

Mindeststandard Informationssicherheit

Uniklinik Köln



Informationssicherheit in der Uniklinik Köln





Inhaltsverzeichnis

A.	Einleitung	3
B.	Grundlegende Anforderungen	3
C.	Umzusetzende Maßnahmen	4
1.	Sichere Grundkonfiguration	4
2.	Benutzerverwaltung	4
3.	Standardpasswörter	4
4.	Protokollierung	5
5.	Sicherheits-Patches und weitere Konfigurationsdaten	5
6.	Softwarestände und Lizenzen	5
7.	Einsatz von Virenscannern	6
8.	Unbelegte USB Zugänge	6
9.	Verschlossene Systemschränke	6
10.	Netzwerkzugänge innerhalb der IT/MT/OT-Systeme	6
11.	Verbindung von IT/MT/OT-Systemen mit externen Netzen	6
12.	Firewalls zu externen Systemen	7
13.	Sicherer Fernzugang	7
14.	Verschlüsselung vertraulicher Daten	7
15.	Datenschleuse zum sicheren Datenaustausch mit IT/MT/OT-Systemen	8
16.	Kryptographie	8
17.	IDS (Intrusion Detection System) / System zur Angriffserkennung	8
18.	Backupverfahren	9
19.	Umgang mit nicht mehr genutzten Datenträgern u. Datenaufzeichnungen	9
20.	Umgang mit Service-Laptops des AN	9
21.	Asset Management	9
22.	Dokumentation	10
23.	Prüfung und Abnahme	10
24.	Benachrichtigung über sicherheitsrelevante Vorfälle beim AN	10



A. EINLEITUNG

Das vorliegende Dokument beschreibt die Anforderungen an die Informationssicherheit in Bezug auf die Informationstechnik (IT), Medizintechnik (MT) sowie Betriebs- und Versorgungstechnik (OT), die bei der Anschaffung, Entwicklung und Instandhaltung von IT/MT/OT-Systemen einzuhalten oder bei einer eventuellen Ausschreibung oder Beschaffung entsprechend zu berücksichtigen sind. Das Dokument behandelt ausschließlich sicherheitsrelevante Anforderungen und 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. GRUNDLEGENDE ANFORDERUNGEN

Als Betreiber kritischer Infrastrukturen 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 vom AN konform nach 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 sowie ggfs. 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 im Rahmen 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.



C. UMZUSETZENDE MAßNAHMEN

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.

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

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-Privileged-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) des AG 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.

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.

Systeme müssen eine Passwortrichtlinie entsprechend dem Stand der Technik unterstützen, die jeweilige Anforderung (Komplexität) an die Passwörter sind mit dem AG abzustimmen. 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.

4. PROTOKOLLIERUNG

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 regelmäßige Routinekontrolle einzusehen sind.

Die Protokollierung muss sowohl für die Betriebssystemebene (Windows) 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.

5. SICHERHEITS-PATCHES UND WEITERE KONFIGURATIONSDATEN

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

Zwischen AG u. AN ist ein geeignetes Verfahren zur Aktualisierung der Sicherheits-Patches für die Betriebszeit nach der Inbetriebnahme (Gewährleistungszeit) abzustimmen. Hierzu zählen auch eventuelle Fallback- bzw. Rollbackfunktionen für den Fall von fehlerhaften Sicherheits-Patches. Darüber hinaus muss die jeweilige Installation und eventuelle Deinstallation von Sicherheits-Patches 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. Firmware-Stände, Parametrierstände oder weitere Konfigurationsdaten.

Das Einspielen von Sicherheits-Patches 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.

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.

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 Antivirenscanner der Uniklinik Köln 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. Andernfalls sollte der Scanvorgang nicht kontinuierlich erfolgen, sondern kann in festzulegenden Zyklen oder auf Anforderung erfolgen (z. B. 1x täglich o. wöchentlich usw.).

Das vorgesehene Verfahren zur Aktualisierung der Virensignaturen ist zu beschreiben. Neue Virenpattern sind über eine Datenschluse in eine dafür vorgesehenen Demilitarisierten Zone (DMZ) einzuspielen. Der aktuell verwendete Stand der Virensignaturen ist in geeigneter Weise zu dokumentieren.

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.

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.

10. NETZWERKZUGÄNGE INNERHALB DER IT/MT/OT-SYSTEME

Alle Netzwerkzugänge innerhalb von IT/MT/OT-Systemen sind gem. Abschnitt 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.

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

11. VERBINDUNG 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.

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. 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.

Jeder Einzelfall 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.

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.

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, Jump-Host) des AG erfolgen. Die Authentifizierung mit dem Zugangsserver muss über eine Multi-Faktor-Authentifizierung sichergestellt sein.

Der Zugriff auf einen Fernzugang muss zentral geloggt und wiederholte Fehlversuche gemeldet werden. Alle Fern-Zugangs-Möglichkeiten 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.

14. VERSCHLÜSSELUNG VERTRAULICHER DATEN

Vertrauliche Informationen und Daten sind nur verschlüsselt zu speichern und zu übertragen.

Zur Sicherstellung des Schutzes von vertraulichen oder personenbezogenen Daten, hat der AN eine Auflistung von den verarbeitenden Information 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.

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.

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. 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 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 des AG 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. IDS, 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.

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 fehlgeschlagene 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.

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 Rückversicherungsverfahren sind ausführlich zu dokumentieren.

Das zur Anwendung kommende Verfahren ist mit dem AG abzustimmen.

19. UMGANG MIT NICHT MEHR GENUTZTEN DATENTRÄGERN U. 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.

20. UMGANG MIT SERVICE-LAPTOPS DES AN

Zur Konfiguration, Parametrierung oder ähnlichen Tätigkeiten, sind vorzugsweise 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.

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.

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 beschreiben, 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.

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.

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.



Abkürzung/ Begriff	Beschreibung
UKK	Uniklinik Köln
B3S	Branchenspezifischer Sicherheitsstandard
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.
AG	Auftraggeber
AN	Auftragnehmer
ISO	International Organization for Standardization / Internationale Organisation für Normung
IEC	International Electrotechnical Commission / Internationale Elektrotechnische Kommission - Normungsorganisation für Normen im Bereich der Elektrotechnik und Elektronik
DIN EN	Deutsches Institut für Normung / EN Europäische Norm
IBN	Inbetriebnahme
ISB	Informationssicherheitsbeauftragter
ISMS	Informationssicherheitsmanagementsystem
SPS	Speicherprogrammierbare Steuerung – Gerät für Steuer- und Regelungszwecke
DMZ	Demilitarisierte Zone
USB	Universal Serial Bus
PAM	Privileged Access Management – System zur Autorisierung und Überwachung von Benutzern



sftp	Secure/SSH File Transfer Protocol – verschlüsseltes Dateiübertragungsprotokoll
BSI	Bundesamt für Sicherheit in der Informationstechnik
IDS	Intrusion Detection System - System zur Erkennung von Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind
Mitm	Man in the middle – Eine Angriffsform, bei der Angreifer sich unbemerkt in eine Kommunikation zwischen verschiedenen Partnern einschaltet
SPAN	Switch Port Analyser - spezieller Port an einem Switch, der eine gespiegelte Kopie des Netzwerkverkehrs innerhalb des Switches an ein Ziel sendet
NAS	Network Attached Storage - konfigurierbarer Datenspeicher, um in einem Netzwerk Speicherplatz zur Verfügung zu stellen.



Dokumentenart	LL = Leitlinie / RL = Richtlinie / AA = Arbeitsanweisung / MU = Mitgeltende Unterlage / FO = Formular / AZ = Aufzeichnung
Dokumententitel	Mindeststandard Informationssicherheit
Dokumentennummer	#17_ISMS_Mindeststandard_Informationssicherheit
Revision	1.0
Autor	A. Wirtz
Geltungsbereich	UKK Konzern
Freigegeben ab	01.08.2023
Freigabe durch	B. Upadek
Vertraulichkeit	UKK-Offen
Mitgeltende Dokumente	

Hinweis: Ausgedruckte Dokumente unterliegen nicht dem Änderungsdienst.