# Information Security Requirements for Contractors

Version: 02.09.2024

| Term [abbreviations] | Definition |
|---|---|
| Information processing facility [system] | Any and all network and information systems belonging to IT and OT |
| ISMS | Information security management system |
| IT | Information Technology |
| NISG | Network and Information Systems Security Act[1] |
| NISV | Network and Information Systems Security Ordinance[2] |
| OT | Operational Technology |
| TAG GmbH | TAG GmbH registered with the companies register of the Commercial Court of Vienna under the registration number FN 122567x, with its registered office in Vienna, Austria, and its business address at Wiedner Hauptstraße 120, 1050 Vienna. |

**Suppliers and contractors (hereinafter referred to as "Contractors") shall comply with the following information security requirements in the context of the provision of services for TAG GmbH. The Contractors for which these requirements are relevant include, but are not limited to, those to whom the operation of information processing facilities in connection with the essential service of TAG GmbH pursuant to the NISG is outsourced or Contractors with (administrative) access to information processing facilities of TAG GmbH.**

| Requirement | Regulation |
|---|---|
| **General** | **The Contractor agrees to comply with the following regulations and to implement measures and technical standards with regard to the provision of services for TAG GmbH. Furthermore, the Contractor legally accepts and acknowledges the rights of TAG GmbH set forth herein with regard to the provision of services for TAG GmbH.** |

[1] Netz- und Informationssystemsicherheitsgesetz (NISG), Federal Law Gazette I no. 111/2018
[2] Netz- und Informationssystemsicherheitsverordnung), Federal Law Gazette II no. 215/2019

| | |
|---|---|
| **Information security measures and information security management** | Comply with security measures pursuant to the Information Systems Security Ordinance *(NISV)* in relation to service provision for TAG GmbH.<br><br>Aligned implementation of information security requirements and technical standards (regarding information security) of TAG GmbH.<br><br>Operate an information security management system (ISMS) certified to recognized standards (e.g. ISO/IEC 27001) and implement information security measures in accordance with state-of-the-art technology. |
| **Subcontractors** | The Contractor is obliged to bind their subcontractors with analogous agreements to ensure compliance with TAG GmbH's information security requirements. At TAG GmbH's request, the Contractor shall provide evidence to this effect. |
| **Access to information and information-processing facilities belonging to TAG GmbH** | Access (on the part of deployed workers) exclusively based on the need-to-know principle (employees of the Contractor shall be granted access to the information and facilities of TAG GmbH to the extent required for the provision of services) and least-privilege principle (no access to information of TAG GmbH and facilities beyond the aforementioned requirement and the associated time period).<br><br>Obligation to notify TAG GmbH immediately if employees of the Contractor, who have access to information-processing facilities of TAG GmbH, leave the Contractor's company or changes position within the Contractor's company and this results in changes in connection with the provision of services for TAG GmbH. |
| **Use of confidential authentication information** | Access to information-processing facilities of TAG GmbH only by means of authentication information (especially passwords) individually assigned per user and application. The multiple use of the same authentication information for other purposes (including for other users, applications, or for other customers of the Contractor) is prohibited.<br><br>Obligation to change initial password upon first use. |
| **Security screening of deployed workers** | Perform and provide evidence of security screenings of key workers deployed in the context of providing services to TAG GmbH. |
| **Physical access**<br>in the case of service provision at a TAG GmbH location | Individuals are admitted (initially) only after having been demonstrably instructed in TAG GmbH's information security rules. |
| **Use of external hardware** | The Contractor's external hardware (e.g. notebook for maintenance) may be connected to TAG GmbH's information-processing facilities only where necessary to ensure operations and only after approval by TAG GmbH.<br><br>The Contractor must without prompting provide evidence that the hardware concerned is equipped with state-of-the-art security controls. |

| | |
|---|---|
| **Handling and transfer of information** | Apply TAG GmbH's information classification rules.<br>Obligation to return information of TAG GmbH received for use (including any and all hardware and software as well as physical assets received for use) and also devices of TAG GmbH enabling access to information and facilities belonging to TAG GmbH (such as keys, access cards and security tokens). |
| **Remote access / remote maintenance** regarding information-processing facilities of TAG GmbH | Authorized methods for remote access to information-processing facilities must be defined together with TAG GmbH.<br>Administration via remote maintenance is, where possible, to be carried out only after prior approval and/or activation of remote maintenance by TAG GmbH (including deactivation following completion of remote maintenance activities).<br>Remote access permission to be time-limited (e.g. for 1 year); TAG GmbH regularly reviews permission based on criteria (including necessity and scope of permissions/rights) and correspondingly renews it.<br>TAG GmbH entitled to log remote access and analyse log files. |
| **Supplier audits** | TAG GmbH entitled to perform, or correspondingly task third parties with performing, periodic information security audits and inspections |
| **Ongoing monitoring of activities under supplier agreements** | TAG GmbH entitled to audit and monitor activities that involve confidential information and information-processing facilities belonging to TAG GmbH (including logging and log file analysis). |
| **Security incidents** | Obligation to immediately report security incidents as well as incidents relating to TAG GmbH's essential service to security@taggmbh.at as well as, if this has been agree upon, a further defined contact point, in accordance with the general provisions of the NISG and the NISV, especially naming a contact person at the Contractor incl. contact information.<br>Together with TAG GmbH, agree response and restoration/recovery procedures after occurrence and periodic audits thereof.<br>Obligation to report on an ongoing basis and in conclusion of an incident, to TAG GmbH on how security incidents are managed. |
| **Reporting obligations** | Periodic (at a minimum annual) reports to security@taggmbh.at as well as, if this has been agree upon, a further defined contact point on the state of information security in the context of providing services to TAG GmbH.<br>Where applicable, reporting of outcomes:<br>• relating to service provision for TAG GmbH<br>• of audits by qualified bodies as referred to in the *NISG* |
| **Confidentiality agreements** | The Contractor mandatorily enters into a confidentiality agreement with TAG GmbH in accordance with the TAG GmbH standard. |

| | |
|---|---|
| **Amendment to supplier agreement** | These information security requirements shall be adjusted from time to time by mutual agreement due to changes in the legal framework (especially changes to the NISG, NISV). |