A1 Information Security Standard for secure service operation

Standard for the
A1 Information Security Management System

Determination of protection needs

For A1 employees:

The protection requirements determine the necessary security measures and must be documented below by an A1 employee. Information on determining the ***protection requirements level ("Standard", "Extended" or "High")*** *can be found in A1 Information Security Guidelines (Chapter 3 – Protection Needs Classification, access only for A1 employees), informationssicherheit@a1.at is happy to help.*

For A1 suppliers:

The security requirements that apply to you for the protection requirements level defined below can be found here: "Standard": from page 6 – "Extended": from page 8 – "High" – from page 12

A1 protection requirements:	☐ **Standard Protection**	➔ continuing on **page 6**
	☐ **Extended Protection**	➔ continuing on **page 8**
	☐ **High Protection**	➔ continuing on **page 12**

Aid to determine the protection requirements (for A1 employees):

- *Top 12 (vital) A1 services:* *High*
- *SOX services and secret information:* *High*
- *Confidential information:* *Extended*
- *Personal data:* *Extended*
- *Internal information & customer-relevant:* *Extended*
- *Internal information:* *Standard*
- *Public information:* *Standard*

Table of Contents

.

1 Scope & general objective

The trust of our customers and the protection of company values are absolutely key to our financial success. For this reason, A1 has set the objective of guaranteeing information security in accordance with the state of technology, identifying new developments and tendencies, evaluating these for their capacity for application and maintaining and continually improving the security level of A1 under the aspects of cost effectiveness and being practicability.

In addition to the A1 Information Security Policy[1], which is the guiding master document, and the A1 Information Security Guidelines[1], which reflect A1's framework for information security, this standard is intended for the operation of A1 services and service components. Whilst the Information Security Policy and Information Security Guidelines are only accessible to A1 employees, this document is intended explicity for external suppliers and partners.

The present standard for the operation of services and service components is addressed to suppliers and partners of A1 (hereinafter also referred to as contractors, providers, service providers, processors) as well as to all A1 employees involved in the planning, development, installation, configuration, operation, maintenance and decommissioning of IT services.The guidelines it contains must in particular be considered in the course of projects, within A1 change management and in the A1 procurement and purchasing process. These apply both to services and applications which are operated within the A1 IT infrastructure (on premises), as well as to services and (cloud) applications which are operated outside of the A1 IT infrastructure.

The present version of this standard replaces all previous versions. The latest version can be downloaded here[1].

For queries and advice, please contact Informationssicherheit@a1.at.

[1] http://www.a1team.at/sicherheitsrichtlinien (access only for A1 employees)

2 Protection Requirements Determination

The protection requirements level of an IT service or IT system results from the highest confidentiality level achieved by the processed information and from the service's required availability and is determined by an A1 employee using a matrix. Information concerning the determination of the protection requirements can be found here[2].

The determination of the actual protection requirements level ("Standard", "Extended" or "High") is made by a responsible A1 employee and is recorded on page 2 of this document. The requirements listed in the following pages for the respective protection requirements level documented on page 2 are deemed as agreed.

[2] A1 Information Security Guidelines (Chapter 3 – Protection Needs Classification, access only for A1 employees)

3 Security Requirements

The requirements in each protection level for applications and services that process A1 information are described in the following sections.

The following requirements apply according to the respective protection requirements level determined and documented on page 2.

3.1 Security Requirements for Protection Level "Standard"

All services operated by or for A1 must fulfil the requirements of the "**standard**" protection requirements level. Services that have "**extended**" or "**high**" protection requirements are governed by additional provisions (see Chapter Security Requirements for Protection Level "Extended"3.2 & 3.3 from page 8 and 12).

3.1.1 Vulnerability & incident management

- All used software / applications (servers, clients, databases, frameworks, libraries etc.) must be supported and must not have any known security vulnerabilities. Updates and security patches must be installed in a timely fashion. The removal of security vulnerabilities may not be charged.
- Security measures are used against malware (anti-virus, spam and trojan horse protection)
- Incidents and data breaches must be reported to the A1 Service Operations Centre (SOC) without undue delay:

A1 Service Operation Centre
T +43 50 664 42029
@ Attacke@A1.at

3.1.2 Network Security

- **Network devices:**
  End devices must not connect to the A1 network ("client zone") until successful authentication has taken place. The current state of the art for LAN access applies to the authentication of the devices. However, new devices in the internal A1 network must support IEEE 802.1X. Each device in the networks of A1 must be individually identifiable.
- IoT devices must not be directly accessible from the Internet. Security updates must be installed automatically and without manual intervention over the entire lifecycle. Passwords must not be hardcoded in the devices, and default passwords must be changed upon commissioning.

3.1.3 Software architecture

- Should multiple clients be set up on the same service, a clear separation of client to other customer data must be guaranteed.

3.1.4 Encryption

- Data communication between a supplier (and its IT services) and A1 must be encrypted via state-of-the-art secure communication channels (SSH, VPN, TLS, https etc.). SSL may no longer be used.

3.1.5 Authentication Methods

- Users (A1 employees) must authenticate themselves to an IT service (AD/Kerberos) using SSO (Single Sign-On). In the event that fewer than 50 users use a service or that implementing SSO is not possible, the responsibility for administration falls to the A1 application data protection officer. In any case, user administration must be possible by A1 (set up, delete, block, change). All users which are set up must also be listed in the A1 Corporate Directory (CD) and the selected course of the authentication must be documented in the A1 configuration database (CMDB) by the A1 responsible person.
- **Password protection:**
  Short and less complex passwords may not be technically permitted. Regular password changes are technically supported. Password storage and transmission is not permitted in plain text.
- **Biometric authentication:**
  - In case of biometric authentication, the authentication data may only be saved locally and securely on the respective device and cannot be read with standard rights (for example from the hard drive).
  - In facial recognition procedures, criteria such as three-dimensionality or temperature are also checked.
  - In case of finger print scanning procedures, criteria such as finger pulse or temperature are also checked.
  - The false acceptance rate for the biometric authentication procedures (unauthorised users are authorised) may not exceed 1 in 50,000.
  - The false rejection rate (authorised user is not authorised) is acceptable.
  - In order to still be able to authenticate oneself in the event of a false rejection (authorised user is not authorised), password protection must be possible as an alternative in accordance with the above specifications.
- **Alternative authentication methods:**
  Alternative authentication methods are permissible provided that they provide an equivalent or better protection level than the procedures cited above.

3.2 Security Requirements for Protection Level "Extended"

For the "**extended**" protection requirements level, the following provisions in this section apply **in addition** to the requirements for the "**standard**" protection requirements level (see Chapter 3.1 page 6).

IT service providers in this protection requirements level *should* be able to demonstrate a strong security awareness and *should* also have a valid **security certification** (e.g. ISO 27001) for the services provided by them. The A1 security check can be carried out in a reduced manner in this case and can therefore be accelerated. The long-term strategy of A1 is to deepen co-operation with such certified IT service providers and to intensify this.

IT service providers that save confidential A1 data on their own infrastructure for a long period of time (protection requirements level "extended" or above) (cloud providers, external hosting, Xaas) ***must*** be able to demonstrate such certification and ***must*** maintain this certification for the entire collaboration period for the services provided. Should such providers hold personal customer data to a large extent, data protection certification (for example ISO 27018) is required. Any used data centres ***must*** hold a relevant security certification.

3.2.1 Formal Criteria

- A1 must be informed of the location of the data centres at which data is stored and processed.
- The data may only then be made accessible to external A1 partners (order processors) if a non-disclosure agreement and a data protection agreement (DPA, should personal data be processed) have been agreed with A1 and signed. Such agreements must also be signed for prototyping, lab setups and POCs (proof of concept) if they involve entry or access to A1 real data.
- All changes to and implementations of A1 assets or applications used by A1 must be executed in accordance with a documented change process. Prior to commissioning, multiple tests should be carried out in the course of the A1 change management process. Amongst others, a comprehensive security check must be carried out. (This should be conducted under A1 Greenlight[3])
- **Right to audit:**
  The A1 supplier submits to an audit by A1 where necessary following prior notification.

3.2.2 Vulnerability & incident management

- The implemented components have a safe basic configuration (e.g. hardening).

[3] https://greenlight.a1.inside (access only for A1 employees)

- Vulnerability scans must be carried out at regular intervals on the infrastructure used by the A1 service.
- Relevant logfiles for forensic analyses must be available in a suitable form and must be made available.
- All A1 On-Premise services and all PaaS & IaaS Cloud services operated by A1 must be connected to the A1 On-Premise SIEM system (Splunk)[4]
- Administrator and user behaviour (log on, log off, password change, relevant copy events etc.) must be logged. The log files must be made available on demand for forensic analysis.
- Regular data backups must be carried out; furthermore, the availability requirements must be agreed with A1 in a Service Level Agreement (SLA) and must be observed.

3.2.3 Network Security

- Security measures must be used against network-based attacks (IPS, firewall).
- Network segmentation must be implemented (especially the separation of management network and userdata). The network must be divided into different segments aligned with protection requirements of the assets within.

3.2.4 Secure Coding & Software Architecture

- The software development process must follow secure development methods, e.g. by considering the OWASP Top10[5] (or API Security Top 10[6]) risks.
- Applications must be set up in several tiers, which must be safely separated from each other; no tier must be skipped during access. Access from one tier to the next can only be done via defined protocols (ports). There must be a separation into test, integration, and productive systems.
- Development- and test-environments may not contain any real personal data.
- Access to production-systems containing real data must be restricted to a limited number of people with a documented business need, and the need-to-know principle and separation of duties must be ensured for critical actions.

3.2.5 Encryption

- Data with extended protection requirements (e.g. confidential information) may only be transmitted in encrypted form.
- If the underlying IT infrastructure is not administered by A1 (e.g. external hosting, cloud), data with extended protection requirements (confidential A1 data, e.g. A1 customer data)

[4] See: https://getsplunk.at.inside (access only for A1 employees) Contact: .GRP.A1-TA.splunk.operation
[5] https://www.owasp.org/index.php/Top_10-2017_Top_10
[6] https://owasp.org/www-project-api-security/

must be stored in encrypted form. To this end, encryption may be applied 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 bits), Camellia (128-256 bits), ECIES (>250 bits), DLIES (>3000 bits), RSA (>3000 bits)
- Obsolete encryption algorithms may not be used: Triple-DES, Serpent, Twofish, DES, RC4, Blowfish
- Network communication to subcontractors and between datacenter locations is encrypted.

3.2.6 Authentication Methods

- Access to confidential A1 data via unprotected networks (e.g. Internet, cloud services) or third-party infrastructure not administered by A1 (BYOD, partner's IT equipment) must be protected by mandatory 2-factor authentication.
- **Password protection:**
  Initial passwords must be randomly generated, must be transmitted in encrypted form, may only be used once and must be valid for at most 2 weeks.
  A password change must be forced after the initial login. If needed, such as after an attack, it is possible to change the login information.
- Following 15 failed login attempts, access must be blocked for 15 minutes, or equivalent methods to prevent unauthorised access must be triggered.
- Passwords must be at least 14 characters long and include letters (upper case and lower case), at least one digit and at least one special character.
- It should not be possible to use the identifier or name of the user as the password, and words from dictionaries as well as simple number series (e.g. 1, 2, 3...) and birthdays or frequently used passwords (e.g. "password") must not be permitted.

3.2.7 Physical Security

- The physical access to offices and computer rooms / datacenters must be monitored.
- The operation of used data-processing components must take place in entry-protected spaces.

3.2.8 Authorisation management

- The A1 application data protection officer must be able to regularly review roles and rights.
- For the authorisation, the standard approval process of the A1 user administration must be used. The service provider must enable A1 to flexibly issue and revoke rights accordance to the internal A1 requirements A centralised listing or insight and an automatic evaluation of all privileges must be made possible.

3.2.9 Deprovisioning & Data Erasure

Security Requirements

- Secure deletion/deprovisioning must be possible; this can be achieved through repeated overwriting of the data, through the destruction of cryptographic keys or through the certified destruction of the storage medium. At the end of the contract, the handover of all existing data to A1 must be provided as an option. Each supplier must securely delete the data if it is no longer required in order to fulfil the contractual obligations.

3.3 Security Requirements for Protection Level "High"

For the "**high**" protection requirements level, the following provisions in this section apply **in addition** to the requirements for the "**standard**" (page 6) and "**extended**" protection requirements (page 8).

3.3.1 External hosting

- Information that is classified as secret may only be stored outside the A1 On-Premise infrastructure (e.g. cloud, external hosting etc.) following explicit and exceptional approval by A1's CISO (informationssicherheit@a1.at).

3.3.2 Formal Criteria

- A defined procedure model for service management must be adhered to (e.g. COBIT, ITIL, ISO 20000).
- There is a defined contact person for security and cryptography.
- Monthly reporting (availability) must be set up.
- Background checks on the appointed personnel (e.g. police certificate of good conduct, character reference) are carried out

3.3.3 Vulnerability & incident management

- All services must be connected to the A1 On-Premise SIEM system (Splunk)[4].
- Emergency management has been planned, documented and set up.
- Recovery tests must be regularly conducted for the data backups.
- Manual security checks (penetration tests) must be regularly conducted on the applications, databases and infrastructure that is used by the service.

3.3.4 Authentication

- Technical measures must be taken to prevent the following password variants: words in the dictionary, common passwords (e.g. admin/admin, admin/1234, root/root, password...), identifier or name of the user, passwords directly associated with the user (e.g. first name, last name, date of birth), repeating or sequential characters (e.g. Aaaaaaa1!, bBbbbbbb2, 3Cccccccc), simple digit series (e.g.: 1, 2, 3...), passwords from previous leaks or publications (e.g. Have I Been Pwned or Darkweb)

3.3.5 Network Security

- A tool for automated denial-of-service (DoS) mitigation must be used.
- All important supply components are designed redundantly.
- A location redundancy over at least 2 computer locations is implemented.
- All components are integrated into a central management system.

3.3.6 Secure Coding & Software Architecture

- Security is part of the software development process (changes, tests, scans, releases).
- Static source code analysis must be carried out to avoid vulnerabilities.

3.3.7 Encryption

- The cryptographic keys that are used for encryption of data-at-rest must be under control of A1.
- Regular encryption key changes can be carried out with technological support. Processes for changing encryption keys are in place. Encryption key changes can be ordered. OR: The key is in the sovereignty of A1 and is generated by A1.

4 Publication & responsibility for content

The content was created by:
A1 Information Security
Informationssicherheit@A1.at