Informationssicherheit

Richtlinie für Dienstleister und Lieferanten

Verfasser	Leitung IMS - Michael Liebl
Datum	13.12.2023
Revision	1.0
Dateiname	Informationssicherheit Dienstleister_Lieferant.docx
Freigabe	ISB
Datum	13.12.2023
Klassifizierung	öffentlich
Änderung	Initiale Version / Erstellung
Verteilung	-ELO -Homepage
Nächste geplante Überarbeitung	jährlich

PROWIN A+W GmbH AUTOMATIONSTECHNIK

Inhaltsverzeichnis

1 Änderungshistorie

Version	Erstellt am	Erstellt von	Freigabe am	Freigabe von	Änderung
1.0	13.12.2023	M. Liebl	14.12.2023	ISB	Initiale Version / Erstellung

2 Einleitung

Die PROWIN A+W Automationstechnik GmbH (im folgendem PROWIN A+W genannt) sieht den Betrieb eines Informationssicherheitsmanagementsystems (ISMS) als wichtigen Faktor zur Gewährleistung der Informationssicherheit innerhalb des Unternehmens.

Mit der Umsetzung der erarbeiteten Elemente trägt die Leitung ihrer freiwilligen Verpflichtung zur Etablierung eines Informationssicherheitssystems Rechnung und legt den Grundstein zu einem umfassenden Informationssicherheitsbewusstsein im Unternehmen.

Zur Einhaltung der notwendigen Informationssicherheitsstandards innerhalb der PROWIN A+W vereinbaren die Parteien in Ergänzung zu den allgemeinen Einkaufsbedingungen und Geschäftsbedingungen die hier folgenden Anforderungen an den Auftragnehmer zur Informationssicherheit.

3 Anwendungsbereich

Diese Richtlinie ist gültig für Auftragnehmer der PROWIN A+W, Standort Jahrdorf, die im Rahmen eines Vertragsverhältnisses Zutritt zu Gebäuden oder Räumlichkeiten, Zugang und/oder Zugriff auf elektronische Informationen oder Informationssysteme der PROWIN A+W erhalten.

Der Auftragnehmer sorgt innerhalb seines Unternehmens für die Bekanntmachung dieser Sicherheitsrichtlinie. Die Regelungen dieser Vereinbarung sind auch für Subunternehmer des Auftragnehmers bindend.

4 Zielsetzung

Die Informationssicherheitsrichtlinie für Dienstleister und Lieferanten dient dazu, die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen zu gewährleisten, die im Rahmen unserer geschäftlichen Beziehungen mit externen Partnern geteilt werden. Diese Richtlinie legt die Erwartungen und Anforderungen an Dienstleister und Lieferanten fest, um sicherzustellen, dass die Sicherheitsstandards und -praktiken unserer Organisation eingehalten werden.

5 Vertraulichkeit der Informationen

Dienstleister und Lieferanten verpflichten sich, alle Informationen, die im Rahmen ihrer Tätigkeiten für unser Unternehmen zugänglich sind, als vertraulich zu behandeln.

Informationen dürfen nur für den vorgesehenen Zweck verwendet werden und dürfen nicht ohne schriftliche Genehmigung unseres Unternehmens an Dritte weitergegeben werden.
Jegliche Übermittlung vertraulicher Informationen muss sicher erfolgen, unter Verwendung angemessener Verschlüsselungs- und Authentifizierungsmethoden.

6 Sicherheitsstandards

Dienstleister und Lieferanten müssen angemessene Sicherheitsvorkehrungen treffen, um die Integrität, Verfügbarkeit und Vertraulichkeit der übertragenen, verarbeiteten oder gespeicherten Informationen zu gewährleisten.
Es müssen angemessene technische und organisatorische Maßnahmen getroffen werden, um Informationen vor unbefugtem Zugriff, Veränderung, Zerstörung oder Offenlegung zu schützen.

7 Compliance

Dienstleister und Lieferanten müssen alle relevanten Gesetze, Vorschriften und branchenspezifischen Standards im Hinblick auf Informationssicherheit einhalten.
Die Einhaltung von Sicherheitsrichtlinien und -verfahren muss regelmäßig überprüft und dokumentiert werden.

8 Meldung von Sicherheitsvorfällen

Dienstleister und Lieferanten sind verpflichtet, jeden Sicherheitsvorfall, der die Informationen unseres Unternehmens betreffen könnte, unverzüglich zu melden.
Eine detaillierte Untersuchung und Berichterstattung über Sicherheitsvorfälle ist erforderlich, um geeignete Maßnahmen zur Behebung und Verhinderung zukünftiger Vorfälle zu ergreifen.

Definition Sicherheitsereignis: Ein erkanntes Auftreten eines Zustands eines Systems, Dienstes oder Netzwerks, der eine mögliche Verletzung der Informationssicherheitspolitik oder die Unwirksamkeit von Maßnahmen oder eine vorher nicht bekannte Situation, die sicherheitsrelevant sein kann, anzeigt.

Definition Sicherheitsvorfall: Als Sicherheitsvorfall wird ein Ereignis bezeichnet, dass die Vertraulichkeit, Verfügbarkeit oder Integrität der Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme, IT-Ausstattung oder IT-Anwendungen mit hohem oder sehr hohem Schutzbedarf derart beeinträchtigt, dass ein Schaden für das Unternehmen, Kunden oder Geschäftspartner entstehen kann.

9 Schulung und Sensibilisierung

Dienstleister und Lieferanten müssen sicherstellen, dass ihre Mitarbeiter angemessen geschult und sensibilisiert sind, um sicherheitsrelevante Praktiken zu verstehen und einzuhalten.

10 Audit und Überprüfung

Unser Unternehmen behält sich das Recht vor, Sicherheitsaudits und Überprüfungen bei Dienstleistern und Lieferanten durchzuführen, um die Einhaltung dieser Richtlinie sicherzustellen.
Dienstleister und Lieferanten sind verpflichtet, bei solchen Audits uneingeschränkte Zusammenarbeit zu gewährleisten.

11 Vertragsbeziehungen

Sicherheitsanforderungen müssen in Verträgen und Vereinbarungen mit Dienstleistern und Lieferanten ausdrücklich festgelegt werden.
Verstöße gegen diese Richtlinie können zu Vertragsstrafen oder zur Beendigung der Geschäftsbeziehung führen.

12 Aktualisierung der Richtlinie

Diese Richtlinie wird regelmäßig überprüft und bei Bedarf aktualisiert. Dienstleister und Lieferanten werden über Änderungen informiert.
Die Einhaltung dieser Richtlinie ist für alle Dienstleister und Lieferanten verbindlich. Bei Nichteinhaltung können rechtliche Schritte und die Beendigung der Geschäftsbeziehung eingeleitet werden.

13 Inkrafttreten

Diese Richtlinie tritt zum 01.01.2024 in Kraft.

Genehmigt durch:	Geschäftsführung
Ort/Datum:	Jahrdorf, 15.12.2023