PUBLIC
ÖFFENTLICH

APPENDIX 17-A

POLICY PACK PUBLIC

March 2023

This document contains company information of MAN Truck & Bus. This document and the information it contains may not be published, forwarded, or used for any other purposes without the express prior written approval of MAN Truck & Bus.

Note: Printed versions and local files may not be updated!

Information Security

Created	Steven Rauwerdink Ralf Schlag	**Approved**	Andre Wehner	**Version**	3.0.
Dept.	FIOS	Dept.	FI	**KSU-Class:**	xx

Applicable as of Date 01.02.2023	**Scope** MAN Truck & Bus SE and its Subsidiaries	**Approved by (Board)** Alexander Vlaskamp, MTB Friedrich Baumann, MTB-S Murat Aksel, MTB-B Michael Kobriger, MTB-P Inka Koljonen, MTB-F Arne Puls, MTB-H Dr. Frederik Zohm, MTB-E **Agreed by**

Contents

Appendix

1 Purpose

The purpose of this Brand Policy is to provide a framework for safeguarding the confidentiality, integrity and availability of the valued information of the MAN Truck & Bus Group. Within this framework, strategies, objectives and implementation responsibilities must be developed in order that each MAN Truck & Bus Group Company achieves the appropriate level of information security.

This Information Security Policy regulates the binding, mandatory objectives and principles for all companies within the Man Truck & Bus Group with regard to information security management, including the distribution of roles and responsibilities between MAN Truck & Bus SE and each company within the Man Truck & Bus Group.

Together with the subordinate Brand Instruction MTB MA_13_1_01 - Standard for Information Security (in the following referred to as MTB Standard for Information Security) and additional Brand Instructions, this Information Security Policy constitutes the framework for information security management within the MAN Truck & Bus Group (cf. section 7). This Policy forms the basis for all additional regulations concerning information security within the MAN Truck & Bus Group.

Note: Printed versions and local files may not be updated!

2 Scope

This Brand Policy applies to MAN Truck & Bus SE and its subsidiaries and their employees worldwide. This Brand Policy is to be implemented directly and does not require conversion policies from the individual subsidiary. In the case of companies in which MAN Truck & Bus SE cannot directly enforce the applicability of this Brand Policy for legal reasons, the policy owner has to be consulted to clarify the extent to which this Brand Policy is applicable. Companies which are not wholly owned by MAN Truck & Bus SE and also not subsidiary with MAN Truck & Bus SE through a control agreement constitute one such example (e.g. Subsidiaries which are wholly owned by MAN Finance and Holding S.A.)

In the event of any subsidiaries having their own regulations governing the enactment of Policies, these must be annulled with immediate effect. Until such time as Policies of this kind, either wholly or in part, are annulled, this Brand Policy takes precedence.

If the rules contained in this Brand Policy cannot be implemented due to mandatory local requirements, the individual Subsidiary needs to inform the policy owner of MAN Truck & Bus SE without undue delay to discuss required changes or adaptations.

3 Terms and definitions

A glossary for the complete information security framework can be found at the additional information “Terms and Definitions in Information Security“.

4 The Objectives of Information Security Management

The primary objective of information security management is the safeguarding of the MAN Truck & Bus Group and its stakeholders, customers and partners against damage and risks that may arise through the use of information and communication technology (ICT) and in dealing with information and data. This includes the secure provisioning of the MAN Truck & Bus Groups products and services.

On this basis the MAN Truck & Bus Group have formulated the following information security objectives:

- Efficient identification and assessment of risks which may arise through the use of ICT and in dealing with information and data.
- Compliance with laws, regulations and agreements concerning the safeguarding of information and data.

- Establishment of functional and effective Information Security Management System (ISMS).
- Corresponding to the level of risk implementation of cost and effort effective measures for safeguarding information and data.
- Minimal restrictions on business and production processes as result of the implementation of critical security measures.
- High efficiency of information security management and the protection of information and data.

5 Principles for Adherence to Information Security at the MAN Truck & Bus Group

The appropriate information security level is realized through ensuring that Information Security risks for each individual MAN Truck & Bus Company and the MAN Truck & Bus Group as a whole are kept to an acceptable level. In each MAN Truck & Bus Group Company an ISMS must be established that ensures both the information security objectives and the MAN Truck & Bus business objectives are met through a specific risk-based approach considering the costs versus the benefits.

The stated requirements for information security management must be adhered to by all MAN Truck & Bus Group Companies. These are specified by the MAN Truck & Bus Standard for Information Security.

5.1 Employee Awareness

All employees of the MAN Truck & Bus Group have to be made aware of the risks involved with the handling and use of information in MAN Truck & Bus by their manager. Staff within their individual area of responsibility must be empowered to protect the Company and/or the MAN Truck & Bus Group from information security incidents and their consequences. The level of information security awareness amongst employees need to be continuously maintained by the management body of the division or Company.

5.2 Information Inventory and Classification

The basis for the classification of information is to compile and maintain an inventory of all relevant intangible information assets. The individuals responsible for the relevant business processes have to determine the protection need of the related information assets according to the classification in terms of Confidentiality, Integrity and Availability requirements. For this, the MTB Brand Instruction MA_13_1_03 - Classification of Information Assets must be used as a basis.

5.3 Risk Identification and Evaluation

The Information Security risks associated with the using, transferring, processing and storing of information by the MAN Truck & Bus Group have to be identified, evaluated and managed in a way that keeps the risks at an acceptable level for each individual Company and the MAN Truck & Bus Group as a whole. The MTB Brand Instruction MA_13_1_04 – Risk Management must be used as a basis.

5.4 Documentation of Information Security Management

Procedures and results related to the management of Information Security must be documented in a verifiable form in order to comply with auditing requirements and for any liability claims.

5.5 Risk-based implementation of Protection Measures

The cost and effort for implementation of measures must be effective in relation to the level of the risk they are addressing. The following principles in the risk-based implementation of measures have to be considered:

Note: Printed versions and local files may not be updated!

- Information as well as communication infrastructures must be protected in accordance with the level of risk for the confidentiality, integrity and availability of information during its usage, transfer, processing and storage (Please refer to MTB Brand Instruction MA_13_1_03 – Classification of Information Assets).
- Information and data privacy protection must be ensured in all phases of the information assets life-cycle. This includes planning, procurement, development, maintenance and acceptance to production of ICT Systems.
- Information and data privacy protection must be ensured in all phases of the identity management life-cycle. This includes employees, suppliers and external contractors.
- Information and data privacy protection must be ensured in all business processes
- All ICT systems must be protected against malicious attacks and malware.
- Information and data on centralized ICT systems must be backed up and successful restore must be ensured.
- The exchange of information within the MAN Truck & Bus Group or with trusted external partners must be appropriately protected.
- Effective processes and technologies must be implemented to ensure that information security incidents and vulnerabilities are identified, reported, monitored and mitigated with appropriate measures. A standardized and effective approach for handling of information security incidents and known technical vulnerabilities must be established.
- Access to information systems must be restricted to authorized personnel only, in accordance with the need-to-know principle. Unauthorized user access, security compromises and theft of information or information-processing facilities must be appropriately identified, reported, monitored and prevented.
- The Corporate Business Continuity Management must consider aspects of Information Security such as Confidentiality, Integrity and Availability of information and data.
- Relevant legal requirements, regulations and other contractual obligations for Information Security must be managed and adhered to.

Note: Printed versions and local files may not be updated!

5.6 Consideration for Standard ISO 27001

The management of Information Security in MAN Truck & Bus Group is based on the internationally accepted standard on information security management, ISO 27001. The basis for this is the MTB Brand Instruction MA_13_1_01 - Standard for Information Security (cf. section 7.1).

5.7 Collaboration with Third Parties

External suppliers and partners that have access to and/or process information on behalf of MAN Truck & Bus must be contractually obliged to adhere to the MAN Truck & Bus requirements for information security. Please refer to MTB Brand Instruction MA_13_1_08 – Information Security for Suppliers (cf. section 7.1).

6 Responsibility for Information Security at the MAN Truck & Bus Group

6.1 Responsibilities for Information Security Management within the MAN Truck & Bus Group

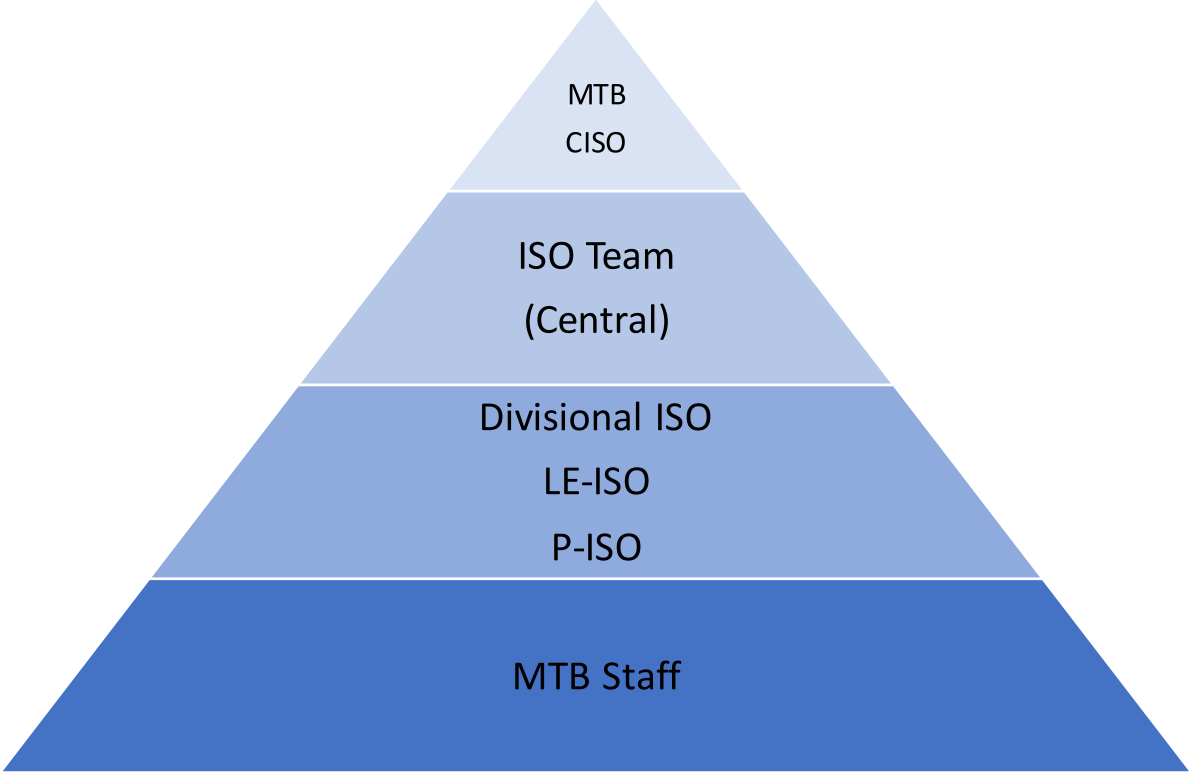


Figure 1 Information Security Organization

Note: Printed versions and local files may not be updated!

For details about responsibilities, please refer to MTB Brand Instruction MA_13_1_02 – Management of Information Security

6.1.1 Chief Information Security Officer (CISO)

The CISO is responsible for the central management and improvement of Information Security within the MAN Truck & Bus Group.

The Chief Information Officer (CIO) appoints a qualified CISO for the MAN Truck & Bus Group. Strongly aligned with to the business strategy of the MAN Truck & Bus Group, the CISO develops and maintains the group-specific Information Security strategy, the risk-oriented protection of the Group information assets and methods for assessing and presenting Group Information Security levels. He is supported by the MAN Truck & Bus ISO Team.

The CISO defines the principles for the Information Security framework at the MAN Truck & Bus Group and monitors compliance.

The CISO of the MAN Truck & Bus Group reports on a regular basis on the degree of implementation of information security management in the divisions and group companies to the MAN Truck & Bus Group Executive Board.

The CISO together with the ISO Team, act as points of contact for all matters related to information security at the MAN Truck & Bus Group.

6.1.2 ISO Team (Central)

The ISO Team has the overarching duty to establish information security in the MAN Truck & Bus Group. The team supports the Group CISO in the achievement of his responsibilities.

6.1.3 Information Security Officers (Divisional ISO / LE-ISO / P-ISO)

For areas outside the central Organization of MAN Truck & Bus it is necessary to establish Information Security Officers that are covering the decentralized implementation of information security at the MAN Truck & Bus Group aligned with the related business processes and with local scope and requirements.

In their area of responsibility, the divisional Information Security Officer, the Legal Entity Information Security Officer (LE-ISO) and the Production Information Security Officer (P-ISO) represent the direct contact to the central MAN T&B Information security organization interfacing with the (local) business departments and the Information Systems departments. They support all Information Security topics in their scope.

The Management Bodies of the individual MAN Truck & Bus Group Companies appoints responsible LE-ISOs / P-ISOs.

The divisional ISOs are located in MAN Truck & Bus SE (e.g. finance, accounting, MHR, procurement, etc.) and should be appointed on department level.

6.2 Responsible Handling of Information and Data

Each Business Process Owner at the MAN Truck & Bus Group must appropriately protect the information required for the proper execution of business and production processes. The Business Process Owner supported by Information Security Officers (Divisional ISO / LE-ISO / P-ISO) is responsible for the implementation of information security measures within his area of responsibility.

All employees of the MAN Truck & Bus Group must protect all information and data held in their area of responsibility in accordance with internal brand regulations. Further information is detailed in the additional MTB Brand Instruction MA_13_1_05 – Information Security for Employees.

6.3 Responsible Use of Information Communication Technology (ICT) Systems

All employees are personally obliged to comply with information security requirements in their respective tasks. Each employee acts with the required systems and resources according to the work order and in compliance with the security policies, standards, guidelines and regulations.

6.4 Responsible Provision of Information Communication Technology (ICT) Systems

All employees of the MAN Truck & Bus Group developing and/or implementing ICT systems for use, as well as involved with the operation of such a systems, are responsible for ensuring information security in compliance with the Security Guidelines. For all applications and IT systems, Asset Owners must be assigned.

7 Additional Regulations on Information Security within the MAN Truck & Bus Group

This Policy is supplemented by target-group-specific instructions and regulations.

Note: Printed versions and local files may not be updated!

7.1 Additional Brand Policy Instructions

This Brand Policy is supplemented by additional Brand Policy instructions regulating the standards for Information Security Management in further detail. These regulations are mandatory for all Group Companies and their employees.

The Brand Policy Instructions supplementing this Brand Policy are to be created by or on behalf of the CISO of the MAN Truck & Bus Group. The CISO is responsible for the compliance of the regulations in regard to the corresponding legal conditions and requirements.

The CISO provides the Brand Policy Instructions to the CIO for validation and approval.

Following the approval of a Brand Policy Instruction the CISO initiates the announcement for the target audience and informs the responsible Policy Coordinator who carries out the publication of the Brand Policy Instruction at the corresponding Policy Portal.

7.2 Additional Information Security Related Instructions

While Brand Policy Instructions govern topics related to the information security for the entire MAN Truck & Bus Group, additional Instructions, that regulate specific technical areas into further detail, may be created and applied in practice.

These Instructions are created by the responsible bodies of the respective technical areas, consulted by the CISO and approved by the CIO.

7.3 Additional regulations of the MAN Truck & Bus Group Companies

In addition to the Brand Policy MAN Truck & Bus MR_13_1 and MTB Brand Instruction MA_13_1_01 - Standard for Information Security, further regulations have to be created to ensure the realization of an effective Information Security Management System (ISMS) in the group company.

These local regulations must comply with legal and contractual requirements for Information Security and be verified on a regular basis and if applicable, amended. The local regulations must be approved by the Management Body of the corresponding Group Company.

The CISO must be informed of decentralized regulations.

8 Change History

Version 3.0

- Added Change Log
- Relabeling MTB
- Change in roles and responsibilities
- Take over a content by AN_MTB_13_1_02
- Rename of sections 6.1.2
- Removal of sections 7.1.1, 7.1.2, 7.1.3

Note: Printed versions and local files may not be updated!

Appendix 1 : Glossary - Terms and Definitions of Information Security

Note: Printed versions and local files may not be updated!

Appendix 1 – Glossary

Terms and Definitions of Information Security

Created	Steven Rauwerdink Ralf Schlag	**Approved**	Andre Wehner	**Version**	3.0.
Dept.	FIOS	Dept.	FI	**KSU-Class:**	xx
Applicable as of		**Scope**		**Approved by (Board)**	
Date	01.02.2023	MAN Truck & Bus SE and its Subsidiaries		Alexander Vlaskamp, MTB Friedrich Baumann, MTB-S Murat Aksel, MTB-B Michael Kobriger, MTB-P Inka Koljonen, MTB-F Arne Puls, MTB-H Dr. Frederik Zohm, MTB-E	
				Agreed by	

Term	Definition
Application Owner / System Owner	The Application Owners and System Owners ensure that the processes, applications, systems and networks for which they are responsible are set up and operated in accordance with the security guidelines. They report on this to the CISO / Information Security department and take care of operative measures, e.g. use of centrally provided security services (e.g. virus protection). The security guidelines and instructions define the standard for the measures and serve as a reference for contractual agreements with service providers as well as for controls and revisions. The application owners and system owners are responsible for: Implementation of the rights concept (product/system dependent) according to central specifications Allocation, administration and revocation of access authorizations for applications, IT systems, networks and information to authorized persons. Review of applications, systems and networks for deficiencies Monitoring compliance with security guidelines Informing users about security risks and related issues Reporting of significant vulnerabilities and serious security incidents to IS Contact or CISO / Information Security Department Secure access to and monitoring of applications, IT systems and networks Technical support in case of security incidents
Business Continuity Management (BCM)	BCP is working out how to continue operations, or the delivery of services, during disruption or interruptions resulting from events such as; fires, floods, power outages, theft, and vandalism, earthquakes and pandemics. Holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. Business Continuity Management (BCM) integrates the disciplines of Emergency Response, Crisis Management, Disaster Recovery (technology continuity) and Business Continuity (organizational/operational relocation).
Business Impact Analysis (BIA)	A Business Impact Analysis (BIA) quantifies risks in relation to specific business processes. It supports the determination of protection requirements for Information Assets.
Business Process Owner	Person responsible for regularly identifying all risks of the processes within his area of responsibility and ensuring they are covered by appropriate controls. This includes documenting the controls and the associated tests, implementing the measures to eliminate any weaknesses in the controls, and regularly checking the controls to ensure they are up to date and fully cover the processes.

Note: Printed versions and local files may not be updated!

CERT	Computer Emergency Response Team.
Chief Information Officer (CIO)	The Corporate **Chief Information Officer** at the MAN Truck & Bus Group is the most senior authority concerned with the management of information and communication technology at the MAN Truck & Bus Group. The CIO of each MAN T&B division is the most senior authority concerned with the management of information and communication technology at an MAN T&B division.
Chief Information Security Officer (CISO)	The **Chief Information Security Officer** at the MAN Truck & Bus Group is responsible for the centralized, group-wide management of information security and for safeguarding the company-wide strategic interests of information security at the MAN Truck & Bus Group. The MTB CISO is appointed by the Corporate CIO of the MAN Truck & Bus Group.
Cloud computing	Refers to a special form of IT outsourcing. A cloud application is a service provided via a network connection (e.g. Internet). Typical cloud models include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Private and Public Cloud.
Compliance	Compliance refers to a strategy that ensures to meet any legal, regulatory, or other relevant standards
Expected Value	In Risk Management, the **expected value** is the value obtained by multiplying the impact and the likelihood after measures.
False Negative	False Negative state is a failure to identify a malicious event as such. It suggests that we are in a secure status whereas in reality a breach has occurred.
False Positive	False Positive is a false alarm. The activity was reported by an Agent as a malicious activity, but in fact it was recognized in a later stage as legitimate activity.
GDPR	Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (general Data Protection Regulation).
ICT system configuration	MAN T&B **ICT system configuration** means all settings that influence the behavior of a MAN T&B ICT system in terms of its availability, protection of confidentiality, and integrity.
Information and Communication Technology System (ICT system)	MAN T&B **ICT systems** include all processes and products (hardware and software) that are required for the secure processing, transfer/transportation, and storage of electronic information of the MAN Truck & Bus Group. Products (hardware and software) also include all necessary passive infrastructure (racks, cables, patch panels, etc.), real estate (buildings, rooms, areas, etc.), and the associated technology (power supply systems, cooling systems, access control systems, fire protection technology, etc.).

Note: Printed versions and local files may not be updated!

Information Asset	**Information Assets** cover all forms of information, whether digitally processed or presented as an image, drawing, spoken word, or visible object.
Information Owner	Publisher, originator, creator of information.
Information Security	Aims for protecting information against risks for confidentiality (disclosure to unauthorized users), integrity (improper modification) and availability (non-access when required).
Information Security Incident (IS Incident)	An **Information Security Incident** (IS incident) is an event which affects the availability, confidentiality, or integrity of MAN T&B information assets and leads to an unacceptable level of risk for the MAN Truck & Bus Group, a division or group company.
Information Security Management System (ISMS)	The **ISMS** is a management system that aims to use economically reasonable measures to protect information assets in a manner that corresponds to the risk involved. Information security management at the MAN Truck & Bus Group is based on the ISO 27001 standard.
Information Security Officers (Divisional ISO / LE-ISO and P-ISO)	The Information Security Officers undertake activities in their area of responsibilities. They represent the direct contact for all topics related to the Information Security for the ISO Organization and for all employees in their area of responsibility. Their goal is to increase information security and raises awareness of the issue.
ISO 27001	**ISO 27001** "Information technology – Security techniques – Information security management systems – Requirements" specifies the requirements for the development, introduction, operation, monitoring, maintenance, and improvement of a documented Information Security Management System (ISMS), taking into consideration methodically determined risks within a defined scope.
IT outsourcing	Serves as a generic term and refers to the outsourcing of corporate tasks or structures of IT to external or internal service providers (e.g subsidiary, external data center). These include e.g. managed services, external hosting and cloud services (IaaS, PaaS, SaaS)
IT system	Technical infrastructure to execute software applications on that protects the results and make it available to the authorized persons.
Malicious Code (Malware)	A program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system. Types of Malware • **Ransomware:** A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again. • **Spyware**: Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

Note: Printed versions and local files may not be updated!

	• **Virus**: A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a Cloud computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. • **Worm**: A computer program or algorithm that replicates itself over a computer network and usually performs malicious actions.
Security Incident Response Team (SIRT)	The **Security Incident Response Team** (SIRT) within the MAN Truck & Bus Group defines the procedures for dealing with IS incidents and meeting the responsibilities within the process as a whole with a view to minimizing the negative impact on MTB business operations and restoring normal operation as quickly as possible.
Measure	A **measure** is action that is suited to reduce a risk or raise an opportunity or to exploit an opportunity by influencing the impact or the likelihood.
NDA	Non-disclosure agreement between two parties to regulate the treatment of confidential information.
Opportunity	An **opportunity** is the chance to top defined revenue and profit goals.
Protection Need	For each security objective a required protection need can be defined as a measure of the impact if the security objective for that asset is compromised by an attacker. This protection need is usually expressed on a scale of four levels - "low", "medium", "high" and "very high".
Risk	A risk arises where a threat can effectively compromise a security objective because of a vulnerability. Risks are assessed using a risk matrix depicting the probability of the threat on one axis and the maximum impact value of the asset on the second. The risk values from the risk matrix are classified into risk categories. Depending on the risk category, there are specifications for risk treatment.
Risk Evaluation	The **evaluation** of a risk or an opportunity is an assessment based on the monetary *impact* (on operating profit if it occurs) and the *likelihood of occurrence*. The gross evaluation presents the initial values while net evaluation includes measures already implemented.
Risk Mitigation	A mitigation measure (also known as a countermeasure or a security control) is a measure to protect an asset from a threat. Mitigation either reduces the probability of a threat (examples: longer key length, improved access control) or reduces the impact (examples: network segmentation, partitioning of the asset's storage). Consequently, by implementing countermeasures, the risk value will change and the risk will be classified in another risk class (HIGH → MEDIUM).
Risk object	The entity which is associated with a risk and which constitutes a relevant area for a risk assessment. Objects can be, among other things, systems, applications, processes or people.

Note: Printed versions and local files may not be updated!

Risk Owner	The responsible person or role that takes ownership and can decide how to treat a risk. The Risk Owner is also responsible for continuously monitoring and re-evaluating the risk assessment.
Risk Treatment	As part of the Risk Strategy, a decision has to be made on how to treat risks. The following possibilities of treatment are possible: • Risk Avoidance: Eliminating impact or likelihood of a risk. • Risk Mitigation: Implementation of further measures to reduce risk to an acceptable level • Risk Acceptance: Acceptance of the net risk (if it is within the risk appetite) • Risk Transfer: Shifting the risk to another instance (e.g. signing for an insurance) • Risk Sharing: Distributing risks amongst organizations
Run Book	A Run Book is a compilation of routine procedures and operations that the Operator carries out. Run Books are used for reference and guidance and can be in either electronic or in physical book form. Typically, a Run Book contains procedures to begin, stop and manage the process and it may also describe procedures for handling special requests. An effective Run Book allows other team members, with prerequisite expertise, to effectively manage the process themselves.
SDLC	Software Development Life Cycle.
Security Assessment	A Security Assessment verifies the implementation of Information Security requirements for an organization. For example, one standardized assessment is based on the questionnaire for "Information Security Assessment" (ISA), developed by Association of automotive industries (VDA), published on the internet sites of the VDA.
Security Incident	A security incident is an event that may indicate that an organization's information or data have been compromised or that measures put in place to protect them have failed.
Security Requirement	A Security Requirement is a concrete software or organizational requirement that contributes to one of the Security Goals. For example, it might specify the need for a mitigation from the risk treatment decision.
Security zones	Security zones are areas that protect information or data that is being processed within. They could be of physical (security zone in the R&D area) or logical nature (network zones to separate office from shopfloor systems).
SLA	A service-level agreement (SLA) sets the expectations between the service provider and the service receiver and describes the products or services to be delivered, the single point of contact for issues, and the metrics by which the effectiveness of the services provided is monitored and approved.
Software Application	Computer program that processes, transfers and/or stores information or data. The results can be used to support business processes.

Note: Printed versions and local files may not be updated!

Subject Matter Expert	A Subject Matter Expert (also known as SME) is an individual with a deep understanding of a particular process, function, technology or type of equipment. Individuals designated as subject matter experts are typically sought out by others interested in learning more about the subject or leveraging their unique expertise to solve specific problems or help meet particular technical challenges.
System operator	A system operator operates IT systems by ensuring their availability and regular maintenance.
Threat	A threat is an event or condition that has the potential for compromising one or more security objectives for assets which results in undesirable consequences. Threats are referred to as relevant if they apply to one or more assets. Threats are evaluated according to the probability of their occurrence.
TRATON SE Chief Information Security Officer (CISO)	The **Chief Information Security Officer** at TRATON SE is the chair of the TRATON CISO Board. This gremium consists of CISOs of all TRATON brands.
True Positive	True Positive is a successful identification of a malicious activity.
Vulnerability	A vulnerability is a (usually undesirable) property of an Information System that can affect one or more security objectives. Whereas most vulnerabilities stem from design or implementation errors some are unavoidable as they are inherent to the usability of the system or the technology in use. One example of the latter is the susceptibility of open network ports to DDoS attacks.

Note: Printed versions and local files may not be updated!

Standard for Information Security

Note: Printed versions and local files may not be updated!

Created	Steven Rauwerdink Ralf Schlag	**Approved**	Andre Wehner	**Version**	3.0
Dept.	FIOS	Dept.	FI	**KSU-Class:**	xx
Applicable as of		**Scope**		**Approved by (Board)***	
Date	01.02.2023	MAN Truck & Bus SE and its Subsidiaries			
				Agreed by	

* Only required for Brand Instructions that do not relate to a superior Brand Policy

Contents

Note: Printed versions and local files may not be updated!

1 Purpose

The purpose of the Brand Policy MAN Truck & Bus MR_13_1 Information Security is to define the standard for information security within the MAN Truck & Bus Group that must be complied with by all MAN Truck & Bus Group companies and their employees worldwide.

Based on Brand Policy MAN Truck & Bus MR_13_1, this MTB Brand Instruction MA_13_1_01 - Standard for Information Security sets out the basic principles for all other regulations, security concepts, and specific rules.

They define the minimum requirements for protecting the information assets of MAN Truck & Bus, proportionate to the risk, and refer to the protecting and/or the security of all information, irrespective of the form it takes within the Company.

Brand Instruction MA_13_1_01 takes into account the requirements of ISO27001:2013 Annex A (cf. MAN Truck & Bus MR_13_1, Section 5.6).

Note: Printed versions and local files may not be updated!

2 Scope

This brand instruction applies to MAN Truck & Bus SE and its subsidiaries and their employees worldwide. This brand instruction has to be implemented directly and does not require specific policies from the individual subsidiary. In case of companies in which MAN Truck & Bus SE cannot directly enforce the applicability of this brand instruction for legal reasons, the regulation owner has to be consulted to clarify the extent to which this brand instruction is applicable. Companies which are not 100% owned by MAN Truck & Bus SE and which are also not connected to MAN Truck & Bus SE through a domination agreement constitute such an example (e.g. Subsidiaries which are wholly owned by MAN Finance and Holding S.A.)

If companies have issued their own regulations on this matter, these must be annulled immediately. Until such guidelines or parts of guidelines are annulled, this instruction is leading.

If requirements of this brand instruction cannot be implemented due to mandatory local regulations, the company concerned must immediately inform the regulation owner of MAN Truck & Bus SE in order to discuss any necessary changes or additions.

3 Terms and definitions

A glossary for the complete information security framework can be found in the document “Additional Information Terms and Definitions in Information Security“.

4 Target Group

MTB Brand Instruction MA_13_1_01 - Standard for Information Security is directed towards functions responsible for the management of Information Security within the MAN Truck & Bus Group (cf. MAN Truck & Bus MR_13_1, Section 6.1).

5 Standard for Information Security

The information security regulatory system comprises MTB Brand Policy MR_13_1, the MTB Brand Instruction MA_13_1_01 - Standard for Information Security, and additional subordinate central and decentralized regulations which govern the principles of information security management (cf. Brand Policy MAN Truck & Bus MR_13_1) in more detail.

5.1 Management of Information Security

The function and structure of an Information Security Management System (ISMS) are defined in detail in the MTB Brand Instruction MA_13_1_02 – Management of Information Security. This includes defining the roles and responsibilities as well as the committees for monitoring and further development of the ISMS.

The procedure for managing Information Security Risks shall be performed on the basis of the Brand Policy MAN Truck & Bus MR_04_8 "Central Risk Management System of the MAN Truck & Bus Group". This shall be defined more specifically in the MTB Brand Instruction MA_13_1_04 – Information Security Risk Management with regard to the risks associated with information assets.

5.2 Requirements for the Protection of Information Assets

The following table defines the MAN Truck & Bus group-specific requirements for protecting information assets. These requirements are tailored to the respective functions and are defined more specifically by additional MAN Truck & Bus Brand Policy Instructions.

Article	Function and Purpose	Regulation
Article 1	Function Segregation of duties and responsibilities. Purpose To distribute tasks and responsibilities such that the misuse or unauthorized modification of IT services and systems is limited to the greatest possible extent.	(1) As part of the risk management process, tasks and responsibilities in business processes together with critical functions shall be identified and evaluated by each MAN Truck & Bus Group company. The misuse and manipulation of information and IT systems shall be prevented to the greatest possible extent through the separation of tasks.
Article 2	Function Confidentiality agreements with internal/external individuals and companies. Purpose Contractual protection of the confidentiality of sensitive MAN information.	(1) Each MAN Truck & Bus Group company shall ensure that employees, contract partners, and third parties who are granted access to sensitive information in the MAN Truck & Bus scope of responsibility, sign non-disclosure agreements in respect to the type of processed information. (2) Specific non-disclosure agreements must be signed for performance of administrator tasks on IT systems.
Article 3	Function Prevent and detect of threats and vulnerabilities at an early stage. Purpose To ensure an optimized approach and response to security incidents and identification of potential hazards.	(1) The handling of information security incidents shall be supported by a security incident management process that is defined and documented throughout the MAN Truck & Bus Group. The process describes the behavior of employees, contract partners, and third parties in the event of security weaknesses and security incidents, including an escalation path to be followed if required. (2) Each MAN Truck & Bus Group company shall ensure that the Group-wide procedure is implemented in accordance with the MTB Brand Instruction MA_13_1_09 – Information Security Incident Management. All employees must be instructed and trained in the procedure by the MAN Truck & Bus Group companies.
Article 4	Function Ensure the secure cooperation with suppliers, partners, and customers. Purpose To appropriately protect information, IT applications and infrastructures in the scope of the responsibility of MAN Truck & Bus that are used by, communicated to, managed by, or made accessible to external parties.	(1) Access to MAN information shall be granted to third parties where there is a specific reason, and their access must be restricted to such an extent that it can be monitored and properly traced. (2) The compliance to the requirements of the MAN Truck & Bus Group concerning the levels of confidentiality, integrity and availability of information, IT services and IT systems shall be clearly defined in contracts with external service providers with regard to their duties. (3) Agreements or contracts signed with third parties, regulating access and processing of data, shall cover all relevant security requirements.

Note: Printed versions and local files may not be updated!

Article	Function and Purpose	Regulation
Article 5	Function Business and IT service continuity management. Purpose To ensure an optimized approach concerning IT Service Continuity in case of disaster or emergency.	(1) All MAN Truck & Bus Group companies shall establish an integrated business and IT service continuity management process. (2) Based on a business impact analysis, Emergency measures appropriate to the determined risk shall be identified, regularly tested, and adjusted. (3) Information- and personal data protection must be ensured even during disasters and emergencies.
Article 6	Function Evaluate and manage company assets with regard to Information security. Identification and classification of information assets. Purpose To create basic principles for assessing an appropriate security level at MAN Truck & Bus Group.	(1) Information assets and associated information and communication technology facilities and rooms, incl. their software and supply equipment shall be clearly identified, classified, and managed as inventory stock. (2) Compilation of the inventory shall incorporate all necessary assets and shall be verified and managed on a regular basis. (3) All information assets and associated information and communication technology facilities incl. their software and supply equipment shall be assigned to a responsible data/asset owner. (4) All information processed and stored at and/or for MAN shall be classified with regard to its confidentiality, availability and integrity level in accordance with the MTB Brand Instruction MA_13_1_03 – Classification of Information Assets.
Article 7	Function Appointment Employment and hiring of personnel. Purpose To ensure that employees, contractors, and third-party users understand their responsibilities with regard to the protecting of MAN Truck & Bus SE information values. To ensure that personnel possess appropriate corresponding skills for to their intended tasks and with regard to protecting information appropriately.	(1) Before taking up a task and/or assuming a function in the MAN Truck & Bus Group, employees, contract partners, and third parties shall make themselves aware of the policies and guiding principles for information security that are relevant to their activity/functional division. Employees, contract partners, and third parties are required to commit themselves to comply to these regulations in their respective contracts. (2) Individuals with that have access to sensitive areas with relevance to information assets security (e.g., Data Center, development department) or with access to other sensitive information (e.g. personal data) shall separately be required to commit themselves to adhere to the information and data protection requirements.

Note: Printed versions and local files may not be updated!

Article	Function and Purpose	Regulation
Article 8	Function Control and management of personnel. Purpose To ensure that employees, contractors, and third-party users recognize potential threats to information security, understand their requirements when it comes to protecting information values, and comply with corresponding policies and guidelines.	(1) Regular information security training shall be conducted and documented on a workplace level. Employees shall be informed of changes, news, and threats on a regular basis. (2) Individuals with a supervisory function shall not take on any administrator roles in the same scope of responsibility. (3) Employees performing tasks with a particular impact on information security interests shall be allocated sufficient time for the proper fulfillment of these tasks. (4) It shall be ensured that contacts are available outside of normal working hours to handle for critical security issues topics and to timely respond in good time, for example, to warnings alarms, for example, from facilities that are critical to security. (5) The Brand Policy MAN Truck & Bus MR_13_1 - Information Security which forms the basis for the MAN Truck & Bus Standard for Information Security and additional relevant regulations shall be considered an official regulatory system of MAN Truck & Bus SE the company and shall be agreed with employees and service providers as a contractual obligation. Violations of these regulations shall be met with appropriate measures under industrial law and/or contractual penalties.
Article 9	Function Termination and change of employment of personnel. Purpose To ensure as little impact as possible for MAN Truck & Bus with regard to the protection of information in case that employees, contractors, and third-party users change the organization or their role/function within the organization.	(1) It shall be ensured that in the event of termination or the change of role of personnel, information and assets are immediately returned to MAN Truck & Bus and entry and access rights are immediately revoked. This shall also apply to service providers where these conduct work for MAN Truck & Bus as part of their tasks.

Note: Printed versions and local files may not be updated!

Article	Function and Purpose	Regulation
Article 10	Function Security zones. Purpose To protect against unauthorized access and damage or interruption to IT infrastructures and information required for MAN Truck & Bus business and production processes.	(1) Based on the security requirements determined in a risk analysis, appropriate security zones shall be defined and established to offer appropriate protection against unauthorized access, environmental threats, fire, sabotage and power or cooling system outage. (2) The security zones shall be established according to the onion-skin principle. When connecting zones with different protection requirements access shall be terminated and controlled within the outer zone and reinitiated according to the protection requirements of the inner zone. (3) Access to a security zone shall only be granted where a specific need exists and the approval process shall be fully documented. The protection of zones shall also be guaranteed in delivery areas.

Note: Printed versions and local files may not be updated!

Article	Function and Purpose	Regulation
Article 11	Function Protection of information and communication technology facilities. Purpose To appropriately protect information and communication technologies against physical and environmental threats.	(1) Information and components of information and communication technology shall be secured in accordance with the required level of protection. They shall be protected against unauthorized access, environmental hazards, power outage, and cooling system outage whit the use of technical and organizational measures. (2) When using mobile information and communication devices, in particular, it shall be ensured that sensitive information cannot be compromised. The need to protect the information shall be determined as part of a risk analysis. (3) Power and cooling circuits which ease the transport of information shall be protected against damage. (4) Data and communication lines which transport confidential or strictly confidential information and/or data shall be protected against interception and if necessary, connections shall be encrypted. Data and supply lines that are critical to business operations shall be designed to include redundant lines. (5) Security and supply facilities shall be serviced and maintained such that their availability and integrity is ensured. (6) Suitable processes must be established for devices meant for reuse, disposal or resale to ensure that all confidential or strictly confidential data and licensed software on devices (fixed or mobile) are removed or securely overwritten. Storage media shall be disposed or destroyed in a way that data cannot be restored. (7) It shall be ensured that there is no unauthorized removal of information and communication facilities, software, or information from the security zones de fined for operation or storage. (8) In the case of remote working, it shall also be ensured that appropriate security measures are implemented in accordance with (1) – (6).

Article	Function and Purpose	Regulation
Article 12	Function Separation of development, test and production environments. Purpose To prevent unintended and/or unmonitored changes to productive system environments.	(1) Development and test environments must be separated from the production environment in order to prevent unauthorized access or changes to these systems. (2) A security concept must also be defined for test networks and a responsible person assigned. (3) In the event that production data files or copies thereof must be accessed for test purposes, these must be protected in the same way as with production processes. Use and the reasons for use must be documented. (4) Test data which represent confidential or strictly confidential information must be deleted immediately after processing. (5) Comprehensive processes shall be established for the transition from development and test environments into production in order that errors in the production environment are avoided.

Note: Printed versions and local files may not be updated!

Article	Function and Purpose	Regulation
Article 13	Function Ensure secure MAN Truck & Bus network and its interfaces. Purpose To protect against unauthorized use, interruption, and unauthorized flows of information.	(1) According to the required protection level the confidentiality, availability, and integrity of data shall be protected during transport over networks. Security measures shall be selected according to the nature and composition of the transmission path within the network (wireless LAN, WAN, LAN) and must consider the protection requirement. Confidential company data must be encrypted when being transferred over public networks. (2) With regard to functional use, all network components must be configured as restrictive as possible and protected against unauthorized access. The principle of least privilege shall be applied. (3) For network components that are related to critical business processes, the need for monitoring and logging measures shall be assessed and set up accordingly. The resulting log data shall be verified, if possible, automatically, on a regular basis. (4) For the connections of networks with different security requirements a risk analysis shall be conducted. Based on this suitable processes shall be defined and documented. An approval process shall be established and documented. (5) Access between different networks with different security levels shall be restricted. For the definition of permitted access options to internal resources, a zone concept shall be developed. Networks shall be separated logically according to their security requirements. (6) The security characteristics, service levels and administration requirements of all network Services must be identified and documented. Compliance with applicable security requirements in the network must also be part of contracts with external service providers. (7) Remote access of users to systems or applications may only be carried out by means of strong authentication. (8) All systems connected to the MAN network (internal network) must be clearly identifiable.

Article	Function and Purpose	Regulation
Article 14	Function Protection of information on portable media. Purpose To prevent unauthorized publishing, modification, removal, or destruction of MAN information.	(1) When exchanging information using portable media, the media shall be adequately protected in accordance with their protection needs. (2) Removable media shall be handled in accordance with the protection needs of the data stored. (3) If disposal is necessary, it shall be ensured that confidential data is destroyed such that it cannot be restored from the media. (4) Documented procedures for secure handling (storage and distribution) of information (on portable media) must be established to prevent unauthorized access, misuse, or manipulation. All employees must be made aware of the correct handling of information and data storage media according to Appendix 1 to MA_13_1_03 – Handling of Classified Information (5) Employees are to be obliged to protect information and media against unauthorized access when leaving their workplace, even for a short period. (6) Encryption mechanisms must be established following a cryptographic concept with regard to their application, key management, and legal aspects.

Note: Printed versions and local files may not be updated!

Article	Function and Purpose	Regulation
Article 15	Function Protect internal and external communication. Purpose To prevent leakage or disclosure of MAN information.	(1) The transfer of data within the MAN Truck & Bus network or from there to the outside may only take place via approved interfaces in accordance with their respective protection requirements. Regulations must be documented. (2) When transferring personal data, legal requirements and the specifications of the MAN Truck & Bus Data Protection Policy shall be complied to. If necessary, the agreement of the person who is the subject of the data being transferred must be requested in advance. The same applies to automatic call procedures. (3) Regulations and/or contractual agreements (non-disclosure agreements) must be signed in relation to the need for handling of any sensitive data by the recipient. (4) To cover the risks of electronic data transfer separate regulations for sending sensitive information must be made. Users of e-mail systems must be aware of the risks of electronic communication. Corresponding training measures shall be documented. (5) Senders and recipients of non-public data must ensure that the confidentiality of the information is preserved. If the stored data is no longer required, it must be deleted. Data subject to retention must be archived accordingly. (Appendix 1 to MA_13_1_03 – Handling of Classified Information). (6) The storage of business e-mails is only be permitted in MAN Truck & Bus environments or environments operated on behalf of MAN Truck & Bus. (7) Access to centrally stored e-mails via public networks shall only be permitted via secure, verifiable connections. Secure authentication procedures shall be used. (8) The use of electronic communication means shall only be permitted for business purposes and only via centrally provided Internet gateways or preset access paths.

Note: Printed versions and local files may not be updated!

Article	Function and Purpose	Regulation
Article 16	Function Management of authorizations and authentications. Purpose Allocation of access permissions according to the least privilege principle, appropriate documentation and effective access protection	(1) A policy for access rights shall be established and verified regularly based on business and security requirements. (2) A formal procedure shall be established for the registration and de-registration of users. Registrations and de-registrations shall be documented in an audit-proof form. It shall be ensured that users only receive authorization appropriate to the tasks that they are required to carry out (least privilege and need-to-know principle). (3) The allocation of administrative system authorizations shall be carried out restrictively, documented with care, and verified on a regular basis. (4) Privileged user accounts shall not be used for everyday work. (5) Requirements for authentication shall be defined centrally and shall be evaluated on a regular basis and be implemented in accordance with the requirements of developing technologies. Authentication factors shall be managed in accordance with documented procedures. (6) Existing access authorizations shall be reviewed at regular intervals. These intervals shall be determined according to the extent and criticality of the access rights.
Article 17	Function Protection of electronic commerce Purpose Protection of E-Business applications.	(1) The online business services of MAN Truck & Bus shall ensure the authorization and authentication as well as the confidentiality of the information stored or processed to an extent appropriate to the need for protection. (2) The integrity of MAN information that is made available on a publicly accessible system, shall be protected to prevent unauthorized modification.

Article	Function and Purpose	Regulation
Article 18	Function Protect system use and logs Purpose To identify unauthorized use and modification of systems and applications.	(1) In the event of a legal obligation to provide evidence, contractual business requirements or for the purpose of averting danger, log data must be collected and stored. In doing so, the principle of data economy must be applied and – as far as in accordance with the intended purpose, anonymization must be carried out. (2) General conditions shall be created to allow security incidents and serious interruptions to MAN Truck & Bus business processes to be tracked and evaluated via all participating networks, systems, and applications. The system times of all MAN Truck & Bus systems and network components shall be synchronized if this is technically feasible. (3) Log data and log files shall be retained for a fixed period in case they may be useful in future investigations. Logs shall be protected against unauthorized access and manipulation and shall be deleted upon expiry of the fixed retention period. Personal data shall be deleted as soon as they are no longer required. (4) Employees who are involved in the creation, verification, and evaluation of log data are required to sign a confidentiality agreement. The evaluation of personal data shall be coordinated and jointly undertaken with the responsible data protection officer and the responsible works council. (5) As a result of a risk assessment, the necessary scope and content of protocol information of the identified systems shall be measured on the basis of the legal and operational requirements. As a minimum, information shall be available which adequately enables the tracking of security incidents. (6) Privileged activities within the operational management of IT systems must be logged and personally traceable. The protocol procedures shall be checked cyclically by an independent authority for conformity with the defined procedures. (7) The evaluation of the log files must be carried out in such a way that events critical to security are detected promptly. Care must be taken to ensure that personnel are adequately trained to evaluate the protocol information. (8) All access to systems containing vulnerable data or functions shall be ensured by means of access protection where the identity of the user is determined. (9) IT systems that process information with specific protection requirements shall be located in a dedicated (or isolated) environments where possible. Isolation may be affected either physically or logically. Information shall only be exchanged by these IT systems with pre-determined systems. In the event that IT systems and/or applications with high protection requirements have to be stored in heterogeneous environments, the resulting risks must be identified and evaluated separately.

Article	Function and Purpose	Regulation
Article 19	Function Use of information and communication facilities and equipment Purpose To secure the use of information and communication facilities and devices.	(1) After a defined period of inactivity of the user, an automatic blocking must take place where technically possible [e.g. screen, smartphone]. (2) It is prohibited to connect personal equipment to the internal LAN/WLAN or Intranet of the MAN Truck & Bus Group.
Article 20	Function Documentation of procedures, systems and functions relevant for the operational security of IT by internal and external IT service providers, as well as protection of procedures, systems and functions relevant for operational security by internal and external IT service providers Purpose The operating procedures are documented in such a way that in the event of a failure of personnel or the disruption of system functions, the normal operating condition can be restored as quickly as possible. Documentation of operating procedures, system configurations and operational organization is protected against unauthorized inspection.	(1) All procedures and systems necessary for proper operation must be documented in such a way that a restriction of business operations or security due to missing or defective documentation is excluded. (2) For operating procedures in which several organizational units or service providers work together regularly, the processes must be defined and documented in such a way that a restriction of MAN's business operations or the security of MAN due to insufficient definition or documentation is excluded. (3) For documentation which is necessary for operational processes or the restoration of critical business processes, it must be ensured that these are available in the event of far-reaching disturbances (e.g. in printed form, as an encrypted emergency CD). (4) The documentation must be protected against unauthorized access in accordance with the respective need for protection.
Article 21	Function Change management for internal IT services and services provided by external service providers Purpose Changes have the smallest possible impact on MAN Truck & Bus business operations.	(1) Changes to IT services or parts thereof (personnel, processes, hardware, and software) shall always be performed in accordance with standardized change management processes. All changes must be documented. (2) In the event of changes, the effects on the corresponding business processes shall be analyzed, evaluated, and documented as part of the risk management process.

Article	Function and Purpose	Regulation
Article 22	Function Controlled provision, monitoring and auditing of IT services by external service providers Purpose To ensure that the services and scope of supply are defined and can be complied to by external service providers, that deviations from the agreed services or scope of supply are identified and evaluated, and that suitable countermeasures are Initiated.	(1) In service contracts agreed with third parties and partners, in addition to functionality and quantity, the necessary protection of MAN's information assets with regard to their respective levels of availability, confidentiality and integrity must also be clearly regulated. The MAN information security regulations must be included in an appropriate form. (2) Controls and regular reports to confirm the compliance to requirements information security by service providers are to be evaluated, defined and contractually agreed. (3) Services provided by the supplier with regard to measures for protecting MAN information assets shall be documented in full by the corresponding contract partner on the basis of reports and logs and must be suitable for checking compliance with the agreed service level. (4) In contracts with service providers, MAN Truck & Bus must be granted the right to conduct audits at service providers' premises. This must also extend to all subcontractors. (5) If operating resources, devices or IT systems are sent away for maintenance or repair by MAN Truck & Bus or the service provider, all confidential or strictly confidential data located on data media, physical or digital storage device must be deleted or destroyed in advance to prevent the reconstruction of the stored data. The companies commissioned with the repair are obliged to comply to the necessary confidentiality agreements and NDAs. Specifically, it shall be determined that data that are stored externally as part of the maintenance work shall be deleted upon completion of the work and shall not be used for any other purpose.
Article 23	Function Manage capacities for internal IT services and those provided by external IT providers Purpose The timely identification and prevention of service bottlenecks.	(1) Capacity utilization for all IT components critical to business shall be documented and monitored on a regular basis. (2) Future capacity requirements shall be determined on the basis of trends and requirements in order to avoid bottlenecks and allow advance planning.

Article	Function and Purpose	Regulation
Article 24	Function Acceptance of systems based on defined criteria Purpose Definition and compliance with system requirement for IT services	(1) It shall be ensured that all new IT systems and services fulfill the MAN Truck & Bus Group's requirements for information security, in particular the information security standard. Exceptions from the baseline system hardening shall be evaluated and documented. The MAN Truck & Bus Standard for Information Security and its additional regulations represent minimum requirements for proper and secure operation. (3) A secure configuration shall be defined as part of system hardening for business-critical systems. Those shall be used as basis for a secure installation and serve as a checklist for monitoring.
Article 25	Function Data backup and recovery Purpose To ensure the restoration of lost or damaged data as quickly as possible, as well as outsourcing of data to cover emergency situations.	(1) A concept for data backup and recovery shall be defined for each system. This general concept shall also appoint responsibilities. (2) If data is distributed over different systems, overarching data consistency shall be ensured. (3) In the event of local or mobile data management, critical data shall only be stored as a copy or and only as long as necessary. For permanent storage only central storage systems shall be used. (4) The data security concept shall undergo a detailed test at least once a year. The result of the test shall be documented and stored as proof. (5) The same access restrictions shall apply to the transport procedure and the storage location of data backups as for systems on which original data are stored. Moreover, measures shall be taken to protect the data backup media against external impacts such as fire, water, theft, or sabotage. (6) Data backup media must be catalogued and have their completeness and readability tested on a regular basis. These shall be documented in an audit-proof form. (7) The ability to restore data critical to business shall be tested at least once a year. All tests carried out must be documented. (8) Specific measures shall be established for encrypted data or data media. (9) Data media that are no longer required or have been replaced shall be destroyed to prevent the reconstruction of stored data.

Article	Function and Purpose	Regulation
Article 26	Function Prevent malicious software and - mobile code Purpose To prevent the intrusion and spread of malicious software/code.	(1) A virus protection concept shall be drawn up by the responsible operator(s), to incorporate multi-stage examination of relevant items that may be affected by viruses by at least two different products from different manufacturers. (2) A virus scanner shall be installed on each workplace computer or server on which data is stored or via which data are exchanged. The virus scanner shall be initiated automatically on system start, shall download updates automatically where possible, and shall be prevented from being shut down during operation. (3) Different products from different developers shall be used for workplace computers and servers. (4) All data traffic from or within public networks shall be automatically checked for viruses by a central virus protection system. Virus protection shall be able to check compressed or encrypted files where technically possible. Internal e-mail traffic shall also be checked by a virus scanner. It shall be ensured that the scanner used for e-mail traffic virus scanning cannot become the victim of an attack itself. Suitable measures to protect the virus scanner shall be taken. (5) A procedure must be developed and introduced for the correct handling of virus-prone content in electronic media such as e-mails or text files. Active content, for example in downloads or web offers from public networks, must be checked for system-compliant behavior by central systems before it is transmitted to the MAN Truck & Bus network. (6) Only those services and functionalities shall be made available on the systems (client and server) that are required for the intended purpose. (7) Security software and settings shall be configured such that no modifications are possible by the user and that the function cannot be switched off. (8) IT systems in production environments (such as industrial PCs) shall be protected against malicious software if these systems provide access to the Internet, or mobile data media are used. If this is not possible, these systems shall by isolated as appropriate by means of network separation and deactivation of ports. (9) Mobile devices with access to MAN Truck & Bus Company data must be suitably protected against malicious software and spying on Company data.

Article	Function and Purpose	Regulation
Article 27	Function Procurement, development, and maintenance of information systems Purpose Protecting the procurement, development, and maintenance of information systems.	(1) The procurement of information-processing components (software, systems, networks, telecommunication systems, etc.) shall be subject to a comprehensive release and change management process in which a defined acceptance and release procedure is also included. Predetermined ordering regulations shall be maintained. (2) The consideration of risks and protection requirements must be an integral part of the processes for the procurement and development of new information processing components (software, systems, networks, telecommunications systems, etc.). (3) A catalog of requirements shall be compiled already at the pre-selection phase, in which the security requirements are formulated. The requirements shall be documented and approved. In the case of software, it shall be documented which versions of executable files have been approved. (4) It shall be ensured that hardware and software cannot be modified or manipulated after their approval. (5) In the event that program errors occur during operation in spite of intensive acceptance tests, these shall be resolved as part of the incident/problem management and release management processes. (6) The installation and/or use of unapproved software shall be prohibited and technically prevented. Approved programs shall be checked for modifications on a regular basis. (7) The use of unapproved software shall be detected by means of regular checks. The results of these checks shall be documented in audit-proof form. (8) In the case of software that is developed internally or externally, the requirements of the Standard for Information Security and additional guiding principles shall be taken into account in the development process.
Article 28	Function Continuous improvement Purpose To identify and evaluate deviations and vulnerabilities as well as ensure their timely resolution.	(1) It shall be possible to obtain and evaluate information concerning technical vulnerabilities in the systems and applications used at MAN Truck & Bus in a timely manner. (2) The risk of identified vulnerabilities shall be evaluated. Measures shall be taken to appropriately address the associated risk. (3) Organizational structures, roles, responsibilities, and lines of communication shall be defined. (4) In order to identify and tackle attacks and network hacking attempts at MAN Truck & Bus in a timely manner, systems shall be used to automatically detect and/or prevent attack patterns and hacking attempts. (5) Compliance to information security rules and measures shall be verified on a regular basis by an independent body and also in the event of significant changes with an impact on information security. The audits can be carried out by the auditor, MAN's data protection officer, independent quality departments and/or external experts.

Article	Function and Purpose	Regulation
Article 28	Function Continuous improvement Purpose To identify and evaluate deviations and vulnerabilities as well as ensure their timely resolution.	(6) It shall be possible to obtain and evaluate information concerning technical vulnerabilities in the systems and applications used at MAN Truck & Bus in a timely manner. (7) The risk of identified vulnerabilities shall be evaluated. Measures shall be taken to appropriately address the associated risk. (8) Organizational structures, roles, responsibilities, and lines of communication shall be defined. (9) In order to identify and tackle attacks and network hacking attempts at MAN Truck & Bus in a timely manner, systems shall be used to automatically detect and/or prevent attack patterns and hacking attempts. (10) Compliance to information security rules and measures shall be verified on a regular basis by an independent body and also in the event of significant changes with an impact on information security. The audits can be carried out by the auditor, MAN's data protection officer, independent quality departments and/or external experts.
Article 29	Function Compliance with legal framework conditions Purpose Ensuring the implementation of legal requirements and early detection of violations.	(1) For MAN Truck & Bus, it must be identified which laws contain relevant regulations on information security and which relevant regulations must be complied with. International laws and regulations to be observed are also included here.. (2) In order to protect the rights to use, for example, proprietary software products, procedures shall be implemented in order to compliance with relevant legal, official and contractual requirements. (3) Legal requirements for storage and documentation obligations are to be identified. Corresponding requirements for their compliance must be implemented. (4) A procedure must be established to ensure that only software for which appropriate licenses are held is used on MAN Truck & Bus systems. (5) With regard to data protection in the MAN Truck & Bus Group, the relevant national and international data protection regulations must be complied with. (6) Appropriate procedures shall be used to ensure that there is no access via the Internet to certain data that violates laws or other regulations or is not desired by MAN Truck & Bus companies.

Article	Function and Purpose	Regulation
Article 30	Function Compliance to the MAN Truck & Bus regulatory system for information security Purpose Ensuring the implementation and compliance of employees with information security regulations in the Group, detecting deviations and initiating appropriate measures	(1) Those responsible for information security (CISO/ISO) must ensure that the MAN information security regulations are correctly applied at MAN in order to achieve compliance with security regulations and standards. (2) In the event of deviation from or violation of the MAN Truck & Bus regulatory system for information security, reasons shall be obtained, measures to prevent violation and deviation shall be developed and introduced, and the effectiveness of these measures shall be verified. (3) A reporting system shall be developed that ensures the transparency of the implementation of the MAN Truck & Bus regulatory system for information security within the MAN Truck & Bus Group and at service providers.
Article 31	Function Verification of information security Purpose Detection of deviations in the planned implementation, determination of non-compliance with information security regulations.	(1) All working processes, plant equipment, devices, and IT systems shall be checked by means of regular audits to ensure their compliance with the MAN Truck & Bus regulatory system for information security. (2) These verifications shall be traceably documented and the results protected against unauthorized inspection. (3) A verification plan shall be formulated to ensure the completeness of verification aspects and verification objects. (4) Technical information security must be assessed by measures such as regular penetration tests or security audits. (5) The organizational information security must be checked by regular process audits such as self-assessments, on-site assessments, management assessments or assessments by external partners.

6 Change History

Version 3.0

- Added Change Log
- Relabeling
- Change in roles and responsibilities
- Adjusted References to reflect new Policy structure

Note: Printed versions and local files may not be updated!

Classification of Information Assets

Created	Steven Rauwerdink Ralf Schlag	**Approved**	Andre Wehner	**Version**	3.0
Dept.	FIOS	Dept.	FI	**KSU-Class:**	xx
Applicable as of		**Scope**		**Approved by (Board)***	
Date	01.02.2023	MAN Truck & Bus SE and its Subsidiaries			
				Agreed by	

* Only required for Brand Instructions that do not relate to a superior Brand Policy

Contents

Note: Printed versions and local files may not be updated!

Appendix

1 Purpose

All information assets at MAN Truck & Bus Group must be classified and labelled by the Information Owner and/or Business Owner of the process with reference to their confidentiality, integrity, and availability levels. Classifications must be documented in a way that ensures traceability. A validation of the classification has to be performed regularly according to the life cycle of the respective information asset.

The purpose of this Brand Policy Instruction is to define the binding principles for classification of information assets and dealing with information as required by Brand Policy MAN Truck & Bus MR_13_1 Information Security.

2 Scope

This Brand Policy applies to MAN Truck & Bus SE and its subsidiaries and their employees worldwide. This Brand Policy is to be implemented directly and does not require conversion policies from the individual subsidiary. In the case of companies in which MAN Truck & Bus SE cannot directly enforce the applicability of this Brand Policy for legal reasons, the policy owner has to be consulted to clarify the extent to which this Brand Policy is applicable. Companies which are not wholly owned by MAN Truck & Bus SE and also not subsidiary with MAN Truck & Bus SE through a control agreement constitute one such example (e.g. Subsidiaries which are wholly owned by MAN Finance and Holding S.A.)

In the event of any subsidiaries having their own regulations governing the enactment of Policies, these must be annulled with immediate effect. Until such time as Policies of this kind, either wholly or in part, are annulled, this Brand Policy takes precedence.

If the rules contained in this Brand Policy cannot be implemented due to mandatory local requirements, the individual Subsidiary needs to inform the policy owner of MAN Truck & Bus SE without undue delay to discuss required changes or adaptations.

3 Terms and definitions

A glossary for the complete information security framework can be found at the additional information „Terms and Definitions to information security “.

4 Target Group

MTB Brand Instruction MA_13_1_03 – Classification of Information Assets is directed to the individuals responsible for the management of information security within the MAN Truck & Bus Group (cf. MTB MR_13_1, section 6.1).

Requirements for external service providers regarding to confidentiality, integrity, availability, IT services and IT systems that result from this instruction must be covered and contractually agreed within the respective contracts according to the task of the service provider.

5 General Principles

Information assets may be available in a variety of forms and media, including the following:

- electronic (e.g., partner systems, customer information, inventory data, e-mails, Internet)
- on data storage media (e.g., external hard disks, CDs, DVDs, USB sticks, chip cards)
- in paper form (e.g., written material, documents, fax printouts, drawings, publications)
- in human memory (e.g., expert knowledge about a business process)

Note: Printed versions and local files may not be updated!

- verbal (e.g., face-to-face conversations, telephone conversations, messages, voice recordings, presentations)
- visual (e.g. as pictures, videos)

All information, regardless of the form in which form it appears, requires the same level of protection based on its classification.

6 Classification of Information Assets

6.1 General requirement

Information assets at the MAN Truck & Bus Group must be protected against the relevant threats identified in an appropriate, effective, and thorough manner. The protection goals of availability, integrity, and confidentiality must be ensured in a way which is appropriate and economically sound.

Protection requirements for the information assets of the MAN Truck & Bus Group are defined using the detailed security levels below. This provides the basis for a uniform method of classifying and assessing protection objectives.

If handling information that require a certain kind of secrecy, e.g. military related information, it is essential to proceed in accordance with the requirements of local legal guidelines, e.g. the German Geheimschutzhandbuch (manual on the protection of classified information) of the Bundesministerium für Wirtschaft und Technologie (Germany's Federal Ministry of Economics and Technology).

All information assets at MAN Truck & Bus Group must be classified and labelled by the information owner and/or business owner of the process with reference to their confidentiality, integrity, and availability. Classifications must be documented in a way that ensures traceability. A validation of the classification has to be performed regularly according to the life cycle of the respective information asset.

6.2 Supporting questions for determining the information class

The following questions can be used to support classification of own information and simplify assignment to the respective classification levels:

- Would there be a legal, financial, operational, privacy and/or safety issues if the information fell into the hands of competitors? If yes, how would you rate the impact?
- Would there be a possible loss or damage for MAN Truck & Bus Group business areas if the information is no longer accessible, available or destroyed? If yes, how would you rate it?
- Is there any expected impact on customer confidence in the MAN Truck & Bus Group, our public image, or the behavior of our shareholders?
- Would the unintentional loss or destruction of information be associated with high costs for the MAN Truck & Bus Group, the division or Group Company?
- Could publication of this information lead to infringements of the law, other legal consequences, or breaches of other regulatory or contractual obligations?
- Could the misuse or the publication of this information lead to investigations by the authorities?

- What impact would unintentional loss or destruction of this information have on the motivation of MAN Truck & Bus Group employees? Can the information be restored in the event of destruction or loss and what would be the necessary effort (in terms of time and money)?
- What could be the consequences if information integrity is compromised? How would you rate financial, operational, privacy and/or safety consequences?
- What would be the impact an information asset is not or no longer available. Would there be financial, operational, privacy and/or safety consequences?

6.3 Confidentiality

Information that is not intended for general publication must be made accessible only to those who are authorized to access it. To achieve the needed confidentiality the access to information has to be managed and information disclosure to unauthorized individuals, entities or processes have to be ensured with the aim to protect MAN Truck & Bus SE‘s intellectual property, customer and employee information. The following methods serve for this:

- Evaluation, classification
- Authentication
- Encryption

The confidentiality of information must be classified by the information owner and/or business owner of the process in one of the following security levels: "Public information", "Internal information", "Confidential information" or "Strictly Confidential information".

Note: Printed versions and local files may not be updated!

Levels of confidentiality

Security level	Significance	Treatment	Examples[1]
Level 1: **Public** **information**	• Information is classified as public if it is not subject to any restrictions and can be published by the company in the media • Public information assets are intended for dissemination or use in the public (e.g. the press) or virtual domain (general Internet, such as forums, Facebook, etc.) and requires approval prior publishing by the relevant parties at MAN Truck & Bus. • Public information does not represent a risk to MAN Truck & Bus in terms of its dissemination or use in the public (e.g. the press) or virtual domain (general Internet, such as forums, Facebook, etc.).	• Special protective measures are not required. • If information assets are documented as "public", steps must be taken to ensure that no information belonging to higher security levels can be disclosed. • Agreement must be reached with the authorized units (e.g. Corporate Communications) as to which information is classified as public before it is disseminated or published. • The formal procedure for the release of public data must be followed. • The word "public" must be written on all items for labeling purposes.	• Press releases after publication • Product catalog for customers • Advertising films • Product descriptions • Contents in terms of Internet presence • Advertising photographs • Press releases • Publications in magazines and books • Pictorial brochures • Presentations at public meetings

Note: Printed versions and local files may not be updated!

[1] Classification of a specific information asset has to be performed case by case. The examples mentioned here are therefore not obligatory.

Security level	Significance	Treatment	Examples[2]
Level 2: **Internal** **information**	• Information is classified as internal if it is intended solely for internal use and not for the general public. • "Internal" information has a limited negative impact on the MAN Truck & Bus Group if made public or revealed to unauthorized parties. **"Internal" is the standard security level for all information at the MAN Truck & Bus Group not classified or labeled in any other way.**	• It is essential to ensure that no person outside the MAN Truck & Bus Group Companies has access to the information. This applies to processing, storage/retention, transport/dispatch, and disposal/destruction. • Information classified as internal may be distributed only within the MAN Truck & Bus SE and the associated majority holding companies. External service providers must sign a separate nondisclosure agreement before access can be granted to "internal" information. These must contain terms of use and the internal character and the protection need must be pointed out. Access to systems providing internal data require at least weak authentication.	• Glossary • Business e-mail address • Department representation • IT-Security Guidelines • Intranet contents • Brand policies and Instructions • Internal informal presentations • Information for employees • Works agreements

Note: Printed versions and local files may not be updated!

[2] Classification of a specific information asset has to be performed case by case. The examples mentioned here are therefore not obligatory.

Security level	Significance	Treatment	Examples[3]
Level 3: **Confidential information**	• Information is classified as confidential if disclosure to unauthorized parties could jeopardize the attainment of product and project objectives. Such information must therefore be made available only to a limited group of authorized persons. • Confidential information is only intended for a limited group of people, usually MAN internal, and not for the public. • Confidential information has a considerable negative impact on MAN Truck & Bus SE as a company when made public or revealed to unauthorized parties (e.g. financially, in terms of the competition, or from a legal perspective). Personal data must always be classified as confidential.	• Confidential information may only be disclosed to a group of employees designated by the information owner and/or business owner/ process owner who need this information to carry out their duties ("need-to-know" principle). The information may only be copied after consultation with information owner and/or business/process owner. • External service providers must sign a separate non- disclosure agreement before access can be granted to confidential information. Access to systems providing confidential data require strong or very strong authentication.	• Budget plan • Roles and rights • Home address • Personal data e.g. salary information • Annual reports for individual Group companies • Development information • Data for internal accounting • Audit reports

Note: Printed versions and local files may not be updated!

[3] Classification of a specific information asset has to be performed case by case. The examples mentioned here are therefore not obligatory.

Security level	Significance	Treatment	Examples[4]
Level 4: **Strictly Confidential information**	• Information is classified as strictly confidential if disclosure to unauthorized parties could jeopardize the attainment of corporate objectives in the long term. Such information must therefore be limited to an extremely restricted distribution list and subject to stringent controls. • Strictly confidential information is only intended for individually nominated people. • "Strictly confidential" information has an extremely negative impact on the MAN Truck & Bus Group, its shareholders, business partners, or employees when made public or revealed to unauthorized parties. (For example, if the existence of one or more MAN Truck & Bus Companies is jeopardized or considerable legal consequences must be expected for MAN Truck & Bus SE.)	• Strictly confidential information/data may only be made available by the information owner and/or business owner/process owner to the persons referred to by name in each case. It is essential to ensure the identity of the recipient can be checked and proven before anything is passed on. • Decisions regarding the passing on or further processing of information are to be made by the owner of the information in each case. • A separate non-disclosure agreement must be signed before access can be granted to strictly confidential information. • Information of this type may not be copied. The information owner and/or business owner/process owner must register each existing copy with a serial number for paper documents and data carriers. In the case of electronic distribution, this numbering may be waived if proof of the transfer is given. The disclosure of strictly confidential information to third parties, e.g. business partners is prohibited. If this is unavoidable in individual cases, the modalities must be determined with the involvement of the Legal Department. Access to systems providing strictly confidential data require very strong authentication.	• Health records • Political, religious and philosophical beliefs of individuals • Personal Data on ethnic and cultural origin • Sexuality • Trade union membership • Design models until SOP • Camouflage information of specific models • Group annual reports for publication • Trade secrets • Insider information • Worker Council minutes • Supervisory Board minutes

[4] Classification of a specific information asset has to be performed case by case. The examples mentioned here are therefore not obligatory.

6.4 Integrity

The integrity of information is important to ensure error-free processing of information as well as protection against unauthorized changes. To achieve a required level of integrity the changes of information must be monitored and unnoticed changes must be avoided. Changes need the right level of authorization and can be controlled with the following methods:

- Changelog
- Change approval
- Checksum

The integrity of information is categorized in one of the following security levels by the information owner and/or business owner/process owner: “Unsecured Integrity”, “Secured Integrity”, “Verifiable integrity” or “Signed Integrity”.

Levels of Integrity

Security level	Significance	Treatment	Examples[5]
Level 1: Unsecured integrity	• Information/data with unsecured integrity is information only used once or which can be restored without any expense. • An unauthorized change has no impact on MAN Truck & Bus Group business operations.	• With information/data classified as "unsecured integrity", no special measures need to be in place for ensuring its integrity or non-repudiation.	• Menus • Copies of public information

Note: Printed versions and local files may not be updated!

[5] Classification of a specific information asset has to be performed case by case. The examples mentioned here are therefore not obligatory.

Security level	Significance	Treatment	Examples[6]
Level 2: Secured integrity	• Information/data with secured integrity is information used more than once or which can be restored at moderate expense if it undergoes unauthorized change. • An unauthorized change to the information/data has a limited negative impact on a division or MAN Truck & Bus Group company and only a very low impact on the MAN Truck & Bus SE. **"Secured integrity" is the standard security level for all information at the MAN Truck & Bus Group not classified or labeled in any other way.**	• Information/data classified as "secured integrity" must feature precautionary measures to prevent changes by unauthorized parties. • This applies to processing, storage/retention, and transport/dispatch. • With this level, the systems or applications used are generally responsible for ensuring the integrity and/or non-repudiation of information. • Changes are restricted to a defined group of people.	• Project work files • Meeting minutes
Level 3: Verifiable integrity	• Information/data with verifiable integrity is information used on several occasions or which can only be restored at very considerable expense if it undergoes unauthorized change. • An unauthorized change to information/data has a considerable negative impact on the MAN Truck & Bus SE.	• Information/data classified as "verifiable integrity" must feature precautionary measures to prevent changes by unauthorized parties. • Information/data classified as "verifiable integrity" must make it possible to identify breaches of integrity. • Verifiable documentation of a clear identifier ensures non-repudiation. • Changes are documented in a way that ensure traceability and may only be made by a limited, authorized, and clearly identifiable group of people.	• Work instructions • Test reports • Security instructions • Minutes of Workers Council meetings • Product descriptions • Contents in terms of Internet presence • Press releases • Pictorial brochures • E-mails

Note: Printed versions and local files may not be updated!

[6] Classification of a specific information asset has to be performed case by case. The examples mentioned here are therefore not obligatory.

Security level	Significance	Treatment	Examples[7]
Level 4: Signed integrity	- Information/data with signed integrity is information used on several occasions or which can no longer be restored if it undergoes unauthorized change. - An unauthorized change to information/data has an extremely negative impact on the MAN Truck & Bus Group, its shareholders, business partners, or employees. (For example, if the existence of one or more MAN Truck & Bus companies is jeopardized or considerable legal consequences must be expected for MAN Truck & Bus SE.)	- This kind of information/data must feature precautionary measures to prevent changes by unauthorized parties. - Information/data must have a personal or digital signature for the purpose of integrity verification. - Activities such as drafting, checking, approving, sending, or ownership of information must be clearly documented. - It must be possible to trace and verify each change according to a clearly documented procedure and changes may only be made by persons referred to by name and uniquely identifiable.	- Brand Policies - Brand Policy Instructions - Works agreements - Annual reports - Balance sheets - Documented development statuses

6.5 Availability

The availability of information must be made available within an agreed time frame. The information have to be classified by the information owner and/or business owner/process owner in one of the following security levels: "Requirement not defined", "Available", "Highly available".

To achieve a good level of availability, the availability should be monitored. To recover in time from failures can be very important why the following methods are important:

- Service monitoring
- Service Level Agreement (SLA)
- Failover plan

The person responsible for information (information owner) must determine and document the criticality of the availability of information. Information of any level of confidentiality can be critical to availability.

[7] Classification of a specific information asset has to be performed case by case. The examples mentioned here are therefore not obligatory

Levels of Availability

Security level	Significance	Treatment	Examples[8]
Level 1: Requirement not defined	- Non-availability of the information has no impact on business operations of a MAN Truck & Bus Company or the MAN Truck & Bus SE.	- Level 1 information/data, IT Systems and IT Services are not subject to any special requirements in terms of availability. - The procedures are based on the sensible and financially reasonable implementation of measures and processes.	- Offline data from the Internet - Working copies
Level 2: Available	- Non-availability of the information has an impact on the business operations of a MAN Truck & Bus Company, but without jeopardizing its existence, and only has a limited negative impact on the MAN Truck & Bus SE. **"Available" is the standard availability level for all information at the MAN Truck & Bus Group not classified or labeled in any other way.**	- With information/data, IT Systems and IT Services classified as "available", it must be possible to restore or replace those within a clearly defined period. - There must be a restoration concept to ensure, in the event of an IT failure, that functions and information are available once more after the clearly defined period. - The availability concept must be documented.	- Internet presence - Brand Policies - Brand Policy Instructions - Intranet - Pictorial brochures - Publications - Time consuming presentations - Development papers - IT Systems, e.g., servers

Note: Printed versions and local files may not be updated!

[8] Classification of a specific information asset has to be performed case by case. The examples mentioned here are therefore not obligatory

Security level	Significance	Treatment	Examples[9]
Level 3: Highly available	- Non-availability of the information has a substantial negative impact on the MAN Truck & Bus Group, its shareholders, business partners, or employees. (For example, if the existence of one or more MAN Truck & Bus companies is jeopardized, considerable legal consequences must be expected for MAN Truck & Bus.)	- Minimum availability levels must be specified for both normal and emergency scenarios for information/data, IT Systems and IT Services. - Redundancy must be built in when using the information to ensure the restrictions to business processes associated with the failure or destruction of information and systems is kept to an acceptable level. - The availability concept must be documented in detail and verified on a regular basis. - A disaster recovery concept must be documented in detail and tested on a regular basis.	- Production management information - Financial reporting

6.6 Authenticity

The Authenticity of information is proving its Genuity. This goal ensures that the information has not been modified while in transit and that the receiving party can verify the source of the message. For tracking of information modification tamper-proof technologies have to be established. Methods for ensuring authenticity are implementing checksums and using digital signatures.

Note: Printed versions and local files may not be updated!

[9] Classification of a specific information asset has to be performed case by case. The examples mentioned here are therefore not obligatory

7 Change History

Version 3.0

- Added Change Log
- Relabeling to MAN Truck & Bus
- Change in roles and responsibilities
- Added reference to disposal policy
- Added requirements for authentication according to password policy
- Set German legislation as example only
- Changed table format for confidentiality to continuous text
- Added short table for confidentiality in appendix
- Take-over of corresponding level 3 document AN_MTB_13_1_02 “Umgang mit Informationen“
- Regular review
- Responsibilities update
- New chapter/table – 6.2 Confidentiality
- New chapter – 6.2.1 Disposal, destruction and deletion
- Rearranged – 6.2.2 Supporting questions for determining the level of confidentiality
- Update chapter – 6.3 Integrity
- Update chapter – 6.4 Availability
- New chapter – 6.5 Authenticity
- Assigned new document code number “MA_13_1_03” – was “MAN 13.1 Instruction 4 – Classification of Information Assets”
- „MAN 13.1 Instruction 3 – Information Security Incident Management“ assigned to new code „MA_13_1_09”

Note: Printed versions and local files may not be updated!

Appendix 1 : Handling of Classified Information

Note: Printed versions and local files may not be updated!

Note: Printed versions and local files may not be updated!

Appendix 1 - Handling of Classified Information

Created	Steven Rauwerdink Ralf Schlag	**Approved**	Andre Wehner	**Version**	1.0
Dept.	FIOS	Dept.	FI	**KSU-Class:**	xx
Applicable as of		**Scope**		**Approved by (Board)***	
Date	01.02.2023	MAN Truck & Bus SE and its Subsidiaries			
				Agreed by	

* Only required for Brand Instructions that do not relate to a superior Brand Policy

Contents

Note: Printed versions and local files may not be updated!

Note: Printed versions and local files may not be updated!

1 Purpose

The purpose of this Appendix is to define and describe in detail the requirements for handling of information with reference to its classification, as required by Brand Policy MAN Truck & Bus MR_13_1 Information Security and MTB Brand Instruction MA_13_1_03 – Classification of Information Assets.

The document provides detailed instructions to all MAN Truck & Bus employees and external contractors on the requirements for secure storage, exchange, presentation, labelling, printing and disposal of information and information assets, according to its confidentiality, integrity, and availability levels. Further, the requirements for secure handling of information in the Cloud and when working remotely are provided.

2 Protecting Information assets

2.1 General Requirements

It is mandatory to always apply the need-to-know principle regardless of the level of classification of information. This means that individuals will be granted access only to the information they need to fulfil their tasks.

- All data and information systems require responsible handling and may only be used for their intended purpose. In addition, information and information systems may only be used in such a way that MAN Truck & Bus SE cannot be legally liable.
- Users of information systems must comply with copyright and licensing agreements.
- Information provided by MAN Truck & Bus SE may not be used for personal gain.
- Any oral communication, whether in person or by telephone, must be conducted in such a way that the confidentiality of the information is ensured and is not accessible to unauthorized third parties.
- Electronic data carriers, such as CDs and USB-sticks, must be handled responsibly and as per their applicable classification level.
- If unsupervised documents marked as confidential or strictly confidential are found, they must be taken into safe custody and returned directly to the person responsible for the information or the owner of the information. If this person cannot be contacted, the documents must be handed over to the local information security officer (IS Manager) or to local or global security functions. Alternatively, the documents can be destroyed according to their classification.
- If unattended documents with personal data are found, they must be taken into safe custody and handed over directly to the responsible data protection officer.
- Confidential information of MAN Truck & Bus Group may not be stored on private systems or data carriers. A transfer to public services (e.g. translation into foreign languages, communication services) is only permitted with appropriate security precautions (e.g. encrypted transmission, dispatch by registered delivery) and non-disclosure agreements.

2.2 Information Security Protection Goals

The confidentiality, integrity, availability and authenticity are the most relevant protection goals related to information security. Specific technical and organizational measures guarantee the achievement of those protection goals.

2.3 Confidentiality

How to label information?

To indicate the confidentiality class of information labels are being used. The purpose is to show and remind the reader to carefully handle the information.

PUBLIC	**INTERNAL**	**CONFIDENTIAL**	**STRICTLY CONFIDENTIAL**
———	———	———	———
ÖFFENTLICH	INTERN	VERTRAULICH	STRENG VERTRAULICH

Example: Labels show the English classification together with the local language.

Including the confidentiality class also in the file name of a document helps to avoid mistakes when storing or transferring this information

Example: ***2022-03_F10-production-plan_confidential.xlsx***

How to achieve confidentiality?

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

Attaining

- Manage access to information,
- Avoid damage from information disclosure to unauthorized individuals, entities or processes,
- Protect MANs intellectual property customer and employee information

Methods

- Evaluation, classification
- Authentication
- Encryption

2.4 Integrity

How to ensure integrity?

Ensuring error-free processing of information as well as protection against unauthorized changes.

Attaining

- Monitor changes of information, avoid unnoticed changes,
- changes require the right level of authorization – review the access rights in regular basis

Methods

- Changelog
- Change approval

Note: Printed versions and local files may not be updated!

- Checksum

2.5 Availability

How to ensure the availability of the information?

Information has to be available within an agreed time frame.

Attaining

- Monitor availability, recover in time from failures,
- Manage expectations

Methods

- Service monitoring
- Service level agreement
- Failover plan

2.6 Authenticity

How to ensure the authenticity of information?

Information has not been modified while in transit and the receiving party can verify the source of the message.

Attaining

- Track modification of information,
- Establish tamper-proof technologies (e.g. document history)

Methods

- Checksum
- Digital signatures

3 How to handle information according to its classification?

3.1 Confidentiality

	STRICTLY CONFIDENTIAL STRENG VERTRAULICH	CONFIDENTIAL VERTRAULICH	INTERNAL INTERN
Storing			
Fileshare	Yes, on classified approved MTB Storage		OK, without special precautions
Outlook Mailbox	OK, if message encryption active	OK, if confidential tag active	
MS Teams / Sharepoint online	No	OK, if managed by TEAMS / SP Owner	
Physical Information	Never leave unattended, store in a safe	Never leave openly accessible, store locked	Never leave in public areas
Exchanging			
E-Mail (external)	No direct E-Mail, links to classified exchange	No direct E-Mail, only encrypted	Internal no precautions, external with NDA
Letter	Internal – personal external - approved courier	Internal – distribution bag external - registered post	Company mail or standard post
Presenting			
Presenter's due diligence	Only approved and confirmed audience Secured location No photos or recordings Corporate equipment	Only approved and confirmed audience Obligation for confidentiality Corporate equipment	Internal audience, no precautions External audience, with NDA

Note: Printed versions and local files may not be updated!

	STRICTLY CONFIDENTIAL STRENG VERTRAULICH	CONFIDENTIAL VERTRAULICH	INTERNAL INTERN
Labelling			
Documents	On each page		On the first page of the document
Pictures	Watermark – strictly confidential	Watermark – confidential	No label required
Printing			
Direct Printing	No, only print2me	OK, without special precautions	
Disposing			
Physical Information	Physically destroyed shredded on-premises or data disposal bin		waste containers on-premises
Digitally stored Information	HDD reliably overwritten USB Sticks, CD/DVD, shredded on-premises or disposed to data disposal bin Data disposal certificate		Reliable deletion of Data Disposal into waste containers on-premises
Mobile / Remote Work			
Employee's due diligence	Information should not leave premises without explicit authorization	Connect to secured network Access with corporate equipment only Maintain privacy, Protect screen, keep documents locked	
Cloud			
Account Owner's due diligence	Usage generally not allowed case by case evaluation by Information security Key management owned by MAN	Transport encryption, storage encryption Strong authentication Cloud provider with passed cloud vendor assessment	

Note: Printed versions and local files may not be updated!

3.2 Integrity

	Level 2 Secured integrity	**Level 3** Verifiable integrity	**Level 4** Signed integrity
Storing			
Digital/Physical Information	Information has to be stored in a place, where changes can be noticed (e.g. Change logs are implemented)		Changes must be noticeable and require a signature (e.g. physical or digital signature of a document)
Exchanging			
Digital Information	Transferring information via trusted channels and trusted routes (e.g. TLS, secure file transfer)	Keep evidence to verify the integrity of the transferred information (e.g. date of last change, last change made by User-ID)	exchanged information include a digital signature of the originator (e.g. of the last individual that changed the information)
Physical Information	Post physical information in an envelope using a trusted deliverer (e.g. letter send by post)	Post physical information in an envelope using a trusted deliverer with confirmation of delivery (e.g. by registered mail)	Sealed Envelope personally to the recipient confirmed by signatures (e.g. certified mail)
Printing			
Direct Printing	Personally verify that printout is correct		

3.3 Availability

	Level 2 Available	**Level 3** Highly available
Storing		
Digital Information	Avoid keeping information stored locally. Transfer information to reliable centrally managed storage (File Server or cloud storage). There information is backed up and can be restored on errors up to a certain age within the required time.	Only use certified storage that is matching the high availability goals using technologies cross data center mirroring, tested disaster recovery plans and certified archiving solutions
Physical Information	Keep documents filed in safe places that are protected against hazards like fire, flood, moisture	Work with copies of a document and keep the original in especially safe place like a vault or a certified document archive
Presenting		
Presenter's due diligence	To protect your presentation, assume technical failures and prepare accordingly (e.g. local copy, cloud copy, alternative presenting device, paper printout …)	
Mobile / Remote Work		
Employee's due diligence	Using the provided company equipment will meet the standard availability goal for accessing information while working remotely	For higher requirements on information availability you may create a local copy on a security certified encrypted device (e.g. secure hard drive)

Note: Printed versions and local files may not be updated!

4 Change History

Version 1.0

- Creation

Note: Printed versions and local files may not be updated!

Note: Printed versions and local files may not be updated!

Information Security for System Operation and Administration

Created	Steven Rauwerdink Ralf Schlag	**Approved**	Andre Wehner	**Version**	3.0
Dept.	FIOS	Dept.	FI	**KSU-Class:**	xx
Applicable as of		**Scope**		**Approved by (Board)***	
Date	01.02.2023	MAN Truck & Bus SE and its Subsidiaries			
				Agreed by	

* Only required for Brand Instructions that do not relate to a superior Brand Policy

Contents

Note: Printed versions and local files may not be updated!

1 Purpose

This Brand Instruction is derived from Brand Policy MAN Truck & Bus MR_13_1 Information Security and the MTB Brand Instruction MA_13_1_01 - Standard for Information Security. It defines the Information Security regulations that must be observed by all MAN Truck & Bus employees or external partners responsible for Information and Communication Technology systems (ICT systems) and infrastructure operation, administration and architecture. The document defines the responsibilities and regulations for protecting the confidentiality, integrity and availability of ICT systems and networks in their design phase as well as during their operation. Further, the password complexity requirements for administrator accounts are provided in this instruction.

2 Scope

This Brand Policy applies to MAN Truck & Bus SE and its subsidiaries and their employees worldwide. This Brand Policy is to be implemented directly and does not require conversion policies from the individual subsidiary. In the case of companies in which MAN Truck & Bus SE cannot directly enforce the applicability of this Brand Policy for legal reasons, the policy owner has to be consulted to clarify the extent to which this Brand Policy is applicable. Companies which are not wholly owned by MAN Truck & Bus SE and also not subsidiary with MAN Truck & Bus SE through a control agreement constitute one such example (e.g. Subsidiaries which are wholly owned by MAN Finance and Holding S.A.)

In the event of any subsidiaries having their own regulations governing the enactment of Policies, these must be annulled with immediate effect. Until such time as Policies of this kind, either wholly or in part, are annulled, this Brand Policy takes precedence.

If the rules contained in this Brand Policy cannot be implemented due to mandatory local requirements, the individual Subsidiary needs to inform the policy owner of MAN Truck & Bus SE without undue delay to discuss required changes or adaptations.

3 Terms and definitions

A glossary for the complete information security framework can be found at the additional information Terms and Definitions in Information Security“.

4 Target Group

This document is directed at MAN Truck & Bus employees or external partners who are responsible for developing, installing, operating, and configuring information and communication technology systems (ICT systems), as well as their managers.

Such MAN Truck & Bus employees include IT managers, system architects, personnel in charge of operations and all employees or external partners assigned with the tasks to configure ICT systems.

5 Information Security for ICT Systems

ICT systems are constantly exposed to a wide range of threats, therefore effective protection of these is essential in ensuring MAN Truck & Bus business objectives are met.

These threats are the following:

- Information loss due to breaches
- Unwanted Publication
- Disclosure to competitor

Note: Printed versions and local files may not be updated!

- Manipulation
- Infringement
- Losing ability to supply

5.1 Responsibility for the Information Security of the ICT Systems

The Application/System Owner is responsible for implementing the risk-oriented approach in regards to protecting the information security goals of the MAN Truck & Bus Group. Effective protection can only be achieved by implementing a combination of suitable measures. Part of these measures include:

- Integration of our employees with the corporate culture
- Security awareness for the entire company
- Compliance with defined processes and procedures
- Appropriate protection of information and communication devices and software

All MAN Truck & Bus Group employees or external partners assigned with the tasks to configure ICT systems are responsible to comply with the relevant MAN Truck & Bus regulations.

All application developers and system architects at MAN Truck & Bus Group are responsible for ensuring that the design, specifications, testing and migration of the ICT systems are in accordance with the relevant MAN Truck & Bus Brand Policy Instructions and regulations.

All individuals responsible for operation must ensure the operational security of the ICT systems within their area of responsibility in accordance with the relevant MAN Truck & Bus requirements. As part of this, the individuals concerned must be highly vigilant of any threats to the confidentiality, integrity and availability of information.

5.2 Requirements for the Design of ICT Systems

Brand Policy MAN Truck & Bus MR_13_1 Information Security and MTB Brand Instruction MA_13_1_01 - Standard for Information Security must be complied with when designing ICT systems. In addition to the above, the following also apply:

- As part of the development and specification phase of an ICT system, a risk analysis, based on the ISi Assessment methodology must be performed.
- Planning of future capacity requirements must take into account new business and system requirements as well as current and foreseeable trends.
- Concepts for implementation, integration and testing must take into account the results of the risk analysis and the resulting action plans. Here it must be ensured that independent testers are assigned, who have not been involved in the development and specification phase of the respective ICT systems.
- For each ICT system an acceptable use concept must be defined.
- When designing ICT systems, the physical and environmental security of the installation location must be ensured depending on the risk-oriented requirements for the availability, confidentiality, and integrity of information (cf. Brand Policy MAN Truck & Bus MR_13_1 Information Security, article 10 and 11).

  These are as follows:

Note: Printed versions and local files may not be updated!

  - Access protection and access management – administrative and technical control and tracking of the physical access to the information and communication technology systems, incl. delivery areas, guards, fences, gates and the security areas
  - Intrusion detection/protection – measures to identify and prevent unauthorized access to, and the sabotage of information and communication technology systems including surveillance.
  - Fire protection – measures to identify and prevent the spread of a fire and the adverse effects of fumes (smoke), incl. fire alarm systems, fire doors and containment zones, extinguishing equipment and smoke extraction systems
  - Protection against environmental hazards – earthquake, flooding, etc.
  - Ambient air conditioning – air change rates, temperature control, humidity control and monitoring
  - Protection against failure of supply facilities (power and cooling systems) for information and communication technology systems, incl. management of the supply capacity, uninterruptable power supply and emergency power generators
  - Structural protection – load capacity of the ceilings/floors, suitability of the delivery and traffic routes
  - Protection of cables and lines – locked cabinets against wiretapping and damage and clear labeling to ensure quick fault resolution
  - Terms of operation as required by the technical component manufacturer

- In order to adequately protect information and avoid unacceptable Risks to the MAN Truck & Bus business processes, the following points in addition to MTB Brand Instruction MA_13_1_07 – Information Security Requirements for Secure Application Development and Appendix 1 to MA_13_1_07 – Requirements for Secure Application Development must be considered:
  - The production, testing, and development environments shall be separated to avoid interference (e.g. run on different systems or processors and in different domains or directories).
  - The rules governing the transport of software from the development phase to the production phase must be defined and documented
  - Compilers, editors, and other development tools or system utility programs must not be accessible from systems in production if this is not required
  - The test system environment must simulate the production system environment as closely as possible
  - Users must use different authentication for production systems and test systems
  - Test systems and development systems must be clearly marked so that the system is guaranteed to be properly identified, in order to avoid user errors
  - Confidential or Strictly confidential information and data from the production systems must not be used in the test system environments. If this cannot be

Note: Printed versions and local files may not be updated!

avoided, information must be protected in accordance with the requirements for production data.

- Use of new device classes and software technologies for the MAN Truck & Bus Group may only occur once implementation and integration tests have been successfully completed and approval has been obtained from the relevant MAN Truck & Bus committees.
- In the case of overarching architectures, approval must be obtained from the CIO and IT Director Board at the MAN Truck & Bus Group.
- The acceptance of residual information security risks has to be formally confirmed by the responsible Owner(s) (Process, Application or System).
- The externally facing systems must be designed with extra resilience against cyber-attacks such as distributed denial-of-service (DDoS) attacks, malicious code, unauthorized access, etc.
- For ICT systems processing information with high or very high protection needs, end-to-end encryption has to be ensured.
- When designing business applications and systems the following criteria must be observed at a minimum, in addition to the general requirements defined in the MTB Brand Instruction MA_13_1_07 – Information Security Requirements for Secure Application Development:
    - Ensure appropriate authentication and authorization methods are implemented in accordance with the confidentiality and integrity levels of the information, shared with commercial partners
    - Guarantee that the commercial partners are aware of their granted authorizations
    - Definition and fulfilment of the requirements concerning confidentiality, integrity, proof of dispatch, and receipt of important documents, as well as non-repudiation of contracts, e.g. in conjunction with offer submission processes and contractual processes.
    - Prevention of loss or duplication of transaction information
    - Liability relationships with regards to information ownership
    - Compliance with the relevant legal requirements with regards to the country and use of the business application or system
- Authorization concepts must be defined for all MAN Truck & Bus ICT systems. The following aspects must be incorporated into the authorization concepts as a minimum:
    - Security requirements of the underlying business process
    - Legal and contractual obligations with regards to access to information or services
    - Process and procedure for access and rights management, incl. approvals, assignment, modification and revocation
    - Audit-compliant documentation of the current authorizations (audit report) and the rights assignment/revocation procedures (audit log)

Note: Printed versions and local files may not be updated!

- A verification procedure to determine the correctness of the current authorizations
- Management of critical authorizations (privileged access)

5.3 Requirements for the Design of Networks

MAN Truck & Bus networks must be designed in such a way that the networks are separated in different classes/areas according to the risk involved (DMZ, business applications, IT infrastructure applications, cloud applications, Engineering applications, HR applications, Facility Management applications and Production and Logistics applications, etc.).

Network gateways must only allow the required network traffic and must be specially protected against tampering or unauthorized access.

Remote access to MAN Truck & Bus internal networks requires strong authentication and end-to-end encryption.

Authorization concepts must be defined for all MAN Truck & Bus networks. The following aspects must be incorporated into the authorization concepts as a minimum:

- Security requirements of the underlying business process
- Process and procedure for security compliance verification of devices prior to connecting to MAN Truck & Bus internal networks
- Process and procedure for security compliance verification and approval of network management tools
- Management of critical authorizations (privileged access to network components)
- Process and procedure for access and rights management for managing networks and network services, incl. approvals, assignment, modification and revocation
- Management procedures and technical measures to protect access to network connections and network services
- Management procedures and technical measures to protect access to diagnostic or configuration ports

Note: Printed versions and local files may not be updated!

5.4 Requirements for the Operation of ICT Systems

Brand Policy MAN Truck & Bus MR_13_1 Information Security and MTB Brand Instruction MA_13_1_01 - Standard for Information Security must be complied with when operating MAN Truck & Bus ICT systems. In addition to the above, the following also apply:

- Process and procedures for decommissioning and secure disposal of ICT systems must be in place. For ICT systems containing internal, confidential, or strictly confidential information (cf. MTB Brand Instruction MA_13_1_03 – Classification of Information Assets) the storage devices must be either physically destroyed, or the information stored on these systems must be irretrievably deleted. This activity must be adequately documented and records need to be retained.
- In case of shortfall in staff or system functions are disrupted, operating procedure and documentation must be available for all ICT systems used at MAN Truck & Bus Group to ensure that normal operation can be resumed as quickly as possible. This includes:
    - Data processing

- Backup and restore
- Operation scheduling
- Interfaces and dependencies with other ICT systems
- Instructions for error handling or how to deal with other exceptional circumstances, including restrictions on the use of tools
- In case of errors, a contact list for technical and operational support should be available
- System restart and reboot procedures
- Management of audit trails and system log information
- System-specific change procedure
- Description of roles and responsibilities

- The documentation of system configurations must be protected against unauthorized access and disclosure.
- In order to minimize the impact on the confidentiality, integrity and availability of processed information, changes to ICT systems must be implemented in accordance with the documented standardized Change Management process. The following points must be considered in the change procedure:
  - Identification and documentation of significant changes
  - Planning changes and conducting of corresponding tests
  - Evaluation of potential risks related to these changes, including the impact on the MAN Truck & Bus SE business processes
  - Formal approval procedure for proposed changes
  - Communication of the details of the proposed changes to all relevant stakeholders
  - Procedure and responsible individuals for cancelation of a change:
  - Roll back plan following to failed change attempts or unforeseeable events
  - Emergency changes procedure
- The performance of the information and communication technology systems must be monitored and reconciled with the target values.
- New information systems, upgrades, and new versions may only be implemented into production environment once formal approval has been obtained. For this, the following points must be taken into consideration as a minimum:
  - Completeness and adequacy of the security measures
  - Incident management procedures
  - Completeness and adequacy of the operational procedures
  - Continuity management and contingency plans
  - Operational training has been conducted for the new systems

Note: Printed versions and local files may not be updated!

- The requirements laid down in MTB Brand Instruction MA_13_1_01 - Standard for Information Security, article 26, must be implemented to prevent the intrusion and spread of malicious software and code.
- For the identification and evaluation of vulnerabilities and their remediation, information about technical weaknesses of the systems and applications used must be timely determined and evaluated. A procedure for regular and emergency installation of security patches must be available for every MAN Truck & Bus information and communication technology system. The following aspects are to be considered:
  - The sources of information about vulnerabilities must be determined and documented
  - Vulnerabilities must be evaluated in terms of risk.
  - Dependent on the risk evaluation of a vulnerability, an action plan must be defined and prioritized
  - Patches are to be obtained from trusted sources
  - A procedure must be in place to be able to deploy critical patches in a timely manner outside of the regular maintenance windows
  - Patching procedure must be integrated into the Change Management process
- A backup and recovery procedure must be implemented for each ICT system used at MAN Truck & Bus Group. This procedure must correspond to the requirements laid down in the MTB Brand Instruction MA_13_1_01 - Standard for Information Security, article 25. The backup strategy is dependent on the risk for the MAN Truck & Bus Group business processes and resulting from the classification of the information values (cf. MTB Brand Instruction MA_13_1_03 – Classification of Information Assets, section 6). In addition, the backup and recovery concept must consider the following points:
  - The backups must be traceable and backup media clearly labeled
  - Backup and recovery concepts need to be aligned with Business Continuity Management (BCM) requirements. This includes storage of backup media with sufficient physical distance from the main site where the information is stored. backup location to ensure that it is not affected by the same disaster.
  - Backup media must be protected at the remote storage location according to the classification of information it contains.
  - Backup media must be protected during transportation between sites (handover procedure, packaging, transportation means, reliable courier service) according to their classification in conformance with Appendix 1 to MA_13_1_03 – Handling of Classified Information.
  - Disposal of data storage media must be performed according to their classification in conformance with Appendix 1 to MA_13_1_03 – Handling of Classified Information.
- The MAN Truck & Bus ICT systems must be configured in accordance to Global Standards and recognized Best Practices for securing IT Systems (ref. CIS Security Benchmarks).

Note: Printed versions and local files may not be updated!

- The clocks in all MAN Truck & Bus Group systems must be synchronized to an agreed reference time provided by a central time server.
- For all information systems and services, traceable procedures must be in place for registering and deregistering of regular and privileged users. This also applies for the entire lifecycle of authorizations. All changes to the authorizations must be recorded.
- All users of MAN Truck & Bus ICT systems must be assigned a unique personal user ID.
- An adequate authentication method must be selected to confirm the specified user's identity.
- For regular users, if technically possible, the MAN Truck & Bus ICT systems must be configured such that they accept only passwords with a minimum of 12 characters (see more details in MTB Brand Instruction MA_13_1_05 – Information Security for Employees), which must be changed at least annually, and which consist of a combination of 3 of the following 4 attributes:
    - Lowercase letters, (a-z)
    - Uppercase letters, (A-Z)
    - Digits/Numbers, (0-9)
    - Special characters (!,@,#,%,$,+)
- Granted authorizations must be verified at regular intervals. These intervals must be determined according to the extent and criticality of the access rights, but not longer than once a year. The checks carried out must be documented in a clear and understandable manner and this documentation must be securely stored for verification purposes.
- For all MAN Truck & Bus ICT systems, access to operating systems must be protected by a secure log-in procedure. In this regard it must be ensured that:
    - No system or application identifiers are displayed before the log-in process has been successfully completed.
    - ICT systems with high protection requirements must clearly display the confidentiality level of the information processed (i.e. as a label in the GUI)
    - The log-in information is not confirmed until all input data has been entered and if an errors occurs, the system does not show which part of the data is correct or incorrect.
    - The number of permitted unsuccessful log-in attempts and the permitted maximum and minimum durations are limited.
    - Passwords must not be transferred over the network in plain text.
    - Preferably, password management systems should be used to force the use of secure Passwords.
- The use of system utility programs that can override system and application settings must be reserved for users with privileged authorization. Their usage must be logged and protected from use by other users.

Note: Printed versions and local files may not be updated!

- The MAN Truck & Bus ICT systems must be configured such that inactive sessions are terminated after a defined period of inactivity.

5.5 Requirements for the Operation of Network Infrastructure

The protection of internal and external communication must meet the requirements of the MTB Brand Instruction MA_13_1_01 - Standard for Information Security, Article 15. The following also apply:

- The management of Gateway configurations must follow a defined change management process including the approval, the regular reviews and the expiration of such rules.
- Privileged access to the configuration of network devices must be sufficiently logged. Logs must be protected against unauthorized modification or deletion.
- Security measures that are required for a particular service must be determined. It must be ensured that the relevant network operators implement these measures.

5.6 Requirements for Administrators

Resulting from their responsibilities (the MTB Brand Instruction MA_13_1_01 - Standard for Information Security, Article 16) in respect to operations of ICT systems the following also applies for administrators:

- Administrators require regular awareness for the specific risks involved in their area of work. This includes instructions, trainings and drills.
- For individual-related administrative accounts with privileged access rights used for administrative tasks on ICT systems passwords must consist of at least 15 characters and fulfill at least 3 out of 4 of the following criteria:
  - Lowercase letters, (a-z)
  - Uppercase letters, (A-Z)
  - Digits/Numbers, (0-9)
  - Special characters (!,@,#,%,$,+)
- Passwords shall be managed in accordance with documented procedures.
- Privileged user accounts shall not be used for everyday work.
- Identical administrative passwords must not be used for different applications.
- Server panels and consoles must be locked when not in use.
- Sessions must be closed immediately after finishing the task(s).
- The area of responsibility of an employee with enhanced rights must be defined and documented in terms of the ICT systems to be configured and the employee's competences (rights and obligations) must correspond to the definition "Configuring the ICT systems in their area of responsibility".
- Responsibilities must be segregated appropriately and distributed over two or more individuals in order to prevent misuse of ICT systems.

Note: Printed versions and local files may not be updated!

- For ensuring operational security it is required that administrative resources are planned and provided adequately.
- Administrative resources require a Non-Disclosure Agreements (NDAs) as part of the contracts

5.7 Security Incidents

Security incidents primarily refer to the kinds of incidents or circumstances capable of causing MAN Truck & Bus or its employees, customers, or partners to suffer an unacceptable level of loss or damage. In most cases only an expert will be able to determine whether something is a security incident or whether it only amounts to a technical fault or a mistake. It is always important to identify a security incident as early as possible to limit the loss or damage. The behavior during security incidents is described in detail of MTB Brand Instruction MA_13_1_09 – Information Security Incident Management.

All system operators and administrators at MAN Truck & Bus Group are responsible for creation of specific reports within their area of responsibility.

In addition to the regular monitoring and operational reports, they must also be able to provide specific Information Security reports on a regular basis and ad-hoc. Some examples of reports applicable for system operators and administrators are listed in Chapter 6.4 of MTB Brand Instruction MA_13_1_08 – Information Security for Suppliers.

Note: Printed versions and local files may not be updated!

6 Change History

Version 3.0

- Added Change Log
- Relabeling
- Change in roles and responsibilities
- Added new chapter “Security Reporting”
- Added Contact Partners for Information Security moved to MTB Brand Policy Instruction 09 – Information Security Incident Management
- Changed document title
- Assigned new document code number “MA_13_1_06” – was “MAN 13.1 Instruction 7 – Information Security for Users with privileged IT responsibilities”.
- “MAN 13.1 Instruction 6 – Management of Information Security“ assigned to new code „MA_13_1_02”

Information Security Requirements for Development of Secure Applications

Note: Printed versions and local files may not be updated!

Created	Steven Rauwerdink Ralf Schlag	**Approved**	Andre Wehner	**Version**	3.0
Dept.	FIOS	Dept.	FI	**KSU-Class:**	xx
Applicable as of		**Scope**		**Approved by (Board)***	
Date	01.02.2023	MAN Truck & Bus SE and its Subsidiaries			
				Agreed by	

* Only required for Brand Instructions that do not relate to a superior Brand Policy

Contents

Appendix

Note: Printed versions and local files may not be updated!

1 Purpose

Derived from Brand Policy MAN Truck & Bus MR_13_1 Information Security and MTB Brand Instruction MA_13_1_01 - Standard for Information Security this MTB Brand Instruction MA_13_1_07 – Information Security Requirements for Secure Application Development defines the security requirements for software and development of applications at MAN Truck & Bus.

The purpose of this instruction is to anchor the MAN Truck & Bus Secure Software Development Life Cycle (SSDLC) and to define security requirements for secure software applications that is also demanded by the certified CSMS (UNECE R155 Cyber Security).

The aim of the SSDLC's activities is to establish a uniform process at MAN Truck & Bus Group that ensures that information and cyber security aspects are adequately taken into account at every stage of software development in to the MAN Truck & Bus Group.

The document provides an overview of the Secure Software Development Process and describes the Roles and Responsibilities within the SSDLC Governance.

Note: Printed versions and local files may not be updated!

2 Scope

This Brand Policy applies to MAN Truck & Bus SE and its subsidiaries and their employees worldwide. This Brand Policy is to be implemented directly and does not require conversion policies from the individual subsidiary. In the case of companies in which MAN Truck & Bus SE cannot directly enforce the applicability of this Brand Policy for legal reasons, the policy owner has to be consulted to clarify the extent to which this Brand Policy is applicable. Companies which are not wholly owned by MAN Truck & Bus SE and also not subsidiary with MAN Truck & Bus SE through a control agreement constitute one such example (e.g. Subsidiaries which are wholly owned by MAN Finance and Holding S.A.)

In the event of any subsidiaries having their own regulations governing the enactment of Policies, these must be annulled with immediate effect. Until such time as Policies of this kind, either wholly or in part, are annulled, this Brand Policy takes precedence.

If the rules contained in this Brand Policy cannot be implemented due to mandatory local requirements, the individual Subsidiary needs to inform the policy owner of MAN Truck & Bus SE without undue delay to discuss required changes or adaptations.

3 Terms and definitions

A glossary for the complete information security framework can be found at the additional information ”Terms and Definitions to information security “.

4 Target Group

This document is directed at MAN Truck & Bus employees who are responsible for the design and development of software applications, as well as their managers.

In some cases the responsible individuals can be external partners and suppliers.

5 Development of Secure Applications

5.1 Objective

The objective of this chapter is to prevent the occurrence of vulnerabilities in software applications caused by design and implementation in software development on behalf of or by MAN Truck & Bus Group.

5.2 Software Development Process

In order to develop secure software applications, security aspects must be considered in all stages of the development process. Security must be part of the functional and technical requirements of an application development process.

Functional and technical requirements must be defined first. Then, security requirements must be modelled as part of the analysis and design phase. Secure code methodology must be followed to ensure development of secure software applications.

A responsible person or unit must be assigned to each phase of the process of development. The SSDLC phases are described in detail in Appendix 07.1 – Requirements for Development of Secure Applications as part of this instruction.

Software applications that are subject to the regulation of the MAN CSMS (as defined in the Subgroup Policy MTB 8.103 "Automotive Cyber Security Management System (CSMS) and Software Update Management System (SUMS)") and specifically for software applications in AN_MTB_13_508_01 "Use of SSDLC", have to fulfill the MAN-CSMS-SSDLC as specified in the Security Knowledge Base. Hence, the MTB Brand Instruction MA_13_1_07 – Information Security Requirements for Secure Application Development as provided with this document is compliant with the aforementioned instructions and can be used as an additional source for information and reference.

5.3 Secure Software Development Process

All software applications in scope of this instruction must follow a minimum set of requirements for a Secure Software Development Lifecycle (SSDLC).

The following chart provides a high-level overview of a secure software development process.

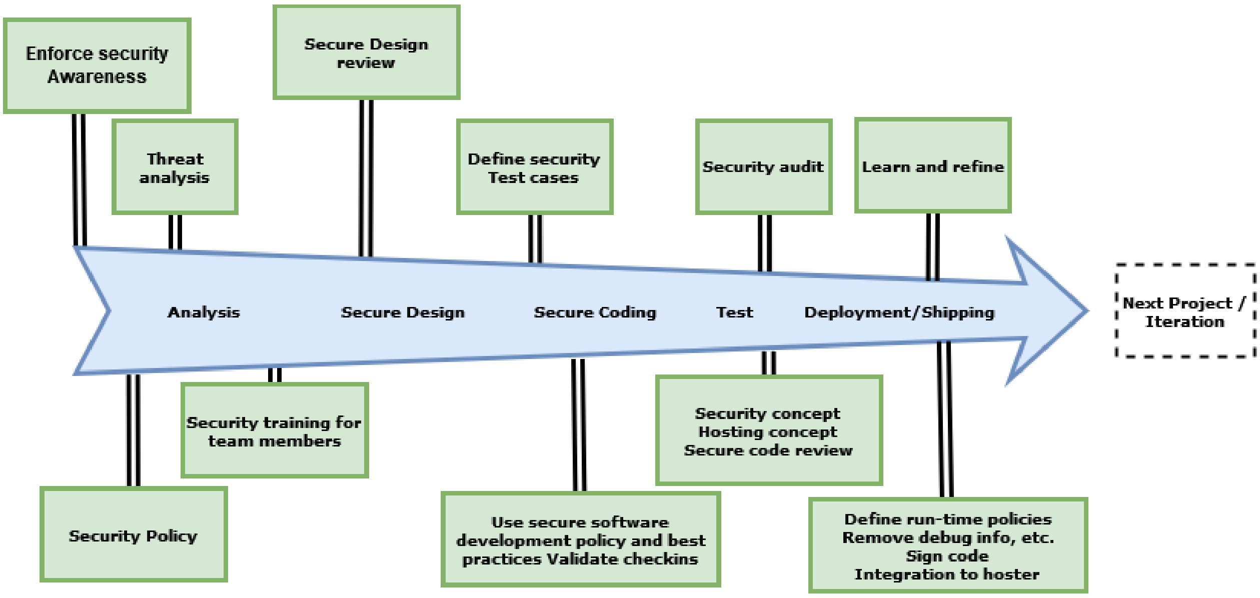


Figure 1: Secure software development process

The process itself and each phase in it are described in details in Appendix 1 to MA_13_1_07 – Requirements for Secure Application Development.

Note: Printed versions and local files may not be updated!

5.4 Procedural and organizational

The MAN Truck & Bus IT-PEP is a standardized IT project management method. The use of IT-PEP is mandatory for projects that meet certain criteria. All software development projects must reach major milestones during the project phases (see AN_MTB_13_101_03: Use of the IT-PEP).

6 SSDLC Governance

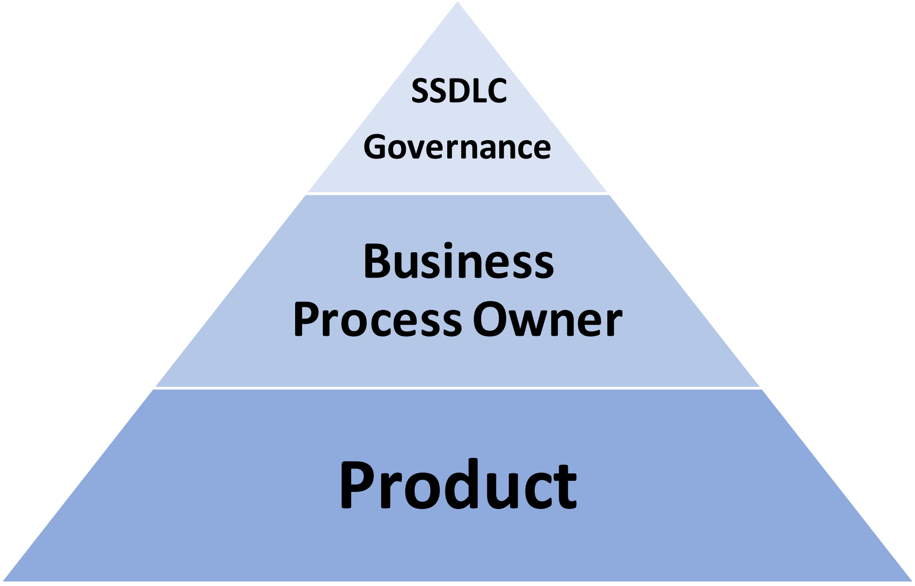
The aim of this process is to provide a SSDLC Governance function and to enable and ensure ISMS compliance of the developed software applications. By establishing responsibility, authority, and an adequate channel of communication, the SSDLC governance empowers project and Business Process Owners within a software development organization to establish measuring and control mechanisms towards a more secure software development. The SSDLC Governance goal is to ensure that the results delivered by the process meet the strategic requirements of the MAN Truck & Bus Group.

SSDLC Governance has three main concerns:

- Manage value: Align the business and the software at the organizational/project levels, balance risk and provide clarity and accountability.
- Develop flexibly: Leverage global resources by enabling agile development choices and the use of iterative processes to reduce risk.
- Control risk and change: Continuously implement improvements to reduce risks, enable change management lifecycle and meet internal and external compliance needs.

6.1 Roles and Responsibilities of SSDLC Governance

In the SSDLC area the following roles are notable and further ISMS structures and roles build on this. For additional information, please refer to the subgroup guideline MTB 8.103 CSMS & SUMS, including appendices.



Note: Printed versions and local files may not be updated!

- **SSDLC Governance**

  The SSDLC Governance Lead is responsible for the overall establishment and maintenance of an adequate security level throughout the entire SSDLC. By means of processes, roles and other necessary operational structures, the SSDLC Governance Lead ensures the requirements of the MAN Information Security Framework as well as the Cyber Security Management System are met in the area of SSDLC. For this, strong collaboration with the Business Process Owners is necessary.

  Details about the SSDLC Governance Lead role and responsibilities can be found in SSDLC Security Knowledge Base.

- **Business Process Owner**

  The Business Process Owner is responsible for:

  - Supporting system teams with queries related to the implementation
  - Maintaining the process documentation and ensuring it is up-to-date
  - Support activities for increasing the level of cyber security
  - Process design, monitoring and continuous improvement
  - Technical and functional support for system owners, incl. feedback collection from system teams and owners
  - Technical escalation point of contact for exceptions (to be assessed individually and with the SSDLC Governance) and execution of defined process specific activities.

  Details about the Business Process Owner role and responsibilities can be found in SSDLC Security Knowledge Base.

- **System / Product (Owners)**

  The System / Product Owner is responsible for implementing adequate security requirements throughout the entire life cycle. In this sense, the coordination of security requirements with other functional requirements must be ensured. The standard for SSDLC-related requirements is described in the Security Knowledge Base. Details about the SSDLC System / Product Owner role and responsibilities can be found in SSDLC Security Knowledge Base.

Details on the respective process content and activities can be found in Appendix 1 to MA_13_1_07 – Requirements and also in the Security Knowledge Base.

7 Change History

Version 3.0

- New document creation. Assigned document code “MA_13_1_07”.
- Relabeling
- Added roles and responsibilities.
- Added chapter procedural and organizational
- Added SSDLC Governance
- “MAN 13.1 Instruction 7 – Information Security for Users with privileged IT responsibilities” assigned to new name and code - “MA_13_1_06 Information Security for System Operation and Administration”.

Note: Printed versions and local files may not be updated!

Appendix 1 : Requirements for Development of Secure Applications

Note: Printed versions and local files may not be updated!

Note: Printed versions and local files may not be updated!

Appendix 1 - Requirements for Development of Secure Applications

Created	Steven Rauwerdink Ralf Schlag	**Approved**	Andre Wehner	**Version**	1.0
Dept.	FIOS	Dept.	FI	**KSU-Class:**	xx
Applicable as of		**Scope**		**Approved by (Board)***	
Date	01.02.2023	MAN Truck & Bus SE and its Subsidiaries			
				Agreed by	

* Only required for Brand Instructions that do not relate to a superior Brand Policy

Contents

Note: Printed versions and local files may not be updated!

1 Purpose

The purpose of this Appendix is to define and describe in detail the SSDLC process phases and maturity levels, as required by the Brand Policy MAN Truck & Bus MR_13_1 Information Security and MTB Brand Instruction MA_13_1_07 – Information Security Requirements for Secure Application Development. Further, the security requirements for Software Development by External Service Providers are defined and described in this document.

2 Security Knowledge Base

The Security Knowledge Base is the central repository of requirements and knowledge of the CSMS-SSDLC as specified in in AN_MTB_13_508_01 "Use of SSDLC". Those requirements can be applied for every software development project and the Knowledge Base can serve as a valuable source of information how to fulfill the minimal SSDLC requirements in MAN Truck & Bus Group.

3 Maturity levels in SSDLC

Based on the OWASP SAMM[1] framework, a target maturity level was defined for the individual activities, which Software Development teams must achieve to comply with the requirements with sufficient security controls aimed at protection of information security and cybersecurity aspects in regards to IT systems development and operation. Each level within a security practice is characterized by a successively more sophisticated objective defined by specific activities, and more stringent success metrics than the previous level. Additionally, each security practice can be improved independently, though related activities can lead to the optimizations.

	Maturity levels 1	Maturity levels 2	Maturity levels 3
		Governance	
Strategy & Metrics	Identify objectives and means of measuring effectiveness of the security program.	Establish a unified strategic roadmap for software security within the organization.	Align security efforts with the relevant organizational indicators and asset values.
Policy & Compliance	Identify and document governance and compliance drivers relevant to the organization.	Establish application-specific security and compliance baseline.	Measure adherence to policies, standards, and 3rd-party requirements.
Education & Guidance	Offer staff access to resources around the topics of secure development and deployment.	Educate all personnel in the software lifecycle with technology and role-specific guidance on secure development.	Develop in-house training programs facilitated by developers across different teams.
		Design	
Threat assessment	Best-effort identification of high-level threats to the organization and to individual projects.	Standardization and enterprise-wide analysis of software related threats within the organization.	Proactive improvement of threat coverage throughout the organization.

Note: Printed versions and local files may not be updated!

[1] OWASP Software Assurance Maturity Model (SAMM) provides an effective and measurable way to analyze and improve their software security postures.

	Maturity levels 1	Maturity levels 2	Maturity levels 3
Design			
Security requirements	Consider security explicitly during the software requirements process	Increase granularity of security requirements derived from business logic and known risks	Mandate security requirements process for all software projects and 3rd party dependencies
Security architecture	Insert consideration of proactive security guidance into the software design process	Direct the software design process toward known secure services and secure-by-default designs	Formally control the software design process and validate utilization of secure components.
Implementation			
Secure build	Build process is repeatable and consistent	Build process is optimized and fully integrated into the workflow	Build process helps prevent known defects from entering the production environment
Secure deployment	Deployment processes are fully documented	Deployment processes include security verification milestones	Deployment process is fully automated and incorporates automated verification of all critical milestones
Defect management	All defects are tracked within each project	Defect tracking used to influence the deployment process	Defect tracking across multiple components is used to help reduce the number of new defects
Verification			
Architecture assessment	Review the architecture to ensure baseline mitigations are in place for typical risks	Review the complete provision of security mechanisms in the architecture	Review the architecture effectiveness and feedback results to improve the security architecture
Requirements driven testing	Opportunistically find basic vulnerabilities and other security issues	Perform implementation review to discover application specific risks against the security requirements	Maintain the application security level after bug fixes, changes or during maintenance
Security testing	Perform security testing (both manual and tool based) to discover security defects	Make security testing during development more complete and efficient through automation complemented with regular manual security penetration tests	Embed security testing as part of the development and deployment processes

Operations			
Incident management	Best-effort incident detection and handling	Formal incident management process in place	Mature incident management
Environment management	Best-effort patching and hardening	Formal process with baselines in place	Conformity with continuously improving process enforced
Operational management	Foundational practices	Managed, responsive processes	Active monitoring and response

4 Secure Software Development Process

4.1 Analysis Phase

- A risk assessment must be conducted, analyzing existing threats, evaluating the risk, defining adequate security requirements by employing the ISi Assessment process.
- All security requirements from relevant instructions, guidelines and security concepts as well as application-specific requirements must be identified and documented.
- All employees participating in a software development project must be trained for security aspects in their field. This training must include appropriate usage of software development tools, technologies, frameworks and programming languages and relevant libraries.

4.2 Secure Design Phase

- Based on the identified security requirements a secure architecture must be designed. Detailed security measures must be specified as per the demand coming out of the ISi Assessment.
- A security concept must be developed. It must contain the security measures that have to be implemented.
- Verification of all security requirements for selected:
  - technologies,
  - software development tools,
  - frameworks,
  - programming languages and relevant libraries
- The security of the architecture must be evaluated in an architecture review. The architecture review must be conducted by developers having the necessary expertise and using the four eyes principle in case of significant change in the design.
- All identified flaws as a result of the architecture review must be addressed or the identified residual risks must be formally accepted.
- The development and test environments of software applications must be separated from the production environment.

4.3 Secure Coding Phase

- Coding must be conducted according to the defined architecture and corresponding specification of the security requirements.
- The organization responsible for application development must define coding guidelines.
- Architecture changes and deviations from the specified security requirements must result in a review of the ISi Assessment.
- Secure Code review must be performed with the following checks, where these are applicable:
  - Static application security testing (SAST) – analyze source code for known vulnerabilities.
  - Before deployment, the code must be verified against the defined security requirements and measures.
  - If software modules are being developed by 3rd parties, they shall follow the same MAN Truck & Bus information security requirements.
  - Risk must be evaluated via risk assessment (ISi Assessment). It has to be assessed if the implementation or integration of new application/software affects sensitive information and cyber security of the MAN Truck & Bus Group.
  - If identified risks cannot be mitigated, they must be formally accepted as per the process described in MTB Brand Instruction MA_13_1_10 – Exception Handling.
  - Identified flaws must be documented and addressed.
  - In case of design flaws, the security concept must be updated and approved prior to deployment in production environment.
- For applications handling information with high or very high protection requirements the code review must cover the following additional aspects:
  - input and output data validation.
  - correct processing of data within the application.
  - authenticity and protection of message integrity.

4.4 Test Phase

The test phase is conducted after deployment of the software application in the testing environment. The tests allow to verify that the entire software application works in accordance with the security specifications and to ensure that all security requirements are met. The testing must at least cover the following aspects:

- Automated scan of the software application for known vulnerabilities
- Dynamic application security tests (DAST) – analyze the running application for known vulnerabilities
- Dependency check – check dependencies of the application for known vulnerabilities
- Static application

Note: Printed versions and local files may not be updated!

- In case of design flaws the security concept must be updated based on the results of the tests prior to deployment in production environment.

4.5 Code Signing

Code Signing validates code for being used in dedicated environments. It confirms that all required testes have been conducted and passed successfully. With this software/applications can be validated at runtime.

Code signing should be done as a formal approval process step. To ensure non-repudiation, executables, software modules and scripts shall be digitally signed. For this, a central code signing service must be used.

4.6 Deployment / Provisioning

Deployment is the step where the software/application gets deployed to its final target infrastructure. The responsible deployment manager validates the approvals, checks for adequate maintenance plan and the roll-back plan. The deployment manager observes the roll-back conditions and decides on performing the roll-back steps in case of failure.

5 Software Development by External Service Providers

Software development services that are supplied by external service providers must follow the same requirements for secure software development as for MAN Truck & Bus internal development. These requirements and the required maturity level shall be provisioned in the related contractual agreement and shall also include a right to audit the service provider by MAN Truck & Bus as per Appendix 1 to MA_13_1_08 – Supplier Verification Methods and Requirements.

Especially, the following topics have to be observed:

- External service providers shall follow the defined security concepts and conduct risk assessments.
- External service providers shall observe the coding guidelines defined in Chapter 4.3.
- Code review and testing must take place and the results must be documented.
- The externally developed software requires to be assessed as part of the ISi Assessment for the related project.
- Depending on the outcome of the ISi Assessment, an independent external penetration test might be necessary
- Vulnerabilities identified must be properly addressed in a timely manner.

6 Change History

Version 1.0

- Initial Version

Note: Printed versions and local files may not be updated!

Note: Printed versions and local files may not be updated!

Information Security for Suppliers

Created	Steven Rauwerdink Ralf Schlag	**Approved**	Andre Wehner	**Version**	3.0
Dept.	FIOS	Dept.	FI	**KSU-Class:**	xx
Applicable as of		**Scope**		**Approved by (Board)***	
Date	01.02.2023	MAN Truck & Bus SE and its Subsidiaries			
				Agreed by	

* Only required for Brand Instructions that do not relate to a superior Brand Policy

Contents

Note: Printed versions and local files may not be updated!

Appendix

1 Purpose

Derived from Brand Policy MAN Truck & Bus MR_13_1 Information Security and MTB Brand Instruction MA_13_1_01 - Standard for Information Security this Brand Instruction defines and describes the information security requirements for management of suppliers who are responsible for or handling on behalf of MAN Truck & Bus IT services, systems and infrastructure.

When commissioning, cooperating with and controlling service suppliers with responsibility for the development, installation, operation and configuration of MAN Truck & Bus ICT Systems the responsible application/system Owners have to ensure that the requirements of this Brand Policy Instruction are appropriately considered and met.

Considering the type and extent of the Supplier's tasks, the regulations specified in the MAN Truck & Bus Group Information Security framework have to be applied in the contractual agreements with the Suppliers.

Existing contracts are not required to be changed. For contracts that are subject to renewal the necessity of contractual changes or amendments have to be evaluated. Exceptions that may result from the evaluation and possible risk acceptances have to be handled according to the regulations of the MTB Brand Instruction MA_13_1_10 – Exception Handling.

2 Scope

This Brand Policy applies to MAN Truck & Bus SE and its subsidiaries and their employees worldwide. This Brand Policy is to be implemented directly and does not require conversion policies from the individual subsidiary. In the case of companies in which MAN Truck & Bus SE cannot directly enforce the applicability of this Brand Policy for legal reasons, the policy owner has to be consulted to clarify the extent to which this Brand Policy is applicable. Companies which are not wholly owned by MAN Truck & Bus SE and also not subsidiary with MAN Truck & Bus SE through a control agreement constitute one such example (e.g. Subsidiaries which are wholly owned by MAN Finance and Holding S.A.)

In the event of any subsidiaries having their own regulations governing the enactment of Policies, these must be annulled with immediate effect. Until such time as Policies of this kind, either wholly or in part, are annulled, this Brand Policy takes precedence.

If the rules contained in this Brand Policy cannot be implemented due to mandatory local requirements, the individual Subsidiary needs to inform the policy owner of MAN Truck & Bus SE without undue delay to discuss required changes or adaptations.

3 Terms and definitions

A glossary for the complete information security framework can be found at the additional information "Terms and Definitions in Information Security".

4 Target Group

MTB Brand Instruction MA_13_1_08 – Information Security for Suppliers is directed to individuals responsible for the management of suppliers within the MAN Truck & Bus Group.

5 Information Security of MAN Truck & Bus ICT Systems

Information constitutes an important asset of the MAN Truck & Bus Group. Company business and production processes only run if the right information is provided at the correct time and at the correct location. Protecting these information assets in the MAN Truck & Bus ICT systems effectively is a decisive factor in ensuring company business success.

Note: Printed versions and local files may not be updated!

Since the information assets are daily exposed to a wide range of threats, such as:

- Destruction or encryption of information by computer viruses.
- Theft of information by spying on passwords.
- Theft of data storage media, smartphones or computers.
- Failure of MAN Truck & Bus ICT systems due to power outages, sabotage, or vandalism.
- Destruction of important data by fire or water.

special measures to protect them must be taken. Protection will only be effective if it is based on a wide range of interconnected measures and safeguards.

In addition to the measures stated in the MAN Truck & Bus framework for information security, the necessary measures to safeguard information security also include in particular:

- The security culture among all employees working for a service supplier.
- Compliance with defined processes and procedures.
- Ensuring information and communication devices and software are appropriately handled and protected.
- A risk-oriented appropriate reporting of the implementation and effectiveness of the service supplier's information security management to MAN Truck & Bus.
- The right to audit relevant information security aspects (also at the service supplier).

The term "risk-oriented" addresses the risks to the MAN Truck & Bus Group's business processes and must be coordinated with MAN Truck & Bus.

6 Responsibility of the Service Suppliers

All employees at a MAN Truck & Bus service supplier with responsibility for configuring the MAN Truck & Bus ICT systems have to ensure that the configuration complies with the relevant MAN Truck & Bus Group information security regulations. In particular:

- All application developers and system architects at a MAN Truck & Bus service supplier are responsible for a secure design, adequate security specifications, appropriate testing and migration of the MAN Truck & Bus ICT systems in accordance to the relevant MAN Truck & Bus information security regulations.
- All employees at a MAN Truck & Bus service supplier with operation responsibility have to ensure operational security of the ICT systems in accordance with the relevant MAN Truck & Bus information security regulations. As part of this, the service supplier must be vigilant of any potential threats, notify the contact partners at the MAN Truck & Bus Group of any threats found and prevent information from being placed at risk unnecessarily.

MAN Truck & Bus information security management is implemented on basis of the risk-based approach. This considers risks for the relevant business processes.

All service suppliers of MAN Truck & Bus Group Companies are obligated to identify risks related to the provided service area and to manage these in coordination with the IS organization of MAN Truck & Bus.

Depending on the requirement of the MAN Truck & Bus Group and the related service the supplier has to:

Note: Printed versions and local files may not be updated!

- Support the information security objectives defined by the MAN Truck & Bus Group in an appropriate manner.
- Comply with the MAN Truck & Bus framework for information security as a binding framework for all provided services.
- If required, based on the MAN Truck & Bus framework for information security, publish additional instructions for the service supplier's area of responsibility.
- Provide sufficient resources for setting up, implementing, operating, monitoring, checking, maintaining, and continually improving the management of information security.
- At least fulfil the MAN Truck & Bus minimum information security requirement for the service.
- Take also into account the availability, confidentiality, and integrity of information assets/IT services/ICT systems as per the MAN Truck & Bus requirements for the suppliers own risk management.
- Develop risk treatment plans or measures for any identified unacceptable risks associated to the services that the supplier delivers for the MAN Truck & Bus Group.
- Ensure independent assessments to improve information security are conducted.
- Carry out own management reviews of the information security level at regular intervals.
- Together with MAN Truck & Bus, to define the security level and corresponding indicators appropriate to the risks and report those regularly to MAN Truck & Bus.
- Identify and handle legal and regulatory requirements and contractual obligations related to information security.
- Ensure that required technical and organizational security measures are implemented for handling personal data in compliance with applicable regulations.
- Report any information security incident in a timely manner according to defined requirements.
- Identify awareness of the information security and enhance these with training sessions if required.
- Establish and communicate internal and external points of contact and sources of information for information security.
- Take into account the requirements for the design and operation of ICT systems.

The implementation of these requirements must be documented in a verifiable manner in order to comply with auditing requirements and for any liability claims and reported to the Service Owner.

6.1 Contact Partners for Information Security

If contractually required service suppliers must appoint a responsible individual for information security to deal with any information security topics. This person acts as a point of contact for the CISO or the Information Security Organization of MAN Truck & Bus.

The CISO at the MAN Truck & Bus Group is the responsible contact partner for the service supplier to handle any Company or Group-wide information security topics. This particularly applies to the handling of information security incidents.

Issues related to personal data protection in MAN Truck & Bus Group companies have to be reported to the responsible DPO or to the MAN Truck & Bus Group Data Protection Department (see more details in MTB Brand Policy MTB MR_4_6 Handling Personal Data and Data Protection Organization).

6.2 Information Security Standard

If contractually defined, MAN Truck & Bus Group service suppliers are obliged to implement a functional Information Security Management System (ISMS) based on the ISO 27001 standard, and to maintain and continually improve this system.

6.3 Verification and Requirements for Suppliers

The MAN Truck & Bus Information Security Organization determines the requirements for suppliers to provide secure services. These are related to the classification of information and to the protection level that the related service requires (see MTB Brand Instruction MA_13_1_03 – Classification of Information Assets).

The responsible service owner ensures that information security requirements are verified and met before the contract for service delivery is signed.

For addressing information security risks adequately, in case of high or very high protection needs, the suppliers are required to have a valid information security certification (e.g. ISO 27001 or TISAX).

If a potential supplier fails to provide a valid certification, a contract can only be concluded if the supplier commits to undergo a certification within a defined period (the contract must contain a special clause for describing this deviation and the requirement for certification e.g. within 9 months).

This verification procedure confirms compliance and suitability of the supplier for the provision of the respective service and handling of information on behalf of MAN Truck & Bus securely.

For detailed information on Verification and Requirements for Suppliers see Appendix 1 to MA_13_1_08 – Supplier Verification Methods and Requirements.

6.4 Reporting

Suppliers are obliged to provide regular reports on the security levels when required by MAN Truck & Bus. Some examples of reports are listed in the following:

- **Policy Compliance** – the aspect is that the system operators and administrators confirm compliance with MAN Truck & Bus Group Information Security policy, instructions and regulations – they must be aware of the policy, instructions and regulations and comply to them. The provisioning of this report is on a yearly basis.
- **System Access** – the aspect is to maintain an actual list of all individuals access to the systems. The provisioning of this report is on a quarterly basis.
- **Changes in System Access** – the aspect is to contain a list with all changes in system access to the service including the Suppliers. The provision of this report is on a quarterly basis.
- **System Access Rights** – the aspect is to contain a list of roles and access rights of the individual’s system access. The provision of this report is on a quarterly basis.
- **System Security Change Management** – the aspect is to contain a list of system changes with relation to information security. The provision of this report is on a quarterly basis.

Note: Printed versions and local files may not be updated!

- **Security Event & Incident Management** – the aspect is to contain a list of all occurred/detected security related events and incidents. The provision of this report is on a quarterly basis**.**
- **Security Incident Management - Response Time** – the aspect is to contain a list of all security incident response times and verify compliance with the Incident Management process in MAN Truck & Bus Group**.** The provision of this report is on a quarterly basis.
- **System Analysis tools** – the aspect is to show and describe the usage of security tools within the scope of systems provisioning (firewalls, antivirus, patch management, incl. their versions). The provision of this report is on a quarterly basis
- **Patch Management (do)** – the aspect is that all listed critical patches are applied. The provision of this report is on a quarterly basis.
- **Patch Management (check)** – the aspect is to report on the regular verification of patch levels of all systems. The provision of this report is on a quarterly basis.
- **Antivirus Management (do)** – the aspect is to present that all centrally managed systems have installed antivirus and antimalware protection. The provision of this report is on a quarterly basis.
- **Antivirus Management (check)** – the aspect is to present all systems are regularly scanned and use the latest recommended versions. The provision of this report is on a quarterly basis.
- **System Risk Report** – the aspect is to present Information Security related risks which are identified, documented, and managed. The provision of this report is on a quarterly basis.
- **System Audit Reports** – the aspect is to present the status of all audit findings, gaps and audit results and verify that they are reviewed/updated regularly. The provision of this report is on a yearly basis.
- **System Data Privacy Standard Report** – the aspect is to present the status of the implemented measures for compliance with the regulations regarding data protection**.** The provision of this report is on a yearly basis.
- **System Data Privacy Incident Report** – the aspect is to present all incidents that are occurred from a data protection perspective, including a description of measures to avoid such incidents. Regularity of this report must be per incident and the report must be presented immediately after completion of the incident analysis.

Note: Printed versions and local files may not be updated!

7 General Requirements for ICT systems and IT Service Suppliers

- For each individual employee of the supplier with responsibility for configuring the MAN Truck & Bus ICT systems, the employee's competences (rights and obligations) must be defined and documented.
- The employees' skills must correspond to the task.
- The service supplier must appropriately separate the tasks to prevent the misuse of ICT systems.
- Plan for and provide the required resources for ensuring operational security.
- Raise employee awareness of the importance of information security for the success of MAN Truck & Bus.

- Regular threat-based evaluation of the information security risks related to the provided service and adjustment to the requirements.

7.1 Requirement for Integration into Risk Management

The Risk and Opportunity Management (ROM) is regulated within the MAN Truck & Bus Group and aims to identify risks and opportunities at an early stage, to manage opportunities with potential for success and to avoid risks that could endanger the company.

A service supplier that provides services for ICT Systems that supports MAN Truck & Bus business processes has to provide a risk analysis. The impact to the Confidentiality, Integrity and Availability of the information assets has to be determined by using realistic threat scenarios. For the evaluation of the gross and net risks, the probability of occurrence and the impact to the information have to be assessed once without taking any risk treatment measures into account and once with taking the measures into account.

The decision for selecting suitable Information Security measures for managing the risks should be taken jointly between the service supplier and the MAN Truck & Bus service owner.

For this the minimum requirements from the MAN Truck & Bus information security framework or an equivalent set of security requirements must be applied.

7.2 Requirements for the Design of ICT Systems

The requirements are described in detail in Chapter 6.1 at MTB Brand Instruction MA_13_1_06 – Information Security for System Operation and Administration.

7.3 Requirements for the Design of Networks

The requirements are described in detail in Chapter 6.2 at MTB Brand Instruction MA_13_1_06 – Information Security for System Operation and Administration.

7.4 Requirements for the Operation of ICT Systems

The requirements are described in detail in Chapter 6.3 at MTB Brand Instruction MA_13_1_06 – Information Security for System Operation and Administration.

7.5 Requirements for the Operation of Network Infrastructure

The requirements are described in detail in Chapter 6.4. at MTB Brand Instruction MA_13_1_06 – Information Security for System Operation and Administration.

7.6 Requirements for Administrators at the IT Service Suppliers

Because administrators at the service supplier company have a special operational responsibility for ICT systems, they must meet the following requirements in line with the MTB Brand Instruction MA_13_1_01 - Standard for Information Security, article 16:

- To consider higher protection requirements for the usage and handling of administrative passwords.
- Administrators require regular awareness for the specific risks involved in their area of work. This includes instructions, trainings and drills.
- Passwords shall be managed in accordance with documented procedures.
- Privileged user accounts shall not be used for everyday work.
- Elevated access rights must be verified on regular intervals. The intervals are determined according to the extent and criticality of the access right.
- Identical administrative passwords must not be used for different applications.

- Server panels and consoles must be locked when not in use.
- Sessions must be closed immediately after finishing the task(s).

8 Change History

Version 3.0

- Added Change Log
- Relabeling
- Changes in roles and responsibilities
- Added section 6.3 – Verification and Requirements for Suppliers
- Added section 6.4 - Reporting
- Deleted double section
- Changed the name of the instruction – was “MAN 13.1 Instruction 8 – Information Security for the collaboration with IT Service Providers”.

Note: Printed versions and local files may not be updated!

Appendix 1 : Supplier Verification Methods and Requirements

Note: Printed versions and local files may not be updated!

Note: Printed versions and local files may not be updated!

Appendix 1 - Supplier Verification Methods and Requirements

Created	Steven Rauwerdink Ralf Schlag	**Approved**	Andre Wehner	**Version**	1.0
Dept.	FIOS	Dept.	FI	**KSU-Class:**	xx
Applicable as of		**Scope**		**Approved by (Board)***	
Date	01.02.2023	MAN Truck & Bus SE and its Subsidiaries			
				Agreed by	

* Only required for Brand Instructions that do not relate to a superior Brand Policy

Contents

Note: Printed versions and local files may not be updated!

1 Purpose

The purpose of this Appendix is to define and describe in detail the Information Security requirements for Suppliers handling information on behalf of MAN Truck & Bus.

The Appendix supplements MTB Brand Instruction MA_13_1_08 – Information Security for Suppliers.

2 Verification Methods and Requirements

2.1 Suppliers Handling Information

The starting point of the verification is the correct identification and classification of key information assets associated with the service to be provided by the supplier. The service owner classifies the information that will be handled by the partner. The handling includes transferring, storing and using the information. The classification helps with identifying the protection needs as well as the requirements which the supplier has to be compliant with in relation to the provided service. For this purpose, the ISi assessment process, in cooperation with the information security department, is implemented.

To determine the suitability of a potential supplier other aspects may require to be verified. Those could be of legal nature, such as handling personal related information, services around financial systems related to reporting, information that may be subject to export control, companies that could be raising issues with anticorruption, anti-bribery or supply chain regulations.

2.1.1 Certification Requirements

For addressing information security risks adequately, Suppliers that are handling information on behalf of MAN Truck & Bus, which has been classified as confidential, strictly confidential and thus with a high or very high protection need, require a valid information security certification.

- ISO 27001 Certificate

  A suitable ISO 27001 certification requires the following aspects:

  - The certificate is up to date.
  - The scope of the certified information security management system includes the entire area that is involved with the MAN Truck & Bus information processing activity.

- TISAX Certificate

  A TISAX Certification requires the following aspects:

  - The TISAX Certification is up to date.
  - A TISAX Certification exists for every location that is involved with the MAN Truck & Bus information processing activity.
  - The information of the certification is shared with the VW ENX ID "PVPT9Z" on the ENX Database[1].

[1] TISAX list - on section 3, there is reference to all suppliers who have shared their TISAX results with VW Group (Updated every two weeks).

- The TISAX label is aligned with the classification of information that is processed:
  - (Info, high) for information with high protection requirement (e.g. confidential)
  - (Info, very high) for information with very high protection requirement (strictly confidential or special personal related information)
  - (data) for personal related information

2.1.2 Deviations

If a potential supplier fails to evidence a valid certification, a contract can only be concluded if the supplier commits to undergo a certification within a defined period.

- The contract contains a clause with a text such as:
  - TISAX: For its primary site and any other site processing information on behalf of MAN Truck & Bus, the Supplier agrees to carry out a certification in accordance with the TISAX method at the Assessment Level 2 no later by XX.XX.202X.

    The Certification shall include at least the following modules:
    - Basic module Information Security (Info, high)
    - Additional module Data Protection (Data)
  - ISO 27001: The Supplier undertakes to carry out a certification in accordance with ISO 27001 by XX.XX.202X. In this case, the provision of services for MAN Truck & Bus is fully to be covered by the scope of the Supplier’s certified information security management system.
- The supplier will provide a GAP Analysis including an action plan for reaching the certification level in the projected timeframe.
- MAN Truck & Bus Information Security organization will review the analysis and confirm the supplier.

2.1.3 Supplier Contract

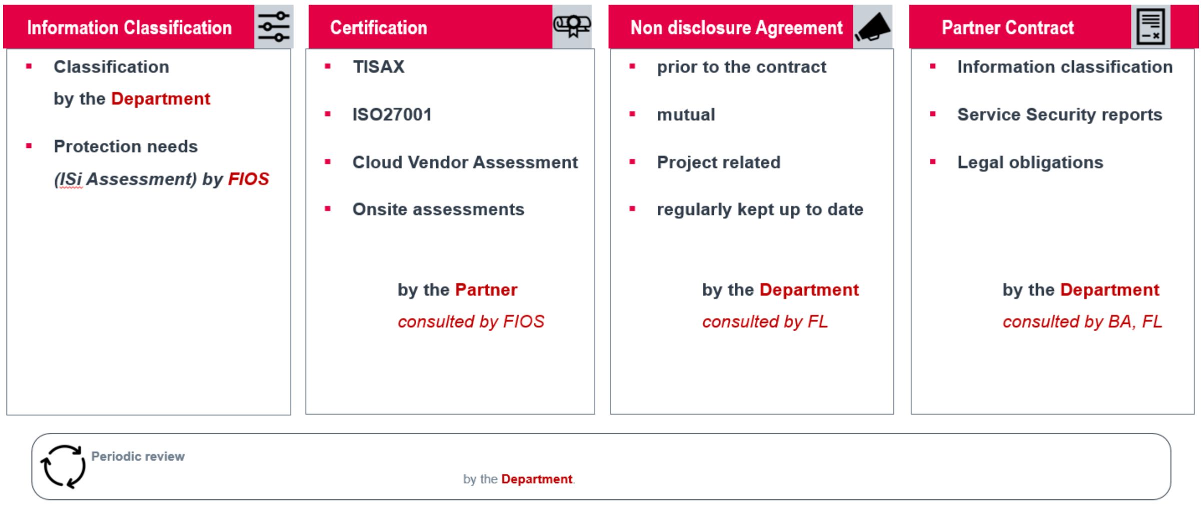
After classification of information assets and validation of information security certification requirements, the cooperation with the supplier should be based on a valid contract between MAN Truck & Bus SE and the supplier. Prior to the contract a non-disclosure agreement must be signed and regularly kept up to date. The contract includes relevant information items:

- Information classification shared with the supplier.
- The contract shall include the obligation of providing regular supplier reports relevant to information security.
- Additional clauses and appendices shall include legal and regulatory requirements, for example data privacy, antitrust law or export control.

Note: Printed versions and local files may not be updated!

2.1.4 Review

Regular reviews of changes related to classification of information assets and supplier compliance as per agreed information security requirements must be conducted.



Information Classification

- Classification by the Department
- Protection needs (ISi Assessment) by FIOS

Certification

- TISAX
- ISO27001
- Cloud Vendor Assessment
- Onsite assessments

by the Partner
consulted by FIOS

Non disclosure Agreement

- prior to the contract
- mutual
- Project related
- regularly kept up to date

by the Department
consulted by FL

Partner Contract

- Information classification
- Service Security reports
- Legal obligations

by the Department
consulted by BA, FL

Periodic review

by the Department

2.2 Cloud Vendor Assessment (CVA)

Cloud services require additional verification to determine that Information Security standards are fulfilled. The reason for this is that the service is usually accessible directly from the Internet. Also the exact location of information and the individuals that have got access to the information is often not clearly defined.

A Cloud Vendor Assessment evaluates the level of security of cloud service suppliers. The purpose is to evaluate the internal control systems of Cloud Vendors with respect to information security.

Such an assessment is based on a cross-industry criteria catalogue yielding a profound indication of the state of information security specific to cloud vendors. It consists of controls in various subjects (domains) of information security.

A CVA (e.g. DCSO CVA, CSA STAR and BSI C5) is mandatory for projects and solutions with a high or very high protection need using third party cloud services such as Software as a Service and Platform as a Service.

3 References

- VW Group Supply Procurement conditions IT (MAN (vwgroupsupply.com))
- ISi Assessment - (MAN Intranet > Corporate > Information Security > ISi Assessment)
- Supplier Reports (MAN Intranet > Corporate > Information Security > Supplier Assessments > Supplier Reports)
- VW KRL13 Appendix 1
- TISAX List (TISAX Liste - Konzern Sicherheit - Group Wiki (volkswagen-net.de))
- Regulation 03.01.017 Cloud Security (Regulation Cloud Security Group Wiki (volkswagen-net.de))

- Regulation 03.01.016 Third Party Delivery Management (Regulation Third Party Delivery Management Group Wiki (volkswagen-net.de))

4 Change History

Version 1.0

- Creation

Note: Printed versions and local files may not be updated!

Handling personal Data and Data Protection Organization

Note: Printed versions and local files may not be updated!

Created	Heike Bösl	**Approved**	Karl-Heinz Müller	**Version**	3.0
Dept.		Dept.		**KSU-Class:**	xx
Applicable as of		**Scope**		**Approved by (Board)**	
Date	01.07.2020	MAN Group		Drees Dr. Intra Schenk Cortes	
				Aggreed by	

Contents

Note: Printed versions and local files may not be updated!

Note: Printed versions and local files may not be updated!

1. Purpose

Treating each other respectfully as well as customers, employees, suppliers and other business partners and participants is a characteristic element of the companies in the MAN Group. In the area of data protection, this respect is expressed in the activities which aim to protect the personal rights of natural persons at a high level when processing their personal data. At the same time, this should also enable appropriate use of personal data and thus supporting the business activities of the MAN Group in general and its digital transformation in particular. Last but not least, data protection-relevant legal infringements and any legal and economic disadvantages that may result from them are to be avoided as far as possible.

The purpose of this policy is to ensure that the objectives pursued are achieved by ensuring that for all relevant companies in the MAN Group

- basic rules and framework conditions for handling personal data are defined,
- a practicable organizational structure for data protection is established, and
- an adequate data (protection) management is established.

This policy implements the requirements of the Volkswagen Group Policy "Data Protection in the Volkswagen Group" and the TRATON Policy 4.2 "Protection of Personal Data and Organization of Data Protection".

This policy does not regulate the topics of data security, document retention and document classification. These topics are covered by separate regulations.

Note: Printed versions and local files may not be updated!

2. Scope

The functional scope of this policy covers all processes in which personal data of natural persons are collected, stored, organized, linked, transmitted, used, changed, read, destroyed or otherwise processed in a fully or partially automated manner. This applies in particular to personal data of employees, customers, suppliers or other business partners. This policy also applies to the non-automated processing of personal data in structured data collections.

This policy applies directly to MAN SE and its employees. In addition, the contents of this policy are to be implemented in all companies in which MAN SE directly or indirectly has a shareholding of more than 50% and in which data processing operations of the type mentioned in paragraph 1 take place (Group companies).

In some countries, national data protection legislation protects information about legal persons in the same way as information about natural persons. In these cases, the company's management must determine, by means of a supplementary regulation at company level, to what extent the contents of this policy also apply to information about legal entities.

Insofar as the contents of this policy are not compatible with the provisions of national or supranational law in a country, these provisions of national or supranational law shall take precedence. This applies in particular if national law provides for a higher level of data protection than this policy.

Every supplementary regulation serving the implementation of this policy shall be submitted to the data protection officer responsible for approval in good time before publication.

3. Terms and Definitions

For the sake of simplicity, the roles and responsibilities set out in this policy are also used to rep-resent the feminine and divers forms exclusively in the masculine form.

Anonymization of personal data means that all identification features (e.g. name, e-mail address, user ID) are deleted or changed to such an extent that the identity of the person concerned can no longer be traced or can only be traced with disproportionately great effort.

Consent is any voluntary, informed and unambiguous expression of will in the specific case, in the form of a statement or any other clear affirmative action by which the data subject indicates his or her consent to the processing of personal data relating to him or her.

Data controller is any natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Data protection manager is the person formally appointed by a department, division, location, company or group of companies who serves as a contact person for the company's data protection officer and the respective higher-level data protection managers in data protection-relevant issues and who is responsible for the operational implementation of data protection regulations in his or her area of responsibility and is bound by instructions. Depending on the area of responsibility, the persons named are referred to as Group, company, division or departmental data protection managers or in a comparable manner.

Data protection officer is the person who, on the basis of this policy, national law or supra-national, has been formally appointed by the company management as responsible for data protection issues in this company and who is not bound by instructions in this function.

Data recipient is the natural or legal person, authority, institution or other body to whom personal data are transferred or to whom they are otherwise disclosed.

Data subject is the identified or identifiable natural person to whom personal data relates, e.g. employees of a group company or contact persons at a customer.

Personal data is information about an identified or identifiable natural person. A person is identifiable if he or she can be identified directly or indirectly by one or more pieces of information (e.g. name, personnel number, user ID or address).

Procedure for processing personal data is a bundle of related processing activities that serve a uniform purpose. Examples: payroll accounting, customer relationship management, video surveillance.

Processing is any operation carried out manually or automatically in relation to personal data, in particular collection, storage, organizing, amendment, transmission, extraction, disclosure, combination, restriction, deletion or destruction.

Processor means any natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller.

Pseudonymization is the processing of personal data in such a way that the personal data can no longer be assigned to a specific person without the inclusion of additional information. This additional information must be stored separately and be subject to technical or organizational measures that ensure that the personal data cannot be assigned to an identified or identifiable natural person.

Restriction of processing is the marking of stored personal data in order to limit their processing in the future. Example: data stored only for tax reasons are marked so that they can no longer be used for marketing purposes.

Sensitive personal data (special categories of personal data) are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, genetic and biometric data, personal data concerning the health, sex life or genetic characteristics of a natural person and personal data relating to offences, offences or criminal convictions.

Third party means any natural or legal person, public authority, agency or other body other than the data subject, the data controller and the processor.

Note: Printed versions and local files may not be updated!

Transfer is any disclosure of personal data to another natural or legal person, public authority, agency or body. A transfer also exists if another body is given the opportunity to access personal data.

4. Principles Governing the Processing of Personal Data

When processing personal data, the following principles must be observed. If there is any doubt about the permissibility of processing, it must be suspended until further notice and the data protection officer must be contacted.

4.1 Processing in Good Faith

Personal data is processed fairly and in accordance with the principles of good faith.

4.2 No Processing Without Legal Basis

Personal data may only be processed if there is a corresponding legal basis for the respective processing and if this is sufficiently documented. Processing without a sufficient legal basis is not permitted and must therefore not take place.

For the processing of personal data by a company and its employees, the following legal bases come into consideration:

Contract | Personal data required for the conclusion, implementation or termination of a contract with the data subject may be processed. This also applies to personal data required for the initiation of contractual relationships or the fulfilment of post-contractual obligations as desired by the data subject.

Law | Personal data may be processed if a law or a binding court or authority decision makes this necessary.

Balance of interests | Personal data may be processed if and to the extent that this is necessary to safeguard the legitimate interests of the data controller or a third party and if, on the other hand, the interests of the data subject in refraining from processing do not outweigh these interests.

Consent | If the data subject has given his or her consent to the processing of his or her data on a voluntary, specific, unambiguous and informed basis, the personal data covered by the consent may be processed. If the processing is based on consent, the data controller must at all times be able to demonstrate by appropriate documentation that the data subject has consented to the processing of his or her personal data.

Vital interests | The processing of personal data is permitted if it is necessary in order to protect the vital interests of the data subject or of another natural person.

Public interests | The processing of personal data is permissible if it is in the public interest or in the exercise of official authority vested in the data controller.

4.3 Purpose Limitation

Personal data may only be collected if they are necessary to achieve a specifically defined, legitimate purpose. The department requesting the data processing must document the purposes prior to processing, unless they are obvious.

The use of personal data for a purpose other than the original purpose is permissible if this new purpose is compatible with the original one. The change of purpose shall be documented. If the new purpose is not compatible with the original purpose, the use of personal data is only permissible if there is a specific legal basis for the use of personal data for the new purpose.

4.4 Proportionality, Data Minimization

The principle of proportionality must be respected when processing personal data. A processing operation

Note: Printed versions and local files may not be updated!

shall only be proportionate if

- it is suitable for achieving a legitimate purpose.
- there is no milder, equally suitable means of achieving that purpose. In particular, the collection of data without personal reference or the processing of anonymized or pseudonymized data is a milder means.
- the number of persons concerned and the scope of the processed data have been reduced to the necessary extent (data minimization).
- the circle of persons who are granted access to personal data is limited to those who need such access in order to carry out their intended activities (need-to-know principle).
- the processing is not opposed by any overriding interests of the data subject worthy of protection.

4.5 Principle of Direct Collection

Personal data must always be collected directly from the data subjects. A collection from third parties is permissible if a legal provision provides for or requires this, if it is in the interest of the data subject or if a direct collection would only be possible with disproportionate effort. Irrespective of whether personal data are collected directly or not directly from the data subject, the data subject must be informed in accordance with Section 4.6.

4.6 Transparency and Information of the Data Subject

Personal data shall be processed in a way that is comprehensible to the data controller and the data subjects.

The data subjects shall therefore be informed by the department requesting the data processing at the latest at the time of data collection about the processing of their personal data in a transparent, easily understandable form and in accordance with national requirements. The information shall contain the following elements in particular:

- the identity of the data controller,
- the purposes of the processing,
- the legal basis for the processing,
- the legitimate interests, if the data processing is based on a balancing of interests,
- the categories of personal data processed,
- the storage duration,
- the data recipient or the categories of data recipients,
- the source from which the data originate, unless they are collected directly from the data subject, and
- information on how to exercise any data protection rights to which the data subjects may be entitled.

The information may be omitted if it does not appear to be necessary in view of the circumstances of the collection, the purpose of the processing or the overriding interests of the data controller. This is the case, for example, if the data subject already has knowledge of the processing or if the processing is required by law. When collecting personal data, it must be made clear which information is voluntary and which is obligatory.

4.7 Data Quality

Personal data must be collected and processed in a factually correct manner. Appropriate measures must be taken to ensure that incorrect or incomplete data is corrected, supplemented or deleted in good time.

4.8 Data Security

The data controller shall take appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing, destruction, loss or alteration. These measures shall ensure a level of protection appropriate to the risks presented by the processing and the nature of the personal data to be protected, taking into account the state of the art, the costs incurred in their implementation and other efforts. In this context, the policies and instructions applicable to the respective company in the field of data security must be observed in particular.

4.9 Deletion of Data

Personal data no longer required must be deleted. In principle, the corresponding deletion concept must be drawn up before the data is collected. Personal data is no longer required in particular if the purpose for which it was originally collected no longer exists, if the data is no longer required to achieve this purpose or if a prerequisite for the permissibility of data processing has subsequently ceased to apply. If deletion of the data is only possible at disproportionately high expense or if the personal data are only required to fulfil storage obligations or comparable purposes, they must be marked with the aim of restricting their future processing accordingly.

When drawing up the deletion concept and deleting personal data, the rules for retention periods and classification in accordance with the group-wide Classification System for Documents (KSU) in its currently valid version shall be taken into account, unless mandatory legal provisions stipulate otherwise.

Note: Printed versions and local files may not be updated!

5. Special Forms of Data Processing

5.1 Commissioned Data Processing

In the case of commissioned data processing, personal data are processed by a data processor (contractor) on behalf of the data controller (principal). The controller remains responsible for the proper processing of the personal data.

Companies that fall within the scope of this policy may only carry out commissioned data processing as a principal if the following conditions are met:

- The principal has concluded a commissioned data processing agreement with the contractor, in which at least the following issues are regulated: the object, duration, nature and purpose of the processing, the nature of the personal data, categories of data subjects, erasure periods, the fate of the personal data after termination of the contract and the rights of control and instructions of the principal.
- The contractor has taken sufficient technical and organizational measures to protect the personal data. The responsible operative department is responsible for checking these measures.
- The contractor shall not engage any other contractor (subcontractor) to perform its tasks without the prior general or specific approval of the principal. The contractor shall carefully select its subcontractors and conclude contracts with them that also include the minimum contents mentioned above. The principal must regularly satisfy himself of the proper performance of the contract.

Since the contractor is not a third party within the meaning of this policy, the transfer of data from the principal to the contractor does not require a separate legal basis in accordance with section 4.2.

5.2 Transfer of Personal Data to Third Parties

The transfer of personal data to third parties is only permitted if it is based on a separate legal basis in accordance with section 4.2. This also applies if the third party is a another Group company or another company of the Volkswagen Group.

The processing of the transferred data by the data recipient requires a separate legal basis, the existence of which must be ensured by the data recipient prior to processing.

5.3 Joint Data Controllers

Where two or more data controllers jointly determine the purposes and means of the processing, they shall be joint data controllers. Joint data controllers shall enter into an agreement to determine transparently which of them has to fulfil which data protection obligation.

5.4 Transfer of Personal Data to Third Countries

The transfer of personal data from a Member State of the European Union to a country outside the European Economic Area must comply with the specific rules applicable.

6. Group-wide Binding Data Protection Measures

The MAN Group companies falling within the scope of this policy take the following binding measures within their area of responsibility in order to ensure comparable standards in data protection, to achieve synergies within the MAN Group and to enable a uniform, Group-wide reporting system.

6.1 Records of Processing Activities

The MAN Group companies shall draw up and continuously update a complete and informative list of their data protection-relevant processing activities. Binding specifications issued by the MAN Group for this purpose will be complied with unless they contravene mandatory legal provisions of the country concerned.

6.2 Notification Process for Personal Data Breaches

The MAN Group companies shall implement reporting processes in their area of responsibility to ensure that personal data breaches in their area of responsibility are detected as quickly as possible and their negative impact is limited as far as possible by taking appropriate measures. Any reports to supervisory authorities that may be required must be made in a timely manner.

6.3 Risk Management, Monitoring

The MAN Group companies shall install an appropriate data protection risk management system and also comply with the relevant central policies.

For the purpose of structured and systematic monitoring, the Group companies will, in particular, anchor appropriate controls in their internal control systems or effectively implement and execute centrally prescribed controls. In consultation with the brand spokesman for data protection, suitable monitoring can also be ensured in other ways.

6.4 Deletion and Access Authorization Concepts

The MAN Group companies shall draw up and implement deletion and access authorization concepts in their respective areas of responsibility to ensure that personal data is processed and deleted in compliance with data protection regulations.

When creating deletion concepts and deleting personal data, the rules for storage and classification in accordance with the KSU in its currently valid version shall be taken into account, unless mandatory legal provisions require otherwise.

6.5 Establishing a Data Protection Reporting

The Group companies shall establish data collections and processes in their area of responsibility that enable appropriate data protection reporting within the MAN, TRATON and Volkswagen Group.

7. Roles and Responsibilities

7.1 Management Boards

The Management Board of the respective company is legally responsible for compliance with the statutory and company-specific regulations relevant to data protection. The Management Board supports the departments and the members of the data protection organization in the performance of their duties, in particular by providing sufficient personnel and material resources.

The Management Board nominates one of its members to be professionally and organizationally responsible for compliance with the statutory and company-specific regulations issued for the protection of personal data. This member has to be notified to the brand speaker data protection (see section 8.3.1).

If several data protection functions report to the same member of the Management Board, this member may appoint a reporting responsible to coordinate the reports.

7.2 Employees

Every employee has the individual duty to carry out his or her work in accordance with the regulations relevant to data protection. Managers are also obliged to act as role models in this respect.

7.3 Departments

It is the responsibility of the departments to ensure compliance with the legal and company-specific regulations on data protection within their area of responsibility and to take the necessary measures in this respect. These measures include in particular the proper documentation of the data protection activities relevant to their area in terms of content and organization.

The head of the department shall inform the data protection officer (see section 8.3.3) or the corporate data protection manager (see section 8.4.2.) of any matters from his or her department that also concern the area of responsibility of the data protection officer or the corporate data protection manager in a timely and appropriate manner and without being asked. The head of the department shall be responsible for bringing the matter to the attention of the data protection officer and corporate data protection manager. He will also take measures and establish processes to ensure the implementation of the data protection principles "Privacy by Design" and "Privacy by Default" in his area of responsibility.

If necessary, the head of the department will appoint a departmental data protection manager (see section 8.4.3) to support the fulfillment of his or her data protection-related tasks.

7.4 Data Protection Organization

The MAN data protection organization works to ensure that data protection in the companies of the MAN Group is implemented in accordance with the law, is practical and supports MAN business activities. It is active both in an advisory and monitoring capacity as well as in the operative implementation of the data protection regulations. The design and implementation of data protection should be as efficient and effective

Note: Printed versions and local files may not be updated!

as possible. For details on this, please see section 8 below.

7.5 Information Security Organization

Data protection and Information security tasks overlap in the area of technical and organizational protection of personal data. Information security supports the company's data protection activities, in particular by defining, providing and testing the necessary technical and organizational measures. In addition, the data protection and information security organizations regularly inform each other about matters that may be relevant to the other area.

7.6 Internal Audit

As part of its general tasks, Internal Audit supports the data protection activities of the companies by also considering suitable audit proposals of Data Protection when planning its annual audit program.

7.7 Legal

Data Protection and the Legal regularly inform each other about matters from their own area of responsibility that may also be of importance to the other area.

7.8 Employee Representative Bodies

The tasks of the Employees Representative Bodies and those of Data Protection overlap in the area of safeguarding the personal rights of employees relevant to data protection. In this respect, Employee Representative Bodies and Data Protection work together in a spirit of trust. The rights of the Employee Representative Bodies are not affected by this policy.

Note: Printed versions and local files may not be updated!

8. Data Protection Organization

8.1 Task of the Data Protection Organization

The MAN data protection organization works to ensure that data protection in the companies of the MAN Group is implemented in accordance with the law, is practical and supports MAN business activities. The design and implementation of data protection should be as efficient and effective as possible.

Persons who perform corresponding roles within the data protection organization must be sufficiently qualified for this and must be given the opportunity to fulfil their respective roles effectively and in accordance with the provisions of this policy.

8.2 Unit Consisting of Parts Not Subject to Instructions and Parts Subject To Instructions

The data protection organization of the MAN Group basically consists of two organizationally separate areas with different tasks, which in their entirety are intended to ensure the proper fulfilment of the data protection requirements that apply to the company. One of these areas is the data protection organization, which is not subject to directives. It consists of the functions described in section 8.3. The other part is the data protection organization subject by instructions. It consists of the functions described in section 8.4.

The division of the data protection-related tasks affecting the company into two organizationally separate areas is necessary in order to comply with the task description for data protection officers in the EU General Data Protection Regulation and comparable laws. On the other hand, it serves to avoid conflicts of interest between advisory and auditing functions on the one hand and the operational implementing functions on the other.

8.3 Data Protection Organization Not Subject To Instructions

8.3.1 Brand Group Spokesperson Data Protection

The brand group spokesperson data protection coordinates the data protection activities of the brands combined under TRATON in matters that are cross-brand or of fundamental importance. His contact persons are in particular the Management Board of TRATON SE, the respective brand spokespersons data protection, the brand data protection managers as well as Group Legal and the Group Data Protection Officer both at Volkswagen AG.

The brand group spokesperson data protection is appointed by the Management Board of TRATON SE. The appointment is performed in writing by means of an employment contract or internal company regulation. The brand group spokesperson for data protection does not have to be an employee of TRATON SE, but an employee of a company in the TRATON Group.

8.3.2 Brand Spokesperson Data Protection

The brand spokesperson data protection coordinates the data protection activities of the data protection officers of the companies grouped under a brand in matters that affect more than one company or that are of fundamental importance for the brand. His contact persons are, in particular, the management of the brand-leading company of the respective brand, the data protection officers of the companies or comparable functions combined in the respective brand, the brand data protection manager and the brand group spokesperson data protection. In this capacity, the brand spokesperson data protection reports directly to the Management Board of the brand-leading company.

The brand spokesperson data protection is appointed by the Management Board of the brand-leading company. The appointment is made in writing by means of an employment contract or internal regulations. The brand spokesperson data protection does not have to be an employee of the company itself, but an employee of a company of TRATON group. The representation of several brands by the same brand spokesperson data protection is permissible. Insofar as the brand-leading company has not appointed a brand spokesperson data protection, this function is performed by the brand group spokesperson data protection.

8.3.3 Data Protection Officers

The Management Board of every company in the MAN Group is obliged to appoint a person with their consent in writing as data protection officer or in a comparable function. This obligation only ceases to apply if and insofar as the company employs less than 20 employees on average in the past calendar year or the brand spokesperson data protection has granted a written exemption.

In order to avoid conflicts of interest, the data protection officer should not, as a matter of principle, be a member of the management or head of the local IT or HR department. Deviations from this principle are only permitted with the consent of the brand spokesperson data protection. The data protection officer does not have to be an employee of the appointing company, but an employee of a company in the TRATON Group.

Insofar as the company must appoint or has already appointed a data protection officer in accordance with local data protection law, this person simultaneously exercises the function of data protection officer. It is irrelevant whether the data protection officer is designated as data protection responsible, data protection officer, or with comparable terms under local law and whether the rights and obligations of the data protection officer under local law are regulated differently from those of this policy.

The data protection officers shall perform the tasks assigned to them by law or this policy. In their

Note: Printed versions and local files may not be updated!

capacity as data protection officers, they report directly to the Management Board of their company. Exceptions must be agreed with the brand spokesperson data protection.

The tasks of the data protection officers include in particular

- informing and advising management and staff on data protection issues,
- monitoring compliance with legal and company-specific data protection regulations,
- assistance in meeting any reporting obligations under local data protection laws,
- his or her own training in data protection,
- the provision of guidelines for the operational implementation of data protection in the company,
- the provision of appropriate templates for data protection contracts, data protection clauses, data protection declarations, privacy notices and other documents,
- reporting on the company's data protection activities to the Management Board and the brand spokesperson data protection, and
- act as a professional contact point for the data protection authorities.

The duties of the data protection officer and his or her auxiliary staff in the MAN Group companies do not include professional responsibility for the operational implementation of legal, regulatory and company-specific data protection requirements or the approval of data protection concerns or specific processing activities.

The data protection officers are obliged to treat all matters that come to their attention in their function as data protection officers as confidential and to maintain confidentiality in this respect.

Note: Printed versions and local files may not be updated!

8.4 Data Protection Organization Subject To Instructions

8.4.1 Brand Data Protection Manager

The brand data protection manager coordinates the data protection activities of the data protection managers of the companies grouped under a brand in matters that are of fundamental importance to the brand or that affect more than one company. In particular, his or her contact persons are the Management Board of the brand-leading company, the data protection managers of the companies combined under the respective brand, the brand spokesperson data protection and the brand group spokesperson data protection. In this capacity, the brand data protection manager reports directly to the Management Board of the brand-leading company.

The brand data protection manager is appointed by the brand-leading company. The appointment is made in writing by means of an employment contract or internal regulations. The brand data protection manager does not have to be an employee of the company itself, but an employee of a TRATON Group company.

8.4.2 Company Data Protection Manager

The Management Board of every company in the MAN Group is obliged to appoint a person belonging to the company with their consent in writing as company data protection manager. This obligation only ceases to apply if and insofar as the company employs less than 20 employees on average in the past calendar year or the brand spokesperson data protection has granted a written exemption.

The core task of the corporate data protection manager and the employees directly or indirectly assigned to him in this function is the operative implementation of data protection in the company. He or she coordinates and supports the heads of the departments in fulfilling their data protection tasks. He or she is the first point of contact for all data protection-related questions and matters in the company, un-less this task is performed by the department data protection managers assigned to him or her.

As long as the company has not appointed a corporate data protection manager, although this is required under paragraph 1, this function shall be performed by the member of the company's Management Board responsible for data protection.

8.4.3 Department Data Protection Manager

If necessary, the heads of departments shall appoint one or more departmental data protection managers in writing to provide internal support for the data protection tasks that fall to them un-der the law and this policy. The core task of the departmental data protection managers is to ensure the operational implementation of data protection in the respective department.

In their capacity as departmental data protection managers, they are professionally assigned to the corporate data protection manager.

Paragraph 1 applies analogously to other organizational units within the company, such as locations, departments or divisions.

8.4.4 Übersicht

As described in sections 8.3 and 8.4.1-8.4., the employees entrusted with data protection tasks are basically active at the following levels:

Level	Example	Data Protection not subject to instructions	Data Protection subject to instructions
Brand Group	TRATON	Brand Group Spokesperson DP	./.
Brand	MAN, Scania	Brand Spokesperson Data Protection	Brand Data Protection Manager
Company	MAN Truck & Bus SE, Scania CV AB	Data Protection Officer	Company Data Protection Manager
Department, area	IT, HR, Sales	./.	Department Data Protection Manager

Deviations from this nomenclature are only permitted in agreement with the brand group spokesperson data protection.

9. Rights of the Data Subjects

The rights of the persons concerned to information, deletion, correction, restriction of processing, objection and revocation of declarations of consent are determined by the data protection law applicable to the company in question, by the procedures agreed at brand level and by the company-specific regulations applicable to these rights.

10. Notification of Personal Data Breaches

10.1 Persona Data Breach

A personal data breach occurs when the security of personal data has been breached and this has resulted in the destruction, alteration, unauthorized disclosure or loss of or unauthorized access to personal data.

Note: Printed versions and local files may not be updated!

Violations of data protection must be identified and stopped as soon as possible.

10.2 Involvement of the Data Protection Officer

The data protection officer shall be informed immediately if

a) personal data have come to the knowledge of unauthorized persons, have been processed unlawfully or in breach of this policy in any other way or where there are specific grounds for suspecting that they have been processed unlawfully or in breach of this policy, and where there is a serious risk that the rights or legitimate interests of a significant number of data subjects may be prejudiced as a result,

b) there is a legal obligation to notify a public authority of a breach of the rules on the protection of personal data, or

c) sanctions are to be imposed or have already been imposed on the company by the courts or public authorities for breaches of data protection legislation.

10.3 Involvement of Brand (Group) Spokesperson Data Protection

The responsible brand spokesperson and the brand group spokesperson will be included in the notification if the personal data breach or its sanctioning is relevant or of fundamental importance for more than one brand company.

10.4 Involvement of Group Legal and Group Data Protection at VW AG

In the event of personal data breaches or enquiries from supervisory authorities which are relevant or of fundamental importance for more than one brand, the brand group spokesperson data protection or the responsible brand spokesperson data protection shall immediately involve Group Legal at VW or the Group Data Protection Officer at VW.

10.5 Notification of Personal Data Breaches to Authorities

Notifiable personal data breaches must be reported to the authorities in due form and time. Personal data breaches are reported to authorities in accordance with the legal provisions applicable to the companies concerned. The legally or officially prescribed forms and deadlines for reporting must be observed.

11. Exceptions

Exceptions to the regulations contained in this policy are only permitted if they have been agreed in advance in text form with the brand spokesperson data protection.

Note: Printed versions and local files may not be updated!

VOLKSWAGEN
AKTIENGESELLSCHAFT

Information Security

Guidelines
– Guideline for System Operators and Administrators –

Publisher
Group Information Security

Regulation No.
02.03

Status
Published

Version
4.1

Classification
Internal

Date
November 03, 2022

Scope

This guideline applies to Volkswagen AG (organizational units (OU) on Group level and on brand level of the Volkswagen Passenger Cars brand, Volkswagen Commercial Vehicles brand and Volkswagen Group Components). All system operators and administrators must adhere and comply with this guideline.

With regard to the implementation of the Information Security Regulations at other Volkswagen Group companies, ORL 1 "Organizational Regulations of Volkswagen AG" applies.

Table of Contents

I 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.2.1).

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.2.2).

1 Context

The following overview shows how the Information Security Guidelines fit into the Information Security Regulations Framework.

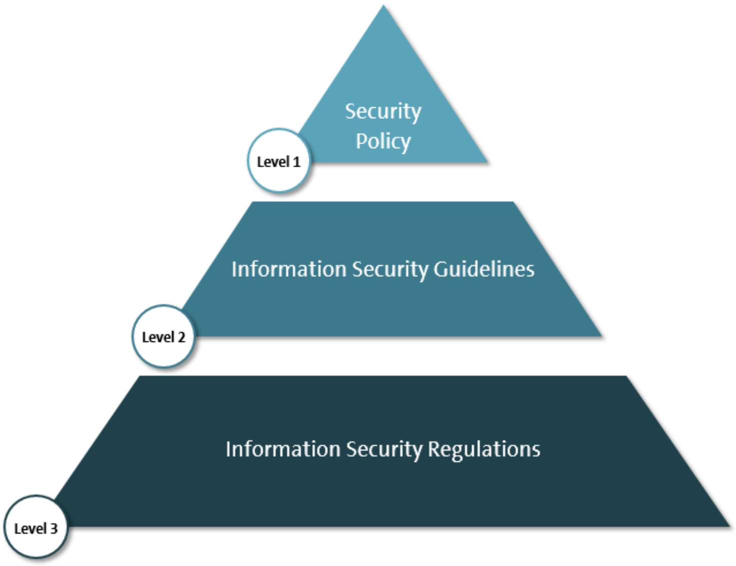

Security Policy
Level 1
Information Security Guidelines
Level 2
Information Security Regulations
Level 3

Illustration 1: Information Security Regulations Framework

Level 1 Information Security Policy:
Defines the basic objectives, strategies and responsibilities to ensure a minimum level of information security and is documented in Group Policy 18 and the derived brand characteristics (see appendix B.2.3).

Level 2 Information Security Guidelines:
Design of information security policy into organizational instructions for individual user groups

Level 3 Information Security Regulations:
Specification of regulatory requirements in the technical environment and description of technical functions and processes of information security

2 Asset management

All company-owned IT systems (see appendix B.2.5) 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

3 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)

4 Communications and operations management

4.1 Operational procedures and responsibilities

4.1.1 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.2.6). The system operator is obliged to follow the established operational procedures (e.g. of the change process).

4.1.2 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.

4.1.3 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.

4.1.4 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 B.2.18) 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.

4.2 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.2.7). In doing so, the requirements of the regulations (see appendix A.1.6) must be followed.

4.3 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).

4.4 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.2.7). 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).

4.5 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.

4.6 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.

4.7 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.

4.8 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).

4.9 Monitoring

4.9.1 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

4.9.2 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.2.8).

4.9.3 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.

4.9.4 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.

Die Inhalte, die Protokolle mindestens enthalten müssen, sind in der Regelung (siehe Anhang A.1.2) dokumentiert.

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

4.9.5 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.

4.9.6 Time synchronization

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

5 Access control

5.1 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.

5.2 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 more than 400 days must be blocked.

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.

5.3 Obligations of users with privileged rights

5.3.1 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).

5.3.2 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.

5.3.2.1 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).

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

5.3.2.2 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).

5.3.3 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.2.15) 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.2.16).
- Create local accounts

5.4 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).

5.5 Operating system access control

5.5.1 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).

5.5.2 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.2.7).

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

5.5.3 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).

5.5.4 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).

5.5.5 Session timeouts

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

5.5.6 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.2.17).
- Proof of secure deletion must be kept.
- Only approved tools may be used for secure deletion (see appendix B.2.14).

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.

6 Procurement, development and maintenance of IT systems

6.1 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.

6.1.1 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

6.1.2 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)

6.1.3 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.

6.2 Cryptographic measures

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

6.3 Security of system files

6.3.1 Control of operational software

Software may only be installed by authorized employees (see appendix B.2.9).

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.2.10).

6.3.2 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).

6.4 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.

6.5 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.

7 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).

8 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.2.11), 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.2.12).

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.2.13).

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.

II 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://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk

A.2 Attachments

A.2.1 Feedback form

The feedback form for suggestions for improving the Information Security Regulations can be downloaded from the Group's Information Security website https://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk.

Please send the completed form to: VWAG R: WOB, IT Security Regulations <itsr@volkswagen.de>.

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: September 2023

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

B Company-specific characteristics

B.1 Group-wide valid

This chapter lists characteristics that apply to the entire Group. These specific characteristics must not be changed.

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:
https://iserve.vw.vwg/vw/catalog_item_detail.do?sysparm_document_key=sc_cat_item,7f89128a50e61600ac0ade4eccc3502f

B.2 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.2.1 *Programmable logic controllers (PLCs) and robot controllers must be operated in networks where only the communication required for operation is permitted.*

B.2.2 Published on the intranet:
https://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk+-+Politik

B.2.3 For Volkswagen Brand documented in ORL 18

B.2.4 *Further information can be found in the Self Service Portal of Group Security K-SK-3:*
https://volkswagen-net.de/wikis/display/Konzernsicherheit/Selfservice-Portal

B.2.5 IT systems are complete IT systems with hardware and software components, including their two-way communication relationships.

B.2.6 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.2.7 Responsibility: Group Information Security Organisation, e-mail: ITSG@volkswagen.de

B.2.8 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.2.9 Responsibility : IT system administrators and local administrators

B.2.10 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.2.11 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.2.12 Responsibility: Legal department

B.2.13 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.2.14 for instance, the application „Blancco“

B.2.15 Passwords for administrative accounts must be securely managed (e.g. password vault, rotation, CyperArc)

B.2.16 Allowed only in emergency situations and in collaboration with the work council and ”Kommission Datenschutz.

B.2.17 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.2.18 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"

VOLKSWAGEN

AKTIENGESELLSCHAFT

Information Security

Guidelines

– Guideline for IT System Developers –

Publisher

Group Information Security

Regulation No.

02.04

Status

Published

Version

4.1

Classification

Internal

Date

November 03, 2022

Scope

This guideline applies to Volkswagen AG (organizational units (OU) on Group level and on brand level of the Volkswagen Passenger Cars brand, the Volkswagen Commercial Vehicles brand and Volkswagen Group Components brand). All IT system developers (according to definition in A.4) must adhere and comply with this guideline.

With regard to the implementation of the Information Security Regulations at other Volkswagen Group companies, ORL 1 "Organizational Regulations of Volkswagen AG" applies.

Table of Contents

I Purpose

This information security guideline defines the organizational guidelines and rules for information security that must be followed by IT system developers in their area of responsibility for IT systems and IT infrastructure.

In addition, the Information Security Guideline for employees or third parties applies to the target group of IT system developers, provided that the IT system developer is an employee of a partner company. IT system developers (see appendix A.4) must obtain information about all (role-specific) requirements and comply with them when working in additional roles.

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.2.1).

1 Context

The following overview shows how the Information Security Guidelines fit into the Information Security Regulations Framework.

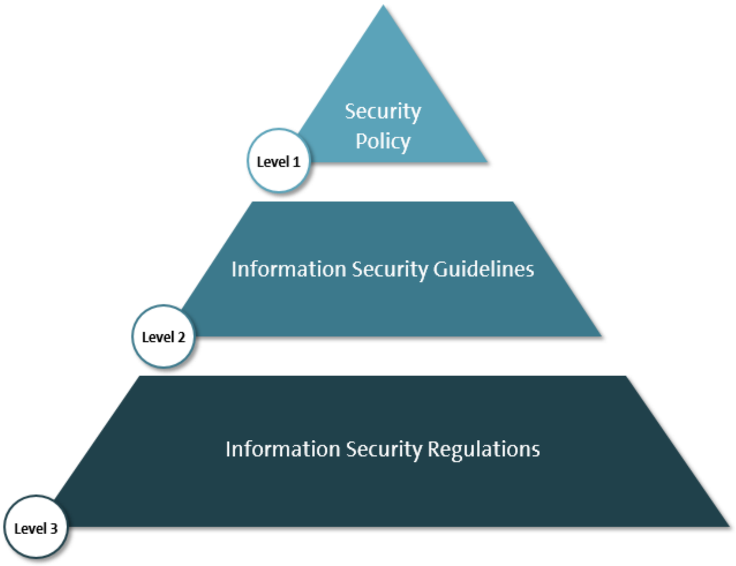

Security Policy
Level 1
Information Security Guidelines
Level 2
Information Security Regulations
Level 3

Illustration 1: Information Security Regulations Framework

Level 1 Information Security Policy:
Defines the basic objectives, strategies and responsibilities to ensure a minimum level of information security and is documented in Group Policy 18 and the derived brand characteristics (see appendix B.2.2).

Level 2 Information Security Guidelines:
Design of information security policy into organizational instructions for individual user groups

Level 3 Information Security Regulations:
Specification of regulatory requirements in the technical environment and description of technical functions and processes of information security

2 Asset management

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

3 Communications and operations management

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.2.5). In doing so, the requirements of Regulation No. 03.01.16 Third party service delivery management must be followed.

The capacity requirements for an IT system must be specified during the planning phase.

The protection requirements for an IT system must also be specified in the planning phase together with the information owners.

IT system planning (functional specification, IT system design, IT system implementation) and IT system acceptance (IT system introduction) must be carried out in accordance with the Group-wide standards for IT system development (e.g. IT PEP).

Information provided via publicly accessible IT systems (e.g. via the Internet) must be protected against unauthorized access and changes by appropriate security measures (e.g. encrypted transmission of authentication information, integrity checks).

4 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.

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).

Authentication requirements shall be implemented in accordance with the regulations (see appendix A.1.2). All authentication information (e.g. passwords or keys) must be classified as at least "confidential" and treated accordingly.

Authentication information must be protected from unauthorized access. Passwords must never be stored in plain text.

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

When communicating with or between IT systems that are classified as confidential or secret, mutual (bidirectional) authentication (e.g. TLS) must be used.

The processing of information must be determined jointly with the information owner. This expressly includes any use in IT systems or transfers between IT systems. The approval by the information owner must be documented.

5 Procurement, development and maintenance of IT systems

5.1 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).

For IT systems (e.g. databases and backup media), the requirements for handling information also apply (see Information Security Guideline for Employees, section "Handling classified information").

5.1.1 Confidentiality

Information must be protected against unauthorized 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

5.1.2 Integrity

Information shall be protected against undesirable changes and unauthorized 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)

5.1.3 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.

5.2 Processing in applications

The security of IT systems must be ensured by implementing the measures from the Group-wide standards for IT system development (e.g. IT PEP).

For all consulting activities for the introduction of IT systems, the regulations and internal agreements of the respective Group company apply (see appendix B.2.3).

5.3 Cryptographic measures

Basic decisions on the strategy, use and handling of cryptographic methods must be determined by the responsible organizational units (see appendix B.2.4).

The requirements of the regulation on cryptography (see appendix A.1.3) must be followed. Only the methods/procedures specified therein may be used.

5.4 Security of IT system files

5.4.1 Protection of IT system test data

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

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.

After testing has been carried out, information used for this purpose must be completely deleted from productive IT systems.

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 B.2.6) of the department.

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.

5.4.2 Access control to source code

Source code must be classified according to the data classification (see chapter 5.1) and protected accordingly.

5.5 Security in development and support processes

All procedures and processes that affect IT systems must be designed to achieve and maintain the desired information security level.

Formal change management procedures must be implemented. These must ensure that the IT system's security and monitoring procedures are not compromised by modifications.

If changes are made to software packages or their source code, their effects on existing regulations and security measures must be determined.

6 Compliance and compliance with legal obligations

When using encryption and/or electronic signatures, all country-specific regulations for the import and export of or access to hardware, software and information must be followed.

The license and usage rights of third parties in accordance with the applicable provisions (including contract law) must be observed and complied with during system development.

II 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. 03.01.09 Exception process

A.1.2 Information Security Regulation No. 03.01.05 IAM

A.1.3 Information Security Regulation No. 03.01.02 Cryptography

The relevant documents can be found on the Group Information Security website:
https://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk

A.2 Attachments

A.2.1 Feedback form

The feedback form for suggestions for improving the Information Security Regulations can be downloaded from the Group's Information Security website https://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk.

Please send the completed form to: VWAG R: WOB, IT Security Regulations <itsr@volkswagen.de>.

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: September 2023

A.4 Abbreviations and definitions

Abbreviation/term	**Explanation**
IT system developer	all persons involved in the definition, design, development and implementation of an IT system These are typically the following roles: • IT system planer • IT system architect • Software architect • System developer • Software developer • Application developer • Programmer • Tester

A.5 Document history

Version	Name	Org. unit	Date	Comment
1.0	K-SIS/G1	K-SIS/G1	May 24, 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 Review: 2.4.2019
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 5.4.1

B Company-specific characteristics

B.1 Group-wide valid

This chapter lists characteristics that apply to the entire Group. These specific characteristics must not be changed.

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.1.1) must be observed.

Contact for Volkswagen AG via My.Serve:
https://iserve.vw.vwg/vw/catalog_item_detail.do?sysparm_document_key=sc_cat_item,7f89128a50e61600ac0ade4eccc3502f

B.2 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.2.1 Published in Group Wiki:
https://volkswagen-net.de/wikis/display/Security/Informationssicherheitsregelwerk+-+Politik

B.2.2 For Volkswagen Brand documented in ORL 18

B.2.3 The application software used must be discussed with the works council as per BV 2/80 "Briefing and consultation concerning system projects for information processing."

B.2.4 Responsibilities: Group's Information Security Organization, IT Projects, Architectures & Standards

B.2.5 Responsibilities: Group's Information Security Organization

B.2.6 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"

VOLKSWAGEN

AKTIENGESELLSCHAFT

Information Security

Guidelines
- Guideline for Third Parties -

Editor

Group Information Security

Regulation No.

02.06

Status

published

Version

5.0

Classification

Internal

Date

22.09.2022

Scope

These instructions apply to all third parties who process sensitive information for the Volkswagen Group in accordance with contractual agreements.

Table of Contents

I Purpose and definitions

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.

I.I Document structure and target group

This guideline is aimed at the management of third parties. The management of the third parties must ensure that their employees and their vicarious agents/vicarious agents are bound to this information security guideline.

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 access to Volkswagen information outside the Volkswagen Group infrastructure.
4	Third parties who provide Volkswagen with information outside the Volkswagen infrastructure.

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

1 General requirements for all third parties

1.1 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 can be marked with an expiration date.

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.

1.2 Handling with classified information

Information may only be made available to an authorised 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 confidential or secret information, the corresponding IT devices must be set up in such a way that access by unauthorized persons is prevented and the risk of inspection by unauthorized third parties is minimized.

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: proper disposal

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: proper disposal - 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: proper disposal • 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.

1.3 Further requirements

- Information security events (e.g. malfunctions that occur, violations of the information security regulations) concerning information or IT systems of the client must be reported immediately to the competent authority (see Annex A.3.1).
- 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 A.3.1).
- If there is a suspicion of loss of confidential or secret information of the customer, this must be reported immediately to the Volkswagen Group contact person.
- The transfer of data or information to other third parties is only permitted with written approval by the information owner.
- 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 securely deleted there. Storage media that are no longer needed must be disposed of in a safe manner.
- 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.

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

2.1 Definition

A third party works in the Volkswagen Group Infrastructure if:

- clients (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.

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

2.2 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 on a case-by-case basis with the responsible Volkswagen Group contact person. Exceptions for the purpose of accessing the corporate network, remote access or for 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 Volkswagen Group contact person.
- 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 service provider 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 Volkswagen Group contact person.
- 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 in the context of official activities. A transfer of this data to unauthorized third parties 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.

2.3 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 Volkswagen Group contact persons 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 means that are no longer required must be returned immediately to the responsible Volkswagen Group contact person.
- 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.

  Note: For a secure password, you can use donkey bridges or abbreviations as well as falsifications (example: "Every day I go to the bathroom and wash myself thoroughly with a washcloth!" becomes the password "JTg11B&wmgmeW!"). The example given here must not be used as an actual password.

2.4 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.

2.5 Additional requirements for mobile work

The user is responsible for ensuring that the affected regulations on data and information security as well as data protection during mobile work are fully complied with. Working documents, data and information must not be visible and accessible to third parties in public places or in private rooms.

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.

3 Additional requirements for third parties who have access to Volkswagen Group information outside the Volkswagen Group infrastructure

3.1 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.

3.2 Requirements

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

4 Additional requirements for third parties who provide information of the Volkswagen Group outside the Volkswagen Group infrastructure

4.1 Definition

A third party then provides information of the Volkswagen Group outside the Volkswagen Group infrastructure if this Volkswagen Group provides information in its own IT infrastructure for the Volkswagen Group or other third parties on behalf of the Volkswagen Group.

4.2 Requirements

The requirements of the Information Security Action Guideline No. 02.03 for system operators and administrators must be complied with (see A.3.2).

II Responsibilities

Violations of the guidelines for action will be examined individually in accordance with valid legal and contractual provisions and punished accordingly.

Deviations from these guidelines for action that impair the level of safety are only permitted for a limited period of time and after consultation with the contact person of the Volkswagen Group company.

A General

A.1 Validity

This Information Security Policy shall enter into force at the time of publication. Updated content of this scheme shall be implemented within a transitional period of six months.

Next review date: September 2023

A.2 Document history

Version	Name	Department	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

A.3 Company-specific characteristics

A.3.1 CERT VW - via Enterprise Help Desk (EHD, Tel. +49 531 9 33000, <EHD@volkswagen.de>)

A.3.2 Information security and IT security requirements (volkswagen.de)

VOLKSWAGEN
AKTIENGESELLSCHAFT

Information Security

Global Regulations and Processes
- Third Party Service Delivery Management -

Publisher

Group Information Security

Regulation No.

03.01.16

Status

published

Version

3.0

Classification

Internal

Creation date

September 29, 2022

Publication date

October 06, 2022

Scope

These instructions apply to Volkswagen AG (Group departments, the brand divisions of Volkswagen Passenger Cars, Volkswagen Commercial Vehicles and Volkswagen Group Components).

ORL 1 “Volkswagen AG Organizational Regulations” applies with regard to the implementation of these instructions in the other Group companies.

Table of Contents

I Purpose

In the Volkswagen Group, third parties are engaged for activities that involve IT services in whole or in part, such as outtasking (e.g., external consulting) or outsourcing projects (e.g., external hosting). To provide comprehensive protection for information, external service providers must also comply with security regulations and legal requirements. This regulation defines specific information security requirements and processes for all phases of outtasking and outsourcing projects.

1 Service Provision by Third Parties

1.1 Objective

This regulation defines security requirements that must be implemented when working with external service providers (third parties) in order to ensure that the information security level within the Group is not reduced. The requirements of this regulation apply for all kinds of service provision and contractors.

Before awarding the contract for the services to an external service provider, a process must ensure an adequate level of security and the adherence to internal regulations.

It must be ensured that the interests of information security, data protection and group security are adequately observed. The interests of data protection and Group security must be ensured regardless of this regulation by the appropriate policies of these stakeholders. Common Requirements Concerning Outtasking and Outsourcing

1.2 Common requirements for outtasking and outsourcing

1.2.1 General Requirements

- The unit responsible for contracting services as defined in this regulation shall ensure that processes for compliance within the requirements of this regulation are coordinated with, established, and implemented by Information Security.
- The following requirements must be addressed in these processes.
  - A procedure (with roles and responsibilities) for commissioning an outtasking or outsourcing project (referred to below in general terms as "a project"[1]) must be defined, documented, and established.
  - For security-critical projects (projects with access to confidential, secret data or data with very high availability or integrity requirements), the service provider must define, document and establish a procedure that allows the service provider to verify the trustworthiness of the employees it will employ (e.g., assurance of police clearance certificates or assurance of trustworthiness by the service provider as part of the contract).
  - The data owner must be involved in the decision on outtasking/outsourcing projects.
  - It must be regularly checked if the project relevant[2] information security requirements are followed by the contracted third parties. A procedure[3] must be developed for this purpose.

[1] A project ends when the contract expires, is cancelled and all migration steps are finished.

[2] See Chapter 1.2.2

  - Organizational and technical changes regarding information security within the Group company that are relevant to third parties (e.g., version changes to systems, changes to regulations) must be reported to the third parties concerned.
  - Third parties must be requested to report all changes relevant to information security for the contracted service to the ordering party.

- When personal data is handled by third parties, the responsible Group Company must ensure that local legal and company specific requirements are met.
- The third party must ensure that required technical and organizational security measures are implemented for handling personal data in compliance with applicable regulations[4].
- Additional requirements of the Group Security Department must be observed[5].

1.2.2 Managing External Service Providers in Project Management

- For every outtasking and outsourcing project, the Group Company must define persons[6] who are responsible for the compliance with information security requirements in the phases “Planning and Design”, “Detailed Planning”, “Migration”, “Operation” and “Completion" of the project.
- Any information security requirement that the service provider has to fulfill within the project must be defined and documented (e.g. relevant security regulations and project specific requirements).
- Every subcontractor with relevance to the project must be approved by the respective Group Company and the data owner upon request.
- The documented information security requirements also apply to subcontractors of the service provider.
- A group methodology should be chosen that ensures standardized vendor management[7].

1.2.3 Selecting Service Providers

- Only service providers that can ensure compliance with information security requirements for the entire lifetime of the contract must be chosen.
- A standardized process for the selection of service providers in compliance with security regulations must be implemented[8].
- If personal data is processed only service providers that fulfill data protection requirements may be selected.
- The trustworthiness of the employees of the service provider must be ensured using the defined procedure[9] before contracts for security-critical projects can be signed.
- Additional requirements apply for external hosting[10].

1.2.4 Concluding the Contract

Contracts with service providers must at least include the following:

- All project-related information security requirements that apply to the service provider.

[3] E. g. as part of the project management process
[4] See Appendix B.2.1.2
[5] See Appendix A.1.7
[6] E. g. project manager
[7] E. g. Leistungsbaukasten
[8] See Appendix B.2.1.3
[9] See chapter 1.2.1
[10] See Chapter 1.4

- Implemented security measures of the service providers that are relevant for the contract[11].
- Requirements concerning the type and method of information exchange between the parties of the contract
- Ownership and usage rights of the information which, as part of the project, are
    - provided to the service provider
    - created by the service provider or
    - outsourced to the service provider.
- The duties of the service provider to cooperate and to exercise due care, which must cover the following aspects as a minimum:
    - Confidentiality (NDA[12])
    - Compliance with the laws that apply to the project (e.g. Federal Data Protection Law)
    - Compliance with all relevant requirements of the Corporate IT Security Regulations
    - Assurance that the external project staff is trustworthy
    - Assurance that the external project staff has received sufficient training on information security risks relevant for their duties.
- Requirement that the service provider must send reports in regular intervals to the named responsible person of the Group Company about incidents, changes, risks and service interruptions. Additionally, the service provider must inform this person about major incidents and security vulnerabilities directly depending on the criticality of the incident/vulnerabilities.
- Obligations in the case of ordinary or extraordinary termination of contract, which must cover the following aspects as a minimum:
    - Full transfer of all results, information and tools required to continue the project (e.g. documentation or descriptions of procedures) or being relevant to the Volkswagen Group within a defined period.
    - Return of hardware and software belonging to the Volkswagen Group
    - Secure deletion of passwords and user IDs that allow access to the IT of the Volkswagen Group from the external service provider's systems
    - Return of assets (especially tokens, admission cards, keys, ...)
    - Secure deletion of all project-related data sets at the service provider's premises[13] after confirmation by the ordering party
- Obligations concerning the commissioning of subcontractors, which must cover the following aspects as a minimum:
    - Obtaining approval for the use of named subcontractors for defined tasks by the respective Group company, but at least reporting these subcontractors on request
    - A statement of the subcontractor to comply with all those requirements that the direct contractor must also comply with.
    - Rules concerning liability and breach of contract

[11] According to Appendix A.1.7 ORL13

[12] Non-disclosure Agreements

[13] See Appendix A.1.2 Information Security Guidelines No. 02.02 for Employees

- Rights and permissions to conduct audits at the service provider. The service provider must also ensure permission to audit subcontractors.
- Return of assets when contract ends.
- Additional requirements of the Group Security Department must be observed[14]
- Applicable company specific requirements must be observed.
- For external hosting, additional requirements apply[15].

1.2.5 Operation within the Duration of the Contract

- During operation, all contractual requirements[16] must be observed.
- Both parties must name a contact person responsible for the project.
- The responsible person of the Group Company will function as a contact person between the contract partner and the local responsible for information security.
- The person responsible at the Group Company must verify that the employees of the service provider are familiar with and conform with the relevant information security requirements and the contractual requirements.

1.2.6 Ending the Project

- When the project ends, the requirements from the contract[17] concerning end of project must be satisfied. In addition, all access rights (both physical and electronic) must be revoked with immediate effect[18] as far as the legally required traceability is not limited.

1.3 Additional Requirements for Outsourcing

1.3.1 Planning and Design

- The unit responsible for information security[19] (or IT security) must be involved no later than the planning and design stage of an outsourcing project. This also applies to other relevant departments/roles (e. g. Data Protection Officers, corporate group security).
- A risk analysis[20] for the outsourcing project must be carried out. All information, services and IT components directly affected by the outsourcing project must be included in the risk analysis. The outsourcing object must be precisely defined.

1.3.2 Concluding the Contract

- The contractual agreements must include test criteria to check the implementation of information security requirements.
- The company responsible for the outsourcing object must be allowed to perform regular checks concerning the compliance with the information security regulations within the outsourcing project.
- These checks can be outtasked to a third party provider.

[14] See Appendix A.1.7
[15] See Chapter 1.4
[16] See chapter 1.2.4
[17] See chapter 1.2.4
[18] See Appendix A.1.3 Information Security Regulation No. 03.01.05 Access and Identity Management
[19] See Appendix B.2.1.1
[20] See Appendix A.1.4 Information Security Regulation No. 03.01.15 Information Security Risk Management

1.3.3 Detail Planning

- The service provider must define a contact person and deputy for all aspects of information security and data protection.
- The responsible company and the service provider must draw up a security concept for the outsourcing project based on the determined security requirements. The following aspects must be at least considered in the security concept:
  - Interfaces between the company and service providers
  - Measures for all of the following phases of the outsourcing project that are required to comply with the security requirements
  - Tests with which the implementation and effectiveness of the defined measures can be checked, both during and following migration
  - The service provider’s security concept must also provide an interface to the company's
    - Incident Management
    - Change Management
    - Information Security Risk Management or IT Risk Management
    - IT Service Continuity Management
- During the detailed planning, a migration plan with roles and responsibilities must be defined and documented covering the entire implementation of security concepts.

1.3.4 Migration

- Measures must be implemented in accordance with the defined migration plan.
- The approval for implementation may only be granted after the successful completion of the tests defined in the security concepts.

1.3.5 Operation

- Information on the status of information security (e.g. updated regulations, updated requirements etc.) must be regularly exchanged between the person responsible for the project and the service provider. The person responsible of the Group company must initiate the adaptation of the contract if required by changes in information security or legal requirements.
- Changes to the outsourcing object must go through the same process as a new outsourcing procedure before implementation, in order to make the necessary adjustments to the already completed steps of the outsourcing procedure there.
- The provider must report on the implementation status regularly.
- The service provider cooperates actively on investigating security incidents and makes relevant information available.
- The service provider shall actively cooperate on investigating security incidents and provide relevant information without any culpable delay.
- The service provider must document all of the activities it carries out, e. g. system maintenance according to the risk for information security.
- The security concept and defined contractual services related to information security must be checked for completeness and timeliness at least once a year. The responsible person for the project and the service provider are responsible for the execution of adequate measures..

- The service provider monitors the effectiveness of the security measures it has implemented and proposes measures for keeping the security level or improving it, if necessary.

1.3.6 Ending the Outsourcing Project

- The transfer of the outsourcing object to another service provider must be treated as if it was a new outsourcing project.
- Should the outsourcing project be ended (insourcing), the requirements from the "Detail Planning" phase and the "Migration" phases must be satisfied.
- When renewing the contract, it must be checked if information security and legal regulations are still valid as agreed, if not, the contract and the technical and organizational security measures must be adapted accordingly.

1.4 Additional Requirements for External Hosting

The following conditions apply to external data hosting including cloud services:

- Generally speaking, compliance with the IT security regulations of the Volkswagen Group must be ensured, particularly with regard to access protection, authentication required by the regulations, and the design of physical security. In case of external hosting, encryption of the storage medium must be used in addition to the IT security regulations of the Group[21].
- For cloud computing applications and infrastructure components must be provided as described in the definition of Cloud Computing[22]. Company specific regulations for Cloud Computing in relation to personal data must be observed[23].
- The Group Company must be given the option to carry out an on-site audit of the environment at least with regard to auditing by an independent third party in accordance with international IT security standards. This is also valid for subcontractors.
- The process defined by the unit responsible for information security of the brand in question for remote audits or on-site audits must be followed. The process description must be made available by the unit responsible for information security of the brand affected (e.g., in a wiki). If an audit reveals a deficient maturity level, the resulting risk must be dealt with in accordance with the Group risk management process by the specialist responsible for the brand in question. The unit responsible for information security of the brand concerned reserves the right to veto the risk that has been set
- The security level of the Provider shall be proven by him through appropriate ISMS certifications prior to providing the service and regularly during this process. These certifications are carried out at the expense of the provider. Depending on the required IT security level, different certifications may be required. This is determined by the unit responsible for information security[24].
- The unit responsible for information security shall be provided with documentation of the planned infrastructure coordinated with the unit responsible for IT and application architecture[25].

[21] A.1.5 Information Security Regulation No. 03.01.02 Cryptography
[22] See Appendix A.1.6
[23] See Appendix B.2.1.5
[24] See Appendix A.1.7
[25] See Appendix B.2.1.4

- An external hosting project must be approved by the data owner, the responsible unit for information security and, if necessary, Data Protection, the Works Council and the Legal Department of the companies concerned.
- For network connections the requirements of the regulation network access[26] must be observed.
- As part of the contract, an application security audit must be performed by an independent third party. the findings identified must be commensurate with the need for protection. (i.e. penetration test according to OWASP ASVS or FedRAMP or another internationally recognized standard).
- External hosting of secret data is only permitted:
  - Annual individual case assessment by the unit responsible for information security
  - Acceptance by the data owner (TMK)
  - Inclusion in Risk Management

[26] See Appendix A.1.9 Information Security Regulation No. 03.02.04 Network Access

II Responsibilities

This regulation is to be used and followed by all units which work together with external service providers.

Appendix

A General

A.1 Other Applicable Documents

A.1.1 Information Security Regulation No. 03.01.09 Exception Process

A.1.2 Information Security Guidelines No. 02.02 for Employees

A.1.3 Information Security Regulation No. 03.01.05 Access and Identity Management

A.1.4 Information Security Regulation No. 03.01.15 Information Security Risk Management

A.1.5 Information Security Regulation No. 03.01.02 Cryptography

A.1.6 Definition Cloud Computing: see Attachment in Intranet (Security Regulations > 03.01.16 Third party service delivery management > Regulation No 03 01 16 Third Party Service Delivery Management_Appendix Cloud Computing.xlsx)

A.1.7 ORL 13 Security at Volkswagen AG

A.1.8 ORGA 27 Application for accepting an external company

A.1.9 Information Security Regulation No. 03.02.04 Network Access

A.2 References to Standards

The following table illustrates references to ISO/IEC 27001:13, ISO/IEC 27001:2005 and VDA (2014).

Topic	Chapter	ISO 27001:2013	ISO 27001:2005	VDA
Monitoring and review of supplier services	0, 1.3	A.15.2.1	A.10.2.2	15.2
Managing changes to supplier services	0, 1.3	A.15.2.2	A.10.2.3	-

A.3 Attachments

A.3.1 Attachment 1 Feedback Form

The feedback form for suggestions concerning regulations can be downloaded from the Information Security Regulations - Informationssicherheit - Group Wiki (volkswagen.com) website.

Please send the completed form to: VWAG R: WOB, IT Security Regulations itsr@volkswagen.de .

A.4 Abbreviations and Definitions

Term	Definition
CISO	Chief Information Security Officer
Outsourcing	Outsourcing involves transferring all or part of an organization's work or business processes to external service providers.. Outsourcing can affect services as well as the use and operation of hardware and software.
Outtasking	Unlike outsourcing, outtasking involves individual tasks being performed by an external service provider. However, Volkswagen remains in control of the process. Such tasks include external consulting, help with software development, operational support, etc.

A.5 Validity

This IT security regulation is valid immediately with the publication. For new companies, the content of this regulation must be implemented within a transitional period of six months.

Next inspection date: 06.10.2023

Please use the specified form to report any requests for changes[27].

[27] See Appendix A.3.1 Attachment 1 Feedback Form

A.6 Document History

Version	Name	Org. Unit	Date	Comment
1.0	ISSO	K-SIS/G1	06.02.2015	GISSC approved version
2.0	K-FIS	K-FIS/G	07.11.2018	Update for secret data
2.1	K-FIS	K-FIS/G	28.09.2021	Addition inserted after fourth bullet point in chapter 1.4
3.0	Alpers, Mareike Barbric, Mirko Bickel, Holger, Dr.	K-DAI/P K-DS/P K-DS/P	27.09.2022	Content and editorial review

B Specific Characteristics

B.1 Group wide

This chapter contains specific characteristics which are valid for the entire group. These specific characteristics must not be changed.

B.1.1 Chapter 1: Service Provision by Third Parties

-

B.2 Company specific

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

B.2.1 Chapter 1: Service Provision by Third Parties

B.2.1.1 K-GR-5 and K-FIS can be consulted

B.2.1.2 ORL 50 Schutz Personenbezogener Daten, BDSG

B.2.1.3 Standardized process for the selection of service providers: „Vergabe von Konzern-IT-Support Dienstleistungen an Dritte für Systeme mit schützenswerten Daten“ (Contracting Group IT Support Services to third parties for systems with sensitive data)

B.2.1.4 Responsible unit for information security K-DS/G

B.2.1.5 Storage or processing of personal data in cloud computing applications and infrastructure components is only permitted in accordance to the EU data protection directive and all data protection laws of the respective countries]

VOLKSWAGEN

AKTIENGESELLSCHAFT

Information Security

Global Regulations and Processes
- Cloud Security -

Publisher

Group Information Security

Regulation No.

03.01.17

Status

Published

Version

3.4

Classification

Internal

Creation date

September 27, 2022

Publication date

September 29, 2022

Scope

These instructions apply to Volkswagen AG (Group departments, the brand divisions of Volkswagen Passenger Cars, Volkswagen Commercial Vehicles and Volkswagen Group Components).

ORL 1 “Volkswagen AG Organizational Regulations” applies with regard to the implementation of these instructions in the other Group companies.

Table of Contents

I Purpose

This Security Guideline is aiming to provide an overview on relevant security requirements, processes and frameworks for all Group IT Cloud (GITC)[1] platforms and its relevant services. These regulations are mandatory and must be observed by all persons dealing with cloud topics, especially:

- Account Owners responsible and accountable for a GITC account (e.g. subscription, tenant, ...)
- Platform Owners responsible for GITC platforms (PaaS)
- Service Owners providing GITC cloud services for the Volkswagen Group
- Service Owners providing cloud services for the Volkswagen Group
- External Service Providers working on GITC cloud platform or services for the Volkswagen Group (SaaS)
- Application Owners migrating to / deploying on GITC platforms for the Volkswagen Group.

[1] GITC includes private and public clouds used in the Volkswagen Group.

1 General Requirements

If not explicitly specified for GITC, security requirements and regulations from the Group IT Security Policy Framework apply. Especially the following guidelines and regulations provide guidance on how to deal with Information Security:

- Regulation No. 02-03: IS Guidelines for System Operators and Admins
- Regulation No. 02-04: IS Guidelines for System Developers
- Regulation No. 03-01-16: Third Party Service Delivery Management
- Group IT Architecture Guiding Principles Frame - Policy

In addition, requirements in regard to data retention according to "Classification System for Documents (CSD)" / "Klassifizierungssystematik für Unterlagen (KSU)" apply as defined in ORL 24.

1.1 Terms of Use

Services developed and provided on Cloud environments must be in line with general "Cloud Terms of Use" documented in the company repository.

1.2 Approval of Cloud Services

Available and approved Cloud Services and corresponding Service Usage Rules are documented in the company Cloud Service Portfolio:

- All services must be used in the manner described in the respective Service Profile page.
- All services must be documented in the Cloud Service Portfolio.
- All services must be approved by responsible of IT Security department via a documented approval before usage.

1.3 Service Hardening

All concepts and configurations must be in line with CIS benchmarks, CIS Settings and hardened accordingly.

1.4 Confidentiality and Commitment of GITC Cloud Services

The following confidentiality rules are binding.

The classification for the use of available GITC Services is mandatory according the cloud type and service model. The protection goal regarding the confidentiality depending on the cloud type can be found in attachment A1.16 to Information Security Regulation No. 03.01.16: Third Party Service Delivery Management.

2 GITC Onboarding

2.1 Initial Supplier Onboarding

For any service, an operating concept, a support process and a service owner (management responsibility) must be defined.

Contracts with external service providers (IaaS, PaaS, SaaS) relevant for GITC must be in accordance with available standard purchasing processes.[2]

The following requirements must be considered:

- in general:
  - Contracts for software, licenses or any additional services must be managed according to IT-PEP
  - Open Source Services have to be compliant, and especially checked for possible license violations
  - Non-disclosure agreements[3]
  - Data Processing Agreement (DPA)[4] as required by GDPR (It is not allowed to process any personal related data in cloud environments without data protection contracts)
- for external Suppliers
  - IT Security Regulation No. 02-06: IS Guidelines for Suppliers who are using Volkswagen Infrastructure is mandatory
  - TISAX certification for external suppliers who are accessing Volkswagen data is mandatory[5]
  - A Cloud Vendor Assessment (CVA) is mandatory for cloud providers (PaaS, SaaS)
  - Onboarding of all service provider employees working with Volkswagen Infrastructure (Volkswagen clients, Volkswagen Server) or have access to Volkswagen network (on-premises, externally hosted or cloud) must be managed via ONE.Konzern Business Plattform (ONE.KBP) and according the B2B-Identity Process.[6]

These processes ensure that mandatory security requirements are considered in contracts with external parties.[7]

2.2 Project Onboarding

To ensure a secure onboarding on existing platforms the specific platform requirements for onboarding have to be followed. The Secure Cloud Onboarding process is also part of IT-PEP.[8]

The secure onboarding of users has to be compliant with the IAM requirements (e.g. Information Security Regulation No. 03.01.05 Authentication and IAM).

As part of the project onboarding an IT security assessment has to be executed.

[2] Company purchasing processes and requirements have to be considered.
[3] ORL 13 Security at Volkswagen Aktiengesellschaft. For the Volkswagen Group refer also KRL 13 Appendix 2.
[4] German: AVV "Auftragsverarbeitungsvertrag".
[5] ORL 13 Security at Volkswagen Aktiengesellschaft. For the Volkswagen Group refer also KRL 13 Appendix 2.
[6] The B2B-Identity Process is not used by all brands. In this case a corresponding process applies.
[7] Company purchasing processes and requirements have to be considered.
[8] Further information on the secure onboarding can be found in the https://group-wiki.wob.vw.vwg/wikis/display/CLOUD

In general, for any migrations or deployments of applications to GITC, milestones with mandatory deliverables and approvals according to the IT-PEP process apply. In addition, it is mandatory for each project to create at least one technical risk entry for the project itself in the company risk management solution.[9]

[9] e.g. IRMA or corresponding Risk Management System (RKS/IKS) required by each brand or company.

3 GITC Service Design & Implementation

3.1 Development Methodology

GITC Service Development and Deployment must follow the IT-PEP process.

3.2 Secure Software Development

Security requirements as defined in IS Guideline 02.04 "Information Security Guidelines for System Developers" and Regulation 03.04.02 – Provisioning of secure Applications as part of the Group IT Security Policy Framework R6 apply.

For development and testing of applications the following criteria have to be taken into account and developers have to be aware of the following contents:

- OWASP Application Security Verification Standard (ASVS), Level 2 (or higher)
  https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
- OWASP Top 10
  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

It is expected that an equivalent procedure is followed by vendors of off-the-shelf software.

Note: Any secrets and special credentials have to be handled in secure manner. For example, it has to be ensured that passwords used by technical users in DevOps workflows are not stored in plain text.[10]

Part of the cloud software development is a secure build and deployment process.

> As an example a Continuous Integration/Continuous Delivery (CI/CD) pipeline shall be used to automate builds, tests, (security) scans and the deployment to different environments.

Application Owners of GITC services are responsible for source code reviews, including the used open source artefacts.

Security source code analysis with automated inspection and evaluation of the findings has to be carried out before the code (binary) is deployed according to the IT PEP process and the above mentioned regulation. Findings have to be fixed and included in the risk management with defined measures and timeline.

Penetration tests (manual and automated inspection) of the systems include network and application testing. The tests shall be carried out by an independent third party or organizational unit before the service is provided and regularly thereafter as stipulated in the IT PEP process. Detected vulnerabilities have to be fixed and included in the risk management. Measures and timeline shall be defined.

Cloud Penetration tests have to be in line with laws and regulations by cloud providers.

[10] see also the password policy (A01.070).

3.3 Images and Repositories

Centrally provided images and repositories for GITC (e.g. OS Image Factory) shall be used according to the corresponding group / brand procedures.[11]

3.4 Resource Tagging

All resources created in GITC must be tagged according to the GITC Tagging Policy.

The tags are used to assign metadata to the cloud resources.

3.5 Information Security Risk Analysis

Before any GITC Service can be deployed, there must be a dedicated and documented asset and risk assessment. As part of the ISMS all relevant risks must be documented. This includes for example:

- relevant threat scenarios
- impact of threats

3.6 Network Communication

All allowed communications are documented in a communication matrix, which in turn has to be approved by a CISO responsible.

The communication approved in the matrix has to be enforced by the use of a host-based Firewall.[12]

For details on restrictions and communication patterns refer to the A.1.18 Group IT Architecture - Secure Environments Architecture - Policy

3.7 Network Auditing

The network auditing must be conducted regularly in accordance with the communication matrix. A responsible person for network auditing must exist. The auditing must not be done by the projects itself.

[11] Centrally means images per foundation provided either for the group or by a brand.

[12] This can be achieved either via a cloud / hypervisor based firewall (i.e. Security Groups, NACL) or a host-based firewall The use of the former is encouraged as they remove the possibility to switch of filtering from within the secured entity, and enable strict segregation of duties. The same network segregation has to be implemented for any kind of overlay, e.g. for containers.

4 GITC Monitoring

4.1 Compliance Monitoring

Configuration of GITC services must be in line with defined compliance rule sets (see chapter 1.4) and follow the exception regulation (Information Security Regulation No. 03.01.09 Exception Process) and the Information Security Regulation No. 03.01.04 Security Logging and Monitoring.

The Service Owner for GITC services must support remediation of identified deviations from compliance rule sets in a timely manner.

4.2 Security Monitoring

All critical GITC services on all layers (IaaS, PaaS, SaaS) have to be monitored and mandatory logs sources connected to a Security Incident and Event Management (SIEM) system. Applications have to be continuously monitored to quickly react to security incidents (see Information Security Regulation No. 03.01.18 Information Security Incident and Vulnerability Management).[13]

For each service critical security events and their impact have to be identified and included in the cloud security risk catalogue and monitored respectively by the Service Owner.

[13] Operational monitoring regarding the availability is not considered here.

5 Vulnerability Management

Vulnerability Management is mandatory for all GITC platforms. The objective of implementing scans in several cloud life cycle phases is to scan and report vulnerabilities to support the running of clean, secure and compliant:

- Images/Containers,
- Web-Applications,
- Accounts and Instances,
- Software and Source Code.

The simplified vulnerability management life cycle includes the following steps:

- Vulnerability Identification
- Assessment
- Reporting
- Remediation and Mitigation

5.1 Vulnerability Scans

Vulnerability Scans must be run on a regular basis, depending on the environment. The specific scanning requirements are defined in the Cloud Security Policies.

The following should be in the scope of vulnerability scans:

- Assets like containers & instances
- Web pages
- Registries
- Container images
- Network
- Software & source code

The visibility into the accounts is compulsory.

5.2 Vulnerability Remediation and/or Mitigation

Ensure active life cycle management and patching process (see below). The software products used must always be kept up to date. Vulnerabilities classified as security “critical” or “high” must be eliminated immediately (see Information Security Regulation No. 03.01.18 Information Security Incident and Vulnerability Management). If patching is not an option, make sure that mitigation factors are in place and ensure that these are documented in the risk management catalogue.

6 Patch Management

In the operations concept it has to be considered that a Life Cycle and Patch Management for all assets in the cloud is ensured. As part of the Life Cycle Management cleaning & cleansing measures shall be defined and followed regularly.

Patch Management describes the framework for patches of all assets, including OS, containers, instances, software, accounts etc. For the general definition of assets see regulation Information Security Regulation No. 03.01.13 Asset Management.

The regulation on Change and Patch Management applies and must be observed by all units responsible for operating of IT systems (see Information Security Regulation No. 03.01.08 Change and Patch Management). Deviations from this regulation reducing the security level are only temporarily acceptable after consultation with Group Information Security.

7 Backup and Recovery

The protection level for backed up data in cloud systems have to be aligned with IS standards and regulations.

As part of an operating concept for cloud services and applications, a backup and recovery process has to be defined. The account owner has to ensure that the necessary backup and recovery measures are taken and tested according the backup and recovery regulations (see Information Security Regulation no. 03.01.06 Backup and Archiving).

As part of the operation processes and the Business Continuity Management, a Disaster Recovery Plan (DRP)[14] has to be defined for every service that has been identified as critical in terms of availability.

[14] The DRP shall be tested if feasible.

Appendix

A General

A.1 Other Applicable Documents

A.1.1 Information Security Guidelines No. 02.02 for Employees

A.1.2 Information Security Guidelines No. 02.03 IS Guidelines for System Operators and Admins

A.1.3 Information Security Guidelines No. 02.04 IS Guidelines for System Developers

A.1.4 Information Security Guidelines No. 02.06 IS Guidelines for Suppliers

A.1.5 Information Security Regulation No. 03.01.04 Security Logging and Monitoring

A.1.6 Information Security Regulation No. 03.01.05 Authentication and IAM

A.1.7 Information Security Regulation no. 03.01.06 Backup and Archiving

A.1.8 Information Security Regulation No. 03.01.08 Change and Patch Management

A.1.9 Information Security Regulation No. 03.01.09 Exception Process

A.1.10 Information Security Regulation No. 03.01.13 Asset Management

A.1.11 Information Security Regulation No. 03.01.16 Third Party Service Delivery Management

A.1.12 Information Security Regulation No. 03.01.18 Information Security Incident and Vulnerability Management

A.1.13 Information Security Regulation No. 03.04.02 – Provisioning of secure Applications

A.1.14 Information Security Regulation - Business Process Manual for CIS Security Settings

A.1.15 Information Security Regulation - Glossary

A.1.16 Group Cloud Security Policies

A.1.17 Group IT Architecture Guiding Principles Frame - Policy

A.1.18 Group IT Architecture - Secure Environments Architecture - Policy

A.1.19 Platform Delivery Center (PDC)

A.1.20 Group IT Cloud Wiki in Group WIKI

A.1.21 Group Security (Konzernsicherheit)

A.2 Attachments

A.2.1 Attachment 1 Feedback Form

The feedback form for suggestions concerning regulations can be downloaded from the Information Security Regulations - Informationssicherheit - Group Wiki (volkswagen.com) website.

Please send the completed form to: VWAG R: WOB, IT Security Regulations itsr@volkswagen.de

A.3 Abbreviations and Definitions

See A.1.15 Information Security Glossary

A.4 Validity

This Information Security regulation is valid immediately with the publication.

Next inspection date: 29.09.2023

A.5 Document History

Version	Name	Org. Unit	Date	Comment
1.0	K-FIS	K-FIS/G	18.09.2019	Initial Version as developed by ODP/K-FIS-Team
2.0	K-FIS	K-FIS/G	07.01.2020	Scope definition and feedback from version 1
3.0	K-FIS, Audi	K-FIS/P, K-FIS-I, I/BT-C1	20.05.2020	Revised general edition for cloud security (provided by GISP2020)
3.3	VW, Audi	K-FIS/G, K-FIS-I, I/BT-C1	26.01.2021	Group-wide general edition of regulation for cloud security after Veto Process
3.4	K-DS/G	K-DS/G	27.09.2022	Editorial revision