Directive

Information Technology **Document ID: 1_D_59**

Version: 4.1

Standards in the IT Infrastructure

Governance Area	Information Technology
Effective from / published on	2024-11-01 / 2024-10-01
Scope of validity	All Siemens Healthineers Companies

Previous version v4.0 valid until: 2024-10-31

Target group

This Directive addresses all employees who are required to use and work with IT Hardware and/or Software as well as employees in IT functions.

Purpose

The IT infrastructure (Hardware and Software) is a fundamental requirement to maintain continuous operations of the company. Therefore, in the global setup of the company, specific standards must be observed to

- reduce complexity and costs (e.g., efficient procurement and service delivery),
- foster interoperability (e.g., data flow across organizational boundaries),
- increase security (e.g., prevention for cybersecurity attacks),
- ensure value-oriented IT Services across Siemens Healthineers.

This Directive defines the basic principles regarding IT hardware and software standards. This Directive is not applicable for hardware and software used in (medical) products or solutions.

Content

1 Glossary

Specific roles

IT Enterprise Architecture & Infrastructure Board	The team responsible for defining IT-Software-Platform standards, facilitated by IT EA. The Board focusses on key technology & platform decisions for Siemens Healthineers in regard to Technology & Innovation Roadmap, Strategic Platform Decisions, Infrastructure Projects & Roadmaps (e.g. Cloudification), Business Architecture & Capabilities and Major Release Upgrades (e.g. SAP). It ensures the alignment of technology roadmap with business goals and priorities within and across your areas of responsibilities. The meeting cadence is quarterly
IT Standard Hardware Circle	The team responsible for defining hardware standards, facilitated by IT DEI.
IT Executive Board	The board responsible for alignment on IT strategic direction, prioritization of key IT projects and major IT investments, steering of overall IT developments and operations, facilitated by IT. The board focusses on values, projects and budget and is sponsored by Jochen Schmitz and Elisabeth Staudinger. Members are the heads (of finance) of Business Areas, Business Horizontals and Functions. The meeting cadence is quarterly.

Specific terms

IT Hardware	Cover term for physical, tangible parts of an IT system or its components (= Desktop PC, laptop, Mac, ... | Accessories, such as monitor, keyboard, headset, printer, … | mobile phone, tablet, … | server, … | router, network components, ...) with regard to this Directive: limited to internal use (i.e.: not part of products and solutions for customers)
IT Platform	From a technical perspective, the term "IT Platform" generally refers to software that serves as the basis for developing applications and connects data with applications. Platform categories ensure optimal support, operation and further development and are categorized as "mandatory", "standard" and "optional". IT Platforms form the basis for Siemens Healthineers' applications.
IT Software	Cover term for programs (= software platforms, desktop-, cloud-based-, web-based- , mobile-applications, includes Software as a Service-/Platform as a Service-solutions and public cloud services, …), its documentation and data. Regarding this Directive: limited to internal use (i.e.: not part of products and solutions for customers)
Standard	Regarding this Directive: standard = pre-defined, pre-selected, pre-configured or pre-validated

2 Procedure/Requirements

2.1 General principles

The use of *unauthorized* IT hardware is prohibited.

The installation, operation, or use of *unauthorized* IT software on devices provided or authorized by Siemens Healthineers is prohibited.

Unauthorized: Siemens Healthineers requires users to not acquire/use hard- or software intended to evade or disrupt information systems security, to not install software inappropriately licensed for use by the company, or to not access nor download any programs or files that may be considered offensive, illegal, not in the best interests of Siemens Healthineers, or contrary to the direction of the management.

To ensure proper authorization the required approach is to only use standard IT hardware and software which can be ordered or is provided via Siemens Healthineers processes (ordering via Purchasing, download from the “Software-Center” or the “Company Portal”).

The use of the standard (= pre-defined / pre-selected / pre-configured / pre-validated) IT hardware, IT platforms and IT software shall have priority over alternative solutions!

Standards for IT hardware, IT platforms and IT software are determined and published by the IT Function.

2.1.1 IT Hardware

The IT Function under consultation of the “IT Standard Hardware Circle” is the decision-making body for all IT hardware related topics. It defines binding standards and rules. Corresponding guidelines and information such as standard IT hardware catalogues are published e.g., on the intranet: Workplace Hardware Catalog

In addition to this global catalogue, there may be regional or organizational unit-specific catalogs that represent a subset of the global catalog. Adding hardware that is not included in the global catalog is not permitted.

If new hardware is to be added to the global hardware catalogue, the demand process must be followed. Information about the demand process can be found in KB0028085

2.1.2 IT Platforms

The "IT Enterprise Architecture & Infrastructure Board" under the leadership of IT Function makes all decisions regarding the use of overarching IT platforms and specifications for the enterprise architecture. It shall define binding Siemens Healthineers-wide standards and rules for the use of IT software platforms (e.g., the use of “Microsoft Office 365”, "ServiceNow" as a technology platform for Customer Service or IT service management applications for Siemens Healthineers). Corresponding guidelines and information are published on the intranet:

Platform Strategy

2.1.3 IT Software

The IT Function provides catalogues/lists with pre-defined, -selected, -configured, -validated standard IT software, which is made available via the “Software-Center” or the “Company Portal”. Corresponding guidelines and information are published on the intranet, among other places.

Adding or removing IT software from the standard IT software catalogues can be requested by raising a Software Management request via Service Catalog - Service Portal.

In addition to standard IT software catalogues, the IT Function maintains and publishes a so-called “disallow-lists” restricting or prohibiting the use of certain IT software, due to IT security reasons or requests from other Governance Owners (for example Cybersecurity (TE), Data Privacy (LC), etc.): Disallow-List for IT Software.

Additionally, IT Function maintains and publishes a so-called “allow-list” for browser extensions: Browser Extensions Allow-List

The IT Function is responsible for periodically checking whether certain non-standard IT software is still required and/or can be replaced by comparable standard IT software.

2.1.4 Generative AI

Generative AI platforms play an increasingly important role in companies. Due to the sensitivity of data privacy and information security, only compliantly implemented (e.g., CAP Rating, DP, Cloud/SaaS Assessment und Q-relevant, …) platforms and services are allowed to be used. The following decision was made by the IT Executive Board:

- **Siemens Healthineers process-specific or general employee service-related use cases** shall be implemented on the IT managed **GenAI platforms**, e.g., **Azure OpenAI Service** or on any platforms approved by IT.
- **Product or customer related use cases** need to be aligned with the respective business / Governance Owners (e.g., TE) and must be released on **Sherlock** or IT-managed **Azure OpenAI Service** only.

Information about the managed GenAI platforms could be found here: Generative AI and LLM

2.1.5 Trainings on Artificial Intelligence

On August 1st, 2024, the EU Artificial Intelligence Regulation (EU AI Act) has entered into force. Article 4 of the EU AI Act requires both providers and users of artificial intelligence systems to **take measures to ensure that their own staff and third parties involved in the use of artificial intelligence systems on their behalf have sufficient knowledge of artificial intelligence**. This group of people **must** be made aware of their rights and obligations in this regard and **must** be able to adequately assess the opportunities and risks of the use of artificial intelligence.

The following training concept applies to all Siemens Healthineers units that offer and/or use artificial intelligence systems or their output within the European Union - as part of the "EU AI Act Project":

1. As a **basic training** for all employees (except employees in production), the web-based training **#DigitalTogether with Generative AI and Large Language Models: Introductory Training** is available in Learn4U.
2. For the use of **AI in the development of products and services,** dedicated trainings will be provided by the Function Quality. Target Group for this training and need of completion will be communicated separately.
3. Each **business unit** and each **function must** examine the specific uses of AI within the unit and, if necessary, **create** and **implement a training concept** for the relevant groups of people based on points 1. or 2.

For Siemens Healthineers employees, the qualification measures and proof of participation must be documented in Learn4U. For third parties working on behalf of Siemens Healthineers, the contractual obligation to ensure needs-based qualifications is generally considered sufficient.

For all current employees these measures must be **initiated by January 31, 2025 and documented;** for all **new employees,** these measures must be initiated latest **within three months** of starting work for Healthineers.

2.2 Exceptions

Use of IT hardware or software outside of those approved (i.e. not in the “Workplace Hardware Catalog” or “Software Center” or the “Company Portal”) requires an approval and clearance according to Directive 1_D_106 “Registration of IT Applications” and 1_D_108 “Software Asset Management” prior to use. In this case the respective user, operator, or authorizer (approver) is responsible for ensuring non-violation of any internal regulations and rules and for providing a justified business need.

To avoid IT compliance risks, purchasing IT Software licenses or subscriptions for (public) cloud services in the interest of the company with personal funds and requesting reimbursement via travel expenses is not permitted. The standard purchasing processes must be followed.

The respective IT Business Partner or respective local IT department shall be informed if no standard IT hardware or software is available that meets the specific business need(s).

If larger scale, general exceptions are required, e.g., for entire regions or business units, then these shall be aligned with the IT Function and all respective Governance Owners and documented accordingly. For these cases, a formal exception needs to be requested with the Governance Owner.

Any Governance Owners, for example for Cybersecurity, Information Technology, Data Privacy, or Strategic Procurement, may maintain and publish a so-called "disallow-list" (in former times sometimes also called "black-lists") restricting or prohibiting the use of certain, dedicated IT hard- or software.

If requested by a Governance Owner, the user must terminate the use of IT hardware or switch off the hardware and/or terminate the use of IT software or uninstall the software.

Depending on the risk or urgency, a Governance Owner may authorize the IT Function to shut down IT Hardware or block the execution of IT Software, or even remove IT Software.

3 Implementation notes

All employees shall be informed about the content of this Directive and the mandatory compliance via appropriate communication and/or training measures and via the existing network of Business Partners and SME. It is recommended that this Directive is referenced in quality management systems/process frameworks.

IT Business Partners or respective local IT departments shall ensure awareness of this Directive's principles within the organizations they support.

With respect to usage of Generative AI platforms or applications and due to their relevance and current momentum, Business Lines / Business Area / Horizontals / Functions / Regions must instruct their employees to comply with the stipulations outlined in chapter 2.1.4 and 2.1.5 above. Respective training basic training (#DigitalTogether with Generative AI and Large Language Models: Introductory Training) is available in Learn4U and shall be assigned by the respective managers to all Healthineers employees who use AI professionally. These employees must have completed the basic training by February 1st, 2025, at the latest. All employees in development of products and services must complete the training courses accordingly, which will be set up centrally by the function Quality.

The IT Function shall provide and maintain global and/or local standard IT hard-/software catalogues (e.g., IT Hardware-Catalogue, Software-Center, Company-Portal, etc.).

The IT Function shall carry out checks (e.g., via automated network scans or assessments) to monitor compliance with the requirements of this Directive.

The migration of existing IT hard- and software to the standard IT hard- and software is not mandatory in general, however might be considered from an economic or strategic point of view (e.g., in cases of post-merger integrations).

Specific tasks for Managing Directors / Finance Directors:[1]

Task	MD/ ARE-CEO	FD / ARE-CFO	accountable	responsible
no specific ARE-MD/-FD task from this Directive	n/a	n/a	n/a	n/a

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 in accordance with the IC system.

The Control Requirements resulting from this Regulation are:

PCMB ref.	New CR tbd	that the Heads of Business Areas / Business Lines, Regions / Zones, Business Horizontals, Functions and TE ensure implementation of the Generative AI decisions based on a provided check list.

[1] Condensed summary of the immediate tasks for the executive management of an ARE resulting from this Directive. The management is in general jointly responsible in the external relationship. This is only concretized in those cases where the task specified in the Directive is explicitly assigned to only one member. “Accountability” to be understood as: being in charge, but no need to do him-/herself. The task can be delegated // “Responsibility” to be understood as: this needs to be done by that person.
The fact that no explicit task is mentioned here does not mean at all that this Directive is not applicable or not relevant; all Directives are binding and must be complied with within the Healthineers group. The absence of mention of an explicit task therefore means (only) that there is no immediate need for action to be taken by the above-mentioned persons as a result of this Directive.

Appendix

a) Document Release

Role	Name, First Name	OrgCode
Governance Owner	Henkel, Stefan	IT
Content Owner	Doma, Peter	IT DEI MWP
Content Owner & Author	Koch, Dietmar	IT ST SMA

b) Change History

Revision	Changes	Date	Author
4.0	Addition of Generative AI, IT Hardware and IT Software and Control Requirement, editorial changes.	2024-03-12	Koch, Dietmar Doma, Peter
4.1	Addition of Trainings on Artificial Intelligence according to Art. 4 of the EU AI Act	2024-09-19	Koch, Dietmar

c) Reference documents

n.a.

d) List of attachments

n.a.