Anhang Informationssicherheit
(Umgang mit Informationen der Viega)

Version 1.0
01.10.2023

Inhaltsverzeichnis

Änderungshistorie

Änderungsdatum		alte Version	neue Version	Bearbeitung	Freigabe
17.10.2023		*-*	*1.0*	*M. Kirchmaier*	*B. Heintel*
Kapitel		Änderung			
-	-	Erstellung des Anhangs			

1 Einführung

Dieser Anhang beschreibt die Regelungen in Bezug auf den Umgang mit Daten und Informationen der Viega zur durchgängigen Sicherstellung der Einhaltung aller informationssicherheitsrelevanten Aspekte bei der Beschaffung und beim Einsatz externer Dienstleister.
Um Daten und Informationen umfassend schützen zu können, müssen Lieferanten, externe Dienstleister und Subauftragnehmer mit in die Informationssicherheit einbezogen werden.

2 Geltungsbereich

Die Regelungen in diesem Anhang gelten für alle Personen, die im Lebenszyklus der Auftragnehmer-Auftraggeber-Beziehung mit Daten und Informationen der Viega in Kontakt kommen.
Die weiteren Inhalte der technischen Liefervorschrift bleiben für den Auftragnehmer verpflichtend bestehen bzw. Abweichungen sind durch den jeweiligen Viega Projektleiter freizugeben.

Alle Abweichungen von diesem Anhang sind schriftlich beim Viega Projektleiter bzw. dem CISO (Chief Information Security Officer) der Viega anzufragen. Eine Freigabe der Abweichungen kann nur mit Zustimmung der auftraggebenden Fachabteilung vor Vertragsabschluss erteilt werden. Die Annahme unserer Bestellung schließt die ausdrückliche Anerkennung dieser Liefervorschrift unter Verzicht auf widersprechende, eigene Verkaufsbedingungen ein. Sie ergänzen die jeweils gültigen Allgemeinen Einkaufsbedingungen von Viega.

Bei Weitergabe von Aufträgen an Unterlieferanten ist der Auftragnehmer dafür verantwortlich, dass dieser Anhang eingehalten wird.

3 Daten und Informationen

In der Welt der Informationssicherheit sind Daten und Informationen zwei verschiedene Konzepte, die jedoch eng miteinander verbunden sind.

Daten: Daten sind rohe, unstrukturierte Fakten oder Zeichen, die noch keine Bedeutung haben. Sie sind die grundlegenden Einheiten von Informationen und können in verschiedenen Formen vorliegen, wie z.B. als Text, Zahlen, Bildern oder Tönen. Daten allein haben keinen Kontext und keine spezifische Bedeutung.

Informationen: Informationen entstehen, wenn Daten in einen Kontext gesetzt und interpretiert werden. Informationen sind Daten, die organisiert, verarbeitet oder strukturiert wurden, um eine bestimmte Bedeutung zu haben oder einen Nutzen zu bieten. Sie sind für Entscheidungen relevant und helfen den Menschen, ein Verständnis für eine spezifische Situation zu entwickeln.

Sowohl Daten als auch Informationen liegen in unterschiedlichen Formen vor. In der Regel werden sie jedoch elektronisch oder in Papierform ausgetauscht.

Es ist wichtig sicherzustellen, dass sowohl Daten als auch Informationen angemessen geschützt werden. Hierzu legt Viega großen Wert auf Integrität, Verfügbarkeit und Vertraulichkeit der ausgetauschten Daten. Dies kann bedeuten, den Zugriff auf sensible Daten zu beschränken, Verschlüsselungstechnologien anzuwenden, regelmäßige Sicherheitsüberprüfungen durchzuführen und sicherzustellen, dass Informationen nur autorisierten Personen zugänglich sind, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten und Informationen zu gewährleisten.

4 Informationsklassen

Viega klassifiziert alle Informationen entsprechend ihres Schutzbedarfs hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität.

Es ist die Aufgabe jedes Viega Mitarbeiters dazu beizutragen, dass Informationen gemäß ihrer Klassifizierung verwendet und Verstöße dagegen dem Informationseigentümer und in gravierenden Fällen dem CISO gemeldet werden. Dieses Prinzip gilt auch im Lieferantenverhältnis.

Informationen innerhalb der Viega Gruppe werden entsprechend ihrer Anforderungen in vier Schutzklassen eingeteilt. Diese gliedern sich in die Klassen A-D. Personenbezogene Informationen unterliegen dem Datenschutz und müssen daher entsprechend spezifisch behandelt werden.

Klasse	Charakterisierung	Beispiele Unternehmensinformationen
A	**Streng vertrauliche Informationen** und **Geschäftsgeheimnisse**, deren unkontrollierte Veröffentlichung Schaden für den Bestand von Viega bedeuten könnten.	• Strategiepapiere • Innovationsdokumente • Patentanmeldungen • Geschäftsgeheimnisse nach GeschGehG
B	**Vertrauliche Informationen**, die nur für eine Gruppe von Mitarbeitern, z. B. eine Abteilung, bestimmt sind und deren Veröffentlichung Schaden für den Betrieb von Viega bedeuten könnten.	• Produktions- und Versandinformationen • Merkmale neuer Produkte vor dem Vertrieb • Verträge von besonderer Bedeutung • Aufträge • Transaktionsdaten • Konstruktionszeichnungen
C	**Interne Informationen**, die für die Mitarbeiter oder Vertragspartner des Unternehmens bestimmt sind und deren Veröffentlichung keinen Schaden für den Geschäftsbetrieb von Viega bedeutet.	• Rechnungen, Gutschriften • Projektportfolio • Prozessbeschreibungen • Meeting-Protokolle • Hausmitteilungen • Intranet Inhalte (falls nicht anders klassifiziert)
D	**Informationen**, die für Kunden und die interessierte Öffentlichkeit erstellt und entsprechend veröffentlicht wurden und **uneingeschränkt** weitergegeben werden dürfen.	• Internetauftritte • Social-Media Content • Broschüren, Prospekte • Präsentationen für Messen und Veranstaltungen

Die Kennzeichnung der Schutzklasse erfolgt unabhängig von der Klassifizierung. Dies erfolgt über den Aufdruck der **Vertraulichkeitsklasse** („uneingeschränkt“, „intern“, „vertraulich“, „streng vertraulich“) auf jeder Seite des Dokuments.

Zulässig sind ebenso die englischen Bezeichnungen „unrestricted“, „internal“, „confidential“ und „strictly confidential“.

5 Umgang mit Informationen

Je nach Schutzklasse einer Information gelten bei Viega unterschiedliche Regelungen zum Umgang. Dabei wird unterschieden, wie diese Informationen gebraucht, gedruckt, übertragen, gespeichert und vernichtet werden müssen.

5.1 Schutzklasse A (Streng vertraulich)

allgemeiner Umgang	*Streng vertraulich* klassifizierte Informationen sind für den Gebrauch von benannten Personen bestimmt. Es ist darauf zu achten, dass diese Informationen nie unverschlossen und unbeaufsichtigt herumliegen. Eine Weitergabe an Externe ist nur mit gültiger Geheimhaltungsvereinbarung (Non-Disclosure-Agreement, NDA) zulässig. Es wird empfohlen, die Weitergabe zu dokumentieren.
Ausdruck/Vervielfältigung	Unbeaufsichtigtes Drucken und Kopieren von *streng vertraulichen* Informationen ist nicht gestattet. Ausdrucke, Originale und Kopien dürfen nach dem Druck nicht im Drucker verbleiben. Die Drucker-Option „Vertraulicher Druck“ muss verwendet werden.
Datenübertragung	Vom Postversand ist nach Möglichkeit abzusehen. Sollte keine andere Möglichkeit bestehen, ist darauf zu achten, dass ein konkreter Empfänger angegeben ist und die Zustellung per Einschreiben erfolgt. Dazu ist in der ersten Adresszeile die Zustellanweisung „Einschreiben Eigenhändig“ anzugeben. Der Empfänger hat darauf zu achten, dass die Sendung unversehrt bei ihm ankommt. Andernfalls ist der CISO der Viega zu benachrichtigen. Eine elektronische Übermittlung ist nur verschlüsselt gestattet. Ausnahmen sind durch den CISO der Viega zu genehmigen.
Lagerung/Speicherung	Um *streng vertrauliche* Informationen entsprechend zu schützen ist eine Aufbewahrung nur in abgeschlossenen Büros, Archiven, Safes oder verschlossenen Schränken erlaubt. Rollcontainer sind nicht ausreichend gesichert und somit nicht zur Aufbewahrung von *streng vertraulichen* Informationen geeignet. Werden *streng vertrauliche* Informationen außerhalb der Viega-Rechenzentren gespeichert, so sind die Daten zu verschlüsseln. Zusätzlich muss die Zugangsberechtigung mit Single Sign-On oder einer Multi-Faktor-Authentifizierung überprüft werden.
Entsorgung	Die Entsorgung erfolgt durch Schreddern.
Vernichtung/Löschung	Das Vernichten erfolgt über mehrfaches Überschreiben oder physische Vernichtung des Datenträgers.

5.2 Schutzklasse B (Vertraulich)

allgemeiner Umgang	*Vertraulich* klassifizierte Informationen sind für den Gebrauch innerhalb einer definierten Gruppe (Abteilung, Fachbereich, Projektteam, etc.) bestimmt. Über die Weitergabe an Externe entscheidet der Informationseigentümer. Eine Weitergabe an Externe ist nur mit gültiger Geheimhaltungsvereinbarung (Non-Disclosure-Agreement, NDA) zulässig.
Ausdruck/Vervielfältigung	Unbeaufsichtigtes Drucken und Kopieren von *vertraulichen* Informationen ist zu vermeiden. Ausdrucke, Originale und Kopien dürfen nach dem Druck nicht im Drucker verbleiben. Nach Möglichkeit ist von der Drucker-Option „Vertraulicher Druck“ Gebrauch zu machen.
Datenübertragung	Beim Versand per Post ist darauf zu achten, dass ein konkreter Empfänger angegeben ist, in der ersten Adresszeile ist zusätzlich die Zustellanweisung „persönlich / personal“ anzugeben. Der Empfänger hat darauf zu achten, dass die Sendung unversehrt bei ihm ankommt. Andernfalls ist der CISO der Viega zu benachrichtigen. Eine elektronische Übermittlung ist nur verschlüsselt gestattet. Ausnahmen sind durch den CISO der Viega zu genehmigen.
Lagerung/Speicherung	*Vertrauliche* Informationen müssen nach Arbeitsende verschlossen aufbewahrt werden. Die Archivierung muss in einem verschlossenen und gesicherten Raum erfolgen. Werden *vertrauliche* Informationen außerhalb der Viega-Rechenzentren gespeichert, so sind die Daten zu verschlüsseln. Zusätzlich muss die Zugangsberechtigung mit Single Sign-On oder einer Multi-Faktor-Authentifizierung überprüft werden.
Entsorgung	Die Entsorgung erfolgt durch Schreddern.
Vernichtung/Löschung	Das Vernichten erfolgt über mehrfaches Überschreiben.

Für den Zugang zu Informationen der Schutzklassen A (streng vertraulich) und B (vertraulich) gilt das „Need-to-Know“-Prinzip, d. h. der Informationseigentümer hat Sorge dafür zu tragen, dass der Zugang zu diesen Informationen in dem Maße berechtigt wird, wie es für die Erfüllung der Arbeit erforderlich ist. Daraus folgt, dass Informationen, die eingesehen werden können, auch eingesehen werden dürfen. Im Zweifel ist der CISO der Viega zu informieren.

5.3 Schutzklasse C (Intern)

allgemeiner Umgang	*Intern* klassifizierte Informationen sind für den Gebrauch innerhalb Projektgruppe bestimmt. Die Weitergabe an Kollegen und an an Projekten beteiligte Externe ist gestattet
Ausdruck/Vervielfältigung	Das Ausdrucken und Kopieren von *internen* Informationen ist grundsätzlich gestattet. Gedruckte Dokumente und Kopien sollten zeitnah aus den Druckern entnommen werden.
Datenübertragung	Bei der Datenübertragung sind keine besonderen Sicherheitsmaßnahmen vorgeschrieben. Verschlüsselung sollte jedoch dort eingesetzt werden, wo dies möglich ist.
Lagerung/Speicherung	*Interne* Informationen sollten an Arbeitsplätzen nach Arbeitsende verschlossen aufbewahrt werden. Die Speicherung darf nur auf freigegeben Speichermedien, Netzlaufwerken und Webseiten erfolgen. Werden personenbezogene Informationen der Klasse C außerhalb der Viega-Rechenzentren gespeichert, so sollten die Daten verschlüsselt werden. Zusätzlich muss die Zugangsberechtigung mit Single Sign-On oder einer Multi-Faktor-Authentifizierung überprüft werden.
Entsorgung	Die Entsorgung darf über den Papierkorb erfolgen; das Schreddern wird empfohlen.
Vernichtung/Löschung	Das Vernichten erfolgt über einfaches Löschen.

5.4 Schutzklasse D (Uneingeschränkt)

allgemeiner Umgang	*Uneingeschränkte* Informationen unterliegen keinerlei Restriktionen im Umgang. Sie dürfen und sollen unter Beachtung der gesetzlichen Regelungen genutzt und verbreitet werden.
Ausdruck/Vervielfältigung	Das Ausdrucken und Kopieren von *uneingeschränkten* Informationen ist grundsätzlich gestattet.
Datenübertragung	Bei der Datenübertragung sind keine besonderen Sicherheitsmaßnahmen vorgeschrieben.
Lagerung/Speicherung	Es gibt keine Anforderungen an die Lagerung oder Speicherung.
Entsorgung	Die Entsorgung erfolgt über den Papierkorb.
Vernichtung/Löschung	Das Vernichten erfolgt durch (einfaches) Löschen.

6 Herausgabe und Rückführung von Daten und Informationen

Bei Beendigung der Vertragsbeziehung sind alle hierfür im Vertrag definierten Maßnahmen zu erfüllen. Der Auftragnehmer ist für die ordnungsmäßige Umsetzung verantwortlich und liefert zur Kontrolle entsprechende Nachweise.

Der Auftragnehmer verpflichtet sich, alle Daten und Informationen der Viega, die im Besitz des Auftragnehmers sind, nach Beendigung des Vertragsverhältnisses herauszugeben.

Der Auftragnehmer gewährleistet, dass alle übergebenen Daten im Übergabeprozess sicher und vertraulich behandelt werden und nur autorisiertem Personal zugänglich sind.

Der Auftragnehmer verpflichtet sich, alle übergebenen Daten sicher und endgültig zurückzuführen.

Die Rückführung der Daten umfasst die sichere Löschung oder Vernichtung aller elektronischen und physischen Datenträger, auf denen die Daten gespeichert sind, so dass eine Wiederherstellung der Daten unmöglich ist. Der Auftraggeber kann anstelle der Herausgabe/Rückführung auch die Vernichtung der Daten und Informationen verlangen.

Der Auftragnehmer stellt dem Auftraggeber eine schriftliche Bestätigung über die ordnungsgemäße Rückführung der Daten zur Verfügung.

7 Sensibilisierung von Mitarbeitern

Der Auftragnehmer stellt sicher, dass alle Mitarbeiter, die mit Daten und Informationen der Viega in Berührung kommen, über diesen Anhang informiert sind und über eine ausreichende Schulung im Umgang mit Daten und Informationen je Schutzklasse verfügen.

8 Überprüfung der Informationssicherheit beim Partner

Der Auftragnehmer erklärt sich bereit, dem Auftraggeber Zugang zu seinen technischen und organisatorischen Maßnahmen zu gewähren. Dies gilt vor allem bei Daten und Informationen der Schutzklassen „A“ und „B“.

Der Auftraggeber behält sich das Recht vor, Überprüfungen der Informationssicherheitsmaßnahmen des Auftragnehmers durchzuführen. Diese Überprüfungen sollen sicherstellen, dass der Auftragnehmer angemessene technische, organisatorische und physische Sicherheitsvorkehrungen getroffen hat, um die Vertraulichkeit, Integrität und Verfügbarkeit der Daten des Auftraggebers zu gewährleisten.

Die Kontrollen können, sofern erforderlich, Aspekte wie Zugangskontrolle, Verschlüsselung, Datensicherung, Incident-Response-Pläne und Schulungen der Mitarbeiter umfassen. Der Auftragnehmer verpflichtet sich, alle relevanten Informationen und Unterlagen bereitzustellen, die für die Durchführung dieser Kontrollen erforderlich sind. Diese Überprüfungen können in regelmäßigen Abständen oder nach Bedarf erfolgen.

Nach jeder Überprüfung wird der Auftragnehmer dem Auftraggeber einen Bericht über die Ergebnisse der Kontrollen vorlegen. Sollten während der Kontrollen Schwachstellen identifiziert werden, verpflichtet sich der Auftragnehmer, angemessene Maßnahmen zu ergreifen, um diese Schwachstellen zu beheben und die Informationssicherheit zu verbessern. Der Auftraggeber kann angemessene Fristen für die Umsetzung dieser Maßnahmen festlegen und hat das Recht, die Wirksamkeit dieser Maßnahmen erneut zu überprüfen.

Beide Parteien stimmen zu, dass alle Informationen, die während der Informationssicherheitskontrollen offengelegt werden, vertraulich behandelt werden. Weder der Auftraggeber noch der Auftragnehmer dürfen ohne die vorherige schriftliche Zustimmung der anderen Partei vertrauliche Informationen offenlegen oder für andere Zwecke als die Durchführung der Kontrollen verwenden.