A1 Information Security Standard for secure service operation

Standard for the
A1 Information Security Management System

Version history

Version 2.2		
Regarding:	**Creation**	**Approval**
Changes: - Document history inserted - Note on protection requirements inserted - Phone number of the SOC corrected - email addresses corrected - Chapter 2 - Deleted - Chapter 2.1.6 inserted - Chapter 2.2.10 inserted - Chapter 2.3.8 inserted - Table of contents updated	Friedrich HEIGL Information Security January 25th 2022	Alexandra Fehringer Head of Information Security January 25th 2022
Note: There is no version history for earlier versions of this document.		

Determination of Protection Requirements

For A1 employees:

The protection requirements determine the necessary security measures and must be documented at the end of this page by an A1 employee responsible for the service concerned. Information on determining the **protection requirements** ("standard", "extended" or "high") can be found in the A1 Information Security Guidelines (Chapter 3 – Protection Requirements Classification, access only for A1 employees), Security@A1.at is happy to help.

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

The following information applies as login data, in each case also individually:

- email address
- First name and/or last name
- IP address

For A1 suppliers:

The supplier agrees to be available for a safety review meeting with an A1 employee every 3 years.

You can see the applicable security requirements for the defined protection requirements on the basis of the following table:

Protection requirements	Chapter 3.1	Chapter 3.2	Chapter 3.3
Standard	x	-	-
Extended	x	x	-
High	x	x	x

Protection requirements established: ☐ Standard ☐ Extended ☐ High

Table of Contents

Gender clause

For readability purposes, gender-specific formulations are not used in this document. Insofar as personal designations are only written in the masculine form, they shall refer to both men and women in the same way.

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 explicitly 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. Contained guidelines must be taken into account in the course of projects, within A1 change management and the A1 procurement and purchasing process in particular.
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 Security@A1.at.

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

2 Security Requirements

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

The following requirements apply according to the respective protection requirements class determined and documented on page 3.

2.1 Security Requirements for the Protection Needs Class "Standard"

All services operated by or for A1 must fulfil the requirements of the "**standard**" protection needs class. Services that have "**extended**" or "**high**" protection requirements are governed by additional provisions (see Chapter Security requirements in relation to the Security Requirements for the Protection Needs Class "Extended" 2.2 from page 9 and for "High" 2.3 from Page 15).

2.1.1 Vulnerability & Incident Management

- The used software must be supported and must not have any known vulnerabilities. Updates and security patches must be installed in a timely fashion. The removal of security weaknesses may not be charged.
- Security measures are used against malware (anti-virus, spam and trojans)
- Incidents and data breaches must be reported to the A1 Service Operations Centre (SOC) without undue delay:

A1 Service Operation Centre
T 0800 501 511
@ Attacke@A1.at

2.1.2 Network Security

- **Network devices:**
  End devices may 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 may not be directly accessible from the Internet. Security updates must be installed automatically and without manual intervention over the entire lifecycle. Passwords may not be hardcoded in the devices, and default passwords must be changed upon commissioning.

2.1.3 Software Architecture

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

2.1.4 Encryption

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

2.1.5 Authentication Methods

- Users (A1 employees) must authenticate themselves using SSO (Single Sign-On) to an IT service (AD/Kerberos). In the event that fewer than 50 users use a service or that 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.

2.1.6 "Standard" Protection Requirements

The following list can be used to check the relevant criteria for 4 service categories with "**standard**" protection requirements.

	Question	SW supplier	HW supplier	Cloud service	Human supplier
1	Do you use a cloud service/storage?			X	
2	Is there a process for alerting if a data breach happens?	X	X	X	X
3	Do you know where the data are located?			X	
4	Do you have a NDA and DPA signed with a 3rd party?			X	X
5	Is the software supported by the vendor?	X		X	
6	Are security updates and security patches are installed or made available in a speedy manner?	X	X	X	
7	Are security measures in place against malware (anti-virus, spam and trojans protection)?	X	X	X	X
8	Is there awareness regarding handling incidents and data breaches?	X	X	X	X
9	Is there a guaranteed service time?	X	X	X	X
10	Is it possible to identify each individual device/user accessing via the A1 network?			X	X
11	Is there a clean seperation of client data.			X	X
12	Are secure (encrypted) protocols used for communication (e.g. Https, ftps, ssl)?	X	X	X	X
13	Are you using (A1) AD authentication			X	
14	Is Single-Sign On supported?	X		X	
15	Is multi-factor authentication supported and can it be enforced?	X		X	
16	Do password rules reflect the current the A1 Security Guidelines?	X	X	X	
17	Are passwords stored hashed?	X	X	X	
8	Does documentation covering the security concepts and measures exist?		X	X	X

2.2 Security requirements in relation to the Security Requirements for the Protection Needs Class "Extended"

For the "**extended**" protection requirements class, the following provisions in this section apply **in addition** to the requirements for the "**standard**" protection needs class (see Chapter 2.1 page 6).

IT service providers in this protection needs class *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 outside the A1 network for a long period of time (protection requirements class "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. Also, computer centres which are used **must** always hold a relevant security certification.

2.2.1 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[2])
- **Right to audit:**
  The A1 supplier submits to an audit by A1 where necessary following prior notification.

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

2.2.2 Vulnerability & Incident Management

- The implemented components have a safe basic configuration (e.g. hardening).
- 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)[3]
- 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.

2.2.3 Network Security

- Security measures must be used against network-based attacks (IPS, firewall).
- Network segmentation must be implemented (especially the separation of management network / user data). A categorisation into defined network protection areas, geared towards the protection requirements of the assets contained in them, must be set up.

2.2.4 Secure Coding & Software Architecture

- The software development process must follow secure development methods, e.g. by considering the OWASP Top10[4] (or API Security Top 10[5]) risks.
- Applications must be set up in several tiers (levels), 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 productive systems that contain the 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] See: https://getsplunk.at.inside (access only for A1 employees) Contact: .GRP.A1-TA.splunk.operation
[4] https://www.owasp.org/index.php/Top_10-2017_Top_10
[5] https://owasp.org/www-project-api-security/

2.2.5 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) 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 methods may not be used: Triple-DES, Serpent, Twofish, DES, RC4, Blowfish
- Network communication to subcontractors and between computer locations is encrypted.

2.2.6 Authentication Methods

- Access to confidential A1 data via unprotected networks (e.g. Internet, cloud services) or third-party IT 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 designation 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.

2.2.7 Physical Security

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

2.2.8 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 authorisations must be made possible.

2.2.9 Deprovisioning & Data Erasure

- 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.

2.2.10 Checklist for "Extended" Protection Requirements

In addition to the prerequisites for the protection requirements "**standard**" listed under 2.1ff, the following additional criteria apply for the protection requirements "**extended**":

Question		SW supplier	HW supplier	Cloud service	Human supplier
19	Is the documented change process for software development, testing, staging, deployments and maintenance implemented?	X		X	
20	Are there security checks in place before releasing a mayor software release?	X		X	
21	Are we (A1) allowed to test the used environment at the vendor?	X		X	
22	Are regular 3rd party security tests scheduled?	X		X	
23	Does the vendor hold a relevant security certification?	X		X	
24	Are the used data center(s) holding a relevant security certification?	X		X	
25	Have the used components been hardened?		X	X	
26	Are there vulnerability scans scheduled on a regular basis?	X	X	X	
27	Do we have access to the log files on request?			X	
28	Is the access to the log files available at least for 18 months?			X	
29	Are there regular backup and restore tests scheduled			X	
30	Are there recovery tests scheduled?			X	
31	Is it possible to split between data- and management network?			X	
32	Is there a segmentation between management and data network?			X	
33	Are there security measurements in place to protect the software/environment? (please specify in the comments field)	X	X	X	
34	Is there a process implemented for software releases?	X		X	
35	Are there secure coding methods in place?	X		X	
36	Are the applications structured in independent tiers?	X		X	

Security Requirements

	Question	SW supplier	HW supplier	Cloud service	Human supplier
37	Are there separated environments for development / quality&integration / production?	X		X	
38	Is software configured on a safe base?	X		X	
39	Are confidential data (e.g. personally identifiable information, passwords) transferred and stored encrypted by default?			X	X
40	Are the used certificates/cryptographic key stored securely?	X	X	X	
41	Is A1 holding the encryption keys?	X	X	X	
42	Is state-of-the-art encryption used?	X	X	X	
43	Is it possible to enforce regular password changes?	X	X	X	
44	Are passwords stored in plain text?	X	X	X	
45	Is a first-time access password change enforced?	X	X	X	
46	Is there access control for offices and server rooms?			X	
47	Are the used components in an access restricted room?			X	
48	Is there a process scheduled for review user/admin roles and rights?			X	
49	Is an automatic report about user/admin roles & rights available?			X	
50	Is a secure data erasure process in place?	X		X	
51	Is there an agreement on how A1 data will be archived at A1 at the end of service consumption?	X		X	
52	Are there retention policies in place?			X	

2.3 Security Requirements for the Protection Needs Class "High"

For the "high" protection needs class, the following provisions in this chapter apply **in addition** to the requirements for the "**standard**" (page 6) and
"**extended**" protection requirements (page 9).

2.3.1 External Hosting

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

2.3.2 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. criminal record certificate) are carried out.

2.3.3 Vulnerability & Incident Management

- All services must be connected to the A1 On-Premise SIEM system (Splunk)[3].
- Emergency management is 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, databanks and infrastructure used by the service.

2.3.4 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...), designation 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)

2.3.5 Network Security

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

2.3.6 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.

2.3.7 Encryption

- The cryptographic keys used to encrypt stored data ("data-at-rest") are under A1 control.
- Regular encryption key changes can be carried out with technical 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.

2.3.8 Checklist for "High" Protection Requirements

In addition to the prerequisites for the protection requirements "**standard**" listed under 2.1ff and the prerequisites for the protection requirements "**extended**" listed under 2.2ff, the following further criteria apply for the protection requirements "**high**".

	Question	SW supplier	HW supplier	Cloud service	Human supplier
53	Do you follow the standard service management process?	X	X	X	X
54	Is there a named contact for cryptography and security?	X		X	
55	Do you have monthly reporting?	X	X	X	X
56	Are people working in / administrating this environment been screened?	X		X	X
57	Is there performance monitoring in place?			X	
58	Have you connected the service with A1 SIEM?			X	
59	Do you have an emergency management established?			X	
60	Is the used environment geo-redundant?			X	
61	Is there a tool for automatic mitigating DDOS attacks?	X	X	X	
62	Is the service included in a central management.			X	
63	Will the encryption key be changed regularly?	X	X	X	

3 Publication & Responsibility for Content

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