

ICT Integrationsvorgaben

Vorgaben für die ICT Integration von Gebäudetechnik und Medizintechnik Systemen

Autoren: Kantonsspital Baden
Amstein + Walthert Progress
Version: v03.00
Status: Freigegeben
Erstelldatum: 14. Dezember 2018
Revision: 24. Februar 2020

Inhaltsverzeichnis

Inhaltsverzeichnis	2
Änderungsverzeichnis	3
1 Einführung	4
1.1 Ziel des Dokuments	4
1.2 Zielpublikum	4
1.3 Ausnahmen	4
2 ICT Basisinfrastruktur	5
2.1 Netzwerkaufbau	5
2.2 Datacenter6	
3 Anforderungen	7
3.1 Systembeschreibung	7
3.2 Netzwerkerschliessung	7
3.3 Standard-Hardware	8
3.4 Systemsicherheit	9
3.5 Datenschutz	11
3.6 Management	11
3.7 Systemverfügbarkeit	12
3.8 Lieferobjekte	12
3.9 Dokumentation	13
Glossar	14
Impressum	15
Anhang	15
Anhang 1 – Vertraulichkeitsvereinbarung	15
Anhang 2 – Merkblatt Fernzugriff	15
Anhang 3 – Standardsoft- und -hardware	15

Änderungsverzeichnis

Datum	Version	Änderung / Bemerkung	Verantwortung
14.12.18	00.01	Erstellung Initialdokument Kapitelstruktur gemäss Workshop vom 6.12.18	AWP
Januar 19	00.02	Ergänzungen ICT Infrastruktur	HUG
11.02.19	00.03	Ergänzungen ICT Infrastruktur, Sicherheit und Strategie	MEN, HUG
26.02.19	00.04	Zusammenführung Arbeiten AWP und KSB	AWP
08.04.19	00.05	Textuelle Aufbereitung der Anforderungen	AWP
02.07.19	00.06	Revision zur finalen Besprechung	AWP
14.07.19	01.00	Version 1.0	AWP, KSB
28.10.19	01.01	Ergänzungen zu SQL Anforderungen	DLE
28.10.19	02.00	Version 2.0	KSB
24.02.20	02.01	Ergänzungen zu Netzwerkprotokolle	DLE
24.02.20	03.00	Version 3.0	KSB

1 Einführung

Das Kantonsspital Baden (KSB) betreibt auf dem gesamten Areal eine leistungsfähige, sichere und hochverfügbare ICT-Infrastruktur. Diese dient als stabile Grundlage für ein modernes, hochintegriertes Spital. Durch die gewählte Architektur können Sicherheit und Verfügbarkeit für alle Nutzer der ICT-Infrastruktur auf hohem Niveau sichergestellt werden.

Leistungsfähigkeit, Sicherheit und Verfügbarkeit können nur für alle Nutzer im gleichen Masse erreicht werden, wenn die gesamte ICT-Infrastruktur zentralisiert aufgebaut und verwaltet wird. Somit ist es unablässig, dass alle Systeme im gesamten Areal, welche IP-Dienste beziehen, gemäss den in diesem Dokument definierten Anforderungen in die zentrale ICT-Infrastruktur eingebunden und gesichert werden.

Die im Folgenden aufgelisteten Vorgaben werden durch die Informatikabteilung des KSB (KSB-ICT) als Betreiber der ICT-Infrastruktur durchgesetzt und die Erfüllung dieser im Rahmen der Angebotsbewertung geprüft und bewertet. Die Vorgaben gelten gleichwohl für alle netzwerkfähigen Geräte.

1.1 Ziel des Dokuments

Im ersten Teil des Dokuments wird die verfügbare ICT-Infrastruktur und deren Funktionalität beschrieben. Hier werden die für Anbieter von Techniksystemen (im Folgenden als Unternehmer bezeichnet) notwendigen Informationen und Rahmenbedingungen erläutert.

Im zweiten Teil werden die Anforderungen an die Systeme zur Integration in die ICT-Infrastruktur aufgelistet. Diese Anforderungen sollen eine klar definierte Planungsgrundlage schaffen und somit spätere Planungsänderungen und Mehraufwände vermeiden.

Der Unternehmer hat im Rahmen des Angebotes die Anforderungen zu bewerten und die für eine Prüfung durch die Bauherrin notwendigen Grundlagen beizulegen. Die Erfüllung der Anforderungen ermöglicht einen hohen gemeinsamen Standard bezüglich Datensicherheit und Datenschutz.

1.2 Zielpublikum

Dieses Dokument ist bestimmt für:

- Lieferanten im Rahmen von RFI/RFP zum Erwerb von neuen Produkten/Lösungen.
- Mitarbeitende des Spitals, welche für Akquisitionen oder Verträge verantwortlich sind.
- Mitarbeitende des Spitals, welche für Installation und Konfiguration von technischen Geräten und Lösungen verantwortlich sind.
- Betriebsprüfer und Auditoren.

1.3 Ausnahmen

In zwingenden Fällen, z.B. bei gesetzlichen Vorgaben, können die hier beschriebenen Vorgaben durch den zuständigen Fachplaner in Absprache mit der KSB-ICT angepasst werden. Diese müssen schriftlich dokumentiert werden.

2 ICT Basisinfrastruktur

Auf dem gesamten Areal des KSB wird ein modernes, leistungsfähiges, hochverfügbares ICT-Netzwerk zur Verfügung gestellt. Dieses ist so ausgelegt, dass es heutigen und zukünftigen Anforderungen des Spitalumfeldes gerecht wird und soll durch die KSB-ICT verwaltet werden. Die ICT-Basisinfrastruktur ist so aufgebaut, dass sie als sicher, zuverlässig und flexible Plattform für alle IP-fähigen Systeme genutzt werden kann. Dabei erfüllt es die Anforderungen von einschlägigen Normen und unterstützt alle gängigen IP-basierende Übertragungsprotokolle.

2.1 Netzwerkaufbau

2.1.1 Topologie

Das ICT-Netzwerk ist als Collapsed-Core aufgebaut. Entsprechend wird auf dem Areal auf eine Distribution-Ebene verzichtet und die Access-Switches direkt von den Core-Switches erschlossen. Die Access-Switches werden in den ICT-Etagenverteilern untergebracht. Zwischen Core-Switches und Access-Switches werden Singlemode-Fibers eingesetzt. Ab den Access-Switches werden die Endgeräte mittels UKV-Links angebunden. Dabei werden die Maximallängen eingehalten. Die beiden Core-Switches werden georedundant über DWDM ins MPLS und hiermit mit den beiden unabhängigen Rechenzentren verbunden.

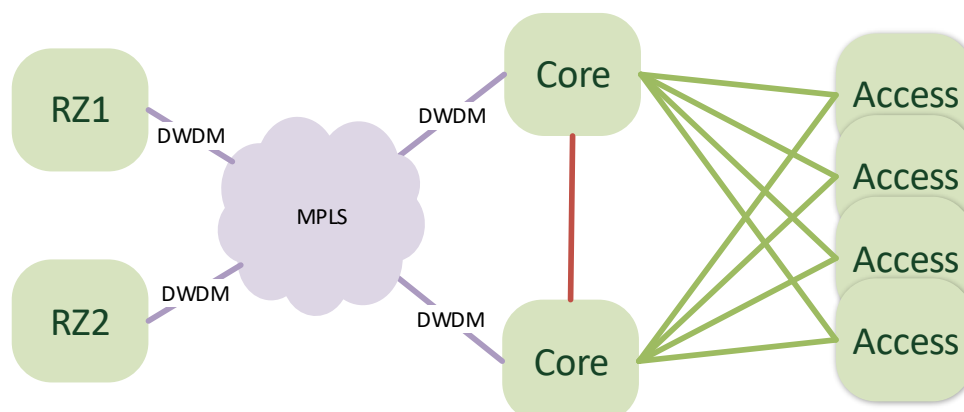


Abbildung 1: Grobe Skizze des redundanten Aufbaus der ICT-Basisinfrastruktur

2.1.2 Redundanz

Alle Verbindungen zwischen Core-Switches und Access-Switches sind redundant über unterschiedliche Wege ausgeführt. Die Anbindung an das hochverfügbare MPLS wird ab beiden Core-Switches ausgeführt. Eine redundante Querverbindung zwischen den Core-Switches garantiert auch beim Ausfall einer ausgehenden Verbindung die Verfügbarkeit aller Services.

Neben den physischen Verbindungen zwischen den Komponenten ist die Redundanz auch auf Komponentenebene gewährleistet. Dies um jegliche Single Points of Failure (SPOF) bis zu den Access-Switches auszuschliessen.

2.1.3 Wartung

Die Wartungen der ICT-Infrastruktur werden grundsätzlich im laufenden Betrieb durchgeführt. Es ist jedoch nicht ausgeschlossen, dass während eines Wartungsfensters einige Dienste nicht oder nur teilweise verfügbar sind. Bei Bedarf können Wartungsfenster frühzeitig bekanntgegeben werden.

2.1.4 Endpunkte/Übergabepunkte

Client-seitig werden die Endpunkte mittels Gigabit UKV-Kupferkabeln (der Kategorie 7a unter Verwendung von Kategorie 6a RJ-45 Steckerverbindern) erschlossen. Grundsätzlich werden Client-seitige Endgeräte nicht redundant an die Access-Switches erschlossen. Alle Client-seitigen Netzwerk-Ports verfügen über 1Gbit/s Bandbreite und PoE+ Spannungsversorgung. Für gewisse Bereiche bestehen Ausnahmen.

In den Datacenters können die Komponenten redundant über LC-Singlemode-Fiberanschlüsse oder RJ45-Steckverbinder erschlossen werden. Die Netzwerkanschlüsse verfügen wahlweise über 1Gbit/s oder 10Gbit/s Bandbreite. In den Datacenters wird keine PoE/PoE+ Spannungsversorgung angeboten.

Neben den kabelgebundenen Netzwerkanschlüssen sind alle Gebäude des KSB mit flächendeckenden WLAN ausgerüstet. Über WLAN-Verbindungen können nicht dieselben Serviceverfügbarkeiten wie über kabelgebundene Verbindungen garantiert werden. Deshalb sollen nur Geräte und Applikationen über das WLAN betrieben werden, für welche die Mobilität unabdingbar ist.

2.1.5 Netzwerksicherheit

Das gesamte Netzwerk erfüllt höchste Sicherheitsanforderungen. Entsprechend können nur Geräte mit zulässigen Autorisierungsmechanismen im Netzwerk freigegeben und betrieben werden. Unbekannten Geräte oder solchen die die Minimalanforderungen nicht erfüllen, wird der Zugang zur ICT-Infrastruktur verweigert.

2.1.6 Zentrale Netzwerkdienste

Alle notwendigen zentralen Dienste wie IP-Management (DHCP, DNS), Benutzerverzeichnis, Public Key Infrastruktur und NTP-Server, werden durch den Betreiber des ICT-Netzwerkes zur Verfügung gestellt.

Das ICT-Netzwerk ist entsprechend dem aktuellen Stand der Technik aufgebaut. QoS-Funktionen, Multicastfähigkeit sowie Zugriffsteuerung und Verwaltung wird dabei mittels zentraler Managementebene gesteuert.

2.2 Datacenter

Die KSB-ICT betreibt keine eigenen Datacenter auf dem Campus. Das primäre Datacenter wird in einem gemieteten Cage im Grossraum Zürich betrieben. Das sekundäre Datacenter befindet sich in einer Colocation von Avectris in Lupfig. Für zwingend lokal vorhandene Redundanzsysteme steht stark eingeschränkter Platz im Neubau zur Verfügung.

3 Anforderungen

Im Folgenden werden die minimal zu erfüllenden Anforderungen an die Systeme, welche in die ICT-Infrastruktur integriert werden sollen, beschrieben. Der Erfüllungsgrad dieser Anforderungen ist durch den Unternehmer im Angebot aufzuzeigen. Mit Eingabe bestätigt der Unternehmer, diese Vorgaben verstanden zu haben und diese einzuhalten.

3.1 Systembeschrieb

Alle Hardware- und Software-Komponenten müssen im Detail beschrieben werden. Dabei muss die Systemarchitektur inklusive aller einzusetzender Komponenten und die Konformität bezüglich der Anforderungen aufgezeigt werden.

Der Unternehmer hat die Anforderungen der Komponenten an das ICT-Netzwerk (Redundanzen, PoE Leistung, etc.) pro Gerät im Detail zu beschreiben. Es sind dabei alle notwendigen Kommunikations-verbindungen bezüglich Ports, Protokolle, Anforderungen an QoS, Multicast und weitere Netzwerk-Services auszuweisen.

Der Systembeschrieb muss dem Angebot beigelegt werden.

3.2 Netzwerkerschliessung

3.2.1 Grundsatz

Für jegliche IP-basierte Datenkommunikation ist zwingend die zur Verfügung gestellte ICT-Infrastruktur zu verwenden. Es dürfen keine eigenen ICT-Netzwerke oder Internetanbindungen (DSL, o.ä.) erstellt werden. Ausnahmen müssen durch den Anbieter begründet beantragt werden und bedürfen einer schriftlichen, unterzeichneten Bewilligung des Leiter ICT, Leiter ICT Infrastruktur und ICT-SIBE.

Es sind die durch die Bauherrin bereitgestellten zentralen Dienste und Benutzerverwaltungssysteme zu verwenden. Grundsätzlich sind jegliche Endgeräte über eine kabelgebundene Verbindung anzubinden. Die Notwendigkeit einer mobilen Anbindung über WLAN ist im Angebot darzulegen.

3.2.2 Netzwerkprotokolle

Über die zur Verfügung gestellte ICT-Infrastruktur können alle gängigen auf IP-basierenden offenen Netzwerkprotokolle übertragen werden. Alle Netzwerkanbindungen basieren auf dem Ethernet-Standard. Proprietäre Protokolle werden grundsätzlich nicht unterstützt.

3.2.3 Nutzung LAN

Jedem angeschlossenen Endgerät (kabelgebundene Verbindung) wird ein einzelner Netzwerk-Port zugewiesen. An jedem Netzwerk-Port darf jeweils nur ein Gerät angeschlossen werden. Zusätzliche Netzwerkkomponenten (Router, Switches, Access-Points, etc.) dürfen nicht installiert werden.

3.2.4 Nutzung WLAN

Für die mit WLAN eingebunden Geräte sind das Roaming-Verhalten, die Sende- und Empfangsleistung sowie die Antennencharakteristik im Angebot auszuweisen. Die Geräte sollen Funktionen zur Verbesserung des Roaming-Verhaltens wie IEEE 802.11k, 802.11r und 802.11v

unterstützen. Die Sendeleistung der WLAN-Geräte sollte 15dBm, die Empfangsempfindlichkeit -90dBm, nicht unterschreiten. Die verfügbaren Protokolle, Antennencharakteristiken und Leistungsanforderungen sind in der Dokumentation auszuweisen.

3.2.5 Authentifizierung

Für die korrekte Identifizierung und die Freigaben von Netzwerkzugriff müssen angeschlossene Geräte authentifiziert werden. Hierfür wird standardmässig Authentifizierung mittels IEEE 802.1X eingesetzt.

Der Unternehmer muss im Angebot präzisieren, ob dieser Standard unterstützt wird. Gegebenenfalls muss der Unternehmer einen alternativen Mechanismus mit einem äquivalenten Sicherheitsniveau aufzeigen und anbieten.

3.3 Standard-Hardware

Die KSB-ICT stellt für den Betrieb der Systeme standardisierte Hardware zur Verfügung. Soweit wie möglich sollen die Systeme auf diese Hardware installiert und betrieben werden.

3.3.1 Standard-Clients

Es stehen verschiedene Client-Konfigurationen zur Verfügung. Detaillierte Beschreibungen inklusive möglicher Konfigurationen sind als Anhang 3 beigelegt. Softwarekomponenten werden mittels Applikationsvirtualisierung auf Basis von Microsoft AppV bereitgestellt.

Die Administration und der Betrieb wird durch die KSB-ICT übernommen. Im Angebot sind die Anforderungen an die Standard-Clients auszuweisen.

3.3.2 Standard-Server

Es werden virtualisierte Server von der KSB-ICT zur Verfügung gestellt. Detaillierte Beschreibungen inklusive möglicher Konfigurationen können angefragt werden. Die Virtualisierung erfolgt mittels Produkte von VMware.

Speicher für die virtuellen Server wird mittels einem zentralen Speichersystem zur Verfügung gestellt. Die Speicher-Shares werden mittels SMB (Version 2.0 bzw. 3.0) eingebunden.

Durch die Bauherrin werden Microsoft SQL- und Oracle-Datenbanken unterstützt. Diese werden auf einem High-Availability Cluster betrieben. Grundsätzlich ist diese Lösung zu verwenden. Wird eine andere Lösung benötigt, ist dies im Angebot zu spezifizieren. Folgende SQL Dienste werden angeboten: Database Engine Services, Client Tools Connectivity, Client Tools Backwards Compatibility, Lesend Replica möglich.

Die Administration und der Betrieb wird durch die KSB-ICT übernommen. Im Angebot sind die Anforderungen an die Standard-Server auszuweisen.

3.3.3 Backup-System

Die KSB-ICT betreibt ein zentrales Backup-System welches für die Sicherung aller Serversysteme, Datenablagen und Datenbanken verwendet werden muss. Es werden verschiedene Technologien wie Snapshot, Dump und File-basierte Backup-Methoden angewendet. Im Rahmen des Angebots hat der Lieferant eine Empfehlung bezüglich Backup-Modulation abzugeben.

Die Aufbewahrung der vom System produzierten Daten muss gemäss den geltenden Regeln des Spitals und der KSB-ICT erfolgen. Dies betrifft die technischen, personenbezogenen und sensiblen personenbezogenen Daten.

Das Backup dieser Daten muss nach den Standard-Methoden und -Prozessen des Spitals durchgeführt werden. Auf keinen Fall dürfen hierzu lokale Festplatten oder Wechselmedien eingesetzt werden.

Es muss eine Schätzung des Backup-Volumens für eine Aufbewahrung der Daten von 10 Jahren unter der angegebenen Backup-Modulation abgegeben werden.

3.4 Systemsicherheit

Der Unternehmer hat die Betriebssicherheit der Systeme während der gesamten Betriebsdauer im Spital sicherzustellen. Hierfür müssen die Risikoszenarien aufgezeigt und dokumentiert werden, dabei sind potenzielle Auswirkungen bezüglich medizinischer Versorgung, Datenschutz, physischer Sicherheit und Gesetzeskonformität zu beschreiben.

3.4.1 Software-Versionen

Betriebssystem und Software auf den Komponenten müssen bezüglich Sicherheitspatches auf dem jeweils aktuellsten Stand sein. Es dürfen keine abgekündigten oder veralteten Versionen installiert werden. Wo immer möglich sollen die neusten Versionen mit den aktuellen Patches installiert werden. Für Microsoft-Produkte kann eine Kompatibilitätsliste bei der KSB-ICT angefragt werden.

Alle Softwarekomponenten müssen über die gesamte Lebensdauer des Systems auf einem aktuellen Stand gehalten und mit Patches versorgt werden. Software Updates müssen durch den Betreiber zeitnah installiert werden. Wird der Evolution der Software nicht mehr gefolgt, ist die KSB-ICT umgehend zu informieren.

3.4.2 Härtung

Das System muss gegen Angriffe gehärtet sein. Es muss im Rahmen des Angebotes dargelegt werden, welche Härtungsmassnahmen ergriffen werden. Insbesondere Firewall-Einstellungen, Internetzugang, eingerichtete Benutzer, aktivierte und deaktiverte Dienste, etc. sind auszuweisen. Grundsätzlich sollen auf allen Komponenten nur die zwingend notwendigen Software-Teile und -Dienste installiert bzw. aktiviert werden.

3.4.3 Risiko-Software

Technologien mit erhöhtem Risiko dürfen nicht zum Einsatz kommen. Dies betrifft insbesondere Adobe Flash, Adobe Shockwave, Adobe Reader, Microsoft Silverlight, Oracle Java und Office-Makros. Es sollen alternative Produkte zu Risiko-Software zur Anwendung kommen.

Falls für den Betrieb des Systems eine solche Software zwingend notwendig ist, muss im Rahmen des Angebots der genaue Verwendungszweck aufgezeigt und deren Verwendung begründet werden.

3.4.4 Security-Updates

Der Unternehmer muss innert einer Frist von 30 Tagen ab Datum der Publikation eines Security-Bulletins die Kompatibilität seines Produkts mit dem veröffentlichten Patch/Update garantieren. Dies bezieht sich auf das Betriebssystem sowie all weitere im Produkt verwendete Software.

3.4.5 Anti-Malware

Die Softwarekomponenten des Systems müssen durch eine durch die KSB-ICT validierte Anti-Malware Lösung geschützt werden. Der Unternehmer muss präzisieren, ob die

standardmässig im KSB eingesetzte Lösung von McAfee verwendet werden kann. Falls nicht, ist eine Alternativlösung und der Grund zu spezifizieren.

Gegebenenfalls muss der Lieferant die von den Schutzaktivitäten auszuschliessenden Verzeichnisse angeben und die erlaubten Ausführungspfade präzisieren.

Ein Mechanismus des Typs «Application Whitelisting», welcher die Ausführung von nicht erlaubter Software blockiert, wird ebenfalls als akzeptabel betrachtet. Unter diesen Umständen verpflichtet sich der Unternehmer, die «Application Whitelist» auf dem aktuellen Stand zu halten.

Wenn er keinen der oben beschriebenen Mechanismen vorschlägt, muss der Unternehmer die Gründe rechtfertigen und die damit verbundenen Risikoszenarien präzisieren. Falls der Verlust einer Zulassung (z.B. CE-Kennzeichnung) als Grund für das Fehlen eines Anti-Malware-Schutzes aufgeführt wird, muss der Lieferant den entsprechenden Beweis erbringen.

Die für den Einsatz der Anti-Malware Lösung notwendigen Signaturen und Versionsupdate müssen mindestens einmal täglich vollautomatisch mittels eines sicheren Referenzservers (oder gleichwertige Update-Lösung) aktualisiert werden.

3.4.6 Externe Speicher

Werden externe Speicher für den Betrieb des Systems benötigt, müssen entsprechende Sicherheitsmassnahmen (Deaktivierung AutoRun, etc.) implementiert werden. Die Verwendung ist im Angebot aufzuzeigen und zu begründen.

3.4.7 Netzwerkprotokolle

Die verschlüsselten Versionen der Kommunikations- sowie Authentifizierungsprotokolle (z.B. SSH, SFTP, SSL/TLS, LDAPS) müssen verwendet werden. Dies ist insbesondere der Fall für Zugriff auf Systemverwaltungsfunktionen und den eventuellen Export von technischen, personenbezogenen oder sensiblen personenbezogenen Daten.

Ungesicherte Dienste (z.B. Telnet, RLogin, FTP) sind nicht zulässig und müssen auf allen Komponenten deaktiviert werden.

Im Angebot sind die verwendeten Kommunikationsprotokolle im Detail auszuweisen.

3.4.8 Middleware

Als Middleware-System setzt das Spital das Produkt WSO2 ein. Eine neue Applikation, welche Schnittstellen zu anderen Systemen hat, muss zwingend über den Middleware-Server des Spitals konfiguriert werden. Details zum WSO2 können angefragt werden.

3.4.9 Passwörter

Alle Standard-Passwörter - insbesondere für Administratoren-Konten und solche mit hohen Privilegien - müssen vor der ersten Verbindung mit dem Netzwerk geändert werden. Die Passwortrichtlinien der KSB-ICT sind strikte einzuhalten. Die entsprechenden Regeln sind in der Benutzerweisung der KSB-ICT definiert.

3.4.10 Systemkonten

Die auf dem Produkt installierten Softwarepakete und Anwendungen müssen unter einer Identität mit eingeschränkten Rechten ausgeführt werden. Administratorkonten sind ausschliesslich für Wartungs- und Konfigurationsarbeiten reserviert und idealerweise deaktiviert.

3.5 Datenschutz

Die einschlägigen Gesetze und Verordnungen zum Datenschutz müssen zwingend eingehalten werden. Der Unternehmer legt dar, dass alle von ihm offerierten Systeme die aktuellen Gesetze und Verordnungen bezüglich Datenschutzes und Datensicherheit des Bundes und des Kantons Aargau einhalten. Dies betrifft sowohl die Verarbeitung als auch Aufbewahrung der Daten.

Der Unternehmer hat im Angebot aufzuzeigen, wie und welche Daten bearbeitet und gespeichert werden. Insbesondere hat er darzulegen und zu begründen, welche technischen oder personenbezogenen Daten potenziell aus der ICT-Umgebung der Bauherrin exportiert werden. Dabei müssen Verhältnismässigkeit, Zweck, Aufbewahrungsdauer, Aufbewahrungsort sowie der Übertragungsweg aufgezeigt werden. Jegliche externe Kommunikation hat verschlüsselt zu erfolgen. Die verwendeten Standards, Algorithmen und Schlüssellängen sind zu deklarieren. Bei Transit über einen externen Zwischenanbieter wird eine Verschlüsselung der Daten auf der Anwendungsebene empfohlen.

Werden Daten in Länder mit nicht angemessenem Datenschutz-Niveau (gemäss Liste des EDÖB) exportiert, müssen bei Abschluss des Vertrages besondere Vertragsklauseln festgelegt werden.

3.6 Management

3.6.1 Fernwartung

Die Zugriffe auf die Systeme per Fernwartung (Remote Access) müssen über die durch die KSB-ICT zur Verfügung gestellte Infrastruktur erfolgen. Zugriffe im «On Demand» Modus sind für ein persönliches Konto, unter Verwendung von starker Authentifizierung, für eine limitierte Dauer erlaubt. Übertragungen zwischen dem System und dem Betreiber der Fernwartung müssen verschlüsselt werden.

Ein persönliches Konto wird nur im Bedarfsfall für die Fernwartung geöffnet.

Der Unternehmer muss darauf hinweisen, falls der Fernzugriff über die zur Verfügung gestellte Infrastruktur für das Produkt nicht umgesetzt werden kann. In diesem Fall muss der Lieferant die Gründe rechtfertigen und eine alternative Lösung mit vergleichbarem Sicherheitsniveau präsentieren.

Es dürfen keine parallelen Kommunikationskanäle eingesetzt werden.

3.6.2 Lizenzmanagement

Es liegt in der Verantwortung des Unternehmers, alle für den Betrieb des betreffenden Produkts erforderlichen Lizenzen zu erwerben und zu gewähren.

Der Unternehmer verpflichtet sich, der Bauherrin alle besagten Lizenzen bei Unterzeichnung des Vertrages zu gewähren. Dies betrifft im Besonderen die Nutzungsrechte für die Software, das Material und alle verwendeten logischen Schichten (z.B. Betriebssystem, Algorithmus, Sicherheitssoftware, Netzwerk-Software, Datenbank-Software, Systemsoftware, Transfer-Software, Fernwartungssoftware, Anwendungssoftware).

3.6.3 Logging

Alle Bedienungen und Änderungen am System, wichtige Systemzustände, unerwartete Ereignisse sowie funktionale Beeinträchtigungen müssen geloggt werden. Die Log-Einträge müssen mit korrekten Zeitstempel versehen (mindestens Jahr / Monat / Tag / Stunden / Minuten / Sekunden) und auf dem zentralen Log-File-Server abgelegt werden.

3.7 Systemverfügbarkeit

Die Systeme im KSB werden in entsprechend ihrer Kritikalität für den Betrieb in drei Kategorien (A, B und C) eingeteilt. Für die verschiedenen Kategorien sind die in Tabelle xx aufgeführten Verfügbarkeitswerte einzuhalten. Die Einstufung der Systeme wird durch die KSB-ICT vorgenommen und richtet sich grundsätzlich nach folgendem Schlüssel:

A: Notwendig für den Geschäftsbetrieb oder mögliche Gefährdung von Personen bei einem Ausfall.

B: Notwendig für den Normalbetrieb oder relevant bezüglich Datenschutzes.

C: Alle anderen nicht kritischen Systeme

Nr.	Kriterium	A	B	C
01	Insgesamt garantierte Verfügbarkeit pro Jahr und System	>99.99%	> 98%	> 95%
02	Resultierender maximaler Ausfall pro Jahr und System Basis: 365 Kalendertage à 24h	8:45h	175:12h	438:00h
03	Recovery Time Objective (RTO)	180 Minuten	24 Stunden	7 Tage
04	Recovery Point Objective (RPO)	8 Stunden	24 Stunden	72 Stunden

Tabelle 1: Systemverfügbarkeitswerte pro Verfügbarkeitsstufe

3.8 Lieferobjekte

Um die IP-Netzwerkintegration während der Realisierung reibungslos sicherstellen zu können, müssen folgende Dokumente im Rahmen der Ausführungsplanung erstellt und der KSB-ICT zur Verfügung gestellt werden. Vorlagen für die entsprechenden Dokumente werden dem Unternehmer im Rahmen der Erarbeitung des Realisierungspflichtenhefts abgegeben. Mehraufwendungen für Koordination und Konfiguration aufgrund fehlerhafter Anträge gehen zu Lasten des Unternehmers.

Portanträge:	Alle Geräte, welche ans ICT-Netzwerk angeschlossen werden, müssen mittels Portantrag dem Betreiber des Netzwerkes bekanntgegeben werden. Der Portantrag ist durch den Unternehmer auszufüllen und wird zur Vergabe von virtuellen und physischen Ports benötigt. Aufgrund des Portantrages werden die notwendigen IP-Adressen und Zertifikate für die angeschlossenen Geräte vergeben. Der Portantrag beinhaltet Anzahl und Art der benötigten Ports, Informationen zu den anzuschliessenden Geräten, benötigte Netzwerkperformance, etc.
Kommunikationsmatrix:	Die Kommunikationsmatrix dient dem Netzwerkprovider zur Konfiguration der Netzwerkübergänge (Firewalls) und Switches. In der Kommunikationsmatrix muss der Unternehmer für alle notwendigen Kommunikationsbeziehungen zwischen zwei Netzwerkgeräten die benötigten Kommunikations-Protokolle, -Ports, -Richtung, Netzwerkperformance, etc. angeben.
Fernzugriffsantrag	Wird Zugriff auf das System oder Systemteile von ausserhalb des Spitalnetzwerks benötigt bzw. benötigt das System oder Systemteile Zugriff auf Ressourcen ausserhalb des Spitalnetzwerks, muss zwingend ein Fernzugriffsantrag erstellt werden. Es müssen sowohl die Informationen über freigegebene Daten, verwendete Protokolle, berechnete Parteien, etc. angegeben werden.

Hardwareantrag Der Hardwareantrag wird benötigt, um die notwendigen Standard-Clients, Standard-Server (physisch oder virtuell) oder Höheneinheiten zur Verfügung zu stellen. Der Serverantrag muss durch den Unternehmer ausgefüllt werden und beinhaltet alle notwendigen Informationen zu den Servern (virtuell oder physisch, benötigte Rechenleistung, benötigter Speicher, benötigte Performance, benötigte Höheneinheiten, etc.).

3.9 Dokumentation

Durch den Unternehmer ist sicherzustellen, dass folgende Teile in der Bauwerksdokumentation behandelt werden und vor Abnahme durch den Bauherrn freigegeben wurden:

- Die **technische Dokumentation** dient dem ICT-Netzwerk Betreiber zum Verständnis der angeschlossenen Systeme. Die technische Dokumentation beinhaltet Spezifikation, Konfiguration und Funktionsweise des fertiggestellten Systems.
- Die **IT-Sicherheitsdokumentation** beschreibt sowohl die technischen als auch die organisatorischen Sicherheitsvorkehrungen des Systems und dessen Anbieter, Lieferanten und Externen.
- Die **Architektur- und Betriebsdokumentation** beschreibt die gewählte Architektur des Systems, verwendete Schnittstellen, Datenflüsse, Anforderungen an das Netzwerk, etc. Zusätzlich werden alle für den ICT-Netzwerk Betreiber relevanten Informationen über den fachgerechten Betrieb des Systems übergeben.

Die Dokumentation ist während der gesamten Vertragsdauer auf dem aktuellen Stand zu halten.

Glossar

Nr.	Begriff	Beschreibung
01	DHCP	Dynamic Host Configuration Protocol <i>Protokoll zur automatischen Erkennung IP-Geräten und deren Einbindung in das IP-Netzwerk</i>
02	DNS	Domain Name System <i>Dienst zur Auflösung von IP-Namen in einem Netzwerk</i>
03	DWDM	Dense Wavelength Division Multiplexing
04	FTP	File Transfer Protocol
05	ICT	Information and Communication Technology
06	IEC	International Electrotechnical Commission <i>Internationale Normungsorganisation im Bereich der Elektrotechnik und Elektronik</i>
07	IEEE	Institute of Electrical and Electronics Engineers <i>Internationaler Berufsverband von mehrheitlich Elektrotechnik und Informationstechnik Ingenieuren.</i>
08	IP	Internet Protocol
09	KSB	Kantonsspital Baden <i>Auftraggeber / Bauherr</i>
10	LAN	Local Area Network <i>Lokales abgeschirmtes IP-Netzwerk</i>
11	LDAPS	Secure Lightweight Directory Access Protocol <i>Sicheres Protokoll für den Zugriff auf das Benutzerverzeichnis</i>
12	MAC	Media Access Control <i>Sublayer des Datalink-Layers im OSI Modell, zuständig für Adressierung und Kanalzugang.</i>
13	MPLS	Multiprotocol Label Switching
14	OSI	Open Systems Interconnection <i>Modell zur Charakterisierung und Standardisierung von Kommunikationsfunktionen.</i>
15	PoE	Power over Ethernet
16	PKI	Public-Key-Infrastruktur
17	QoS	Quality of Service
18	UKV	Universelle Kommunikationsverkabelung
19	VLAN	Virtual LAN <i>Virtualisiertes Netzwerk, ermöglicht den betrieb mehrerer logischer Netzwerke auf demselben physischen Netzwerk.</i>
20	WAN	Wide Area Network <i>Bezeichnet ein Rechnernetz, welches sich über Länder oder sogar Kontinente erstreckt.</i>
21	WLAN	Wireless LANs <i>Lokales Funknetz, meistens werden Standards der IEEE 802.11-Familie verwendet.</i>

Impressum

Auftraggeber: Kantonsspital Baden, Informatik, Rolf Menzi
Ersteller: Amstein + Walthert Progress AG, Zürich
Autoren: KSB Rolf Menzi
Patrick Hug
Daniel Leimgruber
AWP Michael Schaffner
Marc Müller
Severin Lang
Daniel Burri
Projekt: LN/710624/KSB_ICT_Integrationsvorgaben_v03.00.docx

Anhang

Anhang 1 – Vertraulichkeitsvereinbarung

Anhang 2 – Merkblatt Fernzugriff

Anhang 3 – Standardsoft- und -hardware