Minimum IT Security Standards for External Partners
(Technical and Organizational Measures)

The Processor/Contractor (hereinafter: the "Contractor") agrees to fully comply with the following Minimum IT Security Standards for External Partners (Technical and Organizational Measures) as part of the provisioning of the services agreed-upon with the Controller/Client (hereinafter: the "Client"). The obligation shall apply to all the Contractor's employees, including the employees of any subcontractors that may be hired.

The Contractor shall take all measures

- to prevent accidental or unlawful destruction of data and
- to protect the confidentiality of the Client's or the voestalpine Group's data.

Every security-related incident (e.g., inadvertent or unlawful destruction, loss, alteration, unauthorized disclosure or access to data) shall be promptly reported to the Client irrespective of the cause. This shall also apply to serious disruptions of operational processes (e.g., data loss, destruction or deletion of files, computer virus infestations, failure of all hardware components, software failures due to programming errors and incorrect configurations) or other irregularities in the handling of the Client's data. Moreover, any additional contractually agreed-upon obligations must be met.

Furthermore, the Contractor shall meet the following requirements, among others:

Risk management (regular review, assessment, and evaluation)

- There shall be a regular risk analysis with respect to the tangible and intangible losses that may occur within the context of processing activities or with respect to underlying systems.
- Plans to ensure the continuity of operations shall be regularly tested and updated to guarantee that they are effective.
- The Contractor shall regularly take risk-appropriate actions (e.g., penetration tests, security audits) to check the effectiveness of the measures taken and provide the results to the Client upon request.

Admission controls

- There shall be a physical security concept, which gives due consideration to security zones (e.g., areas accessible to the public, offices, computer centers, high-security areas). Information-processing equipment shall be physically protected with safety locks against unauthorized access and user access as well as against damage or interference.
- IT security areas shall be protected by admission controls to ensure that only authorized personnel are admitted. In particular, authorizations shall be adjusted or deactivated when employees are replaced or leave the company.
- The access or user access rights to information and information-processing systems of all employees, contractors, and third parties shall be deactivated when their employment, contract, or agreement ends.
- All Contractor employees with user access in voestalpine computer centers shall follow the security guidelines in the voestalpine computer centers (behavior in case of fire, etc.) and shall confirm their acknowledgment of the instructions in writing. The mandatory security and environmental briefings shall be completed, and this shall be confirmed.

User access controls

- In assigning tasks, the Contractor shall determine which of its employees and hired employees shall be authorized to access the Client's systems. The Contractor shall make this determination and define the scope of the respective authorizations in agreement with the Client.
- Authorizations shall be issued restrictively depending on the Contractor employees' need for such authorization to perform their tasks ("need to know" principle) and documented so as to be traceable.
- The number of system administrators shall be kept to the required minimum.
- The Contractor shall reasonably protect the systems operated on behalf of the Client against operation by unauthorized persons.
- User authorizations shall be checked regularly to ensure that they are up-to-date and necessary to perform the employee's tasks.
- User authorizations shall be cancelled when they are no longer needed.
- User access to data must be effectuated by means of a secure login procedure and a secure password policy (e.g., strong passwords, regular change of password).
- Equipment belonging to the Contractor (e.g., notebooks, external storage media), on which the Client's data is temporarily stored (to the extent that this is absolutely necessary to fulfill the order), shall have appropriate user access protection (at least secure passwords and adequate encryption conforming to the current state of the art methods).
- Remote access via the Internet is only allowed if the following prerequisites are met:
    - Communication via the Internet is tunneled, encrypted, and with strong authentication (e.g., a one-time password as the second factor).
    - Authorizations are restricted to the necessary minimum.
    - The product used does not allow further connections to the Internet in addition to the remote access connection at the same time.
- At the end of the contract, after the completion of providing agreed-upon services or upon the request of the Client, all voestalpine assets used by the Contractor (notebooks, mobile phones, etc.) shall be promptly returned or irretrievably destroyed – at the Client's choice.
- The Contractor notes that its activities on voestalpine Group systems are logged.

Network controls

- The Contractor shall take the customary state-of-the-art security precautions at gateways (firewalls, VPN connections, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), etc.). In particular, the systems shall be securely sealed off from external access by public networks by means of a firewall.
- Technical systems shall be correctly serviced and maintained to ensure their availability and completeness.
- The equipment used by the Contractor's employees shall meet state-of-the-art security requirements (antivirus, firewall, latest patch status, etc.).

Transfer controls

- The transport of data on notebooks or on external storage media or the like presents a high risk and therefore must be reduced to the absolute minimum possible. If this cannot be avoided, the greatest care shall be taken. Confidentiality shall be ensured by using encryption techniques that reflect the current state of the art technologies.
- To the extent that the Contractor receives user access to the Client's systems, the Contractor cannot store any data from these systems on external systems outside the voestalpine Group (e.g., Cloud) without the permission of the Client.
- If data carriers or media are no longer needed, they shall be reliably, securely, and properly disposed of or destroyed so that it is impossible to read or restore the relevant data. The Contractor shall verifiably document this disposal or destruction and confirm this to the Client upon request.

Storage controls

- Operating systems and operations-related applications shall be monitored, and incidents relevant to information security shall be recorded. Unauthorized user access shall be logged to prevent any misuse of systems and information. To ensure that problems with information systems are detected, operating and error logs shall be periodically evaluated.
- The activities of system administrators and operators shall be logged.

Controls on the instructions issued

- Responsibilities for the processing of personal data must be clearly described (controller, processor, sub-processor, etc.).
- The Contractor shall verifiably (via confidentiality agreement) require its employees and hired employees (particularly any subcontractors hired) to maintain confidentiality with respect to all information of which they become aware in the course of providing services – including after the time services are provided and after the employment relationship ends.
- All employees shall receive appropriate awareness training and regularly updated information on IT information security and data protection, to the extent that these matters are of importance to their work.
- The data available to the Contractor shall be used solely for the agreed-upon purpose. Therefore, the Contractor can only process data belonging to the Client or the voestalpine Group temporarily and for its intended purpose. At the end of the contract, after the completion of providing the agreed-upon services or upon the request of the Client, all voestalpine data shall be promptly returned or irretrievably deleted – at the Client's choice. In this regard, supplementary agreements shall be taken into account.
- Sub-processors/subcontractors which are given access to the Client's data shall comply with all technical and organizational measures agreed-upon between the Contractor and the Client.

Availability controls

- Business-critical information processing systems shall be protected against power outages and failures of other facilities.
- Procedures shall be established to ensure a quick, effective, planned response to information security-related incidents.
- There shall be regular backups of data.

- The ability to restore data shall be checked regularly.
- Business continuity plans and emergency plans must be developed and implemented to maintain or restore operation and to ensure the availability of data to the extent necessary and within the required period after interruptions or failures of critical business processes.

Separation controls

- User access to different areas shall follow a regulated approval procedure by authorized persons working for the Contractor. There shall be an authorization concept which prevents Contractor employees who do not perform tasks for the Client from having user access to the Client's data.
- The Contractor employees shall be instructed that data may only be processed for the intended purposes.
- The data of different customers (clients) of the Contractor shall be processed in logically or physically separated infrastructures.

Compliance

- The equipment operated by Contractor employees in the voestalpine network may only contain software licensed by the Contractor.
- The Contractor shall be obliged to provide all necessary information to prove its compliance with the obligations set forth in the Minimum IT Security Standards for External Partners (Technical and Organizational Measures) and to enable and facilitate reviews conducted by the Client or an auditor hired by the Client, after at least seven days' advance notice. If there is a suspicion or indication of serious violations of these provisions by the Contractor or third parties, the Client shall be granted immediate access to the systems or immediate admission to the areas being used. Deficiencies and shortcomings detected in the course of an audit must be promptly eliminated.