



dbeyond at+

Leitlinie

Informationssicherheit

2 Inhaltsverzeichnis

1 LENKUNGSDATEN	2
2 INHALTSVERZEICHNIS	3
3 LEITLINIE FÜR INFORMATIONSSICHERHEIT	4
3.1 ZWECK.....	4
3.2 GELTUNGSBEREICH	4
3.3 GRUNDSATZ	4
3.4 STELLENWERT DER INFORMATIONSSICHERHEIT	4
3.5 EINLEITUNG.....	5
3.6 ZIELE DES INFORMATIONSSICHERHEITSMANAGEMENTSYSTEMS	5
3.7 DEFINITION DER INFORMATIONSSICHERHEIT.....	5
3.8 RAHMENWERK FÜR DIE INFORMATIONSSICHERHEITSPOLITIK	6
3.9 ROLLEN UND ZUSTÄNDIGKEITEN IM BEREICH DER INFORMATIONSSICHERHEIT	7
3.10 ÜBERWACHUNG	7
3.11 RECHTLICHE UND REGULATORISCHE VERPFLICHTUNGEN.....	7
3.12 SCHULUNG UND SENSIBILISIERUNG.....	7
3.13 KONTINUIERLICHE VERBESSERUNG DES MANAGEMENTSYSTEMS.....	7
3.14 VERSTÖßE GEGEN DIESE RICHTLINIE	7

3 Leitlinie für Informationssicherheit

3.1 Zweck

Die vorliegende Informationssicherheitsrichtlinien legt die für die Organisation dbeyond at+ gmbh geltenden Vorgaben zum Schutz der Vertraulichkeit, der Integrität und der Verfügbarkeit von Daten fest.

3.2 Geltungsbereich

Diese Informationssicherheitsrichtlinie gilt für alle Mitarbeiter Auftragnehmer und Partnerunternehmen, die Zugriff auf die IT-Systeme, Daten und Informationen der dbeyond at+ gmbh haben. Alle Mitarbeiter haben diese Richtlinie zu beachten und einzuhalten. Diese Leitlinie kann auch externen interessierten Parteien zur Verfügung gestellt werden.

3.3 Grundsatz

Die Vorgaben und Handlungen zur Gewährleistung der Informationssicherheit werden auf der Grundlage von Risikomanagement, gesetzlichen und behördlichen Anforderungen sowie geschäftlichen Erfordernissen festgelegt und nachgehalten.

3.4 Stellenwert der Informationssicherheit

„Die sichere und verantwortungsvolle Verarbeitung von Informationen ist für den Erfolg unseres Unternehmens von zentraler Bedeutung. Deshalb hat der Schutz unserer Informationen höchste Priorität. Wir verpflichten uns, die Grundwerte der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – in all unseren Geschäftsprozessen zu gewährleisten:

- **Vertraulichkeit:** Wir schützen sämtliche Informationen vor unbefugtem Zugriff und stellen sicher, dass sensible Daten ausschließlich autorisierten Personen zugänglich sind.
- **Integrität:** Wir sorgen dafür, dass unsere Informationen vollständig und korrekt bleiben und vor unbefugter Veränderung oder Manipulation geschützt sind.
- **Verfügbarkeit:** Wir stellen sicher, dass Informationen und IT-Systeme jederzeit für berechtigte Nutzer zugänglich und nutzbar sind, wenn sie benötigt werden.

Unabhängig davon, ob es sich um Mitarbeiter-, Kunden- oder Geschäftsdaten handelt, nehmen wir unsere gesetzlichen Verpflichtungen – insbesondere im Rahmen der DSGVO und des Data Protection Act 2018 – sehr ernst. Wir stellen die notwendigen Ressourcen bereit, um ein angemessenes Informationssicherheitsmanagementsystem zu entwickeln, umzusetzen und kontinuierlich zu verbessern.“

Dr. Markus Junginger, 14.07.2025

3.5 Einleitung

Die Informationssicherheit schützt die Informationen, die uns anvertraut werden. Wenn wir bei der Informationssicherheit Fehler machen, kann das erhebliche negative Auswirkungen auf unsere Mitarbeiter, unsere Kunden, unseren Ruf und unsere Finanzen haben.

3.6 Ziele des Informationssicherheitsmanagementsystems

Mit der Implementierung des Informationssicherheitsmanagementsystems verfolgt die dbeyond at+ folgende Ziele:

- Gewährleistung der Einhaltung der gesetzlichen, behördlichen und vertraglichen Verpflichtungen
- Gewährleistung einer hohen Verlässlichkeit des Handelns, auch in Bezug auf den Umgang mit Informationen (Verfügbarkeit, Integrität, Vertraulichkeit) und der Aufrechterhaltung der Kernprozesse der Organisation
- Gewährleistung des Schutzes von personenbezogenen Daten im Sinne der Datenschutz-Grundverordnung
- Sicherung der hohen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen

Die Organisation strebt an, sich durch die konsequente Umsetzung ihrer Informationssicherheitsziele als vertrauenswürdiges und verantwortungsbewusstes Unternehmen zu etablieren, um somit das Vertrauen unserer Kunden an die Organisation zu stärken und somit eine langfristige Kundenzufriedenheit und -bindung zu schaffen.

3.7 Definition der Informationssicherheit

Informationssicherheit dient der Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen.

Vertraulichkeit	Der Zugang zu Informationen ist nur für Personen mit entsprechender Autorität. Die richtigen Personen mit dem richtigen Zugriff
Integrität	Die Informationen sind vollständig und korrekt. zu den richtigen Daten
Verfügbarkeit	Informationen sind verfügbar, wenn sie benötigt werden. zum richtigen Zeitpunkt.

3.8 Rahmenwerk für die Informationssicherheitspolitik

Das Informationssicherheitsmanagementsystem stützt sich auf ein Rahmenwerk an Informationssicherheitsrichtlinien. In Verbindung mit dieser Richtlinie bilden die folgenden Richtlinien die vollständige Informationssicherheitsrichtlinie:

- DP 01 Leitlinie für Datenschutz
- DP 02 Datenaufbewahrungsrichtlinie
- DP 03 Datenlöschkonzept
- IS 01 Leitlinie für Informationssicherheit (diese Richtlinie)
- IS 02 Richtlinie für Zugriffskontrollen
- IS 03 Asset Management Richtlinie
- IS 04 Risikomanagement Richtlinie
- IS 05 Informationsklassifizierungs und -handhabungs-Richtlinie
- IS 06 Informationssicherheits- und Datenschutz-Schulungsrichtlinie
- IS 07 Richtlinie der akzeptablen Verwendung
- IS 08 Clear Desk and Clear Screen Richtlinie
- IS 09 Richtlinie für mobiles Arbeiten
- IS 10 Richtlinie für Notfallmanagement
- IS 11 Backup-Richtlinie
- IS 12 Richtlinie zum Schutz vor Schadsoftware
- IS 13 Richtlinie zum Änderungsmanagement
- IS 14 Richtlinie zur Sicherheit von Drittparteien
- IS 15 Richtlinie zur kontinuierlichen Verbesserung
- IS 16 Richtlinie für Protokollierung und Überwachung
- IS 17 Richtlinie für Netzwerksicherheit
- IS 18 Richtlinie zum Informationsaustausch
- IS 19 Richtlinie für sichere Entwicklung
- IS 20 Richtlinie für physische Sicherheit und Umgebungssicherheit
- IS 21 Richtlinie für die Verwaltung kryptografischer Schlüssel
- IS 22 Richtlinie für kryptografische Kontrolle und Verschlüsselung
- IS 23 Richtlinie zur Dokumentierung und Aufzeichnung
- IS 24 Richtlinie für Sicherheitsvorfallmanagement
- IS 25 Richtlinie für Patch Management
- IS 26 Richtlinie für Cloud-Dienste
- IS 27 Richtlinie für geistige Eigentumsrechte
- IS 28 Richtlinie für Personalsicherheit

3.9 Rollen und Zuständigkeiten im Bereich der Informationssicherheit

Im Rahmen der Informationssicherheit ist es die Aufgabe von jedem, diese Richtlinien zu verstehen und zu befolgen, die Prozesse einzuhalten und vermutete oder tatsächliche Verstöße zu melden.

Spezifische Rollen und Verantwortlichkeiten für den Betrieb des Informationssicherheitsmanagementsystems sind definiert und in dem Dokument „Zugewiesene Informationssicherheits-Rollen & Verantwortlichkeiten“ festgehalten.

3.10 Überwachung

Die Einhaltung der Richtlinien und Verfahren des Informationssicherheits-Managementystems wird durch das Management sowie durch unabhängige Überprüfungen durch interne und externe Audits in regelmäßigen Abständen überwacht.

3.11 Rechtliche und regulatorische Verpflichtungen

Die Organisation nimmt ihre rechtlichen und behördlichen Verpflichtungen ernst und führt diese Anforderungen in einem Kataster für rechtliche und vertragliche Anforderungen.

3.12 Schulung und Sensibilisierung

Die Richtlinien werden allen Mitarbeitern und Drittnutzern leicht und einfach zugänglich gemacht.

Im Zuge eines Schulungskonzeptes wird definiert, welche Richtlinien, Verfahren und Konzepte der Informationssicherheit vermittelt werden müssen. Im Zuge dessen wird auch der Schulungsbedarf ermittelt.

3.13 Kontinuierliche Verbesserung des Managementsystems

Das Informationssicherheitsmanagementsystem wird kontinuierlich verbessert. Der Ansatz zur kontinuierlichen Verbesserung findet sich in die Richtlinie für kontinuierliche Verbesserung und der kontinuierliche Verbesserungsprozess findet statt.

3.14 Verstöße gegen diese Richtlinie

Verstöße gegen diese Leitlinie sowie Richtlinien der Informationssicherheit können zu erheblichen negativen Konsequenzen für dbeyond at+ führen. Deshalb ist bei vorsätzlichen und grob fahrlässigen Handlungen, die einen Verstoß darstellen, mit arbeitsrechtlichen Konsequenzen zu rechnen. Darüber hinaus können derartige Zuwiderhandlungen auch straf-oder zivilrechtliche Schritte nach sich ziehen.