UNIKLINIK KÖLN

# ISMS-Richtlinie Informationssicherheitsanforderungen an Lieferanten, Dienstleister und Dritte

## Informationssicherheit in der Uniklinik Köln

**Dokumentenlenkung**

| | |
|---|---|
| **Dokumentennummer** | 035 |
| **Version** | 2.0 |
| **Verantwortung** | Stabstelle Informationssicherheit |
| **Geltungsbereich** | UKK gesamt |
| **Freigegeben ab** | 15.04.2025 |
| **Freigabe durch** | B. Upadek |
| **Vertraulichkeit** | UKK-Intern / TLP-GREEN |
| **Mitgeltende Dokumente** | |

Hinweis: Ausgedruckte Dokumente unterliegen nicht dem Änderungsdienst.

**Dokumentenhistorie**

| Version | Datum | Änderung | Autor |
|---|---|---|---|
| 2.0 | 08.04.2025 | Aufteilung in zwei separate Dokumente – mit und ohne Selbstauskunft | Tim Fischer |
| 1.0 | 24.02.2025 | Ersterstellung | Daniel Kleer |

## INHALT



## A. ZIELSETZUNG UND GELTUNGSBEREICH

Lieferanten, Dienstleister und Dritte (im Folgenden Auftragnehmer (AN) genannt), deren Leistungen im Kontext der kritischen Dienstleistung der stationären Patientenversorgung zum Einsatz kommen, müssen bezüglich der Qualität ihrer Arbeit und der Einhaltung von Maßnahmen zur Informationssicherheit die folgenden Mindestanforderungen an die Informationssicherheit erfüllen. Die beschriebenen Mindestanforderungen werden von der Uniklinik Köln (im Folgenden Auftraggeber (AG) genannt) zudem für eine interne Bewertung des AN herangezogen.

Die in dieser Richtlinie aufgestellten Informationssicherheitsanforderungen für AN zielen darauf ab, einen angemessenen Schutz der Ressourcen im Bereich der stationären Patientenversorgung zu gewährleisten. Durch Auslagerung bzw. durch die Beschaffung von Produkten oder Dienstleistungen darf sich das Niveau des Datenschutzes und der Informationssicherheit des AG nicht verschlechtern oder herabsenken. Es wird ein Mindestniveau von Schutzmaßnahmen festgeschrieben, welche von jedem AN im Hinblick auf dessen IT--Systeme und Prozesse abzudecken ist. Eine Festlegung von technischen Details und einzusetzenden Produkten erfolgt i.d.R. nicht, da die konkrete Umsetzung in der Planungshoheit und Verantwortung des jeweiligen AN liegt. Die Informationssicherheitsanforderungen für AN im Bereich der kritischen Dienstleistung sind von allen AN einzuhalten, die Zugriff auf Ressourcen des AG erhalten sollen.

Dazu gehören insbesondere:

- AN, die direkt oder über einen Remote-Zugang auf Systeme bzw. Netze im Bereich der stationären Patientenversorgung zugreifen.
- AN, die sensible Daten aus dem Bereich der stationären Patientenversorgung in eigenen IT-Systemen speichern oder verarbeiten.
- AN, die ausgelagerte Aufgaben im Bereich der stationären Patientenversorgung übernehmen.
- AN, die dem AG Cloud-Services zur Verfügung stellen, in welcher der AG Daten verarbeitet.

Die Verpflichtung auf diese Anforderungen ist dem AN möglichst bereits im Rahmen der Vertragsverhandlungen mitzuteilen. Alle auf die Informationssicherheitsanforderungen verpflichteten AN müssen die Einhaltung der vereinbarten Maßnahmen rechtlich verbindlich zusichern. Eine entsprechende Verpflichtungserklärung wird Bestandteil der Vertragsunterlagen. Verstöße oder Zuwiderhandlungen werden im Rahmen der Haftungsklauseln aus dem Vertrag mit dem AN behandelt.

Der AG informiert den AN bei festgestellten Abweichungen über notwendige korrektive Maßnahmen. Prüfungen der daraus resultierenden Maßnahmenumsetzung können durch den AG durchgeführt werden.

# B. INFORMATIONSSICHERHEITSANFORDERUNGEN AN AUFTRAGNEHMER

## 1. EINLEITUNG

Für einen angemessenen Umgang mit Fragen der Informationssicherheit sind grundsätzliche Regelungen im Hause des AN erforderlich. Der AG empfiehlt, dass AN mit datenschutzrechtlicher bzw. informationssicherheitstechnischer Relevanz, ein Managementsystem für den Datenschutz bzw. die Informationssicherheit umsetzen. Dabei können anerkannte Standards wie zum Beispiel die ISO/IEC 27001 oder der BSI IT-Grundschutz als Grundlagen dienen. Entsprechende Managementsysteme sind für Lieferanten für Produkte und Dienstleistungen in diesen Kategorien jedoch nicht verbindlich, sofern sie nicht im Rahmen von Ausschreibungen oder Verträgen explizit gefordert sind.

Sofern der AN die Umsetzung eines Managementsystems im obigen Sinne für sich reklamiert, so muss der Geltungsbereich des jeweiligen Managementsystems die gelieferte Dienstleistung bzw. das Produkt vollständig einschließen.

Weitere, über diese Richtlinie hinausgehende Anforderungen, können vom AG im Rahmen der Ausschreibung bzw. der Beschaffung festgelegt werden. Anforderungen in Ausschreibungen bzw. Verträgen gelten unabhängig von den Anforderungen dieser Richtlinie für den AN.

## 2. INFORMATIONSSICHERHEITSANFORDERUNGEN AN AUFTRAGNEHMER

### 2.1. Organisatorische Anforderungen

#### 2.1.1. Benennung eines Ansprechpartners für den Datenschutz

Die gesetzlichen Bestimmungen des Datenschutzes und das Telekommunikationsgeheimnis sind einzuhalten. Alle Informationen über Daten und Vorgänge, die bei der Durchführung des Auftrages bekannt werden, sind auch nach Beendigung des Vertrages vertraulich zu behandeln. Der AN ist angehalten, Verantwortlichkeiten hinsichtlich der Umsetzung zu beschreiben. Zuständige Ansprechpersonen für den Datenschutz sind durch den AN zu benennen und transparent zu kommunizieren.

#### 2.1.2. Benennung eines Ansprechpartners für Informationssicherheit

Es ist ein zentraler Ansprechpartner zu benennen, der verbindliche Auskünfte zur Informationssicherheit – sowohl im internen Bereich als auch im Außenverhältnis zum AG – geben kann. Bei entsprechender Unternehmensgröße können die Aufgaben auch von mehreren Mitarbeitern wahrgenommen werden. Zuständige Ansprechpersonen für die Informationssicherheit sind durch den AN zu benennen und transparent zu kommunizieren. Für den Fall der Abwesenheit ist eine Vertretung sicher zu stellen.

#### 2.1.3. Sicherstellung der Informationssicherheit und Implementierung eines ISMS

Die Einhaltung der Informationssicherheit muss vom AN sichergestellt werden. Hierfür hat der AN ein ISMS in seiner Organisation implementiert. Dabei müssen die Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität, Authentizität, Patientensicherheit und Behandlungseffektivität berücksichtigt werden. Der AN hat dem Antrag des AG nachzukommen, Informationen seiner Sicherheitsorganisation offenzulegen, um eine Bewertung durch den AG zu ermöglichen. Dies kann durch die Formulierung umzusetzender Informationssicherheitsanforderungen und die Bereitstellung von Zertifikaten wie ISO/IEC 27001 sowie weiteren relevanten Dokumenten erfolgen.

### 2.1.4. Verbot der privaten Nutzung

Alle IT-Komponenten, von denen unmittelbar oder mittelbar ein Zugriff auf Ressourcen des AG möglich ist, dürfen nur für dienstliche Zwecke genutzt werden. Eine private Nutzung durch die Mitarbeiter ist nicht zulässig. Private IT-Komponenten dürfen ebenfalls nicht für den Zugriff auf Systeme des AG benutzt werden bzw. nicht an Systeme bzw. Netze des AN angeschlossen werden, die für den Zugriff auf Ressourcen des AG vorgesehen sind.

### 2.1.5. Notfallvorsorge

Der AN bestimmt die Anforderungen an die Informationssicherheit und zur Aufrechterhaltung des Informationssicherheitsmanagements in Abhängigkeit der beauftragten Dienstleistung und stellt sicher, dass die Dienstleistung gegen widrige Situationen (Notfall, Krise oder Katastrophe) in angemessenem Umfang abgesichert ist. Der Verfügbarkeitsbedarf kann dazu in Abstimmung mit dem AG bestimmt werden.

Dafür hat der AN ein BCM (Business Continuity Management) etabliert, das im Rahmen einer Notlage oder Großstörung die Aufrechterhaltung einer minimalen Servicequalität und die schnellstmögliche Wiederherstellung aller für den AG bereitzustellenden Dienste sicherstellt.

### 2.1.6. Dokumentation

Der AN ist angehalten, Bedienabläufe, die im Zusammenhang mit der zu erbringenden Dienstleistung stehen, in angemessenem Umfang zu dokumentieren und dem AG diese Dokumentation auf Anfrage vorzulegen.

Es wird vom AN erwartet, dass dieser jegliche Dokumentation zur Verfügung stellt, die die Nutzung der angebotenen Dienstleistung erleichtert. Der gebräuchliche Umfang einer derartigen Dokumentation, wenn auch nicht auf diese beschränkt, inkludiert die folgenden Punkte:

- Liste der Hardware
- Liste der Software (inklusive Betriebssystem und Patch-Level)
- Überblick über die Systemarchitektur (kann Teil der Designdokumentation sein)
- Kommunikationsmatrix
- Existierende Benutzerkonten und Rollen sowie deren Berechtigungen
- Beschreibung von proprietären (nicht in der Industrie standardisierten) Sicherheitsmechanismen

Weitere Dokumentationen, spezifiziert als Teil des Liefergegenstandes oder Auftrages, die die Sicherheit der Dienstleistung gewährleisten.

Sollten Änderungen an der Dienstleistung durchgeführt werden, wird vom AN erwartet, diese in die Dokumentation einzupflegen (siehe nächste Anforderung).

### 2.1.7. Änderungs-/ Change-Management

Der AN stellt sicher, dass alle Änderungen (z.B. Änderung der bereitgestellten Dienste, Organisatorische Änderungen beim AN) gemeldet und dokumentiert werden. Dazu betreibt der AN ein Change-Management mit Schnittstelle zum AG oder stellt durch geeignete Richtlinien/Betriebskonzepte diese Information des AG sicher.

### 2.1.8. Vorfalls-/ Incident-Management

Der AN stellt sicher, dass Informationssicherheitsvorfälle mit möglichen Auswirkungen auf die Unternehmenswerte des AG innerhalb eines Tages gemeldet werden. Informationssicherheitsvorfälle, die direkte Auswirkungen auf die kritische Dienstleistung des AG haben könnten, sind unverzüglich zu melden. Dazu betreibt der AN ein Incident-Management mit Schnittstelle zum AG oder stellt durch geeignete Richtlinien/Betriebskonzepte diese Information des AG sicher.

Der AN hat im Falle eines Vorfalls auf Nachfrage des AG Ressourcen zur Minderung und/oder Beseitigung des Vorfalles sowie den finalen Korrekturbericht bereitzustellen.

### 2.1.9. Asset-Management

Der AN hat alle Assets in seinem Informationssystem zu identifizieren und zu dokumentieren, die einen Bezug zu Systemen des AG zwecks Wartung oder Betriebszugang haben können. Die Verantwortung für die Aufrechterhaltung der entsprechenden Sicherheitskontrollen dieser Assets muss zugewiesen werden. Die Assets sind zu dokumentieren. Zum Schutz der Assets kann der AN die Anwendung spezifischer Sicherheitsmaßnahmen delegieren, jedoch bleibt der AN für den angemessenen Schutz der Assets, die in Bezug zum Informationssystem des AG stehen, verantwortlich.

### 2.1.10. Umgang mit Informationen

Alle Informationen und Daten, insbesondere Gesundheitsdaten, die dem AN im Rahmen seiner Tätigkeit bekannt werden bzw. anfallen, müssen vertraulich behandelt werden. Ausgenommen hiervon sind nur offensichtlich nicht vertrauliche Informationen. Im Zweifelsfall hat der AN eine Klassifizierung durch den AG anzufordern. Die Informationen müssen entsprechend ihrer Klassifikation behandelt werden. Dies gilt insbesondere bei der Übertragung über öffentliche Netze, beim Versand via Briefpost oder E-Mail und bei der Speicherung auf mobilen Datenträgern. Daten (in elektronischer und/ oder gedruckter Form), die nicht mehr benötigt werden, müssen nicht wiederherstellbar gelöscht bzw. zerstört werden.

### 2.1.11. Informationsverarbeitung außerhalb der EU

Für alle Informationen und Daten die dem AN im Rahmen seiner Tätigkeit bekannt werden bzw. anfallen, muss sichergestellt sein, dass sie nicht in ein Land außerhalb der EU übertragen, dort verarbeitet oder gespeichert werden.

### 2.1.12. Vertraulichkeitsvereinbarung

Die Mitarbeiter sind durch ihren Arbeitsvertrag bzw. getrennte Verpflichtungserklärungen auf Vertraulichkeit und Einhaltung der datenschutzrechtlichen Bestimmungen auch über das Ende ihrer Beauftragung hinaus zu verpflichten.

### 2.1.13. Informationssicherheitsschulung

Die Mitarbeiter sind über die sicherheitstechnischen Anforderungen der IT-Ressourcen des AG zu informieren. Das betrifft insbesondere die möglichen Risiken, adäquate Gegenmaßnahmen sowie die persönlichen Verantwortungen der Mitarbeiter im Rahmen ihrer Tätigkeiten. Zusätzlich sind die Mitarbeiter in Bezug auf Informationssicherheit regelmäßig durch entsprechende Schulungen oder Mitteilungen nachweislich zu unterweisen. Hierzu gehören auch sicherheitsbezogene Informationen bei Einführung neuer Techniken und Verfahren.

#### 2.1.14. Abmeldung

Die Mitarbeiter sind zu verpflichten, sich nach Aufgabenerfüllung vom IT-System bzw. von der IT-Anwendung abzumelden.

#### 2.1.15. Ausscheiden von Mitarbeitern

Beim Ausscheiden von Mitarbeitern des AN ist durch geeignete Maßnahmen sicherzustellen, dass der Zugriff auf Systeme und Anwendungen des AG verhindert wird.

#### 2.1.16. Physische und umgebungsbezogene Sicherheit

Der AN hat dafür Sorge zu tragen, dass der unbefugte Zutritt in Räume, Büros und Einrichtungen, in denen Informationen des AG verarbeitet werden, ausgeschlossen ist. Dies gilt weiterhin auch für Anlieferungs- und Ladebereiche, über die unbefugte Personen die Räumlichkeiten betreten könnten. Besondere Bedeutung sollte auf Büroräume, in denen Supporttätigkeiten in Form von Remoteverbindungen durchgeführt werden, gelenkt werden.

Von Seiten des AN sind Richtlinien zu erstellen, die aufgeräumte Arbeitsumgebungen sowie Bildschirmsperren bei Nichtbenutzung regeln.

#### 2.1.17. Audits

Der AN stellt sicher, dass der AG oder ein von diesem beauftragten Drittem die Organisation in Bezug auf die Informationssicherheit auditieren darf. Dies kann einmal oder mehrmals geschehen. Die Prüfungen werden auf der Grundlage der von dem AN zur Verfügung gestellten Dokumentation durchgeführt. Der genaue Umfang, die Dauer und die Organisation werden jeweils einvernehmlich vereinbart.

#### 2.1.18. Subdienstleister / Lieferkette

Die Mindestanforderungen für den AN gelten gleichfalls für vom AN eingesetzten Subdienstleister. Sicherheitsvereinbarungen die mindestens den hier definierten Mindeststandards entsprechen, sind Teil der Verträge/Vereinbarungen mit AN.

### 2.2. Technische Anforderungen

#### 2.2.1. Zugriffsschutz für IT-Komponenten

Alle IT-Komponenten, von denen unmittelbar oder mittelbar ein Zugriff auf Ressourcen im Bereich der Prozessdatenverarbeitung (beispielsweise IT-Systeme oder Daten) des AG möglich ist, müssen mit einem Zugriffsschutz versehen sein. Dabei ist gleichermaßen der physische Zugriff als auch der logische Zugang zu schützen. Es sind die bereits vom Betriebssystem vorgegebenen Mechanismen zur Authentisierung (z.B. Kerberos) zu nutzen. Das Booten von bootfähigen Datenträgern sowie die parallele Installation mehrerer Betriebssysteme ist zu verhindern.

#### 2.2.2. Speicherung von Daten

Sofern vertrauliche oder sicherheitsrelevante Daten auf externen oder mobilen Geräten (beispielsweise Notebooks oder Speichermedien) gespeichert werden, müssen die Daten kryptographisch nach

aktuellem Stand der Technik verschlüsselt werden. Sofern die Daten auf externen Datenträgern gespeichert werden, hat der AN für den physikalischen Schutz und die sichere Verwahrung Sorge zu tragen. Zur Sicherung der Arbeitsergebnisse sind geeignete Sicherungen anzufertigen, die genauso zu sichern sind.

### 2.2.3. Datenübertragung

Der Einsatz einer kryptographischen Absicherung der Kommunikation ist insbesondere notwendig, wenn Daten mit hohem Schutzbedarf über öffentliche oder als nicht ausreichend sicher geltende Netzwerke übertragen werden.

Es muss sichergestellt werden, dass keine veralteten und als unsicher bekannten kryptografischen Lösungen zum Einsatz kommen. Hierfür ist eine Richtlinie zu etablieren, die mit dem AG abgestimmt ist, wo die zulässigen Kryptografiealgorithmen definiert sind.

Diese Richtlinie muss sich an einen Industriestandard (z.B. BSI TR-02102) orientieren und wird regelmäßig durch den AN überprüft und ggf. aktualisiert.

### 2.2.4. E-Mail-Versand

Vertrauliche oder sicherheitsrelevante Daten dürfen per E-Mail nur versendet werden, wenn sie kryptographisch nach aktuellem Stand der Technik verschlüsselt wurden.

### 2.2.5. Reparatur von IT-Komponenten und Systemen

Werden Systeme und IT-Komponenten, die vertrauliche Daten enthalten, zur Reparatur oder Entsorgung gegeben, so ist die durchgängige Wahrung der Vertraulichkeit (z.B. durch vorherigen Ausbau der Datenträger) sicherzustellen.

### 2.2.6. Netzwerksicherheit

Netzwerkkomponenten und -systeme sind abhängig vom Schutzbedarf so abzusichern und durch geeignete Maßnahmen zu trennen, dass bei Störungen und Ausfällen die Auswirkungen auf weitere Systeme und Netze möglichst begrenzt werden. Die Trennung von Netzwerken hat sowohl vertikal (Zone) als auch horizontal (Segment) zu erfolgen. Idealerweise sind drei Zonen „Externe DMZ“, „Interne DMZ" und „Internes Netz“ vorzusehen. Die Übergänge zwischen Zonen sind immer mit einer geeigneten dedizierten Sicherheitskomponente (Firewall, Proxy) abzusichern. Ein einfacher Paketfilter gilt nicht als ausreichend. Die Firewall darf nur explizit benötigte und freigegebene Dienste erlauben.

Der Zugang zum Netz ist z.B. per MAC-Adress-Filterung und/oder Network Access Control auf valide Endgeräte zu begrenzen.

### 2.2.7. Extern erreichbare Dienste und Remote-Access ins interne Netz

Direkte Zugriffe aus dem Internet in das interne Netz sind nicht zulässig und müssen von der Firewall unterbunden werden. Sofern Remote-Access in das interne Netz des AN erforderlich ist oder Dienste vom Internet aus erreichbar sein müssen (z.B. Webserver, Mailserver, etc.), darf eine Umsetzung erst nach einer dokumentierten Sicherheitsanalyse erfolgen. Die Ergebnisse dieser Analyse sind dem AG auf Anfrage zur Verfügung zu stellen.

### 2.2.8. Drahtlose Verbindungen

Der Einsatz von drahtlosen Verbindungen darf nur bei angemessener Sicherung, insbesondere durch kryptographisch Authentisierung und Verschlüsselung auf aktuellem Stand der Technik, gemäß den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI), erfolgen.

### 2.2.9. Virenschutz am Arbeitsplatz

Der ständige Einsatz einer Virenschutzsoftware auf allen Arbeitsplatzrechnern ist verpflichtend. Die Überprüfung muss dabei automatisch beim Zugriff auf Dateien (auch verschlüsselte) erfolgen (On-Access-Scanner) und darf vom Benutzer nicht unterbunden werden können. Ebenso ist der ein- und ausgehende Datenstrom zu überprüfen (online-Scan on demand and on access). Zusätzlich sind alle Arbeitsplatzrechner regelmäßig auf eventuell vorhandene Viren zu prüfen.

### 2.2.10. Zusätzlicher Virenschutz

Neben dem Virenschutz am Arbeitsplatz sind Viren-Scanner im Gateway- bzw. Serverbereich zur Überprüfung der bei E-Mail, Filetransfer (z.B. FTP) und Webverkehr übertragenen Daten einzusetzen.

### 2.2.11. Regelmäßige Aktualisierung der Virenpattern

Die Virenschutzdatenbanken sind aktuell zu halten. Die Virenschutzprogramme müssen über die Möglichkeit des automatisierten Downloads von Viren-Pattern verfügen. Das Update der Viren-Pattern muss mindestens einmal pro Tag durchgeführt werden.

### 2.2.12. Zeitnahes Einspielen von Sicherheitsupdates / Patchmanagement

Der AN hat ein wirksames Patch-Management für seine IT-Einrichtungen im eigenen Hause zu etablieren, dass dem jeweils aktuellen Stand der Technik entspricht und kontinuierlich der technischen Entwicklung angepasst wird.

Sicherheitsupdates für das Betriebssystem und für Kommunikationsprogramme, mit denen auf Internetdienste zugegriffen wird, müssen auf allen Systemen umgehend eingespielt werden. Ebenso sind die Firewall und alle öffentlich erreichbaren Server auf aktuellem Stand zu halten. Sicherheitsupdates sind auf diesen Systemen ebenfalls umgehend einzuspielen.

Es ist jährlich ein Bericht zu erstellen und dem AG zur Verfügung stellen, in dem jede in dem jeweiligen Zyklus adressierte Schwachstelle dokumentiert ist. Dieser Bericht kann detaillierte oder aggregierte Daten unter Berücksichtigung der Kritikalitätsstufe und der betroffenen Bereiche (Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit, Patientensicherheit, Behandlungseffektivität) enthalten.

### 2.2.13. Keine Gefährdung für die stationäre Patientenversorgung

Der AN verpflichtet sich, während der gesamten Erbringung der Lieferungen und Leistungen dafür Sorge zu tragen, dass von seinen Programmier- und Parametriergeräten, Speichermedien und Datenträgern keine Gefährdungen für den kritischen Prozess der stationären Patientenversorgung ausgehen.

### 2.2.14. Überprüfung auf Schadsoftware

Der AN hat auf Anfrage des AG die getroffenen Vorsorgemaßnahmen unverzüglich im Detail darzustellen. Der AN stimmt hiermit zu, dass der AG die vorgenannten Geräte und Speichermedien des AN jederzeit einer Überprüfung auf Schadsoftware mit geeigneter Anti-Schadsoftware unterziehen darf.

### 2.2.15. Fernwartungszugang

Fernwartungszugriffe auf Infrastrukturkomponenten in den Rechenzentren des AG erfolgen über die Privileged-Access-Management-Lösung (PAM).

Alle Zugriffe werden über diese PAM-Lösung abgesichert und protokolliert (Vgl. B3S 6.13.2 im Sinne des § 8a BSI-Gesetz). Bei Verdacht werden die Protokolle und Aufzeichnungen der Zugriffe und damit verbunden Tätigkeiten zum Zwecke der Gefährdungsanalyse geprüft. Die PAM-Lösung ist für die User über VPN durch Einrichtung eines 2. Faktor via Mobiltelefon erreichbar.

Die Fernwartungszugänge werden personalisiert vergeben. Zur Verwaltung bedarf es der namentlichen Angabe vom zuständigen Mitarbeiter durch den AN. Änderungen oder Austritte von im PAM erfassten Mitarbeiter müssen umgehend durch den AN mitgeteilt werden, damit die entsprechenden Zugänge geändert oder deaktiviert werden können.

### 2.2.16. Physikalische Sicherheit

Die für den Zugriff benötigten Ressourcen sind durch entsprechende Maßnahmen vor unberechtigten physischen Zugriff zu schützen, beispielsweise durch Installation in verschlossenen Räumen mit angemessenen Zugangsschutz oder Lagerung in verschlossenen Schränken bei Nichtbenutzung.

### 2.2.17. Grundsicherung und Systemhärtung

Alle Systeme und Netzwerk-Komponenten müssen anhand anerkannter Best-Practice- Guides nach aktuellem Stand der Technik, z.B. gemäß den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) gehärtet und mit aktuellen Service-Packs und Sicherheitspatches versehen sein. Unnötige Benutzer, Programme, Netzwerkprotokolle, Dienste und Services sind zu deinstallieren, oder – falls eine Deinstallation nicht möglich ist – dauerhaft zu deaktivieren und gegen versehentliches Reaktivieren zu schützen. Der AN muss zudem, im Rahmen seiner Möglichkeiten sicherstellen, dass seine Lösungen frei von „Backdoors“ sind, die die verwendeten Sicherheitsmechanismen umgehen können.

Die sichere Grundkonfiguration der Systeme muss überprüft und dokumentiert sein.

### 2.2.18. Sichere Administrations- und Wartungstools

Die eingesetzten Tools unterstützen eine personalisierte Anmeldung, kryptographischen Schutz der Passwörter, eine Authentisierung nach Stand der Technik und eine Rechteverwaltung mit Einschränkung des Zugriffs auf den erforderlichen Umfang.

### 2.2.19. Umgang mit Schwachstellen

Die Produkte des AN werden regelmäßig auf Schwachstellen geprüft und in Bezug auf die Kritikalität und die geschäftlichen Auswirkungen hin untersucht.

Sind vom AN entwickelte Software-, Firmware- oder Hardware-Komponenten betroffen, ist der AN verpflichtet, umgehend die Schwachstellen an den AG zu melden und diese bzgl. möglicher funktionaler und sicherheitsrelevanter Auswirkungen zu bewerten. Eine mögliche Bewertung der Kritikalität kann z.B. auf Basis der Schutzbedarfsanalyse durch den AG festgelegt werden. Der Umfang des Schwachstellenmanagements umfasst jede potenzielle Schwachstelle, die möglicherweise Einfluss auf die Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit, Patientensicherheit oder

Behandlungseffektivität der Vermögenswerte (materielle oder immaterielle) oder auf eine bei dem AG operierende Dienstleistung des AN nehmen kann.

### 2.2.20. Berechtigung Mitarbeiter

Der AN muss Berechtigungsprozesse (Vergabe, Ändern und Löschen von Benutzern und deren Berechtigungen) umsetzen, die sicherstellen, dass nur dafür bestimmte Mitarbeiter Zugriff auf Informationen des AG erhalten. Die Prozesse (Vergabe, Änderung und der Entzug von Berechtigungen) müssen nachvollziehbar dokumentiert sein.

Durch geeignete Maßnahmen ist sicherzustellen, dass nur namentlich benannte und nach den Informations-Sicherheitsrichtlinien des AG unterwiesene Mitarbeiter Zugang zu diesen Ressourcen des AG erhalten. Benutzer- und Administrator-Accounts müssen getrennt sein.

Durch entsprechende Identifikations- und Authentifikationsmechanismen muss ein eindeutiger Rückschluss auf diese Personen möglich sein.

### 2.2.21. Einsatz sicherer Passwörter

Die zur Zugangssicherung verwendeten Passwörter müssen eine Qualität nach der Richtlinie „Identitäts- und Berechtigungsmanagement“ des AG besitzen. Auslieferungspasswörter dürfen nicht auf Systeme im produktiven Einsatz übernommen werden. Authentifizierungsinformationen sind an keiner Stelle im Klartext abzulegen. Eine entsprechende Passwortrichtlinie des AN muss vorliegen. Passwörter dürfen nicht unverschlüsselt gespeichert werden.

Die Verwendung von Passwort-Speicher-Programmen darf nur bei vorheriger Vorlage eines Sicherheitskonzepts durch den AN erfolgen.

### 2.2.22. Anforderungen an Softwareentwicklungsprozesse

Insofern AN Software für den AG entwickeln, müssen die Prinzipien des Security by Design eingehalten und sich an den allgemein anerkannten Industriestandards orientiert werden. Dazu müssen geeignete technische und organisatorische Maßnahmen umgesetzt sein.

### 2.2.23. Robuste/resiliente Architektur

Die Architektur der IT-Systeme und Medizingeräte muss robust und resilient gestaltet sein, um eine hohe Verfügbarkeit und Versorgungssicherheit zu gewährleisten. Dies beinhaltet den Schutz vor Ausfällen externer Versorgungsdienste wie Strom- und Wasserversorgung, die Einhaltung herstellerseitig definierter Umgebungsanforderungen durch geeignete Verfahren wie Klimatechnik, und die Vermeidung von Beeinträchtigungen durch Wechselwirkungen zwischen Infrastruktureinrichtungen und Versorgungseinrichtungen, sofern diese Einfluss auf die stationäre Patientenversorgung des AG haben könnten.

Für die Versorgungssicherheit relevante IT-Systeme und Komponenten mit Bezug auf die stationäre Patientenversorgung (kDL des AG) müssen redundant ausgelegt sein, und wo dies nicht möglich ist, sind geeignete Maßnahmen vorzusehen.

### 2.2.24. Angriffserkennung

Im Rahmen einer Angriffserkennung müssen Verfahren implementiert werden, die nicht autorisierte Aktivitäten und gefährliche Software erkennen und verhindern. An den Perimeterschnittstellen müssen

Systeme zur Angriffserkennung (wie IDS/IPS) eingesetzt werden, die Bedrohungen von außerhalb blockieren. Diese Systeme können auch bei internen Übergängen unter Berücksichtigung kritischer Prozesse und wirtschaftlicher Aspekte eingesetzt werden. Es sollen regelmäßige Überprüfungen auf Schwachstellen im eigenen Netz erfolgen, um sowohl externe als auch interne Schwachstellen zu identifizieren.

### 2.2.25. Sicheres Löschen und Entsorgung von Datenträgern

Für das sichere Löschen und die Entsorgung von Datenträgern müssen Maßnahmen ergriffen werden, um die Wiedergewinnung von Informationen zu verhindern. Es muss eine definierte Vorgehensweise zur Außerbetriebnahme und Löschung von Datenträgern geben, die dokumentiert ist und regelmäßig kontrolliert wird.

Speichermedien mit Daten des AG müssen vor Wiederverwendung oder Entsorgung datenschutzkonform gelöscht oder physisch zerstört werden.

## C. GLOSSAR

| Abkürzung/ Begriff | Beschreibung |
|---|---|
| AG | Auftraggeber |
| AN | Auftragnehmer |
| AVV | Auftragsverarbeitungs-Vertrag |
| B3S | Branchenspezifischer Sicherheitsstandard |
| BCM | Business Continuity Management |
| ISMS | Informationssicherheitsmanagement |
| PAM | Privileged Access Management |
| SLA | Service Level Agreement |
| UKK | Uniklinik Köln |