Certification Regulation for Information Security MS

Standard or Certification scheme:	**ISO 27001:2013 - ISO/IEC 27001:2022** **ISO 27701:2019**	**Accreditation Standard:**	**ISO 17021-1:2015**

Certification Cycle:

The certificate is valid for three years. To maintain the validity of the certificate, annual surveillance audits shall be carried out. Before the expiration date of the certificate, a recertification audit is conducted in order to renew the validity of the certificate for the next three (3) year cycle.

Certification audit is conducted in two stages. Stage 1 concerns the control of the basic and required by the standard documentation. The audit documentation includes a review of the Risk Assessment methodology and results of its implementation. Stage 1 may not be conducted in the client's premises. Stage 2 is an onsite audit and concerns the audit of the existence, operation and efficiency of the management system. The interval between stage one and stage 2 cannot exceed six (6) months. If this period elapses or significant changes occur that affect the MS, stage 1 must be repeated. Stage 1 audit findings may lead to postponement or cancellation of Stage 2.

Audit planning and time table. Surveillance audit process has to be completed annually, with due date the date of the certification decision after the Initial Certification audit. Correspondingly the re-certification audit process has to be completed within the same time frame. Example:

Certification Decision	**1st Surveillance audit**	**2nd Surveillance**	**Re-certification audit**
15/7/2023	*15/7/2024*	*15/7/2025*	*15/7/2026*

In case of exceeding time limits certificate is suspended for six months and after this period finally withdrawn.

The valid Statement of Applicability is stated on the certificate and is reviewed during the audit. The client during the operation of the MS and the certificate maintenance is obliged to inform TAH for any changes that may occur to the Statement of Applicability. In any case, changes to the Statement of Applicability leads to cancellation of the previous certificate and issuance of a new one. Before the issuance of the new certificate, TAH shall consider whether an audit should be conducted in order to review changes. In general, special audits are required in cases where new control points of the standard (Annex A), are included to the client's MS as it will appear in the Statement of Applicability.

In recertification audits, a stage 1 may be conducted when there have been significant changes in the management system or in the framework within which it operates (eg changes in legislation), and the client.

Audit Conduction ISO/IEC 27701	Certification to ISO/IEC 27001 is obligatory in order to obtain certification for ISO/IEC27701. The scope of the ISO/IEC 27701 certification ✔ is within or identical to the scope of the ISO/IEC 27001 certification. ✔ is included within boundaries of the activities of the client as defined in the scope of the PIMS. ✔ PII processing is included TÜV Austria will suspend, withdraw or reduce the scope of certification of ISO/IEC 27701 where its base ISO/IEC 27001 certification is suspended, withdrawn or its scope (which includes the scope of ISO/IEC 27701 certification) is reduced.	
Transition audits	TÜV Austria (TA) may conduct the transition audit in conjunction with the surveillance audit, recertification audit or through a separate audit. The transition audit shall not only rely on the document review, especially for reviewing the technological information security controls. The transition audit shall include, but not be limited to the following: ✔ The gap analysis of ISO/IEC 27001:2022, as well as the need for changes to the client's ISMS. ✔ The updating of the statement of applicability (SoA). ✔ If applicable, the updating of the risk treatment plan. ✔ The implementation and effectiveness of the new or changed information security controls chosen by the clients. TA may conduct the transition audit remotely if they ensure the transition audit objectives is met. After the positive certification decision, the certificate is issued based on the certification cycle of the existing ISO/IEC 27001:2013 certificate.	
Transition timeline	✔ A three-year transition period is provided for the adaptation to the requirements of the ISO/IEC 27001:2022, starting from its date of issue, until 31.10.2025. ✔ The transition period of ISO/IEC 27001:2022 expires on 31.10.2025. All certificates according to ISO/IEC 27001:2013 will be suspended or withdrawn at the end of the transition period. ✔ TÜV Austria may conduct initial or recertification audits according to ISO/IEC 27001:2013 until 30.04.2024. All certificates issued according to ISO/IEC 27001:2013 during the transition period must take account of the above deadline (whether or not the usual three-year period of validity of the certificate will be completed). Organizations that have in place ISO/IEC 27001:2013 certificate will have the ability to switch to the new ISO/IEC 27001:2022 standard during their annual surveillance audits or recertification audit or separate transition audit, with prior written notification of TÜV Austria.	
Audit Evaluation Criteria / Characterization of Non Conformities:	**1:** Full conformity	**3:** Minor Non-Conformity(-ies): reviewed and accepted the client's plan for correction and corrective action
	2: Observation, the effectiveness of the corrective action is evaluated during the next audit	**4:** Major Non-Conformity(-ies): Correction through submission of Documents or Re-audit
	OFI: Opportunities for Improvement: No further action is required by the client	
Time allowed to close Non	**Certification Audit:** 2 months after the completion of stage 2. **Surveillance Audit:** 2 months after the date of the audit or no later than the due date of the Certification Decision	

Conformities:	**Recertification Audit:** 2 months after the date of the audit or no later than the due date of the Certification Decision
Contractual Duration:	The duration of the service and the contractual obligation comes into force upon signature by both parties (TÜV AUSTRIA and Client Organization) and is valid for (3) three years of the relevant offer in cases of initial certification or re - certification. In case of Accredited Certification Transfer, the duration covers the validity period of the transferred certificate. In case of transition to a new version of the standard, the duration of contractual obligation is valid until the certification expiry date mentioned on the relative paragraph of the regulation.