HIL

IT security of technical systems – Requirements

This standard defines IT security requirements for technical systems that may be connected to a hospital's computer network. It reflects the consensus of the group of experts known as "HIL" (Hospital Infosec Liaison), representing public health hospitals of the following Swiss cantons: Fribourg, Geneva, Ticino, Valais, Vaud.

HUG Hôpitaux Universitaires de Genève

CHUV Centre hospitalier universitaire vaudois

Hôpital du Valais Spital Wallis

FHV Fédération des hôpitaux vaudois

HFR hôpital fribourgeois freiburger spital

eoc Ente Ospedaliero Cantonale

Version 3.0

June 2015

Reference number: HIL H.TEC:2015/v3.0 (E)

Table des matières

0.1 Version history

Date	Author	Modifications	Version	Status
2011-03-18	F. Calcavecchia (HUG)	HUG version 1.0	1.0	Final
2013-06-18	F. Calcavecchia (HUG)	HUG version 2.0	2.0	Final
2015-06-08	HIL (HUG, CHUV, EOC, FHVI, HFR, HVS)	First HIL validated version (French)	3.0 (F)	Validated
2016-09-05	J.Kenaghan (CHUV)	English version	3.0 (E)	Validated

0.2 Approvals

Institution, canton	Represented with the HIL group by	Date
HFR/State FR, Fribourg	A. Jordi, A. Müller	08.06.2015
HUG, Geneva	F. Calcavecchia	08.06.2015
EOC, Ticino	M. Marazza	08.06.2015
HVS, Valais	M. Buri	08.06.2015
CHUV, Vaud	J. Kenaghan	08.06.2015
FHV/FHVI, Vaud	P. Cohen	08.06.2015

0.3 Terms and abbreviations

Term/abbreviation	Meaning in this document
H.TEC.nn	Reference number of a security requirement described in this document.
HIL	"Hospital Infosec Liaison", a group of experts in information security, representing several Swiss hospitals. The "HIL" group is the author of this document.
Hospital	According to the context in which the term appears in this document, "the hospital" means the institution (care supplier or group of establishments) responsible for: (a) the system acquisition project, (b) operation and use of the system, and/or (c) the computer department and the computer network. *[These responsibilities may be clarified in additional documents, if necessary, especially if the organizational structure is complex.]*
ISD	Information Systems Department, i.e. the hospital's IT department.
IT	Information Technology
IT Security Officer	Person or organisational structure, designated by the hospital to validate (or refuse) requests for exceptions to the security requirements. The official title of this job function may vary between hospitals. *[Implicitly, a project to install a technical system requires a collaborative effort by a multidisciplinary team. The distribution of responsibilities between the various actors may depend on the hospital's structure and the specific project organization. If necessary, the roles of certain actors may be clarified in additional documents.]*
NDA	Non-Disclosure Agreement, or Confidentiality Agreement
OS	Operating System
PACS	Picture Archiving and Communication System
P	See section 2.2 *Requirement categories.*
Q	See section 2.2 *Requirement categories.*
RFT, Request For Tender	This term is meant to include any form of RFI (request for information), RFQ (request for quotation), RFP (request for proposal), etc.
Technical system	See section 1.2 *Definition*.

1 Introduction

1.1 Context

In technical fields such as biomedicine or building management, it is becoming common for technical systems to be connected to a computer network: for example, in order to communicate with computer applications or to be accessed by an external third party [e.g., the system's supplier or support organisation].

Unfortunately, information security "good practice" is not always systematically applied within such systems. With the increased connectivity of technical systems, hospitals have indeed noticed an increasing number of security incidents related to these systems: malware infections, data leakage, etc.

Concerned by such risks, several Swiss hospitals – working together as a group named "*Hospital Infosec Liaison*" (HIL) - collectively decided to formalize in this document a certain number of security requirements applicable to any **technical system that can potentially be connected to the hospital's computer network**.

1.2 Definition

The term "**technical system**" [also known as "technical equipment"] is here intended to include any device that combines hardware, software and communication (network) components, and that is used in the hospital, notably in any of the following areas:

- biomedical (where the medical device is involved in a healthcare process, including any form of medical care, analysis, diagnosis or supervision);
- laboratories (medical analysis or similar);
- building management (technical building management, centralized facilities management, detectors, uninterruptable power supplies (UPS), air-conditioning, video surveillance, access controls, etc.).

1.3 Uses of this document

Swiss hospitals are free to use this document for any purpose, in particular as a **reference framework**, either for acquisition and installation of new systems, or for auditing existing systems.

In the context of a Request For Tender (RFT), this document (or a copy of the requirements from chapter 2 « Technical security requirements ») will usually be an integral part of the RFT and of the contractual documents. Suppliers are in this case required to complete a checklist (provided by the hospital) in which they respond to **every** requirement, whether categorized as obligatory ("Prerequisite") or not. The hospital reserves the right to eliminate any offer in which the checklist has not been fully completed.

The hospital's checklist may be based on the model provided in Appendix A, which the hospital is free to adapt or to extend with additional requirements and details, according to its needs.

1.4 Intended audience

This document is intended for:

- suppliers contacted in relation to purchase of a new technical system (this document being annexed to the specifications or the RFT),
- the hospital's teams responsible for acquisitions or contracts,
- the teams responsible for the technical system's installation and configuration,
- auditors.

2 Technical security requirements

2.1 Goal of these requirements

These requirements aim:

- to protect the technical system against malware infections and against attacks within the hospital network or from external networks;
- to protect the Hospital Information System from risks related to the technical system.

2.2 Requirement categories

The requirements detailed below are categorized as follows:

- **P** = Prerequisite: Requirement generally considered vital. In the context of a RFT: the hospital reserves the right to eliminate a non-compliant offer, without other justification. The obligatory nature is recalled hereafter by the colour red and by underlining the reference number (e.g., **H.TEC.8**).
- **Q** = Qualification criterion: Desired feature; good security practice. In the context of a RFT: the supplier's response is taken into account when evaluating their tender. Exceptions or requests for exemption must be justified (e.g., a constraint imposed by an application) and validated by the hospital's designated *IT Security Officer*.

2.3 List of requirements

REFERENCE	P / Q	SECURITY MEASURE
2.3.1 Documentation		
H.TEC.1	**P**	**Technical documentation of the technical system** In the technical documentation provided to the hospital, the supplier must specify and maintain up-to-date the list of installed software (operating system, applications and all other significant or useful components), indicating for each item the publisher, license, version number and patch level (including security patches). The supplier must also specify and document appropriately all used services and network ports, and especially all listening ports.
H.TEC.2	**P**	**Architecture and operations documentation** The system must be documented. Documentation must include details of the architecture and the data flows (e.g. HL7, DICOM,…), installation, operations and maintenance. These documents will be submitted to the hospital's ISD (Information Systems Department) for approval before the system will be allowed to be connected to the network.
2.3.2 Basic configuration		
H.TEC.3	**Q**	**Standard operating system** If the hospital will be responsible for the technical system's administration and operation, the system must run a standard operating system approved by the hospital's ISD.
H.TEC.4	**Q**	**Attack surface** In order to reduce the attack surface of components that are exposed on the hospital's network, the supplier must ensure that only essential software is installed on the technical system. All unnecessary software must be uninstalled or disabled. If any network ports are in listening mode, this must correspond to an operational need validated by the hospital.
H.TEC.5	**Q**	**Supported operating system versions** To obtain authorization for connecting a new technical system to the hospital's network, the supplier must commit to following the cycle of operating system (e.g., Windows) updates proposed by its publisher (e.g., Microsoft). A technical system connected to the hospital's network must not run an operating system which is no longer supported by its publisher. (For example, Windows XP is no longer supported by its publisher, Microsoft, since April 2014.) If it is technically impossible to maintain the operating system up-to-date, the Hospital's ISD may be obliged to isolate the system from the main network or to move it to a different network. [Such measures will need to be taken into account by the hospital, as they may significantly increase the "total cost of ownership" of the system.]

Reference	P / Q	Security measure
H.TEC.6	**Q**	**Security patch management** To guarantee the security of its infrastructure, the hospital applies a process of security patching and updating of operating systems and other important software, in response to published security bulletins. Consequently, for components of the technical system that are to be connected to the hospital's network, the supplier must validate and guarantee that the system will work correctly (possibly by installation of a specific software update) after installation of the latest security patches proposed by publishers (of the operating system and other, potentially vulnerable, standard software), **within 2 months after the publication date**. If it is technically infeasible to maintain the operating system up-to-date with all security patches, the Hospital's ISD may be obliged to isolate the system from the main network or to move it to a different network. [Such measures will need to be taken into account by the hospital, as they may significantly increase the "total cost of ownership" of the system.]
H.TEC.7	**P**	**Management of personally identifiable information** The supplier must describe the types of *personally identifiable information* [also known as *personal data*] that is stored or handled by the system. For systems that store personally identifiable information durably (in particular, patient data), this description is required in order for the system to be validated by the hospital, which may require complementary information or impose additional security measures. Validation of the system is obligatory before the system is put into productive use (or preferably, before its purchase). Obtaining this validation is usually the responsibility of either the project manager or the person requesting connection of the system to the network, with the support of the hospital's designated *IT Security Officer*.
2.3.3 Protection against malware		
H.TEC.8	**P**	**Anti-malware** The components of the technical system exposed on the computer network must be protected by an anti-malware solution validated by the hospital. If the loss of certification or approval (e.g., "EC" certification) is given as the reason for lack of anti-malware protection, the supplier must provide proof of this. If necessary, the manufacturer must specify any directories that are to be excluded from such protection. He must also specify all authorized execution paths. Instead of a traditional antivirus which requires daily updates, an acceptable alternative is a "white-list" solution, guaranteeing the integrity of the software components of the system.
H.TEC.9	**P**	**Anti-malware / signature updates** In order to profit from the latest signatures and versions, the anti-malware solution must imperatively be updated **daily** from a central server that may be on-site (if the hospital supports this configuration) or off-site. Updates must be automatic. For solutions based on "white-listing", daily updates are (by definition) unnecessary.

Reference	P / Q	Security measure
H.TEC.10	**P**	**Control of external media** The supplier must specify whether operation of the technical system requires the use of external storage devices (USB key, CD or DVD disks, external disk drive, etc.), and must explain the reason for use of such devices. In all cases, in order to reduce the risk of malicious code execution, the “autorun” (automatic execution) function of such devices must be disabled on the technical system.
2.3.4 Network access		
H.TEC.11	**Q**	**Machine authentication** It is recommended to use a suitable method of machine authentication, and to give preference to 802.1x in particular. The methods of machine authentication supported or recommended must be specified.
H.TEC.12	**Q**	**Secure network protocols** When available, secure communication protocols (SSH, SFTP, SSL…) must be favoured, in particular for access to system administration functions and for any communication of patient data. Indeed, it is preferred that all communications be encrypted, even within the hospital network. Insecure equivalent services (telnet, rlogin, ftp…) must be disabled.
H.TEC.13	**P**	**Double network connections** For doubly-connected systems (for example, when a component of the technical system is connected to both the hospital’s network and the technical system’s internal network), any possibility of routing or bridging between the two interfaces must imperatively be disabled.
H.TEC.14	**P**	**Wireless connectivity** Communication between the different components of the system must use wired connections. Wireless links (for example, Wi-Fi or Bluetooth) are prohibited unless specifically validated by the hospital’s designated *IT Security Officer*.
H.TEC.15	**P**	**External connections** For technical systems which need to exchange data with external sites via Internet, encryption of such communications is obligatory. Encryption must be based on standard algorithms and on key-lengths that are generally recognized to provide an appropriate level of security. If communications transit via an intermediate third-party, it is recommended to also apply application-level encryption.
2.3.5 Access rights		
H.TEC.16	**P**	**Change default passwords** For the components of the technical system that are connected to the hospital’s network, standard or “default” passwords (delivered with the configuration and possibly available on Internet) – and in particular those of administrators and other privileged accounts – **must imperatively be changed** during or immediately after the installation phase.

Reference	P / Q	Security measure
H.TEC.17	**Q**	**Rules for passwords of privileged accounts** The password of any privileged account must comply with the following rules: a) Minimum length of 10 characters. b) No obligation to renew the password. c) Specific to the institution. d) Prohibition to use any password containing an “obvious” element (for example: the user name, the default password, or any names or abbreviations specific to the hospital or the supplier, etc.). e) Complexity based on obligatory use of at least 3 different categories of characters (from these 4 categories: upper-case, lower-case, digits and special characters), or based on a random character generator. f) Stored in a secure location that is accessible by a limited list of users, and managed by specific named persons. Passwords may be managed with the aid of a specialized tool. g) Account lockout after N rejected log-on attempts (possibly in a period of time T1). Alarm sent to a specific address. Automatic unlock at the end of a period of time T2. By default: N = 5 attempts, T1 = 1 minutes, T2 = 20 minutes. The precise parameters desired by the hospital (address for alerts, N, T1, T2) are available on request. **For automated logins between systems** (for example, with a monitoring system or an image storage system), the application of these rules should be decided on a case-by-case basis depending on the potential impact on patient health or on process integrity.
H.TEC.18	**P**	**Use of technical accounts** Programs and applications installed on the technical system must be executed under an account with restricted privileges. The system administrator account is reserved exclusively for configuration and maintenance operations.
H.TEC.19	**Q**	**Generic accounts** For hospital users who need to connect to the technical system, it is prohibited to use **generic accounts** that are locally defined on the system itself. Ideally, the system’s user-account management should be interfaced with the hospital’s internal, central directory system (e.g., Active Directory). If this is not the case, the supplier must provide appropriate procedures for management of named user accounts: these procedures must be compatible with the hospital’s identification and authentication standards (documentation available on request).
H.TEC.20	**Q**	**User passwords** For access or processing of the technical system’s local data, user authentication should be performed by the hospital’s central directory (e.g., Active Directory). If this is not possible and authentication is performed locally by the technical system, it must comply with the hospital’s identification and authentication standards (documentation available on request).
H.TEC.21	**Q**	**Authorization model** Access rights to data (configuration settings, user data, etc.) must be organized and configured based on application roles or business profiles, in such a way as to restrict “who can access what” (e.g., a radiology technician role would not have system configuration rights).

Reference	P / Q	Security measure
H.TEC.22	**Q**	**Protection of local data** In the biomedical field: in order to ensure the confidentiality of any personally identifiable medical data stored on the technical system, the system must encrypt such data.
2.3.6 Traceability		
H.TEC.23	**Q**	**Logging** Logging must trace all attempts to access data. The storage capacity for logging data must permit at least 6 months of conservation. The supplier must specify the format and the contents of logging data. Logs should contain, for example: date and time, user identity, action taken, affected data, result of the operation. Logs should be easy to use. For example, the system may provide a multi-criteria query function to search for accesses and other actions (by user, date, access type, etc.). Exporting logs to external media should not require interruption of the system's normal functioning.
2.3.7 Backups		
H.TEC.24	**Q**	**Data backups** Any data produced by the technical system that needs persistent storage (for a duration defined by the hospital) must be able to be backed up and restored. Such backups should preferably use the hospital's standard storage and backup methods, and in any case must not use simple local, removable media such as cassettes or USB discs, since these might easily be compromised or even stolen. The supplier must estimate the storage capacity required for data.
2.3.8 Maintenance		
H.TEC.25	**P**	**Confidentiality Agreement (NDA)** Establishing an access for remote maintenance of the technical system is subject to the supplier's acceptance and signature of the hospital's Confidentiality Agreement. ***(As an APPENDIX: Confidentiality Agreement, for signature)***
H.TEC.26	**P**	**Remote maintenance** Access for remote maintenance of the technical system must imperatively use the network services and standards for remote maintenance that are proposed and approved by the hospital. The establishment of other connections (by modem, Wi-Fi, mobile 3G+, or other) on the technical system is strictly prohibited: such devices must imperatively be disabled. Transmissions between the technical system and the remote maintenance operator must imperatively be encrypted. If communications transit via an intermediate third-party, it is recommended to also apply application-level encryption. Two-factor authentication is recommended; otherwise, the remote IP address must be fixed.

REFERENCE	P / Q	SECURITY MEASURE
H.TEC.27	P	**Outbound remote maintenance connections** Outbound remote maintenance connections on Internet are restricted to only the network addresses (restricted range of IP addresses) defined beforehand by the supplier. In addition, the supplier must commit to notifying in advance any change of these addresses.
H.TEC.28	Q	**Authorizations in remote maintenance mode** Except in emergency situations, the supplier's technicians who carry out onsite or remote maintenance, are not authorized to access personally identifiable information (notably, patient data).
H.TEC.29	P	**Destruction of data media** If a maintenance operation necessitates the replacement of storage media (e.g., a hard drive) containing personally identifiable information (notably, patient data), the supplier must imperatively give the original media to the hospital: the ISD support team will then apply standard procedures to ensure destruction of the media.
2.3.9 Compliance		
H.TEC.30	P	**License management** It is the supplier's responsibility to acquire and concede to the hospital all licenses necessary for operation of the technical system. This includes the "right to use" for software packages, hardware components, and all associated software (operating system, algorithms, security software, network software, database software, systems software, file transfer software, remote maintenance software, application software, etc.).
H.TEC.31	P	**Security audits** The supplier acknowledges the right of the hospital to organize security audits and penetration testing of the technical system.
2.3.10 Data management		
H.TEC.32	Q	**Monitoring of transmission failures** If the technical system uploads data (whether technical or biomedical) towards a centralized system on the hospital's network (for example, upload of images to a PACS), any transmission failures must be immediately reported to the user (for example, via a simple visual alarm), as well as to the ISD support team via an appropriate communication method (e.g., E-mail, SNMP Trap, etc.) approved by the ISD.
H.TEC.33	Q	**Monitoring of data storage** The supplier must implement an alarm mechanism that anticipates possible saturation of the local hard drives (for example, in the event of transmission failures).

A. Appendix A (informative) – Checklist template

NB: This template is an example: each hospital is free to adapt it to its own procedures.

A.1 Procedure to be followed by the supplier

1. For each requirement, the supplier must indicate if the technical system is compliant with the requirement (by indicating “YES” or “NO”), and specify:
    a. if **compliant,** what principles or features provide compliance (for some requirements, the type of information expected is indicated in the checklist);
    b. if **non-compliant,** what are the reasons for not meeting the requirement, and what compensatory security measures are foreseen or recommended in order to limit the risk.
2. The supplier must complete the checklist for the exact system that is planned to be installed at the hospital in the context of the current project. (If it is judged pertinent to mention foreseen future developments, the supplier should clearly distinguish these as such.)
3. The supplier’s commitment to the contents of the completed checklist is attested by the signature of an authorized representative.
4. In the event of any changes to the system that imply changes to the contents of the checklist, an updated version of the completed checklist must be submitted to the hospital for validation.
5. Even if the proposed technical system is identical to an existing installed system, this does not justify omission of the checklist, which remains necessary to obtain authorization for the network connection.

A.2 Identification of the technical system

TECHNICAL SYSTEM	
Manufacturer, brand	
Model, version, other identifiers	
Type of equipment, brief description	
Supplier (company name, contact details)	

A.3 Security requirements – checklist

Requirement	P/Q	Compliant? YES/NO	Comment or justification of non-conformity (with possible references to additional documents)
H.TEC.1	P		
H.TEC.2	P		
H.TEC.3	Q		
H.TEC.4	Q		
H.TEC.5	Q		
H.TEC.6	Q		
H.TEC.7	P		
H.TEC.8	P		< Specify the method and who is responsible for implementation >
H.TEC.9	P		< Confirm that the update will be automatic and daily >
H.TEC.10	P		< Specify whether port blocking is physical or logical >
H.TEC.11	Q		
H.TEC.12	Q		

H.TEC.13	**P**		
H.TEC.14	**P**		
H.TEC.15	**P**		< Specify the algorithm (AES, DES, …) and key length >
H.TEC.16	**P**		
H.TEC.17	**Q**		< Indicate points of compliance: a, b, c, d, e, f, g >
H.TEC.18	**P**		< Specify the privilege level of accounts used >
H.TEC.19	**Q**		< Specify whether authentication is central (AD) or local >
H.TEC.20	**Q**		< Specify the number and types of profiles >
H.TEC.21	**Q**		
H.TEC.22	**Q**		
H.TEC.23	**Q**		
H.TEC.24	**Q**		< Specify the proposed backup method >
H.TEC.25	**P**		
H.TEC.26	**P**		
H.TEC.27	**P**		
H.TEC.28	**Q**		
H.TEC.29	**P**		
H.TEC.30	**P**		
H.TEC.31	**P**		
H.TEC.32	**Q**		
H.TEC.33	**Q**		

A.4 Signatures

SUPPLIER		
Company:		Signature:
Name:		
Job function:		
Place and Date:		

HOSPITAL		
Institution:		Note:
Service:		
Name:		
Job function:		Signature:
Place and Date:		

HOSPITAL		
Institution:		Note:
Service:		
Name:		
Job function:		Signature:
Place and Date:		

HOSPITAL		
Institution:		Note:
Service:		
Name:		
Job function:		Signature:
Place and Date:		