Information Security Guidelines for External Companies

Valid from:	25.05.2004	Status:	Published
Revised:	25.07.2018	Version:	4.0
Issued by:	I/GG-81, Datenschutz- / Datensicherheits-management, Office des DSB	Regulation No.	02.06

Scope
These guidelines apply to any third party company (hereinafter referred to as suppliers) that is providing services to the AUDI AG based on contractual relationship.

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

Table of Contents

I. Purpose

These Information Security Guidelines comprise the information security regulations that suppliers must observe when using information and/or IT devices (e.g. personal computers, workstations and mobile devices) of the ordering party.

Suppliers are defined as any third party companies that are providing services to the Volkswagen Group based on a contractual relationship. Subsidiary companies, Brands of the Volkswagen Group and companies that are majority owned by the Volkswagen Group are excluded from this definition. These guidelines are aimed at the suppliers' management, employees and relevant sub-contractors. This group is hereinafter referred to as the "contractor".

The Information Security Guidelines protect the confidentiality, integrity and availability of information and the rights and interests of the ordering party and all natural persons and legal entities that maintain a business relationship with the ordering party and/or perform work for it.

The responsibilities of the Group Auditing department are not covered within this regulation.

I.I Document Structure and Target Audience

The document contains three chapters. The following table lists the document structure and the target audience for each chapter.

Chapter	Target Audience	Notes
1	All Suppliers	The requirements of this chapter must be observed by all suppliers. Additional requirement are contained in chapters two and three, depending on the type of access to the Group network or systems
2	Suppliers that have access to the Group network or systems	Additionally, the requirements contained in chapter 1 must be observed
3	Suppliers that do not have access to the Group network or systems	Additionally, the requirements contained in chapter 1 must be observed

1. Basic Requirements

The following requirements must be observed by all suppliers within the scope of this document.

Requirements for the ordering party are not within the scope of this document

1.1. Organizational requirements

Regulations of the respective Group Company on bringing IT devices that do not belong to the ordering party on the companies' premises or secure areas must be observed.

Usage of software or data belonging to the ordering party on IT systems or storage devices that are not provided or approved by either the ordering party or the supplier is not permitted.

Usage of software and data belonging to a Volkswagen Group Company on file-services or internet cloud-services that are not approved by the ordering party is not permitted.

The distribution of data to third parties is only permitted with written approval by the data owner of the ordering party.

The regulations of the ordering party for usage, storage and any processing of personal data (see appendix, B.1.1) must be observed.

Employees of the contractor must be obligated by their company management to non-disclosure in accordance with the non-disclosure agreement between the contractor and the ordering party. The ordering party may inspect these agreements at any time.

If data of the ordering party is stored on mobile systems or IT devices it must be encrypted using current state of technology hardware or software. Additional requirements for encryption and authentication can be found on the Group Suppliers Portal[1].

Before travel abroad, the country specific regulations for use of security technologies (e.g., encryption) must be observed.

After end of the contract, data of the ordering party must be handed over and deleted on the devices and storage media of the supplier. Legal requirements (e.g. retention periods) must be observed.

1.2. Human resources security

A user ID that is no longer needed or access authorization that is no longer needed for access to data of the ordering party must be reported promptly to the ordering party and responsible units (e.g. responsible user administrator of the ordering party), so that the corresponding Blocking/Deletion can occur.

Identification media that is no longer needed (e.g., Smartcards, SecurID cards) must be returned immediately to the ordering party.

Allocated devices (e.g. laptops), data and storage media must be returned to the ordering party when they are no longer needed or at the end of the assignment.

The loss of IT devices or media for authentication must be immediately reported to the responsible unit of the ordering party (see appendix, B.1.2).

1.3. Physical and environmental security

IT devices that store or process data of the ordering party must be used in a way that prevents unauthorized persons to view or access this data. Special care must be taken when using mobile devices.

Confidential and secret documents must not be left unattended to prevent unauthorized viewing.

1.4. Asset management

1.4.1. Classification guidelines

Classification includes the three security objectives confidentiality, integrity and availability and must be carried out for all information and IT Systems processing information.

The supplier must request the confidentiality, integrity and availability classification from the ordering party (for the scope of the services or work provided).

Information (security objective confidentiality) must be protected from unauthorized access throughout its entire life cycle in accordance with measures required by its confidentiality classification. Confidentiality classification may include an expiration date.

For processing data the classification for integrity and availability must be examined and determined by the respective process owner, if necessary. This classification must be evaluated regularly and adapted if necessary.

Correctness of the classification must be confirmed by the Information Owner.

1.4.1.1. Confidentiality

Information that is not intended for general publication must be made accessible only to those who are authorized to access it (Need to Know Principle).

[1] http://www.vwgroupsupply.com

Requirements for information creators and information owners:

- Newly created information and data must be labeled by the creator[2]
- The information owner[3] is responsible for the classification.
- The creator must request the correct classification from the information owner.
- Confidentiality classification must be defined for all IT systems.
- If the classification is currently unclear, for example, because the document / IT system was just newly created, the classification "Confidential" must be used.
- The Information owner must check the confidentiality classification for internal / confidential / secret information (at the latest during next revision or update) if the classification is still correct and label the information accordingly.

Requirements for the recipient:

- Unlabeled information and data is defined as internal.
- The information owner must be contacted if there are any doubts about the correctness of the classification.

The following classification levels for information with regard to requirements for confidentiality are defined:

Classification	Definition
Public	Information that is not subject to any restrictions and, e.g., can be published by the company in newspapers or in the internet. The public use of company information requires the approval of the responsible unit (see appendix, B.1.3). Examples: press releases, product catalog for customers
Internal	Unauthorized knowledge, sharing or usage of this Information only has minor influence on reaching product or project targets. Therefore, this information can be made accessible to an eligible group of persons. Loss of confidentiality may have consequences, albeit of a minor nature; for example: • claims for damages by individual persons or organizations are unlikely Examples: business communication data (e.g. phone number, mail-address), occupational safety specifications, work regulations
Confidential	Information whose knowledge or disclosure to unauthorized persons could jeopardize the achieving of product and project objectives and must therefore only be made accessible to a limited group of authorized persons. Consequences in the event of loss of confidentiality are probable and measurable, e.g.: • loss of customers • downturn in sales figures/turnover • claims for damages by individual persons or organizations Examples: personal data, that are above business communication data (e.g. salary) budget plans, revision reports

[2] Definition: See A.2
[3] Definition: See A.2

Secret	Information whose knowledge or disclosure to unauthorized persons could seriously jeopardize the achieving of company objectives and must therefore be subject to a highly restrictive distribution list and strict controls. Violation of confidentiality has considerable effects on the image/the appearance of the company and/or economic consequences, e.g.: • considerable loss of customers • sharp declines in sales figures/turnover • claims for damages by numerous persons or organizations • exclusion from certain markets • negative effects on public standing Examples: special types of personal data (e.g. health information), cycle plans, plans about the company's strategy, design picture of prototypes

1.4.1.2. Integrity

Error-free information processing and protection against unauthorized changes must be ensured.

The following classification levels for information with regard to requirements for integrity are defined:

Classification	Definition
Low	A violation of integrity has no foreseeable effects on the business activity or on the image/appearance of the company.
Medium	A violation of integrity has only a minor impact on business activity and/or the image/appearance of the company. Consequences are possible, but minor in nature; for example: • Minor delays in work processes • Errors/faults do not affect work results (no production downtimes) • Decisions are not negatively affected • Claims for damages by individual persons or organizations are unlikely Examples: location plans, organization charts, and individual internal phone numbers
High	A violation of integrity has perceivable effects on the business activity and/or on the image/appearance of the company. Consequences are probable and measurable, e.g.: • loss of customers probable • downturn in sales figures/turnover probable • definite delay in work sequences • faults/malfunctions have a perceptible effects on work results (high production downtimes) and/or a few service processes fail • decisions are negatively affected/incorrect decisions are probable • claims for damages by individual persons or organizations are probable Examples: JIT orders, press releases, contents of the Internet presence, data for production control

Very high	A violation of integrity has considerable effects on the business activity and/or on the image/appearance of the company with corresponding consequences, e.g., • considerable loss of customers • claims for damages by numerous individual persons or organizations • sharp declines in sales figures/turnover • exclusion from certain markets • considerable delays in work sequences • faults/malfunctions have severe effects on work results and/or several service processes fail (very high production downtimes) • decisions are seriously negatively affected/incorrect decisions Examples: financial reporting (e.g., annual financial statement), patents, cryptographic keys, payroll

1.4.1.3. Availability

Information must be made available within an agreed time frame.

The following classification levels for information with regard to requirements for availability are defined:

Classification	Definition
Low	The availability of the IT system can be less than 95 percent regarding failure or unacceptable response time without resulting in significant damage (financial or to the image of the company). Example: Intranet application containing general information for employees
Medium	The availability of the IT system must be at least 95 percent regarding failure or unacceptable response time. Lower availability will lead to significant damage (financial or to the image of the company). Example: Applicant portal
High	The availability of the IT system must be at least 98 percent regarding failure or unacceptable response time. Lower availability will lead to significant damage (financial or to the image of the company). Examples: Payroll, bookkeeping
Very high	The availability of the IT system must be at least 98 percent regarding failure or unacceptable response time. Lower availability will lead to significant damage (financial or to the image of the company). Example: IT system, whose failure will result in an immediate production halt. Significant damage is, for example: • Loss of customers • Claims for damages by numerous individual persons or organizations or associations • Sharp declines in sales figures/turnover • Exclusion from certain markets • Faults/malfunctions have severe effects on work results and/or several service processes fail (very high production downtimes)

1.4.2. Information labeling and handling

Information must only be made accessible to the authorized group of persons. This is only permissible in the scope of the tasks agreed on and with compliance to existing regulations. The "Need to know" principle must be applied.

Information must be protected against access by unauthorized persons according to its current confidentiality classification during the entire life cycle. The following regulations apply:

Classification	Requirements
Public	• Labeling: none / optional (e.g. in imprint) • The corporate design guidelines regarding the position of the classification label must be observed • Duplication and distribution: no restrictions • Storage: no restrictions • Deletion: no restrictions • Disposal: no restrictions
Internal	• Labeling: Confidentiality level in national language/none or Internal on the first page of the document. • The corporate design guidelines regarding the position of the label must be observed • Duplication and distribution: only to authorized group employees and authorized third parties within the task or application area • Storage: protection against unauthorized access • Deletion: data that are no longer needed must be deleted. • Disposal: proper disposal (see appendix, B.1.4)
Confidential	• Labeling: Confidentiality level in national language/confidential" indicated on each page of the document in electronic and printed form • The corporate design guidelines regarding the position of the label must be observed. • Duplication and distribution: Only to a limited range of authorized group employees and authorized third parties within the task and application area. The person distributing the information is responsible for using suitable distribution routes, in order to protect the information and data from unauthorized access and/or unauthorized overhearing (e.g., encryption). • Storage: only accessible to a limited range of authorized group employees and authorized third parties within the task and application area (e.g., by closed user groups). Suitable storage locations and/or storage media must be used. • Confidential documents must be stored in locked steel furniture or in rooms that are locked when they are not in use and which can only be opened by a restricted group of people. • Deletion: data that are no longer needed must be deleted. • Disposal: proper disposal (see appendix, B.1.4) • Authentication: Strong Authentication (see appendix, B.1.5) • Transportation: Confidential documents and storage media must be sent in sealed neutral envelopes; if appropriate “personal” may be added, meaning that the documents can only be handed to the named recipient.

Secret	• Labeling: Confidentiality level in national language/Secret" indicated on each page of the document. • The corporate design guidelines regarding the position of the label must be observed. • Also, each page must indicate page x of y. • Duplication and distribution: Only to an extremely limited range (e.g., list of names) of authorized group employees and authorized third parties within the task or application area after prior approval by the information owner. If technically possible data has to be encrypted according to the current state of technology. Comparable security solutions have to be used if this is not possible. Additional case-related technical or organizational protective measures must be implemented (e.g., denying forwarding or printing, watermarks). Suitable communication media must be used in order to prevent listening in (e.g., encrypted video conference). • Storage: only accessible to an extremely limited range (e.g., list of names) of authorized group employees and authorized third parties within the task or application area (e.g., by closed user groups). If technically possible data must be encrypted according to the current state of technology. Comparable security solutions have to be used if this is not possible. • Secret documents must be stored in locked steel furniture locked with different locks to the standard locks. Mobile Storage devices with secret information must be stored in appropriate data safes. • Deletion: data that is no longer needed must be deleted • Disposal: proper disposal (see appendix, B.1.4) • Authentication: Strong Authentication (see appendix, B.1.5) • Transportation: Secret documents and storage media must be placed in a closed neutral outer envelope (no additions such as “personal”, “secret”, or similar) with another inner envelope labelled “secret” inside. In the inner envelope must be the secret content.

The regulations for handling information (labeling, duplication, distribution, storage, deletion and disposal) also apply to IT systems (e.g., for databases, backup media).

1.4.3. Media handling

Data media (e.g., CDs, DVD, USB sticks, hard drives) must be secured against loss, destruction, and mix-ups, as well as against access by unauthorized parties.
Data media that are no longer needed must be sent to secure disposal (see appendix, B.1.4).

1.4.3.1. Exchange of information

During all discussions of confidential or secret information, including telephone calls and web- or video conferences, it must be ensured that these cannot be overheard without authorization.

Fax numbers and e-mail addresses must be taken from current communication directories or requested from the recipient to prevent data from being transferred incorrectly.

For transport of IT devices and data media beyond the plant boundaries of the ordering party, the regulations and operating agreements of the respective group company must be observed (see appendix, B.1.6).

As the originator of an e-mail, the author is responsible for the content and distribution; the receiver for further processing and further distribution of an e-mail.

The creation and sending of chain letters is not permissible.

1.5. Information Security Incident Management

Information security events (e.g., vulnerabilities, violations of the Information security regulation) concerning data or systems of the ordering party must be reported immediately to the responsible unit (see appendix, B.1.7).

Suspected vulnerabilities and weak points concerning IT systems of the ordering party must be reported to the responsible unit (see appendix, B.1.8). Testing of vulnerabilities and weak points (e.g. penetration testing) must only be performed by the responsible unit (see appendix, B.1.9).

Any suspected loss of confidential or secret information must be reported to the responsible unit (see appendix, B.1.10) immediately.

1.6. Compliance

Compliance Management observing legal and organizational requirements (including resource management, internal control system, IT continuity management and protection of information) must be implemented by the supplier covering all information, hard- and software of the ordering party.

The compliance management must include the following aspects.

1.6.1. Early detection of risks

A process for early detection of risks and potential threats to IT systems and data must be in place.

Preventive action and measures must be taken to mitigate detected risks.

1.6.2. Intellectual property rights / License Management

Intellectual property rights (e.g., copyrights for software, documents, and other image material, rights to drafts, trademarks, patents, and source code licenses) must be observed.

Usage of unlicensed software (pirate copies) is not permitted.

License software is subject to legal provisions for copyright protection (e.g., the reproduction of software, except for backup and archiving purposes, represents an infringement of copyright). Infringements of these provisions may lead to penal measures as well as injunctive relief and damage claims.

Company specific regulations must be observed (see appendix, B.1.11).

License software must only be used for the agreed purpose and exclusively in compliance with existing provisions and the license agreements entered into with the manufacturer.

1.6.3. Data protection

The respective national laws and regulations for data protection (see appendix, B.1.12) must be complied with.

Contractors must be obligated by the management of the supplier company to comply with the legal requirements concerning data protection (see appendix, B.1.12).

1.6.4. Contractual compliance

The Supplier‘s IT organization must be in compliance to the contractual requirements of the ordering party. Measures must be implemented to ensure that the suppliers own organizational regulations are reviewed and updated according to the current contractual requirements.

1.6.5. Policies and Regulations

The supplier must provide policies and regulations to its employees to ensure compliance with the requirements and adequate handling of information, hard- and software of the ordering party.

1.7. Violations and Enforcement

Violations of the information security guidelines must be followed up individually as per applicable operational, contractual and legal regulations or agreements and sanctioned appropriately.

2. Additional requirements for suppliers with access to the internal Group network

2.1. Definition

The following requirements must be observed by all suppliers belonging to one of the following categories:

- Are provided with clients owned by a VW Group Company
- Are connected via Remote Access (e.g. TravelX, Safe, Secure i.Do-Client) or other VPN-Solutions with access to the Volkswagen Corporate Backbone (CBB)
- Are connected directly to the Volkswagen Corporate Backbone (CBB)
- Are connected to the Volkswagen Corporate Backbone (CBB) via PFN (CSN)

These suppliers may be located on the premises of the Group Company or on their own companies' premises.

2.2. Requirements

2.2.1. Internal organization

Suppliers must only request or initiate procurement and installation of hardware and software via the organizational unit (business department of the ordering party) that is responsible for them.

The use of the provided hardware and software is subject to the regulations of the respective group company (see appendix, B.1.13).

Only the responsible units are permitted to open the IT device, make changes to the hardware (e.g., installation/removal of hard drives and memory modules), and make manual changes to security settings (e.g., browser settings) (see appendix, B.1.14).

The use or subsequent modification of programs is only permissible with the authorization of the responsible units (see appendix, B.1.14).

Data of any other customer that does not belong to the Volkswagen Group must not be processed on the provided IT devices.

The use of IT devices and data of the ordering party by employees of the supplier requires the express consent of the ordering party. The ordering party is entitled to prohibit access/use at any time (e.g., in cases of misuse).

2.2.2. Physical and environmental security

The provided devices must be handled correctly and protected from loss or unauthorized modification.

The manufacturer's regulations on the protection of devices must be complied with.

Devices provided by the ordering party (e.g., laptops, cellular phones) may only be taken outside of the plant of the ordering party after approval.

2.2.3. Protection against malicious and mobile code

IT devices and data storage devices that are suspected of being infected with malware must not be used any further. The responsible unit (see appendix, B.1.7) must be informed immediately.

2.2.4. Backup

Data should be stored on the assigned storage systems and not on the local hard drive, since a central and automatic data backup is only ensured this way.

The user himself/herself is responsible for backing up data that is not stored on a central network storage (e.g. local hard disks, mobile data storage devices) or systems with similar functions (e.g. eroom, sharepoint, …).

Backup media and data must be handled the same way as the original data.

2.2.5. Access control

2.2.5.1. User responsibilities

The following requirements must be observed by all users:

General Requirements

- Usage of another person's user ID or account is not permitted.
- Passing identification media (e.g., Smartcards, SecurID cards) to somebody else is not permissible.
- Passwords or PINs of a user ID assigned for personal use (defined as "person-related user ID") must not be shared or disclosed.
- Keeping a record (e.g. on paper, in mobile devices or in files) must be avoided unless these are considered as a secure method (see appendix, B.1.15).
- Passwords or PINs must be changed immediately whenever there is any indication that those are compromised or became known.
- Temporary passwords (e.g. for new accounts) must be changed at the first log-on
- Password or PINs must be changed at first use and then at least every year. The change interval does not apply to PINs.
- Spying out passwords is not permissible.
- Passwords must at least be classified as confidential.
- If passwords have to be stored in written form, they must be stored by the employee in a sealed envelope at a suitable location that is protected against unauthorized access (e.g., safe) and be updated each time the password is changed. The sealed envelope must be signed by the respective employee. The persons authorized to open the envelope must be listed on it by name. In exceptional cases (e.g., in case of illness) it may be necessary to use the stored password. This must be done according to the "two-man rule". Each opening must be documented and reported to the employee. After each opening, the employee must change the password promptly and deposit it again. IT systems offering a functionality that matches these requirements are also permissible (e.g., electronic password safe).
- When leaving the system during ongoing operation (e.g., break, meeting), the user must activate a system lock (e.g., password-protected screen saver).
- Employees who use their multifunction badge to log on to IT systems must remove the badge from the reader when leaving the system.

2.2.5.2. Password Generation

During password generation, the following minimum requirements must be observed:

- Employees must not generate identical passwords for business and non-business purposes
- Employees must not generate identical passwords for VW group provided systems and systems, provided by 3rd parties, e. g in the Internet (applications, registration services, …)
- Users must observe the minimum password length enforced by the system. These are defined in the password policy[4].
- Simple passwords (e.g. “Test123456”, “123456abcde”) or context-specific words (e.g. personal related topics like name, date of birth) must not be used.
- If higher password complexity is demanded by specific systems or applications (as defined in the password policy[4]) the enforced complexity must be used.
  Hint: Use mnemonic verses or abbreviations and falsifications of mnemonic verses (e.g. mnemonic verse: “In the morning I get up early and brush my teeth” results in a password of: “Itm1guE&bmT”). The examples listed here must not be used as passwords.
  Alternatively, a combination of four randomly selected words (e.g. “SunWoodTeaTime”) results in a very strong password and is easy to remember. The examples provided here must not be used as passwords.

2.2.5.3. PINs for unlocking Smartphones and Tablets

The same requirements as defined in chapter 2.2.5.2 must be observed.

2.2.5.4. PINs for Smartcards for Authentication

The same requirements as defined in chapter 2.2.5.2 must be observed.

2.2.5.5. Collective User IDs

Reuse of specific collective user IDs by various persons (e.g., training participants, interns, graduating students) is permissible if the following requirements are observed.

- The assignment of the user IDs must be managed by a responsible person. This person must provide written verification of who used which user ID, and when. This person must archive this verification.
- Receipt of the user ID must be confirmed in writing by the respective user. The confirmation is retained by the person responsible for the user ID.
- During receipt of the user ID the password must be changed by the respective user into a password only known to him/her.
- During return of the respective user ID, the password must be changed by the responsible person to a password only known to him/her.
- The company specific archiving periods must be complied with for archiving the verifications.

User IDs that can be used simultaneously by several persons (so-called "group IDs") are not permissible unless exclusively applications can be started up with this user ID that have a separate user management including a personal authentication or only allow read access.

[4] Information Security Regulation 03.01.05 Authentication and IAM

2.2.6. Network and access control

2.2.6.1. Policy on use of network services

An IT device provided by the ordering party must only be connected to networks (exempt mobile communications network) outside the company (e.g., hot spot, private WLAN) in order to set up a connection with the Group network. Direct surfing etc. is not permitted (exempt with mobile communications networks connected smartphones and tablets).

If no longer required, the connection must be disconnected.

2.2.6.2. Equipment identification in networks

The unrestricted connection of communication devices (e.g. without firewalls) to the internal network (Intranet) is only permitted if these are made available by the Group or by companies in which the Group or one of its companies is a majority shareholder.

3. Additional requirements for suppliers without direct access to the internal Group network

3.1. Definition

The requirements contained in chapter 3 must be observed by all suppliers that fall in one of the following categories:

- The supplier does not have direct access to the network of a Group Company
- The supplier is not provided with clients owned by a VW Group Company and only uses clients owned by its own company.
- Is not connected via Secure Partner, remote access or any VPN solution.
  - Virtual Desktop solutions only permitting transfer of display and control data are excluded from this definition and may be used. For those the requirements defined in this chapter apply.
- The supplier is interchanging data with Audi

These suppliers are located on the premises of their own companies and obliged to follow the regulations of their own company.

3.2. Requirements

3.2.1. Internal organization

Group company data must be separated from the data of third parties (e.g via rights management) and especially from data of other customers of the supplier. It must not be accessible (e.g. implementable via encryption) by other 3rd parties.

The Audi classification must be mapped to classification schemes of the supplier to ensure that all required security measures are fulfilled.

The supplier must map the information security requirements of the regulations received within the scope of his tasks to appropriate security measures in the suppliers own company.

Only employees with a need to know must be able to access data belonging to the ordering party.

II. Responsibilities

This regulation must be observed by all suppliers as defined in the scope of this document.

Deviations from this regulation, that reduce the security level, are only allowed temporarily and after consultation with the responsible unit (see appendix B.1.16) and the ordering party.

Appendix

A General

A.1 Validity

This information security regulation is valid immediately after publication.

Next inspection date: November 11, 2018

A.2 Abbreviations and Definitions

Abbreviation/Term	Explanation
Information Creator	The information creator is the person or group of people creating an information or document. The creator must classify/label the document or information in accordance to the classification level determined by the information owner.
Information Owner	The information owner is the person or group of people who have been identified by management as having responsibility for the maintenance of the confidentiality of that information. The information owner may change during the lifecycle of the information.

A.3 Document History

Version	Name	OE	Datum	Bemerkung
2.0	Fröhlich	I/GA-2	12.03.2013	Approved version
3.0	Fröhlich	I/GG-81	24.10.2016	Revision
4.0	Fröhlich	I/GG-81	25.07.2018	Renaming of the IT security regulations in Information security regulations; reorganization security goals; new regulation for authentication

B Specific Characteristics

B.1 Company specific

B.1.1 The collection, processing or usage of personal details (e.g. name, phone number, e-mail address, date of birth) is only permissible provided that

- the consent of the party involved (individual) has been obtained or
- there is a legal basis for it.

The handling and usage of personal data stored at Audi is only allowed to act within the scope of ones duties. An transmission of these data is not allowed to unauthorized third person (e. g. customers, external employees, employees).

In principle, communication devices and data media, on which personal, confidential or secret data of the ordering party are stored, may only leave the AUDI AG site in an encrypted form.

B.1.2 Audi ServiceDesk, Tel. 0049 841 89 36565

B.1.3 Responsibility: unit Kommunikation Audi

B.1.4 Personal related, confidential and secret paper documents must be disposed of in secure way (e. g. document containers). Data carriers that are no longer needed must be deleted reliably by overwriting or be physically destroyed.

B.1.5 For internal, confidential or secret data of the ordering party the following authentication methods are permitted:

Authentication class	Data classification	Description
Strong authentication	Secret or Confidential	2 of 3 (knowledge, possession, quality criteria), e. g.: Authentication via VOLKSWAGEN PKI Card with PIN without a time component or biometric component One-Time-Password Token (e.g. SecurID card) with PIN-Pad One-Time-Password Token (e.g. SecurID card) without PIN-Pad with PIN-request
Weak authentication	Internal	1 of 3 (knowledge, possession, quality criteria), e. g.: One-Time-Password Token (e.g. SecurID card) without PIN-Pad without PIN-request Software certificate with/without passphrase central defined User-ID with password

B.1.6 In principle, communication devices and data media, on which personal, confidential or secret data of the AUDI AG are stored, may only leave the AUDI AG site in an encrypted form.

B.1.7 Audi ServiceDesk, Tel. 0049 841 89 36565

B.1.8 Audi ServiceDesk, Tel. 0049 841 89 36565

B.1.9 It-sec@audi.de

B.1.10 informationssicherheit@audi.de

B.1.11 Copyright of the Federal Republic of Germany (only binding on companies in Germany):

§ 97. UrhG claim to omission and damages.
Who violates the copyright or another after this law protected law illegally, can be taken up by the violated on removal of the impairment, with repetition danger on omission and if to the violator´s intention or negligence is a burden also on damages. At place of the damages the violated can require the delivery of the profit which the violator has achieved by the violation of the law and bill lapping about this profit.

§ 106. UrhG unauthorized utilization of works protected by copyright.
Who reproduces a work or a treatment or transformation of a work in others than the legally admitted cases without consent of the legitimate, spreads or returns publicly, it is punished with term imprisonment up to three years or with fine.
The attempt is liable to penalty.

B.1.12 Data protection in the Federal Republic of Germany (only binding on companies in Germany): In the Federal Republic of Germany the respective legal regulations of data protection are to be adhered.

B.1.13 Every contractor is responsible that information, programs and communication devices are only used in a correct manner and in accordance to assigned tasks and in the company's interests.

The use of private software and data on company provided communication devices is not permitted.

B.1.14 Responsibility: IT Office Services, CAE/CAT-Service. For production devices the respective

maintenance und planning are responsible.

B.1.15 Recommended is the usage of password vaults like KeePass

B.1.16 datenschutzdatensicherheit@audi.de