5.1 u. 5.2 Informationssicherheitspolitik

Last updated by | Lisa-Maria Brucker Blumatix | 10. Sep. 2025 at 16:02 MESZ

Zweck und Geltungsbereich

Mit dem vorliegenden Dokument wird die Informationssicherheitsrichtlinie der Blumatix Intelligence GmbH („Blumatix") im geltenden Anwendungsbereich beschrieben.

Die Richtlinie stellt eine klare Richtungsvorgabe und Unterstützung durch die Geschäftsführung der Blumatix dar und gibt, in Übereinstimmung mit Geschäftsanforderungen sowie geltenden Gesetzen und Regelungen, einen Rahmen zur Erreichung der Informationssicherheitsziele vor.

Der Anwendungsbereich des Informationssicherheits-Managementsystems (ISMS) umfasst sämtliche Hard- und Softwarekomponenten sowie Schnittstellen, welche für die Entwicklung und Bereitstellung des Capture Services BLU DELTA erforderlich sind. Diese Details sind im Kapitel 4.3 Festlegen des Anwendungsbereichs des ISMS nachzulesen.

Die Einhaltung dieser Richtlinie gilt für alle Mitarbeiter/innen der Blumatix unabhängig von ihrer Rolle und Stellung sowie für alle externen Berater, Lieferanten und Servicepartner.

Ziele

Die Geschäftsführung von Blumatix engagiert sich explizit für die Informationssicherheit. Alle Mitarbeiter/innen und relevanten externen Parteien werden regelmäßig und nachhaltig hinsichtlich der Wahrung der Informationssicherheit sensibilisiert.

Die Informationsverarbeitung nimmt eine wesentliche Rolle in der Erfüllung der Kundenanforderungen ein. Strategische und operative Funktionen werden maßgeblich durch Informations- und Kommunikationstechnologie unterstützt.

Informationssicherheit bedeutet für Blumatix, dass folgende Grundwerte sichergestellt werden:

- **Vertraulichkeit**: Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in zulässiger Weise zugänglich sein.
- **Integrität**: Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.
- **Verfügbarkeit**: Dienstleistungen, Funktionen der IT-Systeme, -Anwendungen oder -Netze sollen von den Anwendern stets wie vorgesehen genutzt werden können.

Die Sicherheitsziele der Blumatix werden in folgender Tabelle übersichtlich dargestellt:

Nr.	Sicherheitsziel	Beschreibung des Ziels
1	Bewusstsein und Sensibilisierung der Mitarbeiter	Erhöhung des Sicherheitsbewusstseins bei allen Beschäftigten und relevanten externen Parteien.
2	Sicherstellung der Informationssicherheit nach CIA	Gewährleistung der Grundwerte Vertraulichkeit, Integrität, Verfügbarkeit aller informationsverarbeitenden Systeme und Prozesse.
3	Risikomanagement und Minimierung der Risiken	Regelmäßige Identifikation und Minimierung von Informationssicherheitsrisiken durch proaktives Management.
4	Schutz der Integrität und Vertraulichkeit gemäß Gesetz und Kundenanforderungen	Einhaltung gesetzlicher Vorgaben und spezifischer Kundenanforderungen hinsichtlich Integrität und Vertraulichkeit.
5	Sicherstellung des Datenschutzes bei personenbezogenen Daten	Uneingeschränkte Einhaltung der Anforderungen des Datenschutzes.
6	Kontrolle des Informationszugriffs und Schutz der Infrastruktur	Umsetzung eines wirksamen Berechtigungskonzepts und Schutzmaßnahmen für IT-Infrastruktur und Räumlichkeiten.
7	Erfüllung der Normanforderungen nach ISO 27001 und Empfehlungen nach ISO 27002	Aufbau, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung des ISMS nach ISO-Standards.

Sicherheitsstrategie

Zur Erreichung der Informationssicherheitsziele und der kontinuierlichen Verbesserung des Sicherheitsniveaus orientiert sich Blumatix an den Normen ISO 27001 und ISO 27002. Das ISMS wird entsprechend diesen Normen aufgebaut, implementiert, aufrechterhalten und stetig verbessert. Blumatix verfolgt dabei einen fortlaufenden Prozess der Risikominimierung und sensibilisiert alle Beteiligten regelmäßig für Informationssicherheit.

Verantwortungen

Führungskräfte und Mitarbeiter/innen tragen gemeinsam Verantwortung für ein angemessenes Sicherheitsniveau. Es wird erwartet, dass erkannte Sicherheitsprobleme proaktiv gemeldet werden und jeder aktiv zur Verbesserung des Sicherheitsniveaus beiträgt. Trainingsmaßnahmen werden regelmäßig durchgeführt, um das Sicherheitsbewusstsein zu fördern.

Verstöße gegen diese und ergänzende Richtlinien werden konsequent geahndet.

Verpflichtung zur Bereitstellung von Ressourcen

Die Geschäftsführung verpflichtet sich, alle erforderlichen Ressourcen (Personal, Ausstattung, Räumlichkeiten, Zeit) zur Verfügung zu stellen, um das ISMS aufrechtzuerhalten und kontinuierlich weiterzuentwickeln.

Inkraftsetzung und Kommunikation

Die vorliegende Informationssicherheitspolitik tritt mit Bekanntgabe durch die Geschäftsführung in Kraft und ist verbindlich für alle Mitarbeiter/innen und externe Parteien. Sie ist öffentlich im ISMS-Wiki abrufbar.

Überprüfung der Richtlinie

Diese Richtlinie wird regelmäßig, mindestens jedoch bis zum 30. Juni 2026, überprüft und aktualisiert.

RACI

- **R:** Kurt Berthold
- **A:** Martin Loiperdinger
- **C:** –
- **I:** Alle Mitarbeiter/innen und interessierte Parteien der Blumatix

Klassifizierung und Zugriff

Dieses intern erstellte Dokument ist öffentlich und im ISMS-Wiki abrufbar.

Überprüfung der Richtlinie

Die nächste Überprüfung diese Richtlinie durch den Informationssicherheitsbeauftragten findet bis zum 30.6.2026 statt.

Martin Loiperdinger

Blumatix Intelligence GmbH
Schwarzstrasse 48 / A-5020 Salzburg
+43 662 243410
office@blumatix.com
www.blumatix.com