Group Information Security Policy – Public Version

Table of content

Table of content 2

Introduction 3

Scope 4

Objectives 5

Priorities 6

Governance & organizational structure for Information Security 7

- Board responsibility 7
- Security committees 7
- CSO & CISO 8
- Security capabilities/organization 8

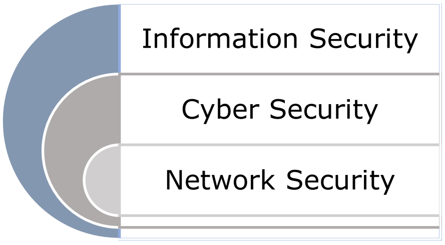
Security & Guiding Principles 9

Confidentiality Levels of Information 10

- Public 10
- Internal 10
- Confidential 10
- Secret 11

Introduction

Information Security is defined as the practice of enabling business in a secure way as well as preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction of data / information. It is a general term that can be used regardless of the form the data may take (e.g. electronic or physical). In the context of this policy, data and information are used interchangeably and refer to an asset worth protecting. For A1 information security is including the domains of cyber security[1] and network security[2]. The primary area of concern for the field of Information Security is the balanced protection of the confidentiality, integrity, and availability of data, while maintaining a focus on enablement of business, efficient policy implementation and no major hampering of organizational productivity.



This A1 Group Information Security Policy is the highest-ranking document in the A1 internal framework. It serves as a key component of A1 Groups overall Information Security strategy and management. It must be considered as the main document alongside more detailed "supporting documents", such as "Security Guidelines", or "Security Standards".

In principle, all technical structures of units within A1 Group are untrusted against each other. However, a unit ("trusting unit") may trust another unit ("trusted unit") if the following conditions are met:

- The trusted unit accepts at minimum the A1 Group Information Security Policy as well as all supporting documents of the trusting unit or it is assured by SLAs that equivalent or higher security measures are effective.
- The trusting unit controls and maintains the network as well as all connected devices of the trusted unit or the trusting unit is entitled to verify the compliance of the required Information Security measures in the trusted unit with a security control assessment.

[1] Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

[2] Network security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

Scope

This policy is applicable to all employees of A1 Group. This includes A1 Group, all operating companies (OpCos), subsidiaries, and connected entities as well as third parties who interact with information held by A1 Group and the corresponding information systems used to store and process it.

This includes, but is not limited to:

- Any systems attached to the A1 Groups data or telephone networks, including but not limited to
    - All systems managed by A1 Group's OpCos
    - Mobile devices used to connect to A1 Groups networks
    - Operational Technology (OT) and Internet-of-Things (IoT) devices
- Any data processed in A1 Group data/telephone networks, over which A1 Group holds the intellectual property rights or is the data controller or data processor, including but not limited to
    - Electronic communications sent to and from A1 Group's OpCos
    - Data stored on portable devices, portable storage media, OT and IoT devices
    - Data stored outside of A1 data or telephone networks (external hosting, Cloud etc.)
    - Data in analogue form (e.g. files, photographs, media, etc.)

Compliance with this A1 Group Information Security Policy is mandatory for the above mentioned.

A1 Group is obliged to abide all relevant legislation as well as the specific regulations valid in the country of a local unit. The requirement to comply with this legislation must be devolved to employees of A1 Group, who may be held personally accountable for any breaches of Information Security. The relevant duties must be further specified in more detailed "supporting documents", such as "Security Guidelines", or "Security Standards".

Objectives

A1 Group regards data & information as one of its most valuable business assets. An effective A1 Information Security governance to protect these information assets is essential to the long-term existence of A1 Group. By adopting a high standard of Information Security, A1 Group can conduct business and stay competitive.

The overall objective of A1 Information Security is to reduce the security risk to the A1 Group risk appetite which is formalized in the security framework.

The "A1 Group Code of Conduct (CoC)" sets out the principles and practices that are binding for all A1 employees to follow unreservedly both in letter and in spirit.

A1 Group adheres to the highest standards of Information Security. It is committed to treating customer information responsibly, thereby enabling digital trust from our customers. A1 Group maintains the confidentiality of any entrusted information, except when disclosure is authorized by the customer or required by applicable laws, rules or regulations. Information is shared internally with appropriate discretion.

Any security breach of A1 Groups information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems and will be handled in accordance with all relevant Information Security regulations.

The loss or breach of confidentiality of personal data can be an infringement of the General Data Protection Regulation and may result in criminal or civil action against A1 Group. Any noncompliance with Information Security objectives may result in the loss of business, financial penalties or criminal or civil action against A1 Group. Therefore, it is crucial that all employees of A1 Group adhere to the A1 Group Information Security Policy and the relevant framework.

The objectives of A1 Groups Information Security Policy therefore are to preserve:

- **Confidentiality** – Access to data and information assets must be confined to those with appropriate authority and not be disclosed to others. The decision process for employees to gain access to data must be based on the need-to-know and need-to-have principle, which means that access to covered data must be necessary for conducting the job function.
- **Integrity** – Data must be complete, intact and accurate. All systems, assets and networks need to operate correctly, according to specification. A modification of data must not be possible without having the required permissions. All changes to important data sets must be tracked at any given time.
- **Availability** – Data must be available and delivered to the right employee, customer, 3rd party or system at the time when it is needed.
- **Compliance** – All employees or 3rd parties must be aware of and comply with relevant internal or external specifications, policies, standards and/or laws.

Priorities

1. Secure critical infrastructure (NIS Scope) as state-of-the-art with highest priority
2. Protect legacy systems as secure as feasible
3. Use group synergies in leveraging available resources and know-how
4. Develop group security approach on new systems to leverage different locations and cost structures
5. Deliver group services where appropriate to be cost efficient

Governance & organizational structure for Information Security

Board responsibility

- The Group CEO is fully and finally functional accountable for the state of Information Security at A1 Group. While A1 Group Information Security Governance is located in the Group CEO domain, the operational execution and responsibility stays in the OpCos and entities.
- A local LT function must be appointed as accountable for the state of Information Security for the relevant entity.

Security committees

- A1 Group has a Group Security Committee. It consists of the Group CEO, Group CSO (Director Security), Group Director of Technology & Business Evolution, CEOs of each OpCo.

Committee	Members	Frequency	Deliverables
A1 Group Security Committee	• Group CEO • Group CSO • Group Director of Techr & Bus. Evolution • CEO of each OpCo • OpCo CISOs (per cluste on demand	• Bi-annually	• Security Report
	Topics (e.g.) • Approval of security strategy and related measures • Approval of significant security initiatives • Approval of the Group Information Security Management Policy and framework • Definition and review of group security risk appetite • Decision of the treatment and acceptance of significant security risks affecting Group • Creation and closing of relevant Group Security Services and contracts • Alignment of strategic and governance planning with regards to security • Definition of Group Security KPIs/KRIs		

- Local A1 units have a Local Security Committee. The structure of the Local Security Committee is derived from the Group Security Committee, based on OpCo roles in the organization. The Local Security Committee is accountable for controlling the implementation of Security Policies, Standards and Baselines in the corresponding local A1 Unit.

Committee	Members	Frequency	Deliverables
OpCo Security Committee	Based on the OpCo structure, recommended: • CEO • Risk responsible LT member • CSO/CISO • IT & Network & ICT directors	• Bi-annually	• Presentation incl. Security Report
	Topics (e.g.) • Approval of OpCo security strategy • Approval of significant security initiatives • Definition and review of OpCo security risk appetite • Decision of the treatment and acceptance of security risks affecting OpCo • Verification of the implementation of the Information Security Framework • Alignment of strategic and governance planning and initiatives with regards to security risks		

CSO & CISO

- A1 Group must have one G-CSO who is accountable for the governance of Information Security across A1 Group.
- Every OpCo[3] must have one local CISO (L-CISO). All CISO-functions must be reporting to a LT member.
- The respective L-CISO is accountable for the implementation of the Group security framework and responsible for the local security management. He/She must ensure that the different security domains are aligned and interacting (e.g. Physical Security, BCM)

Security capabilities/organization

- Every entity must have an adequate information security capability. For OpCos this must be a dedicated security organization (cluster organizations are possible), while small entities must have at least a nominated person to act, apart from his daily business, as the main contact point for security.
- All employees and externals hired by an OpCo, subsidiaries, and connected entities or the Group directly must comply with the Information Security framework including the maintenance of above-mentioned Information Security objectives.
- More information about the roles & responsibilities can be found in the relevant role descriptions

This A1 Group Information Security Policy will be maintained, reviewed, and updated by the Group Security Committee regularly.

[3] A CISO per OpCo cluster is possible

Security & Guiding Principles

Security as a business enabler

Security sees A1´s employees and management as internal customers whom we support to securely enable their business goals

Security by design

Security must be integrated into all business processes and life cycles as early as possible to be efficient and effective

Effectiveness and efficiency

We strive for effectiveness, then compliance and then efficiency in order to protect A1´s assets and capabilities

Risk-based Approach

We make risk-informed decisions based on high quality data

Automation

As a response to the ever-enlarging threat and attack surface we leverage and enforce automation wherever possible

Resilience

Moving away from only protecting certain assets, we shift our focus to ensuring our critical capabilities to enable resilient business processes

Business Need

Protected information may be accessed, stored, read, altered, or transferred if and only if there is a still valid business need. Access rights must be revoked as soon as businesses need for its existence vanishes.

Least Privileges

Accounts must be restricted to minimum access rights level in order to fulfil a business need

Segregation of Duties

This is the concept of having more than one person required to complete a task. Its primary objective is the prevention of fraud and errors. It also helps in reducing the potential damage from the actions of one person. Duties must be separated for:

a. Lawful inspection of personal data, traffic data, or communication.
b. Operational changes that might affect confidentiality, availability, or integrity of our critical systems.
c. Security checks that effect data of employees.

Confidentiality Levels of Information

All information is classified according to a defined level of confidentiality. The confidentiality level of documents (e.g. electronic formats of Word, Excel, PowerPoint, PDF as well as printouts) shall be labelled explicitly in or on the document itself. Publications, press communications and correspondence with customers are excluded from explicit labelling.

Admission to shares containing confidential information should be limited in accordance with the principles of "least privileges" and "business need". Each share shall have an owner who is responsible to grant and revoke access to the share.

The duty for classification of information has always the responsible owner (of a database) and/or the author of a report, contract or document, unless specified differently within a specific classification label. If there is no owner identified, the person who has the de-facto power of decisions for the contents has also the responsibility for classification, e.g. the manager and not the assistants creating a report is the owner of the report. The confidentiality level of data should be visible on every page of an item of information. In online applications, the confidentiality level should be visible at least on the start screen of the used application.The A1 Telekom Austria Group uses the following classification labels:

Public

All information that is classified "public" can be forwarded to internal and external recipients (e.g. published annual report, promotional material after the product launch). Only authorized employees (e.g. press contact people, executives, product marketing director) may classify information to be "public".

Internal

This is not public information, which is neither confidential nor secret and which may therefore be passed on to other staff members as needed. A publication of internal information is not permitted. Disclosure to external recipients is permitted if there is a business need for it.

All information without confidentiality label or with unclear classification shall be regarded as "internal" information.

Contents from our companies' Intranets have the confidentiality level "internal".

Confidential

If the disclosure of information to any unauthorized internal or external recipient can cause a damage to the company (e.g. confidential contracts, purchasing conditions, payroll lists), then it has to be classified as "confidential" by the creator of the information. Confidential information may be forwarded only in compliance with the "need to know" principle to the smallest possible group of recipients, unless that creator of the information has defined criteria for the dissemination of this information.

All business and operational secrets as well as all personal data other than those found in intranet shall be classified "confidential". These data can be transferred between companies of the Telekom Austria Group, if the business need is evident (e.g. reporting). All confidential data needs to be transferred encrypted.

Secret

Documents and data with the confidentiality level "secret" are the most sensitive ones. Decision about the classification of documents and information as "secret" is made centrally at board (management Level 0/1). (Examples: documents for frequency auction, M&A projects).

Secret information may be passed on only after receiving an explicit authorization from the data owner. Even managers and supervisors may not view "secret" data without the permission of the data owner. By this restrictive method of data distribution, the data owner keeps full control about the legitimate receivers of secret information. If the data owner decides to delete secret data, then he has to inform all authorized receivers who must personally confirm the fulfilment of the deletion order. All secret data needs to be transferred and stored encrypted.