A1 Group Minimum Security Requirements for Suppliers

A1 Group Security Controls Framework

Version	1.0
Classification	Public
Document ID	TPE-STD-GRP-ENG-V1.0
Document status	APPROVED
Document owner	A1 Group Risk & Resilience
Master copy location	Link
Effective date	01.12.2025

***Note**: This document is maintained in electronic form. Printed copies may differ from the current version.*

TABLE OF CONTENTS

1 INTRODUCTION

1.1 OVERVIEW

This document describes the minimum security requirements ("controls") for suppliers ("3rd parties") of A1 Group.

1.2 PURPOSE

The aim of this Standard is to ensure the integrity, confidentiality, and availability of the information resources of A1.

The A1 third party risk management ensures that all third parties, especially those A1 classifies as particularly security-relevant, meet the high internal security standards of A1 as well as external regulatory and normative requirements (e.g. Network and Information Security Act 'NISG', ISO 27001 certification).

A1 expects all third parties to work towards full compliance to these security requirements, thereby contributing to the security of the shared business relationship. This doesn't however imply mandatory full compliance at the time of entering a business relationship. A1 requires suppliers to provide adequate information about deviations to A1's requirements to assess related risks.

Through this proactive approach in third party risk management, A1 is able to ensure that information security remains at the highest level and risks can be addressed early on.

1.3 SCOPE

In the digital age, the security and integrity of data managed by telecommunication companies and their suppliers is of critical importance. This document establishes the minimum security requirements for suppliers (hereinafter also referred to as contractors, external partners, external suppliers, providers, 3rd parties, service providers, or data processors) of A1.

Suppliers are all external companies, organizations, strategic partners, consultants or individuals that provide goods or services to A1 or otherwise have access to A1's information systems or data. This includes both physical goods, (digital) services and software solutions.

1.4 TARGET AUDIENCE

All controls in this document are valid for all 3rd parties of A1 Group.

1.5 HOW TO USE THIS DOCUMENT

Suppliers are required to carefully review A1's security requirements for 3rd Parties and to ensure that they work towards compliance to them. This includes all minimum security requirements set out in this document.

1.6 NOTIFICATION OF DEVIATIONS

The supplier must provide a complete and accurate report on A1's request, detailing points of non-compliance with the requirements in this document. This also includes answering questionnaires sent out by A1 regarding the security posture as well as providing (independent) evidence (ISO27001 certificate, ISAE SOC2 report,…).

Risk Mitigation

Should suppliers find that they cannot meet individual security requirements, they must immediately notify A1 at the email address supplychainsecurity@a1.group. In such cases, A1 will assess whether the control deviation poses a risk to the company.

It is necessary for suppliers to keep A1 informed on how they will mitigate potential risks arising from control deviations. This will involve the provision of detailed information on measures taken and/or planned to reduce risk exposures at the request of A1.

Regular security assessments for suppliers with high security relevance

It is expected that all suppliers classified by A1 as particularly relevant for security (e.g. because their products and/or services contribute to Sarbanes-Oxley Act 'SOX'-, Digital Operational Resilience Act 'DORA'- or Network and Information Security 'NIS'-relevant services) are available at least once every 36 months for a reassessment (e.g. interview, questionnaire or by other means). to evaluate their security status. This expectation includes the provision of adequate resources to do so. This conversation is intended to assess the current security posture of the supplier and ensure they meet A1's requirements.

ISO27001-Flag

To facilitate compliance with these requirements, this document contains a detailed mapping of each control to the ISO 27002:2022 standard in annex A. Suppliers who already have an ISO 27001 certification can easily identify which of the required controls they presumably already satisfy with their existing certification. The controls affected are also marked with a ISO27001 symbol in the respective chapter. This reduces the effort to implement additional security measures and promotes a standardized security culture amongst the companies involved.

2 GENERAL SECURITY REQUIREMENTS

ISO27001 **TPE-STD-GRP-GSR-001** The supplier must have a defined set of policies for information security, which is approved by management, published, and communicated to employees and relevant external parties. The policies for information security are reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.

ISO27001 **TPE-STD-GRP-GSR-002** The supplier must define, allocate and formally document security and business continuity management responsibilities in their organization (e.g. formal nomination, RACI-Matrix, Shared Responsibility Model…).

ISO27001 **TPE-STD-GRP-GSR-003** The supplier must provide a point of contact for security and business continuity management topics to A1. Changes to these points of contact must be communicated immediately to A1. In case of crisis, the points of contacts may be called upon for the supplier to consult as technical experts.

ISO27001 **TPE-STD-GRP-GSR-004** The supplier must have an information classification scheme in place, based on the business impact for the supplier. All documents are classified following an appropriate set of procedures for information labelling and are labelled in accordance with the confidentiality of the information therein.

TPE-STD-GRP-GSR-005 The supplier must ensure that the service provision is subject to a defined approach for service management (e.g. COBIT, ITIL, ISO 20000).

ISO27001 **TPE-STD-GRP-GSR-006** The supplier must carry out changes to systems or infrastructure that process A1 data in accordance with a documented IT change management process.

ISO27001 **TPE-STD-GRP-GSR-007** The supplier conducts assessments of internal controls at regular intervals, as documented in an annual audit plan, according to defined assessment instructions and performed by dedicated, knowledgeable personnel.

TPE-STD-GRP-GSR-008 The supplier must, if necessary, undergo an audit by A1 (or by a party accepted by A1) after adequate prior notice. The scope of the audit will be determined by A1 and will provided in a reasonable time.

ISO27001 **TPE-STD-GRP-GSR-009** The supplier must ensure that measures are taken to verify the trustworthiness of its employees in accordance with applicable laws (e.g. through background checks, checks of criminal records,…) and that information made accessible to them in their respective job function is subject to a Non-Disclosure Agreement (NDA; e.g. via a clause in their employee contracts or a separate document).
The supplier acknowledges that A1 has the right to demand and review the evidence(s) of trustworthiness provided by the employees to the supplier before access rights will be awarded. This entails particularly employees of the supplier who should be awarded privileged access rights for service delivery. If employees or their suppliers refuse to produce such evidence(s), or employees have an entry resulting in the loss of confidence, A1 has the right to reject providing access to its systems, data or infrastructure.

ISO27001 **TPE-STD-GRP-GSR-010** The supplier must ensure that all their personnel and, where relevant, (sub)contractors, receive appropriate awareness training regarding security requirements and procedures, as relevant to their job function.

ISO27001 **TPE-STD-GRP-GSR-011** The supplier acknowledges that user credentials (username, password…) may never be shared with others.

TPE-STD-GRP-GSR-012 The supplier acknowledges that A1 reserves the right to award any access rights, either to locations, systems or infrastructure of A1, only after their employees have been made aware of and had the chance to sign A1-internal security requirements (e.g. Acceptable Use Policy, system-specific security measures, confirmation of receipt for access cards/user equipment).

ISO27001 **TPE-STD-GRP-GSR-013** The supplier acknowledges that actions of accounts on selected A1 services may be recorded to ensure traceability & reconstruction of events.

TPE-STD-GRP-GSR-014 The supplier must inform A1 immediately about every change (leave, move, suspension or termination) in employee status, if that change affects the necessary physical and logical access rights for service delivery to A1. A1 reserves the right to terminate and/or revoke all access rights granted to the supplier's employee(s).

TPE-STD-GRP-GSR-015 The supplier must ensure that all issued access cards, equipment and control of accounts are returned to A1. If physical access rights (access cards, chips, keys or others) cannot be returned for whatever reason (loss, theft,…), A1 reserves the right to charge a reimbursement of costs.

ISO27001 **TPE-STD-GRP-GSR-016** The supplier must ensure that access to A1 data or A1 data itself is only used for service delivery according to contractual arrangements with the supplier. Access to A1 data or A1 data itself may only be transferred to suppliers, contractors or subcontractors after receiving written confirmation from A1.

ISO27001 **TPE-STD-GRP-GSR-017** The supplier must group their networks, information systems, and users in a way that implements the "Least Privilege" principle.

ISO27001 **TPE-STD-GRP-GSR-018** The supplier must implement measures for systems and infrastructure that process A1 data to ensure:

- that access to productive systems (real data) is restricted, as well as
- the principles of "need to know" and "segregation of duties" (see Appendix A)

are being ensured. This mainly concerns the administrative access of the supplier to these systems and infrastructure.

TPE-STD-GRP-GSR-019 The supplier must ensure user rights and roles can be assigned/revoked on their systems and infrastructure where A1 data is processed.

ISO27001 **TPE-STD-GRP-GSR-020** The supplier must – where possible – enable multi-factor authentication (2FA/MFA) to access their system(s) and infrastructure via insecure networks (e.g. networks not under the control of the supplier).

ISO27001 **TPE-STD-GRP-GSR-021** The supplier must have an endpoint security solution (e.g. antivirus software) in place on all endpoints accessing or modifying A1 data or accessing A1 infrastructure. The endpoint security solution must be regularly updated and provide real-time monitoring and response capabilities. Identified malicious software must be removed immediately.

ISO27001 **TPE-STD-GRP-GSR-022** The supplier must implement security measures against network-based attacks (e.g. Intrusion Prevention Systems - IPS, firewall, network segmentation) for systems and infrastructure processing A1 data.

TPE-STD-GRP-GSR-023 The supplier must, for systems and infrastructure processing A1 data and being accessible from the internet, have measures in place for the prevention or mitigation of Denial-of-Service (DOS) attacks. These measures must be documented and evidence provided to A1 upon request.

TPE-STD-GRP-GSR-024 Security updates for IoT devices must be offered by the manufacturer and/or supplier throughout the entire lifecycle of the products and must be distributable and installable automatically or without manual intervention. There must be no hardcoded passwords in the devices.

2.1 Users with privileged access rights

ISO27001 **TPE-STD-GRP-GSR-025** The supplier must ensure that users in control of accounts with privileged access rights have adequate knowledge in the domain of system administration.

ISO27001 **TPE-STD-GRP-GSR-026** The supplier acknowledges that accounts with privileged access rights may only be used for administrator-related work (maintenance, patching…).

TPE-STD-GRP-GSR-027 The supplier must ensure that the identities of employees of the supplier in control of accounts with privileged access rights for systems and infrastructure of A1 have been verified. Upon request of A1, the supplier must provide written confirmation that the employees are who they claim they are. The supplier bears all responsibility for the accounts with privileged access rights awarded to and entrusted with the supplier to fulfil their contractual obligations.

3 INCIDENT MANAGEMENT

ISO27001 **TPE-STD-GRP-INC-001** Security incidents and personal data breaches with potential impact on the products/services that A1 receives from the supplier and/or with potential impact on data received by the supplier from A1 must be reported without undue delay (but no later than 20 hours after having become aware of it) to abuse@a1.at and cert@a1.at. The report must contain the following information at a minimum:

- A description of the nature and scope of the incident (including categorization, time frame, affected information, and estimation of the expected impact),
- Point(s) of contact and information channels,
- Measures already taken by the supplier and suggestions for measures that A1 should take,
- or, if A1 data containing personal identifiable information could be affected, any further information required in accordance with privacy legislation (e.g. General Data Protection Regulation - GDPR).

TPE-STD-GRP-INC-002 The supplier acknowledges that A1 must be contacted immediately in case physical or logical access rights (access cards, physical access tokens…) to A1 systems or infrastructure are lost (this also includes „stolen", „misplaced", „not recoverable", or any other suspicion of abuse or unauthorized access to credentials). Relevant contact details may be found in control TPE-STD-GRP-INC-001.

TPE-STD-GRP-INC-003 The supplier must inform A1 in case of any extraordinary set of circumstances impacting the continuity of services rendered or availability of product(s)/ system(s) offered to A1 (e.g. change of control, insolvency, bankruptcy…). This information must entail information about possible impacts to A1 and potential remediation strategies.

TPE-STD-GRP-INC-004 The supplier is obligated to assist in the investigation of security-related incidents and therefore must ensure that security-relevant log information (admin and user behaviour, relevant copying processes, etc.) of the infrastructure processing A1 data exists for a period of at least 3 months for forensic analysis. These logs are to be provided to A1 upon request to assist in such an investigation.

TPE-STD-GRP-INC-005 The supplier must ensure penetration testing is performed on systems and infrastructure processing A1 data (and which is managed by the supplier) at least every 18 months. Adequate measures are to be derived and implemented to rectify any findings from such a penetration test. Upon request, the supplier must provide A1 evidence of tests conducted. If A1 has doubts about the quality of the penetration tests conducted, the supplier agrees to have their product(s), system(s) or infrastructure processing A1 data penetration tested by A1 or a party (agreed between all parties) on behalf of A1 after adequate prior notice and scope definition.

ISO27001 **TPE-STD-GRP-INC-006** The supplier must perform regular data backups on systems and infrastructure processing A1 data and which is managed by the supplier (including, where applicable, according to contractual arrangements with such supplier) and demonstrably test their recoverability. Upon request from A1, evidence of the completion of these tests must be provided.

4 REPORTING

TPE-STD-GRP-REP-001 A quarterly reporting by the supplier to A1 regarding the services provided must be carried out and include at least the following points:

- Availability of the system on a monthly basis,
- Incident Reaction Time,
- Incident Resolution Time on a monthly basis,
- Implemented technical security measures,
- Identified vulnerabilities classified by CVSS,
- Resolved vulnerabilities, and
- Remediation times for vulnerabilities.

Where reporting on specific KPIs is not technically feasible or not applicable due to the nature of the service, the supplier must:

- Explicitly document the limitation, including a technical or operational justification, and
- Propose alternative monitoring or reporting mechanisms, where applicable.

The supplier is expected to support reasonable efforts to improve KPI reporting capabilities over time.

5 SOFTWARE ARCHITECTURE & VULNERABILITY MANAGEMENT

ISO27001 **TPE-STD-GRP-SAV-001** The supplier must ensure that security updates/patches must be offered by the supplier (or the manufacturer of the respective product[s] or system[s] purchased via the supplier) throughout the entire product lifecycle.

ISO27001 **TPE-STD-GRP-SAV-002** The supplier must ensure that all product(s) or service(s), including those provided by manufacturer via the supplier, are free of known software vulnerabilities (e.g. via static/dynamic code testing, fuzzing or other means). Any remaining known vulnerability must be documented, communicated to A1 and dealt with according to control TPE-STD-GRP-SAV-005. The supplier ensures that all components, including third party libraries, are included in this documentation.

TPE-STD-GRP-SAV-003 The supplier must implement measures (e.g. static/dynamic source code analysis) for detecting software vulnerabilities in source code during software development. These measures must be documented and provided to A1 upon request.

TPE-STD-GRP-SAV-004 The supplier must ensure that systems and infrastructure processing A1 data are periodically evaluated for current vulnerabilities (e.g. through vulnerability scans, software inventory checks, code- and library analyses). Upon request from A1, evidence of the completion of these evaluations must be provided. Found vulnerabilities must be dealt with according to control TPE-STD-GRP-SAV-005.

TPE-STD-GRP-SAV-005 The supplier must ensure that found vulnerabilities in systems and infrastructure processing A1 data or, if the supplier is the manufacturer of the respective product(s) or service(s), found in those product(s) or service(s), must be addressed according to the following table (starting from the identification of the vulnerability in the system): HIGH 30 days, CRITICAL 15 days. The classification is based on the assessment according to VPR (Vulnerability Priority Rating). If categorization according to VPR is not available, CVSS version 3 must be used.

TPE-STD-GRP-SAV-006 The supplier must ensure that neither they nor the manufacturer of the respective product(s) or service(s) charge for the rectification of security vulnerabilities contained within the respective product(s) or service(s) purchased via the supplier during the term of the maintenance contract.

TPE-STD-GRP-SAV-007 The supplier must harden systems and infrastructure that process A1 data according to accepted methods of hardening (such as the "CIS Benchmarks" – see appendix A). Upon request from A1, evidence of the methods used, and the degree of implementation, must be provided.

ISO27001 **TPE-STD-GRP-SAV-008** The supplier must adhere to the principles of "Secure Software Development" (e.g. in the Software Development Life Cycle - SDLC, Threat Modelling, etc.) and ensure secure scaling as well as logical segmentation of the application during the development phase of said applications – for example, by dividing the application into layers/tiers and microservices.

TPE-STD-GRP-SAV-009 When dividing applications into layers/tiers, the supplier must ensure that no layer (tier) can be skipped when accessing applications, and that only defined protocols (ports) are used when transitioning from one layer (tier) to the next.

ISO27001 **TPE-STD-GRP-SAV-010** The supplier must implement adequate (logical or physical) measures to ensure tenant separation between A1 and other customers of the supplier. These measures must be documented and provided to A1 upon request.

ISO27001 **TPE-STD-GRP-SAV-011** The supplier must ensure that a separation between pre-production and production systems is implemented. The specific technical implementation of the separation must be documented and provided to A1 upon request.

TPE-STD-GRP-SAV-012 The supplier may only process productive data (real data) received from A1 in production environments and may only use anonymized or synthetic data in test/pre-production environments.

6 ENCRYPTION

ISO27001 **TPE-STD-GRP-ENC-001** A1 data being stored on supplier's infrastructure or systems must be encrypted.

ISO27001 **TPE-STD-GRP-ENC-002** The data transfer between the supplier's infrastructure or systems, including external infrastructure and systems the supplier uses to facilitate such a transfer via 4th parties, and A1's infrastructure or systems must be encrypted.

ISO27001 **TPE-STD-GRP-ENC-003** The supplier must ensure that cryptographic keys are generated, stored, and archived in a secure environment.

ISO27001 **TPE-STD-GRP-ENC-004** The supplier must ensure that cryptographic algorithms used in systems and infrastructure, where A1 data is processed, are being documented and communicated to A1 upon request.

TPE-STD-GRP-ENC-005 The supplier must ensure that on systems and infrastructure, where A1 data is processed, only encryption methods considered 'State of the Art' are used (e.g. AES with a key length of 128-256 bits, Camellia with 128-256 bits, ECIES with >250 bits, DLIES with >3000 bits, RSA with >3000 bits, PQC/QKD). "State of the art" may be constituted to be verified also by independent third parties (as defined by Germany-based "Bundesamt für Sicherheit in der Informationstechnik" – BSI or US-based "National Institute for Standards and Technic" – NIST).

ISO27001 **TPE-STD-GRP-ENC-006** The supplier must ensure that no outdated encryption methods are being used on systems and infrastructure where A1 data is processed (e.g. Triple-DES, Serpent, Twofish, DES, RC4, Blowfish).

TPE-STD-GRP-ENC-007 The supplier must ensure that for A1-relevant systems:

- regular changes of cryptographic keys are technically supported,
- processes for key changes are established,
- key changes are carried out upon request by A1 (by the supplier), or
- key changes can be carried out independently by A1.

The execution must be documented and evidence provided to A1 upon request.

7 AUTHENTICATION AND AUTHORIZATION MANAGEMENT

TPE-STD-GRP-AAM-001 If the supplier's product(s) or system(s) entails local user accounts, A1 must be able to manage them independently (create, delete, lock, modify).

TPE-STD-GRP-AAM-002 If the supplier's product(s) or system(s) entails local user accounts, the following requirements for secure passwords must be met:

- Require a length of at least 14 characters,
- require at least 3 of these 4 criteria: uppercase letters, lowercase letters, numbers, special characters;
- regular and/or spontaneous password changes must be technically supported,
- storage and transmission of passwords in plain text are not permitted and
- password storage must use salting.

TPE-STD-GRP-AAM-003 If the supplier's product(s) or system(s) entails local user accounts, the supplier must ensure that the following requirements for initial passwords are met:

- must be generated randomly,
- are transmitted in encrypted form,
- can only be used once and
- are valid for a maximum of 14 days.

TPE-STD-GRP-AAM-004 If the supplier's product(s) or system(s) entails local user accounts, the supplier must ensure that end user accounts are technically forced to change their initial password immediately after initial login It should further be possible to trigger this forced password change functionality manually when needed e.g. after an incident where credentials are leaked.

TPE-STD-GRP-AAM-005 If the supplier's product(s) or system(s) entails local user accounts, the supplier must implement adequate measures against unauthorized access (e.g. time-lapse thresholds, temporary account lockout after repeated unsuccessful login attempts to avoid brute force attacks). These measures must be documented and provided to A1 upon request.

TPE-STD-GRP-AAM-006 Alternative authentication methods are permissible, provided they offer an equal or higher level of protection compared to the methods described in these requirements. The approval of A1 for an alternative authentication method must be obtained.

8 CLOUD OR OTHER ONLINE SERVICES

ISO27001 **TPE-STD-GRP-COS-001** The supplier must ensure that cloud or other online services are operated redundantly at a minimum of 2 data center locations.

ISO27001 **TPE-STD-GRP-COS-002** The supplier must ensure that all A1-relevant components of its cloud or other online services are integrated into a central configuration management system.

ISO27001 **TPE-STD-GRP-COS-003** If the supplier delivers cloud services or other online services to A1, the supplier must ensure that systems and infrastructure processing A1 data protocol and hold available security relevant events in a structured, common, immutable ("audit proof") as well as machine readable manner (log files). An integration into A1's SIEM must be supported by the supplier.

9 4TH PARTIES, SUB-SUPPLIERS AND SUB-CONTRACTORS

ISO27001 **TPE-STD-GRP-SSC-001** The supplier must have formal security requirements in their contracts with suppliers (hereinafter also referred to as '4th parties', sub-suppliers, subcontractors, suppliers of suppliers) in place.

TPE-STD-GRP-SSC-002 The formal security requirements in contracts with suppliers must not be less stringent than those stated in this standard.

TPE-STD-GRP-SSC-003 The supplier must have a process in place to monitor, review and audit, on a regular basis, the security and service delivery of their supplier(s).

TPE-STD-GRP-SSC-004 The supplier must produce a list of 4th parties, in particular Cloud providers, which are critical for the supplier to ensure the service delivery for A1 services. Each time a critical supplier changes or upon request of A1, this list must be revised and communicated to A1.

10 AI SYSTEMS AND COMPONENTS

TPE-STD-GRP-ASC-001 If the supplier provides an AI system as defined in Article 3(1) of Regulation (EU) 2024/1689 (the "AI Act"), or an AI model, including a general-purpose AI model as defined in Article 3(63) of the AI Act, the supplier must assess and classify the respective AI system(s) and/or model(s) in accordance with the risk categories and assessment criteria established under the AI Act.
The resulting classification, together with a detailed description of the methodology used to determine such classification (e.g. decision tree, checklist, risk assessment, or expert evaluation) must be fully documented. This documentation must be provided to A1 in written form upon request.

11 DEPROVISIONING & DATA DELETION

ISO27001 **TPE-STD-GRP-DDD-001** At the end of the contract all A1-relevant data (in consideration of other contractual obligations with A1 and the requirements laid out in control TPE-STD-GRP-DDD-002) must be handed over from the supplier to A1. The handover must be in a common format that is readable by A1.

TPE-STD-GRP-DDD-002 The supplier must ensure that A1 data (if no longer needed to fulfill contractual obligations and the handover obligation from control TPE-STD-GRP-DDD-001 has been met) is deleted. This can be achieved by overwriting the data multiple times, destroying cryptographic keys, or certified destruction of the data carriers. Proof of data deletion carried out must be provided to A1 upon request.

12 PHYSICAL SECURITY

ISO27001 **TPE-STD-GRP-PHS-001** The supplier must take adequate measures to monitor physical access to its office premises and service/operations rooms. These measures must be documented and provided to A1 upon request.

ISO27001 **TPE-STD-GRP-PHS-002** The supplier must ensure that systems and infrastructure processing A1 data are located in access-controlled areas.

ISO27001 **TPE-STD-GRP-PHS-003** The supplier must ensure that all supporting utilities (e.g. power supply) are redundant, if they serve the maintenance and operation of A1-relevant systems.

TPE-STD-GRP-PHS-004 The locations of the computer systems, where A1 data is being processed by the supplier and/or its subcontractors ("4th parties"), must be disclosed to A1 upon request.

13 CONTINUITY MANAGEMENT

ISO27001 **TPE-STD-GRP-COM-001** The supplier must create, regularly evaluate, and test emergency plans for A1-relevant systems. These emergency/disaster recovery plans must be documented and provided to A1 upon request.

ISO27001 **TPE-STD-GRP-COM-002** The supplier must create, regularly evaluate, and test crisis management as well as disaster recovery plans. Upon request, evidence of such crisis management and disaster recovery plans must be provided to A1.

ISO27001 **TPE-STD-GRP-COM-003** The supplier must ensure that the scope of his emergency/disaster recovery plans encompass all locations, personnel, infrastructure and (information) systems used to provide the contractual services to A1.

TPE-STD-GRP-COM-004 The supplier must provide all necessary documentation regarding products or services to enable the creation of A1-internal business continuity plans.

14 APPENDICES

14.1 APPENDIX A – LIST OF TERMS

TERM	DEFINITION
CVSS	The "Common Vulnerability Scoring System" (CVSS) is a free and public system for assessing the severity of computer security vulnerabilities. It provides a numerical rating which helps in understanding and prioritizing the urgency and risk of security vulnerabilities. For more information on CVSS, please see: CVSS v4.0 Specification Document (first.org).
CIS Benchmarks	These benchmarks are a set of best practice guidelines and configuration recommendations developed by the "Center for Internet Security" (CIS). They provide detailed, consensus-based configurations for a wide range of technologies, including operating systems, cloud services, and network devices. By adhering to CIS Benchmarks, organizations can improve their security posture, ensure compliance with regulatory requirements, and reduce the risk of security breaches. You can find additional information here: CIS-Benchmarks.
Data Processing	According to Article 4 lit. 2 of the General Data Protection Regulation (GDPR), processing of (personal) data means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of data. This definition will also be used going forward in this document.
"Need to Know" principle	This principle restricts the sharing of information to individuals who require it to perform their specific job functions. Access to sensitive information is granted only to those whose roles and responsibilities necessitate it, ensuring that information is protected and only disclosed to authorized personnel.
"Least Privilege" principle	This principle ensures that individuals are granted the minimum levels of access—or permissions—needed to perform their job functions. It aims to reduce the risk of misuse or unauthorized access by only providing access to the information and resources that are absolutely necessary for an individual's role.
"Segregation of Duties" principle	This principle involves dividing responsibilities and tasks among different individuals or departments to reduce the risk of fraud, error, or unauthorized actions. In the context of information security, it ensures that no single person has control over all aspects of any critical process, minimizing the risk of misuse of information and enhancing checks and balances within the system.

14.2 APPENDIX B – ISO MAPPING TABLE

Chapter and control number	**ISO 27002:2022**	
	Covered with an existing ISO certification	A1-specific requirement with reference to the relevant ISO-chapter
2. General Security Requirements		
TPE-STD-GRP-GSR-001	5.1	
TPE-STD-GRP-GSR-002	5.29, 5.30	
TPE-STD-GRP-GSR-003	5.2, 5.19, 5.20, 5.29, 5.30	
TPE-STD-GRP-GSR-004	5.12, 5.13	
TPE-STD-GRP-GSR-005		5.22
TPE-STD-GRP-GSR-006		
TPE-STD-GRP-GSR-007	5.1, 5.2, 5.3, 5.8, 8.9 (ISO 27001:2022: 9.2)	
TPE-STD-GRP-GSR-008		8.34
TPE-STD-GRP-GSR-009	6.1	
TPE-STD-GRP-GSR-010	5.20, 5.21, 6.3	

TPE-STD-GRP-GSR-011	5.16, 5.17	
TPE-STD-GRP-GSR-012		5.15, 5.19, 5.20
TPE-STD-GRP-GSR-013	8.2	
TPE-STD-GRP-GSR-014		5.18, 5.22
TPE-STD-GRP-GSR-015		5.11, 5.15, 5.18, 5.26, 6.5
TPE-STD-GRP-GSR-016	5.20, 5.21	
TPE-STD-GRP-GSR-017	8.2, 8.22	
TPE-STD-GRP-GSR-018	8.2, 8.3	
TPE-STD-GRP-GSR-019		5.2, 5.18, 8.2, 8.3
TPE-STD-GRP-GSR-020	6.3, 8.7	
TPE-STD-GRP-GSR-021	8.1, 8.7	
TPE-STD-GRP-GSR-022	8.20, 8.21, 8.22, 8.23	
TPE-STD-GRP-GSR-023		8.6, 8.14, 8.16, 8.20, 8.21
TPE-STD-GRP-GSR-024		7.13
2.1 Users with privileged access rights		
TPE-STD-GRP-GSR-025	6.3, 8.7	
TPE-STD-GRP-GSR-026	5.22, 8.2	
TPE-STD-GRP-GSR-027		8.2
3. Incident Management		
TPE-STD-GRP-INC-001	5.24	
TPE-STD-GRP-INC-002		5.15, 5.18, 5.26
TPE-STD-GRP-INC-003		5.19, 5.20
TPE-STD-GRP-INC-004		5.19, 5.20, 5.21, 5.22, 8.15
TPE-STD-GRP-INC-005		5.35, 8.34
TPE-STD-GRP-INC-006	5.19, 5.20, 5.21, 5.22, 5.24, 5.25, 5.26, 5.27, 5.29, 5.30, 5.31, 5.33, 8.13, 8.14	
4. Reporting		
TPE-STD-GRP-REP-001		5.21, 5.22, 5.23, 5.24, 5.26, 5.28, 6.8
5. Software Architecture & Vulnerability Management		
TPE-STD-GRP-SAV-001	7.13, 8.8, 8.30	
TPE-STD-GRP-SAV-002	8.8	
TPE-STD-GRP-SAV-003		8.28, 8.29, 8.30
TPE-STD-GRP-SAV-004		5.19, 5.20, 5.21, 5.22, 8.8
TPE-STD-GRP-SAV-005		8.8, (8.30)
TPE-STD-GRP-SAV-006		None
TPE-STD-GRP-SAV-007		5.36, 8.9, 8.16, 8.20, 8.26
TPE-STD-GRP-SAV-008	8.25, 8.27, 8.28	
TPE-STD-GRP-SAV-009		8.25, 8.27, 8.28
TPE-STD-GRP-SAV-010	5.23, 8.21, 8.22, 8.27	
TPE-STD-GRP-SAV-011	8.22, 8.31	
TPE-STD-GRP-SAV-012		8.11
6. Encryption		
TPE-STD-GRP-ENC-001	8.24	
TPE-STD-GRP-ENC-002	8.24	
TPE-STD-GRP-ENC-003	5.33, 8.24	
TPE-STD-GRP-ENC-004	8.24, 8.27	
TPE-STD-GRP-ENC-005		8.24, 8.27
TPE-STD-GRP-ENC-006	5.14, 5.19, 5.20, 5.21	
TPE-STD-GRP-ENC-007		8.24, 8.27
7. Authentication & Authorization Management		
TPE-STD-GRP-AAM-001		5.15, 5.16, 5.17, 5.18, 8.5
TPE-STD-GRP-AAM-002		5.17,8.5, 8.24, 8.27
TPE-STD-GRP-AAM-003		8.5, 8.24, 8.27

TPE-STD-GRP-AAM-004		5.17 5.26, 8.5, 8.27
TPE-STD-GRP-AAM-005		8.5
TPE-STD-GRP-AAM-006		8.5
8. Cloud or other online services		
TPE-STD-GRP-COS-001	5.30, 8.14	
TPE-STD-GRP-COS-002	5.9, 8.9	
TPE-STD-GRP-COS-003	8.15, 8.16	
9. 4th Parties, Sub-Suppliers and Sub-Contractors		
TPE-STD-GRP-SSC-001	5.19, 5.20, 5.21	
TPE-STD-GRP-SSC-002		5.19, 5.20, 5.22
TPE-STD-GRP-SSC-003		5.20, 5.21, 5.22
TPE-STD-GRP-SSC-004		5.10, 5.19, 5.20, 5.21, 5.29, 5.30
10. AI Systems and Components		
TPE-STD-GRP-ASC-001		5.31
11. Deprovisioning & Data Deletion		
TPE-STD-GRP-DDD-001	5.11, 5.23	
TPE-STD-GRP-DDD-002		5.11, 5.23, 8.24
12. Physical Security		
TPE-STD-GRP-PHS-001	5.15, 5.18, 7.2, 7.3, 7.4	
TPE-STD-GRP-PHS-002	5.15, 5.18, 7.2, 7.3, 7.8	
TPE-STD-GRP-PHS-003	7.11, 8.14	
TPE-STD-GRP-PHS-004		7.9
13. Continuity Management		
TPE-STD-GRP-COM-001	5.29, 5.30	
TPE-STD-GRP-COM-002	5.29, 5.30	
TPE-STD-GRP-COM-003	5.24, 5.25, 5.26, 5.28, 5.29, 5.30	
TPE-STD-GRP-COM-004		5.30

15 REVISION AND UPDATES

15.1 REVISION HISTORY

Version	Date	Created by	Description of changes
1.0	01.12.2025	Group Risk & Resilience	- Initial release