



ISL_00D_GF_

Informationssicherheitspolitik

– extern –

Das Urheberrecht hat die aLIVE-Service GmbH (im Folgenden: aLIVE). Ihr stehen ausschließlich sämtliche Verwertungsrechte zu. Jede Haftung wird ausgeschlossen.

aLIVE-Service GmbH
Gustav-Ricker-Str. 62
39120 Magdeburg

Telefon: 0391-99978-5200
Web: alive-service.de
E-Mail: info@alive-service.de

Sitz der Gesellschaft: Magdeburg
Eingetragen beim Amtsgericht Stendal HRB 19225

Inhaltsverzeichnis

1	Verantwortung	3
2	Geltungsbereich.....	3
3	Normative Referenzen	3
4	Zweck.....	3
5	Sicherheitsziele.....	3
6	Grundsätze.....	4

1 Verantwortung

Die Geschäftsführung von aLIVE sieht Informationssicherheit als entscheidend für die Dienstleistungsprozesse an. Es ist Teil der Firmenphilosophie, firmeninterne Informationssicherheitsrichtlinien einzuhalten. Alle Mitarbeitenden müssen diese Notwendigkeit verstehen, um ihre täglichen Aufgaben entsprechend auszuführen. Die Geschäftsführung unterstützt Strukturen und Prozesse für Informationssicherheit und überprüft regelmäßig deren Wirksamkeit zur fortlaufenden Verbesserung.

2 Geltungsbereich

Die Regelungen gelten für alle Mitarbeitenden der aLIVE.

3 Normative Referenzen

Die Grundlage für diese Richtlinie bildet die ISO/IEC 27001:2017 (im Folgenden: ISO 27001):

- 5.1 Führung und Verpflichtung
- 5.2 Politik
- A.5.1 Informationssicherheitsrichtlinien

sowie den zugehörigen Dokumenten in der jeweils gültigen Version.

4 Zweck

Als Dienstleistungsunternehmen hat aLIVE täglich Zugang zu sensiblen Kundeninformationen. Die Informationssicherheitspolitik legt die Grundprinzipien fest, um die Sicherheit und Integrität dieser Daten zu gewährleisten.

5 Sicherheitsziele

- Sicherung der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Daten der aLIVE und ihrer Geschäftspartner.
- Transparente Absicherung der Dienstleistungsprozesse durch eine etablierte Sicherheitsorganisation.
- Erkennung und Begrenzung von Informationssicherheitsrisiken auf ein akzeptables Niveau.
- Prävention von Reputations- oder finanziellen Schäden durch den Verlust von Daten oder Informationen.
- Bereitstellung von Nachweisen zur Sicherheit der Organisation gegenüber Kunden, Gesetzgebern, Partnern, Versicherungen und Lieferanten.

6 Grundsätze

- Die aLIVE dokumentiert und zeigt ihren Schutz der Vertraulichkeit und Integrität von Kundendaten in einer leicht nachvollziehbaren Weise für Kunden.
- Regelmäßige Schulungen zu Datenschutz und Informationssicherheit für Mitarbeitende werden durchgeführt.
- Daten und Informationen werden entsprechend ihrer Klassifizierung behandelt.
- Es existiert ein Risikomanagementsystem, um Risiken für Daten und Informationen zu erkennen und zu begrenzen.
- Ein Notfallmanagementsystem dient dazu, die Verfügbarkeit von Daten und Informationen im Notfall schnell wiederherzustellen.
- System- und Anwendungsänderungen werden über einen definierten Change-Management-Prozess kontrolliert, der Datenschutz- und Informationssicherheitsaspekte berücksichtigt.
- Ein Berechtigungskonzept regelt den Zugriff auf Daten entsprechend den Arbeitsanforderungen.
- Die Infrastruktur wird auf dem neuesten Stand der Technik betrieben.
- Interne Audits gewährleisten die Umsetzung von Datenschutz- und Informationssicherheitsrichtlinien, decken Schwachstellen auf und identifizieren Verbesserungsmöglichkeiten.