VOLKSWAGEN GROUP

IS-Regulation 02.03

Guideline for system operators and administrators

Version: 4.3
Applicable as of: 22.02.2024

Responsible Department: Information Security Governance – K-DS/G
itsr@volkswagen.de

Issued by: Information Security Governance – K-DS/G
(itsr@volkswagen.de)

Content

Notes on the document

Changes in the regulation text are highlighted with font color #E67364..

For all gender-related designations the chosen wording refers to all genders, even if the generic masculine is used here for reasons of easier readability.

1 Purpose

This Information Security Guideline defines the rules for information security that system operators and administrators must follow when handling information and IT devices (e.g. PCs, laptops or other mobile devices). For the protection of programmable logic controllers (PLCs) and robot controllers, the specific requirements set out in the appendix apply (see appendix B.1.2).

In addition, the Information Security Guideline for employees or third parties applies to the target group of system operators and administrators, provided that the system operator or administrator is an employee of a partner company.

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.1.3).

2 Area of application

This guideline applies to Volkswagen AG, i.e. Group functions, the Volkswagen Passenger Cars brand, Volkswagen Commercial Vehicles and Volkswagen Group components. All system operators and administrators must adhere and comply with this guideline.

3 Asset management

All company-owned IT systems (see appendix B.1.6) must be entered in a register. Operational responsibility for an IT system is to be assigned to a person or organizational unit that actively manages the system.

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

That register of IT systems shall include at least the following information: :

- description of IT systems, including interfaces to other IT systems
- the responsible organizational unit or person
- the business processes to which the IT systems are assigned
- the hosting location (e.g. data center)
- business process affiliation
- classification of data and, if necessary, information on specific protection requirements and protective measures
- existence of personal data
- information owner

4 Physical and environmental security

- Business-critical IT systems must be protected against power outages (e.g. with the help of an uninterruptible power supply).
- Within the scope of its competences, the system operator ensures the availability of data by ensuring that all equipment is properly maintained at all times. This includes, among other things, the maintenance of IT equipment in accordance with the manufacturer's specifications.
- Operation of IT equipment according to the specifications of the manufacturers (e.g. temperature, humidity)
- Protection of IT equipment from unauthorized access, manipulation, damage or harmful environmental conditions (e.g. fire, water, dirt load)

5 Communications and operations management

5.1 Operational procedures and responsibilities

5.1.1 Documented operating procedures

The system operator is responsible for ensuring that all documentation required for the operation of IT systems (e.g. operational service manuals) is available and up to date. For publications, it should be noted that unauthorized persons do not have knowledge of confidential or secret data, including security-relevant information (e.g. firewall configuration settings).

Documentation must be archived in accordance with company-specific regulations (see appendix B.1.7). The system operator is obliged to follow the established operational procedures (e.g. of the change process).

5.1.2 Change management

Änderungen an laufenden IT-Systemen sind vor ihrer Implementierung in diesen IT-Systemen im Rahmen eines festgelegten Prozesses zu planen, zu testen, freizugeben und zu dokumentieren. Die Vorgaben aus der Regelung (siehe Anhang A.1.5) sind zu befolgen.

Changes to ongoing IT systems must be planned, tested, released and documented before they are implemented in these IT systems as part of a defined process. The requirements of the regulations (see appendix A.1.5) must be followed.

5.1.3 Segregation of duties

The use of different employees for executive (e.g. programming, development) and controlling (e.g. audit, acceptance) activities must be determined organizationally.
In addition, tasks must be divided, otherwise there is an increased risk of intentional or accidental misuse at the expense of the Group (four-eyes principle).

The principle of segregation of duties in accordance with the regulations (see appendix A.1.2) must be observed.

5.1.4 Separation of development, test and production environments

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

exception are large production facilities, where this would not be possible without reasonable effort.

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.

If only personal data of the testers from the data protection categories IT usage data and/or professional contact and identification data are contained in the development or test system, this is generally permissible. All requirements of the GDPR must be complied with in this context. If you have any questions, please contact the responsible DSMO (see Appendix A.1.9) of the department.

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.

5.2 Service delivery by third parties

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.1.8). In doing so, the requirements of the regulations (see appendix A.1.6) must be followed.

5.3 System planning and acceptance

The capacity requirements for an IT system must be specified during the planning phase.
The security requirements for an IT system must also be specified in the planning phase in cooperation with the information owners. For the commissioning of new IT systems, a documented and executed handover to the system operator must be carried out.
System planning (functional specification, system design, system implementation) and system acceptance (system introduction) must be carried out in accordance with the Group-wide standards for system development (e.g. IT PEP).

5.4 Protection against malicious and mobile code

IT equipment and IT systems must be protected against malware by means of

protective measures (e.g. virus scanners) approved by the responsible organizational unit (see appendix B.1.8). The respective protective measures must be documented and kept up to date.
If IT devices are infected with malware they must be disconnected from the network while estimating possible effects (e.g. production downtimes). The requirements of the regulations apply (see appendix A.1.1).

5.5 Backup

All persons responsible for IT systems must ensure sufficient data backups to allow for any necessary recovery of information within a reasonable timeframe. The requirements of the regulations (see appendix A.1.7) must be followed.

5.6 Network security management

After the installation of network components (e.g. routers), their system-specific protection functions (e.g. password protection) must be activated immediately and default passwords must be changed according to the specifications for passwords. All active network components must be centrally managed and monitored using a management system in order to detect errors or critical events in good time.

5.7 Electronic communications

The following requirements apply:

- System-generated emails must be assigned to a responsible person.
- E-mail mailboxes must be protected against unauthorized access.

5.8 Publicly available information

Only secure gateway components may be used to access internal networks from publicly accessible IT systems.

Information of the respective brands and companies of the Volkswagen Group that is provided via publicly accessible IT systems must be protected against unauthorized access and changes by appropriate security measures (e.g. encrypted transmission of authentication information).

5.9 Monitoring

5.9.1 Audit logging

Users' access to IT systems that process information classified as "secret" must be logged. The logs must be kept in accordance with the company's operational regulations (see appendix A.1.2).
The logs must at least contain the following information:

- unambiguous identification of the logged person (e.g. name or ID)
- records of attempts to access the IT system
- records of access to data and other resources

5.9.2 Use of the monitoring system

All logs must be checked regularly as part of audits or in case of suspected information security incidents.

When examining logs, the necessary approval procedures shall be followed (see appendix B.1.9).

5.9.3 Protection of log information

All logs shall be kept in such a way that the logged persons have no authority to modify or change the log information. Logs must not be tampered with or disabled. System administrators must not be able to disable logging unnoticed.

If logs contain information classified as "secret" (e.g. the data itself before and after a change, transmitted data, etc.), it must be ensured that only those persons for whom the information owner has given permission have access to it.

5.9.4 Administrator and operator logs

All activities of administrators and system operators in IT systems that contain information classified as "confidential" or "secret" must be logged. At least for IT systems in which information classified as "secret" is processed, activity logs of the system operators must be stored in such a way that even persons with extended access rights cannot change or delete the log information.

The contents, which logs must contain at least, are documented in the regulations (see appendix A.1.2).

5.9.5 Error logging

All errors and malfunctions reported by users must be logged. All measures taken by operators for the purpose of troubleshooting must be documented.

5.9.6 Time synchronization

Information systems in which log information is stored must be synchronized to a precisely agreed common reference time.

6 Access control

6.1 Business requirements for 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. The roles and permissions specified by the information owner must be implemented. Further requirements on the subject of access control are documented and must be observed in the regulations (see appendix A.1.2).
A request for access rights for IT systems must be made in writing using a corresponding form (e.g. user application) or via a defined and approved IT system (see appendix A.1.2). It must be documented which persons have access rights to a particular IT system.
The assignment of access rights must be approved by the management of the user's organizational unit as well as by the information owner (four-eyes principle). Exceptions are central services (e.g. the intranet). The transfer for approval is permitted.
User IDs must always be assigned to individuals. The distribution of means of identification (e.g. SmartCards or SecurID cards) for the purpose of maintenance access is permitted under the following conditions:

- The distribution is documented by a responsible person. The responsible person shall ensure that it is recorded in writing by whom means of identification were distributed to whom, for what reason and at what time.

- The same retention periods apply to this documentation as to the retention of user requests. Procedures for generating and resetting passwords must be defined and published.

6.2 User administration

Further requirements on the subject of user administration are documented and must be observed in the regulations (see appendix A.1.2).
After the installation of an IT system or software, the manufacturer's default passwords must be changed immediately in accordance with the specifications for passwords.
All information required to periodically check user permissions must be provided to the management of each OU.
As far as technically feasible, the access authorizations of employees of external suppliers/partner companies for IT systems are to be limited to the duration of a project (maximum one year).
User IDs that have not been used for a long time must be blocked. The period must be defined in the authorization concept and should not exceed 400 days.

Passwords must meet the following minimum requirements (these do not apply to PINs):

- 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).
- Login to IT systems must be securely encrypted. If this is not possible, one-time passwords must be used.
-

For the handling of passwords, the following minimum requirements must be met:

- Predefined or standard passwords in IT systems must be changed to individual passwords.
- Passwords must never be stored in plain text.
- Every user must have the possibility to change his password at any time.
- Passwords must not be displayed as plain text when entered on screens.

6.3 Obligations of users with privileged rights

6.3.1 General requirements

The following requirements must be observed by all system operators and administrators:

- The requirements of the Information Security Guideline for employees (handling passwords) or for third parties, if the system operator or administrator is an employee of a partner company, must be followed.
- The requirements of the regulations (see appendix A.1.2) must be followed and implemented in IT systems and applications. In all IT systems/applications, the requirements for passwords from the regulations must be enforced.
- Routine activities that do not require administrative rights must not be carried out with privileged/administrative user IDs. For this purpose, a user ID with limited rights must be used. The password of an administrative user ID may not be used for other user IDs. Additional accounts may be required, for

example, if applications or IT systems are not connected to the central authentication service, or for different roles (user/administrator).

6.3.2 Password generation (personal administrator accounts and IT system-related accounts)

When generating a password, the following minimum requirements must be met:

- No trivial passwords are allowed (e.g. "Test1234") or passwords from the personal environment (e.g. name, date of birth).
- Identical passwords may not be generated for professional and private purposes.
- Identical passwords may not be generated for IT systems provided by the Volkswagen Group and IT systems provided by third parties (e.g. applications, registration services on the Internet).
- Passwords must be changed at least once a year.

6.3.2.1 Personal administrative user IDs

Administrator accounts may only be assigned to users who have completed the mandatory information security awareness training for administrators (see appendix A.1.8). This training must be repeated after two years at the latest.

Further requirements on the subject of personal administrative user IDs are documented and must be observed in the regulations (see appendix A.1.2).

6.3.2.2 System-related user IDs

The availability of system-related passwords must be ensured by the person responsible for the IT system (e.g. by storing passwords).

Further requirements on the subject of system-related user IDs are documented and must be observed in the regulations (see appendix A.1.2).

6.3.3 Use of administrative user IDs

Administrative functions (such as user administration) may only be used for the respective task and under the responsibility of the individual administrator. Administrative permissions must be restricted using feature/role-specific profiles in accordance with the principles of least privilege and need to know.
Only personal administrator accounts may be used.
The company-specific regulations (see appendix B.1.16) must be followed.

The following administrative activities are permitted using the available administrative functions:

- Maintenance and troubleshooting
- Management of access rights for users in their own organizational unit for access to data of their own organizational unit. For the assignment of access rights for data of the own organizational unit to users who do not belong to the own organizational unit, the documented approval of the responsible management of the organizational unit is required.
- Installation of tested and approved software according to the license terms
- For the execution of administrative activities for customers (e.g. for

troubleshooting), the prior approval of the responsible user is required. No approval is required to install standard software or security updates provided through centralized software distribution.

The following administrative activities are not permitted:

- Remove user groups or system accounts of central offices from the local administrators group without supervisor approval
- Create additional administrator accounts (bypassing the process of creating administrator accounts)
- Administration of external groups or external workstations (non-responsible OEs)
- Create accounts with passwords with no expiration date
- Access to users' storage areas unless required for administrative activities. Access to content (e.g. opening files) requires approval in accordance with company-specific regulations (see appendix B.1.17).
- Create local accounts

6.4 Network access control

Only registered and authorized users may gain access to the Group's internal network. The requirements of the regulations (see appendix A.1.9) must be followed. External access to the Group's internal network must be protected by two-factor authentication (e.g. by means of a PKI card). Data transmissions must be protected by secure encryption. The requirements of the regulations (see appendix A.1.9) must be followed.

All unnecessary services and ports must be deactivated.

All required network communication must be documented.

Each IT system must be integrated into a network segment that offers the required level of security. Details can be found in the relevant regulations (see appendix A.1.10).

6.5 Operating system access control

6.5.1 Secure login procedures

Access to IT systems containing non-public data must be secured by appropriate means (e.g. authentication) and restricted to authorized users.

The IT system manager is responsible for the implementation of secure login procedures (e.g. strong authentication using PKI card) according to the respective data classification.

Further requirements on the subject of secure login procedures are documented and must be observed in the regulations (see appendix A.1.2).

6.5.2 User identification and authentication

Where technically feasible, strong authentication (two-factor authentication via "knowledge and ownership") must be set up for administrative tasks. If this is not

possible, alternative security methods (e.g stronger passwords) must be used after agreement with the responsible organizational units (see appendix B.1.8).

When generating or resetting a password, the minimum requirements for passwords must be met.

6.5.3 Password management

The persons responsible for the respective IT systems must implement the minimum password requirements laid down in the regulations (see appendix A.1.2).

6.5.4 Use of IT system tools

Appropriate measures (e.g. withdrawal of corresponding authorizations) must be taken to prevent unauthorized users from changing security-relevant IT system and application settings (e.g. via IT system tools).

6.5.5 Session timeouts

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

6.5.6 Secure deletion of data media

When disposing of or recycling data media, secure deletion or destruction must be ensured.
It must be ensured that there is a high probability that data can no longer be recovered.

The following requirements must be observed for secure deletion:
General requirements:

- If secure deletion is not possible (or fails), the data media must be physically destroyed.
- Secure deletion shall be carried out by the responsible organizational unit (see appendix B.1.18).
- Proof of secure deletion must be kept.
- Only approved tools may be used for secure deletion (see appendix B.1.15).

Magnetic data media (HDDs):

- Pseudo Random Number Generation Stream must be used to overwrite.
    - Internal data: simple overwriting is sufficient
    - Confidential and secret data: These must be overwritten at least twice. The successful overwriting must be checked by the deleting organizational unit.

Non-magnetic data media (USB drives, flash cards, etc.):

- The use of Pseudo Random Number Generation Stream is recommended.
- Simple overwriting is sufficient.

Solid State Disks (SSDs):

- The "Enhanced Secure Erase" procedure, which must be supported by the manufacturer of the SSD, must be used.

- The manufacturer must confirm that the method of deletion used is considered a safe method for his products.
- If this cannot be fulfilled, the SSD must be physically destroyed.

7 Procurement, development and maintenance of IT systems

7.1 Security requirements for IT 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).

The respective IT system manager is responsible for the implementation of the imposed information security measures. This also applies to the use of centrally provided security technologies.

7.1.1 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

7.1.2 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)

7.1.3 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.

7.2 Cryptographic measures

The requirements of the regulations (see appendix A.1.11) must be complied with.

7.3 Security of system files

7.3.1 Control of operational software

Software may only be installed by authorized employees (see appendix B.1.10).

New or modified programs may only be used in running systems if they have been successfully tested and approved in accordance with the valid change management processes (see appendix A.1.5). The version or status of the correction of the software used must be documented and archived in accordance with the company-specific regulations (see appendix B.1.11).

7.3.2 Access control to source code

Program source code must be classified and protected according to the respective data classification (with regard to confidentiality, integrity and availability).

7.4 Security in development and support processes

The use of administration tools and logs must not compromise the security of applications.
Before installing new versions or patches for any software, tests must be carried out to ensure that the modifications do not affect ongoing operation or security.
Applicable procedure descriptions and operational documentation must be adapted if necessary after changes.
If changes are made to software packages, their effects on existing regulations, contracts and security measures must be determined. A change may only be made if it is permitted under licenses and maintenance contracts.

7.5 Management of patches and technical vulnerabilities

To minimize potential risks, all available security updates and patches must be

tested and installed immediately.
Applicable process descriptions and operational documentation must be adapted if necessary.
The requirements of the regulations (see appendix A.1.5) must be followed.
Regular checks for vulnerabilities must be carried out.

8 IT service continuity management

Unpredictable or unexpected events that can lead to unreasonably long IT system failures and threaten business processes are collectively referred to below as IT emergencies.
Methods for identifying and evaluating critical IT business processes need to be developed to ensure business continuity as described in the regulations (see appendix A.1.12).

9 Compliance and compliance with obligations

For the use of IT systems on IT infrastructures, the protection guaranteed by the IT infrastructure in terms of confidentiality, integrity and availability must not be exceeded. If this cannot be ensured in exceptional cases, the IT system managers are obliged to find appropriate solutions together with the person responsible for the IT infrastructure so that an appropriate profitability is achieved.
When using encryption and/or electronic signatures (see appendix B.1.12), all country-specific regulations for the import and export of or access to hardware, software and information must be followed. This applies in particular to the use abroad.
If you have any questions about country-specific regulations, please contact the relevant organizational units (see appendix B.1.13).
All system operators must conduct random checks on their IT systems to verify compliance with security-related regulations and guidelines. The results shall be documented.
Methods and tools for system monitoring (e.g. audit functions of the operating system) shall be set up and used in accordance with the applicable approval procedure (see appendix B.1.14).
All system operators are obliged to close security gaps discovered in IT systems.
The requirements and activities in the context of audits must be carefully planned (especially for ongoing systems) in order to minimize the risk of disruption of business processes.
The following guidelines must be followed:

- The scope of the test must be defined and checked.
- For testing purposes, software and data may only be used with read access.
- IT resources must be identified and made available for testing.
- All procedures, requirements and responsibilities must be documented.

In order to prevent the misuse or compromise of audit tools, only authorized employees may use the tools for IT system audits.
The unlimited audit authorization of the audit department is not affected by this.

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.1.1).

Appendix

A General

A.1 Further documents

A.1.1 Information Security Regulation No. 03.01.01 Anti malware and system security

A.1.2 Information Security Regulation No. 03.01.05 IAM

A.1.3 Information Security Regulation No. 03.01.09 Exception process

A.1.4 Glossary Information Security

A.1.5 Information Security Regulation No. 03.01.08 Change and patch management

A.1.6 Information Security Regulation No. 03.01.16 Third party service delivery management

A.1.7 Information Security Regulation No. 03.01.06 Backup and archiving

A.1.8 Information Security Regulation No. 03.01.10 Awareness and training

A.1.9 Information Security Regulation No. 03.02.04 Network access

A.1.10 Information Security Regulation No. 03.02.02 Zoning and Segregation

A.1.11 Information Security Regulation No. 03.01.02 Cryptography

A.1.12 Information Security Regulation No. 03.01.14 IT service continuity management

The relevant documents can be found on the Group Information Security website: https://soco.volkswagen.com/wikis/pages/viewpage.action?pageId=3509813371

A.2 Feedback

Feedback or suggestions for improvement can be sent to the following e-mail address: VWAG R: WOB, IT Security Regulations itsr@volkswagen.de.

In order to be able to better assign the proposed changes, please provide the following information:

- number and name of the regulation
- chapter/subchapter
- reason for the amendment
- proposed amendment

All proposed amendments are evaluated in accordance with the process for the

creation, approval and publication of Volkswagen AG regulations.

A.3 Validity

This Information Security Regulation is valid immediately after publication. The updated content of this regulation must be implemented within a transitional period of six months.

Next inspection date: Feb 2025

A.4 Document history

Version	Name	Org.-unit	Date	Comment
1.0	K-SIS/G1	K-SIS/G1	May 25, 2004	Initial version
2.0	K-SIS/G1	K-SIS/G1	January 30, 2013	Update via GISSC Process
3.0	K-SIS/G1	K-SIS/G1	November 11, 2015	Update via GISSC Process
3.0a	K-FIS/G	K-FIS/G	March 14, 2019	C2.15: removed specific product
4.0	K-DS/G	K-DS/G	September 22, 2022	Update due to approval in K-DS management round
4.1	K-DS/G	K-DS/G	November 03, 2022	Additions in chapter 4.1.4 und 6.1
4.2	K-DS/G	K-DS/G	February 22, 224	Update due to approval in K-DS management round

B Company-specific characteristics

B.1 Company-specific characteristics

This chapter contains specific characteristics which are valid company-wide. These characteristics can be adapted to company needs. For information characteristics valid within the Volkswagen Brand are included in italics.

B.1.1 The responsible organizational unit for deviations from these guidelines that reduce the level of security is the respective information security organization of the brand or company. In general, the requirements of the exception process (see appendix A.1.3) must be observed.

B.1.2 Contact for Volkswagen AG via My.Serve: Service Catalog - Volkswagen Service Portal (service-now.com)

B.1.3 Programmable logic controllers (PLCs) and robot controllers must be operated in networks where only the communication required for operation is permitted.

B.1.4 Only the online version is valid:

https://soco.volkswagen.com/wikis/pages/viewpage.action?pageId=3509813371

Communication of changes:

- Viva Engage (Please subscribe if required)

- Mailing List (Please enter yourself)

B.1.5 For Volkswagen Brand documented in ORL 18.

B.1.6 Further information can be found in the Self Service Portal of Group Security K-SK-3: Cooperation with partner companies - Konzern Sicherheit - Group Wiki (volkswagen-net.de)

B.1.7 IT systems are complete IT systems with hardware and software components, including their two-way communication relationships.

B.1.8 Documentation must be archived in accordance with legal and departmental requirements. For instance, any documentation that is also indirectly related to accounting must be archived as per the "Generally Accepted Principles of Computerized Accounting Systems (GoBS)" for the system's lifetime and 10 years thereafter. Further details can be found in ORL 24 "Retention of documents": Regelungsportal

B.1.9 Responsibility: Group Information Security Organisation, e-mail: ITSG@volkswagen.de

B.1.10 The creation of personal logs must be approved by the responsible human resources department, the data protection office and the respective committees. The testing of performance and behaviour is not permitted.

B.1.11 Responsibility : IT system administrators and local administrators

B.1.12 The version or the correction status must be archived in accordance with legal and departmental requirements. For instance, any documentation that is also indirectly related to accounting must be archived as per the "Generally Accepted Principles of Computerized Accounting Systems (GoBS)" for the system's lifetime and 10 years thereafter. Further details can be found in ORL 24 "Retention of documents": Regelungsportal.

B.1.13 National legislation on the recognition of electronic signatures: In Germany, the Digital Signature Act (SigG) applies. The legislated general conditions for the use of electronic signatures in Germany are described therein. This law was adapted to conform to the EC Directive "Community Framework for Electronic Signatures" [ECRL99], dated December 13, 1999, and came into effect on May 22, 2001, as "Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations", thereby superseding the Signature Act of 1997. The legislation establishes the framework conditions that, when complied with, allow a qualified electronic signature to be considered at least as secure as a handwritten signature. It specifies in which instances qualified electronic signatures are considered equal to handwritten signatures as per the Signature Act. As a result, digital signatures as per the Signature Act are awarded a high level of security, even before a court.

B.1.14 Responsibility: Legal department

B.1.15 Audit requirements must be approved. The audit requirements are approved in writing by the appropriate personnel department, the data protection body, and the appropriate committees.

B.1.16 for instance, the application „Blancco"

B.1.17 Passwords for administrative accounts must be securely managed (e.g. password vault, rotation, CyperArc)

B.1.18 Allowed only in emergency situations and in collaboration with the work council and "Kommission Datenschutz.

B.1.19 The contents of storage media that are no longer needed must be reliably deleted by overwriting or physical destruction of the medium. For proper disposal, data carrier disposal bags for Volkswagen storage media are used, which are available from the secretariat (via the normal procurement process for office consumables). The secure deletion or scrapping of storage media is carried out by IT Client Support (https://volkswagen-net.de/wikis/display/SFWIKI/IT+Client+Support).

B.1.20 Data Protection Manager Organization (DSMO): Contact persons for your department can be found in the Data Protection Wiki. For further information see also: ORL 50 "Data Protection and Data Protection Governance"