DIE SPITÄLER DER SCHWEIZ
LES HÔPITAUX DE SUISSE
GLI OSPEDALI SVIZZERI

Informationssicherheit und Datenschutz

Anforderungen zur ICT-Sicherheit von Fremdsystemen

Version 1.2

H+: Schweizer Spitäler, Kliniken und Pflegeinstitutionen
H+: Hôpitaux, cliniques et institutions de soins suisses
H+: Gli Ospedali, le cliniche e gli istituti di cura svizzeri

Geschäftsstelle · Lorrainestrasse 4A · 3013 Bern
T 031 335 11 11 · F 031 335 11 70
geschaeftsstelle@hplus.ch · www.hplus.ch

Inhaltsübersicht

1 Einleitung

Die ICT-Systemumgebung eines Spitals umfasst nebst der von der internen ICT beschafften und verwalteten Systeme, bestehend aus Plattform (Hardware und Betriebssystem) und Applikationen eine Vielzahl von Systemen, welche anderweitig beschafft und ganz oder teilweise durch Dritte integriert oder betrieben werden. Solche Systeme werden summarisch als Fremdsysteme bezeichnet.

Typischerweise handelt es sich bei Fremdsystemen um Systeme der Medizin- oder Gebäudetechnik. Ziel des vorliegenden Dokumentes ist es, mittels geeigneter Massnahmen die Betriebssicherheit der Fremdsysteme und daraus folgend die Patientensicherheit sicherzustellen, die Privatsphäre von Patienten und Mitarbeitenden zu schützen, die Fremdsysteme angemessen gegenüber ICT-Risiken sowie im Speziellen Cyberangriffen zu schützen sowie andere Systeme im Netzwerkverbund des Spitals gegenüber den Fremdsystemen zu schützen.

1.1 Gegenstand und Zweck

Das vorliegende Dokument beschreibt die minimalen ICT-Sicherheitsanforderungen von Fremdsystemen für die Phasen Beschaffung, Integration und Betrieb. Im Speziellen wird dabei auf medizintechnische Systeme eingegangen. Die Anforderungen gemäss Katalog im Kapitel 2 sind bei Beschaffungen von Fremdsystemen im Rahmen von Projekten, Gross- und Kleininvestitionen sowie bei der Inbetriebnahme und dem Betrieb von Fremdsystemen zu berücksichtigen.

Das vorliegende Dokument regelt explizit nur den ICT-Teil eines Fremdsystems und keinesfalls den fachlichen Teil, welcher keine ICT-Relevanz hat.

1.2 Geltungsbereich und Verbindlichkeit

Das vorliegende Dokument hat verbindlichen Charakter für alle Fremdsysteme und insbesondere alle medizintechnischen Systeme inkl. deren Anwendungen, welche in die lokalen Netzwerkinfrastrukturen des Spitals integriert werden.

Als Entscheidungsgrundlage wird das Vorhandensein einer Netzwerkkonnektivität definiert, welche mit dem Netzwerkverbund des Spitals aktiv verbunden ist.

Der Geltungsbereich umfasst dabei die Phasen der Beschaffung, Inbetriebnahme und Betrieb. Die Handhabung in den drei Phasen ist im Anhang A erläutert.

Angesprochen sind folgende Kreise:

- Dienstleister (z.B. Anbieter/Lieferanten, Integratoren) im Rahmen der Beschaffung von Fremdsystemen.
- Interne Mitarbeitende, welche im Rahmen der Beschaffung, Integration und des Betriebs von Fremdsystemen verantwortlich, entscheidungsbefugt oder anderweitig involviert sind, namentlich Investitions- und Projektleiter.

Die in diesem Dokument genannten Anhänge B bis H werden von den Spitälern im Rahmen des Erwerbs von Fremdsystemen zur Verfügung gestellt. Der Inhalt ist jeweils pro Spital unterschiedlich.

2 Anforderungskatalog

2.1 Dokumentation

Nr.	Anforderung	Kategorie
SEC-1.1	**Architekturdokumentation** Der Anbieter dokumentiert die Architektur des Systems resp. der Gesamtlösung. Die Architekturdokumentation umfasst dabei mindestens: ■ Gesamtübersicht aller der Lösung zugehörigen Systeme, Applikationen und Komponenten. ■ Schnittstellen (in der Form Quelle, Ziel, Protokoll(e) und Zweck) zu bereits vorhandenen internen (Spital) und externen Systemen. ■ Anderweitige Datenkommunikationen zu bereits bestehenden internen (Spital) und externen Systeme (z.B. Übermittlung von Verbrauchsdaten, Fernzugriffe, Monitoring). Der Anbieter ist aufgefordert, dem Spital während der gesamten Lebensdauer wesentliche die Architekturdokumentation betreffende Änderungen unaufgefordert mitzuteilen.	☑ obligatorisch ☐ gewünscht
SEC-1.2	**Technische Betriebsdokumentation** Der Anbieter dokumentiert die Systeme und deren Konfiguration in der Form: System-Bezeichnung, eingesetztes Betriebssystem, installierte Applikationen mit Angabe der Versionsnummer, Dienste und Accounts (insbesondere jene mit privilegierter Berechtigung), Hardware Seriennummern und MAC Adressen. Der Anbieter führt die technische Betriebsdokumentation über den gesamten Lebenszyklus des Systems in Zusammenarbeit mit dem Spital weiter oder übergibt sie in die Verantwortung des Spitals zur Weiterführung. Die technische Betriebsdokumentation umfasst dabei mindestens: ■ Gesamtübersicht aller der Lösung zugehörigen Systeme (z.B. Betriebssystem, Applikationen, COTS[1]/SOUP[2]) und jede andere wesentliche Komponente, welche für einen sicheren Betrieb notwendig sind. ■ Installation, Konfiguration, Betrieb und Wartung (vor Ort und/oder aus der Ferne), Beschreibung aller der Lösung zugehörigen Systeme, Applikationen und Komponenten, inklusive deren Herausgeber, Produktlizenz und Versionsnummer. ■ Port-Matrix im folgenden Format: Quelle, Ziel, Netzwerkprotokoll, Port sowie Zweck. Die technische Betriebsdokumentation ist Teil der Abnahme.	☑ obligatorisch ☐ gewünscht
SEC-1.3	**Operative Betriebsdokumentation** Ein System wird durch den Anbieter gemeinsam mit der zuständigen Fachstelle des Spitals dokumentiert. Diese operative Betriebsdokumentation umfasst dabei mindestens: ■ Die internen (Spital) und externen (Anbieter) Verantwortlichkeiten und Kontakte sowie die zugehörigen Wartungs-, Support- und Administrationsprozesse. ■ Die Benutzerdokumentation der Lösung (Benutzerhandbuch). Der Anbieter ist aufgefordert, dem Spital während der gesamten Lebensdauer wesentliche die operative Betriebsdokumentation betreffende Änderungen unaufgefordert mitzuteilen. Die operative Betriebsdokumentation ist Teil der Abnahme.	☑ obligatorisch ☐ gewünscht
SEC-1.4	**Sicherheitsdokumentation** Diese Sicherheitsdokumentation umfasst dabei mindestens: ■ Sicherheit und Informationsschutz Unternehmenspolitik. ■ ISO 27'001 Zertifikat, falls zutreffend. ■ IEC 62'304 Zertifikat, falls zutreffend. ■ Weitere Zertifizierungen im Bereich Sicherheit und Datenschutz.	☑ obligatorisch ☐ gewünscht

[1] COTS : Commercial off-the-shelf

[2] SOUP : Software of unknown provenance

Nr.	Anforderung	Kategorie
	▪ Das Dokument „Manufacturer Disclosure for Medical Device Security“ (https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx) liegt vor. ▪ CE-Zertifikat der Lösung. ▪ Umsetzung von Empfehlungen und best-Practices im Sicherheit und Datenschutz (z.B. ISO 27018). Der Anbieter ist aufgefordert, dem Spital während der gesamten Lebensdauer wesentliche die Sicherheitsdokumentation betreffende Änderungen unaufgefordert mitzuteilen.	
SEC-1.5	**Manufacturer Disclosure for Medical Device Security** Das Dokument „Manufacturer Disclosure for Medical Device Security“ (http://www.himss.org/resourcelibrary/MDS2) liegt vor.	☑ obligatorisch ☐ gewünscht
	Ausnahmen: Das Kriterium SEC-1.5 ist nur für medizintechnische Systeme relevant.	
SEC-1.6	**Abnahme und Inbetriebnahme** Ein Fremdsystem darf erst nach der Abnahme durch den Fachbereich, die Supportabteilung (z.B. Spitaltechnik, Medizintechnik) und die ICT produktiv in Betrieb genommen werden. Die Abnahme ist schriftlich zu protokollieren.	☑ obligatorisch ☐ gewünscht

2.2 Grundkonfiguration

Nr.	Anforderung	Kategorie
SEC-2.1	**Unterstützte Plattformen und Betriebssysteme** Der Anbieter teilt mit, ob das Spital die Verantwortung für Administration und Betrieb der Lösung teilweise oder total zu übernehmen hat (siehe auch SEC 1-3). Gegebenenfalls basiert die Lösung vollumfänglich auf vom Spital unterstützten Plattformen und Betriebssystemen gemäss Anhang B.	☑ obligatorisch ☐ gewünscht
SEC-2.2	**Veraltetes Betriebssystem** Der Einsatz vom Hersteller nicht mehr unterstützten Betriebssystemen ist nicht zulässig. Der Anbieter präzisiert, ob das in der angebotenen Lösung verwendete Betriebssystem vom Hersteller unterstützt wird, unter Angabe des «End-of-Support» Datums. Falls das «End-of-Support» Datum in die vorgesehene Lebensdauer der Lösung fällt, zeigt der Anbieter den Upgrade-Pfad inklusive allfälliger Kosten im Detail auf.	☑ obligatorisch ☐ gewünscht
SEC-2.3	**Lebenszyklus der integrierten Software-Produkte** Der Anbieter verpflichtet sich für alle integrierten Software-Produkte (z.B. Betriebssystem, Datenbank, COTS/SOUP): ▪ Die vom Softwarelieferanten veröffentlichten Updates und Versionsupgrades zeitnah zu installieren. ▪ Die ICT umgehend zu informieren, falls er der Evolution der integrierten Software nicht mehr folgt, und dies unabhängig von der Lebensdauer des Gerätes. Die Gründe hierfür müssen genannt werden. ▪ Für Microsoft Windows: Den jeweils aktuellen «Current Branch for Business» und «Deferred Channel», respektive «Semi-Annual Channel» und «Long Term Servicing Channel» zu unterstützen. ▪ Für Microsoft Office-Produkte: die Version "On Premise" oder die Office 365 "Cloud" - Version.	☐ obligatorisch ☑ gewünscht
SEC-2.4	**Minimierung der Systemexposition** Um die System-Exposition zu minimieren, werden folgende Anforderungen erfüllt: ▪ Internetzugang ist gesperrt. Andernfalls müssen die Zugriffe auf das Internet beschrieben werden. ▪ Installation nur von notwendigen Software-Paketen und Diensten des Betriebssystems	☑ obligatorisch ☐ gewünscht

Nr.	Anforderung	Kategorie
	■ Deinstallation resp. Deaktivierung aller nicht notwendiger Software-Paketen und Netzwerk-Diensten ■ Installation einer lokalen Firewall, welche nur die Erreichbarkeit von vordefinierten Netzwerk-Ports erlaubt ■ Deaktivierung der USB-Ports sowie anderweitiger Anschlussmöglichkeiten für Wechselmedien ■ Deaktivierung der Funktionen «AutoRun/AutoPlay»	
	Ausnahmen: Abgesehen von dem Punkt über den Internetzugang, ist das Kriterium SEC-2.4 nicht relevant bei reinen Applikationslösungen. Die Nutzung der USB-Schnittstelle für Dongles zu Lizenzierungs- und Authentisierungszwecken ist zulässig; in diesem Fall entfällt die Deaktivierung der USB-Ports.	
SEC-2.5	**Technologien mit hohem Cyberrisiko** Das Spital strebt an, Technologien mit hohem Cyberrisiko zu eliminieren. Der Anbieter präzisiert, ob eine der vom Spital als Risiko klassifizierte Technologie Teil der Lösung ist. Die Liste der Risiko-Technologien sind im Anhang C aufgeführt. Der Anbieter schlägt gegebenenfalls eine alternative Technologie vorschlagen. Falls keine Alternativen möglich ist, muss folgendes präzisiert werden: ■ Verwendungszweck der Lösung, welche diese Technologien benötigen. ■ Erläuterung, weshalb keine Alternative in Frage kommt. ■ Plan und Frist für den Ersatz dieser Technologien in der betroffenen Lösungsproduktlinie.	☐ obligatorisch ☑ gewünscht
SEC-2.6	**Release-Management** Zum Auslieferungszeitpunkt des Systems muss für jede Applikation die jeweils aktuellste vom Hersteller freigegebene Version installiert sein.	☐ obligatorisch ☑ gewünscht
	Hinweis: Das Falls keine Möglichkeit besteht, die aktuellste freigegebene Version zu installierenden, kann die ICT veranlassen, die Lösung vom Netzwerk zu isolieren. Diesen Umstand kann sie in die Berechnung der TCO einbeziehen, mit Auswirkungen auf die Bewertung des Angebots.	
SEC-2.7	**Security-Management** Der Prozess zur Handhabung von sicherheitsrelevanten Aktualisierungen (Securitypatches, -updates und -fixes) orientiert sich an den Securitybulletins der jeweiligen Hersteller. Dies betrifft sowohl Betriebssystem als auch Applikationen. Der Anbieter kommuniziert auftretende Sicherheitslücken, Mängel oder Fehlfunktionen innert 30 Kalendertagen und stellt sicher, dass vom Hersteller (auch Dritthersteller wie z.B. Microsoft) bereitgestellte Aktualisierungen spätestens 60 Kalendertagen nach Veröffentlichung des Securitybulletins des Herstellers installiert resp. für die Installation durch das Spital freigegeben wird. Bei einer Risikosituation (z. B. Wannacry) muss dieser Zeitraum entsprechend den Anforderungen des Spitals verkürzt werden.	☐ obligatorisch ☑ gewünscht
	Hinweis: Bei reinen Applikationslösungen bezieht sich das Kriterium SEC-2.7 nur auf die Applikation selber.	
	Hinweis: Das Falls keine Möglichkeit besteht, die aktuellste freigegebene Version zu installierenden, kann die ICT veranlassen, die Lösung vom Netzwerk zu isolieren. Diesen Umstand kann sie in die Berechnung der TCO einbeziehen, mit Auswirkungen auf die Bewertung des Angebots.	
SEC-2.8	**Betriebssicherheit der Lösung** Der Anbieter gewährleistet zu jeder Zeit die Betriebssicherheit der Lösung während ihrer Lebensdauer im Spital. Falls es dem Anbieter nicht möglich ist: ■ Dem Zyklus der Software-Upgrades zu folgen (siehe SEC-2.3) und/oder ■ Innerhalb von 60 Kalendertagen die letzten Sicherheits-Patches und/oder Software-Updates zu validieren und installieren (siehe SEC-2.7) ist er aufgefordert, die daraus resultierenden Risikoszenarien zu dokumentieren. Der Anbieter dokumentiert mögliche Risikoszenarien, in denen er die potenziellen Auswirkungen auf das Spital hinsichtlich der folgenden Punkte aufzeigt: ■ Sicherheit der medizinischen Versorgung.	☐ obligatorisch ☑ gewünscht

Nr.	Anforderung	Kategorie
	▪ Sicherheit der Daten von Patienten und/oder Mitarbeitenden ▪ Physische Sicherheit der Patienten/Mitarbeitenden ▪ Gesetzeskonformität.	
SEC-2.9	**Verschlüsselungsmechanismen** Verschlüsselungsmechanismen und Wahl der Eigenschaften (z.B. Schlüssellänge) erfolgen nach Anforderung der zuständigen Referenzstellen (z.B. BSI, NIST) .	☑ obligatorisch ☐ gewünscht

2.3 Schutz vor Schadsoftware

Nr.	Anforderung	Kategorie
SEC-3.1	**Schadsoftware-Scanner** Ein Schadsoftware-Scanner ist auf allen Kernsystemen, Umsystemen und Clientsystemen der Lösung installiert. Ein Mechanismus des Typs «Application Whitelisting», welcher die Ausführung von nicht erlaubter Software blockiert, wird ebenfalls als akzeptabel betrachtet. Ausschlüsse der Schadsoftware-Prüfung sind zulässig, pro System zu definieren und dokumentieren. Wenn der Anbieter keinen der oben beschriebenen Mechanismen vorschlägt, muss er die Gründe rechtfertigen und die damit verbundenen Risikoszenarien präzisieren. Führt der Einsatz eines Virenscanners zu einer Verletzung der CE-Konformität, dann ist dies auszuweisen.	☑ obligatorisch ☐ gewünscht
SEC-3.2	**Regelmässigkeit der Prüfungen auf Schadsoftware** Die Prüfung durch den Schadsoftware-Scanner erfolgt regelmässig. Eine Vollprüfung erfolgt mindestens wöchentlich. Die Resultate der Prüfungen werden dem Spital auf Anfrage zur Verfügung gestellt. Entdeckte Schadsoftware sind dem Spital zu melden.	☑ obligatorisch ☐ gewünscht
SEC-3.3	**Aktualisierung der Schadsoftware und der Signaturen** Der eingesetzte Schadsoftware-Scanner wird regelmässig, mindestens aber täglich mit Signaturen und Versionen aktualisiert.	☑ obligatorisch ☐ gewünscht
SEC-3.4	**Standard Schadsoftware-Scanner des Unternehmens** Der Standard des Spitals gemäss Beschreibung in Anhang D wird eingehalten. Die Aktualisierung der Signaturen und Versionen erfolgt von den zentralen Systemen des Spitals.	☐ obligatorisch ☑ gewünscht
Ausnahmen: Die Kriterien SEC-3.1 bis SEC-3.4 sind nicht relevant bei reinen Applikationslösungen.		

2.4 Netzwerkzugang

Nr.	Anforderung	Kategorie
SEC-4.1	**Sichere Verbindungsprotokolle im Intranet** Für jegliche Kommunikationen im Intranet werden sichere/verschlüsselte Verbindungsprotokolle (SSH, SFTP, TLS, etc.) verwendet. Abweichungen sind zu nennen.	☐ obligatorisch ☑ gewünscht
SEC-4.2	**Sichere Verbindungsprotokolle ins Internet** Für jegliche Kommunikationen ins Internet werden sichere/verschlüsselte Verbindungsprotokolle (SSH, SFTP, TLS, etc.) verwendet.	☑ obligatorisch ☐ gewünscht
SEC-4.3	**Routingfunktionalitäten** Das System erbringt keine Bridging-, Routing- oder anderweitige Forward-Funktion für andere Netzwerksegmente. Entsprechende Funktionen sind zu deaktivieren.	☑ obligatorisch ☐ gewünscht

Nr.	Anforderung	Kategorie
SEC-4.4	**Netzwerkadressierungen** Netzwerkadressierungen werden vom Spital vorgegeben oder in Rücksprache mit dem Spital definiert.	☑ obligatorisch ☐ gewünscht
SEC-4.5	**Drahtgebundene Kommunikationsverbindungen** Für drahtgebundene Kommunikationsverbindungen werden ausschliesslich die Netzwerkkomponenten des Spitals genutzt gemäss Anhang E.	☑ obligatorisch ☐ gewünscht
SEC-4.6	**Drahtlose Kommunikationsverbindungen (WLAN)** Für drahtlose Kommunikationsverbindungen werden ausschliesslich die Netzwerkkomponenten des Spitals genutzt gemäss Anhang E. Für den Netzwerkzugang wird eine Authentisierung über WPA2 Enterprise / EAP-TLS vorausgesetzt. Die dazu benötigten Zertifikate werden des Spitals ausgestellt.	☑ obligatorisch ☐ gewünscht
SEC-4.7	**Ausgehende Verbindungen ins Internet** Ausgehende Verbindungen über das Internet dürfen nur auf definierte IP-Adressen des Dienstleisters erfolgen. Ein direkter Zugriff von internen Systemen auf Internetsysteme ist nicht zulässig und wird zwingend über ein DMZ-System geführt.	☐ obligatorisch ☑ gewünscht
SEC-4.8	**Netzwerk-Authentisierung (Network Access Control)** Die Lösung unterstützt Methoden zur Netzwerk-Authentisierung IEEE 802.1x. Gegebenenfalls bietet der Anbieter einen alternativen Mechanismus zur Netzwerk-Authentisierung auf einem vergleichbaren Sicherheitsniveau an.	☐ obligatorisch ☑ gewünscht
SEC-4.9	**Synchronisierung der Systemzeiten** Die Lösung unterstützt die Synchronisierung der Systemzeit über das Netzwerkprotokoll NTP.	☑ obligatorisch ☐ gewünscht
Ausnahmen: Die Kriterien SEC-4.3 bis SEC-4.6 sowie SEC-4.8 bis SEC-4.9 sind nicht relevant bei reinen Applikationslösungen.		

2.5 Zugriffsregelungen

Nr.	Anforderung	Kategorie
SEC-5.1	**Passwortregeln** Lokale und Generische Benutzerkontos, im Speziellen administrative Benutzerkontos sowie solche, über welche der Zugriff auf schützenswerte Informationen möglich ist, namentlich Personen- und Patientendaten, sind über Passwörter geschützt. Die Passwortregeln des Spitals sind in Anhang F ersichtlich.	☑ obligatorisch ☐ gewünscht
SEC-5.2	**Passwortwechsel** Lokale und Standard/Default-Passwörter müssen vor produktiver Inbetriebnahme geändert werden. Eingesetzte Passwörter dürfen bei anderen Kunden nicht zum Einsatz kommen. Besteht die Möglichkeit, dass unberechtigte Dritte Kenntnis über solche Passwörter erlangen, dann ist dies dem Spital anzuzeigen und die Passwörter sind umgehend zu ändern.	☑ obligatorisch ☐ gewünscht
	Hinweis: Das Kriterium SEC-5.2 setzt keine technische Umsetzung voraus sondern kann auch organisatorisch erfüllt werden.	
SEC-5.3	**Hinterlegung des Passwortes bei nur einer Rolle** Falls das Gerät pro Rolle nur einen Rolleninhaber zulässt, wird das zugehörige Passwort im Spital hinterlegt.	☑ obligatorisch ☐ gewünscht
SEC-5.4	**Sperrung von Benutzerkontos nach Falscheingaben** Ein Benutzerkonto ist nach drei Falscheingaben zu sperren. Eine automatische Entsperrung erfolgt nach einer konfigurierbaren Zeitspanne, die auf eine in Anhang F definierte Zeit gesetzt sein muss.	☐ obligatorisch ☑ gewünscht

Nr.	Anforderung	Kategorie
SEC-5.5	**Sperrung der Benutzersession bei Inaktivität** Nach einer in Anhang F definierten Benutzerinaktivität wird die Benutzersession gesperrt, und eine erneute Anmeldung ist erforderlich.	☐ obligatorisch ☑ gewünscht
SEC-5.6	**Separierung von technischen Benutzerkonten und Diensten** Technische Benutzerkonten separieren Dienste und Anwendungen. Diese müssen mit minimalen Rechten versehen sein.	☑ obligatorisch ☐ gewünscht
SEC-5.7	**Nutzung von lokalen Administratorenkonten** Lokale Administratorenkonten dürfen nur für Wartung und Konfiguration verwendet werden. Die betriebliche Nutzung erfolgt über persönliche Benutzerkennungen.	☑ obligatorisch ☐ gewünscht
SEC-5.8	**Rollenbasierte Autorisierung** Die Autorisierung erfolgt rollenbasiert. Die Rollen sind mindestens teilweise frei konfigurierbar.	☐ obligatorisch ☑ gewünscht
SEC-5.9	**Zentrales Management über Active Directory** Systeme mit einem Windows Betriebssystem werden in das Active Directory des Unternehmens integriert. Dabei werden folgende Kriterien automatisch abgedeckt: ■ Sperrung von Benutzerkontos nach Falscheingaben (SEC-5.4) ■ Sperrung der Benutzersession bei Inaktivität (SEC-5.5) ■ Nutzung von lokalen Administratorenkonten (SEC-5.7)	☐ obligatorisch ☑ gewünscht

2.6 Protokollierung und Nachvollziehbarkeit

Nr.	Anforderung	Kategorie
SEC-6.1	**Protokollierung** Alle Aktionen auf Systemen und Applikationen, namentlich An- und Abmeldevorgänge sowie Fehlersituationen, werden nachvollziehbar protokolliert.	☑ obligatorisch ☐ gewünscht
SEC-6.2	**Audittrail** Die Protokollierung zeichnet alle Zugriffe auf technische, personenbezogene oder besonders schützenswerte personenbezogene Daten im Sinne eines Audit-Trails auf.	☐ obligatorisch ☑ gewünscht
SEC-6.3	**Manipulationsschutz von Protokolldaten** Auf den Systemen zwischenzeitlich oder dauerhaft gespeicherte Protokolldaten sind vor Manipulation und unberechtigtem Zugriff geschützt.	☐ obligatorisch ☑ gewünscht
SEC-6.4	**Weiterleitung von Protokolldaten** Protokolldaten können an einen zentralen Logserver weitergeleitet werden. Der Anbieter beschreibt die Möglichkeiten dazu (z.B. via Syslog).	☐ obligatorisch ☑ gewünscht

2.7 Datensicherheit

Nr.	Anforderung	Kategorie
SEC-7.1	**Datenbearbeitung** Der Anbieter zeigt auf, welche personenbezogenen und anderweitig schützenswerte Daten von der Lösung bearbeitet und gespeichert werden: ■ Aufstellung der Daten mit der entsprechenden Begründung in Bezug auf die Verhältnismässigkeit und Zweckbindung. ■ Aufbewahrungsdauer von dauerhaft gespeicherten dieser Daten. ■ Nennung der Länder, in welche diese Daten potenziell exportiert werden könnten.	☑ obligatorisch ☐ gewünscht

Nr.	Anforderung	Kategorie
SEC-7.2	**Verschlüsselte Datenspeicherung** Die lokale Speicherung von personenbezogenen und anderweitig schützenswerten Daten erfolgt verschlüsselt.	☐ obligatorisch ☑ gewünscht
SEC-7.3	**Datenübermittlung** Die Übermittlung personenbezogenen und anderweitig schützenswerte Daten zu Drittsystemen ausserhalb des Unternehmens erfolgt ausschliesslich unter folgenden Rahmenbedingungen: ■ Die Daten werden ausschliesslich verschlüsselt übermittelt. ■ Personenbezogene Daten werden ausschliesslich anonymisiert oder pseudonymisiert übermittelt.	☐ obligatorisch ☑ gewünscht
SEC-7.4	**Lebenszyklus der Daten** Der Lebenszyklus (Erhebung, Bearbeitung, Archivierung und Löschung) der Daten ist dokumentiert und berücksichtigt interne und externe Compliance-Vorgaben bezüglich der Aufbewahrungspflicht.	☐ obligatorisch ☑ gewünscht
SEC-7.5	**Datensicherung und -wiederherstellung** Der Anbieter gibt – für die technischen, personenbezogenen und sensiblen personenbezogenen Daten – eine Schätzung des Backupvolumens der Protokolldaten für eine Aufbewahrung von 10 Jahren liefern. Die Aufbewahrung der von der Lösung produzierte Daten muss die in der Schweiz und der Institution geltenden Normen erfüllen. Das Backup dieser Daten muss nach den Standard-Methoden und Prozessen des Spitals durchgeführt werden (siehe Anhang G). Auf keinen Fall dürfen hierzu lokale Festplatten oder Wechselmedium (z.B. USB Festplatte) eingesetzt werden.	☐ obligatorisch ☑ gewünscht
SEC-7.6	**Datenvernichtung** Werden Speichermedien ausgetauscht, so sind die Daten vorgängig zu löschen. Alternativ kann der Dienstleister die Datenträger sicher entsorgen. Dies hat er dem KSGR schriftlich zu belegen. Die physische Datenträgervernichtung erfolgt nach Norm DIN 66399 (Schutzklasse 2). Die sichere Datenlöschung nach Standard VSIT des Bundesamt für Sicherheit Deutschland (BSI) oder nach Standard DoD-5220.22-M (E).	☑ obligatorisch ☐ gewünscht

2.8 Wartung und Support

Nr.	Anforderung	Kategorie
SEC-8.1	**Standardprozess Fernzugriff** Der Fernzugriff erfolgt unter Nutzung der Standards des Spitals gemäss der Beschreibung im Anhang H. Weitere Verbindungsmöglichkeiten sind zu deaktivieren. Falls der Standard des Spitals für die Lösung nicht umgesetzt werden kann, muss der Anbieter die Gründe rechtfertigen und eine alternative Lösung mit vergleichbarem Sicherheitsniveau präsentieren.	☐ obligatorisch ☑ gewünscht
SEC-8.2	**Fernzugriff** Ein Fernzugriff auf Systeme des Unternehmens findet ausnahmslos in Erfüllung der folgenden Anforderungen statt: ■ Die Zugriffe erfolgen verschlüsselt. ■ Die Zugriffe werden revisionssicher aufgezeichnet. Darunter wird die Nachvollziehbarkeit verstanden, welche Person (wer) zu welcher Zeit (wann) auf welches System (wohin) zugegriffen hat. ■ Die Zugriffe werden mindestens einmal mittels einer persönlichen Benutzerkennung authentisiert, bevorzugt auf Systemen des Unternehmens. Sollte diese Authentisierung nicht auf Systemen des Unternehmens erfolgen so werden die Auditlogs dem Spital regelmässig und ohne Zutun des Unternehmens, mindestens aber auf Nachfrage des Spitals zur Verfügung gestellt.	☑ obligatorisch ☐ gewünscht
SEC-8.3	**Vorankündigung von Wartungsarbeiten**	☑ obligatorisch

Nr.	Anforderung	Kategorie
	Sämtliche Wartungsarbeiten durch den Dienstleister, ungeachtet dessen ob diese vor Ort oder per Fernzugriff erfolgen, sind der Fach- und der Supportabteilung voranzumelden. Sollten besondere Umstände sofortige Wartungsarbeiten erfordern so werden diese im Nachhinein innert 24h der Fach- und der Supportabteilung inkl. einer nachvollziehbaren Begründung der Dringlichkeit nachgemeldet.	☐ gewünscht

2.9 Integration

Nr.	Anforderung	Kategorie
SEC-9.1	**Überwachung von Übertragungsfehlern** Der Anbieter **muss** präzisieren, falls eine Dataübertragung von der Lösung auf ein zentralisiertes System des Spitals (e.g. PACS) vorgesehen ist, ob und in welcher Form ein Übertragungsfehler dem Benutzer und der ICT unverzüglich gemeldet wird. Wie kann detektiert werden, wenn z.B. ein bildgebendes System seine Daten nicht mehr an das Bildarchiv geliefert werden? (Schutz vor Datenverlust)	☐ obligatorisch ☐ gewünscht
SEC-9.2	**Datenaustausch** Der Anbieter muss präzisieren, ob die Lösung mit «*Web Services*» Funktionalitäten unterstützt wird. Der Anbieter liefert die technische Dokumentation der aufgeführten «*Web Services*». Der Anbieter muss aufzeigen, falls die Lösung diese Art von Datenaustausch nicht unterstützt, wie seine Lösung in eine SOA-Architektur eingebunden werden kann (e.g. mit Hilfe von Proxies). Der Anbieter **muss** präzisieren, falls keine Alternativen bestehen, ob die Unterstützung von «*Web Services*» auf seiner Lösung Produkt Roadmap aufgeführt ist und in welchem Zeitraum mit deren Verfügbarkeit gerechnet werden kann.	☐ obligatorisch ☐ gewünscht

2.10 Compliance

Nr.	Anforderung	Kategorie
SEC-10.1	**Vertragsvereinbarung** Der Einsatz von nicht mehr unterstützen Systeme (z.B. Betriebssystem) und Applikationen ist nicht zulässig. Dies inkludiert auch Applikationen oder Komponenten von Drittherstellern, welche für den Betrieb der Lösung relevant sind. Die Vertragsvereinbarung zwischen dem Spital und dem Anbieter hält fest, dass der Anbieter für die eingesetzten Systeme und Applikationen den vom Hersteller vorgegebenen Lebenszyklus einhält. Der Anbieter informiert das Spital, sobald eingesetzte Applikationen nicht mehr weiterentwickelt werden.	☑ obligatorisch ☐ gewünscht
SEC-10.1	**Datenschutzvereinbarung (NDA)** Eine Datenschutzvereinbarung nach Schweizer Recht wird ausgehandelt oder liegt als integrierter Teil der Vertragsvereinbarung vor. Bevorzugt wird dazu die Vorlage des Spitals.	☑ obligatorisch ☐ gewünscht
SEC-10.2	**Deklaration der Datenflüsse** Werden Daten an Dritte übermittelt (z.B. Verbrauchsdaten, zur Fehlererkennung oder Qualitätssicherung), sind diese detailliert zu erläutern in der Form: Zweck, Dateninhalt, Schutz der Vertraulichkeit bei Datenübertragung und Datenspeicherung.	☑ obligatorisch ☐ gewünscht

Nr.	Anforderung	Kategorie
SEC-10.2	**Datenspeicherung** Die Speicherung von personenbezogenen und anderweitig schützenswerten Daten erfolgt ausschliesslich in der Schweiz oder in einem Land mit einem angemessenen Datenschutzniveau. Relevant ist diesbezüglich die Länderliste des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB in der jeweils aktuellen Fassung. Als Stichdatum gilt das Datum des Angebots. Im Falle einer Datenspeicherung ausserhalb der Schweiz ist das Angebot der Datenspeicherung in der Schweiz als Option erwünscht. Der definitive Entscheid des Ortes der Datenspeicherung wird durch das Spital während der Beurteilungsphase gefällt.	☑ obligatorisch ☐ gewünscht
SEC-10.3	**Fernzugriff** Der Fernzugriff erfolgt vollumfänglich aus der Schweiz oder einem Land mit einem angemessenen Datenschutzniveau. Relevant ist die Länderliste des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB in der jeweils aktuellen Fassung. Als Stichdatum gilt das Datum des Fernzugriffs.	☑ obligatorisch ☐ gewünscht
SEC-10.4	**Lizenzierung** Der Anbieter ist für ordnungsgemässe Lizenzierung der von ihm ausgelieferten Komponenten verantwortlich. Der Anbieter stellt die uneingeschränkten Nutzungsrechte sicher und stellt Aktualisierungen aller Komponenten bei Bedarf sicher. Gegebenenfalls verpflichtet sich der Anbieter, einen Escrow-Vertrag abzuschliessen.	☑ obligatorisch ☐ gewünscht
SEC-10.5	**Penetrationtesting** Der Anbieter gewährt dem Spital das Recht, erforderliche Sicherheitsüberprüfungen (z.B. Security Audit, Penetrationtesting) eigenmächtig durchzuführen und gewährt dem Unternehmen resp. dem vom Spital Beauftragten uneingeschränkte Einsicht in die erforderlichen Unterlagen.	☑ obligatorisch ☐ gewünscht
SEC-10.6	**Netzautonomer Betrieb** Netzautonome Systeme können im Betriebsmodus (unter Last) für mindestens acht Stunden unabhängig betrieben werden.	☐ obligatorisch ☑ gewünscht

Anhang A Handhabung des Anforderungskatalogs

Der Anbieter muss zu allen Kriterien gemäss Katalog in Kapitel 2 Stellung beziehen, indem er das Beiblatt in Selbstdeklaration ausfüllt.

A.1 Phase

- **Beschaffung**
  Die Anforderungen gemäss Kapitel 2 sind für die Beschaffung eines Systems durch den Dienstleister zu berücksichtigen.

- **Inbetriebnahme**
  Die Anforderungen gemäss Kapitel 2 sind für die Inbetriebnahme eines Systems durch den Dienstleister zu berücksichtigen.

- **Betrieb**
  Die Anforderungen gemäss Kapitel 2 sind für den Betrieb eines Systems durch den Dienstleister zu berücksichtigen.

A.2 Kategorie

- **Obligatorisch**
  Obligatorische Anforderungen sind zwingend zu erfüllen. Das Nichterfüllen eines oder mehrerer obligatorischer Kriterien im Rahmen einer Beschaffung hat den Ausschluss des Angebots zur Folge.

  Zusätzlich zur direkten Erfüllung eines obligatorischen Kriteriums ist auch eine indirekte Erfüllung zulässig. Unter einer indirekten Erfüllung wird die Erfüllung unter Berücksichtigung zusätzlicher Massnahmen und Vorkehrungen verstanden. Diese sind im Beiblatt detailliert zu erläutern.

- **Gewünscht**
  Gewünschte Anforderungen dienen in der Summe der Qualifizierung des Systems, welche im Rahmen von Ausschreibungen Berücksichtigung findet.

A.3 Erfüllung

- **Ja**
  Die Anforderung wird erfüllt.

- **Nein**
  Die Anforderung wird nicht erfüllt.

- **Nicht relevant**
  Die Anforderung ist nicht anwendbar oder nicht zutreffend. Diese Erfüllung ist nur bei Kriterien zulässig, für welche im Anforderungskatalog Ausnahmen definiert sind und wenn die beschriebenen Bedingungen für eine Ausnahme erfüllt werden. Die Erfüllung ist in jedem Fall detailliert und nachvollziehbar zu beschreiben.