**AFFIDAVIT ON SECURITY REQUIREMENTS**

**Public Contract Name:**

**Production and Supply of Chip Prelaminates**

|  |  |
| --- | --- |
| **Name of Contractor (incl. legal form):** | ………………………… |
| **Registered office:** | ………………………… |
| **Reg. No.:** | ………………………… |

(hereinafter “**the Contractor**”)

As a person authorized to act in the name of or for the Contractor, I hereby solemnly declare that the Contractor meets the following requirements regarding the implemented security processes in place to ensure the production security integrity (transport incl.), whereas the Contracting Authority has a right to check the Contractor's security processes according to this affidavit:

**All the following requirements arise from requirements of ISO 14298 and CWA 15374.**

| **No** | **Requirements** | **Minimum level to fulfil the requirement** | ***The Contractor shall state whether it fulfils the requirement:*** *YES/NO* |
| --- | --- | --- | --- |
| 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. reasonably, 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 | YES/NO |
| 02 | The subcontractors, who are participating in the order for STC, 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 in the supply of services to the participant under this contract. Security checks at subcontractors 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. | YES/NO |
| 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 STC, 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 | YES/NO |
| 04 | The security requirements between STC and the supplier have to be set up and documented | Minimum level to fulfil the requirement: The supplier must have set up and documented safety procedures and rules for the production and delivery of services or products for STC. 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. | YES/NO |
| 05 | Regular internal security audits have to be performed | Minimum level to fulfil the requirement: The participant implements and records regular internal security audits of its own procedures and rules (at least once a year). | YES/NO |
| 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 | YES/NO |
| 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 * Allocation of people, tools and other resources | YES/NO |
| 08 | The supplier’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 supplier'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. | YES/NO |
| 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. | YES/NO |
| 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 supplier's premises. The supplier's buildings must have adequate perimeter security (fencing) and mechanical security of all entrances (grilles on windows, hardened entrances-doors, etc.) | YES/NO |
| 11 | A key management has to be implemented | Minimum level to fulfil the requirement: The supplier operates a transparent key mode - registration, assignment and secure storage of keys. It is not possible to take the keys outside the supplier's building. The key mode system must be inspected at least once a year. | YES/NO |
| 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. | YES/NO |
| 13 | The IT specialists are employed by supplier | Minimum level to fulfil the requirement: The supplier has its own IT staff, at least at the level of security management. | YES/NO |
| 14 | A policy for circulation and evidence of materials is implemented | Minimum level to fulfil the requirement: The supplier operates a functional system for registration, circulation and storage of materials and documents. The supplier 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. | YES/NO |
| 15 | The policies for access to information systems during and at termination of employment are implemented | Minimum level to fulfil the requirement: The supplier ensures controlled access to information and has a system in place to terminate access to inf. systems after termination of employment. | YES/NO |
| 16 | There is an own staff for processing of order | Minimum level to fulfil the requirement: To ensure the production of STC products, the supplier uses its own employees or agency employees, who must have a signed confidentiality agreement with both their own agency and the supplier. At the same time, there must be a confidentiality agreement between the contractor and the staffing agency. | YES/NO |