Baseline Protection Requirements for IT Systems

Information Security and Data Protection

Version 2.7 – May 2025

Contents

1 Introduction

1.1 Subject matter and purpose

The system environment of a healthcare institution comprises - in addition to the systems procured and managed by internal ICT consisting of platforms (hardware and operating systems) and applications - a wide range of systems that are procured through other channels and integrated wholly or partially by third parties.

This directive defines the minimum technical and organizational information security and data protection requirements of the healthcare institution applicable to systems. The purpose of this document is to ensure the operational security of these systems, and thereby patient safety, while safeguarding the privacy of patients and staff and adequately protecting the systems against cyber threats..

To ensure broad acceptance of such requirements, coordination with key market stakeholders is essential. The H-CSC therefore aligns these baseline protection requirements with the hospital association H+ and the hospital technology network IHS “Infrastruktur Hospital Schweiz”.

Key suppliers are also involved to ensure that the requirements are understandable and transparent for them and that joint procurement processes can be optimally supported.

1.2 Delimitation

This document defines the Baseline Protection Requirements for IT Systems regarding information security and data protection. Other types of requirements, such as service levels, usability, or functional requirements of a system, are not addressed.

Outsourcing the operation of a system to a service provider gives rise to additional requirements. These are not part of this document. This also applies to the use of Software-as-a-Service (SaaS).

1.3 Scope

This document applies to all systems, in particular to all medical technology systems including their applications, that are integrated into the local network infrastructure of the healthcare institution and/or that process data of the healthcare institution (data of patients, data of staff, as well as medical and non-medical business data).

For network-capable medical systems, this document also applies if the system is not connected to the IT network of the healthcare institution (cf. Art. 74, MepV).

The document covers the phases of procurement, commissioning, operation and decommissioning.

The document is primarily addressed to the following groups:

- Service providers and suppliers;
- Internal employees of healthcare institutions who, in the context of procurement, integration, operation and decommissioning of systems, are responsible and authorized to make decisions or otherwise involved, in particular investment and project managers.

  Note: For healthcare institutions that are members of the H-CSC, additional supporting document are available on the H-CSC platform to support the internal implementation of these requirements. These include, for example, presentations to inform and convince management or procurement departments, as well as a guideline for applying the IT baseline protection requirements in procurement processes or public tenders.

1.4 Fundamentals

The basis for this document is formed by the applicable laws and requirements of Swiss and cantonal regulatory authorities, as well as recognized technical and organizational standards.

1.5 Binding nature and flexibility

The present IT baseline protection requirements become binding when they are required by the respective healthcare institution vis-à-vis the suppliers (e.g. through requests for quotations, tender documents, purchasing conditions, etc.).

The baseline protection requirements evolve in line with new developments but are intended to remain as stable as possible for both healthcare institutions and suppliers. Neither healthcare institutions nor suppliers should repeatedly have to deal with differently worded and differently structured requirements for the same systems.

Nevertheless, requirements must be adaptable to the capabilities of a healthcare institution or to a specific system procurement. For this reason, two different applications of these requirements are supported.

Specification: for reactive procurement processes of healthcare institutions

Healthcare institutions may weaken or strengthen individual baseline protection requirements as needed. Such deviations, as well as the weighting of the requirements, are defined by the healthcare institution in a separate document entitled “IT Baseline Protection Requirements for Systems – Specification” and are provided directly to the suppliers. Through the specification, deviations are easily identifiable for suppliers. The content of the requirements itself is not altered (baseline).

Self-declaration: for proactive procurement processes of suppliers

The self-declaration enables a supplier to assess and document its products against the IT baseline protection requirements on a one-time basis. This self-declaration can then be used by the supplier in its proactive procurement processes for all healthcare institutions. A corresponding template is available on the H-CSC website.

1.6 Definitions

Term	Definition
Healthcare institution	Healthcare institutions are organizations whose primary purpose is the provision of care or treatment to patients or the promotion of public health. These include, among others, hospitals, clinics, and care institutions.
System	A system refers to hardware or software that is supplied, integrated, and/or operated in whole or in part by third parties. A system comprises all components provided by a supplier or service provider. This includes hardware, firmware, operating systems, drivers, middleware, auxiliary and main applications, as well as all components used by the supplier or service provider from subcontractors, such as add-on applications, integrated source code, linked libraries, etc.
Mobile device	A mobile device is a device which, due to its size and weight, can be transported without significant physical effort, used in a mobile manner, and/or removed unnoticed from the area of responsibility of the healthcare institution. Examples include notebooks, tablets, smartphones, or small medical technology devices. Mobile devices may be part of a system.
Data processing	Data processing refers to any handling of data, such as the collection, retention, storage, use, access, modification, alteration, disclosure, or destruction of data, etc.

1.7 Document structure

To support suppliers of medical devices, references to the *Manufacturer Disclosure Statement for Medical Device Security* [R02] are provided where appropriate.

All requirements and template contractual clauses are assigned a reference ID that is unique within this document.

2 Requirements

2.1 Principles and fundamental concepts

ID	Requirement
01.01	Security awareness: It must be ensured at all times and in all areas that the operation of the system does not cause any harm to individuals or to the healthcare institution. Vulnerabilities are taken seriously and remediated in a timely manner.
01.02	System knowledge and compatibility: A supplier of a system must be fully aware of all components that make up its system. The supplier must ensure that these components are compatible with one another within the system at all times.
01.03	Defense in depth: A system must be protected by multiple, mutually reinforcing and complementary security measures in order to achieve redundancy with regard to the fulfilment of security requirements. Taken as a whole, the security measures must have preventive, detective, and reactive effects.
01.04	Least privilege and need-to-know: The assignment of access rights and privileges must be kept to a minimum. This applies to system users, enabled services and additional functionalities, as well as permitted communication relationships.
01.05	Security by default: Systems must be designed, configured, and operated in such a way that all security measures that are appropriate in a specific environment are enabled by default

ID	Requirement
	and can take effect without requiring user intervention. System components that enforce access control decisions must be designed in such a way that, in the event of a malfunction, no unauthorized access is possible.
01.06	Privacy by design and privacy by default: Data protection measures shall be consistently integrated into the system development processes. Systems shall be designed in such a way that secure data protection settings are defined as the default from the outset.

2.2 Organisation

ID	Requirement
02.01	Responsibilities: The tasks, competencies, and responsibilities relating to the system shall be agreed between the healthcare institution and the supplier prior to contract conclusion. Responsibilities for the individual components of a system, as well as responsibilities for the correct interaction of the system with components provided by the healthcare institution, shall be defined.
02.02	Responsibility for the system: The supplier is responsible for the correct functioning of all system components that are part of the system delivery. This also includes the correct interaction with components provided by the healthcare institution that comply with the supplier's contractually agreed specifications.
02.03	Reporting obligation for security incidents: Security incidents (cyberattacks) affecting suppliers and their subcontractors, including data protection breaches, shall be reported in accordance with the statutory deadlines (Information Security Act). The healthcare institution shall be informed within 24 hours of detection via the designated contact point of the healthcare institution and shall subsequently be kept actively informed [R03].
02.04	Active lifecycle management: The supplier shall ensure that manufacturer-defined lifecycles are adhered to for all components of its systems (including applications, operating systems, etc.). Components for which no security updates are available shall be replaced. MDS2 Ref: DOC-8
02.05	Active vulnerability management: The supplier shall maintain vulnerability management for all components of the system. The supplier shall regularly assess system components for vulnerabilities and track vulnerability notifications issued by the respective component manufacturers. The supplier shall proactively and transparently inform the healthcare institution of newly identified vulnerabilities as soon as they are discovered, regardless of whether a countermeasure is already available. The ICT department of the healthcare institution shall designate a contact point for such notifications [R03]. MDS2 Ref: CSUP-11 MDS2 Ref: RDMP-4
02.06	Vulnerability contact point: The supplier shall designate a contact point within its organization to which the healthcare institution can report identified vulnerabilities. The supplier shall ensure that such reports are processed in a timely manner by qualified specialists and that the healthcare institution is informed of the results.
02.07	Remediation of vulnerabilities: The supplier shall provide all resources required to remediate vulnerabilities. Security patches shall be installed without delay from the time they become available, or released to the healthcare institution for installation, depending on the severity of the vulnerability as classified according to the latest version of the Common Vulnerability Scoring System (CVSS).

ID	Requirement
02.08	Timeframes for vulnerability remediation: The remediation timeframes shall be based on the Common Vulnerability Scoring System (CVSS), as follows: ▪ Critical (CVSS 9.0–10.0): as soon as possible[1] ▪ High (CVSS 7.0–8.9): within 2 weeks ▪ Medium (CVSS 4.0–6.9): within 1 month ▪ Low (CVSS 0.1–3.9): within 2 months [1] The timeframe depends on the availability risks associated with the installation. If system components are provided by the healthcare institution in coordination with the supplier, the healthcare institution is responsible for updating these components. Overall responsibility for the correct functionality of the system remains with the supplier. The supplier shall specify to the healthcare institution which components are to be used for updates and shall ensure that compatibility of the updated components with the overall system is maintained.
02.09	Approval for commissioning: The system shall only be put into productive operation after acceptance by the involved specialist departments (e.g. building technology, medical informatics, medical technology) and the ICT department of the healthcare institution [R03]. Acceptance shall be documented in writing.
02.10	Transfer or removal of physical systems: Systems and all their components may only leave the healthcare institution with the approval of the responsible ICT staff [R03]. Prior to the transfer or removal of systems or components, regardless of the reason, all data of the healthcare institution shall be irreversibly deleted [05.05] or securely destroyed [05.06]. This shall be confirmed in writing to the responsible ICT staff of the healthcare institution prior to transfer or removal.

2.3 Documentation

ID	Requirement
03.01	Architecture documentation: The architecture of the system or the overall solution shall be fully documented. The architecture documentation shall include at least the following elements: 1. Diagrammatic overall view of all systems, applications, and components belonging to the solution. 2. Evidence of all components of the software products used and their relationships within the software supply chain (Software Bill of Materials, SBOM). 3. Interfaces to existing internal and external systems, including at least the following information: source, destination, protocol(s), encryption, authentication, transmitted data objects with confidentiality classification, and purpose. 4. Data communications with existing internal and external systems (e.g. transmission of consumption data, remote access, monitoring). 5. Data flows in the following form: purpose, data content, protection of confidentiality during data transmission and data storage. The classification of confidentiality levels of data objects shall be based on the applicable specification of the healthcare institution [R03]. MDS2 Ref: DOC-10

ID	Requirement
03.02	Technical operations documentation: Technical operations documentation must be provided for the system and shall include at least the following: 1. Overall overview of all systems belonging to the solution (e.g. operating systems, applications, COTS/SOUP) and any other essential components required for stable and secure operation. 2. Description of installation, configuration, operation, and maintenance (on-site and/or remote) of all systems, applications, and components belonging to the solution, including their vendor, product license, and version number. 3. Systems and their configuration in the following form: system designation, operating system used, installed applications including version numbers, services, and accounts (in particular those with privileged access rights). 4. List of all electronic data storage media within the system on which data of the healthcare institution may be stored, specifying the storage type (e.g. SSD, HDD, etc.) and the physical location within the device to allow identification of the media. 5. Declaration of all temporary and permanent data storage locations, including specification of which data of the healthcare institution are stored therein. 6. Identification of monitoring checkpoints required for proper operation, including the parameters relevant for proper operation. 7. Communication matrix in the following format: source, destination, network protocol, port, and purpose. MDS2 Ref: DOC-10 MDS2 Ref: SBOM-1
03.03	Operational system documentation: Operational system documentation shall be prepared for the system and coordinated with the responsible specialist unit of the healthcare institution [R03]. This documentation shall include at least: 1. Internal (healthcare institution) and external (supplier) responsibilities and contact points, as well as the associated maintenance, support, and administration processes, in particular: a) Declaration of operational responsibility for the system components b) Instructions for first-level support on how to handle known incidents c) Instructions for second-level support on how to analyse incidents and when to escalate to third-level support (manufacturer) d) Instructions on how to properly shut down the system components e) Instructions on how to properly start up the system components 2. User documentation of the solution (user manual).
03.04	Security documentation: The supplier shall provide the following security documentation for the offered product and/or for its organization: 1. *Information Security Policy* 2. ISO/IEC 27001 certificate, if available 3. Implementation of recommendations and best practices in the field of information security and data protection (e.g. ISO/IEC 27018) 4. Additional certifications in the field of information security and data protection, if available 5. Instructions on how to restart a crashed system and which checks must be performed to ensure data integrity

ID	Requirement
	6. Instructions on how to restore normal operation from a restricted or emergency operation mode MDS2 Ref: SGUD-1
03.05	Security documentation for medical technology systems: For medical technology systems, the following evidence shall be provided: 1. IEC 62304 certificate 2. CE certificate 3. *Manufacturer Disclosure Statement for Medical Device Security* (MDS2) MDS2 Ref: RDMP-1
03.06	Documentation for acceptance: At the time of system acceptance by the healthcare institution, the following documentation shall be available: ▪ Architecture documentation ▪ Technical operations documentation ▪ Operational system documentation ▪ Security documentation ▪ Security documentation for medical technology systems, where applicable
03.07	Form of documentation: Documentation shall be provided in electronic form and in a commonly used format (e.g. PDF).
03.08	Review and acceptance: All documentation shall be submitted to the healthcare institution for acceptance. The system shall only be commissioned after successful acceptance of the documentation. All changes to the documentation, except for minor changes, shall be actively communicated to the healthcare institution throughout the entire operational phase of the system and, where required, coordinated in advance.

2.4 Baseline configuration

ID	Requirement
04.01	Minimization of system exposure: To minimize system exposure, the following measures shall be implemented: 1. Blocking internet access unless it is required for system functionality or to ensure system operation. 2. Uninstallation or deactivation of all unnecessary software packages and network services. Only software packages and services that are strictly required for the operation of the system shall be installed. If auxiliary components are installed temporarily (e.g. during maintenance), they shall be uninstalled once the work has been completed. 3. Installation of a local firewall that allows access only to predefined network ports. 4. Deactivation of USB ports, Bluetooth interfaces, and other connection options unless they are required for operation. 5. Deactivation of the “AutoRun/AutoPlay” functions. MDS2 Ref: SAHD-1
04.02	Use of high-risk technologies: Technologies with known security risks shall not be used, such as protocols including SMBv1, FTP, or Telnet.

ID	Requirement
	MDS2 Ref: TXCF-5
04.03	Restriction of interfaces: Communication connections shall be established exclusively via the interfaces agreed with and documented by the healthcare institution. Unused interfaces shall be disabled to prevent any communication via those interfaces.
04.04	Endpoint protection: The system shall be protected against malware and misuse of system components by means of an endpoint protection solution. If the operation of an endpoint protection solution would compromise the conformity (CE, MDR, etc.) of the system, this shall be explicitly indicated by the supplier. MDS2 Ref: MLDP-2
04.05	Updating of endpoint protection: Security intelligence updates for the endpoint protection solution shall be installed regularly, but at least daily. New versions of the endpoint protection solution shall be installed in a timely manner. For this purpose, the system may establish an internet connection [04.01].

2.5 Data security

ID	Requirement
05.01	Encrypted data storage: Data shall be handled in accordance with the data classification policy of the healthcare institution [R03]. Sensitive data and personal data shall be encrypted using a secure cryptographic method at least at rest; this applies in particular to data stored on mobile devices. MDS2 Ref: STCF-1
05.02	Secure cryptographic methods: Only cryptographic methods and key lengths classified as secure shall be used for encryption. In this regard, the healthcare institution follows the technical guideline TR-02102 of the German Federal Office for Information Security (BSI) [R01].
05.03	Data transmission and storage: The supplier shall not store any data of the healthcare institution on its own IT infrastructure or storage media (USB sticks, disks, etc.). The same applies to data transmission. This requirement does not apply to system data that are strictly necessary to ensure system operation. Data shall not be removed from the healthcare institution without the written consent of the responsible parties [R03]. If cloud systems are used for the processing or storage of data, they shall be documented and their use shall be explicitly approved by the healthcare institution.
05.04	Data lifecycle: The data lifecycle (collection, processing, archiving, and deletion) shall be documented and shall consider internal and external compliance requirements regarding the healthcare institution's data retention obligations [R03]. The system shall only delete data autonomously if such deletion is permitted under the laws and internal policies applicable to the healthcare institution. The system shall provide an interface through which data relevant to the healthcare institution can be transferred to the healthcare institution's archive system in a legally compliant manner (e.g. treatment data). Data backups shall be performed in accordance with the standard methods and processes of the healthcare institution [R03].
05.05	Secure deletion function: The system shall support secure deletion functions that can be used for the irreversible deletion of all data of the healthcare institution from local storage

ID	Requirement
	media, in particular all patient data, access data such as passwords and keys, usage statistics, measurement results, etc. These deletion functions shall comply with the BSI VSIT standard or the DoD 5220.22-M (E) standard and shall be described in detail by the supplier in the documentation. After execution of the deletion functions, only information corresponding to the initial baseline configuration of the system and the factory state shall remain on the device.
05.06	Data destruction: When storage media are replaced, all data stored on them shall be securely deleted in advance [05.05]. Alternatively, the supplier may securely destroy and dispose of the storage media in an environmentally compliant manner or hand them over to the healthcare institution for destruction. This shall be documented in writing to the healthcare institution. Storage media shall not be removed from the healthcare institution without the written consent of the responsible parties of the healthcare institution. Physical destruction of storage media shall be carried out in accordance with DIN 66399 (Protection Class 2) [R04]. MDS2 Ref: SGUD-2

2.6 Data protection

ID	Requirement
06.01	Centralized management: Access to sensitive personal data on systems within the healthcare institution shall be granted exclusively via personal user accounts that are centrally managed by the healthcare institution. Local user accounts for such access shall not be permitted. MDS2 Ref: AUTH-1.1
06.02	Data processing: The processing of personal data and other data requiring protection shall take place exclusively in Switzerland or in a country with an adequate level of data protection. The applicable law shall be the legislation in force that applies to the respective healthcare institution (national or cantonal law). The reference date shall be the date of the offer or the purchase, as applicable.
06.03	Listing of personal data: The supplier shall specify which personal data are processed and stored by the system, including: 1. A list of the data with corresponding justification regarding proportionality and purpose limitation. 2. Retention periods for permanently stored data. 3. Identification of the countries to which such data may potentially be exported (storage, backup, access). MDS2 Ref: MPII-1 MDS2 Ref: MPII-2 MDS2 Ref: MPII-3

2.7 Logging and traceability

ID	Requirement
07.01	Logging: All actions on the system, in particular: ▪ log-on and log-off events, ▪ error conditions,

ID	Requirement
	▪ execution of privileged and administrative functions, ▪ changes to access rights and user roles, ▪ changes to system configurations, shall be recorded in a traceable manner. MDS2 Ref: AUDT-1 MDS2 Ref: AUDT-1.1 MDS2 Ref: AUDT-1.2 MDS2 Ref: AUDT-2.1 MDS2 Ref: AUDT-2.2
07.02	Audit trail: Logging shall record all processing activities involving relevant technical data, personal data, or other particularly sensitive data in the form of an audit trail. MDS2 Ref: AUDT-2 MDS2 Ref: AUDT-2.1 MDS2 Ref: AUDT-2.2 MDS2 Ref: AUDT-2.3 MDS2 Ref: AUDT-2.4 MDS2 Ref: AUDT-2.5 MDS2 Ref: AUDT-2.6 MDS2 Ref: AUDT-2.7 MDS2 Ref: AUDT-2.8 MDS2 Ref: AUDT-2.8.1 MDS2 Ref: AUDT-2.8.2 MDS2 Ref: AUDT-2.9 MDS2 Ref: AUDT-2.10 MDS2 Ref: AUDT-2.11
07.03	Protection against tampering of log data: Log data stored temporarily or permanently on the system shall be protected against tampering and unauthorized access. MDS2 Ref: AUDT-7
07.04	Forwarding of log data: The system shall be capable of forwarding log data to a central log server of the healthcare institution via a standardized interface and in a standardized format (e.g. Syslog). MDS2 Ref: AUDT-5 MDS2 Ref: AUDT-5.1 MDS2 Ref: AUDT-5.2 MDS2 Ref: AUDT-5.3

2.8 Communication and network access

ID	Requirement
08.01	Secure communication protocols: The system shall use exclusively communication protocols employing cryptographic methods and key lengths classified as secure. In this regard, the healthcare institution follows the technical guideline TR-02102 of the German Federal Office for Information Security BSI [R01].
08.02	Monitoring of transmission errors: In the event of data transmission to a central system of the healthcare institution (e.g. PACS), transmission errors shall be detected. Users or the responsible ICT unit of the healthcare institution [R03] shall be informed of transmission errors without delay.
08.03	Encryption: All internal and external communication connections to and from the system shall be encrypted using secure communication protocols.
08.04	Routing capabilities: The system shall not provide bridging, routing, or any other forwarding capabilities for other network segments. Corresponding functions shall be disabled.

ID	Requirement
08.05	Network addressing: The system shall support configurable network addressing so that it can be defined by the healthcare institution.
08.06	Wired communication connections: Wired communication connections shall be established exclusively via the network infrastructure of the healthcare institution. A system connected to the network shall support port-based authentication in accordance with IEEE 802.1X using EAP-TLS or equivalent alternatives approved by the ICT unit of the healthcare institution [R03].
08.07	Wireless communication connections (WLAN): For wireless communication connections, only network components of the healthcare institution shall be used. The encryption standard used shall be at least WPA2 Enterprise. EAP-TLS shall be used as the authentication protocol. Equivalent alternative solutions are permitted if approved by the ICT unit of the healthcare institution [R03].
08.08	Bluetooth connections: Where Bluetooth connections are required, Bluetooth Classic shall comply at least with Security Mode 4 Level 4, and Bluetooth Low Energy (LE) with Security Mode 1 Level 4.
08.09	Outbound web connections to the internet: If internet connections are required, they shall mandatorily be routed via the healthcare institution's web proxy. The system shall therefore support proxy functionality.
08.10	System time synchronization: The system shall support the Network Time Protocol (NTP) for system time synchronization. MDS2 Ref: AUDT-4.1.1

2.9 Access control

ID	Requirement
09.01	Separation of accounts for system services: Service accounts (accounts used for system services) shall be separated from user accounts. They shall have only the permissions required for the operation of the intended system services (principle of least privilege). MDS2 Ref: AUTH-2
09.02	Use of local administrator accounts: Local administrator accounts shall be used exclusively for maintenance and configuration purposes. Operational use shall be carried out via personal user accounts.
09.03	Authenticated access: Access to the system shall be authenticated exclusively. All user accounts shall be protected by appropriate authentication mechanisms. MDS2 Ref: AUTH-1
09.04	Authentication for interfaces: Data transmission via interfaces shall be authenticated exclusively. At a minimum, the sending and receiving systems shall be mutually authenticated. Authentication information (passwords, key material, etc.) shall be stored in a protected manner to prevent unauthorized access.
09.05	Password policy: Default passwords shall be changed prior to productive operation in accordance with the specifications of the healthcare institution [R03]. It shall be ensured that the passwords used are generated specifically for each healthcare institution and are not used for other customers. If there is any possibility that unauthorized third parties may have gained knowledge of such passwords, the supplier shall immediately inform the healthcare institution, and the passwords shall be changed in the affected systems.

ID	Requirement
	MDS2 Ref: PAUT-6
09.06	Handling of access credentials: Access credentials (e.g. passwords, digital or physical keys, etc.) shall be classified as confidential and treated and protected as such by the supplier and its systems. Access credentials shall be changed regularly at intervals to be defined by the healthcare institution [R03].
09.07	Authorization: The system shall provide role-based authorization or a comparable authorization mechanism. MDS2 Ref: AUTH-2
09.08	Provisioning of authorizations: The system shall support integration with the healthcare institution's IAM system via a standardized interface for the provisioning of authorizations. MDS2 Ref: PAUT-2
09.09	Locking of user sessions due to inactivity: The system shall provide the capability for users to manually lock sessions (e.g. when leaving the system). User sessions shall be automatically locked after a period of inactivity defined by the healthcare institution [R03]. MDS2 Ref: ALOF-1
09.10	Federated identity: User authentication and the transmission of information required for access to resources shall be performed via a trust relationship between the system and the designated infrastructure of the healthcare institution (federated identity). MDS2 Ref: PAUT-2

2.10 Maintenance and support

ID	Requirement
10.01	Remote access: Suppliers who require remote access to the systems of the healthcare institution shall comply with the applicable security requirements and shall use exclusively the remote access systems of the healthcare institution [R03]. Remote access shall be performed via personal user accounts. Supplier-specific remote access systems are not supported by the healthcare institution. MDS2 Ref: RMOT-1 MDS2 Ref: RMOT-2 MDS2 Ref: RMOT-3
10.02	Advance notification of maintenance activities: Maintenance activities performed by the supplier, regardless of whether they are carried out on-site or via remote access, shall be announced in advance to the responsible specialist department and the ICT unit of the healthcare institution [R03]. If exceptional circumstances require immediate maintenance activities, these shall be reported retrospectively to the specialist department and the ICT unit within 24 hours, including a substantiated and comprehensible justification of the urgency.
10.03	Maintenance activities using removable media: The connection of removable media to systems of the healthcare institution (including systems supplied by the supplier) shall not be permitted. Removable media for data transfer or data backup shall be provided by the healthcare institution. The supplier shall provide any software required to perform maintenance activities to the responsible ICT staff of the healthcare institution at least two weeks prior to the execution of the maintenance activities. The ICT staff shall review the software and make it available to

ID	Requirement
	the supplier on suitable media provided by the healthcare institution for the maintenance activities.

3 References

#	Designation	Reference
R01	BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen BSI TR-02102 Cryptographic Methods: Recommendations and Key Lengths	Link
R02	Manufacturer Disclosure Statement for Medical Device Security (version 2019)	Link
R03	Applied standards and IT strategy as well as contact points of the healthcare institution. This document is provided directly by the healthcare institution to the suppliers.	Appendix of the healthcare institution
R04	DIN 66399-1 Office and Data Technology – Destruction of Data Media	Link

The references were last reviewed on 2 February 2026.