SECURITY AUDIT REQUIREMENTS

The security audit will be performed by representatives of the Buyer (1-2 persons) and the participation of an employee responsible for security (security manager or a person authorized by him) is required on behalf of the Seller. The audit will be performed in accordance with ISO 19011:2019. The audit can be performed both on site or, if the situation does not allow it, by a remote audit as well (i.e. videoconference in combination with shared document storage).

The security audit will be organized ordinarily in two days with the following agenda:

- 1st Day - security policy, security documentation, risk management, business continuity management, ensuring security processes, inspection of the building,
- 2nd Day - completion of the inspection of the building and checking the settings of security processes, processing the minutes of the security audit, conclusion.

The agenda of the remote audit in the matters of time schedule may be modified.

The Seller will be informed about the security audit at least **1 week in advance** in case of the entry security audit (contact person stated in the tender procedure), and at least **30 days in advance** in case of the subsequent security audits.

The Seller shall fulfill all the following requirements, whereas all the requirements stated below arise from requirements of ISO 14298 and CWA 15374 and shall be interpreted in the meaning of ISO 14298 and CWA 15374:

No	Requirements	Further description on manner of fulfilling the requirement
01	A security policy has to be implemented	**Minimum level to fulfil the requirement**: The document "Security Policy" must be adopted and issued by the company's management, the document must meet: (1) the requirements of ISO 27001, or (2) adequately, Annex No. 5 to Decree No. 82/2018 Coll. On security measures, cyber security incidents, reactive measures, requirements for filing in the field of cyber security and data disposal (Decree on Cyber Security), or (3) it must contain at least the following structure: • Objectives • Priority, • Security commitments **Manner of fulfilling in case of physical audit**: Submission of the document "Security Policy". **Manner of fulfilling in case of remote audit**: Submission of the document "Security Policy" in the form of remote access or display on a shared screen.
02	The subcontractors, who are participating in the order for the Buyer, have to be security checked	**Minimum level to fulfil the requirement**: There must be records of security checks at other subcontractors, who are participating in the supply of services to the participant under this contract. Security checks at subcontractors

No	Requirements	Further description on manner of fulfilling the requirement
		must be performed at least within the scope of this document. If the participant does not have a subcontractor under the contract, this point is not audited. **Manner of fulfilling in case of physical audit**: to provide records with conclusions from security checks. **Manner of fulfilling in case of remote audit**: Submission of records in the form of remote access or display on a shared screen.
03	A system of concluding of confidentiality agreement with the subcontractors must be adopted	**Minimum level to fulfil the requirement**: A non-disclosure agreement (NDA) must be accepted and signed between the participant and other suppliers involved in the order for the Buyer, which must include at least the following parts: • Names of parties to the contract, • Definition of what constitutes confidential information, • Prohibiting any exclusion from confidentiality, • A statement of the appropriate use of the information to be disclosed, • Relevant time period, • Fines and sanctions in the appropriate amount **Manner of fulfilling in case of physical audit**: to submit written document (s) or internal directive regulating this area. **Manner of fulfilling in case of remote audit**: Submission of written documents by remote access or display on a shared screen.
04	The security requirements between the Buyer and the Seller have to be set up and documented	**Minimum level to fulfil the requirement**: The Seller must have set up and documented safety procedures and rules for the production and delivery of services or products for the Buyer. The whole process from the purchase of raw materials / semi-finished products, the production cycle until the dispatch and transport of the products to the customer must be described. The document must include records of materials during the production cycle and the method of disposal of non-conforming production. **Manner of fulfilling in case of physical audit**: to submit written documentation of safety rules and production procedures **Manner of fulfilling in case of remote audit**: Submission of written documents by remote access or display on a shared screen
05	Regular internal security audits have to be performed	**Minimum level to fulfil the requirement**: The participant implements and performs regular internal security audits of its own procedures and rules (at least once a year). **Manner of fulfilling in case of physical audit**: to document the minutes of the audits and the

No	Requirements	Further description on manner of fulfilling the requirement
		implementation of corrective measures in the event of identified deficiencies and the program / plan of internal audits **Manner of fulfilling in case of remote audit**:to document audit records and implementation of corrective measures in case of detected deficiencies and program / plan of internal audits in the form of remote access or display on a shared screen
06	Risk assessment and risk management documents have to be implemented and updated	**Minimum level to fulfil the requirement**: A risk analysis is prepared and regularly updated (at least once a year). The document must meet: (1) Requirements according to ISO 27001, or (2) must contain at least the following parts: • risk identification • risk analysis • risk evaluation • risk mitigation • risk management (resp. its mitigation) • risk monitoring and review **Manner of fulfilling in case of physical audit**: to submit a document risk analysis. **Manner of fulfilling in case of remote audit**: to submit a document risk analysis in the form of remote access or display on a shared screen.
07	Continuous supply of products and services has to be ensured	**Minimum level to fulfil the requirement**: There is a functional and up-to-date Business Continuity Plan to ensure maximum protection in order to ensure the operation of the company and its operation in situations where the company is threatened or facing a disaster. The document must meet: (1) the requirements of the standard according to ISO 22301, or (2) must contain at least the following parts: • Risk and threat analysis • Business impact analysis • Crisis measures and organizational guidelines to keep the organization in crisis • Plans and measures to maintain continuity • Scenarios, plans and measures for recovery of operation • Techniques for quality assurance, preventive measures such as maintenance, exercises, audits • Contact information for members of management (especially crisis) • Instructions for employees in the event of a crisis

No	Requirements	Further description on manner of fulfilling the requirement
		• Allocation of people, tools and other resources **Manner of fulfilling in case of physical audit**: to document the "Business Continuity Plan". **Manner of fulfilling in case of remote audit**: to document the "Business Continuity Plan" document in the form of remote access or display on a shared screen.
08	The Seller's buildings have to be secured via IDS (Intrusion Detection System), FS (Fire System), CCTV, ACS (Access Control System)	**Minimum level to fulfil the requirement**: The Seller's facilities and production facilities must be equipped with defined security systems with a connection to a monitoring centre (internal or external). The camera system must be recorded and must monitor the entire production area and perimeter without blind spots. At least ACS must be installed at all entrances to the production premises. IDS must fully cover at least all production premises, production preparation and storage facilities. FS is not obligatory if this fact is stated in the "Fire safety solution" or similar document. **Manner of fulfilling in case of physical audit**: a physical inspection of the installed security technology, visit to the monitoring centre, submission of the document "Description of physical and logical perimeter," or "Security project " or the directive "Physical protection "or similar documents describing the installed security technologies. **Manner of fulfilling in case of remote audit**: documentation of documents "Description of physical and logical perimeter", or "Security project" or directive "Physical protection" or similar documents describing installed security technologies in the form of remote access or shared screen display (part of this documentation must be photographs of installed technologies, or document the installed security elements by a camera within the online transmission)**.**
09	A space for loading and unloading of goods and materials has to be designated	**Minimum level to fulfil the requirement**: Premises for loading or unloading products must be marked and operated in safety mode. It must be a structurally separate area; at the time of loading/unloading, only the operator performing the material handling and, if necessary, security must be present in the area. The room must be equipped with a camera system with recording, which monitors the entire room without blind spots. **Manner of fulfilling in case of physical audit**: a physical inspection of the area, submission of the document "Description of physical and logical perimeter", or "Security project "or the directive "Physical protection" or

No	Requirements	Further description on manner of fulfilling the requirement
		similar documents describing the security of loading / unloading areas. **Manner of fulfilling in case of remote audit**:: documentation of documents "Description of physical and logical perimeter, or" Security project "or directive" Physical protection "or similar documents describing security of loading / unloading areas by remote access or display on shared screen (part of said documentation must be photographs of installed technologies).
10	A physical security has to be performed by own employees or by licensed outsourced guards	**Minimum level to fulfil the requirement**: Continuous physical security (by own employees or by external qualified entities) must be organized in the Seller's premises. The Seller's buildings must have adequate perimeter security (fencing) and mechanical security of all entrances (grilles on windows, hardened entrances-doors, etc.) **Manner of fulfilling in case of physical audit**: a physical inspection of the security area and mechanical security systems, submission of the document "Description of physical and logical perimeter, or document "Security project" or directive "Physical protection" or similar documents describing the state of physical security. In the case of an external entity, document the contract for the provision of physical security **Manner of fulfilling in case of remote audit**: submission of a document "Description of physical and logical perimeter, or document "Security project" or directive "Physical protection" or similar documents describing the state of physical security by remote access or display on a shared screen be photographs of installed technologies). To document photos of the security of the building and, in the case of an external entity, document the contract for ensuring physical security.
11	A key management has to be implemented	**Minimum level to fulfil the requirement**: The Seller operates a transparent key mode - registration, assignment and secure storage of keys. It is not possible to take the keys outside the Sellller´s building. The key mode system must be inspected at least once a year. **Manner of fulfilling in case of physical audit**: a control of records and storage space for keys, documentation of documents that a check of records of assigned keys is performed at least once a year. **Manner of fulfilling in case of remote audit**: in the form of remote access or display on a shared screen, document the evidence that the key mode is implemented (photo documentation of key storage must be included) and a record of checking the records of assigned keys (at least once a year).

No	Requirements	Further description on manner of fulfilling the requirement
12	The data have to be storage securely, IT systems have to be regularly audited	**Minimum level to fulfil the requirement**: Servers and data storage must be located in a separate space equipped with a camera system with recording, which monitors the entire space without blind spots, secured against unauthorized access - ACS and equipped with IDS, FS is recommended. A system audit must be set up over IT systems. **Manner of fulfilling in case of physical audit**: a physical inspection of the space with servers and data repositories, documentation of audit records, and logs, including their analysis and subsequent classification of deficiencies. Overview of security events and incidents. **Manner of fulfilling in case of remote audit**: in the form of remote access or display on a shared screen, to submit a description of the security of server rooms and data repositories, and to submit a document describing how to perform a system audit.
13	The IT specialists are employed by the Seller	**Minimum level to fulfil the requirement**: The Seller has its own IT staff, at least at the level of security management. **Manner of fulfilling in case of physical audit:** documentation/preview of personnel records **Manner of fulfilling in case of remote audit**: in the form of remote access or display on a shared screen (preview of personnel records)
14	A policy for circulation and evidence of materials is implemented	**Minimum level to fulfil the requirement**: The Seller operates a functional system for registration, circulation and storage of materials and documents. The Seller must have created the storage facilities and must have records of all materials during production, including waste. A waste disposal system must be in place. **Manner of fulfilling in case of physical audit**: submission of a document describing the system of registration, circulation and storage of materials and documents. **Manner of fulfilling in case of remote audit**: in the form of remote access or by displaying on a shared screen to document a document that describes the system of registration, circulation and storage of materials and documents
15	The policies for access to information systems during and at termination of employment are implemented	**Minimum level to fulfil the requirement**: The Seller ensures controlled access to information and has a system in place to terminate access to inf. systems after termination of employment. **Manner of fulfilling in case of physical audit**: to document procedures – e.g. a document output sheet.

No	Requirements	Further description on manner of fulfilling the requirement
		Manner of fulfilling in case of remote audit: in the form of remote access or by display on a shared screen to document, for example, the document output sheet
16	There is an own staff for processing of order	**Minimum level to fulfil the requirement**: To ensure the production of the Buyer products, the supplier uses its own employees or agency employees, who must have a signed confidentiality agreement with both their own agency and the Seller. At the same time, there must be a confidentiality agreement between the Seller and the staffing agency. **Manner of fulfilling in case of physical audit**: documentation/preview e.g. in personnel record. **Manner of fulfilling in case of remote audit**: in the form of remote access or display on a shared screen to allow a preview of personnel record.