Guideline on information security

GMH Group

Document history

Version	Action	Date	Name	Comment
0.1	New	01.08.2023	Anneke Knue	Initial version
0.2	Draft	18.10.2023	Thorsten Kurz	Revision
1.0	Release	08.12.2023	Mathias Hölscher, Dr. Deniz Özcan	Release
1.1	Revision	08.01.2024	Treubrodt / Grühn	Comparison with 1.1.1 Directive
1.2	Q-test	10.01.2024	Treubrodt team	Comparison with 1.1.1 Directive
1.3	Revision	16.01.2024	Anneke Knue	Section on GMH adapted
2.0	Release	23.01.2024	Mathias Hölscher, Dr. Deniz Özcan	Release

Document release

Role	Name	Department	Date
Authors	Knue	IT management	01.08.2023
Reviewer	Short	Quality management	18.10.2023
Authorizer	Hölscher, Özcan	CFO, Director CC-IT	23.01.2024

Contents

List of illustrations

List of tables

For reasons of better readability, the generic masculine is used in this document. Female and other gender identities are expressly included where this is necessary for the statement and personal designations apply equally to all genders.

1 Introduction

The existence of GMH Gruppe can be jeopardized by deliberately damaging actions, human error, a failure of information technology or a breach of the availability, confidentiality and integrity of information. In order to counteract reputational or financial damage, information security at GMH Gruppe is to be permanently established, implemented, maintained and continuously improved. To this end, an information security management system has been established to ensure that the protection goals of confidentiality, integrity and availability of information can be guaranteed. There should also be a uniform understanding of information security within GMH Gruppe.

1.1 The GMH Gruppe

GMH Gruppe is one of the largest privately managed metalworking groups in Europe and comprises a total of 20 medium-sized production companies in the steel, forging and casting sectors with around 6,000 employees. Its wide range of products and services are used in various industries, including automotive, rail technology, power generation, transportation, logistics, aerospace, agricultural and construction machinery as well as general mechanical and plant engineering. The parent company, Georgsmarienhütte Holding GmbH, coordinates the entire GMH Group.

1.2 Scope of application

The guideline on information security applies to all GMH Gruppe employees.

This guideline on information security covers all information that is processed by or with IT systems and non-IT systems. Additional guidelines and regulations may also apply at the individual locations, which in these cases only affect the locations themselves, i.e. the area of application.

All central topics are marked accordingly with the GMH Gruppe logo. Decentralized topics are marked with the location-specific logo.

1.3 Contact person

The contact person for all questions relating to this guideline is the Information Security Manager (ISM), who is located in the Competence Center IT of GMH Gruppe and works on behalf of the GMH Gruppe locations to be certified according to TISAX.

Information security coordinators (ISK) are the point of contact for employees at the individual locations that are certified in accordance with TISAX. These ISKs report to the Group ISM.

1.4 Responsibilities

This guideline has been approved and released by the management of Georgsmarienhütte Holding GmbH. The observance, distribution and implementation of this guideline in the Group companies is the responsibility of the respective management of the sites to be certified according to TISAX. These can be found on the respective Group homepages.

2 Importance of information technology (IT) and information security

Information security and information technology (IT) have a very high priority at GMH Gruppe and represent an important quality feature of data processing, as many key strategic and operational business processes at GMH Gruppe are significantly supported by information technologies.

GMH Gruppe's aim is to secure the availability of data and IT systems in the respective company across all business processes in such a way that the integrity and confidentiality of sensitive company data and personal data are adequately guaranteed. Losses with a high financial impact and immaterial consequences in the form of damage to the company's image must be prevented. Impairments with regard to the availability of the company's own applications can have just as serious an impact as irregularities with regard to the integrity and confidentiality of the information processed or used. The availability, confidentiality and integrity of information, applications and IT systems are not only threatened by external parties, but can also be jeopardized by internal vulnerabilities. Furthermore, information security is given advantages in the market with regard to tenders.

3 Corporate goals

The management of Georgsmarienhütte Holding GmbH has decided that an appropriate level of security for a high protection requirement should be sought. This decision was based on a risk analysis of the value of the assets to be protected and the justifiable expenditure on personnel and financial resources for information security.

The Management Board has set strategic goals:

- the introduction of an information security management system (ISMS) for the GMH Group companies with an automotive focus,
- the certification of Group companies with direct or indirect supplies to the automotive industry,
- communicating the need to actively support information security in the form of employee training.

- Confidentiality of information
- Integrity of the information
- Availability of information

3.1 Compliance with laws or regulations

The information security measures are intended to help ensure that the laws, regulations and contractual obligations relevant to the company are complied with by GMH Gruppe employees and executive bodies. The Group-wide laws are set out below:

- General Data Protection Regulation (GDPR)
- Compliance with the VDA-ISA in writing and form ($^{\text{TISAX®}}$)

Special laws and requirements of the individual Group companies are regulated in the respective legal register.

3.2 Awareness of information security

Appropriate technical and organizational measures are required to ensure information security. These can only be sufficiently effective if all employees are aware of the potential threats to information security and act responsibly in their areas of responsibility. Regular training on information security supports the effectiveness of information security management. Training and information is provided digitally via eLearning or classically in on-site training sessions. The regulatory and informational documents are made available digitally in full or in an appropriately summarized form on the intranet. The ISMS to be introduced has safeguarding processes with regard to the following sections.

3.3 Avoidance of material damage

Direct or indirect financial losses may result from the loss of confidentiality of sensitive data, the alteration of data or the failure of an IT application or system.

3.4 Protection of personal rights and trade secrets The confidentiality and integrity of information important to GMH Gruppe must be protected, regardless of the form in which it is available. Confidentiality instructions must therefore also be strictly followed when handling electronic documents and information.

3.5 Avoidance of loss of reputation or damage to image

Financial damage and a negative image for GMH Gruppe must be prevented. Information security prevents a loss of reputation and damage to the company's image.

3.6 Continuous improvement

GMH Gruppe strives to continuously improve its information security processes. The Group companies must consider and implement a risk-based approach for the continuous improvement process of the ISMS. The improvement activities are to be documented on an interdisciplinary basis using the established processes in the respective Group company in the form of objective evidence. The results must also be taken into account in risk management. Furthermore, there is a regular exchange of experience between the information security manager and the information security coordinators.

3.7 Updating and information

This guideline must be reviewed at least once a year to ensure that it is up to date. The review must be documented in the form of a new revision. The changes are discussed at regular meetings between the Information Security Manager (ISM) and the Information Security Coordinators (ISK). Information security incidents during the year that require an adjustment to the ISMS must be coordinated directly with the ISM. The ISM ensures that information is passed on to the information coordinators.

The CC Risk and Insurance regularly informs the management boards every six months about the risks and opportunities relating to the ISMS. Furthermore, the ISK must conduct and document an annual management review with its management, synchronized with the ISM with the management of the holding company.

The changes to the structure and requirements of the ISMS must be trained and informed in accordance with the established processes of the respective company.

4 Organization of information security management

Overall responsibility for information security lies with top management (strategic level). A multi-level security structure has been set up to ensure that this responsibility is met and that the various tasks and duties arising from information security are implemented appropriately. The responsible employees have been appointed and are appropriately qualified for their tasks.

To avoid conflicts of interest, the responsibilities listed are separated organizationally (separation of functions, separation of duties):

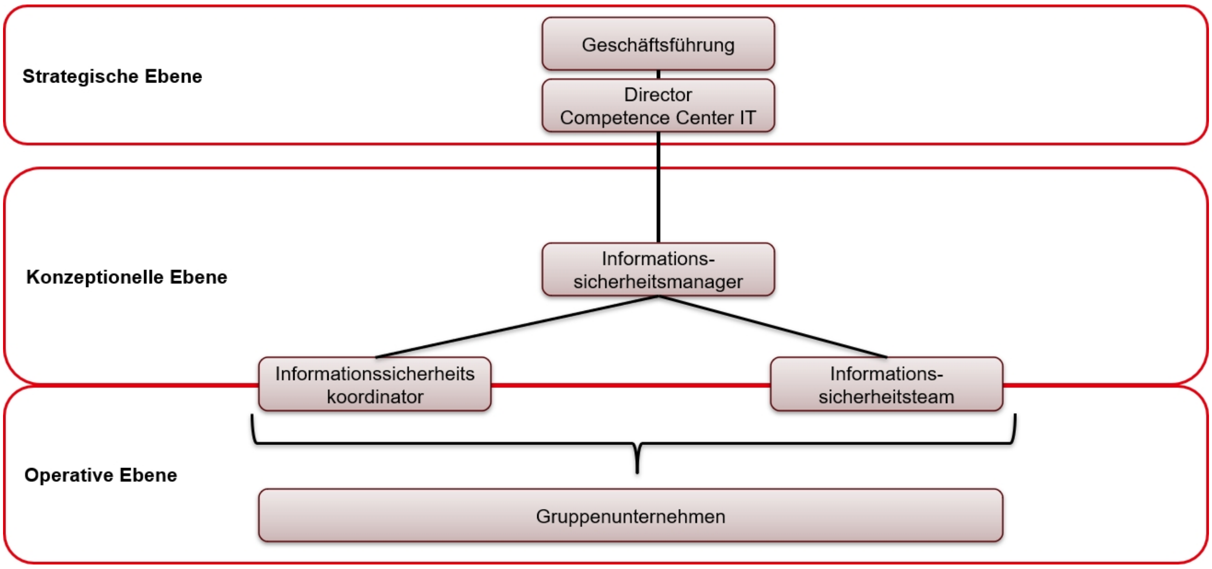
Strategische Ebene
Geschäftsführung
Director Competence Center IT
Konzeptionelle Ebene
Informations-sicherheitsmanager
Informationssicherheits koordinator
Informations-sicherheitsteam
Operative Ebene
Gruppenunternehmen

Figure 1 Organizational structure of information security GMH Gruppe

4.1 Strategic level

4.1.1 Management of the holding company

The management bears overall responsibility for ensuring that an ISMS is established, maintained and further developed in the Group companies. The management of the respective location is responsible for implementing the ISMS in the respective company. The company is responsible for providing technical and personnel resources for the implementation of information security and its appropriate embedding in the structures and hierarchy of the company. It also acts as a role model (tone from the top).

4.1.2 Director Competence Center IT

The Director Competence Center (CC) IT is responsible for the management of IT in the GMH Gruppe. He reports to the management of Georgsmarienhütte Holding GmbH and implements the IT security requirements through appropriate protective measures. To fulfil this task, he makes use of the employees of the IT organization.

4.2 Conceptual level

4.2.1 Information Security Manager

The Information Security Manager has been appointed by the management of Georgsmarienhütte Holding GmbH. He is available to support the strategic level in the following activities:

- control and coordinate the security process,
- to support the strategic level in drawing up the safety guideline,

- coordinating the creation of the security concept and associated sub-concepts and overarching guidelines,
- to draw up implementation plans for security measures and to initiate and review their implementation,
- report on the status of information security to the strategic level and other security officers,
- coordinate security-related projects,
- investigate security-related incidents and
- Initiate and coordinate awareness-raising and training on information security.

4.2.2 Information security coordinator per location

The information security coordinator is appointed for each location. They work closely with the information security manager and consult with them at regular intervals. He coordinates the information security guidelines and processes at the location and monitors compliance with them.

4.2.3 Information security team

The entire information security team (ISMS team for short) is made up of the strategic level, the conceptual level and the operational level (Figure 2).

The team defines measures that need to be taken from a technical perspective to improve and maintain information security. They support the ISM and the ISK in performing their tasks:

- in the definition of security objectives and strategies,
- in developing the safety guideline and reviewing its implementation,
- in the creation of the security concept,
- in initiating, controlling and monitoring the security process,
- in the design of training and awareness programs,
- in advising the specialist managers, IT operations.

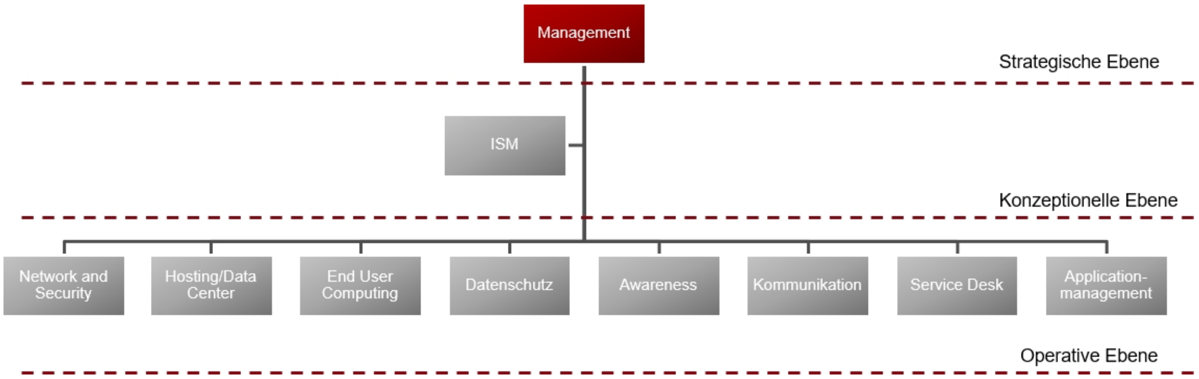

Figure 2 ISMS team structure

4.3 Operational level

The operational level is made up of the specialist IT managers at the respective locations of the Competence Center IT, who are responsible for implementing the security measures to protect information (see Figure 2), as well as the employees. The Competence Center IT is supported by the ISMS team and the ISK. All employees within GMH Gruppe are responsible within their assigned area for ensuring that the information security objectives are realized and implemented through effective measures. To improve information security, all employees of the respective company must cooperate with the respective data protection officer, IT officer and also with the ISMS team.

4.4 Direction of action within the ISMS

Top-down and bottom-up planning applies within the ISMS, i.e. the individual sub-areas are responsible for working out the corresponding results, which are linked and coordinated as part of the overall planning. This can be done either from the strategic level downwards to the operational level or vice versa from the operational level upwards to the strategic level.

5 Structure of the information security documentation

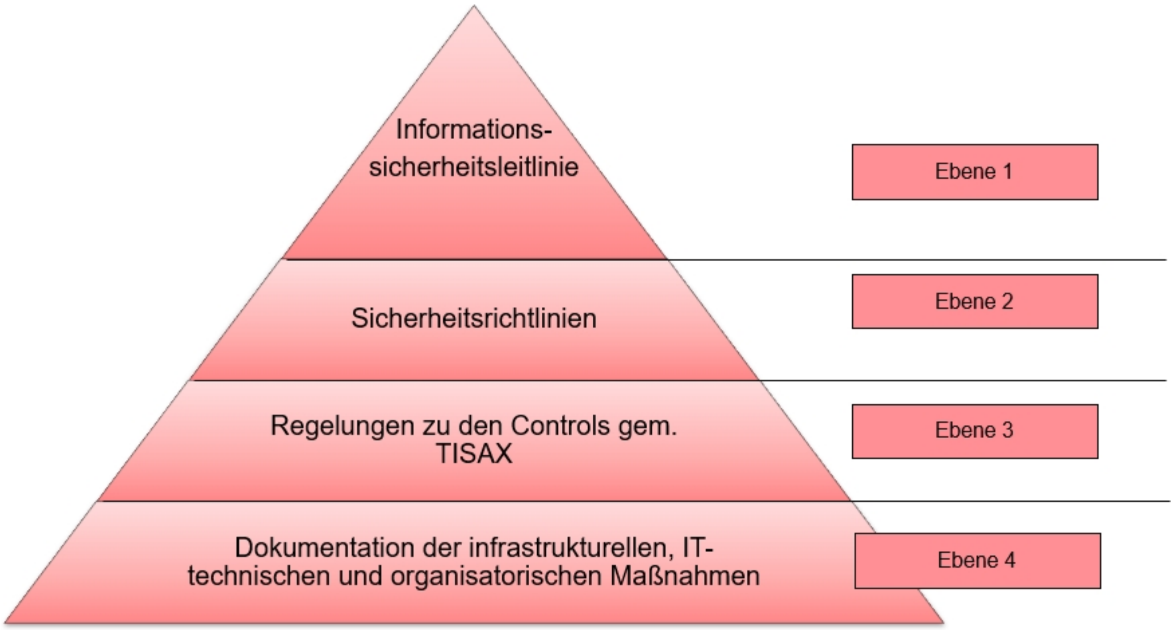
Informations-
sicherheitsleitlinie
Ebene 1
Sicherheitsrichtlinien
Ebene 2
Regelungen zu den Controls gem.
TISAX
Ebene 3
Dokumentation der infrastrukturellen, IT-
technischen und organisatorischen Maßnahmen
Ebene 4

Figure 3 Structure of the information security documentation

The control of the documents is subject to the requirements of the VDA-ISA.

6 Consequences of non-compliance with the ISMS

Intentional or grossly negligent actions that violate the security requirements can result in financial losses, damage employees, business partners and customers or jeopardize the company's reputation. The consequences of violations extend to all areas of information security management. Deliberate breaches of mandatory security rules can have consequences under employment law and, under certain circumstances, also under criminal law and lead to recourse claims.

7 Framework of the ISMS

The framework of an information security management system (ISMS) according to TISAX® is a key guideline for companies operating in the automotive industry. TISAX defines a standardized approach to the assessment and certification of information security.

ID	Structure of the ISMS
1	Information security guidelines and the company
2	Human Resources
3	Physical Security and Business Continuity
4	Identity and Access Management
5	IT Security / Cyber Security
6	Supplier Relationships
7	Compliance

Table 1 Structure of the ISMS

8 Regular review of this guideline

This guideline is reviewed at least once a year by the ISMS team to ensure that it is up to date.

9 Provision of this guideline

This guideline is public and will be made available on the Internet.

Georgsmarienhütte, 23.01.2024

Mathias Hölscher
Mathias Hölscher
24.01.2024 20:11:05 [UTC+1]
Management Georgsmarienhütte Holding GmbH

Deniz Oezcan
23.01.2024 18:05:17 [UTC+1]

Dr. Deniz Özcan
Director Competence Center IT