Richtlinie zum Lieferantenmanagement

Informationssicherheitsmanagementsystem

Bearbeiter	Karl-Heinz Borgheyink / Jörg Ritter
Verantwortliche Organisationseinheit	Informationssicherheitsbeauftragter Datenschutzbeauftragter Fachabteilungen
Verteiler	Alle Mitarbeiterinnen und Mitarbeiter der Kassenzahnärztlichen Vereinigung Westfalen-Lippe und alle Lieferanten und Partner, welche die Fähigkeit zur Beeinflussung der Vertraulichkeit, Integrität und Verfügbarkeit sensibler Informationen der KZVWL besitzen. Eine Weitergabe an Dritte ist nur nach Freigabe durch den ISB erlaubt
Datum der letzten Bearbeitung/Freigabe	05.12.2024
Version	3.0
Vertraulichkeitsstufe	intern
Freigabestatus	Freigegeben

1 Inhaltsverzeichnis

2 Generelle Informationen

2.1 Ziel und Zweck des Dokumentes

Der Zweck dieses Dokuments ist die Festlegung der Vorschriften für Beziehungen zu Lieferanten und Dienstleistern.

Ziel ist es, die Anforderungen an die Informationssicherheit mit den Lieferanten abzustimmen und zu regeln sowie Vorgaben zur Überprüfung der Informationssicherheit zu definieren.

Im Vorfeld jeder Auftragsvergabe sind Sicherheitsaspekte zu bedenken und bei einer Ausschreibung zu berücksichtigen.

Dieses Dokument gilt für alle Lieferanten und Partner, welche die Fähigkeit zur Beeinflussung der **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** sensibler Informationen der KZVWL besitzen.

Anwender dieses Dokuments sind die Innere Verwaltung der KZVWL sowie alle anderweitigen Personen, die bei KZVWL verantwortlich für Lieferanten und Dienstleister sind.

Auf eine geschlechterspezifische begriffliche Trennung wird aus Vereinfachungsgründen bewusst verzichtet. Es wird in der Regel die geläufigere Form gewählt.

2.2 Geltungsbereich

Die vorliegende Richtlinie gilt für den Geltungsbereich, welcher in der Leitlinie Informationssicherheit und Datenschutz [1] definiert ist.

2.3 Freigabe

Die vorliegende Richtlinie tritt mit seiner Freigabe durch den ISB im Namen des Vorstands der KZVWL in Kraft.

2.4 Revision

Dieses Dokument sowie die daraus sich ergebenden Sicherheitsmaßnahmen unterliegen der Dokumentenlenkung [2].

3 Anwendung auf Normen

Auf dieses Dokument werden folgende Maßnahmen der ISO-Normen angewendet. Die definierten Maßnahmen in den ISO-Normen sind selbst als Arbeitshilfen zu bewerten, weil sie beschreiben was in den Dokumenten und Aufzeichnungen erwartet wird.

DIN ISO/ IEC 27001:2022

Maßnahme ISO27001:2022	Beschreibung
A.6.1	Sicherheitsüberprüfung
A.6.2	Beschäftigungs- und Vertragsbedingungen
A.6.3	Informationssicherheitsbewusstsein, -ausbildung und -schulung
A.5.11	Rückgabe von Werten
A.5.19	Informationssicherheit in Lieferantenbeziehungen
A.5.20	Behandlung von Informationssicherheit in Lieferanten-vereinbarungen
A.5.21	Umgang mit der Informationssicherheit in der Lieferkette der Informations- und Kommunikationstechnologie (IKT)
A.5.22	Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
A.8.32	Änderungssteuerung

4 Anforderungen an Lieferantenbeziehungen

4.1 Grundsätze

Informationssicherheitsanforderungen müssen von der KZVWL im Lieferantenmanagementprozess berücksichtigt werden. Lieferanten müssen in Abhängigkeit ihrer Kritikalität bezüglich der Informationssicherheit klassifiziert, überprüft und überwacht werden (siehe Punkt 4.6). In besonderen Fällen erfolgt bei Bedarf eine Prüfung durch Anwendung der Risikoanalyse.

4.2 Auswahl eines Dienstleisters/Lieferanten

Das ISMS-Team, die Beschaffungs- und die Bedarfsstelle entscheiden darüber, ob es notwendig ist, den Hintergrund individueller Lieferanten und Partner zu überprüfen, und falls ja, welche Methoden dazu anzuwenden sind.

Bei der Auswahl ist daher im Vorfeld festzustellen, welche Auswirkungen das angebotene Produkt oder die Dienstleistung auf die Informationssicherheit hat, insbesondere bei Störungen in der Durchführung des abgeschlossenen Vertrages.

In Abhängigkeit des Ergebnisses ist zu prüfen, ob der Auftragnehmer als makellos, unbescholten und unbestechlich einzuschätzen ist (Zuverlässigkeit) und ob ein ernsthaftes und fachkundiges Betreiben der Dienstleistung gewährleistet ist (Seriosität).

Zu diesem Zweck sind je nach Anforderungen u.a. die folgenden Punkte zu hinterfragen:

Allgemeine Kriterien zum Unternehmen
▪ Organisation des Unternehmens sowie Eigentumsverhältnisse
▪ Erreichbarkeit, Transportzeit, Reisezeit
▪ Qualifikation der Mitarbeiter

technische Kriterien
▪ Produktionskapazität
▪ Flexibilität hinsichtlich Auftragsänderungen
▪ Abhängigkeit von Unterlieferanten
▪ eigene Entwicklungsabteilung

Qualitätssicherung
▪ Zertifikate
▪ Umweltmanagement
▪ Total Quality Management (TQM)
▪ Liefertermintreue
▪ SGU-Management (Sicherheit, Gesundheit, Umweltschutz)

finanzielle Kriterien
▪ Marktstellung des Lieferanten
▪ Auskünfte zu Compliance-Themen
▪ Konkurrenzsituation
▪ Entwicklung von Umsatz und Gewinn
▪ Finanzauskunft

Projektmanagement
▪ Organisation des Projektmanagements
▪ Anzahl der Ansprechpartner
▪ Qualifikation/Erfahrung der Projektmanager

kaufmännische Kriterien
▪ Einstands- und Endpreis
▪ Preistransparenz/-aufschlüsselung
▪ Kommunikation (zum Beispiel feste Ansprechpartner, Erreichbarkeit)
▪ Referenzprodukte

Lieferketten Kriterien
▪ Information über eingesetzte Unterauftragnehmer geben und ggf. genehmigen lassen
▪ Regelmäßige Meldung neuer Subunternehmer

operative Kriterien
▪ Termintreue
▪ Produktqualität
▪ Lieferzeit, Reaktionszeit

4.3 Bereitstellung von Dokumenten

Dem Dienstleister/Lieferanten sind folgende, sicherheitsrelevante Dokumente zu übergeben, bevor das Unternehmen beauftragt wird und bevor Informationen über den Auftrag bereitgestellt werden:

- Verpflichtung zur Verschwiegenheit und Wahrung des Datenschutzes,
- Leitlinie Informationssicherheit und Datenschutz,
- Hausordnung für externe Dienstleister [3] (wenn diese vor Ort tätig sind),
- Richtlinie Lieferantenmanagement (dieses Dokument)

4.4 Verträge

Die Bedarfsstelle entscheidet darüber, ob der zu vergebene Auftrag hinsichtlich des Datenschutzes und der Informationssicherheit bewertet werden muss. Wenn „JA“, entscheidet der Datenschutzbeauftragte (DSB), ob individuelle Mitarbeiter des Lieferanten/Partners die Vertraulichkeitserklärung zu unterschreiben haben, wenn sie für die KZVWL tätig sind und ob ein AV-Vertrag notwendig ist.

Der Informationssicherheitsbeauftrage (ISB) entscheidet darüber, welche speziellen Anforderungen der Informationssicherheit erfüllt sein müssen.

Das ISMS-Team ist verantwortlich für die Entscheidung, welche Sicherheitsklauseln im Vertrag mit dem jeweiligen Lieferanten oder Dienstleister aufzunehmen sind. Klauseln über Vertraulichkeit und Rückgabe von Werten sind in jedem Vertrag zwingend vorgeschrieben.

Der Vertragseigentümer jedes einzelnen Vertrages ist die jeweilige Bedarfsstelle, die damit verantwortlich für den jeweiligen Lieferanten oder Partner ist.

4.5 Unterweisung externer Dienstleister

Jeder externe Mitarbeiter von Lieferanten und Dienstleistern der das Gebäude der KZVWL incl. Backuprechenzentrum im Mehrfamilienhaus Piusallee 44c betritt, hat die Vertraulichkeitserklärung, vor Betreten am Empfang zu unterzeichnen.

Diese externen Mitarbeiter sind vor Beginn ihrer Tätigkeit einzuweisen und über die für Sie relevanten hausinternen Regelungen (z.B. Hausordnung für externe Dienstleister) und Vorschriften zur Informationssicherheit sowie die organisationsweite Informationssicherheitsleitlinie zu unterrichten, die auf Wunsch ausgehändigt werden können. Dieses ist jeweils zu bestätigen.

4.6 Überwachung und Prüfung

Die Bedarfsstelle muss zusammen mit dem ISMS Team die Qualitätsstufe der Dienstleistungen und die Erfüllung der Sicherheitsklauseln durch die Lieferanten oder Partner, sowie deren Berichte und Aufzeichnungen regelmäßig überprüfen und überwachen. Dem Informationssicherheitsbeauftragten ist seitens der IT-Abteilung und der Inneren-Verwaltung quartalsmäßig eine aktuelle Lieferanten- und Dienstleisterliste zur Verfügung zu stellen.

Explizit werden Lieferanten/Dienstleister in Abhängigkeit der Kritikalität ihrer Dienstleistung klassifiziert und in Abhängigkeit dieser in Vertragspartnergruppe wie folgt eingeordnet und überprüft.

Kritikalität	Art der Prüfung	Intervall	Beispiele der DL	Vertragspartnerart
kritisch	Audit oder Papierprüfungen	Alle 2 Jahre, sowie bei Änderungen der DL	Citeq	A-Lieferant
moderat	Zwischenzeitliche Papierprüfungen, bei Vorfällen Audit unterjährig	Alle 3-5 Jahre, sowie bei Änderungen der DL	AuraSec	B-Lieferant
unkritisch	Keine Prüfungen	Keine Prüfungen	Fensterputzer	C-Lieferant

A-Lieferant:

Diese Lieferanten/Dienstleister bieten essentielle Dienstleistungen oder Produkte, deren Ausfall oder Scherheitsv orfall gravierende Auswirkungen auf die Informationssicherheit

und den Geschäftsbetrieb hat.

Beispiele sind Clouddienstleister, Softwareanbieter für sicherheitsrelevante Systeme.

B-Lieferant:

Diese Lieferanten/Dienstleister sind wichtig, aber nicht unbedingt kritisch. Ihr Ausfall könnte zu Störungen führen, jedoch nicht zu einem sofortigen oder katastrophalen Einfluss auf die Informationssicherheit. Beispiele sind allgemeine IT-Dienstleister oder Hardware-Lieferanten.

Bei A und B Lieferanten werden z.B. unter anderem je nach Dienstleistung oder Lieferung regelmäßig geprüft:

- Vorhandene Zertifikate (z.B. ISO27001, ISO 9001, Zertifikate zur Entsorgung, etc.)
- AV-Vereinbarungen
- Einhaltung von SLAs
- Leumundszeugnisse
- Verschwiegenheitserklärungen
- Bonitätsauskunft

C-Lieferant:

Diese Lieferanten/Dienstleister haben einen minimalen Einfluss auf die Informationssicherheit. Ihr Ausfall hat in der Regel keine signifikanten Auswirkungen auf den Geschäftsbetrieb. Beispiele sind Lieferanten von Büromaterial oder nicht sicherheitsrelevanten Dienstleistungen.

Beschränkt sich die Dienstleistung lediglich auf Hard- bzw. Softwareprodukte ist ein Dienstleister-/Lieferanten-Audit nicht notwendig. Ein Audit ist ebenfalls nicht notwendig, wenn der Dienstleister/Lieferant über eine Zertifizierung (ISO 27001 oder vergleichbar) verfügt. Hierbei sind der Geltungsbereich und der Ablauf / Gültigkeit des Zertifikats zu berücksichtigen.

4.7 Änderung oder Beendigung von Lieferantenverträgen

Die Bedarfsstelle der KZVWL ist für die Laufzeit, Überwachung, Änderungen oder die Beendigung von Lieferantenverträgen verantwortlich. Falls notwendig, führt das ISMS-Team eine erneute Risikoeinschätzung durch, bevor die Änderungen akzeptiert werden.

5 Sicherheitsmaßnahmen

5.1 Arbeiten durch externe Dienstleister außerhalb des Hauses

Wird Hardware zur Wartung oder Reparatur außer Haus gegeben, sind alle sensitiven Daten, die sich auf Datenträgern befinden, vorher sicher zu löschen. Der Transport von Datenträgern hat sicher zu erfolgen.

5.2 Entzug von Zugangsrechten / Rückgabe von Werten

Bei Beendigung des Auftragsverhältnisses muss eine geregelte Übergabe der Arbeitsergebnisse, Arbeitsmittel (z.B. RFID-Transponder (EMA)) und der erhaltenen Unterlagen in elektronischer oder Papierform und Betriebsmittel erfolgen. Daten, die im Rahmen des Outsourcings extern gespeichert wurden, sind nach Abschluss des Auftrags vollständig und sicher zu löschen.

Es sind außerdem sämtliche eingerichteten Zugangsberechtigungen und Zugriffsrechte im Einklang mit der Richtlinie Zugangsmanagement [4] zu entziehen bzw. zu löschen.

Außerdem sind ausscheidende Mitarbeiter explizit darauf hinzuweisen, dass die Verschwiegenheitsverpflichtung auch nach Beendigung der Tätigkeit bestehen bleibt.

6 Mitgeltende Unterlagen

[1] Leitlinie - Informationssicherheit und Datenschutz

[2] Richtlinie - Dokumentenlenkung

[3] Hausordnung - externe Dienstleister

[4] Richtlinie - Zugangsmanagement

7 Dokumenteninformationen

Historie und Status

Status	Anmerkungen	Datum	Version	Durchgeführt von
Entwurf	Initiale Erstellung	02.06.2021	0.1	ISMS-Team
in Bearbeitung	Inhaltliche Anpassung	09.07.2021	0.2	ISMS-Team
in Bearbeitung	Inhaltliche Anpassung	28.07.2021	0.3	ISMS-Team
in Bearbeitung	Inhaltliche Anpassung	08.07.2021	0.4	ISMS-Team
in Bearbeitung	Inhaltliche Anpassung	17.03.2022	0.5	ISMS-Team
in Bearbeitung	Inhaltliche Anpassung	22.03.2022	0.6	ISMS-Team
in Bearbeitung	Inhaltliche Anpassung	02.05.2022	0.7	ISMS-Team
in Bearbeitung	Inhaltliche Anpassung	17.05.2022	0.8	ISMS-Team
in Bearbeitung	Inhaltliche Anpassung	02.05.2022	0.7	ISMS-Team
in Bearbeitung	Inhaltliche Anpassung	06.10.2022	0.8	ISMS-Team
in Bearbeitung	Inhaltliche Anpassung	06.01.2023	0.9	ISMS-Team
in Bearbeitung	Inhaltliche Anpassung	28.02.2023	0.10	ISMS-Team
in Bearbeitung	Inhaltliche Anpassung	12.04.2023	0.11	ISMS-Team
Freigabe	Freigabe durch ISB	09.06.2023	1.0	ISB
in Bearbeitung	Inhaltliche Anpassung 5.3 Bereitstellung von Dokumenten - Text gelöscht 5.6 Überwachung und Überprüfung - Konkretisierung der Vorgaben zur Kontrolle 6 Zutritts-, Zugangs- und Zugriffsrechte externer Mitarbeiter - in Hausordnung überführt 7.2 Externe Arbeiten über Fernzugriff	16.05.2024	1.1	ISMS-Team

	- wurde in die Verfahrensanweisung Fernwartung überführt 7.3 Entzug von Zugangsrechten / Rückgabe von Werten - wurden gelöscht und in die Hausordnung von externen Dienstleistern eingepflegt			
Freigabe	Freigabe durch ISB	16.05.2024	2.0	ISB
in Bearbeitung	1 Dokumenteninformationen - Historie und Status wurde ans Ende des Dokuments verlegt 3 Anwendung auf Normen - Umstellung auf die neuen ISO27001:2022 Corntrols 4.6 Überwachung und Prüfung - Prüfungsvorgaben für Lieferantenklassen ergänzt	07.10.2024	2.1	ISMS-Team
Freigabe	Freigabe durch ISB	05.12.2024	3.0	ISB