INFORMATION SECURITY

1 Definitions

Data means all financial/business information, designs, dimensions, specifications, drawings, patterns, computer files or software, know how, or other information, including technical data, concerning methods, manufacturing processes, equipment, gauges and tools used in the design and manufacture of Goods or the provision of Services. Data may be recorded in a written or printed document, computer or electronically stored, software, or any other tangible form of expression.

Information Security Incident means (i) any actual or potential incident involving any Information System or equipment owned or controlled by Seller that may involve Buyer's Sensitive Information, or (ii) any actual or potential unauthorized access to, use, or disclosure of Buyer's Sensitive Information.

Information means any communication or representation of knowledge such as facts, Data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual.

Information System means a discrete set of Information resources that collect, process, maintain, use, share, disseminate, or dispose Information.

Procurement Contracting Official (PCO) means the person authorized by the Buyer to administer and/or execute this Contract and who has sole authority to make contractual commitments on behalf of the Buyer, to provide contractual direction, and to change contractual requirements of this Contract.

Sensitive Information means any Information that is collected, processed, maintained, used, shared, or disseminated in connection with this Contract that warrants protection to ensure its confidentiality, integrity and availability including, but not limited to, any Buyer's proprietary or confidential Information and third party proprietary Information, and Personal Data.

2 Reasonable and Appropriate Security Controls

2.1 Seller shall apply reasonable and appropriate administrative, technical, physical, organizational, and operational safeguards and operations to protect Sensitive Information against accidental and unlawful destruction, alteration, and unauthorized or improper disclosure or access regardless of whether such Sensitive Information is on Seller's internal systems or a cloud environment.

2.2 If the Seller's performance of the Contract involves the transmission, storage, or processing of Sensitive Information on an Information System, Seller shall at a minimum apply the following controls:

a) Basic Safeguarding Controls
   1. Limit Information System access only to authorized users, processes acting on behalf of authorized users, or devices (including other Information Systems).
   2. Limit Information System access to the types of transactions and functions that authorized users are permitted to execute.
   3. Verify and control/limit connections to and use of external Information Systems.
   4. Control Information posted or processed on publicly accessible Information Systems.
   5. Identify Information System users, processes acting on behalf of users, or devices.
   6. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to Seller's Information Systems.
   7. Sanitize or destroy Information System media containing Sensitive Information before disposal or release for reuse.
   8. Limit physical access to Seller's Information Systems, equipment, and the respective operating environments only to authorized individuals.

9. Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
10. Monitor, control, and protect Seller's communications (i.e., Information transmitted or received by Seller's Information Systems) at the external boundaries and key internal boundaries of the Information Systems.
11. Implement sub-networks for publicly accessible system components that are physically or logically separated from internal networks.
12. Identify, report, and correct Information and Information System flaws in a timely manner.
13. Provide protection from malicious code at appropriate locations within Seller's Information Systems.
14. Update malicious code protection mechanisms when new releases are available.
15. Perform periodic vulnerability scans of the Information System and real-time scans of files from external sources as files are downloaded, opened, or executed.

b) Additional Basic Security Controls
    1. Establish and enforce security configuration settings for information technology products employed in Seller's Information Systems.
    2. Establish and maintain data protection processes and systems to adequately protect Sensitive Information, including pertaining to destruction methods employed, how audit and system log information is protected, and having the capability to encrypt Sensitive Information during transmission.
    3. Ensure that risks identified in scans performed are promptly addressed.

3 Information Security Incident Response and Notification

3.1 Seller must have documented and traceable processes that address Information Security Incidents. These processes should be a set of written instructions that include, but are not limited to: detecting, responding to, and limiting the effects of an Information Security Incident including the collection of evidence.

3.2 Immediately after and in any event no later than 72 hours of discovery, Seller will notify Buyer's PCO and Buyer's Cyber Security Operator at cybersecurity@litef.de of any Information Security Incident. At Seller's expense, Seller will (i) immediately investigate any Information Security Incident, (ii) make all reasonable efforts to secure Sensitive Information and mitigate the impact of the Information Security Incident, (iii) provide timely and relevant information to the Buyer about the Information Security Incident on an ongoing basis, and (iv) cooperate as applicable with the Buyer to provide notice to affected third parties.

3.3 This Clause does not relieve Seller of any other applicable safeguarding requirements, remedies, or obligations regarding the protection of Sensitive Information required by this Contract, under applicable law or other governmental agencies or departments.

4 Seller shall respond promptly and appropriately to any inquiries from the Buyer related to compliance with this Clause to include documentation of implemented controls and processes discussed above.