Information Technology (IT) Security Guidelines for System Developers

Valid from:	20.10.2006	Status:	Published
Revised:	01.11.2016	Version:	3.0
Issued by:	I/GG-81, Datenschutz- / Datensicherheits-management, 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

The IT Security Policy forms the basis of this document.

These IT Security Guidelines define the Information Security regulations that must be observed by system developers[1] within their area of responsibility for IT systems and infrastructure.

Additionally, the IT Security Guidelines for Employees must be observed by the target audience of system developers. System developers must identify and observe applicable (role specific) regulations if they fulfill additional roles.

The IT Security Guidelines serve to protect the confidentiality, integrity, availability, and traceability of information, as well as to protect the rights and interests of the company and all natural persons and legal entities that maintain a business relationship with our Group Company and/or perform work for it.

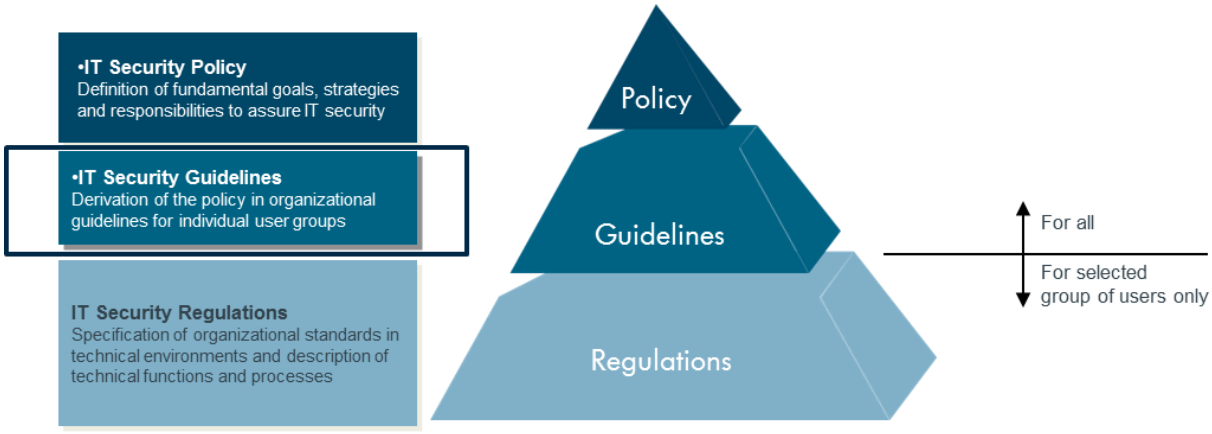
In terms of this regulation the definition information security designates IT security as part of the integral information security.

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

This document and notifications concerning modifications and updates are communicated via usual ways of distribution (see appendix, B.1.1).

1. Context

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



IT Security Regulations

2. Asset management

The information owner is responsible for his specific information. This also applies to information provided via IT systems. Responsibilities can also be delegated.

[1] Definition in A.2

3. Communications and operations management

Security relevant tasks (like administration of encryption keys or security infrastructure or systems) may only be carried out by suppliers/contractors after approval by the responsible unit (see appendix, B.1.2). The requirements of the regulation 03.01.16 Third Party Service Delivery Management must be observed.

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

The security requirements for an IT system must be defined and documented together with the information owners during the planning phase.

System planning (functional specification, system design, system implementation) and system acceptance (system introduction) must be carried out using the valid Group system development standards (e.g. IT-PEP).

Information that is provided via publicly accessible IT systems must be protected against unauthorized access or modifications with appropriate security measures (e.g., encrypted transfer of authentication information, integrity checks).

4. Access control

Based on the information owner's risk assessment, authentication and authorizations mechanisms must be set up for accessing information. This involves implementing the roles and rights system specified by the information owner.

The system owner is responsible for implementing a guideline conform secure logon procedure (e.g. strong authentication via smart card)[2].

Appropriate measures must be implemented to prevent guessing of user IDs and passwords (e.g., extend the waiting time after each failed logon attempt and/or block access after a specified number of failed attempts).

The persons responsible for the systems must implement the requirements defined for passwords (see "IT Security Guidelines for Employees") through appropriate system implementations.

Authentication information (e.g. passwords, keys, …) must at least be classified as „confidential“ and handled accordingly. The owner of the information made accessible with this authentication information may classify them as „secret“.

Authentication information must be protected from unauthorized access. Passwords in systems, applications, databases and tokens must be saved as a one-way hash. Ideally, they should be saved as a “salted hash”[3] or more secure alternatives. Passwords must never be saved as plain text.

Dialog sessions that are no longer actively being used after an extended time period must be deactivated or protected by appropriate measures.

Communication to or between confidential and/or secret systems must use mutual (two way) authentication (e.g. via TLS).

Processing of information must be defined in collaboration with the information owner. This specifically includes any usage in IT systems or transfer between IT systems. The information owner’s approval must be documented.

[2] See IT Security Guideline 02.03 for System Operators and Administrators
[3] “Salt” refers to a randomly generated character string in cryptography which is coupled with a given plain text as input before using a hash function to increase the entropy of the input

5. Information systems acquisition, development and maintenance

5.1. Security requirements of information systems

The required Information Security measures (e.g. system hardening, patch management) must be identified and implemented before the IT systems are developed and used.

Regulations on handling of information (see IT Security Guidelines for Employees, section "Classification and handling of information") also apply to IT systems (e.g., databases, backup media).

5.1.1. Confidentiality

Information must be protected against unauthorized access according to its classification. Confidentiality classification leads to the following security measures:

Classification	Definition
Public	• System hardening (required services only, current security patches)
Internal	• System hardening (required services only, current security patches) • Access control in conformity with "need to know" principle • 1-Factor-Authentication (e.g. user-ID and password)
Confidential	• System hardening (required services only, current security patches) • Access control in conformity with "need to know" principle • 2-Factor-Authentication (e.g. smart card and PIN) –particularly for access to applications - or an additional safeguard like authenticated storage encryption (e.g. encrypted data on file share, encrypted USB device) • Transport encryption
Secret	• System hardening (required services only, current security patches) • Access control in conformity with "need to know" principle • 2-Factor-Authentication (e.g. smart card and PIN) particularly for access to applications • Transport encryption • Storage encryption

5.1.2. Integrity

Information has to be protected against unwanted change or unauthorized manipulation according to its classification. Integrity classification leads to the following security measures:

Classification	Definition
Low	• System hardening (required services only, current security patches)
Medium	• System hardening (required services only, current security patches) • Access control in conformity with "need to know" principle • 1-Factor-Authentication (e.g. user ID and password) • Databases: Referential integrity protection must be enabled
High	• System hardening (required services only, current security patches) • Access control in conformity with "need to know" principle • Validation of input data and output data as well as control of internal processing for error reduction and avoidance of standard attacks like buffer overflows and infiltration of executable code (e.g. field limit control, field limitation on special areas) • Creation of secure hash values for data • Verification of the hash values before processing data
Very high	Additional to the requirements for „high“: • 2-Factor-Authentication (e.g. smart card and PIN) for write access • Generation and verification of digital signatures for stored data or similar security mechanisms • Creation of secure hash values for data • Verification of the hash values before processing data • Signing of hash values (secure storage of keys)

5.1.3. Tracebility

Traceability of access to information and changes on information must be secured. Traceability classification leads to the following security measures:

Classification	Definition
Low	• System hardening (required services only, current security patches) • Standard system error logging, logging of logon failures, etc.
Medium	• System hardening (required services only, current security patches) • Standard system error logging, logging of logon failures, etc. • Logging of user-IDs, system time and type of changes (add, delete, modify) • 1-Factor-Authentication (e.g. user-ID and password) for write access
High	• System hardening (required services only, current security patches) • Standard system error logging, logging of logon failures, etc. • 1-Factor-Authentication (e.g. user-ID and password) for write access • Logging of user-IDs, system time and type of change for write access in a way that the status before the change can be identified
Very high	• System hardening (required services only, current security patches) • Standard system error logging, logging of logon failures, etc. • Logging of user-ID and system time for read access • Logging of user-IDs, system time and type of change for write access in a way that the status before the change can be identified • 2-Factor-Authentication (e.g. smartcard and PIN) for reading and writing access

5.1.4. Availability

System availability must be ensured according to its classification. Availability classification leads to the following security measures:

Classification	Definition
Low	• System hardening (required services only, current security patches) • Recovery measures within 72 or more hours. Adequate measures must be implemented.
Medium	• System hardening (required services only, current security patches) • Recovery measures within 24 and a maximum of 72 hours (BIA-IT: level 3 and 4). Adequate measures must be implemented.
High	• System hardening (required services only, current security patches) • Recovery measures within 1 and a maximum of 24 hours (BIA-IT: level 2). Adequate measures must be implemented.
Very high	• System hardening (required services only, current security patches) • Recovery measures within less than 1 hour (BIA-IT: level 1). Adequate measures must be implemented.

5.2. Correct processing in applications

The security of IT systems must be ensured by the implementation of measures prescribed by the valid Group system development processes (e.g. IT-PEP).

The consultation activities for introduction of IT systems are subject to the regulations and intra-company agreements of the respective group company (see appendix, B.1.3).

5.3. Cryptographic controls

Fundamental decisions concerning strategy, use, and handling of cryptographic methods must be made by the appropriate bodies (see appendix, B.1.4).

The requirements of the regulation on cryptography[4] must be observed and only the methods specified therein must be used.

[4] Regulation 03.01.02 Cryptography

The "Book of Standards" must be taken into consideration for the use of encryption products.

5.4. Security of system files

5.4.1. Protection of system test data

Development-, test- and productive IT systems must be separated.

If possible, tests have to be carried out with generated test data (e.g. with a test data generator).

Systems must only be tested in a test environment designated for this purpose. It must be ensured that the productive system operation is not negatively affected.

If individuals are given access to personal, confidential or secret data that they do not need to fulfill their contractual tasks, the data is to be scrambled in a way that the original data cannot be identified, before the data is transferred from the productive IT system to the test environment.

Copying or usage of information from productive IT systems is only permitted with prior authorization from the information owner. Copied data is subject to the same Information Security requirements as the original data.

After the tests have been performed, data from productive IT systems that has been used in the tests must be completely deleted.

Access and role concepts that apply to productive IT systems must also be implemented for the test systems if copies of live 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, the effects of these changes on existing regulations and security measures must be clarified. Changes may only be made if such changes are permissible by the license and maintenance contract.

6. Compliance

Country specific regulations on import/export/access of/to hardware/software/information must be observed when encryption and/or electronic signatures are used.

For system development, license and usage rights of third parties (including contract law) must be observed as required by applicable regulations.

Questions regarding country specific regulations must be addressed to the responsible units (see appendix, B.1.5)

II. Responsibilities

For circumstances that are subject to mandatory codetermination, the involvement of the legally sanctioned works councils must be ensured.

Infringements of these guidelines will be individually reviewed and punished according to the operational and legal provisions and agreements in force.

Deviations from these guidelines that reduce the level of security are only permissible in agreement with the responsible bodies (see appendix, B.1.6) and only for a limited time.

Appendix

A General

A.1 Validity

This regulation is valid immediately after publication.

Next inspection date: November 11, 2018

A.2 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.3 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

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: Audi IT-Sicherheitsteam

B.1.5 Responsibility: unit Zentraler Rechtsservice.

B.1.6 Responsibility: unit Datenschutz- / Datensicherheitsmanagement, Office des DSB