VOLKSWAGEN GROUP

IS-Regulation 02.06

Guideline for third parties

Version: 5.1
Applicable as of: 29.06.2023

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 organizational requirements and rules for information security that must be followed by third parties when handling Volkswagen Group information. The terms information and data in this document refer exclusively to information and data of the Volkswagen Group.

Third parties are defined as contractual partners who provide services to the Volkswagen Group on the basis of contractual relationships. Subsidiaries and brands of the Volkswagen Group, as well as companies in which the Volkswagen Group holds majority stakes, are excluded from this definition.

1.1 Document structure and target group

This guideline is aimed at the management of third parties. The management of third parties must ensure that their employees and vicarious agents who process information of the Volkswagen Group are bound by this guideline.

This guideline does not apply to customers of a Volkswagen Group company.
This document contains four chapters. The following table lists the document structure and the respective target group per chapter.

Chapter	Target group
1	All third parties
2	Third parties working in the Volkswagen Group Infrastructure.
3	Third parties who have or provide access to Volkswagen information outside the Volkswagen Group infrastructure.

Depending on the cooperation model, a third party can belong to several target groups at the same time.

2 Area of application

These instructions apply to all third parties who process information classified as internal, confidential or secret for the Volkswagen Group in accordance with contractual agreements.

3 General requirements for all third parties

3.1 Classification of information

The purpose of the classification is to classify information in stages depending on its need for protection. Depending on the classification, different protective measures are required.

All Volkswagen Group information must be classified according to confidentiality. Confidentiality ratings may change at certain milestones.

If documents or information are prepared by the third party for the Volkswagen Group, the classification according to confidentiality must be requested from the contact person of the Volkswagen Group and marked accordingly.

3.2 Further requirements

- Information security events (e.g. malfunctions that occur, violations of the information security regulations, cyber attacks) concerning information or IT systems of the client must be reported immediately to the competent authority with the information required to assess criticality (see Annex B.1.1). Further information on the event must be made available to the client upon request.
- If an attack is suspected or detected using malware, the affected IT devices and storage media may no longer be used to process Volkswagen Group information.
- Suspected vulnerabilities and weaknesses of the client's IT systems must be reported immediately to the competent authority (see Annex B.1.1).
- If there is a suspicion of loss of internal, confidential or secret information of the customer, this must be reported immediately to the contact person of the commissioning Volkswagen Group company.
- The transfer of data or information to other third parties is only permitted with written approval by the owner of the information (see Appendix B.1.3).
- Documents and storage media with sensitive information of the Volkswagen Group must be protected against loss, destruction and confusion as well as against unauthorized access. As soon as the data on the storage medium is no longer required, the data must be deleted there securely (by overwriting seven times or by a degaußer). Storage media that are no longer required must be physically destroyed.
- In all conversations and data transmissions (including telephone calls, video and web conferences) that concern or contain confidential or secret information of the Volkswagen Group, it must be ensured that they cannot be overheard or read without authorization.
- Confidential or secret information may not be used as part of file names or in email subject lines.
- Error-free processing of information and protection against unauthorized changes must be ensured.

4 Additional requirements for third parties working in the Volkswagen Group infrastructure

4.1 Definition

A third party works in the Volkswagen Group Infrastructure if:

- IT equipment (physical or virtual end devices) are provided by a Volkswagen Group company, or
- the connection via remote access solutions with access to the internal group network or
- the third party is connected directly to the internal Group network or
- when access-protected applications of a Volkswagen Group company provided via the Internet are used. This does not apply to applications that are used by the user in his role as an end customer.

This applies regardless of whether the third party is located on the premises of a Group company.

4.2 Requirements

- Regulations of the respective Group company regarding the bringing of IT equipment not belonging to the respective Group company to the company premises or in security areas must be complied with.
- IT equipment provided by the respective Group company must be treated properly and protected against loss or unauthorized alteration.
- The manufacturer's regulations for the protection of IT equipment must be complied with.
- The IT equipment provided by the respective Group company may only be taken from the factory premises of the Group company after approval has been granted.
- The provision or installation of hardware and software may only be carried out or initiated by the department of the Group company responsible for them.
- With regard to the use of the hardware and software provided by the respective Group company, the regulations of the respective Group company apply
- Only the use of hardware, software and storage media provided by the respective Group company is permitted. Exceptions can be discussed in individual cases with the responsible contact person in the commissioning department of the Group company. Exceptions for the purpose of access to the Group network, remote access or mobile working are described in Chapter 2.4.
- Opening the IT equipment provided by the respective Group company and making changes to the hardware (e.g. installing/removing components) and changing security settings (e.g. in the web browser) is only permitted to the responsible authorities of the Volkswagen Group. The removal of usage restrictions (e.g. "jailbreaking" or "operating system rooting") is not permitted.
- The use or subsequent modification of programs of the respective Group company is only permitted if this has been approved by the responsible contact person in the commissioning department of the Group company.
- No data of other customers who do not belong to the Group may be processed on the IT equipment provided by the respective Group company.
- Each third party is responsible for ensuring that information, programs and IT equipment are only properly used and used within the scope of the respective task.
- The sending of non-official information is not permitted.
- The use of private software and data on the IT equipment provided by the respective Group company is not permitted.
- The use of IT equipment or data of the respective group company by employees of the third party requires the express consent of the respective group company. The respective Group company is authorized to prohibit access or use at any time (e.g. in the event of misuse).
- Hardware that is no longer required (e.g. laptop, smart cards, SecurID tokens, USB sticks, USB disks) and software must be returned to the respective Group company immediately, but at the latest at the end of the contract.
- Repairs of IT equipment provided by the Group company may only be caused by the Group company.
- The loss of hardware provided by the Group company must be reported

immediately by the corresponding user to the responsible contact person in the commissioning department of the Group company.

- The storage of non-publicly classified company-owned data is only permitted on approved storage media (e.g. shared file or cloud storage services).
- The collection, processing or use of personal data (e.g. name, telephone number, e-mail address, date of birth) is only permitted if
  - there is a consent of the data subject (individual) or
  - there is a legal basis for this.
- Personal data stored in a group company may only be processed and used within the framework of the contractually agreed activities. A transfer of this data to unauthorized persons is not permitted.
- IT devices and data carriers on which personal, confidential or secret data is stored may only leave Volkswagen Group properties in encrypted form.

4.3 Handling with classified information

Information may only be made available to an authorized group of persons for the purpose of the agreed activities and in compliance with the relevant regulations. The need-to-know principle must be followed.

In order to protect internal, confidential or secret information, the relevant IT equipment shall be set up in such a way as to prevent unauthorized access and minimize the risk of access by unauthorized persons.

Information must be protected from access by unauthorized persons throughout its lifecycle in accordance with its current level of confidentiality. The following regulations apply:

Classification	Requirements
Public	• Marking: none/optional (e.g. note in the imprint) • Reproduction and distribution: no restrictions • Storage: no restrictions • Disposal: no restrictions
Internal	• Marking: Indication of the confidentiality level "Internal" or "Internal" on the first page of the document • Reproduction and distribution: only to authorized employees of the Group and authorized third parties within the scope of the activity or the scope of application • Storage: Protection against unauthorized access • Disposal: According to ISO/IEC 21964, protection class 1

Confidential	• Marking: Indication of the confidentiality level "Confidential" or "Confidential" on each page of the document • Reproduction and distribution: only to a limited group of authorized employees of the Group and authorized third parties within the scope of the activity and scope of application. The person distributing the information is responsible for appropriate distribution channels to protect the information and data from unauthorized access and/or eavesdropping (e.g., using encryption). • Storage: Access only for a limited group of authorized employees of the Group and authorized third parties within the scope of the activity and the scope of application (e.g. by closed user groups). Appropriate storage media shall be used. • Disposal: According to ISO/IEC 21964, protection class 2 • Transport/Shipping: Confidential documents and storage media must be sent in sealed, neutral envelopes. If necessary, the addition "personal" can be added. This means that the envelope may only be opened by the addressed person. • Printing: Printout only under the supervision of the printing person

Secret	• Marking: Indication of the confidentiality level "Secret" or "Secret" on each page of the document • In addition, all pages must be marked with "page x of y". • Reproduction and distribution: only to an extremely limited group (e.g. list by name) of authorized employees of the Group and authorized third parties within the scope of the activity or scope of application and with the prior approval of the information owner. All data must be encrypted. Depending on the application, further technical or organizational protective measures must be used (e.g. prohibition of forwarding and printing, watermarks). Suitable media must be used for communication that prevent eavesdropping (e.g. encrypted video conferences). • Storage: Access only for an extremely limited group (e.g. list by name) of authorized employees of the Group and authorized third parties within the scope of the activity and the scope of application (e.g. by closed user groups). All data must be encrypted. • Disposal: According to ISO/IEC 21964, protection class 3 • Transport: Secret documents and storage media must be sent in neutral, sealed outer envelopes (without additions such as "personal, secret, etc."). A second inner envelope must be placed in these, which is marked with the classification "secret". Secret documents or electronic storage media may only be taken from the premises of the company by employees who are authorized to do so in writing by their respective manager. • Printing: Printout only under the supervision of the printing person

The requirements for handling information (labelling, duplication, distribution, storage and disposal) also apply to IT systems (e.g. databases and backup media). In particular, no public Internet translation services may be used for translations of documents containing information from the Volkswagen Group.

4.4 Handling of user accounts

The following requirements when dealing with user accounts and passwords must be followed by all users:

- The use of another person's user account is not permitted.
- User accounts or access authorizations that are no longer required must be reported immediately to the responsible contact person in the commissioning department of the Group company so that they can be deleted or blocked.

- The transfer of means of authentication (e.g. smart cards, authenticator apps and tokens) is not permitted.
- Authentication devices that are no longer required must be returned immediately to the responsible contact person in the commissioning department of the Group company.
- Passwords and PINs of a user account intended for personal use may not be shared or shared.
- As soon as there is a suspicion of compromise or disclosure of a password or PIN, this or more must be changed immediately.
- Passwords or PINs are classified at least confidentially.

To set a password or PIN, the following requirements must be met:

- A separate password must be used in each IT system that uses its own password.
- In particular, it is not permitted to use a password used for business purposes for private purposes.
- Trivial passwords (e.g. "Test12345678") or passwords with a personal reference (e.g. name, date of birth) are not permitted.

4.5 Use of network services

Network-capable devices provided by the Volkswagen Group Company may only be connected to networks outside the company (e.g. hot spot, private WLAN, mobile radio) if this procedure has been explicitly approved by the Group company for the respective device.

The connection of network-capable devices to the Group network is only permitted if this procedure has been explicitly approved for the respective device by the Group company.

4.6 Additional requirements for mobile work

The employees of the third party are responsible for ensuring that the relevant regulations on data and information security as well as data protection during mobile work are fully complied with. Work documents, data and information must not be visible and accessible to unauthorized persons in public places or in private rooms and must not be intercepted. In addition, protection against recordings by speech recognition devices must be ensured.

In principle, secret information may not be processed during mobile work.

The connection of hardware (e.g. mouse, keyboard, USB sticks) to the hardware provided by the Volkswagen Group company is only permitted if it has been provided by the Volkswagen Group company.

Image output devices (e.g. monitors, projectors) that have not been provided by the Volkswagen Group company can be used if the connection is wired and no radio transmission is used.

Headsets and hands-free systems not provided by the Volkswagen Group company may only be connected via the headphone/microphone input, but not via USB.
IT equipment provided by the respective Group company must be physically

protected against theft and misuse:

- If an IT device is left unattended in a motor vehicle, this must be done in such a way that it is not visible from the outside.
- On air and rail travel, IT equipment must be transported in hand luggage.
- If an IT device is unattended for a long time, it must be turned off.

5 Additional requirements for third parties who have or provide access to Volkswagen Group information outside the Volkswagen Group infrastructure

5.1 Definition

A third party then has access to information of the Volkswagen Group outside the Volkswagen Group infrastructure when this Volkswagen Group processes information in its own IT infrastructure or hosts it for the Volkswagen Group or other third parties on behalf of the Volkswagen Group.

5.2 Requirements

The regulations for information security of the third party apply, unless otherwise contractually agreed.

Responsibilities

Violations of this guideline will be examined individually in accordance with valid legal and contractual provisions and punished accordingly.

Deviations from this guideline that impair the security level are only permitted after consultation with the contact person of the Volkswagen Group company and must always be limited in time.

Appendix

A General

A.1 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.2 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: Jun 2024

A.3 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, 2004	Revised by GISSC Process
3.0	K-SIS/G1	K-SIS/G1	November 11, 2015	Revised by GISSC Process
4.0	K-FIS	K-FIS	August 7, 2018 (review 2.4.19)	Adjustment regarding VDA ISA
5.0	K-DS/G	K-DS/G	September 22, 2022	Revision by regulation team and approval by K-DS management
5.1	K-DS/G	K-DS/G	June 29, 2023	Revision by regulation team and approval by K-DS management

B Company-specific characteristics

B.1 Company-specific characteristics

B.1.1 CERT VW - via Enterprise Help Desk (EHD, Tel. +49 531 9 33000, <EHD@volkswagen.de>)

B.1.2 Information security and IT security requirements (volkswagen.de)

B.1.3 The information owner (e.g. head of the organizational unit) is responsible for the classification and compliance with the protection objectives (confidentiality, integrity, availability) in his own area.