Informationssicherheitsleitlinie

für Lieferanten

1. Geltungsbereich

Dieses Dokument gilt für alle Lieferanten der Sozialstiftung Bamberg, des Klinikums Bamberg und dessen Organisationseinheiten, der MedLog und der Service Gesellschaft der Sozialstiftung Bamberg.

2. Ziel und Zweck

Der Zweck dieses Dokuments ist es, Regeln für Lieferanten zu definieren, wenn es sich bei der Beschaffung um Artikel handelt, bei denen die Informationssicherheit und der Datenschutz Berücksichtigung finden müssen. Das Dokument wird als bindende Vorgabe für Lieferanten und Dienstleister gesehen und ist als Solches Bestandteil der Vertragsunterlagen.

3. Verantwortliche Personen

Anwender dieses Dokumentes sind alle Abteilungen, die in die Beschaffung bzw. den Einkauf von datenschutzrechtlich oder informationssicherheitstechnisch relevanten Produkten oder Dienstleistung involviert sind, insbesondere Einkauf, Bau und Technik und die Abteilung technisches Infrastrukturmanagement (TIM) und die jeweiligen Lieferanten. In Verantwortung stehen alle Abteilungen und deren Mitarbeiter, die Lieferanten-beziehungen pflegen, alle Mitarbeiter der Informationssicherheit und alle Lieferanten der Sozialstiftung Bamberg.

4. Integrierte Verfahren / Mitgeltende Dokumente

- ISO/IEC 27001:2022
- DIN/EN/IEC 80001-1(in der jeweils aktuellen Fassung)
- Informationssicherheitsleitlinie der Sozialstiftung Bamberg
- BSI TR-02102-4 (in der jeweils aktuellen Fassung)
- VA Einkauf

Inhaltsverzeichnis

1 Grundsätze

Das Klinikum Bamberg hat ein Managementsystem zum Datenschutz und zur Informationssicherheit implementiert und umgesetzt. Das Management der Informationssicherheit erfolgt auf der Basis des internationalen Standards ISO/IEC 27001:2022. Im Zusammenhang mit der Beschaffung von datenschutzrechtlich bzw. informationssicherheitstechnisch relevanten Produkten und Dienstleistungen müssen die Prozesse und Vorgaben des Datenschutz- bzw. Informationssicherheitsmanagementsystems (ISMS) eingehalten werden.

Durch Outsourcing bzw. die Beschaffung von Produkten oder Dienstleistungen darf sich das Niveau des Datenschutzes und der Informationssicherheit im Geltungsbereich dieses Dokuments nicht verschlechtern.

Die vom Lieferanten bzw. Dienstleister getroffenen technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes und der Informationssicherheit müssen mindestens das Niveau der technischen und organisatorischen Maßnahmen der Sozialstiftung Bamberg bzw. der Tochterunternehmen erreichen.

2 Umsetzung

Die Sozialstiftung Bamberg 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 ISO/IEC 27001 oder BSI-Grundschutz als normative Grundlagen dienen. Entsprechende Managementsysteme sind für Lieferanten für Produkte und Dienstleistungen jedoch nicht verbindlich, sofern sie nicht im Rahmen von Ausschreibungen oder Verträgen explizit gefordert sind.

Sofern Lieferanten die Umsetzung eines Managementsystems im obigen Sinne für sich reklamieren, so muss der Geltungsbereich des jeweiligen Managementsystems die gelieferte Dienstleistung bzw. das Produkt vollständig einschließen. Falls von Lieferanten bzw. Dienstleistern 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 Informationssicherheitsleitlinie für Lieferanten ab Kapitel 5. Dabei müssen jedoch nur die Anforderungen erfüllt werden, die für die jeweilige Dienstleistung bzw. das Produkt auch relevant sind. (Siehe dazu auch Kapitel 5 „Wegweiser“.) Anforderungen in Ausschreibungen bzw. Verträgen gelten unabhängig von den Anforderungen dieser Informationssicherheitsleitlinie für Lieferanten.

Die Sozialstiftung Bamberg behält sich vor, Auftragnehmer, insbesondere diejenigen, die für den Betrieb von kritischen Prozessen und Systemen relevant sind, selbst oder durch dazu beauftragte Experten in Abstimmung mit dem jeweiligen Auftragnehmer einem Audit zu unterziehen. Prüfgrundlage für dieses Audit bildet die vorliegende Leitlinie für die

Informationssicherheit für Lieferanten und weitere vertragliche Vereinbarungen mit dem Auftragnehmer. Das Audit erfolgt in Abstimmung mit dem Auftragnehmer zu den üblichen Geschäftszeiten. Der Auftragnehmer verpflichtet sich zur Mitarbeit an dem Audit und den Auditoren Zutritt zu Geschäftsräumen und Einblick in Dokumente zu gewähren, sofern diese für die Leistungserbringung relevant sind. Kosten, die auf der Seite des Auftragnehmers durch das Audit entstehen, werden von diesem getragen.

3 Wegweiser

Falls im Rahmen einer Ausschreibung bzw. einer Beschaffung keine anderslautenden oder ergänzenden Festlegungen getroffen worden sind und vonseiten des Dienstleisters bzw. Lieferanten kein eigenes Informationssicherheitsmanagementsystem auf der Basis eines anerkannten Standards (z.B. ISO/IEC 27001 oder BSI-Grundschutz) umgesetzt worden ist, dessen Geltungsbereich die gelieferten Dienstleistungen bzw. Produkte miteinschließt, so müssen die Anforderungen in den Kapiteln 6 und ggf. 7 jeweils nach Maßgabe dieses Kapitels im Sinne eines „Wegweisers“ umgesetzt werden.

Abhängig von der Art der Produkte bzw. der Dienstleistungen können ein oder mehrere der folgenden Kapitel relevant sein.

Die Anforderungen der Kapitel 6 und 7 stellen Mindestanforderungen dar.

3.1 Kritische Systeme

Für Lieferanten,

- die Produkte liefern, die zu den kritischen Systemen des Klinikums Bamberg im Sinne des BSI-Gesetzes zählen oder
- die Komponenten liefern, die für den Betrieb der kritischen Systeme von zentraler Bedeutung sind, bzw. Dienstleister,
- die eine zentrale Dienstleistung für den Betrieb der kritischen Systeme erbringen,

sind alle Anforderungen gemäß Kapitel 6 relevant.

Ferner ist Kapitel 7 relevant, sofern ein geliefertes Produkt zu den kritischen Systemen im obigen Sinne zählt und gleichzeitig ein Medizinprodukt ist oder in einem Netzwerk mit Medizinprodukten betrieben wird.

Die Einkaufsabteilung oder der Informationssicherheitsbeauftragte der Sozialstiftung Bamberg erteilen Auskunft darüber, ob die betreffende Dienstleistung bzw. das Produkt den kritischen Systemen zuzurechnen ist.

3.2 Lieferanten kritischer Produkte

Lieferanten von Produkten, die für kritische Dienstleistungen der Sozialstiftung Bamberg insbesondere die medizinische Versorgung unverzichtbar sind, müssen folgende Anforderungen umsetzen:

6.13 Aufrechterhaltung der Informationssicherheit

6.16 Personelle Sicherheit

Zu den Lieferanten kritischer Produkte gehören z.B. Lieferanten von Lebensmitteln, Medikamenten und medizinischem Verbrauchsmaterial. Ob ein Produkt als kritisch in diesem Sinne einzustufen ist, kann bei der beschaffenden Fachabteilung der Sozialstiftung Bamberg erfragt werden.

3.3 Zutritt zu Sicherheitsbereichen der Sozialstiftung Bamberg

Falls der Dienstleister bzw. Lieferant im Rahmen seines Auftrags Zutritt zu Sicherheitsbereichen der Sozialstiftung Bamberg erhält, sind folgende Kapitel relevant:

6.5 Zulässiger Gebrauch von Werten (A.5.10, A.7.8-9, A.7.13)

6.6 Rückgabe von Werten (A.5.11)

6.7 Informationsklassifizierung (A.5.12, A.5.13)

6.12 Handhabung von Informationssicherheitsvorfällen (A.5.24-28, A.6.8)

6.13 Aufrechterhaltung der Informationssicherheit (A.5.29-30, A.7.11)

6.14 Compliance (Kapitel 9.2, A.5.31-35)

6.15 Dokumentierte Bedienabläufe (A.5.37)

6.16 Personelle Sicherheit (A.6.1-3, A.6.5-6)

6.19.1 Geschäftsbereich der Sozialstiftung Bamberg

3.4 IT-Produkte und IT-Services

Falls ein Lieferant IT-Produkte liefert oder IT-Services für den Auftraggeber bereitstellt, sind folgende Kapitel relevant:

6.1 Informationssicherheitsleitlinie (A.5.1, Kapitel 5.2)

6.2 Verantwortlichkeiten für die Informationssicherheit und Ansprechpartner (A. 5.2, Kapitel 5.3)

6.3 Erkenntnisse über Bedrohungen (A.5.7)

6.5 Zulässiger Gebrauch von Werten (A.5.10, A.7.8-9, A.7.13)

6.6 Rückgabe von Werten (A.5.11)

6.8 Informationsübertragung (A.5.14)

6.9 Zugangsberechtigungen (A.5.15, A.5.16, A.5.17, A.5.18, A.8.5)

6.10 Lieferantenbeziehungen (A.5.19, A.5.20, A.5.21, A.5.22)

6.11 Cloud-Dienste (A.5.23)

6.12 Handhabung von Informationssicherheitsvorfällen (A.5.24-28, A.6.8)

6.13 Aufrechterhaltung der Informationssicherheit (A.5.29-30, A.7.11)

6.14 Compliance (Kapitel 9.2, A.5.31-35)

6.15 Dokumentierte Bedienabläufe (A.5.37)

6.16 Personelle Sicherheit (A.6.1-3, A.6.5-6)

6.17 Mobilgeräte und Telearbeit (A.6.7, A.7.10, A.8.24)

6.18 Handhabung von Speichermedien (A.7.10)

6.19.2 Geschäftsbereiche des Auftragnehmers

6.20 Zugangssteuerung für Quellcode von Programmen (A.8.4)

6.21 Kryptographische Maßnahmen (A.24)

6.23 Software- und Systementwicklung und Tests (A.8.31, A.8.33)

6.24 Maßnahmen gegen Schadsoftware (A.8.7)

6.25 Sicherung von Informationen (A.8.13)

6.26 Ereignisprotokollierung und Schutz der Protokollinformationen (A.8.15)

6.27 Installation von Software (A.8.19)

6.28 Handhabung von technischen Schwachstellen (A.8.8)

6.29 Maßnahmen für Audits von Informationssystemen (A.8.34)

6.30 Netzwerksicherheitsmanagement (A.8.20, A.8.22)

6.31 Sicherung von Anwendungsdiensten in Netzwerken (A.8.21, A.8.23)

3.5 Wartung von Systemen allgemein

Falls der Dienstleister mit der Wartung von Systemen (allgemein) der Sozialstiftung Bamberg beauftragt ist, sind folgende Kapitel relevant:

6.5 Zulässiger Gebrauch von Werten (A.5.10, A.7.8-9, A.7.13)

6.6 Rückgabe von Werten (A.5.11)

6.10 Lieferantenbeziehungen (A.5.19, A.5.20, A.5.21, A.5.22)

6.12 Handhabung von Informationssicherheitsvorfällen (A.5.24-28, A.6.8)

6.13 Aufrechterhaltung der Informationssicherheit (A.5.29-30, A.7.11)

6.14 Compliance (Kapitel 9.2, A.5.31-35)

6.15 Dokumentierte Bedienabläufe (A.5.37)

6.16 Personelle Sicherheit (A.6.1-3, A.6.5-6)

6.19 Physische und umgebungsbezogene Sicherheit (A.7.1-A.7.3, A.7.5-7, A.7.12)

6.22 Serviceberichte (A.7.13)

6.25 Sicherung von Informationen (A.8.13)

3.6 Wartung von IT-Systemen oder Medizingeräten oder Remote-Zugriff auf IT-Systeme, Medizingeräte oder Netzwerke der Sozialstiftung Bamberg

Falls der Dienstleister mit der Wartung von IT-Systemen oder Medizingeräten der Sozialstiftung Bamberg beauftragt ist oder auf IT-Systeme, Medizingeräte oder Netzwerke der Sozialstiftung Bamberg remote oder vor Ort zugreift oder eigene IT-Systeme bzw. Komponenten an IT-Systeme, Medizingeräte oder Netzwerke der Sozialstiftung Bamberg anschließt, müssen die Anforderungen in Kapitel 5.4 umgesetzt werden. Ferner sind folgende Kapitel relevant:

6.1 Informationssicherheitsleitlinie (A.5.1, Kapitel 5.2)
6.2 Verantwortlichkeiten für die Informationssicherheit und Ansprechpartner (A. 5.2, Kapitel 5.3)
6.3 Erkenntnisse über Bedrohungen (A.5.7)
6.7 Informationsklassifizierung (A.5.12, A.5.13)
6.8 Informationsübertragung (A.5.14)
6.9 Zugangsberechtigungen (A.5.15, A.5.16, A.5.17, A.5.18, A.8.5)
6.11 Cloud-Dienste (A.5.23)
6.16 Personelle Sicherheit (A.6.1-3, A.6.5-6)
6.17 Mobilgeräte und Telearbeit (A.6.7, A.7.10, A.8.24)
6.18 Handhabung von Speichermedien (A.7.10)
6.20 Zugangssteuerung für Quellcode von Programmen (A.8.4)
6.21 Kryptographische Maßnahmen (A.24)
6.23 Software- und Systementwicklung und Tests (A.8.31, A.8.33)
6.24 Maßnahmen gegen Schadsoftware (A.8.7)
6.26 Ereignisprotokollierung und Schutz der Protokollinformationen (A.8.15)
6.27 Installation von Software (A.8.19)
6.28 Handhabung von technischen Schwachstellen (A.8.8)
6.29 Maßnahmen für Audits von Informationssystemen (A.8.34)
6.30 Netzwerksicherheitsmanagement (A.8.20, A.8.22)
6.31 Sicherung von Anwendungsdiensten in Netzwerken (A.8.21, A.8.23)

3.7 Nutzung von IT-Systemen der Sozialstiftung Bamberg

Falls der Dienstleister im Rahmen seines Auftrags IT-Systeme der Sozialstiftung Bamberg nutzt, sind folgende Kapitel relevant:

6.5 Zulässiger Gebrauch von Werten (A.5.10, A.7.8-9, A.7.13)

6.6 Rückgabe von Werten (A.5.11)
6.7 Informationsklassifizierung (A.5.12, A.5.13)
6.9 Zugangsberechtigungen (A.5.15, A.5.16, A.5.17, A.5.18, A.8.5)
6.10 Lieferantenbeziehungen (A.5.19, A.5.20, A.5.21, A.5.22)
6.11 Cloud-Dienste (A.5.23)
6.12 Handhabung von Informationssicherheitsvorfällen (A.5.24-28, A.6.8)
6.13 Aufrechterhaltung der Informationssicherheit (A.5.29-30, A.7.11)
6.14 Compliance (Kapitel 9.2, A.5.31-35)
6.15 Dokumentierte Bedienabläufe (A.5.37)
6.16 Personelle Sicherheit (A.6.1-3, A.6.5-6)
6.17 Mobilgeräte und Telearbeit (A.6.7, A.7.10, A.8.24)
6.18 Handhabung von Speichermedien (A.7.10)

3.8 Entwicklungsaufträge mit Verwendungen von IT

Falls der Dienstleister bzw. Lieferant mit der Entwicklung von Systemen beauftragt ist, die auch IT-Subsysteme, IT-Komponenten oder Software beinhalten oder verwenden, sind folgende Kapitel relevant:

6.3 Erkenntnisse über Bedrohungen (A.5.7)
6.4 Informationssicherheit im Projektmanagement (A.5.8)
6.5 Zulässiger Gebrauch von Werten (A.5.10, A.7.8-9, A.7.13)
6.6 Rückgabe von Werten (A.5.11)
6.7 Informationsklassifizierung (A.5.12, A.5.13)
6.8 Informationsübertragung (A.5.14)
6.9 Zugangsberechtigungen (A.5.15, A.5.16, A.5.17, A.5.18, A.8.5)
6.10 Lieferantenbeziehungen (A.5.19, A.5.20, A.5.21, A.5.22)
6.11 Cloud-Dienste (A.5.23)
6.12 Handhabung von Informationssicherheitsvorfällen (A.5.24-28, A.6.8)
6.13 Aufrechterhaltung der Informationssicherheit (A.5.29-30, A.7.11)
6.14 Compliance (Kapitel 9.2, A.5.31-35)
6.15 Dokumentierte Bedienabläufe (A.5.37)
6.16 Personelle Sicherheit (A.6.1-3, A.6.5-6)
6.17 Mobilgeräte und Telearbeit (A.6.7, A.7.10, A.8.24)
6.18 Handhabung von Speichermedien (A.7.10)
6.20 Zugangssteuerung für Quellcode von Programmen (A.8.4)

6.21 Kryptographische Maßnahmen (A.24)

6.23 Software- und Systementwicklung und Tests (A.8.31, A.8.33)

6.24 Maßnahmen gegen Schadsoftware (A.8.7)

6.25 Sicherung von Informationen (A.8.13)

6.26 Ereignisprotokollierung und Schutz der Protokollinformationen (A.8.15)

6.28 Handhabung von technischen Schwachstellen (A.8.8)

6.29 Maßnahmen für Audits von Informationssystemen (A.8.34)

6.30 Netzwerksicherheitsmanagement (A.8.20, A.8.22)

6.31 Sicherung von Anwendungsdiensten in Netzwerken (A.8.21, A.8.23)

Falls sich der Auftrag auf Medizinprodukte bezieht oder mit Medizinprodukten im Zusammenhang steht, ist darüber hinaus Kapitel 7 relevant.

3.9 Projektmanagement

Für Dienstleister, die mit der Umsetzung oder Begleitung von Projekten beauftragt sind, oder eigene Projekte umsetzen, um die beauftragten Dienstleistungen oder Produkte zu liefern, sind folgende Kapitel relevant:

6.2 Verantwortlichkeiten für die Informationssicherheit und Ansprechpartner (A. 5.2, Kapitel 5.3)

6.4 Informationssicherheit im Projektmanagement (A.5.8)

6.7 Informationsklassifizierung (A.5.12, A.5.13)

6.8 Informationsübertragung (A.5.14)

6.9 Zugangsberechtigungen (A.5.15, A.5.16, A.5.17, A.5.18, A.8.5)

6.10 Lieferantenbeziehungen (A.5.19, A.5.20, A.5.21, A.5.22)

6.11 Cloud-Dienste (A.5.23)

6.12 Handhabung von Informationssicherheitsvorfällen (A.5.24-28, A.6.8)

6.13 Aufrechterhaltung der Informationssicherheit (A.5.29-30, A.7.11)

6.14 Compliance (Kapitel 9.2, A.5.31-35)

6.16 Personelle Sicherheit (A.6.1-3, A.6.5-6)

6.19 Physische und umgebungsbezogene Sicherheit (A.7.1-A.7.3, A.7.5-7, A.7.12)

6.24 Maßnahmen gegen Schadsoftware (A.8.7)

6.25 Sicherung von Informationen (A.8.13)

3.10 Medizinprodukte

Falls der Auftragnehmer Medizinprodukte liefert, ist Kapitel 7 relevant.

Falls das Medizinprodukt an ein Netzwerk angeschlossen werden kann, sind folgende Kapitel relevant:

6.21 Kryptographische Maßnahmen (A.24)

6.27 Installation von Software (A.8.19)

6.28 Handhabung von technischen Schwachstellen (A.8.8)

6.30 Netzwerksicherheitsmanagement (A.8.20, A.8.22)

6.31 Sicherung von Anwendungsdiensten in Netzwerken (A.8.21, A.8.23)

4 Anforderungen an Dienstleister und Lieferanten

4.1 Informationssicherheitsleitlinie

Der Dienstleister bzw. Lieferant muss eine Informationssicherheitsleitlinie erstellt haben, die mit der Informationssicherheitsleitlinie des Klinikums Bamberg und der vorliegenden Informationssicherheitsleitlinie für Lieferanten im Einklang steht.

4.2 Verantwortlichkeiten für die Informationssicherheit und Ansprechpartner

Der Dienstleister bzw. Lieferant muss Rollen und Verantwortlichkeiten für die Informationssicherheit und gegebenenfalls den Datenschutz festlegen. Die personellen Ressourcen müssen ausreichend sein, um das geforderte Niveau des Datenschutzes und der Informationssicherheit realisieren zu können.

Ein konkreter Ansprechpartner für das Thema Informationssicherheit muss dem Informationssicherheitsbeauftragten der Sozialstiftung Bamberg per E-Mail mitgeteilt werden: isb@sozialstiftung-bamberg.de werden.

4.3 Erkenntnisse über Bedrohungen

Der Dienstleister bzw. Lieferant muss regelmäßig Erkenntnisse über aktuelle Bedrohungen die Informationssicherheit betreffend beziehen und bewerten. Dazu können Newsletter öffentlicher Stellen (z.B. BSI: https://wid.cert-bund.de/portal/wid/fragenundantworten, https://wid.lsi.bayern.de) oder privater Betreiber (z.B. https://www.heise.de, https://www.cvedetails.com) bezogen werden.

Abhängig von der Bewertung müssen bei Bedarf vom Dienstleister bzw. Lieferanten Sicherheitsmaßnahmen angepasst oder neue Sicherheitsmaßnahmen ergriffen werden, um diese Bedrohungen zu adressieren.

4.4 Informationssicherheit im Projektmanagement

Falls im Zusammenhang mit der gelieferten Dienstleistung bzw. dem Produkt auf der Seite des Dienstleisters Projektmanagement erforderlich ist, so muss im Projektmanagement die

Informationssicherheit berücksichtigt werden. Insbesondere muss sichergestellt sein, dass im Rahmen der Projektinitialisierung und bei der Projektabnahme das erforderliche Niveau der Informationssicherheit und gegebenenfalls des Datenschutzes realisiert wird.

4.5 Zulässiger Gebrauch von Werten

Der Dienstleister muss sicherstellen, dass Regeln für den zulässigen Gebrauch von Informationen und anderen Vermögenswerten des Auftraggebers eingehalten werden. Geräte und Betriebsmittel der Sozialstiftung Bamberg dürfen ausschließlich im vertraglich vereinbarten Rahmen und ihrem bestimmungsgemäßen Zweck verwendet werden. Sie sind vor Beschädigung und Verlust zu schützen. Vorgaben zur Wartung von Geräten und Betriebsmitteln der Sozialstiftung Bamberg müssen in Abstimmung mit den Verantwortlichen Ansprechpartnern auf der Seite der Sozialstiftung Bamberg eingehalten werden.

Der Dienstleister kann ergänzend zu den Regeln des Auftraggebers eigene Regeln aufstellen. Dabei muss sichergestellt sein, dass die Regeln auf der Seite des Dienstleisters mindestens das Sicherheitsniveau des Auftraggebers erreichen.

4.6 Rückgabe von Werten

Schließmittel (Schlüssel, Zutrittskarten), Endgeräte und sonstiges Material, das Eigentum der Sozialstiftung Bamberg oder ihrer Tochterunternehmen ist, muss bei Beendigung des Auftragsverhältnisses vollständig und unverzüglich zurückgegeben werden. Sofern im Rahmen der Dienstleistung vertrauliche bzw. personenbezogene Daten des Auftraggebers verarbeitet werden, so muss sichergestellt werden, dass diese Daten bei Vertragsende gelöscht bzw. datenschutzgerecht vernichtet oder an den Auftraggeber zurückgegeben werden. Näheres kann im Hauptvertrag geregelt werden.

4.7 Informationsklassifizierung

Dem Dienstleister kann auf Nachfrage die Richtlinie zur Klassifizierung des Auftraggebers zur Verfügung gestellt werden. Der Dienstleister muss sicherstellen, dass die Regelung zur Beschriftung und zum Umgang mit klassifiziertem Material des Auftraggebers entsprechend dieser Richtlinie zur Klassifizierung umgesetzt wird. Der Dienstleister kann eine eigene Richtlinie zur Klassifizierung nutzen, sofern die darin spezifizierten Regelungen zur Beschriftung und zum Umgang mit klassifiziertem Material den Regelungen des Auftraggebers entsprechen.

4.8 Informationsübertragung

Von Seiten des Auftraggebers werden für die Dienstleistungserbringung ggf. formale Übertragungsrichtlinien, Verfahren und Maßnahmen vorgegeben, um die Übertragung von Informationen für alle Arten von Kommunikationseinrichtungen, die im Zusammenhang mit der Dienstleistungserbringung stehen, zu schützen. Der Auftragnehmer ist verpflichtet, diese Vorgaben einzuhalten.

Ansprechpartner für technische Fragen ist die IT-Abteilung der Sozialstiftung Bamberg.

4.9 Zugangsberechtigungen

Dienstleistern können für die Erfüllung ihrer Aufgaben Zugangsberechtigungen der Sozialstiftung Bamberg erteilt werden. Die Zugangsberechtigungen werden beschränkt auf die durch den Dienstleister vertraglich zu erbringenden Leistungen. Der Zugriff des Dienstleisters auf Systeme des Auftraggebers, darf ausschließlich über die vom Auftraggeber vorgegebenen Prozeduren und autorisierten Zugänge erfolgen.

Die Daten der Zugangsberechtigungen (Identität der Nutzer und Authentisierungsinformationen, z.B. Passworte) müssen vom Dienstleister bzw. Lieferanten angemessen geschützt und über ihren gesamten Lebenszyklus sicher verwaltet werden. Die Vorgaben zum Umgang mit Passworten der Sozialstiftung Bamberg sind einzuhalten.

Falls der Zugang über zwei Faktoren unter Verwendung eines Zugangstoken autorisiert wird, so muss der Dienstleister 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.

Eine Kompromittierung von Zugangsdaten oder der Verlust von Authentisierungsmitteln (z.B. Token) muss der Sozialstiftung Bamberg unverzüglich gemeldet werden.

Zugangsberechtigungen, die einem Mitarbeiter des Dienstleisters zugeteilt werden, dürfen nur von diesem Mitarbeiter verwendet werden. Beim Ausscheiden von Mitarbeitern des Auftragnehmers, die über einen Zugang auf Systeme des Auftraggebers verfügen, ist die Sozialstiftung
Bamberg zu informieren, damit die Zugangsberechtigungen angepasst werden können.

Der Auftragnehmer muss ferner eigene Regelungen für die Verwaltung von Zugangsberechtigungen für seine Systeme festlegen und umsetzen, sofern diese mittelbar oder unmittelbar für die Erbringung der Dienstleistung genutzt werden.

Der Auftragnehmer muss in regelmäßigen Abständen die Zugangsberechtigungen seiner Mitarbeiter prüfen. Die Überprüfung der Berechtigungen ist zu dokumentieren und dem Auftraggeber auf Nachfrage vorzulegen.

4.10 Lieferantenbeziehungen

Falls der Auftragnehmer für die Erbringung der Dienstleistung Unterauftragnehmer in Anspruch nimmt, so hat der Auftragnehmer sicherzustellen, dass durch die Unterbeauftragung das Sicherheitsniveau, das der Auftraggeber vom Auftragnehmer fordert, nicht reduziert wird. Dazu können vom Auftragnehmer Leitlinien verwendet werden, die der vorliegenden entsprechen sollen. Der Auftragnehmer hat sicherzustellen, dass die Dienstleistungserbringung von Lieferanten seinen Vorgaben entspricht. Im Falle von Auftragsverarbeitung gelten die entsprechenden vertraglichen Regelungen.

Der Auftragnehmer muss dem Auftraggeber eine aktuelle Liste aller Unterauftragnehmer übermitteln, die für die Leistungserbringung gegenüber der Sozialstiftung vom Auftragnehmer in Anspruch genommen werden.

4.11 Cloud-Dienste

Die Nutzung von Cloud-Diensten durch den Auftragnehmer zur Erbringung von Dienstleistungen für den Auftraggeber muss zuvor vertraglich zwischen Auftraggeber und Auftragnehmer geregelt worden sein. Der Auftragnehmer hat sicherzustellen, dass das Sicherheitsniveau der Sozialstiftung Bamberg durch die Nutzung von Cloud-Diensten nicht verringert wird. Ferner muss der Auftragnehmer geeignete Vorgaben für die Nutzung der Cloud-Dienste dokumentieren und deren Umsetzung sicherstellen. Diese Vorgaben müssen mit den Vorgaben der Sozialstiftung korrespondieren (siehe dazu Richtlinie Cloud-Dienste der Sozialstiftung Bamberg).

Ferner sind die einschlägigen gesetzlichen Vorgaben zum Einsatz von Cloud-Diensten im Gesundheitswesen nach § 393 SGB V zu beachten.

4.12 Handhabung von Informationssicherheitsvorfällen

Der Auftragnehmer hat sicherzustellen, dass Verantwortlichkeiten und Verfahren festgelegt werden, um eine schnelle, effektive und geordnete Reaktion auf Informationssicherheitsvorfälle zu ermöglichen. Sicherheitsvorfälle, die die beauftragte Dienstleistung betreffen oder Auswirkungen auf den Auftraggeber haben können, sind dem Auftraggeber unverzüglich mitzuteilen. Der Auftragnehmer ist verpflichtet, dem Auftraggeber Schwächen in der Informationssicherheit mitzuteilen, die sowohl ihn selbst als auch den Auftraggeber betreffen, um es dem Auftraggeber zu ermöglichen, geeignete Maßnahmen ergreifen zu können. Der Auftragnehmer unterstützt den Auftraggeber bei der Beurteilung von Sicherheitsvorfällen, die im Zusammenhang mit der beauftragten Dienstleistung stehen, indem er dem Auftraggeber alle relevanten Informationen im Zusammenhang mit dem jeweiligen Sicherheitsvorfall zur Verfügung stellt. Der Auftragnehmer legt Verfahren für die Ermittlung, Sammlung, Erfassung und Aufbewahrung von Informationen fest, die als Beweismaterial dienen können.

4.13 Aufrechterhaltung der Leistungen

Der Auftragnehmer sichert seine Dienstleistung bzw. die Liefermöglichkeit seiner Produkte gegen widrige Situationen (Krise oder Katastrophe) in angemessenem Umfang ab. Sofern seine Leistungen Versorgungseinrichtungen erfordern, müssen diese vor Stromausfällen und anderen Störungen in angemessenen Umfang geschützt werden.

Der Verfügbarkeitsbedarf der beauftragten Dienstleistung bzw. die Liefermöglichkeit seiner Produkte kann in Abstimmung mit dem Auftraggeber bestimmt werden. Der Auftragnehmer legt Prozesse, Verfahren und Maßnahmen fest, dokumentiert diese und setzt sie um, um den erforderlichen Grad an Verfügbarkeit auch in widrigen Situationen aufrechterhalten zu können (Notfallpläne). Die Wirksamkeit der Maßnahmen soll von Seiten des Auftragnehmers in regelmäßigen Abständen geprüft werden. Die Prüfungen sollen dokumentiert werden.

4.14 Compliance

Der Auftragnehmer muss angemessene Verfahren umsetzen, um die Einhaltung gesetzlicher, regulatorischer und vertraglicher Anforderung mit Bezug auf geistige Eigentumsrechte und der Verwendung von urheberrechtlich geschützten Softwareprodukten zu gewährleisten. 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.

Dem Dienstleister wird empfohlen, seine Vorgehensweise für die Handhabung der Informationssicherheit und deren Umsetzung in planmäßigen Abständen oder bei erheblichen Änderungen von unabhängigen Stellen überprüfen zu lassen (interne Auditierungen). Die Auditierungen und ihre Ergebnisse sind zu dokumentieren.

4.15 Dokumentierte Bedienabläufe

Der Auftragnehmer hat sicherzustellen, dass dokumentierte Bedienabläufe und Vorgaben der Sozialstiftung Bamberg im Rahmen seiner Tätigkeit berücksichtigt und umgesetzt werden. Falls aus zwingenden Gründen eine Abweichung von diesen Vorgaben für die Erbringung der Leistung erforderlich ist, muss dazu eine explizite und schriftliche Freigabe vonseiten der Sozialstiftung Bamberg erteilt werden.

Der Dienstleister muss innerhalb seiner Organisation sicherstellen, dass Bedienabläufe im Zusammenhang mit der Leistungserbringung in ausreichendem Maße dokumentiert sind.

4.16 Personelle Sicherheit

Der Auftragnehmer muss sicherstellen, dass für die Erbringung seiner Leistungen nur vertrauenswürdige Mitarbeiter eingesetzt werden. Dazu werden Sicherheitsüberprüfungen im Rahmen der gesetzlichen Vorgaben empfohlen.

Der Dienstleister muss seine Mitarbeiter auf die Einhaltung von relevanten Vorgaben hinweisen bzw. verpflichten.

Der Auftragnehmer muss sicherstellen, dass alle Mitarbeiter, die im Zusammenhang mit der beauftragten Dienstleistung bzw. dem gelieferten Produktes Zugriff auf Informationswerte des Auftraggebers 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. Alternativ können die Mitarbeiter von Dienstleistern an den Schulungen der Sozialstiftung Bamberg zur Informationssicherheit und zum Datenschutz teilnehmen.

Die Verantwortlichkeiten des Auftragnehmers und seiner Mitarbeiter bei Beendigung oder Änderung der Dienstleistung werden im Hauptvertrag geregelt.

4.17 Mobilgeräte und Telearbeit

Sofern im Zusammenhang mit der Dienstleistung bzw. den gelieferten Produkten von Seiten des Dienstleisters ein Zugriff auf Informationswerte oder Systeme des Auftraggebers erforderlich ist, so muss sichergestellt werden, dass dieser Zugriff ausschließlich innerhalb gesicherter Räume erfolgt. Ein Zugriff auf Informationswerte oder Systeme des Auftraggebers aus öffentlichen Bereichen heraus ist verboten. Die Einsichtnahme auf die Endgeräte durch unbefugte Dritte muss in jedem Fall ausgeschlossen werden. Diese Regelungen gelten analog für den Zugriff auf die Systeme des Auftragnehmers, falls auf

diesen Informationswerten bzw. personenbezogene Daten des Auftraggebers verarbeitet werden.

Für den Fall, dass Informationswerte bzw. personenbezogene Daten des Auftraggebers auf mobilen Speichermedien oder Festplatten in Laptops gespeichert werden, so müssen die Speichermedien bzw. Festplatten komplett verschlüsselt werden. Die eingesetzten Verschlüsselungsverfahren müssen dabei den aktuellen technischen Mindestanforderungen der Richtlinien des BSI (BSI TR-02102-1-4) entsprechen.

4.18 Handhabung von Speichermedien

Der Begriff „Speichermedien“ umfasst Festplatten, USB-Speicher, CDs, DVDs, Blue Rays und auch Papier.

Sofern im Zusammenhang mit der Dienstleistung Speichermedien in diesem Sinne gehandhabt werden, die vertrauliche Informationen bzw. personenbezogene Daten des Auftraggebers enthalten, muss der Auftragnehmer angemessene technische und organisatorische Maßnahmen treffen, die den Schutz dieser Informationen sicherstellen. Die Maßnahmen müssen den gesamten Lebenszyklus der Speichermedien vom Erwerb über die Verwendung, dem Transport bis zur Löschung bzw. Entsorgung abdecken.

Weitere Anforderungen dazu können im Hauptvertrag enthalten sein.

4.19 Physische und umgebungsbezogene Sicherheit

4.19.1 Geschäftsbereich der Sozialstiftung Bamberg

Zu den Geschäftsräumen und Außenflächen der Sozialstiftung Bamberg gehören auch Bereiche, die einem besonderen Schutzbedarf unterliegen. Für diese sind restriktive Regelungen zur Zutrittskontrolle erforderlich. Die Regelungen müssen auch von beauftragten Dienstleistern und ihren Mitarbeitern zwingend eingehalten werden. Zu diesen Sicherheitsbereichen zählen:

- Flure in Versorgungsbereichen
- Medizinische- und Behandlungsbereiche mit individueller Zutrittskontrolle
- Lager im Innenbereich
- Lager im Außenbereich
- Büros mit hohem Schutzbedarf
- Räume und Lager mit sehr hohem Schutzbedarf
- Betriebsräume und Infrastruktur

Diese Bereiche dürfen von Mitarbeitern der Auftragnehmer nur im Rahmen ihres Auftrags oder in Begleitung von Mitarbeitern der Sozialstiftung Bamberg betreten werden. Ohne Begleitung dürfen die Bereiche nur im Rahmen des Auftrages und nach expliziter Autorisierung betreten werden.

Die Mitarbeiter des Auftragnehmers müssen die Vorgaben zu Infrastrukturräumen der Sozialstiftung Bamberg beachten. Sofern im Rahmen des Auftrags an Verkabelung gearbeitet werden muss, sind die Vorgaben zur Kabelsicherheit der Sozialstiftung Bamberg zu berücksichtigen.

Im Rahmen des Autorisierungsprozesses durch den zuständigen Fachbereich der Sozialstiftung Bamberg erhält der Mitarbeiter des Dienstleisters einen Besucherausweis. Dieser muss in den Sicherheitszonen durchgängig gut sichtbar getragen werden, sofern nicht Aspekte der Arbeitssicherheit dies ausschließen. Der Besucherausweis muss bei Auftragsende bzw. Beendigung der Tätigkeit an die Fachabteilung zurückgegeben werden. Vom Dienstleister dürfen ausschließlich namentlich autorisierte und der Sozialstiftung Bamberg namentlich bekannte Personen die Sicherheitsbereiche betreten. Türen zu Sicherheitsbereichen sind grundsätzlich verschlossen und verriegelt zu halten. Diese Türen dürfen in der Regel nicht mechanisch offengehalten (verkeilt) werden. Ausnahmen davon sind nur vorübergehend aus zwingenden Gründen (z.B. für eine Lieferung) erlaubt. In dem Fall muss ein Posten abgestellt werden, der den Zutritt zu dem Sicherheitsbereich ohne Unterbrechung kontrolliert. Automatische Brandschutztüren dürfen unter keinen Umständen blockiert werden.

4.19.2 Geschäftsbereiche des Auftragnehmers

Der Dienstleister hat dafür Sorge zu tragen, dass der unbefugte Zutritt in Räume, Büros und Einrichtungen, in denen Informationen des Auftraggebers verarbeitet werden, ausgeschlossen ist. Dies gilt weiterhin auch für Anlieferungs- und Ladebereiche, über die unbefugte Personen die Räumlichkeiten betreten könnten. Der Auftragnehmer muss sicherstellen, dass der Zutritt in Räume, von denen aus Supporttätigkeiten für den Auftraggeber durchgeführt werden, kontrolliert wird. Die Ausübung von Supporttätigkeiten aus öffentlichen Bereichen heraus ist untersagt. Von Seiten des Dienstleisters sind Richtlinien zu erstellen, die aufgeräumte Arbeitsumgebungen sowie Bildschirmsperren bei Nichtbenutzung regeln.

Der Auftragnehmer muss in angemessenem Umfang Maßnahmen zum Schutz vor physischen und umweltbedingten Bedrohungen wie Naturkatastrophen und anderen absichtlichen oder unabsichtlichen Bedrohungen seiner Infrastruktur konzipieren und umsetzen.

4.20 Zugangssteuerung für Quellcode von Programmen

Sofern vom Auftragnehmer Software oder IT-Systeme entwickelt werden, die im Rahmen der beauftragten Dienstleistung zur Anwendung kommen, muss der Auftragnehmer sicherstellen, dass der Zugriff auf Quellcode und vertrauliche technische Dokumente ausschließlich von berechtigten Mitarbeitern oder berechtigten Unterauftragnehmern erfolgen kann. Dies gilt nicht für Open Source Software.

4.21 Kryptographische Maßnahmen

Sollten wir im Zusammenhang mit der Dienstleitung kryptographische Maßnahmen erforderlich sein, so muss der Auftraggeber sicherstellen, dass diese Maßnahmen den Vorgaben der BSI Richtlinie TR-02102-4 entsprechen.

Kryptographische Schlüssel müssen vom Dienstleister gegen unbefugte Verwendung abgesichert werden. Sofern die Verwendung von Schlüsseln zeitlich beschränkt ist, muss der Dienstleister angemessene Prozesse umsetzen, um eine rechtzeitige Aktualisierung sicherzustellen.

4.22 Serviceberichte

Werden Dienstleistungen (Wartungen, Service, Kalibrierungen, etc.) an Anlagen durchgeführt, so ist im Anschluss daran immer ein Servicebericht anzufertigen, der mindestens folgende Punkte enthält:

- Wann wurde die Dienstleistung durchgeführt?
- An welcher Anlage wurde die Dienstleistung durchgeführt?
- Was wurde geändert?
- Sind weitere Maßnahmen bzw. Arbeiten erforderlich?

Der unterschriebene Servicebericht muss bei der beauftragenden Abteilung der Sozialstiftung Bamberg (z.B. TIM oder Bau und Technik) abgegeben werden.

4.23 Software- und Systementwicklung und Tests

Sofern Gegenstand der beauftragten Dienstleistung die Entwicklung von Software oder IT-Systemen ist oder in unmittelbarem Zusammenhang mit der Dienstleistungserbringung steht, so hat der Auftragnehmer in eigener Verantwortung Richtlinien für die sichere Entwicklung von Software bzw. Systemen festzulegen und innerhalb seiner Organisation anzuwenden.

Die Sicherheit von Entwicklungsumgebungen ist vonseiten des Auftragnehmers zu gewährleisten. Wird die Entwicklung von Software oder Systemen vom Auftragnehmer an Unterauftraggeber ausgelagert, so ist der Auftragnehmer verpflichtet, die Entwicklung in angemessenen Umfang zu überwachen. Während der Entwicklung müssen Sicherheitsfunktionen in angemessenem Umfang getestet werden. Systemabnahmetests sind durchzuführen und zu dokumentieren.

Systeme, die für die Entwicklung und den Test genutzt werden, müssen von den produktiven Systemen getrennt sein.

Falls vonseiten des Auftraggebers vertrauliche Testdaten zur Verfügung gestellt werden, so hat der Auftragnehmer die Vertraulichkeit der Testdaten zu gewährleisten. Die Daten dürfen ausschließlich zu diesem Zweck genutzt werden.

4.24 Maßnahmen gegen Schadsoftware

Der Auftragnehmer muss sicherstellen, dass auf allen Computersystemen, 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 Schadcodedefinitionen sind ständig aktuell zu halten. Dies betrifft insbesondere auch solche Geräte, die für Supporttätigkeiten für den Auftraggeber bzw. beim Auftraggeber eingesetzt werden.

4.25 Sicherung von Informationen

Der Auftragnehmer muss angemessene Maßnahmen zur Datensicherung umzusetzen, die einen Verlust von Daten, die im Zusammenhang mit der Beauftragung stehen, ausschließen.

4.26 Ereignisprotokollierung und Schutz der Protokollinformationen

Sofern im Zusammenhang mit der Dienstleistungserbringung von Seiten des Auftragnehmers Computersysteme zum Einsatz kommen, so hat der Auftragnehmer sicherzustellen, dass Ereignisse in angemessenem Umfang protokolliert werden. Der Zugriff auf die Protokollinformationen darf nur berechtigten Mitarbeitern des Auftragnehmers erlaubt sein. Dies gilt insbesondere, falls im Rahmen der Protokollierung personenbezogene Daten gespeichert werden. Die Protokollierung muss insbesondere sicherstellen, dass Fehlersituation analysiert werden können. Die Protokollinformationen müssen im Fehlerfall oder bei Datenschutzverletzungen dem Auftraggeber auf Anfrage vorgelegt werden.

4.27 Installation von Software

Der Auftragnehmer hat eigenverantwortlich sicherzustellen, dass Betriebsabläufe aufseiten des Auftraggebers durch die Installation von Software nicht gestört werden. Die Installation von Software auf Systemen des Auftraggebers ist im Einzelfall mit den zuständigen Mitarbeitern des Auftraggebers abzustimmen. Bei allen Systemen, die im Netzwerk der Sozialstiftung Bamberg betrieben werden, muss sichergestellt werden, dass die Nutzung zum vorgesehenen Zweck auch ohne Administrationsrechte möglich ist. Sicherheitsrelevante Konfigurationsänderungen dürfen nur von einem eingeschränkten Nutzerkreis (z.B. Administratoren) vorgenommen werden können.

4.28 Handhabung von technischen Schwachstellen

Sofern für die Erbringung der beauftragten Dienstleistung Computersysteme des Auftragnehmers zum Einsatz kommen oder IT-Systeme, -Services oder -Komponenten geliefert werden, ist der Auftragnehmer verpflichtet, diese Systeme bzw. Services und Komponenten in angemessenem Umfang und regelmäßig auf Schwachstellen zu überprüfen. Penetrationstests werden empfohlen. Schwachstellen müssen vom Auftragnehmer umgehend beseitigt werden. Die Durchführung von Schwachstellenprüfungen und Penetrationstests sollen dem Auftraggeber auf Anfrage nachgewiesen werden können.

4.29 Maßnahmen für Audits von Informationssystemen

Für den Fall, dass die Überprüfung von IT-Systemen oder sonstigen technischen Produkten Teil oder Gegenstand der beauftragten Dienstleistung ist, so müssen diese Prüfungen vom Dienstleister in Abstimmung mit dem Auftraggeber sorgfältig geplant werden.

4.30 Netzwerksicherheitsmanagement

Sofern im Rahmen der Dienstleistung vonseiten des Auftragnehmers vernetzte Computersysteme zum Einsatz kommen, so muss der Auftragnehmer eigenverantwortlich sicherstellen, dass diese Netzwerke in angemessenem Umfang verwaltet und gesteuert werden, um Systeme und Anwendungen zu schützen. Insbesondere sollen Informationsdienste, Benutzer und Informationssysteme in Netzwerken in angemessenem Umfang gruppenweise voneinander getrennt gehalten werden (Netzwerksegmentierung).

4.31 Sicherung von Anwendungsdiensten in Netzwerken

Sofern von Seiten des Auftragnehmers im Zusammenhang mit der Dienstleistungserbringung Anwendungsdienste über Netzwerke bereitgestellt werden, so hat der Auftragnehmer sicherzustellen, dass die Dienste vor betrügerischer Tätigkeit (insbesondere Hacker-Angriffen), Vertragsstreitigkeiten und unbefugter Offenlegung oder Veränderung in angemessenem Umfang geschützt sind. Die regelmäßige Durchführung von Penetrationstests wird nachdrücklich empfohlen (siehe oben).

5 Anforderungen an Lieferanten und Hersteller von Medizinprodukten

Medizinprodukte müssen über das CE-Zeichen verfügen, über das der Hersteller die Einhaltung der Anforderungen des Konformitätsbewertungsverfahrens nachweist.

Hersteller von Medizinprodukten müssen den Anforderungen der EN 80001-1 nachkommen und die Sozialstiftung Bamberg bei der Einhaltung der Anforderungen dieser Norm unterstützen