Contents

Remarks on the current issue:

Revision: First issue
Previous issues:
Responsible functional unit(s) for the technical content: ITE

X	01	06.2019	Burmeister, ITE	Oeler, GPCEC Rittmeister, ITE Schmitt, QH	Krause, GPCE
Status	Issue	Date	Prepared	Reviewed	Approved

1 Scope

This Linde Standard (LS) applies to orders placed by Linde Engineering with contractors that require access to the Linde IT infrastructure. By accepting the order, the Contractor agrees to these terms and conditions in order to safeguard IT security.

2 Normative references

This LS contains undated references to incorporate provisions of other publications. The normative references are cited at the respective place in the text and the publications are listed below. Issues valid at the effective date of contract shall apply.

EUReg 2016/679 General data protection regulation (GDPR)

3 Access rights

a) In order to be granted access rights to the Buyer's network, the Contractor shall provide the Buyer's technical contact with the names of those individuals requiring access to the network by e-mail without delay, providing any further information that is required on request.

b) The decision on granting access rights to the Buyer's IT infrastructure shall be made exclusively by the Buyer, which can grant these rights to the Contractor in particular if this is essential for the execution of the order.

c) Access to the Buyer's network within the Buyer's company is only possible via clients provided by the Buyer. Access from outside the company is only possible via a Virtual Desktop Interface (VDI). Exceptions can be discussed with the Buyer on a case-by-case basis. If a data connection via VPN (Virtual Private Network) is required, the Contractor will provide the corresponding technical information.

d) Upon termination of the deployment of the Contractor’s personnel who were previously authorized to access the systems and/or upon performance of the contract (prior to the commencement of the warranty), the rights to access the Buyer's systems awarded to personnel deployed by Contractor shall end. The Contractor shall inform the Buyer without delay of any changes in the deployment of its personnel. The Contractor shall return the items provided for authentication (e.g. tokens, smart cards) to the Buyer as soon as the deployment of personnel who were previously authorized to access the systems has ended and/or upon performance of the contract.

4 IT security provisions

a) The access rights made available to the Contractor are awarded to specific individuals and may not be transferred by the Contractor to third parties. The Contractor may only make use of the access rights granted to it to the extent that is essential for the performance of the activities in question.

b) The Contractor undertakes to report any incidents relating to IT security to the Buyer’s technical contact without delay.

c) The Contractor is not permitted to connect to the Buyer’s LAN using its own hardware.

d) The Contractor shall ensure the necessary IT security in its own computer system and shall also ensure that these measures are complied with by the personnel it deploys. This includes, among other things, the following:

   i. The Contractor shall ensure that the systems comply with the latest IT security requirements. These include, among other things, up-to-date licensed antivirus software, a firewall system and the installation of the latest security updates for the operating system or applications used.

   ii. Even if "free software" or "open source software" is used, i.e. software that can generally be obtained free of charge and on an open source basis, the Contractor shall remain responsible for the IT security of the program created using this software.

   iii. In cases involving programs developed for the Buyer, the Contractor shall seek information on the Buyer's current IT security rules that apply to software development within the Buyer’s company and shall comply with these rules.

e) The Contractor shall not violate the security of the Buyer's IT infrastructure and shall ensure that appropriate measures are adhered to by its deployed personnel.

f) Data shall only be processed using remote access if this is agreed in the underlying order. Access is only possible using Linde's own hardware or the Virtual Desktop Infrastructure.

5 Data protection

a) If the use of cloud services (storage/retrieval of data, computing power and software via the Internet) is foreseeable, the Contractor shall inform the Buyer accordingly before the cloud services are used and shall fulfil all requirements, in particular those relating to data protection, in consultation with the Buyer.

b) When processing personal data, the Contractor shall observe the relevant statutory provisions and shall conclude an agreement with the Buyer on contract data processing in accordance with Article 28 of the GDPR.

6 Verification of software and hardware

Deliveries and services, as well as all data media used and data and information that is transmitted electronically (e.g. via e-mail or data transfer) shall be checked by the Contractor for malware (e.g. Trojan horses, viruses, spyware, etc.) using the latest testing and analysis methods before being made available to the Buyer, or before being used by the Contractor in the Buyer's IT infrastructure, thereby ensuring freedom from malware. If malware is detected, this data must not be transferred to the Buyer and must not be used by the Contractor in the Buyer’s IT infrastructure.