the client.

5 Maintenance and modifications

Maintenance, update and repair work on systems and components in the automation environment may only be carried out after prior consultation with and approval by the client.
In doing so, it must be ensured that:

- Changes are controlled, documented and traceable
- security-related updates are implemented promptly and in a coordinated manner
- the functionality and safety of the systems are checked after maintenance work

Uncoordinated or unauthorised maintenance or modification measures are prohibited.

5.1 Documentation and handover obligations in the event of changes

The Contractor is obliged to document all changes relating to the design, implementation, configuration, operation or maintenance of services, systems or components in the Client's IT and automation/OT environment in a complete, traceable and timely manner.

5.2 Documentation obligation

The Contractor must ensure that the following content in particular is documented:

- Description of the change(s) made
- Affected systems, components, interfaces or configurations
- Time and reason for the change
- Persons or organisational units carrying out the change
- Impact on safety, operation and availability

The documentation must be prepared in a form that enables technical traceability and use for operational, maintenance and audit purposes.

5.3 Handover to the client

Change, operational and safety documentation must be handed over to the client in full immediately after the respective change has been made.
The handover must be in a format accepted by the client and must include, in particular:

- updated architecture, system or network plans
- Configuration and operating manuals
- Safety-related parameters and settings

The Contractor shall be solely responsible for the proper and complete handover of the documentation.

5.4 Operational relevance and knowledge retention

The Contractor must ensure that the documentation provided enables the Client to independently ensure the safe operation of the systems, to carry out maintenance and troubleshooting measures in a comprehensible manner, and to meet regulatory, normative or internal audit requirements. Incomplete, delayed or non-delivered documentation shall be considered improper performance of services.

6 Prohibition of unauthorised network connections

The unauthorised connection of devices, systems or components of any kind to the client's existing network, communication or OT structures is strictly prohibited. A connection may only be made after prior express written approval by the client. Violations are considered a serious security breach.

7 Prohibition of USB storage devices

The use of USB storage devices, external data carriers and other removable media is strictly prohibited. Exceptions require the prior written approval of the client.

8 Prohibition of modems and wireless transmission devices

The installation, operation or connection of modems, routers, WLAN, mobile phone or other wireless transmission devices of any kind is prohibited. Deviations are only permitted with the prior written approval of the client.

9 Mandatory safety & secruity training

Before commencing any work in the client's IT/OT environment, it must be ensured that all employees involved have successfully completed the IT/OT-specific safety & security training. Employees without valid IT/OT-specific SATRE training are not permitted to perform any work.

10 Remote access regulations

Access to the client's systems, networks or OT environments via remote access is only permitted under the following conditions.

10.1 Permitted remote access solutions

Only remote access solutions that have been expressly approved by the client may be used for remote access. The use of unauthorised remote access solutions, tools, services or procedures is prohibited. This applies in particular to independently installed or cloud-based remote access solutions, regardless of whether they are used permanently or temporarily.

10.2 Approval and usage requirements

Remote access may only be granted with the prior written approval of the client and exclusively to the extent approved.
Remote access must be limited to the minimum necessary for the provision of services (least privilege principle). A permanent or unattended connection is not permitted unless expressly approved by the client.

10.3 Security requirements for remote access

The remote access used must be state of the art and, in particular, must ensure encrypted communication and strong authentication (e.g. multi-factor authentication). The Contractor must ensure that remote access does not allow the circumvention of existing security mechanisms, network segmentations or access restrictions of the Client.

10.4 Logging and control

Remote access connections are subject to logging and monitoring by the client. The contractor expressly acknowledges that all remote accesses can be recorded in a traceable manner and that corresponding evidence must be provided upon request.

11 Use of voestalpine IT standard equipment and services

Where possible, hardware components (computers with Microsoft, Linux or iOS operating systems, monitors, etc.) must be used in accordance with voestalpine standards. The need for these devices must be specified in the offer; the devices will be provided by voestalpine. Any deviating hardware requirements must be explicitly stated and justified.

If virtualisation (for servers or clients) is to be used, the required virtual machines and their requirements (number of cores, main memory and hard disk requirements, etc.) must be specified. The virtualisation environment will be provided by voestalpine in accordance with voestalpine standards.

12 Client configuration

For Windows client systems in the production area, the latest operating system versions supported by Microsoft at the time of order placement must be used.

13 Asset management

All computer systems must be documented in voestalpine Asset Management. This is done by initially scanning the systems after complete installation and then scanning them regularly with the voestalpine scanner software. Before commissioning, the contractor must provide a complete list of the computer systems included in its scope of delivery, including the computer systems provided by the client at the contractor's request, and announce that the systems are ready for scanning.

14 Licence Management

The plant IT must be complete, including all licences required for operation and access to the plant. To this end, the supplier shall attach to the offer a complete list of all necessary software licences and any free software used (e.g. freeware, open source software, etc.) and all licence conditions applicable to the software, including information on which specific licence conditions apply to which software (parts) listed. The client reserves the right, at the express written request of the client, to provide the licences for software used as standard in the voestalpine Group. For software included in the scope of delivery, the contractor must provide the client with the complete licence certificates in addition to the documents and information mentioned above.

15 Network cabling

Network cabling shall be carried out in accordance with voestalpine standards.

16 Data ownership and right of use

Any access to production plant data and log data by external parties, in particular by the manufacturer of the plant or plant automation, requires the express permission of voestalpine: Data ownership and rights of use for this data lie exclusively with voestalpine.

This includes, in particular, data generated through the use of the system or plant (by voestalpine). All data generated by the plant and its systems are and remain the property of voestalpine. Any use of this data by third parties requires written authorisation and must be documented; voestalpine will verify compliance.

17 Internet connection

A direct internet connection of plant automation systems and IP networks/segments in which plant automation systems are located is not permitted.

18 Access to sensor data

All sensor data generated or recorded within the scope of the contractor's delivery must be made available to voestalpine via a standard interface of the machine or plant automation system. If the client has trained personnel and all necessary development tools at its disposal to expand or recreate interfaces of the machine or plant automation system, complete documentation of all sensor values in the automation system is sufficient in consultation with the client.

19 Source code for custom software

For any custom software (software not available on the open market) for plant automation, the source code, necessary libraries and the development environment must be provided.

20 Service life

The supplier must demonstrate in the offer how it can guarantee the safe operation (including IT security) and further development of the system for at least 10 years. Aspects such as spare parts availability, upgrades of system and standard software, security patches, etc. must be taken into account. At the time of commissioning, the operating systems and all software components used must be upgraded to the latest available version.

21 Data and communication concept

When preparing the offer and in the event of any service provision, the contractor (supplier, AN) must clearly present all communication relationships with systems and their data storage in the available forms ("Communication Matrix EN/GER") and, in any case, have them approved in writing by the client (AG) before the start of implementation.

For the sake of clarity, the contractor may combine individual systems into groups of similar systems if they are identical in terms of function, communication relationships and (non-)affiliation to the scope of delivery and services. At the latest in the (as-built) documentation, the contractor must document for each system which group of similar systems it belongs to.

The Contractor shall be liable to the Client for ensuring that (irrespective of any written approval) no communication relationship is established or used which (a) is suitable for or actually leads to the unlawful transfer of intellectual property belonging to voestalpine, or (b) may endanger or actually endangers the operational or IT security of voestalpine's systems or equipment. Any contractually agreed exclusions and limitations of liability shall expressly not apply in this context.

For each individual violation of point 21, the Contractor shall pay the Client a contractual penalty of 20% of the order value, but at least EUR 20,000, regardless of fault. Any contractual penalty payable shall not be offset against any damages.

22 Violations

Violations of these requirements may result in the immediate withdrawal of access rights, the blocking of employee access, the rejection of services, the termination of the contract for good cause, and claims for damages.

23 APPENDIX 1:
Mapping table: Additional IT/OT security requirements ↔ IEC 62443 / NIS2 (excerpt)

Chapter / Requirement	IEC 62443 Relevant parts	NIS2 – relevant articles / requirements	Audit evidence / proof
Compliance with industry standards (NIS2 / IEC 62443)	IEC 62443-2-1 (IACS Security Programme) IEC 62443-4-1 (Secure Product Development Lifecycle)	Art. 21 – Risk management & security measures Art. 23 – Accountability	Security concept, architecture documentation, standards reference
Security by Design / Security by Default	IEC 62443-4-1 (SR-1 to SR-7) IEC 62443-3-2 (Risk Assessment)	Art. 21(2)(a), (c)	Architecture reviews, design approvals
Prohibition of unauthorised network connections	IEC 62443-3-3 (SR 1.1, SR 1.2, SR 2.1)	Art. 21(2)(f) (access control)	Network approvals, firewall rules
Network & system access only after approval	IEC 62443-2-1 IEC 62443-3-3 (SR 1.x)	Art. 21 para. 2 lit. b, f	Release logs, change management
Prohibition of USB storage devices/removable media	IEC 62443-3-3 (SR 2.6 – Portable Media)	Art. 21(2)(g) (Asset Management)	Removable media policy, technical barriers
Control of external data carriers	IEC 62443-2-1 (Policies & Procedures)	Art. 21(2)(a)	Policy documents, training certificates
Prohibition of modems and wireless transmission devices	IEC 62443-3-3 (SR 5.1, SR 5.2 – Network Segmentation)	Art. 21 para. 2 lit. f	Network topology, OT zone model
Prevention of unauthorised radio/remote access	IEC 62443-3-3 (SR 1, SR 5)	Art. 21(2)(b), (f)	Technical network checks
Mandatory IT/OT-specific SATRE training	IEC 62443-2-1 (Awareness & Training)	Art. 21 para. 2 lit. i (training)	Training lists, certificates
Prohibition of use without proof of training	IEC 62443-2-1	Art. 21(2)(i)	Approval for use, proof of personnel
Obligation to provide evidence to the client	IEC 62443-2-1 (Compliance & Audit)	Art. 23 – Accountability	Audit reports, supplier evaluation
Remote access only with client approval	IEC 62443-3-3 (SR 1, SR 2, SR 5)	Art. 21 para. 2 lit. f	Approval lists, remote access policy
Secure remote access	IEC 62443-3-3 (SR 1.13, SR 1.14)	Art. 21(2)(c)	Configuration, protocols