UNIKLINIK KÖLN

ISMS Richtlinie
Mindeststandard Informationssicherheit

Informationssicherheit in der Uniklinik Köln

Dokumentennummer	017
Version	2.0
Verantwortung	Stabsstelle Informationssicherheit
Geltungsbereich	UKK gesamt
Freigegeben ab	31.01.2025
Freigabe durch	B. Upadek
Vertraulichkeit	UKK-Intern / TLP-GREEN
Mitgeltende Dokumente	

Dokumentenhistorie

Version	Datum	Änderung	Autor
2.0	20.01.2025	Review, Redaktionelle Anpassungen, Anpassungen auf Basis der aktualisierten Richtlinien in diversen Kapiteln	André Lauterbach
1.0	01.08.2023	Ersterstellung	Alexander Wirtz

INHALT

A. Einleitung

Das vorliegende Dokument beschreibt die Anforderungen an die Informationssicherheit in Bezug auf die Informationstechnik (IT), Medizintechnik (MT) sowie Betriebs- und Versorgungstechnik (OT). Sie sind bei der Anschaffung, Entwicklung und Instandhaltung von IT/MT/OT-Systemen einzuhalten und bei Ausschreibungen oder Beschaffungen entsprechend zu berücksichtigten. Das Dokument behandelt ausschließlich sicherheitsrelevante Anforderungen. Es ist als Ergänzung zu weiteren ggf. bestehenden Spezifikationen eines Auftrags zu sehen (wie z.B. die Gesamtspezifikation eines IT/MT/OT-Projekts).

Die Ausführungen in dem Dokument stellen lediglich einen Mindeststandard der einzuhaltenden Anforderungen dar, eventuelle spezifische Ausführungsdetails sind im Rahmen projektspezifischer Vorbereitungen und auf Grundlage der Informationssicherheitsrichtlinien der Uniklinik Köln nach der Auftragserteilung mit dem Auftraggeber (AG) abzustimmen.

Die Maßnahmen stellen Mindestanforderungen dar, die der Auftragnehmer (AN) bei der Realisierung seines Liefer- u. Leistungsumfangs zu beachten hat. Abweichungen sind nur mit ausdrücklicher Freigabe durch den Auftraggeber (AG) zulässig, die entsprechende Freigabe ist in den projektspezifischen Beschreibungen festzuhalten und zu dokumentieren.

Sofern in der Spezifikation keine besonderen Ausführungsvorgaben gemacht werden, hat der AN die Möglichkeit, eigene Lösungsvorschläge zur Umsetzung der Mindestanforderungen vorzulegen. Diese sind dem Auftraggeber (AG) technisch zu erläutern und von ihm vor der Ausführung freizugeben.

B. Mindestanforderungen Informationssicherheit

1. Grundlegende Anforderungen

Als Betreiber kritischer Infrastrukturen (KRITIS) unterliegt die Uniklinik Köln AöR dem IT-Sicherheitsgesetz und den damit verbundenen und jeweils anwendbaren Ausführungsbestimmungen, Verordnungen und eventueller weiterer Regelwerke.

IT/MT/OT-Systeme sind daher entsprechend dem aktuellen Stand der Technik und den für kritische Infrastrukturen geltenden Standards der Informationssicherheit, sowie den gültigen Gesetzen und Regelwerken zu errichten.

Hier zählen insbesondere

- der B3S Medizinische Versorgung,
- die ISO/IEC 27002,
- die DIN EN IEC 80001-1
- der BSI-C5 Standard bei Lösungen mit Einbeziehung von Cloudkomponenten
- sowie Je nach Anforderung weitere relevante Standards wie z.B. IEC/TR 60601-4-5 oder IEC 62443 in der jeweils gültigen Fassung.

Erkennt der AN, dass über die hier beschriebenen Maßnahmen hinaus noch weitere Maßnahmen notwendig sind, um die gesetzlichen Anforderungen zu erfüllen, so ist er verpflichtet, dies dem AG mitzuteilen.

Der AN hat zur Sicherstellung der Informationssicherheit ein Informationssicherheitskonzept nach ISO 27001 zu erstellen und umzusetzen, soweit dies für die Lieferung der Produkte die Erbringung der Dienstleistung erforderlich ist. Auf Verlangen des AG legt der AN diesem das Konzept kostenfrei vor und weist dem AG die Umsetzung nach. Bei Tätigkeiten an Standorten des AG (einschließlich des Fernzugriffs

auf die Infrastruktur des AG) sind durch den AN darüber hinaus die Informationssicherheitsrichtlinien des AG zu beachten.

Sämtliche Informationen des AG, die dem AN im Rahmen seiner Tätigkeiten bekannt werden oder im Laufe eines Auftrages anfallen, sind vertraulich zu behandeln. Entsprechende Vertraulichkeitsvereinbarungen zwischen AG und AN sind im Vorfeld einer Beauftragung abzuschließen und mit der Stabsabteilung Compliance abzustimmen.

2. Umzusetzende Maßnahmen

2.1. Sichere Grundkonfiguration

Ein IT/MT/OT-System muss nach der Bereitstellung/Inbetriebnahme in einem betriebssicheren Zustand konfiguriert sein. Die jeweilige Grundkonfiguration bei Bereitstellung/Inbetriebnahme ist durch den AN zu dokumentieren. Nicht benötigte Dienste und Funktionen sind, sofern dies möglich ist, zu deaktivieren. Nicht benötigte Ordner-/ Laufwerksfreigaben und Netzwerkports sind zu deaktivieren. Vorhandene initiale Standardkonten und -passwörter zu ändern, bzw. sofern möglich zu deaktivieren. Hierbei sind die Anforderungen der UKK an Passwörter zu berücksichtigen (s. Kapitel 2.3).

Eventuelle Testdaten und/oder Informationen, Dienste und Funktionen, welche im Rahmen von Entwicklungs- und Testbetrieb notwendig waren, sind aus den entsprechenden Produktivsystemen nachweislich zu entfernen bzw. zu deaktivieren.

Ausgehende und eingehende Internetverbindungen sind grundsätzlich nicht zugelassen und bedürfen einer Begründung sofern sie erforderlich sind. Werden diese freigegeben sind die weiter unten aufgeführten Anforderungen zu Netzwerkzugriffen zu erfüllen.

2.2. Benutzerverwaltung

In den IT/MT/OT-Systemen ist für jeden Benutzer ein eigenes Benutzerkonto einzurichten. Dies gilt sowohl für die Betriebssystem- und Datenbankebene (z.B. Windows) als auch für die Anwendungsebene.

Für Benutzer mit gleichartigen Aufgaben sind einheitliche Benutzerrollen zu definieren, die entsprechend ihres Tätigkeitsfelds, die notwendigen Rechte erhalten. Bei der Erstellung von Benutzerrollen sind nur solche Rechte zu vergeben, die für die Erfüllung der jeweiligen Aufgabe notwendig ist (Need-To-Know- und Least-Priviledge-Prinzip).

Jeder Benutzer hat sich bei Aufnahme seiner Tätigkeit mit seinen persönlichen Zugangsdaten am jeweiligen System anzumelden. Der Zugriff auf die Systeme ist personenscharf zu registrieren.

Eine Anmeldung als Benutzergruppe (z.B. eine einmalige und dauerhafte Anmeldung als Gruppe / Anmeldung mit sog. Sammelbenutzern) ist nicht zulässig. Sofern aus technischen Gründen eine Anmeldung als Benutzergruppe notwendig ist, ist eine Ausnahmeregelung zu definieren und durch den Informationssicherheitsbeauftragten (ISB) der UKK freizugeben.

Die Zugehörigkeit des AG-Personals zu den jeweiligen Benutzerrollen wird vom AG vorgegeben. Die Realisierung der Zugriffskontrolle und Benutzerverwaltung hat bei umfangreichen IT/MT/OT-Systemen durch Domänencontroller zu erfolgen. Dabei sind notwendige Redundanzen zu berücksichtigen. In Ausnahmefällen können auch alternative Verfahren eingesetzt werden. Das zum Einsatz kommende Verfahren, inklusive der erstellten Rollen und deren Beschreibungen ist mit dem AG abzustimmen und durch den AN zu dokumentieren.

2.3. Standardpasswörter

Alle Standardpasswörter der Hersteller sind bis zur Inbetriebnahme (IBN) von den Systemen zu entfernen und durch individuelle Passwörter zu ersetzen. Dazu zählen auch Passwörter auf eventuellen Datenbanken, Netzwerk- und anderen Peripheriekomponenten. Passwörter sind individuell zu wählen und dürfen nicht mehrfach verwendet werden.

Systeme müssen eine Passwortrichtlinie entsprechend dem Stand der Technik unterstützen, die jeweilige Anforderung (Komplexität) an die Passwörter sind mit dem AG abzustimmen. Es sind ausschließlich sichere Passwörter, mit einer Länge von mindestens 16 Zeichen für privilegierte Konten und 12 Zeichen für normale Nutzerkonten zu verwenden.

Passwörter und andere Authentisierungsinformationen dürfen nur verschlüsselt übertragen und im System gespeichert werden.

Auf Medizingeräten, IoT-Geräten sowie weiteren Komponenten wie z.B. Steuerungen, SPSen und Automatisierungskomponenten oder Gateways sind vorhandene Standardpasswörter auf sichere Werte zu setzen sowie sicherheitserhöhende Konfigurationsoptionen zu aktivieren.

Für Systeme zur Remoteanbindung ist eine 2-Faktor-Authentifizierung umzusetzen. Im Falle einer Störung des Benutzerverwaltungsdienstes sind lokale Notfallpasswörter vorzusehen.

Generell sind die Passwortvorgaben der ISMS-Richtlinie Identitäts- und Berechtigungsmanagement zu beachten.

2.4. Protokollierung

Die Anforderungen aus der ISMS-Richtlinie Protokollierung und Detektion sind als Grundlage zu berücksichtigen.

Systeme und Komponenten sind so zu planen, dass An- u. Abmeldevorgänge der Benutzer sowie weitere Systemereignisse automatisch protokolliert und zentral gespeichert werden. Weitere Kriterien wie z.B. Zeitraum und Anzahl der zu speichernden Meldungen sind mit dem AG abzustimmen. Um eine Auswertung zu erleichtern, müssen sicherheitsrelevante Ereignisse zu markieren sein. Mit dem AN ist abzustimmen, wie und wo die jeweiligen Protokolle für eine regel-mäßige Routinekontrolle einzusehen sind.

Die Protokollierung muss sowohl für die Betriebssystemebene (Windows, Linux, ...) als auch die Anwendungsebene erfolgen. Alle Systeme sind auf eine einheitliche Systemzeit zu synchronisieren, das zu verwendende Zeitnormal ist mit dem AG abzustimmen.

Medizingeräte, IoT-Geräte sowie weiteren Komponenten wie z.B. Steuerungen, SPSen und Automatisierungskomponenten sind so zu planen, dass Systemereignisse und Protokolle erstellt und an einen zentralen Speicher zur Auswertung übertragen werden können.

2.5. Sicherheitspatches und Konfiguration

Sämtliche in den IT/MT/OT-Systemen eingesetzte Komponenten sind mit aktuellen und vom Hersteller geprüften und zugelassenen Sicherheitspatches zu versehen. Die jeweils aktuell verwendeten Sicherheitspatches sind in geeigneter Weise zu dokumentieren. Zum Abschluss der örtlichen Bau-/Inbetriebnahmephase müssen die vom jeweiligen Hersteller aktuell freigegebenen Sicherheitspatches auf den Systemen installiert sein.

Zwischen AG u. AN ist ein geeignetes Verfahren zur Aktualisierung der Sicherheitspatches für die Betriebszeit nach der Inbetriebnahme (Gewährleistungszeit) abzustimmen. Hierzu zählen auch

eventuelle Fallback- bzw. Rollbackfunktionen für den Fall von fehlerhaften Sicherheitspatches. Darüber hinaus muss die jeweilige Installation und eventuelle Deinstallation von Sicherheitspatches vom AG genehmigt werden und sollte nicht automatisch erfolgen.

Ggf. ist hierzu ein Wartungsvertrag mit dem AG abzuschließen.

Vorgenannte Regelungen gelten gleichermaßen für Konfigurationsdaten wie z.B. Firmwarestände, Parametrierstände oder weitere Konfigurationsdaten.

Das Einspielen von Sicherheitspatches und Konfigurationsänderungen haben so zu erfolgen, dass klinische und betriebliche Prozesse möglichst nicht gestört werden. Entsprechende Maßnahmen (z.B. Servicezeiten) sind mit dem AG abzustimmen.

2.6. Softwarestände und Lizenzen

Die aktuell verwendeten Software- und Firmwarestände sowie Lizenzen sind in geeigneter Weise und nach den Vorgaben des ISMS des AG zu dokumentieren und sicher zu archivieren. Es darf nur Software und eingesetzt werden, die vom Hersteller für die jeweiligen Systeme freigegeben ist.

2.7. Einsatz von Virenscannern

Alle vernetzten Komponenten, welche in den IT/MT/OT-Systemen zum Einsatz kommen, sind an geeigneter Stelle mit vom jeweiligen Hersteller zugelassenen Virenscannern auszurüsten, hierbei sind immer die von der Uniklinik Köln eingesetzten und gemanagten Standards (Sophos Endpoint Security, Microsoft Defender) zu bevorzugen.

Die Virenscanner sind in der vom Hersteller vorgegebenen Weise zu konfigurieren. Sofern die technische Entwicklung der Hersteller eine kontinuierliche und rückwirkungsfreie Virenüberwachung zulässt, ist diese zu realisieren. Die notwendigen Reaktionszeiten des jeweiligen IT/MT/OT-Systems dürfen jedoch nicht negativ beeinflusst werden. Sollte der Scanvorgang nicht kontinuierlich erfolgen können, ist dieser in festzulegenden Zyklen oder auf Anforderung einzurichten (z. B. 1x täglich o. wöchentlich usw.). Eine Einbindung in die Überwachungssysteme der UKK ist abzustimmen und möglichst vorzusehen.

Das vorgesehene Verfahren zur Aktualisierung der Virensignaturen ist zu beschreiben. Neue Virenpattern sind mindestens über eine Datenschleuse in eine dafür vorgesehenen Demilitarisierten Zone (DMZ) einzuspielen. Sofern möglich sind diese bevorzugt über die gemanagten Standards der UKK einzuspielen. Der aktuell verwendete Stand der Virensignaturen ist in geeigneter Weise zu dokumentieren.

2.8. Unbelegte USB-Zugänge

Unbelegte USB-Zugänge außerhalb von verschlossenen Serverschränken sind zu deaktivieren. Wo das Deaktivieren aus betrieblicher Sicht nicht möglich oder sinnvoll ist, sind mechanische USB-Schlösser vorzusehen.

2.9. Verschlossene Systemschränke

Serverschränke (inkl. möglicher Seitenwände) sind mit eigener Schließung zu versehen. Die Schließung darf nicht mit einer Standard-Schließung für Serverschränke erfolgen und ist mit dem AG im Vorfeld abzustimmen. Hierbei ist darauf zu achten, dass die Kühlung der Komponenten weiter gewährleistet ist.

2.10. Netzwerkübergänge innerhalb der IT/MT/OT-Systeme

Alle Netzwerkzugänge innerhalb von IT/MT/OT-Systemen sind gem. Abschnitt 2.15 zu überwachen und eventuelle Systemereignisse zu protokollieren. Es ist ein Verfahren zu integrieren, das nur bekannte

Teilnehmer im Netzwerk akzeptiert. Unbekannte Teilnehmer (wie z. B. nachträglich in freie Netzwerkzugänge eingesteckte Laptops) sind von den IT/MT/OT-Systemen abzuweisen.

Es ist sicherzustellen, dass kein unzulässiger Zugriff auf die IT/MT/OT-Systeme, z. B. durch eine am Drucker abgezogene Netzwerkleitung, erfolgen kann (z.B. durch Nutzung von zertifikatsbasierte Portsecurity – dies ist mit dem Bereich Netzwerk abzustimmen).

Unbelegte Netzwerkzugänge außerhalb von verschlossenen Serverschränken, wie z.B. an Switches im Feld, sind zu deaktivieren oder mechanisch zu verschließen.

2.11. Verbindungen von IT/MT/OT-Systemen mit externen Netzen

Für einen eventuellen Datenaustausch mit zentral bereitgestellten oder öffentlichen Diensten, sind die IT/MT/OT-Systeme an zentraler Stelle mit der DMZ verbunden. Hierzu ist zwischen den internen IT/MT/OT-Systemen und der externen DMZ eine Datenschnittstelle vorzusehen bzw. in Abstimmung mit dem AG eine bestehende DMZ zu nutzen. Besonderheiten bzgl. Cloudanbindung s.u. (Kapitel 2.25).

2.12. Firewalls zu externen Systemen

Sämtliche Schnittstellen von IT/MT/OT-Systemen zu Systemen Dritter (externer oder fremder Partner) sind durch Firewalls mit restriktivem Regelsatz zu sichern und die Kommunikation der IT/MT/OT-Systeme darf nur über eine DMZ und (Reverse-)Proxy/Application Layer Gateway erfolgen. Der Verbindungsaufbau muss dabei immer aus der Zone/dem Segment mit dem höheren Schutzbedarf (i.d.R. von Intern in Richtung Extern) erfolgen. Sofern im begründeten Ausnahmefall das IT/MT/OT-System direkt mit Systemen Dritter kommunizieren muss, darf dies nur über vom AG zugelassene Verbindungen mit entsprechenden Firewalls und Sicherheitsmechanismen erfolgen.

Jede Zugriffsfreigabe ist vom AG ausdrücklich freizugeben und im Detail mit ihm abzustimmen.

Die Firewall-Regeln werden vom AG vorgegeben und sind in den vom AN zu liefernden Komponenten der IT/MT/OT-Systeme zu berücksichtigen. Technische Details sind projektspezifisch mit dem AG abzustimmen.

2.13. Sicherer Fernzugang

Zur Systemunterstützung während der Bau- und der späteren Betriebsphase besteht die Möglichkeit dem AN einen Fernzugang für den Zugriff auf die IT/MT/OT-Systeme über öffentliche Netze und der PAM-Lösung des AG einzurichten. Diese PAM-Lösung ist für Fernzugriffe zu verwenden.

Darüber hinaus und sofern die Bereitstellung einer Architektur für Fernzugriffe Bestandteil der Beauftragung ist, gelten folgende Vorgaben und Anforderungen:

Die Architektur der Fernzugänge muss eine Isolation der internen IT/MT/OT-Systeme sicherstellen und eine direkte Einwahl in die Endgeräte unterbinden. Um dies sicherzustellen, muss ein Fernzugriff über eine DMZ und einen zentral verwalteten Zugangsserver (Terminalserver, JumpHost) des AG erfolgen. Die Authentifizierung mit dem Zugangsserver muss über eine MultiFaktor-Authentifizierung sichergestellt sein.

Der Zugriff auf einen Fernzugang muss zentral geloggt und wiederholte Fehlversuche gemeldet werden. Alle Fernzugangsmöglichkeiten sind zu dokumentieren und individuell durch eine berechtigte Person des AG freizugeben. Handlungstätigkeiten sind zu überwachen, evtl. Systeme zur Aufzeichnung dieser Tätigkeiten sind entsprechend zu planen. Es ist zudem eine automatische Sperrung des Fernzugang nach den Vorgaben des AG umzusetzen.

Sofern der AN Leistungen zur Systemunterstützung über einen Fernzugang erbringt, sind entsprechende Vertraulichkeitsvereinbarungen zwischen AN und AG zu vereinbaren.

2.14. Verschlüsselung vertraulicher Daten

Vertrauliche Informationen und Daten sind nur verschlüsselt zu speichern und zu übertragen (Data at-rest und Data in-transit).

Zur Sicherstellung des Schutzes von vertraulichen oder personenbezogenen Daten, hat der AN eine Auflistung der zu verarbeitenden Informationen (Informationskategorien) innerhalb eines IT/MT/OT-System bereitzustellen.

Die Einstufung bzw. Kritikalität von eventuellen Informationen ist durch den AG zu bestätigen und ggfs. an die betrieblichen Anforderungen anzupassen.

2.15. Datenschleuse zum sicheren Datenaustausch mit IT/MT/OT-Systemen

Um einen sicheren Datenaustausch mit externen Netzen zu gewährleisten, ist innerhalb der DMZ eine Datenschleuse bzw. Datengateway einzurichten.

Das Einlesen bzw. das Auslesen von Daten in das bzw. aus den IT/MT/OT-Systemen, darf grundsätzlich nur über diese vom AG kontrollierte Datenschleuse und über sichere Protokollvarianten (z.B. sFTP) erfolgen. Der direkte Datenaustausch über USB Sticks oder ähnliches ist nicht gestattet.

Details zum Umgang mit einer Datenschleuse bzw. Datengateway werden dem AN nach Auftragserteilung mitgeteilt. Sofern die Bereitstellung einer Datenschleuse Bestandteil der Beauftragung ist, gelten insbesondere die in diesem Dokument definierten Vorgaben zur Benutzerverwaltung, Passwortnutzung, Sicherheitspatches und Kryptografie als Mindestanforderungen. Weitere Details zur Bereitstellung einer Datenschleuse sind mit dem AG abzustimmen.

2.16. Kryptographie

Grundsätzlich soll die Kommunikation der IT/MT/OT-Systeme untereinander, sowie auch die Kommunikation mit externen Systemen, durch kryptographische Verfahren gesichert werden. Passwörter dürfen grundsätzlich nicht im Klartext übertragen oder bei der Eingabe auf dem Bildschirm sichtbar werden, sowie in Scripten, Konfigurations- oder Quellcode im Klartext zu sehen sein. Es dürfen nur Verschlüsselungsverfahren verwendet werden, deren Sicherheit nach dem Stand der Technik als ausreichend für den jeweiligen Einsatz und die jeweilige Einsatzdauer bewertet sind. Die Auswahl der zu verwendenden Verschlüsselungsverfahren erfolgt durch Abstimmung mit dem AG und auf Grundlage des Dokumentes vom Bundesamt für Sicherheit in der Informationstechnik (BSI) „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ in der jeweils aktuellen Version. Weitere Details sind der Sicherheits- und Schutzsystemleitlinie ISMS-Kryptographie der UKK zu entnehmen.

Wenn die Gefahr besteht, dass Laufzeiten und Reaktionszeiten von IT/MT/OT-Systemen durch kryptographische Verfahren negativ beeinflusst werden, kann bei interner Kommunikation der IT/MT/OT-Systeme auf kryptographische Verfahren verzichtet werden. In diesem Fall sind weitergehende Sicherheitsmaßnahmen (z.B. Netzisolierung, IDS/IPS, Application Whitelisting etc.) mit dem AG abzustimmen.

Der AN erstellt grundsätzlich einen Übersichtsplan seines Liefer- u. Leistungsumfangs, in dem der Einsatz kryptografischer Verfahren erkennbar ist. Sämtliche zur Anwendung kommenden Lösungen sind mit dem AG abzustimmen.

2.17. IDS (Intrusion Detection System) / System zur Angriffserkennung

Ein Intrusion Detection System bzw. eine Funktion zur Überwachung des Datenverkehrs im IT/MT/OT-System ist zu integrieren. Sofern die Bereitstellung eines solchen Systems Bestandteil der Beauftragung ist, muss im Vorfeld eine enge Abstimmung mit dem AG bezüglich der Auswahl eines solchen Systems erfolgen. Folgende Funktionen sind durch ein solches System mindestens bereitzustellen:

- Automatische Erkennung und Inventarisierung von sämtlichen IT/MT/OT- und Netzwerkkomponenten
- Erstellung und Überwachung einer s.g. Baseline und Alarmierung bei Verletzung dieser
- Erkennung und Überwachung von Parameter-, Funktions- und Konfigurationsänderungen
- Schwachstellen Management anhand von Signaturen, Anomalien und bekannten Schwachstellen
- Heuristische Scans zur Erkennung von akuten Cyberangriffen (z.B. Mitm, Port-Scan)
- Überwachung und Erkennen von eventuellen weiteren Bedrohungen (z.B. häufige fehlschlagende Anmeldeversuche)
- Sichere Fernzugänge, sofern nicht durch andere Systeme bereits vorhanden.

Netzwerkgeräte, Medizingeräte, IoT-Geräte und Komponenten wie Steuerungen, SPSen und Automatisierungskomponenten sind möglichst dahingehend auszuwählen, dass eine Funktion zur Überwachung (z.B. SPAN, Mirror-Port) durch den Hersteller bereits integriert ist. Die Auswahl eines Herstellers solcher Komponenten ist grundsätzlich mit dem AG abzustimmen.

2.18. Backupverfahren

Vor und nach jeder Änderung der Anwendersoftware, der Firmware und des Betriebssystems, ist grundsätzlich ein Backup zu erstellen. Die Backups sind auf zentralen Datensicherungssystemen redundant in verschiedenen Brandabschnitten abzulegen. Alternativ können in Ausnahmen virengeprüfte und vom AG freigegebene mobile Datenträger genutzt werden. Alle Backups sind eindeutig zu kennzeichnen und an einem sicheren Ort aufzubewahren.

Es sind Mechanismen zu planen, mit denen die Vollständigkeit und Korrektheit einer Datensicherung gegen den aktuellen Datenbestand geprüft werden kann. Die Datensicherungs- und Rücksicherungsverfahren sind ausführlich zu dokumentieren.

Das zur Anwendung kommende Verfahren ist mit dem AG abzustimmen.

2.19. Umgang mit nicht mehr genutzten Datenträgern und Datenaufzeichnungen

Alle nicht mehr genutzten Datenträger oder Aufzeichnungen von Daten/Informationen sind sicher und vertraulich zu vernichten und deren Vernichtung zu dokumentieren. Dazu sind diese dem AG zu übergeben oder nachweisbar entsprechend den Vorgaben des AG zu entsorgen.

2.20. Umgang mit Service-Laptops des AN

Zur Konfiguration, Parametrierung oder ähnlichen Tätigkeiten, sind vorzugweise Service-Laptops des AG zu nutzen. Die Nutzungsbedingungen und Vereinbarungen sind durch den AG entsprechend zu kommunizieren und dokumentieren.

Sofern Service-Laptops o.a. PCs des AN genutzt werden müssen und mit den IT/MT/OT-Systemen des AG verbunden werden, ist durch den AN vor Ort die Virenfreiheit dieser Geräte zu prüfen und nachzuweisen. Der Vorgang ist entsprechend zu dokumentieren.

2.21. Asset Management

Zur Integration in das ISMS (Informations-Sicherheits-Management-System) des AG sind alle zum Lieferumfang gehörenden Hard- und Softwarekomponenten durch den AN in einer Asset-Liste nach den Vorgaben des AG zu erfassen und dem AG bereitzustellen.

2.22. Dokumentation

Alle im Rahmen der Systemhärtung erbrachten Lieferungen und Leistungen sind im Rahmen dokumentierter Bedienabläufe nach DIN ISO/IEC 27001 durch den AN zu beschrieben, die Dokumentation ist durch den AG abzunehmen und hat mindestens folgende Informationen zu umfassen:

- Darstellung und Beschreibung der Systemarchitektur (grundsätzlicher Aufbau der Komponenten, Schnittstellen und deren Kommunikation)
- Beschreibung sämtlicher sicherheitsrelevanten Systemeinstellungen und Parameter der eingesetzten Einzelkomponenten
- Auflistung sicherheitsrelevanter Implementierungsdetails wie z.B. eingesetzte Verschlüsselungsverfahren
- Rollen- und Berechtigungskonzept
- System- und Konfigurationseinstellungen

Darüber hinaus sollte der projektspezifische Anteil in einem Pflichtenheft dokumentiert werden.

2.23. Prüfung und Abnahme

Die Erfüllung aller in diesem Dokument beschriebenen Anforderungen ist im Rahmen einer Funktionsprüfung, bzw. spätestens zur Abnahme vom AN nachzuweisen und in einer Checkliste zu dokumentieren. Die Inhalte der Checkliste sind im Vorfeld mit dem AG abzustimmen.

Zum Ende der Inbetriebnahme hat der AN noch einmal die Virenfreiheit der Systeme nachzuweisen und zu dokumentieren.

Im Rahmen der Schlussabnahme wird die Einhaltung der Informationssicherheitsanforderungen vom AG überprüft und im Abnahmeprotokoll dokumentiert.

2.24. Benachrichtigung über sicherheitsrelevante Vorfälle beim AN

Der AN ist verpflichtet, Sicherheitsvorfälle in seiner Organisation, die potenziell einen negativen Effekt die Uniklinik Köln haben könnten, umgehend ohne Zeitverzug der Uniklinik Köln zu melden.

Ein evtl. bestehender Fernzugang auf Systeme der Uniklinik Köln ist ab Bekanntwerden des Sicherheitsvorfalls und bis zur expliziten Freigabe durch den Informationssicherheitsbeauftragten der Uniklinik Köln nicht mehr zu nutzen.

Der AN sichert zu, auf Nachfrage der Uniklinik Köln einen Bericht über die Behandlung des Vorfalles bereitstellen.

2.25. Besondere Anforderungen an Cloud-Lösungen

Bei einer Cloud-Lösung sind angemessene Schutzmaßnahmen nach „Stand der Technik“ anzuwenden. Dies gilt nicht nur für den Betreiber der Cloud-Infrastruktur (z.B. Microsoft oder AWS oder Google), sondern besonders für die in der Cloud betriebene Applikation und den Dienstleister, der die Applikation in der Cloud betreibt. Hier sind die Vorgaben der Richtlinie „Cloud-Sicherheit“ zu berücksichtigen.

Insbesondere:

Bei einer Cloud-Lösung sind angemessene Schutzmaßnahmen nach „Stand-der-Technik“ anzuwenden. Dies gilt nicht nur für den Betreiber der Cloud-Infrastruktur (z.B. Microsoft oder AWS oder Google), sondern auch für die in der Cloud betriebene Applikation und den Dienstleister, der die Applikation in der Cloud betreibt.

Zur Überprüfung der Sicherheitsanforderungen an den Cloud-Dienstleister muss immer der C5-Kriterienkatalog des BSI herangezogen werden.

Für den Betrieb für Cloud-Services mit Gesundheits- oder Sozialdaten / zur Unterstützung kritischer Klinikprozesse gilt:

- Die Datenverarbeitung darf nur im **Inland**, in einem Mitgliedstaat der Europäischen Union oder, sofern ein Angemessenheitsbeschluss gemäß Artikel 45 der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat erfolgen. Voraussetzung ist, dass die datenverarbeitende Stelle über eine Niederlassung im Inland verfügt.
- Für den Betrieb von Cloud-Dienstleistungen im Gesundheitswesen ist lt. § 393 Abs 3 SGB V ein Testat nach dem BSI C5-Standard erforderlich. Der Anbieter muss ein C5-Typ1-Testat nachweisen. Ab dem 01.07.2025 muss er ein C5-Typ2-Testat nachweisen.
- Die UKK muss die im Prüfbericht des Testats enthaltenen, korrespondierenden Kriterien für Kunden umsetzen und die in einem Sicherheits- / Betriebskonzept dokumentieren.
- Wenn der Cloud-Dienst kritische Klinikprozesse bedient, sind die erweiterten Anforderungen des Kriterienkataloges (Zusatzkriterien) anzuwenden. Sollte der Cloud-Dienstleister seinen Cloud-Dienst zertifiziert haben, sind in diesem Fall trotzdem Evidenzen einzufordern.
- Der Betrieb des Cloud-Diensts auf UKK-Seite erfolgt zentral durch die uk-it.
- Für den Cloud-Dienst ist als Freigabe ein expliziter Vorstandsbeschluss einzuholen.

Für den Betrieb von Cloud-Services ohne Gesundheits- und Sozialdaten / keine Unterstützung kritischer Klinikprozesse gilt:

- Sollte keine Zertifizierung nach dem C5-Kriterienkatalog auf Seiten des Cloud-Dienstleisters bestehen, ist der Kriterienkatalog vom Dienstleister abzufragen.
- Es ist per Abfrage des Kriterienkatalogs sicherzustellen, dass die Lösung entsprechend oder vergleichbar der „Basis-Anforderungen“ des BSI-C5-Kriterienkatalogs abgesichert ist.
- Die Anforderungen an die UKK als Cloud-Nutzer (siehe Kapitel E) in den einzelnen C5-Kriterienbereichen müssen umgesetzt und in der Betriebsdokumentation nachgewiesen werden.

C. GLOSSAR

Abkürzung/ Begriff	Beschreibung
AG	Auftraggeber
AN	Auftragnehmer
B3S	Branchenspezifischer Sicherheitsstandard
BSI	Bundesamt für Sicherheit in der Informationstechnik
DIN EN	Deutsches Institut für Normung / EN Europäische Norm
DMZ	Demilitarisierte Zone
IBN	Inbetriebnahme

Abkürzung/ Begriff	Beschreibung
IDS	Intrusion Detection System - System zur Erkennung von Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind
IEC	International Electrotechnical Commission / Internationale Elektrotechnische Kommission - Normungsorganisation für Normen im Bereich der Elektrotechnik und Elektronik
ISB	Informationssicherheitsbeauftragter
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization / Internationale Organisation für Normung
IT/MT/OT/ IoT	IT: Informationstechnologie: Technik zur elektronischen Datenverarbeitung MT: Medizintechnik (Medical IT): Erfassung, Verarbeitung, Speicherung und Verbreitung elektronischer Daten, Informationen und Wissen im Gesundheitswesen. OT: Operational Technology: Verwendung von Hardware und Software zur Identifizierung, Überwachung und Steuerung von physischen Geräten, Prozessen und Ereignissen in Unternehmen. (I)IoT: Internet of Things: System miteinander verbundener (z.B. medizinischer) Geräte und Sensoren, die Daten erfassen und austauschen können.
Mitm	Man in the middle – Eine Angriffsform, bei der Angreifer sich unbemerkt in eine Kommunikation zwischen verschiedenen Partnern einschaltet
NAS	Network Attached Storage - konfigurierbarer Datenspeicher, um in einem Netzwerk Speicherplatz zur Verfügung zu stellen.
PAM	Privileged Access Management – System zur Autorisierung und Überwachung von Benutzern
sftp	Secure/SSH File Transfer Protocol – verschlüsseltes Dateiübertragungsprotokoll
SPAN	Switch Port Analyser - spezieller Port an einem Switch, der eine gespiegelte Kopie des Netzwerkverkehrs innerhalb des Switches an ein Ziel sendet
SPS	Speicherprogrammierbare Steuerung – Gerät für Steuer- und Regelungszwecke
UKK	Uniklinik Köln
USB	Universal Serial Bus