Information Security Guidelines for System Developers

Valid from:	20.10.2006	Status:	Published
Revised:	01.03.2022	Version:	5.0
Issued by:	I/FL-81, Datenschutz- / Datensicherheitsmanagement, Office des DSB	Regulation No.	02.04

Scope

These guidelines extend to the AUDI AG and are to be applied throughout the whole Audi Group, if necessary with concrete IT regulations.

Table of Contents

I. Purpose

This information security guideline defines the organizational guidelines and rules for information security that must be followed by IT system developers (see appendix, A.3) in their area of responsibility for IT systems and IT infrastructure.

In addition, the Information Security Guideline for employees or third parties applies to the target group of IT system developers, provided that the IT system developer is an employee of a partner company. IT system developers must obtain information about all (role-specific) requirements and comply with them when working in additional roles.

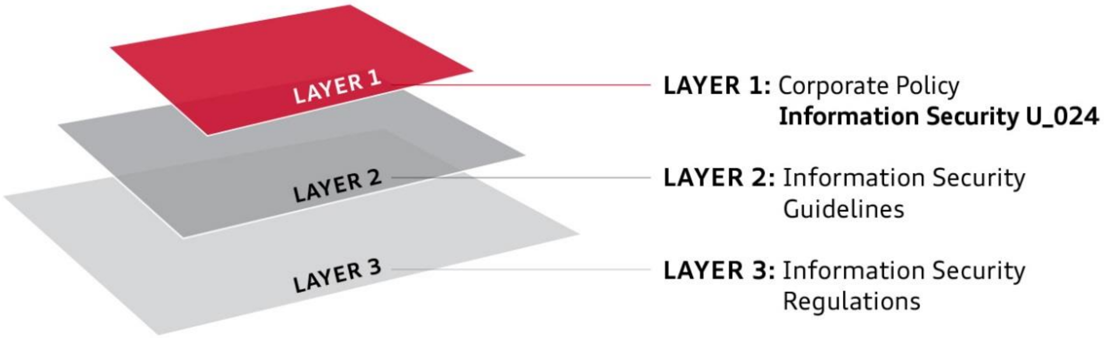
The purpose of this Information Security Guideline is to protect the confidentiality, integrity and availability of information as well as to safeguard the rights and interests of the company and all natural and legal persons who have a business relationship with a Group company and/or carry out activities for it.

This document's content follows the international standard ISO/IEC 27002:2013.

This document and all associated change and update notices are communicated through the usual distribution channels (see appendix B.1.1).

1. Context

The following overview shows how the Information Security Guidelines fit into the overall Information security regulation framework:


LAYER 1
LAYER 2
LAYER 3
LAYER 1: Corporate Policy
Information Security U_024
LAYER 2: Information Security Guidelines
LAYER 3: Information Security Regulations

Information Security Regulations

Level 1 Information Security U_024:
Defines the basic objectives, strategies and responsibilities to ensure a minimum level of information security.

Level 2 Information Security Guidelines:
Design of U_024 into organizational instructions for individual user groups

Level 3 Information Security Regulations:
Specification of regulatory requirements in the technical environment and description of technical functions and processes of information security

2. Asset management

The responsibility for information lies with the respective information owner. This also applies to information provided via IT systems. Responsibilities may be delegated.

3. Communications and operations management

Security-related activities (such as the management of cryptographic keys, the security infrastructure or security systems) may only be carried out by third parties after the responsible organizational unit has approved this (see appendix B.1.2). In doing so, the requirements of Regulation (see Appendix, A.1.1) must be followed.

The capacity requirements for an IT system must be specified during the planning phase.

The protection requirements for an IT system must also be specified in the planning phase together with the information owners.

IT system planning (functional specification, IT system design, IT system implementation) and IT system acceptance (IT system introduction) must be carried out in accordance with the Group-wide standards for IT system development (e.g. IT PEP).

Information provided via publicly accessible IT systems (e.g. via the Internet) must be protected against unauthorized access and changes by appropriate security measures (e.g. encrypted transmission of authentication information, integrity checks).

4. Access control

To access information, authentication and authorization mechanisms shall be put in place based on a risk assessment carried out by the information owner.

Appropriate measures must be taken to prevent the guessing of user IDs and passwords (e.g. extended waiting time between failed login attempts or access blocks after a certain number of failed login attempts).

Authentication requirements shall be implemented in accordance with the regulations (see appendix A.1.2). All authentication information (e.g. passwords or keys) must be classified as at least "confidential" and treated accordingly.

Authentication information must be protected from unauthorized access. Passwords must never be stored in plain text.

Dialog sessions that are no longer actively used after a long period of time must be deactivated or protected by appropriate means.

When communicating with or between IT systems that are classified as confidential or secret, mutual (bidirectional) authentication (e.g. TLS) must be used.

The processing of information must be determined jointly with the information owner. This expressly includes any use in IT systems or transfers between IT systems. The approval by the information owner must be documented.

5. Information systems acquisition, development and maintenance

5.1. Security requirements of information systems

Before an IT system is developed and used, all necessary information security measures must be identified and implemented (e.g. IT system hardening or patch management).

For IT systems (e.g. databases and backup media), the requirements for handling information also apply (see Information Security Guideline for Employees, section "Handling classified information").

5.1.1. Confidentiality

Information must be protected against unauthorised access in accordance with its classification. Depending on the classification in terms of confidentiality, the following security measures are required:

Classification	Definition
Public	• IT system hardening (only required services and current security patches)
Internal	• IT system hardening (only required services and current security patches) • Access control according to the principle "Need to know" • One-factor authentication (e.g. user ID and password)
Confidential	• IT system hardening (only required services and current security patches) • Access control according to the principle "Need to know" • Two-factor authentication (e.g. smart card and PIN) – especially for accessing applications – or additional protection mechanisms such as encrypted storage (e.g. encrypted data on file shares or encrypted USB drives) • Transport encryption
Secret	• IT system hardening (only required services and current security patches) • Access control according to the principle "Need to know" • Two-factor authentication (e.g. smart card and PIN), especially for accessing applications • Transport encryption • Data storage encryption

5.1.2. Integrity

Information shall be protected against undesirable changes and unauthorised manipulation in accordance with its classification. Depending on the classification in terms of integrity, the following security measures are required:

Classification	Definition
Low	• IT system hardening (only required services and current security patches)
Medium	• IT system hardening (only required services and current security patches) • Access control according to the principle "Need to know" • One-factor authentication (e.g. user ID and password) • Databases: Protection of referential integrity must be enabled.
High	• IT system hardening (only required services and current security patches) • Access control according to the principle "Need to know" • Validation of input and output data as well as control of internal

	processing for error reduction and avoidance of standard attacks such as "buffer overflows" or injection of executable code (e.g. control of restriction for fields, field restriction for special areas) • Creation of secure hash values for data • Verification of hash values before processing data
Very high	Additional to the requirements for „High“: • Two-factor authentication (e.g. smart card and PIN) for write access • Generation and verification of digital signatures for stored data or comparable security measures • Signing of hash values (secure storage of keys)

5.1.3. Availability

The availability of IT systems must be ensured according to the respective classification. Depending on the classification in terms of availability, the following security measures are required:

Classification	Definition
Low	• IT system hardening (only required services and current security patches) • Recovery measures in 72 hours or later. For this purpose, suitable measures must be implemented.
Medium	• IT system hardening (only required services and current security patches) • Recovery measures in 24 hours or a maximum of 72 hours (BIA-IT: levels 3 and 4). For this purpose, suitable measures must be implemented.
High	• IT system hardening (only required services and current security patches) • Recovery measures in 1 hour or a maximum of 24 hours (BIA-IT: level 2). For this purpose, suitable measures must be implemented.
Very high	• IT system hardening (only required services and current security patches) • Recovery measures in 1 hour (BIA-IT: level 1). For this purpose, suitable measures must be implemented.

5.2. Correct processing in applications

The security of IT systems must be ensured by implementing the measures from the Group-wide standards for IT system development (e.g. IT PEP).

For all consulting activities for the introduction of IT systems, the regulations and internal agreements of the respective Group company apply (see appendix B.1.3).

5.3. Cryptographic controls

Basic decisions on the strategy, use and handling of cryptographic methods must be determined by the responsible organizational units (see appendix B.1.4).

The requirements of the regulation (see appendix A.1.3) must be followed. Only the methods/procedures specified therein may be used.

5.4. Security of IT system files

5.4.1. Protection of IT system test data

Development environments, test environments and production environments (running IT systems) must be logically and physically separated from each other.

If possible, tests must be executed with generated test data (e.g. using a test data generator).

IT systems may only be tested in test environments that are specifically designed for this purpose. It must be ensured that the operation of productive IT systems is not impaired.

If, for testing purposes, individuals would have access to personal, confidential or secret data that they do not need to carry out their contractual activities, the data must be made so unrecognizable before the tests are carried out in such a way that the original data is not identifiable before it is transferred from the productive IT system to the test or development environment.

The copying or use of information from productive IT systems is only permitted with the prior consent of the information owner. Copied data is subject to the same information security requirements as the original data.

After testing has been carried out, information used for this purpose must be completely deleted from productive IT systems.

The access rights and roles applicable in a productive IT system must also be implemented in the test and development systems and assigned to the intended test persons when copies of the productive data are used.

5.4.2. Access control to program source code

Source code must be classified according to the data classification (see chapter 5.1) and protected accordingly.

5.5. Security in development and support processes

All procedures and processes that affect IT systems must be designed to achieve and maintain the desired information security level.

Formal change management procedures must be implemented. These must ensure that the IT system's security and monitoring procedures are not compromised by modifications.

If changes are made to software packages or their source code, their effects on existing regulations and security measures must be determined.

6. Compliance and compliance with legal obligations

When using encryption and/or electronic signatures, all country-specific regulations for the import and export of or access to hardware, software and information must be followed.

The license and usage rights of third parties in accordance with the applicable provisions (including contract law) must be observed and complied with during system development.

II. Responsibilities

In the case of matters requiring co-determination, the involvement of the works constitutional committees must be ensured.

Violations of the guidelines are examined individually in accordance with valid legal, contractual and company law provisions and punished accordingly.

Deviations from this guideline which affect the security level are only permitted for a limited period of time and after consultation with the appropriate organizational units (see appendix B.1.5).

Appendix

A General

A.1 Further documents

A.1.1 Information Security Regulation No. 03.01.16 Third party service delivery management

A.1.2 Information Security Regulation No. 03.01.05 IAM

A.1.3 Information Security Regulation No. 03.01.02 Cryptography

A.1.4 Glossary for Information Security Guidelines

https://portal.epp.audi.vwg/wps/poc?uri=audi-np:oid:1551257182834@oid:Z7_3Q9IGGC0O0C870QI440ST620E7&epp-media=/content/aepc/mynet/en/2682/628/_jcr_content.download.pdf/13a1f2cd-6493-4e26-94db-e79e5001831b/it-sec_2_glossary_for_security_guidelines_audi.pdf

A.2 Validity

This regulation is valid immediately after publication.

Next inspection date: March 01, 2025

A.3 Abbreviations and Definitions

Abbreviation/Term	Explanation
System Developer	All people involved in defining, designing, developing and implementing an IT system. Typically the following roles are meant by this definition: • IT System Planer • IT System Architect • Software Architect • IT System developer • Software Developer • Application Developer • Computer Programmer • Tester

A.4 Document History

Version	Name	Org. Unit	Date	Comment
2.0	Fröhlich	I/GA-2	12.03.2013	Approved Version
3.0	Fröhlich	I/GG-81	24.10.2016	Revision
4.0	Fröhlich	I/GG-81	25.07.2018	Renaming of the IT security regulations in Information security regulations; reorganization security goals
5.0	Fröhlich	I/FL-81	01.03.2022	Revision

B Specific Characteristics

B.1 Company-specific

B.1.1 The notification about informations of alterations or updates is conducted only via the Audi mynet.

B.1.2 Responsibility: unit IT Sicherheit.

B.1.3 IT systems that require workers' participation have to be consulted within the works council IT commissions.

B.1.4 Responsibility: unit IT Sicherheit.

B.1.5 Responsibility: unit Datenschutz- / Datensicherheitsmanagement, Office des DSB