Alles Gute.
KVBW
Kassenärztliche Vereinigung Baden-Württemberg

ISMS-Richtlinie

Sicherheit im Umgang mit Dienstleistenden und Lieferanten

Verantwortlich:	Informationssicherheitsbeauftragte/r		
Dokumententyp:	ISMS-Richtlinie		
Klassifizierung:	Intern		
Zielgruppe:	Beschäftigte		
Version:	2.0		
Status:	gültig		
Fassung vom:	02.03.2023		
Freigabe durch:	Vorstand	am:	26.05.2023
	Geschäftsführung	am:	16.05.2023
Beschlossen durch:	Vorstand	am:	26.05.2023
	Personalrat	am:	31.05.2023

Dokumenteninformationen

Dokumentenname:	ISMS-Richtlinie Sicherheit im Umgang mit Dienstleistenden und Lieferanten
Aktuelle Version	2.0
Datum der Erstellung:	01.07.2018
Datum der letzten Änderung:	02.03.2023
Nächster Review Termin:	März 2024

Dokumentenhistorie

Version	**Änderungsbeschreibung**
1.0	Finale Fassung
1.1	Review 2022
1.2	Inhaltliche und redaktionelle Anpassungen, Veränderung der Struktur
1.3	Review 2023 und inhaltliche Anpassungen
2.0	Anpassung der ISMS-Richtlinie auf aktuelle Dokumentenvorlage

Dokumentenfreigabe

Name	**Funktion**	**Datum**
Dr. med. Karsten Braun	Vorsitzender des Vorstandes	26.05.2023
Dr. med. Doris Reinhardt	Stellv. Vorstandsvorsitzende	26.05.2023
Rita Roos-Fink	Vorsitzende des Personalrates	31.05.2023
Falk Lingen	Geschäftsführung	16.05.2023

Veröffentlichung

Name	**Datum**
Intranet	05.06.2023
INFOPortal	05.06.2023

Anmerkungen zum Dokument:
Im Interesse des Textflusses und der Lesefreundlichkeit werden nach Möglichkeit geschlechtsunspezifische Begriffe verwendet. Sämtliche Personenbezeichnungen gelten gleichwohl für alle Geschlechter.

Inhaltsverzeichnis

1 Zweck und Geltungsbereich

1.1 Einleitung

Die ISMS-Richtlinie „Sicherheit im Umgang mit Dienstleistenden und Lieferanten“ (ISMS-RL Sicherheit im Umgang mit Dienstleistenden und Lieferanten) legt Vorgaben und Verfahren für die Zusammenarbeit mit IT-Dienstleistenden und Lieferanten im Rahmen der Informationssicherheit für den Geltungsbereich des Informationssicherheitsmanagementsystems (ISMS) fest.

2 Allgemeines

2.1 Begriffe und Definitionen

Unter dem Begriff „Lieferant“ werden alle Arten von IT-relevanten Lieferanten verstanden, die z.B. IT-Infrastruktur-Komponenten, Logistik und Versorgungseinrichtungen, oder auch externe Dienstleistungen bereitstellen.
„IT-Dienstleistende“ sind eine spezielle Art von Lieferanten, die IT-spezifische Serviceleistungen (u.a. Beratung für IT-Lösungen, Installation und Konfiguration von IT-Systemen, Wartungstätigkeiten) bereitstellen.
Als Ansprechpartner für Fragen der Informationssicherheit in der KVBW steht der Informationssicherheitsbeauftragte / -manager (ISB/ISM) zur Verfügung.

Fragen zu Vertragsinhalten werden durch die Fachabteilung Vertrags- und Auftragsmanagement (VAM) zentral beantwortet, für Beschaffungs- und Ausschreibungsfragen ist die zentrale Vergabestelle (ZVS) oder die IT-Beschaffung zuständig. Weitere Beschaffungen können durch einzelne Geschäftsbereiche selbstständig durchgeführt werden.

3 Allgemeine Regelungen

3.1 Grundsätze für die Beauftragung von Lieferanten und Dienstleistende

Mit jedem IT-Dienstleistenden oder Lieferanten, der Zugang zu Informationen der KVBW hat, diese verarbeiten, speichern oder weitergeben kann oder IT-Infrastrukturkomponenten dafür bereitstellt, werden entsprechende Informationssicherheitsanforderungen vereinbart, die für die jeweilige Leistung geeignet und angemessen sind. Bei **erhöhtem Schutzbedarf „vertraulich“** oder sogar **„streng vertraulichen“** Informationen, mit denen der Lieferant oder Dienstleistende in Berührung kommt, ist zusätzlich zu prüfen, ob eine Zertifizierung (bspw. ISO/IEC 27001) verlangt werden sollte.

Hierbei ist zu bedenken, dass das Vereinbaren und Festlegen von Informationssicherheitsanforderungen ein iterativer (sich wiederholender) Prozess ist und nicht jede dieser Anforderungen gegenüber jedem Lieferanten beim Abschluss eines Vertrages durchgesetzt werden kann, sowie die legale und vertragliche Verantwortung für den Schutz sensibler Informationen bei der KVBW verbleibt. Auch aus diesem Grund ist das Recht zur Auditierung von Lieferanten und Dienstleistenden durch die KVBW, wann immer möglich, vertraglich zu vereinbaren.
Die Bedarfsanforderung von IT-Services, IT-Anwendungen und IT-Dienstleistungen hat über den GB IT (ServiceDesk) zu erfolgen. Bei Einhaltung dieses Weges wird durch GB IT mit Unterstützung des ISB bzw. ISM sichergestellt, dass die Informationssicherheitsanforderungen (Technische und Organisatorische Maßnahmen der

KVBW (früher: IT-Sicherheitsstandard KVBW)) bei der nachfolgenden Beschaffung durch den zentralen Einkauf bzw. die IT-Beschaffung berücksichtigt werden.
Die nachfolgenden Vorgaben und Verfahren beziehen sich auf die Erbringung von IT-Dienstleistungen, wobei der Schwerpunkt auf der externen Erbringung von IT-Services liegt.

3.2 Anforderungen an den Datenschutz

Die Einhaltung der Informationssicherheitsanforderungen der KVBW ist mit dem Dienstleistenden vertraglich zu vereinbaren und zu dokumentieren. In der Regel sind die Informationssicherheitsanforderungen durch den Abschluss einer AV-Vereinbarung bei der externen Erbringung von IT-Services abgedeckt.
Die datenschutzrechtlichen Anforderungen an die Auftragsverarbeitung sind zu berücksichtigen und durch AV-Vereinbarungen zu regeln. Zur Klärung kann im Bedarfsfall der Datenschutzbeauftragte (DSB) hinzugezogen werden.

Die Überprüfung der technischen und organisatorischen Maßnahmen eines Lieferanten oder Dienstleistenden sollte entsprechend geprüft werden.

4 Absicherung der Kommunikation

Bei elektronischer Kommunikation zwischen der KVBW und einem IT-Dienstleistenden oder Lieferanten hat der jeweilige Bereich dafür zu sorgen, dass die Sicherheit der Kommunikation gewährleistet ist. So sind z.B. interne und vertrauliche Dokumente dem IT-Dienstleistenden verschlüsselt in einem zip-Anhang zu übermitteln (bei Verwendung eines getrennten Übertragungsweges des zur Verschlüsselung verwendeten Passwortes).
Des Weiteren gelten die Vorgaben aus den ISMS-Richtlinien „Klassifizierung und Kennzeichnung von Informationen“ und „Verschlüsselung und Einsatz kryptographischer Methoden“.

5 Zutritts-, Zugangs- und Zugriffsrechte

Sofern für die Leistungserbringung des IT-Dienstleistenden oder Lieferanten der Zutritt zu Räumlichkeiten der KVBW oder der Zugang zu bzw. der Zugriff auf Daten und IT-Systeme der KVBW erforderlich ist, so muss der jeweilige Bereich die Rechte des IT-Dienstleistenden oder Lieferanten entsprechend regeln und dabei auf das zur Leistungserbringung erforderliche Maß begrenzen.
Es gelten hier zudem die Regelungen der Dienstanweisung „Besucher und Externe Dienstleister“ nebst Anlagen, sowie der Policy „IT-Access-Management“ und der „Technischen und Organisatorischen Maßnahmen der KVBW“ (früher: IT-Sicherheitsstandard KVBW).

6 Sicherheitsanforderungen bei externen IT-Serviceerbringung

6.1 Grundsätze zur Sicherheit externer IT-Services

Wenn IT-Services extern durch einen IT-Dienstleistenden (Outsourcing, Cloud Computing) erbracht werden sollen, ist durch den jeweiligen Bereich mit Unterstützung des ISB bzw. ISM zu prüfen, welche Sicherheitsanforderungen anzuwenden sind. Hierbei sind eine ISO/IEC 27001 Zertifizierung (mit dem entsprechenden Geltungsbereich), die in der KVBW geltenden Anforderungen an die Informationssicherheit sowie auch der Anforderungskatalog Cloud Computing (C5) des BSI zu berücksichtigen. Diese Anforderungen müssen die folgenden Aspekte enthalten:

- Ein IT-Sicherheitskonzept oder ein belastbarer Nachweis (z.B. durch eine Unternehmenszertifizierung einschl. des Zertifizierungsberichts) soll durch den externen IT-Dienstleistenden vorgelegt werden.

- Physische und logische Maßnahmen zur Gewährleistung von Integrität und Vertraulichkeit der Daten von KVBW, u.a. Zutrittsschutz, Brandschutz, Klimatisierung von Serverräumen, Härtung von IT-Systemen, Einsatz von Verschlüsselungstechniken, Schutz vor Schadsoftware und sicheres Löschen von auszusondernden Speichermedien, sollen durch den externen IT-Dienstleistenden dokumentiert und der KVBW vorgelegt werden.

- Die Verwaltung aller Anwendungs- und Systemzugriffe beim externen IT-Dienstleistenden soll auf Basis eines umfassenden Berechtigungskonzepts erfolgen.

- Der externe IT-Dienstleistende soll eine zentrale Überwachung der Netzzugriffe und Absicherung der IT-Infrastrukturen gegen nicht autorisierte Zugriffe umsetzen.

- Notfallpläne und Nachweise für regelmäßig durchgeführte Notfallübungen sollen durch den externen IT-Dienstleistenden vorgelegt werden.

- Ein klar definierter Meldeprozess bei Informationssicherheitsvorfällen und -ereignissen, sowie datenschutzrelevanten Vorfällen ist zu vereinbaren.

- Das Recht der KVBW zum Audit ist zu vereinbaren (einschl. Definition der entsprechenden Audit-Prozesse, z.B. Umfang und Art der Prüffelder, Häufigkeit der Audits, mit oder ohne Vorankündigung).

- Die Rückgabe oder Vernichtung von Informationen nach vereinbarten Zeitpunkten bzw. nach Vertragsende ist zu regeln.

- Der externe IT-Dienstleistende soll ein Backupkonzept umsetzen, das die folgenden Punkte regelt:
  - die Art und den Umfang der Datensicherung,
  - die Wiederherstellzeiten bei Rücksicherungen,
  - die Aufbewahrungszeiten von Datensicherungsmedien sowie
  - die Archivierung von Daten
  - die datenschutzkonforme Löschung von Daten
  - die Wahrung von eventuellen Betroffenenrechten.

7 Umgang mit (IT-)Dienstleistungsänderungen

Änderungen bei der Erbringung von IT-Dienstleistungen durch Lieferanten (Lieferanten- und Dienstleister-Management) müssen geplant werden, wobei die Kritikalität der Geschäftsinformationen und der beteiligten Systeme und Prozesse sowie ggfs. eine Neubewertung von Risiken, einschließlich der Aufrechterhaltung bestehender Verfahren und Kontrollen, zu berücksichtigen ist.

Bei der Erweiterung einer bestehenden IT-Dienstleistung ist eine erneute Sicherheitsbetrachtung (Lieferanten- und Dienstleister-Management) des betroffenen (IT-) Services durchzuführen.
Die Entwicklung neuer Anwendungen und IT-Services muss unter Beachtung der Kritikalität bzw. des Schutzbedarfs der beteiligten Systeme und Prozesse geplant werden.

Bei Änderungen von Dienstanweisungen oder anderer Regelungen sind alle IT-Dienstleistungen bzw. die im Rahmen der Erbringung dieser IT-Dienstleistungen getroffenen Regelungen zu prüfen, ob diese von Änderungen betroffen sind. Sich hieraus ergebende Anpassungen sind zu veranlassen.

Bei Änderungen an extern erbrachten IT-Dienstleistungen durch

- Änderungen und Verbesserung an der Netzwerkinfrastruktur
- Nutzung neuer Technologien
- Einsatz neuer Entwicklungswerkzeuge und Umgebungen
- Änderungen des Sitzes des Dienstleistenden
- Wechsel des Dienstleistenden
- Beauftragung eines Subunternehmers

ist eine Neubewertung der Risiken der beteiligten Systeme und Prozesse unter Berücksichtigung der Kritikalität von Geschäftsinformationen erforderlich (Risikomanagement).

8 Steuerung der Dienstleistungserbringung

Die vereinbarte Dienstleistungsqualität des externen IT-Dienstleistenden ist regelmäßig zu überprüfen und zu steuern (Lieferanten- und Dienstleister-Management). Dazu gehören die Überprüfung von Aufzeichnungen des Dienstleistenden über Informationssicherheitsereignisse, Betriebsprobleme, Störungen und Unterbrechungen bzgl. der Serviceerbringung sowie die Verfolgung von Fehlern. Zusätzlich sollte eine Kategorisierung der Lieferanten und Dienstleistenden (A, B, C, D) erfolgen anhand derer sich die fortlaufende Überprüfung orientiert und diese priorisiert (Lieferanten- und Dienstleister-Management).

Es muss eine Prüfung der Dienstleistungsberichte und die Vereinbarung regelmäßiger Treffen oder Termine zur Abstimmung des vereinbarten Service erfolgen.

Es ist sicherzustellen, dass der IT-Dienstleistende über ausreichend Kapazitäten und eine Planung verfügt, die gewährleisten, dass bei kritischen Serviceausfällen oder Katastrophen das im EVB-IT (Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen) vereinbarte Serviceniveau eingehalten werden kann.

Wenn es für die externe IT-Service Erbringung relevant ist, sollte eine Überprüfung der Informationssicherheitsaspekte der Beziehungen des Dienstleistenden mit dessen Lieferanten erfolgen.

9 Sonstiges

Der Informationssicherheitsbeauftragte und der Informationssicherheitsmanager der KVBW können, im Rahmen des Geltungsbereiches des ISMS, Ausnahmen von dieser Richtlinie empfehlen, wenn die Grundsätze des Datenschutzes und der Informationssicherheit eingehalten werden. Dabei sind die geltenden Gesetze und Verordnungen zu beachten.

Die Ausnahmen von den in dieser Richtlinie vorgegebenen Regelungen müssen schriftlich begründet und nachvollziehbar dokumentiert werden. Sie müssen vorab vom Vorstand und von der Geschäftsführung genehmigt werden.

Stuttgart, den 31.05.2023

Im Original gezeichnet

Dr. Karsten Braun
Vorsitzender des Vorstands

Im Original gezeichnet

Dr. Doris Reinhardt
Stellv. Vorstandsvorsitzende

Im Original gezeichnet

Rita Roos-Fink
Vorsitzende des Personalrates