



A1 Minimum Security Standard for 3rd parties

Version 1.1

Standard for the
A1 Information Security Management System



Content

1. Scope & General Objective.....	3
2. A1 Supplier Risk Management	3
3. Definitions.....	4
4. General Security Requirements.....	6
5. Vulnerability & Incident Management.....	6
6. Network Security.....	7
7. Software Architecture	8
8. Encryption.....	8
9. Authentication and Authorization Management	9
10. Reporting	10
11. Malware Protection and Response Capabilities.....	11
12. Physical Security.....	11
13. Deprovisioning & Data Deletion.....	11
14. Continuity Management.....	11
15. Cloud or other online Services	11
16. Content Responsibility	12
17. Version History.....	12
18. Annex A: Mapping to ISO 27001:2022 controls	13



1. Scope & General Objective

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 or individuals that provide goods or services to A1. This includes both physical goods and (digital) services and software solutions. This also includes strategic partners, consultants, and other third parties that have access to A1's information systems or data.

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

An external company's suppliers (hereinafter also referred to as '4th parties', sub-suppliers, subcontractors, suppliers of suppliers) must contractually adhere to the listed requirements. These requirements must not be weaker, lesser, or otherwise less stringent than those stated in this standard.

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

A1 expects all suppliers to fully comply with these security requirements, thereby contributing to the security of the shared business relationships.

2. A1 Supplier Risk Management

The A1 supplier risk management ensures that all suppliers, especially those A1 classifies as particularly security-relevant, meet the high internal security standards of A1 as well as external regulatory requirements (e.g. Network and Information Security Act 'NISG', Telecommunications Network Security Regulation 'TK-NSiV'). In the follow section, the most critical aspects and expectations of A1 suppliers are explained:

Compliance with Security Requirements

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

Notification of Deviations

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



Risk Mitigation

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 security-relevant (e.g. because their products and/or services contribute to Sarbanes-Oxley Act 'SOX', Digital Operational Resilience Act 'DORA' or NIS-relevant services) are available at least once every 36 months for a personal interview to evaluate their security status. This expectation includes the provision of adequate resourcing to do so. This conversation is intended to assess the current security posture of the supplier and ensure they meet A1's requirements.

Through this proactive approach in supplier (risk) management, A1 is able to ensure that information security remains at the highest level and potential risks are identified as well as addressed early on.

3. Definitions

Several of the requirements listed contain elements like:

- **"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 \(first.org\)](https://first.org/cvss-v4.0-specification-document).
- **"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](https://www.cisecurity.org/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.



4. General Security Requirements

- ISO27001** 1. The supplier must carry out changes to systems or infrastructure that process A1 data in accordance with a documented IT change process.
2. The supplier must, if necessary, undergo an audit by A1 (or by a party accepted by A1) after adequate prior notice.
3. The supplier must ensure that the service provision is subject to a defined approach for service management (e.g. COBIT, ITIL, ISO 20000).
- ISO27001** 4. The supplier must ensure that measures are taken to verify the trustworthiness of its employees (e.g. through background checks or criminal record checks).
5. 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.

5. Vulnerability & Incident Management

- ISO27001** 1. Security updates/patches must be provided by the manufacturer for the offered software.
2. The supplier must not charge for the rectification of security vulnerabilities in the products and services during the term of the maintenance contract.
- ISO27001** 3. 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 the General Data Protection Regulation (GDPR).
4. Vulnerabilities must be addressed according to the following table (starting from the identification of the vulnerability in the system): LOW 90 days, MEDIUM 60 days, HIGH 30 days, CRITICAL 15 days. The classification is based on the assessment according to CVSS v4 (if categorization according to CVSS v4 is not available, earlier versions must be used, e.g. CVSS v3, CVSS v2).
5. The supplier must harden systems and infrastructure that process A1 data according to accepted methods of hardening (such as the CIS Benchmarks). Upon request from A1, evidence of the methods used, and the degree of implementation, must be provided.



6. 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.
7. The supplier is obligated to assist in the investigation and determination of security-related incidents and must ensure that security-relevant log information (admin and user behavior, relevant copying processes, etc.) of the infrastructure processing A1 data exists for a period of at least 18 months and is provided to A1 if requested (e.g. for forensic analysis).
- ISO27001** 8. The supplier must perform regular data backups on systems and infrastructure processing A1 data in accordance with the requirements outlined in relevant contractual documents such as Service Level Agreements (SLAs) and demonstrably test their recoverability. Upon request from A1, evidence of the completion of these tests must be provided.
- ISO27001** 9. 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 as well as machine readable manner (log files). An integration into A1's SIEM must be supported by the supplier.
- ISO27001** 10. The supplier must ensure that an emergency management plan for systems and infrastructure processing A1 data is planned, documented, and implemented.
11. The supplier must ensure penetration testing is performed over systems and infrastructure processing A1 data at least every 18 months. Measures are to be derived and implemented for any identified vulnerabilities. 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 be penetration tested by A1 or a party (agreed between all parties) on behalf of A1.

6. Network Security

1. 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.
- ISO27001** 2. 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.
- ISO27001** 3. The supplier must group their networks, information systems, and users in a way that implements the "Least Privilege" principle.
4. The supplier must, for systems and infrastructure processing A1 data and being accessible to 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.

- ISO27001** 5. 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.

7. Software Architecture

- ISO27001** 1. The supplier must implement adequate 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** 2. 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.

3. 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** 4. The supplier must ensure that a separation between pre-production and production systems is implemented.

5. 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.

- ISO27001** 6. 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 principle of "need to know" (individuals with access rights have a legitimate business need), and
- the principle of "Segregation of Duties"

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

7. The supplier must implement measures (e.g. static/dynamic source code analyses) for detecting software vulnerabilities in source code during software development. These measures must be documented and provided to A1 upon request.

8. Encryption

- ISO27001** 1. The data transfer between the supplier's infrastructure or systems and A1's infrastructure or systems must be encrypted.



- ISO27001** 2. A1 data being stored on supplier's infrastructure or systems must be encrypted.
- ISO27001** 3. The supplier must ensure that cryptographic keys are generated, stored, and archived in a secure environment.
4. 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).
- ISO27001** 5. 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).
6. The supplier must agree with its suppliers ("4th parties") that the data transfer between the supplier and those suppliers ("4th parties") is encrypted.
7. 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.

9. Authentication and Authorization Management

1. Authentication to the supplier's system via an A1-provided Single Sign-On solution (SSO, e.g. Active Directory Federation Services - ADFS) must be technically possible for a user count of 50 or more.
2. If the supplier's solution requires local user accounts, A1 must be able to manage them independently (create, delete, lock, modify).
3. The supplier must ensure user rights and roles can be assigned/revoked on their systems and infrastructure where A1 data is processed. With this information, A1 must be able to perform regular checks and make changes to user rights and -roles.
4. If the supplier's solution requires local user accounts, the following requirements for secure passwords must be met:
 - Require a length of at least 15 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, and
 - storage and transmission of passwords in plain text are not permitted.
5. Biometric authentication:



- In biometric authentication, the authentication data may only be stored locally and securely on the respective device and must not be readable with standard rights (e.g., from the hard drive).
 - For facial recognition methods, criteria such as three-dimensionality or temperature must also be examined.
 - For fingerprint scanning methods, criteria such as finger pulse or temperature must also be examined.
 - The false acceptance rate (unauthorized users are authorized) must be at most 1 in 50,000.
 - The false rejection rate (authorized user is not authorized) must be within an acceptable range.
 - In case of a false rejection, alternative authentication via password protection according to the above specifications must be possible.
6. 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.
7. 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.
8. The supplier must ensure that, for a personal account, after initial login using the initial password, a password change is immediately enforced, and, if necessary (e.g. after an incident), it is possible to change the login information.
9. 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.

10. Reporting

1. A quarterly reporting by the supplier to the service responsible within 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.



11. Malware Protection and Response Capabilities

- ISO27001** 1. An endpoint security solution (e.g. antivirus software) must be in place to continuously scan systems and files for malicious software (e.g., ransomware, malware). The endpoint security solution must be regularly updated and provide real-time monitoring and response capabilities. Identified malicious software must be removed immediately.

12. Physical Security

- ISO27001** 1. 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** 2. The supplier must ensure that systems and infrastructure processing A1 data are located in access-controlled areas.

13. Deprovisioning & Data Deletion

- ISO27001** 1. 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 12.2) must be handed over from the supplier to A1. The handover must be in a common format that is readable by A1.
2. The supplier must ensure that A1 data (if no longer needed to fulfill contractual obligations and the handover obligation from control 12.1 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.

14. Continuity Management

1. The supplier must create, regularly evaluate, and test emergency plans for A1-relevant systems. These emergency plans must be documented and provided to A1 upon request.

15. Cloud or other online Services

- ISO27001** 1. The supplier must ensure that cloud or other online services are operated redundantly at a minimum of 2 data center locations.
- ISO27001** 2. The supplier must ensure that all A1-relevant components of its cloud or other online services are integrated into a central configuration management system.



16. Content Responsibility

The content was created by:
A1 OneSEC (Austria)
Security@A1.at

17. Version History

„ A1 Minimum Security Requirements for 3rd parties“ - version 1.1

Changelog:

- Rectified error in enumeration scheme (5.9; 5.10; 5.11; 9.8; 9.9).

„ A1 Minimum Security Requirements for 3rd parties“ - version 1.0

Changelog:

- Creation of document by complete revision/consolidation of the document "A1 Standard for Secure Service Operation".

18. Annex A: Mapping to ISO 27001:2022 controls

Chapter and control number	ISO 27001:2022	
	Covered with an existing ISO certification	A1-specific requirement with reference to the relevant ISO-chapter
4. General Security Requirements		
4.1	8.32	
4.2		8.34
4.3		5.22
4.4	6.1	
4.5		7.9
5. Vulnerability & Incident Management		
5.1	7.13, 8.8, 8.30	
5.2		None
5.3	5.24	
5.4		8.8, (8.30)
5.5		5.36, 8.9, 8.16, 8.20, 8.26
5.6		5.19, 5.20, 5.21, 5.22, 8.8
5.7		5.19, 5.20, 5.21, 5.22, 8.15
5.8	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	
5.9	8.15, 8.16	
5.10	5.24, 5.25, 5.26, 5.27, 5.28, 5.30	
5.11		5.35, 8.34
6. Network Security		
6.1		7.13
6.2	8.20, 8.21, 8.22, 8.23	
6.3	8.2, 8.22	
6.4		8.6, 8.14, 8.16, 8.20, 8.21
6.5	7.11, 8.14	
7. Software Architecture		
7.1	5.23, 8.21, 8.22, 8.27	
7.2	8.25, 8.27, 8.28	
7.3		8.25, 8.27, 8.28
7.4	8.22, 8.31	
7.5		8.11
7.6	8.2, 8.3	
7.7		8.28, 8.29, 8.30
8. Encryption		
8.1	8.24	
8.2	8.24	
8.3	5.33, 8.24	
8.4		8.24
8.5	5.14, 5.19, 5.20, 5.21, 8.20, 8.24	
8.6		8.24, 8.27



9. Authentication and Authorization Management		
9.1		8.5
9.2		5.15, 5.16, 5.17, 5.18, 8.5
9.3		5.2, 5.18, 8.2, 8.3
9.4		5.17, 8.5, 8.24, 8.27
9.5		8.1, 8.5
9.6		8.5
9.7		8.5, 8.24, 8.27
9.8		5.17, 5.26, 8.5, 8.27
9.9		8.5
10. Reporting		
10.1		5.21, 5.24, 5.26, 5.28, 6.8
11. Malware Protection and Response Capabilities		
11.1	8.1, 8.7	
12. Physical Security		
12.1	5.15, 5.18, 7.2, 7.3, 7.4	
12.2	5.15, 5.18, 7.2, 7.3, 7.8	
13. Deprovisioning & Data Deletion		
13.1	5.11, 5.23	
13.2		5.11, 5.23, 8.24
14. Continuity Management		
14.1		5.24, 5.25, 5.29, 5.30
15. Cloud or other online Services		
15.1	5.30, 8.14	
15.2	5.9, 8.9	