**Verification of the cybersecurity level of SOR suppliers**

The company or its organizational unit responsible for delivering to the SOR shall complete the following questionnaire defining the level of its security standard and the resulting cybersecurity risks. This questionnaire shall also serve as an audit skeleton for any customer audit of the supplier's SOR.

|  |  |
| --- | --- |
| **Supplier** (business name, registration number):  |  |
| Person responsible for completion (name, contact): |  |
| Date of completion:  |  |
| **Evaluation of the questionnaire**: (satisfactory, conditionally satisfactory, unsatisfactory) |  |
| **QUESTIONNAIRE EVALUATION*** **Satisfactory** – fulfillment of requirements in level C is less than 25%
* **Conditionally compliant with Action Plan** – Level C compliance is more than 25% and less than 75%
* **Unsatisfactory -** requirements in level C by more than 75%. Cooperation with this supplier is possible only in exceptional justified cases with the necessary limited sharing of confidential data.
 |
| **SWORN STATEMENT**The above mentioned responsible person, as an authorised representative of the supplier, declares on oath that the information in the questionnaire below corresponds to the actual situation in the supplier's company on the date of completion of the questionnaire. The correctness of these data can be verified by a representative of SOR on request or by a customer audit of SOR at the customer's premises, if necessary, at the time before the conclusion of the commitment or at any time during the commitment. At …………………………, on ………………………… qualified electronic signature / handwritten signature of the authorised person. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Area, requirement** | **Supplier's level of performance** | **Achieved level (A, B, C)** | **Note on the fulfilment of the requirement** |
| **A** | **B** | **C** |
| **A. STANDARDS** |
| 1 | Does the supplier apply the requirements of the standard below in practice? |
| a. | Compliance with the UN Regulation No. 155, 156 | Yes, certified | Yes, not certified | No |  |  |
| b. | ISO/IEC 27001 | Yes, certified | Yes, not certified | No |  |  |
| c. | ISO/SAE 21434 | Yes, certified | Yes, not certified | No |  |  |
| d. | TISAX | Yes, certified | Yes, not certified | No |  |  |
| e. | NIS2 | Yes, we are included in the scope of the NIS2 under the supervision of the national authority | We are not included, but we voluntarily comply with all the conditions of NIS2 | No |  |  |
| In case at least one of the previous questions has been answered with the answer in column A, please provide a certificate or other proof, there is no need to continue with the questionnaire.If level A has not been achieved for at least one question, please continue to complete the following questionnaire. |

|  |
| --- |
| **B. BASIC MEASURES** |
| 2 | Does the supplier have a cybersecurity manager or other designated person with equivalent responsibilities? | Yes, separate defined role | No, it comes under IT, no role description | No |  |  |
| 3 | Is the supplier subject to a cybersecurity audit or analysis? | Yes, performed regularly | Yes, performed randomly or irregularly | No |  |  |
| 4 | Does the supplier conduct a cybersecurity risk assessment? | Yes, regularly, risk analysis maintained | Yes, done once in the past | No |  |  |
| 5 | Which areas are covered by the management documentation (security policies, ICT usage guidelines, …) if such documentation exists at the supplier? |
| a. | Risk management processes | Yes | Partially solved | Unsolved |  |  |
| b. | Classification of assets | Yes | Partially solved | Unsolved |  |  |
| c. | Data protection against disclosure, destruction, integrity and availability | Yes | Partially solved | Unsolved |  |  |
| d. | Personal data protection | Yes | GDPR scope only | Unsolved |  |  |
| e. | User identification and authentication | Yes | Partially solved | Unsolved |  |  |
| f. | Rights-based data access control | Yes | Partially solved | Unsolved |  |  |
| g. | Privileged access control | Yes | Partially solved | Unsolved |  |  |
| h. | End station protection | Yes | Partially solved | Unsolved |  |  |
| i. | Protecting mobile devices and remote access | Yes | Partially solved | Unsolved |  |  |
| j. | Protecting email and intra-company communication (instant messaging) | Yes | Partially solved | Unsolved |  |  |
| k. | Protecting access to the Internet | Yes | Partially solved | Unsolved |  |  |
| l. | Protecting removable media | Yes | Partially solved | Unsolved |  |  |
| m. | Change management processes | Yes | Partially solved | Unsolved |  |  |
| n. | Protecting wireless networks and communications | Yes | Partially solved | Unsolved |  |  |
| o. | Physical security of information assets | Yes | Partially solved | Unsolved |  |  |
| p. | Security training for end users and administrators | Yes | Partially solved | Unsolved |  |  |
| q. | Protection against malware | Yes | Partially solved | Unsolved |  |  |
| r. | Data exchange protection | Yes | Partially solved | Unsolved |  |  |
| s. | Cyber Incident Handling Processes | Yes | Partially solved | Unsolved |  |  |
| t. | Supplier risk management processes | Yes | Partially solved | Unsolved |  |  |
| u. | Human resources security | Yes | Partially solved | Unsolved |  |  |
| v. | Security audits and analysis | Yes | Partially solved | Unsolved |  |  |
| w. | Business Continuity Management and Emergency Planning | Yes | Partially solved | Unsolved |  |  |
| **C. SECURITY TECHNOLOGIES** |
| 6 | Which of the following security technologies does the supplier operate to prevent security threats in relation to data, software development or information systems? |
| a. | Antivirus software on workstations | Yes, a comprehensive solution | Yes, basic solution (Windows Defender) | No |  |  |
| b. | Antivirus software on mobile devices | Yes, part of a complete solution | Yes, by each user | No |  |  |
| c. | Tool for network intrusion detection (IDS/IPS, Intrusion Detection/Prevention System) | Yes | No | No |  |  |
| d. | Privilege Identity/Access Management (PIM/PAM) tool | Yes | No | No |  |  |
| e. | Multi-factor authentication | Yes, using a mobile device or token | Yes, without using a mobile device or token | No |  |  |
| f. | Automated tool for technology vulnerability management | Yes | No | No |  |  |
| g. | Network Access Control (NAC) tool | Yes | No | No |  |  |
| h. | Distributed denial-of-service (DDoS) protection tool | Yes, including connection to SOC | Yes, insular | No |  |  |
| i. | Encryption tools and techniques | Yes, use precisely as prescribed | Yes, randomly | No |  |  |
| j. | Firewall | Yes | Yes | No |  |  |
| k. | SIEM, Security Information and Event Management | Yes, including connection to SOC | Yes, insular | No |  |  |
| 7 | Have the supplier's internal systems ever been penetration tested? | Yes | No | No |  |  |
| **D. DEALING WITH CYBER INCIDENTS** |
| 8 | Does the supplier have a cyber incident management process in place? | Yes, evaluated systematically | Yes, evaluated on an ad-hoc or non- systematically | No |  |  |
| 9 | Are relevant supplier personnel trained in cyber incident recognition and response? | Yes, systematically | Yes, but intermittently | No |  |  |
| **E. DEVELOPMENT OF SECURITY AWARENESS** |
| 10 | Does the supplier have a process in place for training and safety awareness for workers? | Yes, systemically solved | It doesn't, just crash training. | No, no development |  |  |
| 11 | Are new supplier employees trained in cybersecurity before they gain access to data and information systems? | Yes | Yes, Insufficiently | No |  |  |
| 12 | Does the supplier document employee participation in safety training and education programs? | Yes | Yes | No |  |  |
| 13 | Does the supplier require employees with access to data and information systems to sign individual confidentiality agreements? | Yes, for data and IS that require this.  | No, or incompletely. | No |  |  |

|  |
| --- |
| **F. SUPPLIER'S EXPERIENCE WITH CYBER INCIDENTS**What negative impacts, if any, has the supplier experienced in relation to a cyber incident in the past: |
|  | **Impact** | **Solved (yes/no)** | **A more detailed description of how it was solved** |
| a. | Network outage |  |  |
| b. | Unavailability of email and office applications |  |  |
| c. | Unauthorised misuse of identity |  |  |
| d. | Disclosure of protected data |  |  |
| e. | Loss or destruction of data |  |  |
| f. | Financial loss |  |  |
| g. | Loss of intellectual property |  |  |
| h. | Damage to the reputation of the applicant organization |  |  |
| i. | Negative publicity in the media |  |  |
| j. | Loss of value to the applicant organisation |  |  |
| k. | Criminal prosecution of the applicant organisation |  |  |