ISMS bei Blumatix

Richtlinie zur Informationssicherheit

Kurt Berthold V1.0 21.06.2022

Ziele

Mit dem vorliegenden Dokument wird die Informationssicherheitsrichtlinie der Blumatix Intelligence GmbH („Blumatix“) im geltenden Anwendungsbereich (siehe Dokument: 43_D_ISMS_Anwendungsbereich des ISMS_13072021_bertkur_vertraulich.docx) beschrieben.

Die Richtlinie ist die klare Richtungsvorgabe und Unterstützung durch die Geschäftsführung der Blumatix und gibt, in Übereinstimmung mit den Geschäftsanforderungen sowie geltenden Gesetzen und Regelungen, einen Ansatz zur Bewältigung der Informationssicherheitsziele vor.

Die Geschäftsführung der Blumatix bekennt und engagiert sich für die Informationssicherheit durch die Bekanntmachung bei den Beschäftigten sowie relevanten externen Parteien und Aufrechterhaltung dieser Richtlinie.

Unternehmen und Geschäftszweck

Das Kerngeschäft der Blumatix mit Firmensitz in Schwarzstraße 48, 5020 Salzburg ist die Software-Entwicklung auf Basis von künstlicher Intelligenz („KI“). Konkret ist das Thema der Blumatix die automatische Dokumentenverarbeitung. Mittels KI-Technologie bietet Blumatix einen Dienst mit dem Namen BLU DELTA an, der Unternehmen den Schritt von einer semi-automatisierten hin zu einer vollkommen autonomen Dokumentenverarbeitung ermöglicht. Sofort und unmittelbar liest BLU DELTA ähnlich wie ein Mensch ein Bild, PDF oder Scan und extrahiert dabei die nötigen Daten für die weiteren Verarbeitungen. Die am häufigsten verwendete Dokumentenkategorie sind derzeit Eingangsrechnungen, welche in unterschiedlichen Formen vorliegen.

Die Kunden der Blumatix sind Unternehmen, die ihre internen Prozesse im Kontext von Dokumenten automatisieren wollen. Es handelt sich hierbei ausschließlich im B2B Kunden, für welche die Themen Datensicherheit und Datenschutz immer wichtiger werden.

Die Informationsverarbeitung stellt die wesentliche Schlüsselrolle für die Erfüllung der Kundenanforderungen dar. Alle wesentlichen strategischen und operativen Funktionen unserer Dienste werden durch Informations- und Kommunikationstechnik maßgeblich unterstützt.

Informationssicherheit bedeutet für uns, dass wir in allen technischen- und nichttechnischen Systemen, welche wir für die Informationsverarbeitung einsetzen die folgenden Grundwerte sicherstellen:

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

Zudem wollen wir durch die Vorgabe und Einhaltung entsprechender Maßnahmen den Schutz vor Gefahren bzw. Bedrohungen erhöhen und einhergehende Risiken minimieren.

Die Einhaltung der Grundwerte bzw. deren Unterstützung gelten für alle Mitarbeiter/innen der Blumatix im geltenden Anwendungsbereich, unabhängig von ihrer Rolle und Stellung im Unternehmen sowie für alle externen Berater, Lieferanten und Servicepartner.

Sicherheitsziele

Wir bewegen uns in einem hochtechnisierten Umfeld. Um erfolgreich zu sein ist es erforderlich, dass wir uns laufend mit den neuesten Technologien auseinandersetzen. Demgemäß verfolgt Blumatix im Rahmen des Informationssicherheitsmanagements die folgenden Sicherheitsziele:

- Das Image der Blumatix hängt in hohem Maße von der Zuverlässigkeit der ihr übertragenen Aufgabenerfüllung und Vertrauen ihrer Kunden, Mitarbeiter/innen und Partner ab. Vertrauen schafft ein gutes Image und ein gutes Image baut Vertrauen auf. In diesem Sinne ist auf größte Sorgfalt hinsichtlich des bestimmungsgemäßen Gebrauchs der Informationsverarbeitung zu achten, um das Vertrauen und das gute Image aufrecht zu erhalten.
- Informationen und Systeme werden im Hinblick auf ihre Verfügbarkeit so gesichert, dass die zu erwartenden Ausfallzeiten im Rahmen tolerierbarer Grenzen liegen. Ausfallzeiten, welche verhindern, dass Systeme nicht wie vorgesehen genutzt werden können, sollen durch entsprechende Maßnahmen vermieden werden.
- Die Anforderungen an Integrität und Vertraulichkeit orientieren sich an der Gesetzeskonformität und den Anforderungen unserer Kunden und Mitarbeiter/innen sowie Partner.
- Die Anforderungen des Datenschutzes müssen bei der Bearbeitung personenbezogener Daten uneingeschränkt erfüllt werden.
- Sämtliche Maßnahmen der Informationssicherheit müssen in einem sinnvollen wirtschaftlich vertretbaren Verhältnis zum Wert der zu schützenden Informationen stehen. Schadensfälle mit hohen finanziellen oder immateriellen Auswirkungen müssen jedenfalls verhindert werden.
- Der Zugriff auf Informationen muss durch ein Berechtigungskonzept begrenzt werden. So ist auch auf einen angemessenen Schutz der gesamten IT-Infrastruktur und Räumlichkeiten der Blumatix stets zu achten.

Sicherheitsstrategie

Im Hinblick auf die Erreichung der Informationsziele und der kontinuierlichen Verbesserung des Sicherheitsniveaus orientieren wir uns an der ISO 27001 Norm. Zudem werden die Empfehlungen der ISO 27002 Norm beachtet.

Somit haben wir uns verpflichtet, ein Informationssicherheitsmanagementsystem (ISMS) entsprechend den Anforderungen der genannten Normen aufzubauen, zu verwirklichen, aufrechtzuerhalten und fortlaufend zu verbessern.

Wir verstehen die Informationssicherheit als kontinuierlich fortlaufenden Prozess, welcher laufend umgesetzt werden muss und gehen davon aus, dass die schwächsten Glieder im System die wahrscheinlichsten Angriffsziele darstellen. Dahingehend richten wir unsere Risikomanagementprozesse aus, um ein möglichst hohes Sicherheitsniveau zu erreichen. Jede/r kann dazu beitragen, das Sicherheitsniveau zu verbessern. Uns ist bewusst, dass Sicherheit auch von kleinen Handlungen und/oder Entscheidungen abhängen kann.

Der Anwendungsbereich des ISMS enthält sämtliche Hard- und Softwarekomponenten sowie Schnittstellen, welche für die Entwicklung und Bereitstellung des Capture Services BLU DELTA (https://www.bludelta.ai/) erforderlich sind. Es sind dies Module, welche den Kunden der Blumatix zum Zwecke der automatisierten Dokumentenerfassung angeboten werden. Demnach sind konkret alle Bestandteile umfasst, mit welchen den Kunden der Blumatix ein KI-Service zur Verarbeitung von Dokumenten angeboten wird und durch welche dieser Service ermöglicht wird. Die Details zum Anwendungsbereich sind im Dokument

43_D_ISMS_Anwendungsbereich des ISMS_V1.0.0_vertraulich_final.docx

nachzulesen.

HINWEIS: Unsere Informationssicherheitspolitik wird durch weitere themenspezifische Richtlinien unterstützt, die zusätzlich die Umsetzung von Maßnahmen zur Informationssicherheit anordnen. Diese Richtlinien sind so aufgebaut, dass die Bedürfnisse unserer Zielgruppen und für uns sicherheitsrelevante Themen abgedeckt werden.

Verantwortungen

Unsere Geschäftsprozesse und Unternehmenswerte können durch diverse Gefährdungen bedroht werden. Wir identifizieren diese Bedrohungen laufend und bewerten die daraus resultierenden Risiken.

Führungskräfte und Mitarbeiter/innen haben die gemeinsame Verpflichtung, für ein angemessenes Sicherheitsniveau zu sorgen. Jede/r im Unternehmen, unabhängig von Stellung und Aufgabenbereich, trägt die Mitverantwortung für die Informationssicherheit. Es wird erwartet, dass jede/r selbständig und ohne Aufforderung im Falle von erkannten Sicherheitsproblemen aktiv wird.

Zur Aufrechterhaltung und Weiterentwicklung des Sicherheitsbewusstseins werden daher entsprechende Trainingsmaßnahmen umgesetzt. Mitarbeiter/innen und Führungskräfte sind angehalten, an diesen Trainings teilzunehmen und sich aktiv einzubringen.

Alle Mitarbeiter/innen sind verpflichtet, Risiken zu identifizieren und bei der Risikobehandlung mitzuwirken. Ansprechpartner für Verbesserungsvorschläge ist die Geschäftsführung. Alle bestehenden und zukünftigen Vorgaben zur Erreichung der Sicherheitsziele sind zu beachten und umzusetzen.

Vorgehen bei Verstößen

Handlungen, welche

- die Blumatix in Verruf geraten lassen,
- der Blumatix durch eine Verletzung der Sicherheit tatsächlichen oder potenziellen materiellen oder immateriellen Schaden zufügen,
- die Sicherheit der Mitarbeiter/innen, Kunden, Partner oder der Einrichtungen und Systeme sowie der Informationen der Blumatix beeinträchtigen oder
- den unberechtigten Zugriff auf Informationen ermöglichen

gelten als Verstöße gegen die Maßgaben dieser und weiterer Richtlinien.

Derartige und sonstige Verstöße gegen Richtlinien, Verfahrensanweisungen und andere Vorschriften können zu erheblichen negativen Konsequenzen für Blumatix führen. Demnach ist bei vorsätzlichen und grob fahrlässigen Handlungen, die einen Verstoß darstellen, mit arbeitsrechtlichen Konsequenzen zu rechnen. Zudem können derartige Zuwiderhandlungen auch straf- oder zivilrechtliche Schritte zur Folge haben.

Verpflichtung des Managements zur Bereitstellung von Ressourcen für das ISMS

Erforderliche Ressourcen sind im Sinne der Bereitstellung von Personal, Material, Räumlichkeiten, Ausstattung, Schulungen und Zeit zu verstehen.

Die oberste Leitung verpflichtet sich zu Bereitstellung von ausreichenden Ressourcen, um eine ISMS aufzubauen, implementieren und aufrecht zu erhalten.

So wurde zum Beispiel ein eigenes Projektteam gegründet, welches seit Mai 2021 – gemeinsam mit einer externen Beratung – das ISMS aufgebaut und im Unternehmen implementiert hat.

Hinsichtlich der Aufrechterhaltung und Zertifizierung wurde mit der Österreichischen Computergesellschaft ein Zertifizierungsvertrag über 3 Jahre abgeschlossen.

Geltungsbereich des Dokuments

Anwendungsbereich des ISMS der Blumatix; somit für alle Mitarbeiter/innen und Auftragnehmer der Blumatix sowie sonstige externe Dritte, die Einrichtungen oder Informationen der Blumatix nutzen.

Inkraftsetzung und Kommunikation

Die Freigabe dieses Dokuments erfolgt durch den Informationssicherheitsbeauftragten, die Inkraftsetzung durch die Geschäftsführung der Blumatix als oberste Leitung. Dieses Dokument tritt nach Bekanntgabe in Kraft, gilt in der jeweils aktuellen veröffentlichten Form und ist verpflichtend anzuwenden.

RACI

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

Klassifizierung und Zugriff

Dieses intern erstellte Dokument ist öffentlich und unter „5.1_5.2_Informationssicherheitspolitik_V1.0.5_public_final.docx“ am Sharepoint abrufbar.

Überprüfung der Richtlinie

Die nächste Überprüfung diese Richtlinie durch den Informationssicherheitsbeauftragten findet am 30.6.2023 statt.

Versionen

Version #	Datum	Autor	Änderung
0.1	04.08.2021	Berthold	Dokument erstellt
1.0.0	11.08.2021	Loiperdinger	Dokument freigegeben

Version #	Datum	Autor	Änderung
1.0.1	09.05.2022	Loiperdinger	Dokument umbenannt in 5.1_5.2_Informationssicherheitspolitik_V1.0.1_öffentlich_final.docx Das ist die aktuell gültige Version mit 09.05.2022
1.0.2	14.06.2022	Berthold	Dokument nach Stage I Audit überarbeitet
1.0.3	21.06.2022	Loiperdinger	Dokument inhaltlich geprüft
1.0.4	21.06.2022	Loiperdinger	Dokument freigegeben
1.0.5	21.06.2022	Loiperdinger	Dokument von „öffentlich“ auf „public“ umbenannt und erneut freigegeben.

Salzburg, 04.07.2022 Blumatix Intelligence GmbH, Martin Loiperdinger, Geschäftsführung