SIEMENS Healthineers

Directive

Technology Excellence **Document ID: 1_D_19**

Version: 5.0

Cybersecurity

Governance Area	Cybersecurity
Effective from / published on	2024-01-01 / 2023-10-01
Scope of validity	all Siemens Healthineers Companies

Previous version v4.1 valid until: 2023-12-31

Target group

This Directive is addressed to

- all employees with regards to the Cybersecurity Guiding Principles as defined in chapter 2.1
- Heads of Business Areas/ Lines and Business Horizontals as well as Regions/ Zones/ Countries and Corporate Functions incl. Technology Excellence regarding their obligations in their role as Cybersecurity Responsible to implement cybersecurity measures and targets in their organizations as defined in chapter 2.2.3,
- Cybersecurity professionals and employees with an assigned Cybersecurity role (Cybersecurity Ambassador, Officer, Expert, Contact) regarding the complete document.

Purpose

In the interconnected healthcare industry with increasing focus on digital products, solutions, and services, Cybersecurity is a key prerequisite to safeguard production and operations, protect sensitive information and assets, assure business continuity, protect the ability to sell into sensitive markets, and avoid adverse media coverage.

Cybersecurity has not only a trust-building impact but is also demanded by customers purchasing our products, solutions, and services. As the healthcare industry is considered part of the important infrastructure in many countries, international and national laws and regulations demand Cybersecurity from manufacturers and providers in the healthcare industry.

Therefore, this Directive defines the framework for Cybersecurity with its companywide principles, rules, regulations, processes, targets, and responsibilities. This framework is aimed at achieving resilience against cyber-threats by addressing technologies, processes, and people as well as efficient identification and management of cybersecurity risks.

It applies to all Cybersecurity activities not only within the company, but also with customers, business partners, suppliers and other third parties.

Content

1 Glossary

Specific roles

Corporate Cybersecurity Officer (CCSO)	Responsible to execute governance on behalf of the Governance Owner for Cybersecurity including external representation for Siemens Healthineers
Cybersecurity Board (CSB)	Alignment body for all Cybersecurity related topics which require cross-organizational cooperation
Cybersecurity Responsible	Top level Cybersecurity role which is assigned per default to the Heads of Business Areas / Business Lines, Regions / Zones / Countries, Business Horizontals, and Functions (incl. TE)

For further roles, refer to attachment 1 [link]

Specific terms

Cybersecurity (CYS)	Cybersecurity comprises information security and product and solution security, thus the protection against harm caused by (but not limited to) digital attacks against the confidentiality, integrity, availability, and authenticity of - information and assets (IT/OT)[1] - portfolio and installed base (products, solutions, and services)
Cybersecurity Community	Employees of Corporate Cybersecurity, with an assigned Cybersecurity role (CYSA, CYSO, CYSE, CYSC), or connected with Cybersecurity in any other way
Cybersecurity Management System (CYSMS)	CYSMS is a set of requirements stipulated in rules and processes for systematically managing an organization's sensitive assets.
Corporate Cybersecurity	Employees of TE CYS and TE DC CYS under the responsibility of the Governance Owner and direction of the CCSO

2 Procedure/Requirements

2.1 Guiding principles

To leverage the full potential of the digital transformation for our business, Cybersecurity is a prerequisite that requires active cross-organizational engagement from the whole organization, aligned with our customers, business partners, suppliers and other third parties as it touches every aspect of the business. In an increasingly interconnected environment, Cybersecurity cannot be the effort of one central team only, but rather needs to be a joint approach among multiple stakeholders (e.g., employees, managers, special cybersecurity roles, healthcare facilities, providers).

To establish and maintain trust within our market, Siemens Healthineers adopts the following guiding principles:

- Cybersecurity is a quality requirement (pre- and post-market) demanded by interested parties, e.g., customers and regulators,
- Cybersecurity enables our business to protect adequately against cyber-threats and supports the creation of secure products, solutions, and services and to keep them secure throughout their lifecycle,

[1] Information Technology/Operational Technology: Operational Technology (OT) refers to technologies used in the development and production environment, such as programmable logic controllers (PLCs) or supervisory control and data acquisition (SCADA) systems that control the physical devices for the production process of modalities, instruments and reagents through sensors and actors.

- Cybersecurity continuously improves resilience through clear and holistic accountability and drives a culture of ownership.

Therefore, all employees shall be aware of and support the following:

- Protection of data and assets of individuals and companies,
- Prevention of cyber-based damage to people, companies, and infrastructures,
- Implementation of a reliable Cybersecurity foundation on which confidence in a networked, digital world can take root and grow,
- Appropriately addressing Cybersecurity for our portfolio and installed base to keep them secure throughout their lifecycle.
- Reporting of potential Cybersecurity-related events/incidents immediately once suspected or occurred using the defined channels: link.

Cybersecurity guidance for everyday situations is summarized in the Cybersecurity Guidebook: 15_G_1

2.2 Cybersecurity Organization

2.2.1 Corporate Cybersecurity Officer (CCSO)

The Corporate Cybersecurity Officer (CCSO) represents Cybersecurity for Siemens Healthineers globally and

- is responsible for the global Cybersecurity strategy and setting of related objectives, targets, and performance indicators for continuous improvement,
- has authority to specify Cybersecurity requirements and protection measures, and assess compliance with these requirements,
- is responsible for the provision of a Cybersecurity Management System (see 2.3)
- is responsible for the provision of related awareness and training programs for all employees and specific Cybersecurity roles,
- has authority to give direction in case of Cybersecurity incidents including direct access to the designated member of the Managing Board in case of escalations as well as leading respective task forces,
- has to support the development and provision of Cybersecurity related services and tools,
- has to guide and direct the Cybersecurity Community, especially the Cybersecurity Officers.

The CCSO is supported in its responsibilities by the Corporate Cybersecurity team and the Cybersecurity Community. The CCSO shall report the state of resilience against cyber risk and assurance of an adequate security posture to the Managing Board and the Risk Committee on a regular basis.

2.2.2 Cybersecurity Responsibles

Within their scope of responsibility, the Heads of Business Areas / Business Lines, Regions / Zones / Countries, Business Horizontals, and Functions (incl. TE) shall

- appoint and empower applicable Cybersecurity roles (see attachment 1 [link]),
- ensure adequate resourcing of appropriately qualified Cybersecurity personnel and activities,
- actively support the implementation and application of Cybersecurity requirements to protect and ensure business continuity for
  - Siemens Healthineers' portfolio (incl. installed base) along its lifecycle,
  - data of individuals and companies,
  - 3rd party relationships (e.g., customers, suppliers, and partners),
  - IT/OT infrastructure, IT applications, processes as well as associated facilities,
- monitor the implementation and effectiveness of Cybersecurity requirements on a regular basis (see4), take corrective actions where necessary, and perform continuous improvement of the Cybersecurity maturity.

OrgUnits shall be in lead of identifying and implementing Cybersecurity related external technical regulations and standards applicable for their scope of business (e.g. BSI C5, SOC2).

OrgUnits intending to certify any ISO 27000 series standard in addition to the CYSMS shall align with the CCSO and get written confirmation prior to respective activities and ensure adequate resources are available within the OrgUnit.

2.2.3 Cybersecurity Board (CSB)

The CSB supports the CCSO in the implementation of the global Cybersecurity strategy. It shall consist of representatives from Cybersecurity (Chair), Data Privacy, Corporate Security, Information Technology, Quality, and Procurement and other parties upon request.

With regard to their represented Governance Area, the members of the CSB shall

- ensure the implementation of Cybersecurity requirements in own regulations and processes,
- foster cross-organizational cooperation with the objective of providing a holistic Cybersecurity framework.

2.3 Cybersecurity Management System (CYSMS)

Cybersecurity is a risk management activity, and the CYSMS [Link] is the framework addressing risks in a holistic approach.

- The CYSMS maintains mandatory requirements that shall be aligned in balance with market needs (derived from standards, laws, regulations, and contractual obligations) and additional identified requirements that are relevant to protect Siemens Healthineers. They shall be incorporated in Cybersecurity regulations and processes.
- Cybersecurity risks shall be treated in accordance with the Enterprise Risk Management methodology.
- The requirements to protect Information and IT assets shall be identified by applying Cybersecurity Asset Protection (CAP) and implemented accordingly.
- For Cybersecurity risks in the portfolio and installed base the threat and risk analysis (TRA) shall be applied.
- The loss of control over data in outsourcing projects/processes shall be considered as a Cybersecurity risk by the respective application owner, and necessary mitigation measures shall be implemented.
- The risks that can emerge from the involvement of external suppliers shall be treated in Cybersecurity Third-Party Risk Management as part of the supplier management and evaluation processes (see Directive 1_D_84).
- Deviations from Cybersecurity requirements and the associated risks shall be analyzed, approved, and addressed as defined in the CYSMS.

3 Implementation notes

The following implementation steps need to be considered from a legal entity perspective.

Item 1	Task: Enactment
What/How	Enact the Directive to enforce it towards all employees
Authority	Executive Management (MD/FD) of each Legal Entity
Item 2	**Task: Roles and resources**
What/How	For entities hosting a Cybersecurity Responsible: The Cybersecurity Responsibles shall ensure implementation of the Directives' content within their scope of responsibility. For that, the mandatory Cybersecurity roles according to attachment 1 shall be identified, adequately resourced, and authorized to take all further steps (see Item 3)
Authority	Cybersecurity Responsibles
Item 3	**Task: Implementation of CYSMS**
What/How	The upgrade from v4.1 to v5.0 of this Directive does not trigger efforts in the CYSMS implementation on local level as such. Affected roles and the CSB will be informed by the CCSO. Changes in the CYSMS itself will be communicated to the affected target groups upon occurrence.
Authority	Corporate Cybersecurity
Item 4	**Task: all employees awareness**
What/How	Provision of all-employee training and a section in the Business Conduct Guidelines
Authority	Corporate Cybersecurity

4 Risk and Internal Control (RIC) requirements

Compliance with the Control Requirements is to be ensured by the Management of the respective ARE (Managing Director/ARE-CEO, Finance Director/ARE-CFO) through the implementation of appropriate processes and controls. The assessment approach defined by the Governance Owner must be implemented analogously in accordance with the IC system.

The Control Requirements resulting from this Regulation are:

PCMB ref.	2.10.1	that the Heads of Business Areas / Business Lines, Regions / Zones / Countries, Business Horizontals, and Functions (incl. TE) ensure implementation and effectiveness of Cybersecurity requirements

Appendix

a) Document release

Role	Name, First Name	OrgCode
Governance Owner	Schardt, Peter	TE
Content Owner	Arglebe, Carlos	TE CYS
Author	Krause, Martin	TE CYS RCM

b) Change History

Revision	Changes	Date	Author
4.1	- Clarification of the authority of the CCSO in chapter 2.2.2, fourth bullet point - Governance Area changed to “Cybersecurity” - Editorial Change of Chapter 3 and 4 - Minor editorial adjustments	2022-09-15	Krause, Martin
5.0	Comprehensive refinement of the complete document - Adjustments in the responsibilities of the CCSO, Cybersecurity Responsibles and the CSB - Chapter “Processes” replaced by a new one addressing the Cybersecurity Management System with its embedded processes - Added statements with regard to the obligation to report incidents and the application of CAP - Implementation notes updated in accordance with new template - Attachment 1 upgraded (Role Matrix) - Attachment 2 deleted (Implementation plan for Varian) - Changes throughout the document with editorial character, also in Purpose and Target Group	2023-09-19	Krause, Martin

c) Reference documents

n.a.

d) List of attachments

- Attachment 1: Further Cybersecurity Roles [link]