# IT Security

**Contents:**



## 1. Purpose

The IT (Information Technology) security rules described in this Organization Standard define fundamental goals, strategy and responsibilities to ensure IT security within the company Škoda Auto (hereinafter referred to as "the Company"). They are defined on the basis of ČSN ISO 27001:2005 and other international regulations and standards (see Chapter 6) aiming at anchoring them within the Company.
This standard builds upon the VW's IT Security Policy and the related regulations of the VW Concern. The IT Security Policy includes provision of technical infrastructure, and information flow control and management. The security rules are used to protect information confidentiality, integrity and availability as well as to retain all rights and interests of the Company and all natural and legal persons, who are in business relation with the Company or work for the Company.

To create and maintain trust in IT security, regulations for information protection are created and implemented in the Company, which:

- Raise awareness about the possibilities and risks in the area of IT, about the reasons and necessity of information protection
- Introduce IT security as standard in the Company's processes

## 2. Scope of Application

This Organization Standard is binding upon all:

- Company's OU managers and employees appointed by them
- IT users (internal and external)
- Subsidiary companies

## 3. Basic Terms / Abbreviations

| | |
|---|---|
| IT | Information technologies (formed by IS and ICT) |
| IS | Information systems |
| ICT | Information and Communication Technology |
| Communication equipment | Personal computer, workstation, notebook, PDA (Personal Digital Assistant), MDA (Mobile Digital Assistant), cell phone |
| SW / Software | Set of all software placed in communication equipment |
| Harmful SW | Dangerous SW such as viruses and other harmful code |
| HW / Hardware | All physically existing hardware of communication equipment |
| Authorized person | IT user having permission to read or change particular information and IT user having permission to use a certain HW. |
| IT user | Every natural person requesting and using access to IT or Company's |

| | |
|---|---|
| | information stored thereon |
| Data owner | Manager of OU, where data is created, loaded into IS for the first time, or which is the only department of the Company where the specified data is processed or used |
| Information | Assets being of value for the Company, which may exist in different forms (printed, electronic and others) |
| Confidentiality | Information disclosure/communication to authorized person only |
| Availability | Information availability for authorized user at the moment of its need |
| Integrity | Assurance of the truth (validity) and completeness of information |
| Authentication | Identification confirmation when accessing information |
| Authorization | Enabling only authorized persons to access the information to the scope necessary for the fulfilment of tasks |
| Auditing | Information access recording and control |
| Accountability | Indisputability of access to information and its processing |
| CISO (Chief Information Security Officer) | Agent for IT security – EOS manager, manages IT security within the Company |
| ISSO (Information Systems Security Organisation) | Global IT security organization within the Volkswagen concern |
| Agent for data protection | Proposes measures aimed at enhancing data security; takes care of uniform state of knowledge in the matters concerning data security within the Company. Creates data security standards based on risk assessment. Solves incidents in the area of data security, in cooperation with other departments. |
| Relevant administrator of technology HW | OU having the competence to administer technology HW (e.g. in the area of V - maintenance departments, in the area of T - TM/2) |
| EOx | Organizational units (OU) falling under EO, which are responsible for IT administration and development within the Company |
| ServiceDesk | Central place for IT user support |
| IT security standards | System, process and organization documentation related to IT security |
| MFA2 card | Multifunctional employee's Identity Card |

## 4. Competencies

| Activity | Responsibility |
|---|---|
| They define jointly general principles of information security. | ZO, EOS<br>Agent for data protection |
| He/she familiarizes the employees with process and organization documentation, standards in the area of IT security and with the importance of their observance. In his/her sphere of activity, he/she is responsible for ensuring adequate IT security in handling of information and IT. He/she is responsible for applying IT security rules and controls the observance of regulations on a continuous basis.<br>In the interest of reduction of security risks, he/she is obliged to ensure education and training of employees in the area of IT security. | OU manager |
| In the area of IT security - he/she identifies risks, creates standards and rules, and controls systematically their application in practice, performs analyses and audits, plans and controls implementation of effective measures and in cooperation with other departments, solves incidents related to IT security.<br>He/she supports managers in creating awareness about the importance of IT security, takes care of uniform state of knowledge in the matters concerning IT security within the Company.<br>He/she approves exceptions to the provisions of this Organization Standard.<br>He/she prepares supporting documents for induction training of new employees of the Company (in the are of IT security) | EOS |
| He/she makes changes in HW (e.g. installation/removal of hard disks, floppy disk drives, memory modules) and changes in SW and its setting. | EOI |

| | |
|---|---|
| He/she ensures connection of communication equipment to data network of the Company.<br>He/she ensures repairs and disposal of communication equipment. | |
| He/she administers and makes changes in technology HW and SW (e.g. installation/removal of hard disks, floppy disk drives, memory modules) and changes in SW and its setting. He/she ensures repairs and disposal of technology HW and SW. | Relevant administrator of technology HW |
| He/she cooperates with EOS in creating IT security standards, implements them actively and enforces systematically their observance by users. He/she is responsible for ensuring security standards, plans purchase and operation of IT in compliance with IT security standards. He/she adopts measures in order to ensure that the accesses to information are uniquely identifiable, restorable and indisputable.<br>He/she makes sure that only uniquely identified persons having the relevant permission can obtain the access to information protected in an appropriate manner. | EOx |
| He/she coordinates IT security within the VW Concern and enforces introduction of uniform rules and standards. | ISSO (IS Security Organisation) |
| He/she coordinates IT security within the Company and enforces introduction of uniform rules and standards. | CISO (Chief Information Security Officer) |

| **ALWAYS** | **NEVER** | |
|---|---|---|
| He/she is responsible for making proper use of HW, SW and information solely for Company's needs and within the fulfilment of his/her tasks. | He/she does not disseminate information with non-working content within the Company and outside the Company (e.g. chain e-mails, jokes). | IT user |
| He/she uses SW and data owned by the Company only on Company's IT. | He/she does not use and store SW not owned by the Company on Company's IT, not even for work purposes (e.g. freeware, shareware). | |
| Within the tasks assigned, he/she is responsible for specifying the relevant degree of information confidentiality immediately upon its creation and for its security in case of its use. | He/she does use another person's account for his/her work. He/she does not furnish anyone with details about his/her user account and password(s). | |
| He/she treat appropriately the IT and information provided, protects them against loss, damage or unauthorized use or change, possibly falsification. He/she observes manufacturer's instructions and principles of occupational health and safety. | He/she does not use private HW (including accessories and data carriers) for his/her work, and does not connect it to Company's IT (e.g. connection of private USB memory stick to work PC, connection of private cell phone by means of Bluetooth to Company's communication equipment). | |
| He/she reports to his/her superior or EOS/2 any violation, or suspicion of violation of regulations related to IT security or any weakness in IT security in systems, single functions and functional failures relevant to IT security. | He/she does not interfere in HW configuration or SW setting on Company's communication equipment (e.g. RAM memory replacement, closing of running services, change in IE configuration). | |
| When using IT, he/she observes the measures to protect confidentiality, availability, integrity and accountability. | He/she does not provide data by sharing it from assigned communication equipment to other users/communication equipment connected to Company's data network. | |
| He/she observes process and organization documents and standards in the area of IT security applying provably to him/her. | | |
| Once a year, he/she attends training in the area of IT security. | | |

## 5. Procedure

Information and equipment provided in order to process information and to communicate are valuable property of the Company and are subject to protection. In principle, transfer of information and software owned by the Company to external companies (e.g. external persons in joint projects) is permitted only within the written agreed specification of task and with written consent of data owner.

| | |
|---|---|
| Principles of IT security | • Within the tasks assigned, each person, who uses information, is responsible for its security.<br>• All information must be appropriately classified and secured immediately upon its creation.<br>• Only uniquely identified persons having the relevant permission can obtain the access to information protected in an appropriate manner.<br>• All accesses to information must be uniquely identifiable, restorable and provable. |
| Violations | Intentional act or act by negligence is considered to be a violation of IT security, which includes particularly:<br>• Injury of the good reputation of the Company<br>• Threat to safety of employees, contractual partners or Company's property<br>• Actual or potential financial loss incurred by the Company<br>• Unauthorized access to information, its unauthorized disclosure or unauthorized modification<br>• Use of corporate information for unlawful purposes.<br>Violations of IT security regulations are assessed individually according to relevant legal, contractual and operational provisions as amended, and are sanctioned in compliance with relevant generally binding legal regulations. |
| Connection of communication equipment to data network of the Company | Communication equipment can be connected to Company's data network only when such equipment is owned by the Company or when the communication equipment is connected by the company, in which the Škoda Auto Company or one of the companies of the Volkswagen Concern has a majority interest. Connection may only be performed / set by EOI. |
| IT protection against loss, damage and theft | Company's IT should be treated appropriately and protected against loss, damage or theft. Communication equipment must not be left freely accessible and unattended.<br>• Communication equipment can be transported outside the Company only with written consent of ZO (except for cell phones).<br>• Portable communication equipment must not be placed unattended in a motor vehicle.<br>• In principle, when flying and taking trains, portable communication equipment must be transported as hand luggage. |
| IT protection against unauthorized use | Only authorized persons may have access to the Company's communication equipment. Unauthorized persons (applies to family members, friends, etc.) must not have the possibility to use the equipment or to see the information classified as internal, confidential or secret (see OS – 161/3 - Confidentiality). If long-term processing is running on communication equipment, which cannot be interrupted or the user needs to leave the equipment for the necessary period of time (e.g. break, meeting, toilet), the user must secure the communication equipment against unauthorized use by means of password-protected screen saver or any similar mechanism. Users, who uses a card to log into the MFA2 system, must remove the MFA2 card from the reader every time he/she is physically leaving the communication equipment. After completion of work on the communication equipment, the user is obliged to close properly the system and turn off the instrument including screen and all directly connected communication instruments. |

| | |
|---|---|
| Security of terminal equipment against harmful software (antivirus and security update of SW) | Rules of protection against viruses and harmful software are defined by MP Antivirus Protection.<br>Communication instruments, systems and data carriers must be periodically and in case of suspicion of occurrence of harmful SW, immediately checked by means of an updated antivirus SW (on office PCs this is ensured automatically by means of antivirus SW).<br>In case of suspicion of attack by harmful SW or nonfunctional antivirus SW, the communication instrument must not be further used and ServiceDesk (or the relevant administrator of technology HW) must be informed to remove the harmful SW.<br>Security updates are installed automatically on office PCs and the user is informed about their installation. |
| Electronic mail/Internet security | Electronic mail must be automatically checked for presence of unsolicited messages (so-called spam). This unsolicited emails must be automatically deleted. If the user finds any unsolicited message in his/her mailbox, he/she should delete it without opening it.<br>It is not permitted to create, send and forward chain and bulk unsolicited business and private messages. Electronic mail is not intended for transferring large files.<br>A sender, as an author of electronic message, is responsible for the content and distribution list, and a recipient is responsible for further processing and distribution of electronic message.<br>Before their first release, electronic messages and their attachments must be checked by updated antivirus SW for occurrence of any hazardous SW (on office PCs this is ensured automatically by means of antivirus SW).<br>Internet can only be used for work purposes. For more specifications and rules of use see OP 123/2 – Internet – Assignment and Use. |
| Backup | Information may only be stored on network disks intended solely for this purpose, which are provided with central and automatic data backup.<br>Storing information on a local disc of communication equipment is possible only for the purpose of temporary work need. The "Documents" folder (so-called user profile of the relevant user) or its subfolders may only be used as a repository on nontechnology PCs with Windows Operating System.<br>Any user is responsible for backing up this data stored on local data carriers (hard disks of communication equipment, CD, DVD and others) and for its possible loss.<br>Data carriers containing confidential or classified data must be appropriately identified, categorized and stored in locked space (cabinet, drawer). |
| User access to information | Any user may obtain access (except for public information) to only such information, which he/she needs within the fulfilment of his/her task. A larger scope must be provably approved by data owner.<br>Any user account or access right not required any longer must be reported by the user to the relevant originator of the access, who is obliged to delete it.<br>Any unnecessary media for identification purposes (e.g. MFA2 cards, SecureID tokens) must be immediately returned to their issuer or authorized department.<br><br>Access to information, information handling and storage on network disks are governed by MP EOI Network Data Handling. |
| Records of communication equipment | Each communication equipment owned or used by the Company must be registered in IT Central Records (for more details see MP IT Records) |

## 6. Related Supporting Documents

Act No. 140/1961 Coll., the Criminal Code
Act No. 101/2000 Coll., on the Protection of Personal Data
Act No. 148/1998 Coll., on Protection of Classified Information
ČSN ISO/IEC 27001:2005
ISO/IEC 9001:2000
VW's IS Security Policy and related regulations of the VW Concern
Škoda Auto Company Policy
Guideline for Integrated Management System of Škoda Auto
OS 122/4 Data Protection and Security
ON.1.019 Access Rights to Information Systems
OP 123/2 Internet – Assignment and Use
OS 161/3 Confidentiality
OS 162/2 Protective Measures
OS 162/3 Protection of Property
Work Regulations
EO Intranet:
- MP Network Data Handling
- MP Antivirus Protection
- MP IT Records

EOS Intranet:
- User account and user access to information – definition of passwords and PINs

## 7. Documentation

Form of Authorization to Carry Objects Outside the Premises

## 8. Appendices

Not occupied

Holger Kintscher
E/ Economy area

Andreas Hafemann
EO/ Information systems and organization