

Informationssicherheitsanforderungen an Lieferanten, Dienstleister und Dritte

des Städtischen Klinikums Braunschweig und dessen Tochtergesellschaften



Städtisches Klinikum Braunschweig gGmbH
Freisestraße 9-10 | 38118 Braunschweig
www.skbs.de

STÄDTISCHES KLINIKUM
BRAUNSCHWEIG

Geschäftsführung: Jan-Olaf Klok, Sascha Altendorf
Aufsichtsrat: Erster Stadtrat Christian A. Geiger, Vorsitzender

Inhaltsverzeichnis

1. Ziel, Zweck und Geltungsbereich.....	4
2. Grundsätze und Verantwortlichkeiten	4
3. Grundlagen und Rechtsrahmen.....	5
4. Informationssicherheit in Lieferantenbeziehungen	5
4.1. Allgemeiner Grundsatz.....	5
4.2. Managementsysteme und Nachweisfähigkeit	6
4.3. Anforderungen bei fehlendem oder eingeschränktem Managementsystem	6
4.4. Vorrang spezifischer Ausschreibungs- und Vertragsanforderungen.....	6
4.5. Unterauftragnehmer und Lieferkette	7
5. Verpflichtungserklärung.....	7
5.1. Verpflichtung zur Informationssicherheit und zum Datenschutz	7
5.2. Verpflichtung und Eignung der Mitarbeitenden des Auftragnehmers.....	7
5.3. Umgang mit personenbezogenen Daten	8
5.4. Dokumentation und Nachweise	8
6. Sicherheitsanforderungen an Lieferanten.....	9
6.1. Organisatorische Anforderungen	9
6.1.1. Sicherheitsorganisation und Auskunftspflichten	9
6.1.2. Dokumentation.....	9
6.1.3. Asset-Management.....	10
6.1.4. Personalbezogene Sicherheitsanforderungen	10
6.1.5. Physische und umgebungsbezogene Sicherheit	10
6.1.6. Sichere Zugangs- und Anmeldeverfahren	10
6.1.7. Audits, Prüf- und Kontrollrechte	10
6.1.8. Meldung sicherheitsrelevanter Vorfälle	11
6.1.9. Aufrechterhaltung der Informationssicherheit und Leistungsfähigkeit.....	11
6.1.10. Beendigung der Leistungserbringung und Exit-Regelungen	11
6.2. Technische Anforderungen	11
6.2.1. Vulnerability Management	11
6.2.2. Patch- und Update-Management.....	12
6.2.3. Schutz vor Schadsoftware	12
6.2.4. Sichere Konfiguration und Systemhärtung.....	12
6.2.5. Fernzugänge durch Dritte.....	13

6.2.6. Anforderungen an Entwicklungs- und Änderungsprozesse.....	13
6.2.7. Kryptographische Sicherungsmaßnahmen	13
6.2.8. Protokollierung und Nachvollziehbarkeit	14
6.2.9. Datensicherung und Wiederherstellbarkeit	14
7. Überwachung und kontinuierliche Verbesserung	14
8. Inkrafttreten	14

1. Ziel, Zweck und Geltungsbereich

Diese Leitlinie legt die verbindlichen Informationssicherheitsanforderungen für alle Lieferanten, Dienstleister, Auftragnehmer, Unterauftragnehmer sowie sonstigen Dritten fest, deren Leistungen Informationen, Daten, Systeme, Anwendungen, Netze, technische Komponenten oder kritische bzw. sicherheitsrelevante Dienstleistungen des städtischen Klinikums Braunschweig (skbs) betreffen, unterstützen oder beeinflussen.

Ziel dieser Leitlinie ist es, Risiken aus Lieferanten- und Dienstleisterbeziehungen wirksam zu steuern, ein angemessenes und nachweisbares Sicherheitsniveau entlang der gesamten Liefer- und Leistungskette sicherzustellen sowie die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität dauerhaft zu gewährleisten. Darüber hinaus dient diese Leitlinie dem Schutz der Patientensicherheit, der Behandlungskontinuität sowie der Betriebsfähigkeit klinischer und administrativer Prozesse.

Die Vorgaben dieser Leitlinie sind verbindlich anzuwenden, sobald externe Leistungen schutzbedürftige Informationen, personenbezogene Daten, sicherheitsrelevante Systeme, technische oder organisatorische Schnittstellen oder kritische bzw. klinisch relevante Prozesse und Dienstleistungen des skbs berühren. Sie sind in diesen Fällen Bestandteil der jeweiligen Ausschreibung, Bestellung, Beauftragung oder vertraglichen Vereinbarung, sofern keine gleichwertigen oder strengeren Regelungen gelten.

Die Anforderungen gelten entsprechend für Tochtergesellschaften des skbs, soweit diese in die jeweilige Vertrags- und Leistungsbeziehung einbezogen sind.

2. Grundsätze und Verantwortlichkeiten

Informationssicherheit in Lieferantenbeziehungen ist integraler Bestandteil der Unternehmenssteuerung, des Risikomanagements und der regulatorischen Compliance des skbs. Externe Leistungen sind so zu erbringen, dass die festgelegten Sicherheitsanforderungen des skbs jederzeit gewahrt bleiben.

Die zuständigen Organisationseinheiten des skbs wirken bei Auswahl, Bewertung, Beauftragung und Überwachung von Lieferanten und Dienstleistern risikoorientiert zusammen. Dies umfasst insbesondere die einbindungsbezogene Berücksichtigung von Informationssicherheit, Datenschutz, betrieblicher Kritikalität, technischer Abhängigkeit sowie Auswirkungen auf die medizinische Versorgung.

Der jeweilige Auftraggeber innerhalb des skbs stellt sicher, dass die einschlägigen Anforderungen dieser Leitlinie frühzeitig in Ausschreibungen, Leistungsbeschreibungen, Vergaben und Verträgen berücksichtigt werden. Der Auftragnehmer ist verpflichtet, die für die jeweilige Leistung relevanten Anforderungen nachweislich umzusetzen und auf Verlangen des skbs geeignete Nachweise vorzulegen.

3. Grundlagen und Rechtsrahmen

Diese Leitlinie orientiert sich insbesondere an folgenden Vorgaben und anerkannten Standards:

- B3S „Medizinische Versorgung“ in der jeweils gültigen Fassung,
- ISO/IEC 27001 in der jeweils gültigen Fassung,
- ISO/IEC 27002 in der jeweils gültigen Fassung, insbesondere zu Lieferantenbeziehungen und ICT-Readiness,
- KRITIS-Verordnung (KritisV),
- einschlägigen Anforderungen aus dem Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung,
- geltenden datenschutzrechtlichen Vorgaben, insbesondere Datenschutz-Grundverordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG),
- einschlägigen Anforderungen des BSI sowie weiteren anwendbaren gesetzlichen und regulatorischen Vorgaben.

Die in der ISO/IEC 27002 beschriebenen Maßnahmen zu Lieferantenbeziehungen, zur Informationssicherheit in der Lieferkette sowie zum Umgang mit ICT-Dienstleistungen werden durch diese Leitlinie für das skbs konkretisiert.

Ergänzend sind die für die jeweilige Liefer- und Leistungsbeziehung einschlägigen regulatorischen Anforderungen aus der Umsetzung der NIS-2-Richtlinie zu berücksichtigen.

4. Informationssicherheit in Lieferantenbeziehungen

4.1. Allgemeiner Grundsatz

Der Auftragnehmer hat sicherzustellen, dass durch die Leistungserbringung, einschließlich Outsourcing, Fremdvergabe, Beschaffung oder den Bezug von Produkten und Dienstleistungen, keine zusätzlichen oder unangemessen erhöhten Risiken für die Informationssicherheit, den Datenschutz, die Resilienz, die Betriebsstabilität oder die Patientensicherheit des skbs entstehen.

Lieferanten und Dienstleister sind verpflichtet, geeignete technische und organisatorische Maßnahmen zu implementieren, um mindestens ein dem Schutzbedarf der betroffenen Informationen, Systeme und Prozesse entsprechendes Sicherheitsniveau sicherzustellen. Dies gilt insbesondere bei Leistungen mit Bezug zu Patientendaten, medizinischen Fachanwendungen, kritischen Infrastrukturen, Fernwartungszugängen, klinischen Betriebsprozessen sowie zentralen IT- und Medizintechnikdiensten.

Verstöße gegen diese Anforderungen führen zu einer risikobasierten Neubewertung der Geschäftsbeziehung und können, abhängig von Art, Schwere, Dauer und Auswirkungen des Verstoßes, vertragliche, vergaberechtliche oder haftungsrechtliche Konsequenzen nach sich ziehen.

4.2. Managementsysteme und Nachweisfähigkeit

Das skbs erwartet von Lieferanten mit datenschutzrechtlicher, informationssicherheits-technischer oder betrieblicher Kritikalität ein strukturiertes Management von Informationssicherheit und – soweit einschlägig – Datenschutz. Hierfür sollen anerkannte Standards, insbesondere ISO/IEC 27001 oder BSI IT-Grundschutz, herangezogen werden.

Ein zertifiziertes Managementsystem ist nicht in jedem Fall verpflichtend. Es kann jedoch im Rahmen von Ausschreibungen, Leistungsbeschreibungen oder Verträgen verbindlich gefordert werden. Unabhängig hiervon muss der Auftragnehmer jederzeit in der Lage sein, die Angemessenheit und Wirksamkeit seiner Sicherheitsmaßnahmen nachvollziehbar und belastbar nachzuweisen.

4.3. Anforderungen bei fehlendem oder eingeschränktem Managementsystem

Verfügt der Auftragnehmer über kein geeignetes Managementsystem oder deckt der Geltungsbereich eines bestehenden Managementsystems die konkret beauftragte Leistung nicht vollständig ab, gelten die Anforderungen dieser Leitlinie unmittelbar und vollumfänglich, soweit sie für die jeweilige Leistung einschlägig sind.

Das skbs legt im Rahmen der Ausschreibung, Beschaffung, Beauftragung oder Vertragsgestaltung fest, welche Anforderungen dieser Leitlinie aufgrund von Schutzbedarf, Risikoprofil, Kritikalität der Dienstleistung und betroffenen Prozessen zwingend anzuwenden sind.

4.4. Vorrang spezifischer Ausschreibungs- und Vertragsanforderungen

Soweit in Ausschreibungen, Verträgen, Auftragsverarbeitungsverträgen, Service-Level-Vereinbarungen oder ergänzenden Sicherheitsvereinbarungen spezifische Anforderungen definiert sind, gehen diese den allgemeinen Regelungen dieser Leitlinie vor, sofern sie mindestens gleichwertig oder strenger sind.

4.5. Unterauftragnehmer und Lieferkette

Die Einbindung von Unterauftragnehmern bedarf, soweit vertraglich vorgesehen oder aufgrund des Schutzbedarfs erforderlich, der vorherigen Zustimmung des skbs. Der Auftragnehmer hat sicherzustellen, dass Unterauftragnehmer mindestens die gleichen Sicherheitsanforderungen erfüllen wie der Hauptauftragnehmer.

Der Auftragnehmer bleibt für die vollständige, ordnungsgemäße und nachweisbare Umsetzung der Anforderungen entlang seiner Liefer- und Leistungskette verantwortlich.

5. Verpflichtungserklärung

5.1. Verpflichtung zur Informationssicherheit und zum Datenschutz

Lieferanten, deren Leistungen in Form von Software, Hardware, Cloud-Diensten, technischen Services, Wartungsleistungen, Supportleistungen oder sonstigen Dienstleistungen für kritische oder sicherheitsrelevante Prozesse des skbs eingesetzt werden, verpflichten sich zur Einhaltung der Anforderungen dieser Leitlinie sowie der einschlägigen datenschutzrechtlichen und vertraglichen Vorgaben.

Der Auftragnehmer stellt dabei insbesondere sicher, dass folgende Schutzziele gewahrt werden:

- **Vertraulichkeit:** Schutz sensibler Informationen vor unbefugter Offenlegung und Kenntnisnahme,
- **Integrität:** Schutz von Informationen, Daten, Systemen und Prozessen vor unbefugter oder unbeabsichtigter Veränderung,
- **Verfügbarkeit:** Sicherstellung der erforderlichen Nutzbarkeit von Informationen, Anwendungen, Systemen und Dienstleistungen,
- **Authentizität:** Nachweisbarkeit der Echtheit von Informationen, Kommunikationspartnern und Transaktionen,
- **Patientensicherheit und Behandlungskontinuität:** Vermeidung von Beeinträchtigungen, die die medizinische Versorgung, klinische Prozesse oder die Sicherheit von Patientinnen und Patienten gefährden können.

5.2. Verpflichtung und Eignung der Mitarbeitenden des Auftragnehmers

Der Auftragnehmer stellt sicher, dass alle Mitarbeitenden, die im Rahmen der Leistungserbringung Zugang zu Informationen, Systemen, Anwendungen, Netzwerken oder Einrichtungen des skbs erhalten, vor ihrem Einsatz angemessen ausgewählt, auf ihre Aufgaben vorbereitet und nachweislich auf Vertraulichkeit verpflichtet werden.

Darüber hinaus ist sicherzustellen, dass:

- Mitarbeitende regelmäßig und anlassbezogen zu Informationssicherheit und Datenschutz sensibilisiert und geschult werden,
- Zugriffe ausschließlich auf Grundlage eines nachweisbaren dienstlichen Erfordernisses erfolgen,
- Rollen, Verantwortlichkeiten und Berechtigungen eindeutig festgelegt sind,
- bei Tätigkeiten mit erhöhtem Schutzbedarf zusätzliche Eignungs- oder Zuverlässigkeitsanforderungen berücksichtigt werden können, soweit rechtlich zulässig und sachlich erforderlich.

5.3. Umgang mit personenbezogenen Daten

Soweit im Rahmen der Leistungserbringung personenbezogene Daten verarbeitet werden, sind die geltenden datenschutzrechtlichen Vorschriften, insbesondere die Anforderungen der DSGVO, vollumfänglich einzuhalten. Erforderliche datenschutzrechtliche Vereinbarungen, insbesondere zur Auftragsverarbeitung, sind vor Beginn der Verarbeitung rechtswirksam abzuschließen.

Der Auftragnehmer hat insbesondere sicherzustellen:

- die Umsetzung angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten,
- die rechtzeitige und vollständige Meldung datenschutzrelevanter Vorfälle an das skbs,
- die Unterstützung des skbs bei gesetzlichen Melde-, Informations- und Nachweispflichten.

5.4. Dokumentation und Nachweise

Der Auftragnehmer hat die Einhaltung der vereinbarten Sicherheitsanforderungen nachvollziehbar zu dokumentieren und dem skbs auf Anforderung geeignete Nachweise vorzulegen. Hierzu gehören insbesondere:

- Beschreibungen der getroffenen technischen und organisatorischen Maßnahmen,
- Nachweise über Verpflichtung, Schulung und Sensibilisierung der eingesetzten Mitarbeitenden,
- aktuelle Sicherheitskonzepte, Verfahrens- und Betriebsdokumentationen,
- Prüfberichte, Zertifikate, Auditnachweise oder vergleichbare Belege, soweit vorhanden,
- Nachweise zur Behandlung von Schwachstellen, Sicherheitsvorfällen und Abweichungen.

6. Sicherheitsanforderungen an Lieferanten

Die nachfolgenden Anforderungen gelten für Lieferanten, Dienstleister und Dritte des skbs in dem Umfang, der für die jeweilige Leistung, Kritikalität und Risikolage erforderlich ist. Sie sind risikoorientiert anzuwenden, dürfen jedoch bei kritischen oder hochschutzbedürftigen Leistungen nicht unterschritten werden.

6.1. Organisatorische Anforderungen

6.1.1. Sicherheitsorganisation und Auskunftspflichten

Der Auftragnehmer ist verpflichtet, dem skbs auf Anfrage angemessene Informationen über seine Sicherheitsorganisation, Sicherheitsprozesse und Sicherheitsmaßnahmen zur Verfügung zu stellen, soweit dies zur Bewertung der Lieferantenbeziehung erforderlich ist.

Dies umfasst insbesondere, soweit vorhanden:

- Zertifizierungen oder Testate,
- Nachweise zur Wirksamkeit des Informationssicherheitsmanagements,
- einschlägige Richtlinien, Regelungen und Verfahrensbeschreibungen,
- Benennung verantwortlicher Ansprechpersonen für Informationssicherheit, Datenschutz und Incident Management.

Ziel ist die Feststellung, ob die Sicherheitsorganisation des Auftragnehmers dem Schutzbedarf und der Kritikalität der beauftragten Leistung angemessen entspricht.

6.1.2. Dokumentation

Der Auftragnehmer hat alle für die sichere Leistungserbringung relevanten Abläufe, Systeme und Sicherheitsmechanismen angemessen zu dokumentieren. Die Dokumentation muss – soweit einschlägig – mindestens enthalten:

- die eingesetzte Hardware,
- die eingesetzte Software einschließlich Versionen, Betriebssysteme und Patchstand,
- eine Übersicht der Systemarchitektur und der relevanten Kommunikationsbeziehungen,
- Benutzerkonten, Rollen und Berechtigungskonzepte,
- eingesetzte sicherheitsrelevante Schutzmechanismen,
- Betriebs-, Wartungs- und Wiederanlaufverfahren.

Änderungen an der Dienstleistung oder an sicherheitsrelevanten Komponenten sind zeitnah in die Dokumentation zu übernehmen.

6.1.3. Asset-Management

Der Auftragnehmer identifiziert und dokumentiert sämtliche Assets, die im Zusammenhang mit der Leistungserbringung für das skbs eingesetzt werden oder mit Systemen des skbs verbunden sind. Verantwortlichkeiten für Betrieb, Schutz, Wartung und Außerbetriebnahme dieser Assets sind eindeutig festzulegen.

6.1.4. Personalbezogene Sicherheitsanforderungen

Der Auftragnehmer stellt sicher, dass alle eingesetzten Personen nur im erforderlichen Umfang Zugriff erhalten und den für ihre Tätigkeit maßgeblichen Sicherheitsanforderungen unterliegen. Unterauftragnehmer und deren Personal sind dem skbs auf Verlangen transparent offenzulegen, sofern sie Zugang zu schutzbedürftigen Informationen, Systemen oder Einrichtungen erhalten.

6.1.5. Physische und umgebungsbezogene Sicherheit

Räumlichkeiten, in denen Informationen oder Systeme des skbs verarbeitet, betrieben, gewartet oder administriert werden, sind durch angemessene physische und organisatorische Maßnahmen gegen unbefugten Zutritt, Beschädigung, Diebstahl und Manipulation zu schützen. Dies gilt auch für Bereiche wie Lager, Anlieferungszone, Supportstandorte und Administrationsarbeitsplätze.

6.1.6. Sichere Zugangs- und Anmeldeverfahren

Zugriffe auf Systeme, Anwendungen und Netze des skbs dürfen ausschließlich über autorisierte, dokumentierte und angemessen abgesicherte Verfahren erfolgen. Authentifizierungsverfahren müssen dem Schutzbedarf und Risiko angemessen sein. Wo technisch und organisatorisch geboten, ist eine starke Authentisierung, insbesondere Mehr-Faktor-Authentisierung, einzusetzen.

6.1.7. Audits, Prüf- und Kontrollrechte

Der Auftragnehmer gewährt dem skbs oder von diesem beauftragten Dritten nach angemessener Vorankündigung das Recht, die Einhaltung der vereinbarten Sicherheitsanforderungen risikoorientiert zu überprüfen, soweit dem keine zwingenden gesetzlichen, vertraglichen oder berechtigten Geheimhaltungsinteressen entgegenstehen. Der Auftragnehmer ist verpflichtet, festgestellte Abweichungen unverzüglich offenzulegen, zu bewerten und innerhalb angemessener Fristen zu beseitigen. Das skbs kann geeignete Nachweise über die Umsetzung von Korrekturmaßnahmen verlangen.

6.1.8. Meldung sicherheitsrelevanter Vorfälle

Sicherheitsvorfälle, Schwachstellen, Kompromittierungen, Verdachtsfälle oder sonstige Ereignisse, die Auswirkungen auf Informationen, Systeme, Prozesse, Verfügbarkeiten oder die Patientensicherheit des skbs haben oder haben können, sind dem skbs unverzüglich zu melden. Die erste Meldung hat ohne schuldhaftes Zögern, spätestens jedoch innerhalb von 24 Stunden nach Bekanntwerden zu erfolgen.

Der Auftragnehmer hat unverzüglich geeignete Maßnahmen zur Eingrenzung, Analyse, Behebung und Wiederherstellung einzuleiten, das skbs fortlaufend über den Sachstand zu informieren und nach Abschluss einen nachvollziehbaren Bericht zu Ursachen, Auswirkungen, getroffenen Maßnahmen und abgeleiteten Verbesserungen vorzulegen.

6.1.9. Aufrechterhaltung der Informationssicherheit und Leistungsfähigkeit

Der Auftragnehmer hat sicherzustellen, dass die beauftragte Leistung auch in Störungs-, Notfall-, Krisen- und Katastrophensituationen mit angemessenem Sicherheitsniveau erbracht oder geordnet wiederhergestellt werden kann, soweit dies aufgrund der Kritikalität der Leistung erforderlich ist. Hierfür sind angemessene Vorsorge-, Notfall- und Wiederanlaufmaßnahmen zu dokumentieren, regelmäßig zu überprüfen und – soweit erforderlich – zu testen.

6.1.10. Beendigung der Leistungserbringung und Exit-Regelungen

Bei Beendigung der Vertrags- oder Leistungsbeziehung hat der Auftragnehmer sicherzustellen, dass Zugänge entzogen, bereitgestellte Konten deaktiviert, überlassene Informationen und Datenträger ordnungsgemäß zurückgegeben oder datenschutz- und sicherheitskonform gelöscht sowie Übergaben an das skbs oder einen Nachfolger geordnet durchgeführt werden.

6.2. Technische Anforderungen

6.2.1. Vulnerability Management

Der Auftragnehmer verpflichtet sich, alle im Zusammenhang mit der Leistungserbringung eingesetzten Produkte, Systeme und Dienste regelmäßig und anlassbezogen auf Schwachstellen zu prüfen. Identifizierte Schwachstellen sind hinsichtlich Kritikalität, Ausnutzbarkeit und möglicher Auswirkungen auf Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität sowie Patientensicherheit zu bewerten.

Sicherheitsrelevante Schwachstellen mit möglicher Auswirkung auf das skbs sind unverzüglich zu melden. Kritische Schwachstellen sind priorisiert und innerhalb angemessener Fristen zu behandeln.

6.2.2. Patch- und Update-Management

Sicherheitsupdates und Patches sind risikoorientiert, zeitnah und kontrolliert bereitzustellen bzw. einzuspielen. Für Schwachstellen mit hohem oder kritischem Risiko sind beschleunigte Umsetzungsfristen vorzusehen.

Sofern das skbs betroffen ist, sind Informationen über relevante Sicherheitsupdates, bekannte Einschränkungen, Risiken, notwendige Maßnahmen und – soweit erforderlich – Migrations- oder Kompensationsmaßnahmen bereitzustellen.

6.2.3. Schutz vor Schadsoftware

Der Auftragnehmer hat sicherzustellen, dass alle im Zusammenhang mit der Leistungserbringung eingesetzten Systeme und Endpunkte durch angemessene Maßnahmen gegen Schadsoftware, schädlichen Code und vergleichbare Bedrohungen geschützt werden. Schutzmaßnahmen sind aktuell zu halten, zu überwachen und an die Gefährdungslage anzupassen.

6.2.4. Sichere Konfiguration und Systemhärtung

Alle vom Auftragnehmer bereitgestellten, betriebenen oder administrierten Systeme sind nach anerkannten Sicherheitsgrundsätzen sicher zu konfigurieren und zu härten.

Hierzu gehören insbesondere:

- Deaktivierung nicht benötigter Funktionen, Dienste, Schnittstellen und Netzzugänge,
- Änderung unsicherer Standardkonfigurationen und Standardkennwörter,
- Betrieb nach dem Prinzip der minimalen Rechte und des Need-to-know,
- Schutz administrativer Konten und privilegierter Zugriffe,
- regelmäßige Überprüfung sicherheitsrelevanter Konfigurationen.

6.2.5. Fernzugänge durch Dritte

Fernzugriffe auf Systeme, Anwendungen oder Netze des skbs sind nur zulässig, wenn sie fachlich erforderlich, freigegeben, dokumentiert und technisch angemessen abgesichert sind.

Dabei gelten mindestens folgende Anforderungen:

- personengebundene, eindeutig zuordenbare Benutzerkonten,
- starke Authentisierung,
- Protokollierung und Nachvollziehbarkeit der Aktivitäten,
- zeitliche, funktionale und organisatorische Begrenzung des Zugriffs auf das erforderliche Maß,
- unverzügliche Deaktivierung nicht mehr benötigter Zugänge,
- Nutzung ausschließlich freigegebener Fernzugriffsverfahren.

6.2.6. Anforderungen an Entwicklungs- und Änderungsprozesse

Soweit der Auftragnehmer Software entwickelt, anpasst oder betreibt, sind Sicherheitsanforderungen bereits in Planung, Entwicklung, Test, Einführung und Änderung umzusetzen. Es gelten die Prinzipien von Security by Design und Security by Default.

Hierbei sind anerkannte Standards und bewährte Verfahren, insbesondere im Bereich sicherer Softwareentwicklung und Anwendungssicherheit, angemessen zu berücksichtigen. Sicherheitsrelevante Änderungen sind kontrolliert zu planen, zu testen, freizugeben und nachvollziehbar zu dokumentieren.

6.2.7. Kryptographische Sicherungsmaßnahmen

Für die Speicherung, Übertragung und Verarbeitung schutzbedürftiger Informationen sind geeignete kryptographische Verfahren nach aktuellem Stand der Technik einzusetzen. Dies gilt insbesondere bei Datenübertragungen über unsichere oder nicht vollständig kontrollierte Netze sowie bei administrativen Fernzugriffen.

Kryptographische Verfahren, Schlüsselmanagement und Zertifikatsnutzung sind regelmäßig auf Aktualität, Eignung und Sicherheit zu überprüfen.

6.2.8. Protokollierung und Nachvollziehbarkeit

Sicherheitsrelevante Zugriffe, administrative Tätigkeiten, Konfigurationsänderungen, Fernwartungsaktivitäten und sonstige kritische Ereignisse sind in angemessenem Umfang zu protokollieren. Protokolle sind gegen unbefugte Veränderung zu schützen und im Bedarfsfall für Auswertungen, Vorfalluntersuchungen oder Nachweise bereitzustellen.

6.2.9. Datensicherung und Wiederherstellbarkeit

Soweit für die Leistungserbringung erforderlich, sind geeignete Datensicherungs- und Wiederherstellungsverfahren einzurichten. Der Auftragnehmer hat sicherzustellen, dass für sicherheits- oder betriebsrelevante Daten eine angemessene Wiederherstellbarkeit besteht und Wiederanlaufverfahren regelmäßig überprüft werden.

7. Überwachung und kontinuierliche Verbesserung

Das skbs überprüft die Wirksamkeit dieser Leitlinie sowie deren Anwendung in Lieferanten- und Dienstleisterbeziehungen regelmäßig und anlassbezogen. Dabei werden insbesondere Änderungen der Bedrohungslage, technologische Entwicklungen, regulatorische Anforderungen, Ergebnisse aus Audits, Sicherheitsvorfällen sowie Erkenntnisse aus der operativen Zusammenarbeit berücksichtigt.

Festgestellte Schwachstellen, Abweichungen oder Verbesserungsbedarfe sind risikoorientiert zu bewerten und in geeignete Maßnahmen zu überführen. Ziel ist die kontinuierliche Weiterentwicklung des Sicherheitsniveaus in der Liefer- und Leistungskette sowie die nachhaltige Absicherung der medizinischen Versorgung, der Patientensicherheit und der kritischen Betriebsprozesse des skbs.

8. Inkrafttreten

Diese Leitlinie tritt mit Freigabe durch die zuständige Leitung in Kraft und ist verbindlich anzuwenden. Sie ist regelmäßig, mindestens jedoch anlassbezogen bei wesentlichen Änderungen der Risikolage, regulatorischer Anforderungen, technischer Rahmenbedingungen oder der Versorgungsstruktur zu überprüfen und bei Bedarf fortzuschreiben.

Autor	Stabsstelle Informationssicherheit
Geltungsbereich	Städtisches Klinikum Braunschweig sowie dessen Tochtergesellschaften
Freigegeben ab	30.03.2026
Freigegeben durch	Jan-Olaf Klok
Mitgeltend	keine