Information Technology (IT) Security Guidelines for System Developers

History of document:

Version	Name	Org.-Unit	Date	Comment
1.0	Fröhlich, Hafner	Audi I/GO, VW K-GOT	20.10.2006	

Table of Contents:

1. Goal

These IT Security Guidelines summarize the IT Security Regulations for system developers (developers of IT systems (see Appendix, point 1)) applicable for the usage of information and communication devices (e. g. personal computers, workstations including mobile computers like notebooks, PDAs).

These serve to protect confidentiality, integrity and availability of information as well as to uphold the rights and interests of the company and all natural and legal entities, who maintain business relationships with or work for the group company.

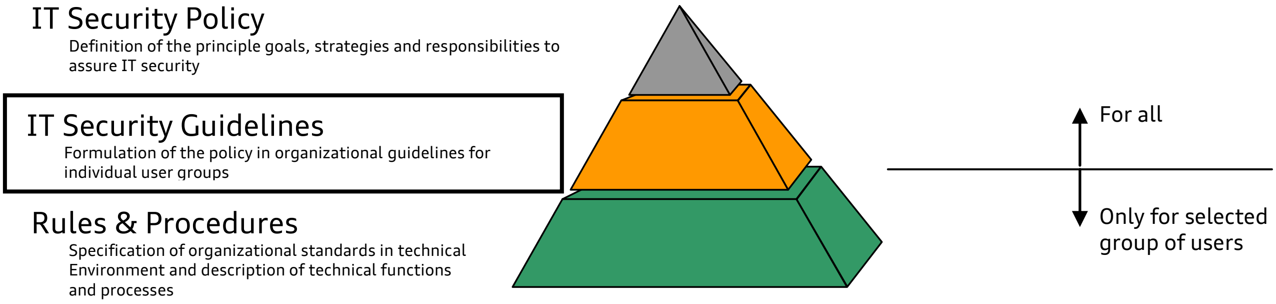
The basis for this document is the IT Security Policy. The principles of the IT Security Policy have been developed for the target group system developers. The structure of this document is based upon the international standard ISO/IEC 17799.

This document is available via intranet (see Appendix, point 2).

The notification about information of alterations or updates is conducted only via intranet (see Appendix, point 2).

2. Context

The following overview shows the position of the IT Security Guidelines in the IT Security Regulations:


IT Security Policy
Definition of the principle goals, strategies and responsibilities to assure IT security
IT Security Guidelines
Formulation of the policy in organizational guidelines for individual user groups
Rules & Procedures
Specification of organizational standards in technical Environment and description of technical functions and processes
For all
Only for selected group of users

IT Security Regulations

3. Scope

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

4. Asset classification and control

The respective information owner is responsible for the information. The information owner is responsible also if the information is provided by IT systems.

5. Communications and operations management

Security requirements of an IT system have to be defined and documented with all users or user representatives during the planning period.

Access to sensitive system documentation is to be restricted to those individuals that require the information to fulfil their specific tasks.

6. Access Control

Suitable procedures have to be in place to avoid guessing of userIDs and passwords (e. g. lengthen the waiting time after each attempt and/or blocking after a defined number of attempts).

The system operator is responsible to implement a secure logon procedure. The following requirements have to be observed for this:

- For false input the IT system must not indicate which part of the details was wrong.
- Wrong attempts have to be recorded.
- The maximum time permitted for the logon has to be limited and mechanisms implemented to automatically logoff when the limit is reached.

The system responsible persons have to support the minimum requirements defined for passwords (see “IT Security Guidelines for employees”) by corresponding system implementations.

Dialog sessions that are not actively used over a longer period have to be deactivated or have to be protected by suitable measures.

7. Systems development and maintenance

7.1. Security requirements of IT systems

Security measures have to be defined and agreed upon before IT systems are designed and deployed. This applies to the infrastructure, standard applications and internally developed applications.

IT security requirements and measures have to consider legal regulations, the value of the affected information as well as the potential damage for the company that could be caused by the lack or non-existence of security.

The analysis of IT security requirements and the identification of measures to fulfil these requirements should necessarily base on risk management.

The following basic IT security requirements have to be ensured in system development depending on classification of data:

- Data Integrity, i. e. implementation of measures, which ensure the accuracy and completeness of all data.
- System Integrity, i. e. implementation of measures, which ensure its processing is complete, accurate and authorized.
- Availability, i. e. implementation of measures, which ensure the provision of data and system ~~assets should be provided when needed~~within an agreed time frame.

- Confidentiality, i. e. implementation of measures, which ensure that only authorized people get access to sensitive information during use, transit, storage or erasure.
- Access Control, i. e. implementation of measures, which ensure, that access to business sensitive information is limited to persons which need these to fulfil their contractual tasks.
- Authentication, i. e. implementation of measures, which ensure, that all IT systems only can be used by authorized persons.
- Authorization, i. e. implementation of access control measures, which ensure, that all IT systems and respectively all IT users can only use data and services which were granted to them explicitly.
- Non-repudiation, i. e. implementation of measures, which ensure that authentication and integrity of contained information can be verified later on.

7.2. Security in IT systems

Measures to ensure confidentiality, integrity and availability (against loss, modification or misuse of data) have to be provided in IT systems. These are measures such as:

- Input data validation
- Control of internal processing e. g. data base transaction tracking
- Message authentication
- Output data validation

Approval procedures have to be strictly followed with when using audit or activity logs (see Appendix, point 3).

The use of special security measures (e. g. encryption, signatures) is necessary for applications systems processing confidential or secret data. The specification and decision on the use of such measures has to be conducted based on risk analyses regarding to the IT security requirements of the business process.

The security of IT systems has to be ensured by deployment of measures required by System Engineering Process (SEP).

Group company specific regulations and works council agreements (see Appendix, point 4) are applicable with regard to the consultation at introduction of IT systems.

7.3. Cryptographic controls

7.3.1. Policy on the use of cryptographic controls

Basic decisions on the strategy, use and handling of cryptographic measures have to be conducted by the responsible units (see Appendix, point 6).

7.3.2. Encryption

The regulations for key management to ensure confidentiality, integrity and authenticity for the creation, distribution and installation of suitable keys have to be defined by the responsible units (see Appendix, point 6).

Encryption tools (see Appendix, point 7) released by responsible units have to be implemented to protect confidential or secret data.

7.3.3. Digital Signatures

At least the advanced electronic signature has to be implemented to protect the authenticity and integrity of secret data during distribution.

An electronic signature is a control information (mechanism) that is attached to a message or file and is linked to the following properties:

- On the basis of electronic signatures it is possible to determine unambiguously who created these signatures.
- The signer confirms by signature his/her agreement with the content and the sending of the data.
- Whether the data transmitted with the electronic signature are identical to the data that were actually signed, is verifiable.

The national laws for the legal recognition of the electronic signature have to be complied with (see Appendix, point 8).

Certificates have a limited validity. Data signed by a signature certificate (key usage “content commitment” or “non repudiation”) have to be re-signed with a key that is valid for a longer time period before validity of the signature certificate expires.

7.3.4. Key management

The keys have to be protected against modification and destruction. If it is suspected that the keys have become known to unauthorized persons they have to be replaced. The number of people who get access to the keys has to be as small as possible and should be documented in a register. It has to be ensured that used keys used to encrypt or sign data are kept at least as long as the archives in case this is not ensured by a central key management (e. g. PKI).

7.4. Security of system files

The installation of software is permitted only by authorized persons (see Appendix, point 9).

New or modified programs for operational systems may be deployed only after successful testing as well as after approval by information owner and approval by system operator. The version and correction status of deployed software has to be documented and archived related to company specific regulations (see Appendix point 10).

Access to test data has to be based on the “need to know” basis only.

Software testing is only allowed in test environments, which are designed for tests. In doing so it has to be ensured that daily operations are not affected negatively.

If persons get access to personal-related, confidential or secret data that they do not need to fulfil their contractual tasks, the data are to be scrambled in a way that the original data can not be identified, before transferring them from the operational IT system into the test environment.

Copying or the use of information from operational IT systems is only permitted after prior authorization by the information-owner. Data that have been copied have to fulfill the same IT security requirements as the original data.

Used information from operational IT systems has to be erased non restorable after completion of the test.

Access rights that apply to operational IT systems have to be followed also for test environments.

7.5. Security in development and support processes

All relevant processes and procedures for IT systems have to be designed so that the aimed IT security level is achieved and maintained holistically.

Formal change management procedures have to be implemented. They have to ensure that security and monitoring procedures of IT systems are not compromised by changes.

Prior to alterations to purchased software packets, the implications on existing regulations and security measures have to be clarified. Alterations may only be made, when covered by license regulations and maintenance contract.

8. Compliance

For the use of encryption and/or electronic signatures (see Appendix, point 8) especially across country borders, the country specific regulations for the import/export/access of or on hardware/software/information have to be followed.

In case of questions about the use of cross-border encryption the responsible units (see Appendix, point 11) have to be contacted.

9. Responsibilities

These guidelines have to be implemented and complied with by all system developers.

Breaches of these guidelines will be individually assessed and may result in prosecution under prevailing company and legal regulations and agreements.

Deviations from these guidelines, that reduce the security level, are only allowed temporarily after consultation with the responsible units (see Appendix, point 12).

Appendix:

Validity:

With publication these regulations are binding directly for development of new IT systems.

Point

1.
The IT system is a complete system consisting of all HW/SW components including their communication among themselves.

2.
In each case the latest information will be published at Audi mynet.

3.
Personal logging that enables checking of behaviour has to be approved by the works council EDV Systems committee.

4.
IT systems that require workers' participation have to be consulted within the works council IT commissions.

5.
Responsibility: IT Security Team.

6.
Responsibility: I/FP-72.

7.
The released encryption tools are available in mynet: Services/IT&O/Produkte & Leistungen/Architektur, Methoden & Standards/IT-Standards – Die verbindliche Vorgabe im Konzern.

8.
National legislation for recognition of the electronic signature:
In the **Federal Republic of Germany** the Signature Law („Signaturgesetz – SigG“) applies. In this, the national legal framework of requirements for deployment of electronic signatures is described.
The national legal framework of requirements for the use of electronic signatures is described here. The “Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften [SigG01]“ modified for the EU-Regulation on common framework of requirements for electronic signatures dated December 13, 1999 [ECRL99] became valid on May 22, 2001 and overrules the “Signaturgesetz” from 1997.
The law should create framework requirements, with a qualified electronic signature to be seen at least as equally secure as a handwritten signature. It contains determinations of, when qualified electronic signature in accordance to the “Signaturgesetz” are to be treated equally to handwritten signatures. In the result, digital signatures in accordance with the “Signaturgesetz” have been approved as high security even before court.

9.
Responsibility: system administrators and employees with administrative rights.

10.
The version and correction status of deployed software has to be archived depending on legal requirements and department requirements. For example all documentation dealing even indirect with invoices has to be archived related to „Grundsätzen ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)“ during life time of the system and after life time 10 years.

11.
Responsibility: Central Legal service.

12.
Responsibility: Information and Data Protection.