



Informationssicherheitsanforderungen für IT-Lieferantenbeziehungen

Uniklinik Köln



Informationssicherheit in der Uniklinik Köln





Inhaltsverzeichnis

A.	Einleitung	3
B.	Zugrundeliegende Anforderungen	3
C.	Management von Lieferantenbeziehungen	5
1.	Informationssicherheit in Lieferantenbeziehungen	5
2.	Verpflichtungserklärung	5
2.1	Verpflichtung zur Informationssicherheit und zum Datenschutz	5
2.2	Zuverlässigkeit in Lieferantenbeziehungen	6
2.3	Änderung oder Beendigung von Lieferantenverträgen	6
2.4	Informationssicherheitsbewusstsein, -ausbildung und -schulung	6
3.	Sicherheitsanforderungen an Lieferanten (je nach Art der Dienstleistung anzuwenden)	7
3.1	Organisatorische Anforderungen	7
3.1.1	Organisation der Informationssicherheit	7
3.1.2	Dokumentation	7
3.1.3	Benachrichtigung über sicherheitsrelevante Vorfälle	8
3.1.4	Asset-Management	8
3.1.5	Human-Resources-Security	8
3.1.6	Physische und umgebungsbezogene Sicherheit	9
3.1.7	Sichere Anmeldeverfahren	9
3.1.8	Audits	9
3.1.9	Aufrechterhaltung der Informationssicherheit	10
3.2	Technische Anforderungen	10
3.2.1	Vulnerability Management	10
3.2.2	Patch Management	10
3.2.3	Maßnahmen gegen Schadsoftware	10
3.2.4	Systemhärtung	11
3.2.5	Fernzugang für Drittanbieter	11
3.2.6	Anforderungen an Softwareentwicklungsprozesse	12
3.2.7	Einsatz kryptographischer Lösungen	12
D.	Glossar	12



E. Dokumenteninformation 12

A. EINLEITUNG

Lieferanten, deren Leistungen (in Form von Software, Hardware oder Dienstleistungen für Systeme) für die kritische Dienstleistungen der medizinischen Versorgung eingesetzt werden, müssen bezüglich der Qualität ihrer Arbeit und der Einhaltung von Maßnahmen zur Informationssicherheit die folgenden Mindestanforderungen erfüllen. Die beschriebenen Mindestanforderungen werden zudem zur internen Bewertung herangezogen.

B. ZUGRUNDELIEGENDE ANFORDERUNGEN

Diesem Dokument liegen die in der folgenden Tabelle aufgeführten Anforderungen zugrunde.

Anforderung	Beschreibung
DIN ISO/IEC 27001:2013	
A.15.1.1	Informationssicherheitsrichtlinie für Lieferantenbeziehungen
A.15.1.2	Behandlung von Sicherheit in Lieferantenvereinbarungen
A.15.1.3	Lieferkette für Informations- und Kommunikationstechnologie
A.15.2.1	Überwachung und Überprüfung von Lieferantendienstleistungen
A.15.2.2	Handhabung der Änderungen von Lieferantendienstleistungen

Anforderung	Beschreibung
B3S	
ANF-MN 70	Zur Sensibilisierung und Schaffung eines Informationssicherheitsbewusstseins MÜSSEN regelmäßig (mindestens alle zwei Jahre) IT-Sicherheitsschulungen der Mitarbeiter und gegebenenfalls im Informationsverbund tätigen Dienstleister durchgeführt und entsprechende Schulungsmaterialien angeboten werden. Darüber hinaus SOLL durch geeignete Maßnahmen sichergestellt werden, dass auch Dienstleister ihre Verantwortlichkeiten im Hinblick auf den sicherheitsbewussten Umgang mit Unternehmens-Informationen verstehen.



ANF-MN 88	Es MÜSSEN Richtlinien für den sicheren Umgang bei einem betrieblichen Datenaustausch mit externen Partnern festgelegt werden.
ANF-MN 89	Es MUSS eine allgemeine Risikobewertung für den Zugang Dritter zu Gesundheitsdaten erfolgen, die auch die potenzielle Gefahr des unberechtigten Zugangs zu Systemen, Daten und Gesundheitsinformationen, die für die Aufrechterhaltung der kritischen Dienstleistung notwendig sind, durch Lieferanten, Dienstleister und Dritte berücksichtigt. Gegebenenfalls ist das bestehende Sicherheitsniveau und die hierfür verwendete Technik anzupassen.
ANF-MN 90	Im Umgang mit Lieferanten, Dienstleistern und Dritten MÜSSEN zum Schutz der Unternehmenswerte Leitlinien zur Aufrechterhaltung der Anforderungen an die eigene Informationssicherheit erstellt, den Lieferanten bekanntgegeben und dies dokumentiert werden.
ANF-MN 91	Lieferanten, Dienstleistern und Dritten SOLL die Informationssicherheitsleitlinie und weitere relevante Regelungen der Informationssicherheit vor Beauftragung (z.B. als Vertragsbestandteil) verbindlich gemacht werden.
ANF-MN 92	Bei der Auslagerung wesentlicher Bereiche, Prozesse oder Systeme, die für die Erbringung der kritischen Dienstleistung notwendig sind, an externe Dienstleister MUSS die Absenkung des Sicherheitsniveaus vermieden werden. Der Auftraggeber MUSS die Einhaltung des für ihn gültigen Sicherheitsniveaus durch geeignete vertragliche und organisatorische Maßnahmen seitens des Dienstleisters sicherstellen.
ANF-MN 134	Die Berücksichtigung von Anforderungen an Informationssicherheit MUSS für die Bereiche Informationstechnik, Medizintechnik, Kommunikationstechnik und Versorgungstechnik als wesentliches Merkmal / Kriterium für Beschaffungsprozesse etabliert werden.
ANF-MN 135	Der Informationssicherheitsbeauftragte SOLL in alle relevanten Beschaffungsprozesse eingebunden werden.



C. MANAGEMENT VON LIEFERANTENBEZIEHUNGEN

1. INFORMATIONSSICHERHEIT IN LIEFERANTENBEZIEHUNGEN

Durch Outsourcing bzw. die Beschaffung von Produkten oder Dienstleistungen darf sich das Niveau des Datenschutzes und der Informationssicherheit der Uniklinik Köln nicht verschlechtern oder herabsenken.

Die Uniklinik Köln empfiehlt Lieferanten von Produkten und Dienstleistungen mit datenschutzrechtlicher bzw. informationssicherheitstechnischer Relevanz, ein Managementsystem für den Datenschutz bzw. die Informationssicherheit umzusetzen. 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 Auftragnehmer 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.

Falls vom Auftragnehmer kein geeignetes Managementsystem zum Datenschutz bzw. zur Informationssicherheit umgesetzt worden ist oder der Geltungsbereich des Managementsystems die gelieferten Dienstleistungen bzw. Produkte nicht miteinschließt, so gelten die Anforderungen dieser Richtlinie für Auftragnehmer ab Kapitel 3. Dabei müssen jedoch nur die Anforderungen erfüllt werden, die für die jeweilige Dienstleistung bzw. das Produkt auch relevant sind.

Welche Anforderungen ab Kapitel 3 relevant sind, wird von der Uniklinik Köln im Rahmen der Ausschreibung bzw. der Beschaffung festgelegt.

Anforderungen in Ausschreibungen bzw. Verträgen gelten unabhängig von den Anforderungen dieser Richtlinie für den Auftragnehmer.

2. VERPFLICHTUNGSERKLÄRUNG

2.1 Verpflichtung zur Informationssicherheit und zum Datenschutz

Der Auftragnehmer verpflichtet sich in Bezug auf die Lieferantenbeziehung mit der Uniklinik Köln zur Einhaltung der Informationssicherheit. Dabei müssen vor allem die Schutzziele

Vertraulichkeit, Verfügbarkeit, Authentizität, Patientensicherheit (da wo anwendbar) und Integrität gewahrt werden.

Die zur Gewährleistung der Informationssicherheit und zur Umsetzung der gesetzlichen Anforderungen im Bereich des Datenschutzes erforderlichen Aufgaben und Pflichten der Uniklinik Köln sind in einer Leitlinie zur Informationssicherheit festgehalten. Die Uniklinik Köln verpflichtet sich, diese Leitlinie den relevanten Auftragnehmern zur Verfügung zu stellen.

Alle Mitarbeiter des Auftragnehmers sind aufgefordert, im Rahmen ihrer Tätigkeit für die Uniklinik Köln auf die Einhaltung der in dieser Leitlinie definierten Ziele hinzuwirken.

Für den Fall, dass sich die Dienstleistung auf die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten bezieht, sind die entsprechenden Vorschriften des Datenschutzes von Seiten des Dienstleisters einzuhalten. Einzelheiten dazu werden im Vertrag zur Auftragsverarbeitung festgelegt.

Der Auftragnehmer muss sicherstellen, dass alle Mitarbeiter, die im Zusammenhang mit der gelieferten Dienstleistung bzw. des gelieferten Produktes Zugriff auf Informationswerte der Uniklinik Köln erhalten können, nachweislich auf die Vertraulichkeit im Umgang mit den Werten der Uniklinik Köln verpflichtet werden.

2.2 Zuverlässigkeit in Lieferantenbeziehungen

Der Auftragnehmer verpflichtet sich, sich stets um eine zuverlässige Anlieferung von Produkten und Erfüllung von Dienstleistungen ohne zeitlichen Verzug zu bemühen. Unregelmäßigkeiten in der Lieferantenbeziehung, bezogen auf die Produktlieferkette oder zeitliche und qualitative Erfüllung der Dienstleistung laut Vertrag sind der Uniklinik Köln unverzüglich mitzuteilen.

2.3 Änderung oder Beendigung von Lieferantenverträgen

Änderungen bei der Bereitstellung von Dienstleistungen, in den Dienstleistungsangeboten oder bei der Dienstleistungserbringung sind rechtzeitig anzukündigen und sollten durch den Auftragnehmer nicht ohne Abstimmung mit der Uniklinik Köln erfolgen. Möglicherweise ist daraufhin die Anpassung eines Vertrages inkl. einer erneuten Risikobewertung erforderlich.

2.4 Informationssicherheitsbewusstsein, -ausbildung und -schulung

Zur Sensibilisierung und Schaffung eines Informationssicherheitsbewusstseins MÜSSEN regelmäßig (mindestens alle zwei Jahre) IT-Sicherheitsschulungen der Mitarbeiter und gegebenenfalls im Informationsverbund tätigen Dienstleistern durchgeführt und entsprechende Schulungsmaterialien angeboten werden. Darüber hinaus SOLL durch geeignete Maßnahmen sichergestellt werden, dass auch Dienstleister ihre Verantwortlichkeiten im Hinblick auf den sicherheitsbewussten Umgang mit Unternehmens-Informationen verstehen.

Der Auftragnehmer muss sicherstellen, dass alle Mitarbeiter, die im Zusammenhang mit der gelieferten Dienstleistung bzw. des gelieferten Produktes Zugriff auf Informationswerte der Uniklinik Köln erhalten können, in angemessenem Umfang zur Informationssicherheit und gegebenenfalls zum Datenschutz geschult und sensibilisiert worden sind. Der Nachweis über die Schulung bzw. Sensibilisierung seiner Mitarbeiter muss vom Dienstleister auf Nachfrage erbracht werden können.

Bei Bedarf besteht die Möglichkeit, dass Mitarbeiter des Auftragnehmers an internen Schulungen zur Informationssicherheit und oder zum Datenschutz der Uniklinik Köln teilnehmen können.

Auch die Informationssicherheitsleitlinie sowie die für die Dienstleistung relevanten Richtlinien zur Informationssicherheit der Uniklinik Köln dienen der Vermittlung eines Informationssicherheitsbewusstseins beim Auftragnehmer und können diesem bei Bedarf zur Verfügung gestellt werden.

3. SICHERHEITSANFORDERUNGEN AN LIEFERANTEN (JE NACH ART DER DIENSTLEISTUNG ANZUWENDEN)

3.1 Organisatorische Anforderungen

3.1.1 Organisation der Informationssicherheit

Der Auftragnehmer hat dem Antrag der Uniklinik Köln nachzukommen, Informationen seiner Sicherheitsorganisation offenzulegen, auf deren Basis die Uniklinik Köln eine Bewertung des Auftragnehmers durchführen kann. Diese Einschätzung ist ein interner Prozess, der die Uniklinik Köln dabei unterstützt, die Metriken und Reife der Sicherheitsorganisation des Auftragnehmers zu beurteilen. Der Auftragnehmer soll, falls vorhanden, ein ISO/IEC 27001-Zertifikat oder Äquivalente sowie weitere Dokumente wie Berichte und Vorschriften etc. in diesem Kontext bereitstellen.

3.1.2 Dokumentation

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

Es wird vom Auftragnehmer 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 Auftragnehmer erwartet, diese in die Dokumentation einzupflegen.

3.1.3 Benachrichtigung über sicherheitsrelevante Vorfälle

Der Auftragnehmer ist verpflichtet, Sicherheitsvorfälle in seiner Organisation, die potenziell einen negativen Effekt auf materielle und immaterielle gelieferte Dienstleistungen oder das Informationssicherheitsniveau der Uniklinik Köln haben könnten, umgehend ohne Zeitverzug der Uniklinik Köln zu melden. Dies könnte z.B. auch Industriespionage oder eine Sicherheitslücke im Source-Code sein.

Der Auftragnehmer wird im Falle eines Vorfalls auf Nachfrage der Uniklinik Köln Ressourcen zur Minderung und/oder Beseitigung des Vorfalles sowie den finalen Korrekturbericht bereitstellen.

3.1.4 Asset-Management

Der Auftragnehmer hat alle Assets in seinem Informationssystem zu identifizieren und zu dokumentieren, die einen Bezug zu Systemen der Uniklinik Köln 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 Auftragnehmer die Anwendung spezifischer Sicherheitsmaßnahmen delegieren, jedoch bleibt der Auftragnehmer für den angemessenen Schutz der Assets, die in Bezug zum Informationssystem der Uniklinik Köln stehen, verantwortlich.

3.1.5 Human-Resources-Security

Jeder, der im Namen des Auftragnehmers agiert, der entfernten oder lokalen Zugriff auf Systeme der Uniklinik Köln haben muss, muss Informationen zu seiner Identität bereitstellen. Der Auftragnehmer stellt sicher, dass in seinem Namen kein Zugang missbraucht wird und er die volle Verantwortung übernimmt, sollte sich herausstellen, dass dieser Fall eintritt.

Sollte der Auftragnehmer mit Subunternehmern zusammenarbeiten, um den Vertrag mit der Uniklinik Köln zu erfüllen, muss der Auftragnehmer diesen ausdrücklich als Subunternehmer

identifizieren und er muss sicherstellen, dass der Subunternehmer die gleichen Anforderungen erfüllt.

Auf Verlangen der Uniklinik Köln ist der Auftragnehmer verpflichtet, nur überprüfetes Sicherheitspersonal, z.B. geprüft von nationalen Behörden, zum Umgang mit sensiblen Equipment einzusetzen, sowohl vor der Integration in das Netzwerk der Uniklinik Köln als auch für die Wartung.

Der Auftragnehmer beauftragt nur Personen, die über entsprechende Kenntnisse und Fähigkeiten bzgl. Installation, Soft- oder Hardware, Wartung oder Betrieb der Lösung verfügen.

3.1.6 Physische und umgebungsbezogene Sicherheit

Der Auftragnehmer hat dafür Sorge zu tragen, dass der unbefugte Zutritt in Räume, Büros und Einrichtungen, in denen Informationen der Uniklinik Köln 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 Auftragnehmers sind Richtlinien zu erstellen, die aufgeräumte Arbeitsumgebungen sowie Bildschirmsperren bei Nichtbenutzung regeln.

3.1.7 Sichere Anmeldeverfahren

Der Zugriff des Auftragnehmers auf Systeme der Uniklinik Köln darf ausschließlich über die von der Uniklinik Köln vorgegebenen Prozeduren und autorisierten Zugänge erfolgen.

Falls der Zugang über zwei Faktoren unter Verwendung eines Zugangstokens autorisiert wird, so muss der Auftragnehmer sicherstellen, dass der Zugriff auf das Token ausschließlich von dazu autorisierten Mitarbeitern ausgeübt werden kann. Die Token müssen, sofern sie nicht verwendet werden, ständig unter Verschluss gehalten werden.

3.1.8 Audits

Der Auftragnehmer stimmt zu, dass die Uniklinik Köln oder ein von dieser beauftragter Dritter im Auftrag der Uniklinik Köln die Organisation in Bezug auf die Informationssicherheit des Auftragnehmers auditieren darf. Dies kann einmal oder mehrmals geschehen. Die Prüfungen werden auf der Grundlage der von dem Auftragnehmer zur Verfügung gestellten Dokumentation durchgeführt. Der genaue Umfang, die Dauer und die Organisation werden jeweils einvernehmlich vereinbart.

Zusätzlich muss der Auftragnehmer die Abweichungen von den vereinbarten Sicherheitsanforderungen melden.

3.1.9 Aufrechterhaltung der Informationssicherheit

Der Auftragnehmer 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 der beauftragten Dienstleistung kann dazu in Abstimmung mit der Uniklinik Köln bestimmt werden. Der Auftragnehmer legt Prozesse, Verfahren und Maßnahmen fest, dokumentiert diese und setzt sie um, um das erforderliche Niveau an Informationssicherheit auch in widrigen Situationen aufrechterhalten zu können. Die Wirksamkeit der Maßnahmen soll von Seiten des Auftragnehmers in regelmäßigen Abständen geprüft werden. Die Prüfungen sollen dokumentiert werden.

3.2 Technische Anforderungen

3.2.1 Vulnerability Management

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

Sind vom Auftragnehmer entwickelte Software-, Firmware- oder Hardware-Komponenten betroffen, ist der Auftragnehmer verpflichtet, umgehend die Schwachstellen an die Uniklinik Köln 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 die Uniklinik Köln festgelegt werden. Der Umfang des Vulnerability Managements umfasst jede potenzielle Schwachstelle, die möglicherweise Einfluss auf die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der Vermögenswerte (materielle oder immaterielle) oder auf eine bei der Uniklinik Köln operierende Dienstleistung des Auftragnehmers nehmen kann.

3.2.2 Patch Management

Der Auftragnehmer verpflichtet sich, mindestens zweimal pro Jahr Updates und Patches bereitzustellen.

Der Auftragnehmer soll für jede im Patchzyklus adressierte Schwachstelle einen Bericht erstellen und der Uniklinik Köln zur Verfügung stellen. Dieser kann detaillierte oder aggregierte Daten unter Berücksichtigung der Kritikalitätsstufe und der betroffenen Bereiche (Verfügbarkeit, Integrität, Authentizität und/oder Vertraulichkeit) enthalten.

3.2.3 Maßnahmen gegen Schadsoftware

Der Auftragnehmer muss sicherstellen, dass auf allen Systemen, die mittelbar oder unmittelbar im Zusammenhang mit der Dienstleistungserbringung verwendet werden, in angemessenem

Umfang Maßnahmen zur Abwehr von Schadcode getroffen werden. Softwareprodukte zur Abwehr von Schadcode und Schadcode-Definitionen sind ständig aktuell zu halten. Davon betroffen sind im Besonderen solche Geräte, die für Supporttätigkeiten für oder bei der Uniklinik Köln Verwendung finden.

3.2.4 Systemhärtung

Der Auftragnehmer verpflichtet sich, die von ihm gelieferten Systeme zu härten, um die Auswirkungen potenzieller Sicherheitsrisiken zu minimieren.

Dabei gelten folgende Anforderungen:

- minimale Installationsprinzipien
- Jeder nicht benötigte Netzwerkzugang (TCP/IP- oder UDP-Port) muss deaktiviert sein. Die Nutzung jedes Zugangs muss in der Dokumentation erläutert werden.
- Insofern zusätzlich vereinbart, müssen die durch die Uniklinik Köln vorgegebenen allgemeinen Konfigurationsstandards und Sicherheitsvorschriften eingehalten werden.
- Der Auftragnehmer stellt sicher, dass jedes Standardpasswort in allen möglichen Fällen geändert werden kann.
- Der Auftragnehmer muss im Rahmen seiner Möglichkeiten sicherstellen, dass seine Lösungen frei von „Backdoors“ sind, die die verwendeten Sicherheitsmechanismen umgehen können.
- Der Auftragnehmer verpflichtet sich, dass er hinsichtlich seiner Produkte mit geeigneten Maßnahmen und Protokollen, die mit der Uniklinik Köln separat abzustimmen sind, nachweist, dass alle in diesem Abschnitt genannten Anforderungen eingehalten werden.

3.2.5 Fernzugang für Drittanbieter

Fernzugänge von Drittanbietern zum Netzwerk der Uniklinik Köln werden unter den folgenden Bedingungen gestattet:

- Der Auftragnehmer muss sicherstellen, dass bei Fernzugängen die Vertraulichkeit, Verfügbarkeit, Authentizität und Integrität der Assets und Services der Uniklinik Köln gewährleistet sind. Dies beinhaltet auch die nachträgliche Verwendung von Informationen, von denen der Auftragnehmer während eines Fernzugriffes Kenntnis erlangt hat. Er ist für alle Aktionen der Benutzerkonten mit Fernzugangsfunktion auf Systemen des Auftraggebers verantwortlich.
- Jeder Nutzer eines Fernwartungszugangs muss ein personalisiertes Nutzerkonto besitzen. Ausnahmen sind zu dokumentieren. Bei Ausnahmen muss die komplette Rückverfolgbarkeit der Nutzung eines Accounts (wer, wann) festgehalten und der Uniklinik Köln auf Verlangen ausgehändigt werden.



- Nicht mehr benötigte Zugänge müssen unverzüglich der Uniklinik Köln gemeldet werden, so dass diese gesperrt werden können.

3.2.6 Anforderungen an Softwareentwicklungsprozesse

Insofern Auftragnehmer Software für die Uniklinik Köln entwickeln, müssen die Prinzipien des Security by Design eingehalten und sich an den allgemein anerkannten Industriestandards orientiert werden.

3.2.7 Einsatz kryptographischer Lösungen

Um sicherzustellen, dass keine veralteten und als unsicher bekannten Kryptografielösungen in den Produkten verwendet werden, soll der Auftragnehmer eine schriftliche Richtlinie etablieren und mit der Uniklinik Köln abstimmen, die die zulässigen Kryptografiealgorithmen definiert. Diese Richtlinie sollte sich an einen Industriestandard halten (z.B. BSI TR-02102) und regelmäßig durch den Auftragnehmer überprüft werden.

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

D. GLOSSAR

Kein Eintrag.

E. DOKUMENTENINFORMATION

Dokumentenart	LL = Leitlinie / RL = Richtlinie / AA = Arbeitsanweisung / MU = Mitgeltende Unterlage / FO = Formular / AZ = Aufzeichnung
Dokumententitel	Informationssicherheitsanforderungen für Lieferanten
Dokumentnummer	0160-2
Revision	03



Autor	Stabstelle Informationssicherheit
Geltungsbereich	uk-it
Freigegeben ab	05.10.2022
Freigabe durch	B. Upadek
Vertraulichkeit	TLP-WHITE
Mitgeltende Dokumente	Keine

Hinweis: Bei ausgedrucktem Dokument aktuelle Revision in qualido prüfen. Gültig ist die in qualido abrufbare Revision.



Erklärung Schutzklassen für die Vertraulichkeit von Dokumenten und Informationen basierend auf dem TLP: Traffic Light Protocol

TLP-WHITE: Öffentlich (Klassifizierung gemäß Datenschutz: Normal)

Mit TLP-WHITE werden Dokumente und Informationen gekennzeichnet, die öffentlich verfügbar sind oder öffentlich verfügbar gemacht werden.

Abgesehen von urheberrechtlichen Aspekten dürfen Dokumente und Informationen der Klasse TLP-WHITE ohne Einschränkungen frei weitergegeben werden.

TLP-GREEN: Intern - Organisationsübergreifende Verteilung (UKK) (Klassifizierung gemäß Datenschutz: Normal)

Mit TLP-GREEN werden Dokumente und Informationen gekennzeichnet, die organisationsübergreifend innerhalb der Uniklinik Köln incl. der Tochterunternehmen verfügbar gemacht werden dürfen. Dokumente und Informationen dieser Klasse dürfen innerhalb der Uniklinik und an Partner, die bezüglich Vertraulichkeit schriftlich verpflichtet sind, weitergegeben oder eingesehen werden. Die Information darf jedoch nicht veröffentlicht werden. Eine Präsentation der Informationen im Intranet der Uniklinik Köln ist zulässig.

TLP-AMBER: Vertraulich - Organisationsinterne Verteilung innerhalb eines Bereiches (hier uk-it) (Klassifizierung gemäß Datenschutz: Hoch)

Mit TLP-AMBER werden Dokumente und Informationen gekennzeichnet, die nur innerhalb eines Bereiches (hier uk-it) verfügbar gemacht werden dürfen. Dokumente und Informationen dieser Klasse dürfen innerhalb des Bereiches (hier uk-it) und an Partner, die bezüglich Vertraulichkeit schriftlich verpflichtet sind, weitergegeben oder eingesehen werden.

Informationen in dieser Klasse können vom Ersteller bezüglich der zulässigen Empfänger weiter eingeschränkt werden. Der Informationsersteller muss diese zusätzlich beabsichtigten Einschränkungen der Weitergabe klar spezifizieren.

TLP-RED: Streng Vertraulich - nur für benannte Empfänger (Klassifizierung gemäß Datenschutz: Sehr Hoch)

Mit TLP-RED werden Dokumente und Informationen gekennzeichnet, die nur einzelnen Personen oder Personengruppen verfügbar gemacht werden dürfen. Hierzu zählen insbesondere personen- oder patientenbezogene Dokumente und Informationen.

Die Datenverarbeitung von TLP-RED deklarierten Dokumenten und Informationen ist nur in den von der Uniklinik dafür vorgesehen IT-Systemen zulässig.

TLP-RED-Informationen im Rahmen von Besprechungen, Video-/Telefonkonferenzen sind auf den Kreis der Anwesenden bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. In den meisten Fällen werden TLP-RED-Informationen im Rahmen dieser Kommunikation mündlich oder persönlich übergeben.