KNORR-BREMSE

# Information Security Guideline

CORPORATE GUIDELINE

December 2019 Version 1.0



Knorr-Bremse AG
Moosacher Straße 80
80809 Munich

KNORR-BREMSE

# Content

# 1 Introduction and Objectives

Knorr-Bremse is the global market leader for braking systems and a leading supplier of other safety-critical rail and commercial vehicle systems. This means that security of information assets plays a key role for the Group. These information assets can be subject to a variety of information security risks, which may result in damage, loss or misuse and, in the worst case, jeopardize the existence of the entire Knorr-Bremse Group.

The objective of this Guideline is to ensure a binding and uniform framework for information security at all locations and for all entities of the Knorr-Bremse Group. Information security is about the confidentiality, integrity and availability of information.

- **Confidentiality** means that information is protected from unauthorized access.
- **Integrity** means that information are accurate, complete and unaltered.
- **Availability** means that information is available and usable by an authorized entity.

Moreover, “must” or “shall” refer to a mandatory requirement and “should” refers to a strong recommendation.

# 2 Scope and Lifecycle

2.1. This Guideline applies to all non-German associated companies in which the Knorr-Bremse Group owns the majority of shares or has the industrial leadership. For German associated companies in which the Knorr-Bremse Group owns the majority of shares or has the industrial leadership, the German-language version of this Guideline applies.

2.2. The regulations laid down within this Guideline apply to employees, including senior management, executives and all other staff. Certain regulations also apply to externals such as business partners, visitors or suppliers.

2.3. The regulations laid down within this Guideline apply to all forms of information assets, e.g. speech, paper documents or electronic files, except for Knorr-Bremse products. Knorr-Bremse products are understood as artefacts (e.g. hardware or software) handed over to customers and may be also part of a service (e.g. hardware units for data collection installed in trucks or trains). On the other hand, business processes as well as services shall be developed in such a way that they comply with the requirements laid down in this Guideline, except for artefacts handed over to customers as part of a service.

2.4. The regulations contained in this Guideline shall reflect the external and internal context of the organization, as well as the needs and expectations of stakeholders. The latter include legal and regulatory requirements, sectoral standards, contractual obligations and the requirements of customers, suppliers or business partners.

2.5. Further requirements derived from local laws or government regulations with respect to requirements laid down in this Guideline overrule the requirements within their area of validity (e.g. in a specific country), if the latter are insufficient to meet the legal requirements. This also holds for sectoral standards, contractual obligations and requirements of customers, suppliers or business partners if approved as mandatory by an appropriate management board.

2.6. This Guideline shall be appropriately published within the Knorr-Bremse Group. This includes publication on the Knorr-Bremse Group Intranet.

2.7. This Guideline shall be reviewed at regular intervals (at least every two years) or earlier, if significant changes occur. The results shall be presented to an appropriate management board. If adaptations are deemed necessary and approved, the Guideline shall be updated to ensure its continuing suitability and effectiveness.

2.8. This Guideline (or extracts thereof) may be provided to external business partners, depending on the respective case.

2.9. This Guideline will be supplemented by supplementary functional guidelines for which the regulations in this chapter also hold analogously (for more details see chapter 9).

## 3 Management Commitment

The Knorr-Bremse Executive Board holds the overall responsibility for information security and expresses its intention and commitment

- to take information security into account in corporate strategy and strategic decisions
- to establish a Group-wide information security organization that sets up a framework and establishes security governance processes
- to provide adequate resources for this Group-wide information security organization, as well as for further functions responsible for processes, projects and activities that deal with information security, and
- to regularly review the information security framework and strategy and to take care of adaptation if required.

## 4 Strategy

Our vision is that the information security organization should address current and future risks as well as relevant regulatory requirements related to confidentiality, integrity and availability of information and associated assets in a balanced manner and therefore acts as a business enabler.

The mission of the information security organization is to establish the Group-wide framework for information security management and security governance processes that are in alignment with industry and sectoral standards and to check compliance with those standards regularly.

## 5 Principles

The following principles should be followed, if appropriate:

- *Risk Orientation*: Information security risks should be systematically identified and evaluated to make them transparent and to assess their relevance. Following risk identification and evaluation, a decision must be taken on how to treat the risk. This can be done using the four options: risk reduction, risk acceptance, risk avoidance or risk transfer.
- *Compliance Orientation*: Measures and procedures to preserve the confidentiality, integrity and availability of information shall be implemented according to legal requirements.

- *Business Alignment*: Decisions, plans and implementations should be aligned with the Commercial Vehicle Systems (CVS) and Rail Vehicle Systems (RVS) divisions.
- *Proactivity*: Information security risks and compliance gaps should be identified at an early stage. Information security should be already considered in the design phase of new developments and projects.
- *Best-Practice Orientation*: Measures and procedures to preserve confidentiality, integrity and availability of information as well as risk treatment should consider best-practice approaches and state-of-the-art procedures.
- *Feasibility*: Measures and procedures to preserve the confidentiality, integrity and availability of information should be designed to be feasible.
- *Measurability*: Processes to preserve confidentiality, integrity and availability of information should be implemented is such a way that their key output is measurable with suitable key performance indices.
- *Collaboration*: Activities related to preserving information security should be carried out in a collaborative manner and include relevant stakeholders.
- *Seriousness*: Deliberate or grossly negligent breaches of the regulations within this Guideline and supplementary functional guidelines which have resulted in material damage should be sanctioned in accordance with applicable legal provisions.
- *Continuous Improvement*: The suitability and effectiveness of measures and procedures should be continuously reviewed and improved.

These principles shall be understood as supplementary and not as preclusive.

# 6 Framework

The operationalization of our strategy is performed by the following functions

- The *Information Security Governance* function steers information security using an information security management system (ISMS). This consists of information security governance processes (including the preparation of information security guidelines) and is led by the Corporate Information Security Officer (CISO).

- The *Operational Information Security* function must be realized by all divisions and departments. It includes implementation of all information security guidelines and support for information security governance processes.

# 7 Organization

## 7.1 Information Security Governance

The *Information Security Governance* function is performed by the Group's information security organization. It consists of the following roles:

- The **Corporate Security Board** decides about the strategic direction of corporate security, including information security.
    - The tasks of the Corporate Security Board include approving the strategic roadmap, authorizing changes and supplements to the information security guidelines, approving information security projects and audit plans as well as the focus on relevant new aspects. It approves deviations and exceptions from this Guideline or supplementary guidelines itself or delegates this task to other roles for specific topics.

- The Corporate Security Board is chaired by the responsible member of the Executive Board, currently the Chief Financial Officer (CFO). Permanent members are representatives from the CVS and RVS divisions as well as the Chief Information Officer (CIO). The Corporate Information Security Officer (CISO) and the Chief Security Officer (CSO) report to the Corporate Security Board. The Corporate Security Board meets regularly, usually four times a year.

- The **Corporate Information Security Officer (CISO)** is the head of the corporate information security organization and responsible for the overall framework as well as the performance of the information security governance processes. He/she prepares key decisions related to information security within the Corporate Security Board. The CISO and his/her team steer and perform the governance processes. Moreover, he/she maintains the further information security organization with consists of RISO, LISO and BISO. He/she also initiates the appointment of the RISO.

- **Regional Information Security Officers (RISO)** for the regions Europe, Asia/Pacific and Americas are announced in written form by the regional management boards and support the CISO in implementing and maintaining the security governance processes in their regions. There are monthly meetings between the CISO and the RISO to discuss current relevant topics. The RISO identifies LISO who leave or are missing and drives the appointment of new LISO by the Managing Director of the local entity (MD). Until the RISO is announced, a regional board member takes over the role by default.

- **Local Information Security Officers (LISO)** are announced in written form for each location by the responsible Managing Director of the local entity (MD) and support the RISO and CISO in implementing and maintaining the security governance processes in their locations. Meetings with the LISO and RISO/CISO are held if needed. Until the LISO is announced, the responsible MD takes over the role by default.

- **Business Information Security Officers (BISO)** can be announced for selected critical business areas or departments. The IT organization is such a critical business area. For the IT organization, the Heads of the Global IT Center of Competence (HCC) take over this role by default for their area of responsibility. Their tasks are analogous to the tasks of the LISO. Further selected critical business areas may be defined by the Corporate Security Board. The head of such a critical business area shall take over this role for their area of responsibility by default, unless he/she appoints another suitable staff member to this role.

### 7.2 Operational Information Security

The *Operational Information Security* function must be ensured by line management in their area of responsibility. This is not restricted to certain business units. Some units such as IT have extensive duties and need to address this by appropriate organizational measures (e.g. dedicated operational IT security units).

## 8 Information Security Management System

The CISO must establish and maintain an information security management system (ISMS). It shall include the following information security governance processes in addition to the organization:

- Guidelines
- Information Security Risk Management
- Information Security Program

- Cyber Monitoring and Defense Center
- Information Security Audit Management
- Information Security Awareness
- Information Security Incident Management

The CISO shall document, steer, maintain and further develop these information security governance processes according to the principle of continuous improvement (e.g. the Plan-Do-Check-Act Model). All processes shall be on an adequate maturity level as defined by the Corporate Security Board and regularly reviewed and adapted if needed.

The ISMS shall be reviewed by an independent and competent body at regular intervals (at least each three years) and in the case of significant changes. The results of the reviews shall be recorded, retained and reported to the Corporate Security Board without undue delay. Correcting measures shall then be initiated and implemented if necessary.

## 8.1 Guidelines

8.1.1. Information security guidelines shall be formulated and maintained in alignment with the relevant industry and branch standards. Their requirements shall reflect the current and projected information security threat environment and shall take Knorr-Bremse Group´s business strategy into account. The handling of deviations and exceptions shall be included.

8.1.2. The information security organization shall identify relevant legislation and, together with the respective business departments, relevant sectoral standards. Possibly, the information security guidelines need to be adapted.

8.1.3. Additional requirements of third parties such as customers, suppliers or business partners with respect to information security (e.g. as part of draft contracts) must be aligned with the information security organization. These requirements may only be guaranteed to third parties with the approval of the Corporate Security Board if extensive information security measures must be implemented to comply with these requirements. Possibly, the information security guidelines need to be adapted.

## 8.2 Information Security Risk Management

8.2.1. An information security risk management shall be set up and maintained in alignment with relevant industry and sectoral standards as well as the Knorr-Bremse Group risk management process.

8.2.2. In addition to definition of the method and provision of templates (context establishment), the sub-processes of risk assessment (risk identification, risk analysis and risk evaluation), risk treatment, risk communication, risk monitoring/review and continuous improvement of the process shall be covered.

8.2.3. Transparency with respect to identified risks and their severity shall be obtained. A decision about risk treatment shall be taken in a timely manner, with locally limited risks at local level, with regionally limited risks at regional level and global risks at the global level.

8.2.4. The Corporate Security Board shall approve the method and its scope (e.g. IT applications).

## 8.3 Information Security Program

8.3.1. Resulting from the information risk management process, audits and further sources (e.g. new insights, new technology, ISMS reference model), risks are regularly identified.

8.3.2. If the Corporate Security Board decides that certain risks shall be reduced, the responsible operative divisions or departments shall compile risk reduction proposals. The information security organization should be involved and check if the proposals are adequate and appropriate.

8.3.3. The Corporate Security Board decides about the proposals.

8.3.4. The implementation of the approved information security projects shall be performed by the responsible operative divisions or departments and is tracked by the information security organisation. The implementation status is reported at the Corporate Security Board meetings.

## 8.4 Cyber Monitoring and Defense Center

8.4.1. A Cyber Monitoring and Defense Center (CMDC) shall be set up and maintained to detect and to record vulnerabilities and information security incidents (e.g. hacker attacks, severe malicious code infections).

8.4.2. A technical service must be set up and maintained by the CMDC that regularly and automatically identifies vulnerabilities in IT systems. Results shall be provided to the respective owner of the IT systems. The severity of vulnerabilities as well as suggestions on how to fix them shall be indicated. Owners of the IT systems are obliged to remediate critical vulnerabilities as a matter of high priority.

8.4.3. A technical service must be set up and maintained by the CMDC to identify security incidents in IT systems. Relevant results shall be provided to the owner of the affected IT system by creating a security incident ticket (see section 8.7).

8.4.4. The CMDC should further consult owners of IT systems on their requests on how to fix the identified vulnerabilities or how to respond to information security incidents properly.

## 8.5 Information Security Audit Management

8.5.1. The audit function of the information security organization shall perform information security audits on a worldwide basis to check whether and to what extent the requirements of the information security guidelines have been appropriately addressed and to identify deviations, potential information security risks and key improvement measures.

8.5.2. As part of their respective audit responsibility, the audit function of the information security organization shall be entitled to obtain information necessary to perform the audit, including read-access to information systems and data as far as this it is legally permissible. Such information or access shall be provided without undue delay on request.

8.5.3. The applied audit methods (e.g. checklist-based audit, self-audit, specialized audit) and an annual audit plan shall be approved by the Corporate Security Board.

8.5.4. The audit function of the information security organization or the owner for the audit target in the case of a self-audit shall perform the information security audits according to the plan. The results of each audit shall be summarized in an audit report.

8.5.5. Implementation of the agreed measures to fix gaps identified during the audits shall be carried out by the respective owner. The implementation shall be tracked by the information security organization.

8.5.6. The audit function of the information security organization shall compile an annual report that sums up the results of the audits performed as well as the implementation status of the agreed measures.

## 8.6 Information Security Awareness

8.6.1. An information security awareness process shall be implemented, using several channels to educate all employees of the Knorr-Bremse Group. This must be done with regard to the importance of information security and raising awareness of how user actions can greatly impact overall information security.

8.6.2. The information security organization shall ensure that the process and the related information security awareness fulfils global, regional or local requirements. RISO and LISO must take care of the implementation of the information security awareness activities for their respective region and location.

## 8.7 Information Security Incident Management

8.7.1. An information security incident management procedure shall be drawn up, documented and maintained. Incidents and the respective response shall be documented.

8.7.2. Categories (incident types) and the severity of an information security incident need to be defined. Owners of affected IT systems or processes are obliged to respond to critical security incidents as a matter of the utmost priority.

8.7.3. The information security incident response for an information security incident with immediate danger shall be performed according to a specific procedure. In these cases, an information security incident response manager shall be established to lead and coordinate all activities. All staff members required to respond to this incident are obliged to work on this topic as a matter of the utmost priority. The information security incident response manager may also use other required company resources, even if these have been reserved by others (e.g. a conference room).

8.7.4. In case of an information security incident with crisis potential, the Corporate Security Officer shall be immediately informed. He/she will initiate further crisis management activities.

# 9 Supplements

In the Knorr-Bremse Group Guideline “Releases of Guidelines” layers of guidelines are described. This Guideline substitutes the chapter 1 to 4 of the *IT Security Guidelines v2.3.3*. There are two types of *functional guidelines* that supplement this Guideline:

- *Functional Guidelines for operational information security* shall be drawn up by the CISO and aligned with the relevant information security standards. This applies to the ISO 27001 framework and further standards approved by the Corporate Security Board. The Corporate Security Board is tasked to perform the formal evaluation (clearing); the guidelines are finally released by the CISO and his/her superior. Until such detailed regulations are approved and published, the corresponding regulations laid down in the chapter 5 to 10 of the *IT Security Guidelines v2.3.3* still apply analogously.
- *Functional Guidelines for operational processes related to information security* such as, for example, the process for emergency user in SAP shall be drawn up by the responsible process owner if needed. The CISO shall be part of the formal evaluation (clearing). The Guidelines shall be finally released by the process owner and his/her superior.