



# **A1 Security Governance**

## **Standard**

### **for secure service operation**

---

Standard for the  
A1 Information Security Management System

---

**For A1 employees:**

The protection requirement is calculated from the service class and the confidentiality class and can be seen in the SIAM.

The need for protection is automatically increased to at least **Extended** as soon as the processing of **personal data** of EU citizens takes place on systems outside the scope of EU Regulation 2016/679 (GDPR). This **does not** apply to the processing of login data.

The following information is considered to be registration data, in each case individually:

- e-mail address
- First name and/or surname
- IP address

**For A1 suppliers:**

It is the supplier's responsibility to provide written information on the protection needs identified by A1. The supplier agrees to be available for a safety review meeting with an A1 employee every 36 months.

The security requirements to be met for the defined protection needs are set out in the following table:

Protection Requirements Requirement	Chapter 2.1	Chapter 2.2	Chapter 2.3
Standard	X	-	-
Extended	X	X	-
High	X	X	X

# Table of contents

---

<b>1</b>	<b>Scope &amp; General Objective</b> .....	<b>4</b>
<b>2</b>	<b>Security</b> .....	<b>5</b>
<b>2.1</b>	<b>Safety requirements for the protection requirement class "Standard"</b> .....	<b>5</b>
2.1.1	Vulnerability & Incident Management .....	5
2.1.2	Network.....	6
2.1.3	Software architecture .....	6
2.1.4	Encryption .....	6
2.1.5	Authentication.....	6
2.1.6	Reporting .....	7
2.1.7	Malware Protection.....	7
<b>2.2</b>	<b>Safety requirements for the protection requirement class "Extended"</b> .....	<b>8</b>
2.2.1	Formal criteria.....	8
2.2.2	Vulnerability & Incident Management .....	9
2.2.3	Network Security.....	9
2.2.4	Secure Coding & Software Architecture.....	10
2.2.5	Encryption .....	10
2.2.6	Authentication.....	11
2.2.7	Physical Security.....	11
2.2.8	Authorization Management .....	11
2.2.9	Deprovisioning & Data Deletion.....	12
<b>2.3</b>	<b>Safety requirements for protection requirement class "High"</b> .....	<b>13</b>
2.3.1	External Hosting .....	13
2.3.2	Formal criteria.....	13
2.3.3	Vulnerability & Incident Management .....	13
2.3.4	Network.....	14
2.3.5	Secure Coding & Software Architecture.....	14
2.3.6	Encryption .....	14
2.3.7	Continuity Management .....	14
<b>3</b>	<b>Security Service Center Contacts</b> .....	<b>15</b>
<b>4</b>	<b>Publication &amp; Content Responsibility</b> .....	<b>15</b>
<b>5</b>	<b>Version history</b> .....	<b>16</b>

## Scope & General Objective

---

### 1 Scope & General Objective

This standard for the secure operation of services and service components is aimed at suppliers and partners of A1 (hereinafter also referred to as contractors, suppliers, providers, service providers, processors) as well as all employees of A1 who are entrusted with the operation, maintenance and decommissioning of ICT services.

These requirements apply both to services, applications and platforms operated within the A1 ICT infrastructure (on-premises) as well as to services, services, (cloud) applications and platforms operated outside the A1 ICT infrastructure.

For questions and advice, please contact the contacts listed in Chapter 3.

## 2 Security

In the following chapters, the requirements according to the protection requirements classes for applications and services that process A1 information / data are described.





The requirements defined on the following pages apply in accordance with the need for protection identified and documented by A1.

### 2.1 Safety requirements for the protection requirement class "Standard"

All services operated by or on behalf of A1 must meet the requirements of this protection requirement class "Standard" is fulfilled. Services with the Protection Requirement "Extended" and "High" are subject to additional provisions (see chap. Safety requirements for the protection requirement class "Extended" 2.2 from page 8 and for "High" 2.3 from page 13.).

#### 2.1.1 Vulnerability & Incident Management

- The software used must be supported.
- Vulnerabilities must be fixed according to the following table. Alternatively, a risk must be created in A1 Risk Management.

VULNERABILITIES	
Criticality	Patching Timelines
 LOW	6 months
 MEDIUM	3 months
 HIGH	1 month
 CRITICAL	2 calendar weeks

- No costs may be charged for the elimination of security vulnerabilities.
- Incidents and data breaches must be reported immediately to the responsible A1 Service Center, see Chapter 3.

# Security

---

## 2.1.2 Network

- Network Devices: Endpoints may only connect to the A1 network ("Client Zone") after successful authentication. The authentication of the devices is based on the current state of the art for LAN access. However, new devices in the internal A1 network must support IEEE 802.1X. Each device in A1's networks must be individually identifiable.
- IoT devices must not be directly accessible from the Internet. Security updates must be installed automatically over the entire life cycle and without manual intervention. No passwords must be hardcoded in the devices, standard passwords from the manufacturer must be changed during initial use.

## 2.1.3 Software architecture

- If multiple tenants are set up on the same service, a clean tenant separation from other customer data must be ensured.

## 2.1.4 Encryption

- Data communication between third-party ICT systems and A1 Austria's ICT systems must be encrypted.

## 2.1.5 Authentication

- Users (A1 Team Members) must authenticate themselves to an ICT service via SSO (Single Sign-On)(AD / Kerberos). If there are fewer than 50 users using the service or if SSO is not possible, the user administration is the responsibility of the responsible A1 team member.
- It must be possible for A1 to manage users (create, delete, block, change).
- Each created user must be listed in a central user directory and the selected authentication process must be documented by the A1 manager.
- **Password protection:** The passwords must not be identical to the A1 password if there is no connection to the A1 authentication system (ADFS) and must meet the A1 requirements for secure passwords:
  - At least 8 characters long (max. 256)
  - Meet 3 of these 4 criteria: uppercase letters, lowercase letters, numbers, special characters
  - Regular password changes must be technically supported.
  - Password storage and transmission in plain text is not permitted.

# Security

---

- **Biometric Authentication:**

- In the case of biometric authentication, the authentication data must only be stored locally and securely on the respective device and must not be readable with standard rights (e.g. from the hard drive).
- In the case of facial recognition methods, criteria such as three-dimensionality or temperature must also be checked.
- In the case of fingerprint scanning procedures, criteria such as finger pulse or temperature must also be checked.
- The false acceptance rate (unauthorized users are authorized) must be a maximum of 1 in 50,000.
- The false rejection rate (authorized user is not authorized) must be within an acceptable range.
- In order to be able to authenticate oneself in the event of a false rejection, it must alternatively be possible to protect one's password in accordance with the information above.

- **Alternative Authentication Methods:**

- Alternative authentication methods are allowed as long as they have an equal or higher level of protection compared to the methods specified above.

## 2.1.6 Reporting

At least quarterly, the provider must report on the services provided and send it to the A1 service recipient. This report must contain at least the following points (keymetrics):

- Availability of the system on a calendar monthly basis
- Incident Reaction Time
- Resolution Time Calendar Monthly
- Technical security measures implemented
- Vulnerabilities found by CVSS class
- Fixed vulnerabilities
- Vulnerability remediation times

## 2.1.7 Malware Protection

At the very least, antivirus software must be in use that continuously checks the systems and files for malware. The software needs to be updated continuously. Malware must be removed immediately.

## 2.2 Safety requirements for the protection requirement class "Extended"

In **addition** to the requirements for the protection requirement class "Standard" (see Chapter 2.1 on page 5), also the following requirements in this chapter apply for the protection class "Extended".

ICT service providers who store confidential A1 data (protection requirements from "Advanced") on their own infrastructure outside the A1 network (cloud providers, external hosting, XaaS) **must** have a valid ISO 27001 certification and maintain it for the entire period of cooperation with A1 for the services purchased from A1.

### 2.2.1 Formal criteria

- The computer locations where A1 data is stored and processed must be disclosed to A1.
- The data may only be made available to external A1 partners (processors) if a confidentiality agreement (NDA) and a data protection agreement (DPA, if personal data is processed) have been agreed and signed with A1. Such agreements must also be signed for prototyping, laboratory setups and POCs (Proof of Concept) if access to/on A1 real data is granted.
- All changes and implementations of A1 assets or applications used by A1 must be carried out according to a documented IT change-enabling process.
- Audit right: If necessary, the A1 supplier must agree be audited by A1 after a corresponding period of notice.



# Security

---

## 2.2.2 Vulnerability & Incident Management

- For essential facilities according to the NISG<sup>1</sup> and TKG<sup>2</sup>, the hardening requirements of the CIS benchmarks must be complied with.
- Vulnerability scans must be performed at regular intervals on the infrastructure used by the A1 service.
- Relevant log files for forensic analysis must be provided 18 months ago.
- All A1 on-premises services as well as PaaS & IaaS cloud services operated by A1 must be connected to an A1 SIEM system.
- Administrator and user behavior (log-on, log-off, password change, relevant copying, etc.) must be logged. The log files must be made available for forensic analysis if required.
- Regular data backups must be carried out and their recoverability tested. In addition, the availability requirements must be agreed upon and adhered to in a Service Level Agreement (SLA) with A1.

## 2.2.3 Network Security

- Security measures against network-based attacks (IPS, firewall) must be in place.
- The networks must be segmented within the network and information systems depending on the need for protection.
- Ownership of network segments must be clearly defined.
- Security within the network segments and the interfaces between the network segments must be ensured.
- Any network traffic that is not necessary for the systems to function must be prohibited.

---

<sup>1</sup> <https://www.nis.gv.at/>

<sup>2</sup> <https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20011678>

# Security

---

## 2.2.4 Secure Coding & Software Architecture

- Applications must be built in several tiers (layers) that must be securely separated from each other.
- No tier may be skipped during access.
- Access from one tier to the next may only take place via defined protocols (ports).
- There must be a separation into pre-productive and productive systems.
- The data on pre-production systems must be anonymized.
- Access to production systems containing real data must be limited to a reduced group of people with documented business needs, and the need-to-know principle as well as separation of duties for critical actions must be guaranteed.

## 2.2.5 Encryption

- Confidential and secret data must be transmitted in encrypted form.
- If the underlying ICT infrastructure is not managed by A1 (e.g. external hosting, cloud), confidential and secret data must be stored in encrypted form. For this purpose, encryption can be used at the file system, operating system, database or application level.
- Cryptographic keys must be generated, stored, and archived in a secure environment.
- State-of-the-art encryption must be used: AES (key length 128-256 bit), Camellia (128-256 bit), ECIES (>256 bit), DLIES (>3000 bit), RSA (>3000 bit)
- Obsolete methods must not be used: Triple-DES, Serpent, Twofish, DES, RC4, Blowfish
- Network communication with subcontractors and between computer locations must be encrypted.

# Security

---

## 2.2.6 Authentication

- Access to confidential or secret A1 data via unprotected networks (e.g. Internet, cloud services) or from third-party ICT infrastructure that is not managed by A1 (BYOD, the partner's ICT equipment) must be accessed via MFA authentication.

### **Password Protection:**

- Initial passwords must be randomly generated, transmitted in encrypted form, may only be used once and may only be valid for a maximum of 2 weeks.
- After the initial entry using the initial password, a password change must be forced immediately. If necessary, for example after an attack, it must be possible to change the credentials.
- After 15 failed login attempts, access must be blocked for at least 15 minutes or equivalent methods must be triggered to prevent unauthorized access.

## 2.2.7 Physical Security

- Physical access to office buildings and computer rooms must be monitored.
- The operation of data processing components must take place in access-protected rooms.

## 2.2.8 Authorization Management

- The regular review of roles and rights by the responsible A1 employee must be possible and take place at intervals of no more than 12 months.
- For authorization, the standard approval process of the A1 user management must be applied.
- The service provider must enable A1 to flexibly assign or revoke authorizations according to A1's internal requirements. A central listing or inspection and automatic evaluation of all authorizations must be enabled.

# Security

---

## 2.2.9 Deprovisioning & Data Deletion

- At the end of the contract, all existing data must be handed over to A1.
- Each supplier must securely delete the data when it is no longer required to fulfil its contractual obligations. This can be achieved by overwriting the data several times, by destroying cryptographic keys, or by certified destruction of the disks.

## 2.3 Safety requirements for protection requirement class "High"

In addition to the requirements of the Protection requirement classes "Standard" (page 5) and "Extended" (page 8), the following provisions in this chapter apply to services with a "High" protection requirement.

### 2.3.1 External Hosting

- Data / information classified as secret may only be stored outside the A1 on-premises ICT infrastructure (cloud, external hosting, etc.) with an explicit exemption from the A1 local CISO.

### 2.3.2 Formal criteria

- A defined process model for service management must be adhered to (e.g. COBIT, ITIL, ISO 20,000).
- Background checks on the personnel deployed (e.g. criminal record certificate) must be carried out.

### 2.3.3 Vulnerability & Incident Management

- All services must be connected to an A1 SIEM system.
- Emergency management must be planned, documented and set up.
- At least every 18 months, the supplier must carry out penetration tests to check the vulnerability. Measures must be derived and implemented from the weaknesses found.

# Security

---

## 2.3.4 Network

- A tool for automated denial-of-service (DoS) mitigation is used.
- All important supply components must be designed to be redundant.
- There must be site redundancy across at least 2 computer locations.
- All components must be integrated into a central management system.

## 2.3.5 Secure Coding & Software Architecture

- Static source code analysis must be performed to avoid security vulnerabilities.

## 2.3.6 Encryption

- The cryptographic keys used to encrypt stored data ("data-at-rest") must be under A1 control.
- It must be possible to carry out regular key changes with technical support. Processes for changing keys must be in place. It must be possible to order a change of keys.  
OR: The key is in A1 sovereignty and is generated at A1.

## 2.3.7 Continuity Management

- Contingency plans must be drawn up, applied, regularly evaluated and tested.

## Security Service Center Contacts

---

### 3 Security Service Center Contacts

In alphabetical order:

A1 Austria and A1 Group	<b>A1 Service Operation Center</b> T 0800 501 511 T +43 50 664 8 501 511 @ <a href="mailto:Attacke@A1.at">Attacke@A1.at</a>
A1 Belarus	@ <a href="mailto:cybersecurity@A1.by">cybersecurity@A1.by</a>
A1 Bulgaria	@ <a href="mailto:security@A1.bg">security@A1.bg</a>
A1 Digital	<b>A1 Digital - Information Security</b> @ <a href="mailto:security@A1.digital">security@A1.digital</a>
A1 Croatia	@ <a href="mailto:informationsystemssecurity@A1.hr">informationsystemssecurity@A1.hr</a>
A1 Macedonia	@ <a href="mailto:InfoSec@A1.mk">InfoSec@A1.mk</a>
A1 Serbia	@ <a href="mailto:security.alerts@A1.rs">security.alerts@A1.rs</a>
A1 Slovenia	@ <a href="mailto:security.slo@A1.si">security.slo@A1.si</a>

### 4 Publication & Content Responsibility

	Content created by: A1 OneSEC (Austria) <a href="mailto:Security@A1.at">Security@A1.at</a>
--	--

# Version history

---

## 5 Version history

Version 2.4		
	Creation	Approval
Name:	Friedrich HEIGL	Alexandra FEHRINGER
Date:	27.10.2023	03.11.2023
Valid from:	01.12.2023	
Changelog:	<ul style="list-style-type: none"><li>- <u>in general</u>: "IT" replaced by "ICT"</li><li>- <u>in general</u>: MUST requirements formulated more clearly</li><li>- <u>in general</u>: Removed checklist tables (previously: 2.1.6, 2.2.10, 2.3.8)</li><li>- <u>Chapter 2.1.1 Vulnerability &amp; Incident Management</u>: Vulnerability Management reformulated</li><li>- <u>Chapter 2.1.4 Encryption</u>: reworded, requirement for contact person deleted</li><li>- <u>Chapter 2.1.5 Authentication</u>: Password Requirements reformulated</li><li>- <u>Chapter 2.1.6 Reporting</u>: new chapter added</li><li>- <u>Chapter 2.1.7 Malware Protection</u>: New chapter added</li><li>- <u>Chapter 2.2.1 Formal criteria</u>: Text regarding changes shortened</li><li>- <u>Chapter 2.2.2 Vulnerability &amp; Incident Management</u>: CIS benchmarks added as a MUST for essential entities according to NISG and TKG; Retention period for log files specified as 18 months; Backup recoverability needs to be tested.</li><li>- <u>Chapter 2.2.3 Network Security</u>: Chapter reworded</li><li>- <u>Chapter 2.2.4 Secure Coding &amp; Software Architecture</u>: reformulated with regard to productive vs. pre-production systems</li><li>- <u>Chapter 2.2.6 Authentication</u>: 2FA replaced by MFA; Password protection: Requirement for inadmissible passwords removed</li><li>- <u>Chapter 2.2.9 Deprovisioning &amp; Data Deletion</u>: Text reworded</li><li>- <u>Chapter 2.3.2 Formal criteria</u>: Requirement for reporting deleted because it is now required in chapter 2.1.6</li><li>- <u>Chapter 2.3.3 Vulnerability &amp; Incident Management</u>: Requirement for backup recoverability deleted because already required in chapter 2.2.2</li><li>- <u>(former) Chapter 2.3.4 Authentication</u>: Chapter deleted</li><li>- <u>Chapter 2.3.5 Secure Coding &amp; Software Architecture</u>: Sentence regarding security as part of the development process deleted</li><li>- <u>Chapter 2.3.7 Continuity Management</u>: Chapter newly inserted</li></ul>	



## Version history

---

Version 2.3		
Concerns:	Creation	Approval
Name:	Friedrich HEIGL	Alexandra FEHRINGER
Date:	25.11.2022	02.05.2023
Valid from:	Release date	
Changelog:		
<ul style="list-style-type: none"><li>- TLP designation updated from "WHITE" to "CLEAR"</li><li>- Replaced parts of the text with more general wording (ADSV and Splunk)</li><li>- Changed "Offices" to "Office Building"</li><li>- Request "Contact person for security and cryptography" moved from protection requirement HIGH to STANDARD</li><li>- Chapter 2.2.8 Authorization management: Added information about the check interval,- Chapter 2.3.1 <u>External hosting</u>: "A1 CISO" changed to "A1 local CISO"</li><li>- General typo corrections</li><li>- Chapter <u>3.3 Security Service Center Contacts</u>: List of Security Service Centers of the A1 Group has been added.</li><li>- Removed references to local guidelines of A1-Austria or formulated them in a generally valid way.</li><li>- Protection need assessment shortened to page 2.</li><li>- Collection debt for suppliers with regard to A1 protection requirement classification entered.</li><li>- Removed protection requirement checkboxes</li><li>- Removed a reference to filing on the intranet, as it is not accessible to suppliers.</li><li>- Changed RFI contact from <a href="mailto:Security@A1.at">Security@A1.at</a> to the contact list in chapter 3.</li><li>- <u>Chapter 2.2.1 Formal criteria</u>: Removed reference to Greenlight.</li><li>- <u>Chapter 2.2.4 Secure Coding &amp; Software Architecture</u>: instead of reference to OWASP Top10, now more general wording</li></ul>		

Version 2.2		
Concerns:	Creation	Approval
Name:	Friedrich HEIGL Information Security	Alexandra FEHRINGER Information Security
Date	25.01.2022	25.01.2022
Valid from:	Release date	
Changelog:		
<p>Document history inserted Added notes regarding increase in protection requirements Corrected SOC phone number Corrected email addresses Chapter 2 deleted Chapter 2.1.6 added Chapter 2.2.10 added Chapter 2.3.8 added Table of Contents updated Note: There is no version history for previous versions of this document.</p>		

--- end of document ---