Information technology security guidelines

For external companies

Published by

Chief Information Security Officer (CISO)

Regulation No.

02.06

Status

Published

Classification

Internal

Version

2.1

Date

May 2015

Scope

These instructions are applied to **Volkswagen Autoeuropa**

Table of Contents:

List of tables and illustrations

1 Scope

These IT Security Guidelines comprise the IT security regulations that external companies must observe when using information and IT devices (e.g. personal computers, workstations, as well as notebooks, smartphones, tablet-pc). These guidelines are aimed at the external companies' management, employees, and agents (referred to hereinafter as the "contractor").

The IT Security Guidelines serve to protect the confidentiality, integrity, and availability of information, as well as to protect the rights and interests of the purchaser and all natural persons and legal entities that maintain a business relationship with the purchaser's Group company and/or perform work for it.

2 Organization of information security

2.1 Internal organization

The procurement and installation of the provided hardware and software is carried out exclusively in cooperation with the appropriate body[1] in accordance with the valid approval procedures.

The use of the provided hardware and software is subject to the regulations of the respective group company.

Only the appropriate bodies 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)[2].
The use or subsequent modification of programs is only permissible with the authorization of the appropriate bodies[3].

The regulations of the respective Group Company, with regards to bringing private IT devices to work, apply.

Group company data has to be separated from data of third parties.

On provided hardware and software Group Company data has to be processed only. Third party data is not allowed to be processed on this equipment.

The distribution of data from the ordering party entrusted to third parties is expressly forbidden, unless agreed to in writing by the ordering party.

The respective group company regulations apply to the storage and other processing and use of personal data and of data that is subject to confidentiality[4].

The usage of private acquired hardware, software or data for business purpose is not permitted.

2.2 External parties

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

The group of authorized external company employees must be determined by the IT department and must be kept as small as possible.

External company employees must be obligated by their company management to non-disclosure as defined by the existing non-disclosure agreement. This is also relevant to employees of subcontractors of the external company. The IT department has the right to inspect these agreements at any time.

[1] See Appendix C.1.1

[2] See Appendix C.1.3

[3] See Appendix C.1.3

[4] See Appendix C.1.4

The distribution of data to third parties is expressly prohibited unless the IT department gives approval.

3 Asset Management

3.1 Classification guidelines

The information owner is responsible for the classification of the information. He has to control the definition, the implementation and regular checks in order to match with the requirements of the classification (e.g. data access).

3.1.1 Confidentiality

Information that is not intended for general use must only be made accessible to those who are authorized to access it.

The following steps for classifying information with regard to requirements for confidentiality are defined:

Table 1: Confidentiality of Information

Classification	Definition
Public	Information that is not subject to any restrictions and is, for example, published by the company in newspapers. The public use of company information requires the approval of the appropriate bodies[5]. Examples: press releases, product catalog for customers
Internal	Information that is intended for internal use only and not for the general public. Loss of confidentiality may have economic consequences, albeit of a minor nature, for example: • No loss of customers • No effect on sales volume/turnover • Claims for damages by individual persons or organizations are unlikely • loss of knowhow and technical edge • no effects on public standing Examples: business communication data (e.g. phone number, mail-address), occupational safety specifications, work regulations.
Confidential	Information whose 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. Loss of confidentiality is likely to result in measurable economic consequences; for example: • Loss of customers • Decreased sales volume/turnover • Claims for damages by individual persons or organizations Examples: personal data, budget plans, audit reports

[5] See Appendix C.1.5

Secret	Information whose 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, management submissions.

3.1.2 Integrity

Error-free processing of information as well as protection against unauthorized changes must be ensured.

The following steps for classifying information with regard to requirements for integrity are defined:

Table 2: Integrity of Information

Classification	Definition
Low	A violation of integrity has no foreseeable impact on 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. Economic consequences are possible, but minor in nature; for example: • No loss of customers • No effect on sales volume/turnover • 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, organizational changes, individual internal phone numbers
High	A violation of integrity has perceivable effects on business activity and/or on the image/appearance of the company. Economic consequences are likely and measurable; for example: • Loss of customers is likely • Decreased sales volume/turnover is likely • Significant delays in work processes • Errors/faults have a noticeable effect on work results (significant production downtimes) or a few service processes fail • Decisions are negatively affected/incorrect decision-making is likely • Claims for damages by individual persons or organizations are likely Examples: JIT orders, press releases, contents of Internet presentations, and data for production control.

3.1.3 Traceability

Access to confidential information and the performance of transactions must be incontrovertible.

The following levels for the classification of information with regard to requirements for traceability are defined for this purpose:

Table 3: Traceability of Information

Classification	Definition
Low	There are no requirements for genuineness, verifiability, trustworthiness.
Medium	For write access, it must be possible to determine the type of change made (adding, deleting, modifying), the person(s) who made the change, and the time the change were made.
High	For write access, it must be possible to view the change made (including the status before the change was made), the person(s) who made the change, and the time the change was made.
Very high	For read and write access, it must be possible to view the change made (including the status before a change), the person(s) who made the change, and the time the change was made.

3.1.4 Availability

Information must be made available within an agreed time frame.

The following steps for classifying information with regard to requirements for availability are defined:

Table 4: Availability of Information

Classification	Definition
Low	The availability of the IT system is less than 95 percent regarding failure or response time without resulting in significant damage (financial or to the image of the company). Example: Intranet application with general information for employees.
Medium	The availability of the IT system is 95 percent regarding failure or response time. After that, significant damages occur (financial or for the image of the company). Example: Applicant portal
High	The availability of the IT system is less is 98 percent regarding failure or response time, otherwise there is a threat of significant damage (financial or for the company image). Examples: Payroll, bookkeeping

Very high	The availability of the IT system is 99 percent regarding failure or response time, otherwise there is a threat of significant damage (financial or for the company image). Example: IT system, the failure of which results in an immediate production standstill. 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).

3.2 Information labeling and handling

Information and programs may only be accessible to the group of persons authorized in each case. This is only permissible within the framework of the agreed task assignments and in compliance with pertinent regulations. The "need-to-know" restriction applies.
Information must be protected from unauthorized access during the entire life cycle corresponding to the respective confidentiality classification. The following regulations apply:

Table 5: Information labeling and handling

Classification	Requirements
Public	• Marking: none • Duplication and distribution: no restrictions • Storage: no restrictions • Deleting: no restrictions • Disposal: no restrictions
Internal	• Marking: none (or internal) • Duplication and distribution: only to authorized group employees and authorized third parties within the task or application area • Storage: protect against unauthorized access • Deleting: use of delete functions present and/or made available on the system side • Disposal: proper disposal[6]

[6] See Appendix C.1.7

Confidential	• Marking: "confidential." Marking on the first page of the document in electronic and printed form • 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., encrypted e-mail communication). • 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. • Deleting: data that are no longer needed must be deleted reliably by overwriting • Disposal: proper disposal[7]
Secret	• Marking: "secret." Marking on each page of the document. • 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 technical possible data has to be encrypted by using the current state of technology. If it is not possible to use the current state of technology, comparable security solutions have to be used. In addition, additional technical or organizational protective measures must be examined (e.g., forwarding or printing prohibited). 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 technical possible data has to be encrypted by using the current state of technology. If it is not possible to use the current state of technology, comparable security solutions have to be used • Deleting: data that are no longer needed must be deleted reliably by overwriting. • Disposal: proper disposal[8]

The author of the information is responsible for its marking.

If information is not marked, this must be treated as "internal."

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

The classification of information regarding integrity, verifiability, and availability is used mainly for derivation of security requirements for information systems that process this information.(see “IT Security Guidelines for Developers”, chapter “Security requirements of information systems”).

4 Human resources security

A user ID that is no longer needed or access authorization that is no longer needed must be reported promptly by the respective user to the appropriate OUs, so that the corresponding Blocking/Deletion can occur.

Identification media that are no longer needed (e.g., SmartCards, SecurID cards) must be returned immediately to the responsible OU.
The loss of IT devices or media for authentication purposes by users has to be immediately reported to the

[7] See Appendix C.1.7

[8] See Appendix C.1.7

appropriate bodies.

5 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.

IT devices that store or process confidential or secret data must be set up in such a way that the risk of unauthorized viewing by unauthorized persons is minimized.

Devices provided by the IT department (e.g., laptops, cellular phones) may only be taken outside of the plant with the approval of that department.

6 Communications and operations management

6.1 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 appropriate bodies[9] must be informed immediately.

6.2 Backup

Data must be stored on the assigned networks and not on the local hard drive, since a central and automatic data backup is only ensured on the network.

The user himself/herself is responsible for backing up data that are not stored on central network storage (e.g. local hard disks, mobile data storage devices).

6.3 Media handling

Data carriers (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 carriers that are no longer needed must be sent to secure disposal[10].

6.4 Exchange of information

During all discussions of confidential or secret information, including telephone calls, it must be ensured that these can not be overheard without authorization.

External 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.

Before a fax transmission of confidential data, the transmission must be reported to the communication partner by phone. After the transmission, proper receipt of the fax must be confirmed by phone. After transmission the fax receipt has to be removed from the fax device by the sender.

It must be ensured that all necessary and suitable precautions are taken (e.g., encryption) that protect from access, modification, and deletion of the information by unauthorized parties during transport (this includes family and friends).

During transport of portable computer devices and data carriers beyond the plant boundaries, the

[9] See Appendix C.1.8

[10] See Appendix C.1.7

regulations and operating agreements of the respective group company[11] must be complied.

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.

7 Access control

7.1 Business requirements for access control

The use of a user I.D. other than one's own is not permitted.
The distribution of identification media (e.g., smartcards, SecurID cards) is not permitted.
The disclosure to a third party of the password or PIN for a user ID assigned for personal use (so-called "personal user ID) is not permitted.
The re-use of personal user IDs by different persons (e.g., training participants, trainees, graduate students) is permissible, if the following measures are complied with:

- The assignment of user IDs must be managed by a responsible person. This person must maintain a written record of who used which user ID and when. This record must be stored by this person.
- The assumption of a user ID must be confirmed in writing by the respective user. The confirmation is stored 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 known only to him/her.
- The company-specific archiving periods must be complied with for archiving the verifications.

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

7.2 User responsibilities

During the password specification, the following minimum requirements must be complied with:

- At least an 8-digit combination of at least 3 out of the following 4 criteria:
  - upper case letters
  - lower case letters
  - numbers
  - special characters

- In particular, no trivial combinations (e.g., "AAAAAAAA") or aspects of the personal environment (e.g., name, birth date) must be used.

During creation of passwords for windows logon at least a10-digit combination is required following at least 3 out of the 4 criteria listed above. This might be memotechnic verse (e.g. “Secure-is-great!”) or also abbreviations and falsifications of memotechnix verses (e.g. memotechnic verse: “In the morning I get up early and brush my tooth’s”. comes to password: “Itm1guEabmT”). (Do not use the listed examples as your own passwords.)

During creation of PINs for identification media (e.g., SmartCards, SecurID cards), the following minimum requirements must be complied with:

- At least a 4-digit combination of numbers must be used for SecurID cards must be used and at

[11] See Appendix C.1.8

least a minim 6-digit combination of numbers for other media (e.g., SmartCards). In particular, no trivial combinations (e.g., "111111") or aspects of the personal environment (e.g., birth date) must be used.

The following minimum requirements for handling personal passwords and/or PINs (called passwords in the following) must be complied with:

- Passwords must only be stored with secure encryption.
- The password must be changed at first use and then at least every 90 days.
- The password must be changed immediately if there is a suspicion that it is known to a third party.
- Spying out passwords is not permissible.
- If passwords must be stored in a written form, they must be stored by the employee in a sealed envelope at a suitable location (protected against access that is not allowed (e.g., safe) and 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 the 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 store it again. System technical implementations are possible as long as they match with these requirements.

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.

7.3 Network and access control

7.3.1 Policy on use of network services

An IT device provided by the principal must only be connected to networks outside the company (e.g., hot spot, private WLAN) if this is done to set up a connection with the Group network.

7.3.2 Equipment identification in networks

The connection of communication devices 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.

Each mobile system or IT device must be encrypted by the current state of technology using hardware or software provided that an approved encryption software is given by the appropriate bodies.

Mobile IT devices must be physically protected against theft; they must not be left open unattended.

- If the portable IT device is unattendedly stored in a motor vehicle, the IT device must not be visible from the outside.
- On plane and train trips, a mobile IT device must be transported in hand-held luggage.

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

8 Information-security incident management

IT security events (e.g., malfunctions that occur, violations of the IT security regulation) must be reported immediately to the appropriate OU[12].

Suspected vulnerabilities and weak points of IT systems must be reported to the responsible OUs[13]. Testing of vulnerabilities and weak points must be performed by the appropriate OUs[14].

9 Compliance

Intellectual property rights (e.g., copyrights for software, documents, and other image material, rights to drafts, trademarks, patents, and source code licenses) must be protected.
In particular, the use of unlicensed software (pirate copies) is prohibited as per the legal provisions in effect.
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[15].
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.

The respective national laws and regulations for data protection[16] must be complied with.

Contractors must be obligated by the business management of the partner company to comply with the legal requirements concerning data protection[17].

10 Responsibility

Violations of the security guidelines must be checked individually as per applicable operational and legal regulations and agreements and punished appropriately.

Deviations from these security guidelines that reduce the security level are only permissible in agreement with the appropriate OUs[18] and only permissible with time limits.

[12] See Appendix C.1.7
[13] See Appendix C.1.8
[14] See Appendix C.1.9
[15] See Appendix C.1.10
[16] See Appendix C.1.11
[17] See Appendix C.1.11
[18] See Appendix C.1.12

Appendix

A General

A.1 Other Applicable Documents

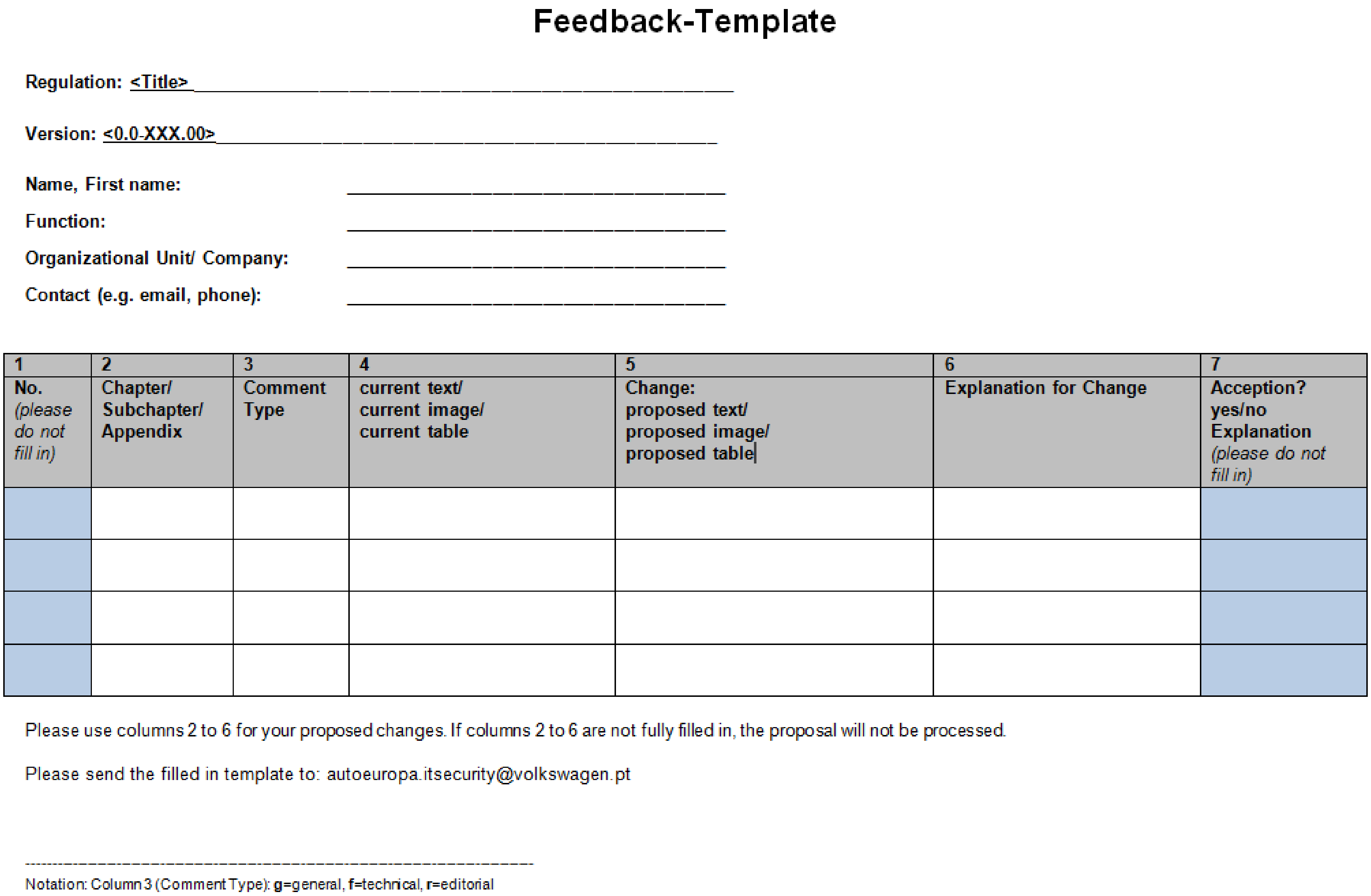
A.2 Attachments

Attachment 1 Feedback Form

The feedback form for suggestions concerning regulations can be downloaded from Volkswagen Autoeuropa intranet in Security IT page, “Outros Documentos” zone.

The feedback form must be completed as follows:

- Columns 2 to 6 must be completed for every proposed change. Changes for which not all of columns 2 to 6 have been completed will be automatically declined without further examination.
- Column 3: The following comment types are possible: g=general, f=technical, r=editorial
- Column 4: Please insert previous text, table or image
- Column 5: Please insert the fully reformulated text, modified table or modified image
- Column 6: Please give as detailed reasons as possible for the desired change.
- Sent the form to: autoeuropa.itsecurity@volkswagen.pt



Feedback-Template

Regulation: **<Title>**____

Version: **<0.0-XXX.00>**____

Name, First name: ________________________________

Function: ________________________________

Organizational Unit/ Company: ________________________________

Contact (e.g. email, phone): ________________________________

1	2	3	4	5	6	7
No. *(please do not fill in)*	**Chapter/ Subchapter/ Appendix**	**Comment Type**	**current text/ current image/ current table**	**Change: proposed text/ proposed image/ proposed table**	**Explanation for Change**	**Acception? yes/no Explanation** *(please do not fill in)*

Please use columns 2 to 6 for your proposed changes. If columns 2 to 6 are not fully filled in, the proposal will not be processed.

Please send the filled in template to: autoeuropa.itsecurity@volkswagen.pt

--

Notation: Column 3 (Comment Type): **g**=general, **f**=technical, **r**=editorial

A.3 Abbreviations and Definitions

Abr. / Expression	Definition

A.4 Validity

This IT Security Regulation enters into force immediately after publication.

Next revision: 30.05.2017

A.5 Document History

Version	Name	Area/function	Date	Comment	Signature (Digital)
1.0	Nuno Branco	IT/CISO	April 2013	Version published	
2.0	Nuno Branco	IT/CISO	May 2013	Version reviewed and published	
2.1	Nuno Branco	IT/CISO	May 2015	Version reviewed and published	Branco Nuno Miguel VWPKI DCF2F734EDEA6560 Digitally signed by Branco Nuno Miguel VWPKI DCF2F734EDEA6560 DN: dc=vwg, cn=Branco Nuno Miguel VWPKI DCF2F734EDEA6560 Date: 2015.05.18 14:39:14 +01'00'

B Implementation Checklist

Table 6: Implementation Checklist

Regulation No.	Chapter	Description	Reasons for non-implementation	Date, Responsible Person
Implementation status[19] of the regulation in %:				

[19] The implementation status of the regulation is calculated by the number of chapters which are implemented and listed in the implementation checklist divided through the total number of chapters listed in the implementation checklist multiplied by 100.

C Company-Specific characteristics

C.1.1 IT Department.

C.1.2 Each contractor is responsible for ensuring the proper use of information, programs, and IT devices only for company purposes and within the scope of the respective assignment.

The sending of data containing non-business content is not permitted.

The use of the Internet for private purposes is only permitted within the framework of the existing company regulations.

The use of company-owned software and data on private IT devices is not permitted.

The use of private software and data on IT devices provided by the company is not permitted.

C.1.3 IT Department.

C.1.4 IT Security Guidelines - Nº 02.02 - for employees. Further details are regulated in: Organizational Instruction no. 50 "Protection of personal data"
http://kdos01.wob.vw.vwg/OR/doo2/ORL50/ORL50Uebersicht.htm including appendix:

1 - Process responsibility and other applicable documents
2 - Information on data protection and obligation to data secrecy
3 - Decentralized processing of employee data
4 - Voice recording and video surveillance
5 - Employee surveys
6 - Outsourced data processing

All personal data that is supplementary to the information necessary for work-related communication is to be classified as confidential at least, and must be protected with technical encryption and powerful authentication, e.g. a PKI certificate. Any deviation from this rule must be approved by the data protection department.
Access to and administration of personal employee data is subject to the special requirements as set out in Organizational Instruction no. 51/1 "Betriebssicherstellung der Informationsverarbeitung", http://kdos01.wob.vw.vwg/OR/doo2/OA51-1/OA51-1Uebersicht.htm

C.1.5 Communication and public relations department from Volkswagen Autoeuropa.

C.1.6 Confidential and secret paper documents must be disposed of in secure document containers.

Data carriers that are no longer needed must be deleted reliably by overwriting or physically destroyed.

For proper disposal, Volkswagen data carrier disposal bags are used that can be procured from the secretary's office (ordering process for office consumables).
Certified data deletion or scrapping of hard drives is performed by K-SF-O/61, IT Client Support.

C.1.7 IT Coordination, Help Desk (Building 11, first floor) phone 21211 2500

C.1.8 IT Department

C.1.9 CERT - Volkswagen Autoeuropa

C.1.10 Additional country specific rights and regulations have to be respected.

C.1.11 The respective legal regulations for data protection in effect must be complied with.

Signatures

Felgendreher Peter Meinhard VWPKI 7C0F2B49B180EC0D

Digitally signed by Felgendreher Peter Meinhard VWPKI 7C0F2B49B180EC0D
DN: dc=vwg, cn=Felgendreher Peter Meinhard VWPKI 7C0F2B49B180EC0D
Date: 2015.05.20 14:30:08 +01'00'

Peter Felgendreher

(IT Manager)

Branco Nuno Miguel VWPKI DCF2F734EDEA6560

Digitally signed by Branco Nuno Miguel VWPKI DCF2F734EDEA6560
DN: dc=vwg, cn=Branco Nuno Miguel VWPKI DCF2F734EDEA6560
Date: 2015.05.18 14:38:45 +01'00'

Nuno Branco

(CISO)