DIENSTLEISTERRICHTLINIE INFORMATIONSSICHERHEIT

VERSION: 22 | DOKUMENTENSTATUS: FREIGEGEBEN

Klassifikation: interner Gebrauch

DOKUMENTENEIGENSCHAFTEN

Dokumentenstand:	13.03.2025
Fachlicher Ansprechpartner:	Sengenberger, Joachim
Verantwortliche Führungskraft:	Willeke, Tanja
Freigabeverantwortlicher	Buettner, Georg

Klassifikation:	interner Gebrauch

INHALTSVERZEICHNIS

Freigabedatum	28. März 2025	Freigegebene Version	22

INHALT

1. GRUNDSÄTZE

In dieser Richtlinie werden Mindestanforderungen zur Gewährleistung von Informationssicherheit definiert, die einen angemessenen Schutz von Daten erreichen sollen. Die Regelungen verfolgen das Ziel, technisch-organisatorische Maßnahmen nach dem Stand der Technik im Sinne des Art. 32 der Datenschutzgrundverordnung (DSGVO) zu standardisieren. Dabei werden anhand der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit Maßnahmen definiert, die Risiken der Datenverarbeitung minimieren sollen.

2. GELTUNGSBEREICH

Diese Richtlinie legt verbindliche Mindestanforderungen an die Informationssicherheit fest. Die Vertragspartner sind verantwortlich für die Einhaltung der Regelungen dieser Richtlinie. Erfolgt seitens des Auftragnehmers eine Unterbeauftragung, so muss der beauftragte Dienstleister für eine Verpflichtung des Unterbeauftragten sorgen, die die Einhaltung dieser Vorgaben durch den Unterbeauftragten sicherstellt. Anforderungen als Ausdruck normativer Festlegungen werden dem RFC 2119 entsprechend durch die deutschen Schlüsselworte MUSS, DARF NICHT, SOLLTE, SOLLTE NICHT, KANN (sowie deren grammatikalische Formen) gekennzeichnet.

3. ALLGEMEINE ANFORDERUNGEN

Allgemeine Anforderungen beinhalten im Wesentlichen organisatorische Prozesse zur Kommunikation und Zuständigkeit.

Anforderung	Maßnahme
Ansprechpartner Informationssicherheit	Der Auftragnehmer MUSS einen Ansprechpartner benennen, der für die Einhaltung der Anforderungen dieser Richtlinie verantwortlich ist.
Meldestelle Sicherheitsvorfall	Der Auftragnehmer MUSS eine zentrale Meldestelle einschließlich der Kontaktdaten benennen.
Organisation der Informationssicherheit	Der Auftragnehmer SOLL, falls vorhanden, ein ISO 27001-Zertifikat oder Äquivalente bereitstellen, sowie Nachweise im Rahmen der Leistungserbringung
Sicherheitsvorfälle	Der Auftragnehmer MUSS Sicherheitsvorfälle, die potenziell negativen Einfluss auf die vereinbarten Leistungen oder die verarbeiteten Daten haben, unverzüglich dem Auftraggeber melden.
Informationsverarbeitung beim Auftragnehmer	Alle Informationen und Daten, die beim Auftragnehmer im Rahmen seiner Tätigkeit bekannt werden oder anfallen, MÜSSEN nach den Anforderungen dieser Richtlinie sicher verarbeitet bzw. gespeichert werden.
Vertraulichkeitsvereinbarung	Der Auftragnehmer MUSS Sorge dafür tragen, dass seine Mitarbeiter bzw. Unterauftragnehmer die Vertraulichkeit der erlangten Informationen sowie die Einhaltung dieser Richtlinie auch über das Ende des Vertragsverhältnisses einhalten.
Auditierungsmöglichkeiten	Der Auftragnehmer stimmt zu, dass der Auftraggeber oder ein beauftragter Dritter des Auftraggebers die Organisation in Bezug auf die Informationssicherheit des Auftragnehmers auditieren KANN.

4. FERNZUGANG

Die Anforderungen zum Fernzugang dienen in erster Linie dem Schutz der Informationen des Auftraggebers, sind jedoch auch bei Zugängen des Auftragnehmers zu berücksichtigen.

Anforderung	Maßnahme
Einhaltung Sicherheitsschutzziele	Der Auftragnehmer MUSS sicherstellen, dass bei Fernzugängen die Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Daten des Auftraggebers gewährleistet wird.
Informationsverwendung	Der Auftragnehmer MUSS insbesondere die durch den Fernzugang erlangten Informationen auch nach Beendigung des Zugriffs angemessen schützen.
Individuelle Benutzerkonten	Der Auftragnehmer MUSS dafür Sorge tragen, dass Konten für den Fernzugriff nur von autorisierten und authentifizierten Personen verwendet werden.
zeitliche Beschränkung	Der Auftragnehmer SOLLTE Fernzugänge nur nach Freischaltung und zeitlicher Begrenzung für einen Wartungsfall einsetzen.
2-Faktor-Authentifizierung	Der Auftragnehmer SOLLTE Fernzugänge sicher verwenden und sowohl Verschlüsselung und insbesondere bei Zugriff über öffentliche Netze eine 2-Faktor-Authentifizierung verwenden.

5. SOFTWAREENTWICKLUNG/PRODUKTE

Die Anforderungen zur Softwareentwicklung gelten auch für Produkte, die in Teilen oder als Gesamtprodukt für den Auftraggeber erstellt oder zur Verfügung gestellt werden.

Anforderung	Maßnahme
Einhaltung von Entwicklungsstandards	Der Auftragnehmer MUSS die Software nach anerkannten Standards zur sicheren Programmierung entwickeln. Anerkannte Standards sind Kriterien für Softwarequalität gem. ISO/IEC 9126 (aktualisiert durch ISO/IEC 25000) und OWASP.
Security by Design	Der Auftragnehmer MUSS bereits bei der Anforderungsdefinition und Konzeption des Produkts die IT-Sicherheit berücksichtigen.
Dokumentation	Der Auftragnehmer MUSS über einen dokumentierten Entwicklungsprozess verfügen, der physische, organisatorische und personelle Sicherheit abdeckt.
Schutzziele berücksichtigen	Der Auftragnehmer MUSS die Software und die damit verarbeiteten Daten in Bezug auf Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit schützen.
Schwachstellenmanagement	Der Auftragnehmer MUSS die Software auf Basis dokumentierter Prozesse entwickeln, die explizit Änderungs- und Schwachstellenmanagement umfassen.
Patchmanagement	Der Auftragnehmer MUSS bei Kenntnisnahme von Fehlern oder Sicherheitslücken, die eine Gefährdung der verarbeiteten Informationen oder Systemen darstellen, zeitnah Aktualisierungen zur Verfügung stellen.
Mitarbeiterschulung	Der Auftragnehmer MUSS zur Erbringung der Dienstleistung die Zuverlässigkeit und Qualifizierung der Mitarbeiter in Bezug auf Informationssicherheitsanforderungen sicherstellen.
Quellcodeverwaltung	Die Entwicklung MUSS auf sicheren Systemen erfolgen, die den Quellcode gegen fremde Zugriffe schützt und gegenüber Schwachstellen auf dem aktuellen Stand hält.

Richtlinien zur sicheren Entwicklung	Der Auftragnehmer MUSS Richtlinien zur eingesetzten Programmiersprache verwenden, die den Best Practice-Empfehlungen der Softwareentwicklung entsprechen.
Open-Source-Komponenten	Die Verwendung von Open-Source-Komponenten MUSS angemessen dokumentiert, konfiguriert und regelmäßig auf Aktualisierung geprüft werden.
Testverfahren	Der Auftragnehmer SOLLTE Testverfahren zu implementierten Sicherheitsmechanismen und -funktionen umsetzen (z. B. Verschlüsselung, Zugriffskontrollen, Authentisierung).
Secure-Code-Reviews/Pentests	Der Auftragnehmer SOLLTE regelmäßige Überprüfungen der Software in Bezug auf sicheren Quellcode und Pentests durchführen und die Ergebnisse dem Auftraggeber zur Verfügung stellen.
Testdaten	Der Auftragnehmer MUSS sicherstellen, dass in Entwicklungsumgebungen ausschließlich Testdaten oder ausreichend anonymisierte Daten verwendet werden.
Cyber-Resilienz	Der Auftragnehmer SOLLTE eine SBOM zur Verfügung stellen, die den Mindestanforderungen der Technischen Richtlinie des BSI TR-03183 entspricht. Dieses wird verpflichtend ("MUSS"), sobald der CRA in Kraft tritt.

6. IT-BETRIEB

Der IT-Betrieb definiert nicht nur Anforderungen an die Bereitstellung von IT-Betriebsdienstleistungen, sondern gilt grundsätzlich für Systeme und Komponenten, die im Rahmen der vereinbarten Leistung eingesetzt werden.

Anforderung	**Maßnahme**
Zugriffsschutz und Berechtigungsvergabe	Der Auftragnehmer MUSS Prozesse und Kontrollen zum Zugriffsschutz und zur Berechtigungsvergabe implementieren
Passwortsicherheit	Der Auftragnehmer MUSS eine angemessene Passwortkomplexität und -gültigkeit umsetzen.
Personalsicherheit	Der Auftragnehmer MUSS angemessene Maßnahmen zur Qualifizierung der Mitarbeiter im Rahmen der Informationssicherheit gewährleisten.
physische Sicherheit	Der Auftragnehmer MUSS zentrale Systeme, die zur Leistungserbringung verwendet werden, ausreichend vor Umwelteinflüssen schützen und den Zutritt kontrollieren.
Netzwerksicherheit	Der Auftragnehmer MUSS das Netzwerk entsprechend dem Schutzbedarf Segmentieren und durch z. B. Firewalls gegen unbefugte Zugriffe schützen.
Datenübertragung	Der Auftragnehmer MUSS Sorge tragen, dass schutzwürdige Daten, insbesondere Passwörter oder Sozialdaten nur verschlüsselt übermittelt werden.
Protokollierung	Systemzugriffe oder administrative Tätigkeiten MÜSSEN angemessen protokolliert werden.
Virenschutz	Der Auftragnehmer MUSS auf IT-Komponenten, die Zugriff auf schützenswerte Informationen oder Systeme haben, einen Virenschutz einsetzen.
Datensicherung	Der Auftragnehmer MUSS Datensicherungs- und Wiederherstellungsprozesse etabliert haben, die zur Aufrechterhaltung der Dienstleistung benötigt werden.

Datenlöschung	Der Auftragnehmer MUSS sicherstellen, dass Datenlöschungen mit ausreichend sicheren Verfahren durchgeführt werden, die eine Wiederherstellung verhindern, z. B. bei Aussonderung.
Änderungsmanagement	Der Auftragnehmer MUSS für Produktionsumgebungen ein Change-Management-Prozess etabliert haben.
Patchmanagement	Der Auftragnehmer MUSS sicherstellen, dass IT-Komponenten regelmäßig mit aktuellen Patches und Sicherheitsupdates versorgt werden.
Schwachstellenmanagement	Der Auftragnehmer MUSS Systeme regelmäßig auf Schwachstellen prüfen und eine zeitnahe Behebung durchführen.
Systemhärtung	Der Auftragnehmer MUSS produktive Systeme härten und nicht benutzte Dienste deaktivieren sowie Anwendungen sicher konfigurieren.
Vorfallsmanagement	Der Auftragnehmer MUSS Prozesse zum Incident-Management und zur schnellen Reaktion auf IT-Sicherheitsvorfälle etabliert haben.
Notfallmanagement	Der Auftragnehmer MUSS ein angemessenes Notfallmanagement etabliert haben, um die Aufrechterhaltung der Dienstleistung im Notfall sicherstellen zu können.

Dieses Dokument wurde per WF signiert. Die Signatur dient als Nachweis für die Authentizität und Integrität des Dokumentes und bestätigt, dass es vom Unterzeichner autorisiert wurde. Die Signatur kann anhand der zugrunde liegenden Daten in Confluence überprüft und nachgewiesen werden.

COPYRIGHT

© Copyright 2025 AOK Systems GmbH. Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch die AOK Systems GmbH nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden.

Bei Verstoß halten wir uns die Durchsetzung von Schadensansprüchen vor.

Hauptsitz AOK Systems GmbH | Kortrijker Straße 1 | 53177 Bonn | T 0228 843 0 | F 0228 843 1111 | aok-systems@sys.aok.de | www.aok-systems.de
Geschäftsführung: Georg Büttner
Vorsitzende des Aufsichtsrates: Dr. Carola Reimann
Handelsregister Bonn HRB 17142 | USt-IdNr. DE19648705917 | Kreissparkasse Köln | IBAN DE79 3705 0299 0002 1374 53 | BIC COKSDE33
Commerzbank AG Troisdorf | IBAN DE87 3704 0044 0310 3595 00 | BIC COBADEFF