Standards of information and communication technology (ICT) component supply for plant systems and pay-per-use production services

Attachment to bid invitations and contractual provisions

1. Compliance with minimum IT security standards
   Compliance with the minimum IT security standards of voestalpine is mandatory and must be guaranteed on a permanent basis (see attachment). In particular, this entails the following:
   - Normal operation must be possible with a single user without administrator rights.
   - The systems must allow operation of the virus scanners currently in use in the voestalpine Group.
   - It must be possible to patch operating systems and standard software components such as Java, .Net etc. without affecting the manufacturer's warranty.
   - Plant system automation must allow scans conducted with commercial vulnerability scanners in use in the voestalpine Group.
   - All services not required by the systems must be deactivated.
   - Compliance with the password regulations of the voestalpine Group is mandatory. Local users with administrator rights must use a different password for each system.
2. Use of standard voestalpine IT devices and services
   To the extent possible, use only hardware components (computers equipped with Microsoft, Linux or iOS operating systems, monitors etc.) based on voestalpine standard. Such devices must be indicated in the bid. The devices shall be provided by voestalpine. Any deviating hardware requirements must be explicitly indicated and justified. To the extent that servers or clients are virtualized, the required virtual machines and their specifications must be indicated (number of cores, main memory and hard drive requirements). The virtualization environment shall be provided based on the voestalpine standard (VMware vSphere).
3. Client configuration
   The Windows 10 64bit configuration for production at voestalpine (currently Windows 10 64bit LTSB – 1607) shall be provided for Windows client systems in the production environment.
4. Asset management
   All computer systems must be documented in voestalpine asset management by initially scanning the systems after they have been fully installed and then regularly scanning them using voestalpine scanner software. Prior to startup, the supplier shall provide a complete list of the computer systems in the scope of supply, including those provided by the customer at the request of the supplier, and shall indicate the scannability of the systems.
5. License management
   The production IT systems must be complete, including all licenses required for operation and access. The supplier shall include in the offer a complete list of all required software licenses and any free software (free ware and open-source software) and all respective licensing conditions, including information on which software (component) is covered by each of the respective licensing terms and conditions. At the express written request of the customer, the customer reserves the right to provide standard software licenses for all software used as a standard in the voestalpine Group. All proofs of license purchase shall be submitted by the supplier to the customer for the software contained in the scope of supply in addition to all documentation and pertinent supplementary information.
6. Network cabling
   Network cabling shall be based on the voestalpine standard.
7. Network topology and address assignment
   Network topology is determined by voestalpine upon recommendation of the supplier. Network addresses are assigned by voestalpine at the request of the supplier.
8. Wi-Fi and other radio connections
   Any radio connections such as Wi-Fi, remote radio controls, voice transmission etc. shall be subject to the approval of voestalpine prior to their installation.

9. Remote maintenance access
   Remote maintenance access and any other external access to the voestalpine networks shall be installed solely upon request and pursuant to voestalpine standards. Access through telephone modems or individual VPN routers are generally not permissible. Remote maintenance access is enabled only when absolutely required and is monitored by voestalpine.

10. Data ownership and rights of use
    Any access to production system data and log data by external parties, even by the system manufacturer, shall be subject to the explicit approval of voestalpine: Data are owned by voestalpine and enjoys the exclusive rights of use. This also includes data created by voestalpine through use of the (production) system. All data created by (production) systems belong exclusively to voestalpine. Any type of use by any third party shall be subject to prior written permission. Compliance is monitored by voestalpine.

11. Internet connection
    A direct Internet connection from production automation systems and from IP networks/segments containing production automation systems is not permissible.

12. Access to sensor data
    All sensor data accrued and recorded within the scope of the supplier must be made accessible to voestalpine through a standard interface of machine or plant system automation. Complete documentation of all sensor values in the automation system shall suffice, to the extent that trained personnel and the required development tools are available to the customer in order to use machine and automation interfaces for the reading of sensor values.

13. Standardization of automation systems
    The applicable standards are defined in the attachment.

14. Source code for individual software
    The source code, required libraries and the development environment shall be supplied for all individual software packages not available in the free market for production systems automation.

15. Long-term operability
    The supplier shall indicate in the offer how secure operation (including secure IT systems) and further development of the systems can be guaranteed for at least ten years. Aspects such as the availability of replacement components, system and standard software upgrades, security patches etc. shall be taken into account. At the time of startup, all operating systems and software components shall be updated to their most recently available versions.

16. Data and communication design
    (i) The Contractor (supplier) shall clearly describe all communications relationships with systems and their data storage on the attached forms when it prepares the offer and provides any services and shall have the client approve them in writing before the start of implementation.
    (ii) For better understanding of the offer, the Contractor can combine individual systems into groups of similar systems if they are similar in terms of function, communications relationships, and (non-) inclusion in the range of goods and services. For each system, the Contractor must document the group of similar systems to which it belongs in the ('as-built') documentation at the latest.
    (iii) The Contractor shall be liable to the client (irrespective of any written approval) for ensuring that no communication relationship is established or used that (a) is likely to or actually does lead to the unlawful transfer of voestalpine intellectual property or (b) that can – or actually does – endanger the operational safety or IT security of systems or plants belonging to voestalpine. It is expressly stipulated that any contractually agreed-upon exclusion or limitation of liability shall not apply in this context.
    (iv) The Contractor shall be obliged to pay the client a contractual penalty in the amount of 20% of the value of the order, but at least EUR 20,000, for each individual infringement/violation of this Article 16. Such contractual penalty shall be independent from any fault or misconduct of the Contractor and shall be applicable in addition to any other claims and rights the Client may have and/or rise against the Contractor.