ISMS at Blumatix

Information Security Policy

Kurt Berthold V1.0 21.06.2022

Goals

This document describes the Information Security Policy of Blumatix Intelligence GmbH ("Blumatix") within its applicable scope (refer to document: 43_D_ISMS_Scope of the ISMS_13072021_confidential.docx). The policy serves as a clear directive and support from the management of Blumatix, providing an approach to address information security objectives in accordance with business requirements, as well as applicable laws and regulations. The management of Blumatix acknowledges and commits to information security by communicating this policy to employees and relevant external parties and maintaining its enforcement.

Company and Business Purpose

The core business of Blumatix, headquartered at Schwarzstraße 48, 5020 Salzburg, is software development based on artificial intelligence (AI). Specifically, Blumatix focuses on automatic document processing. Using AI technology, Blumatix offers a service called BLU DELTA, which enables companies to transition from semi-automated to fully autonomous document processing. BLU DELTA reads images, PDFs, or scans similar to a human and extracts the necessary data for further processing. Currently, the most commonly processed document category is incoming invoices, which come in various formats.

Blumatix's customers are businesses seeking to automate their internal processes in the context of document management. These are exclusively B2B customers for whom data security and privacy are becoming increasingly important.

Information processing plays a key role in meeting customer requirements. All significant strategic and operational functions of our services are significantly supported by information and communication technology.

For us, information security means ensuring the following core values in all technical and non-technical systems used for information processing:

• **Confidentiality**: Protecting against unauthorized disclosure of information. Confidential data and information should only be accessible to authorized individuals in an appropriate manner.

• **Integrity**: Ensuring the correctness (integrity) of data and the proper functioning of systems.

• **Availability**: Ensuring that services, functions of IT systems, applications, or networks are available and can be used by users as intended.

Furthermore, we aim to increase protection against hazards and threats and minimize associated risks by implementing and adhering to appropriate measures. Compliance with these core values and their support applies to all employees of Blumatix within the applicable scope, regardless of their role and position within the company. This also extends to external consultants, suppliers, and service partners.

Security Objectives

We operate in a highly technological environment, and to be successful, it is necessary for us to constantly stay updated with the latest technologies. Accordingly, Blumatix pursues the following security objectives within the framework of information security management:

• The image of Blumatix relies heavily on the reliability of fulfilling assigned tasks and the trust of its customers, employees, and partners. Trust builds a good image, and a good image fosters trust. In this regard, utmost care must be taken regarding the proper use of information processing to maintain trust and a positive image.

• Information and systems are secured to ensure their availability within acceptable limits of expected downtime. Measures should be implemented to avoid downtime that prevents systems from being used as intended.

• The requirements for integrity and confidentiality align with legal compliance and the expectations of our customers, employees, and partners.

• The requirements of data protection must be fully met when processing personal data.

• All information security measures must be economically reasonable in relation to the value of the information being protected. Incidents with significant financial or non-financial impacts must be prevented.

• Access to information must be restricted through an authorization concept. Adequate protection of the entire IT infrastructure and premises of Blumatix should always be ensured.

Security Strategy

In order to achieve the information objectives and continuously improve the level of security, Blumatix follows the ISO 27001 standard and considers the recommendations of the ISO 27002 standard. As such, the company is committed to establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS) in accordance with the requirements of these standards.

Blumatix views information security as an ongoing and continuous process that requires constant implementation. The organization recognizes that the weakest links in the system are likely to be the most vulnerable targets for attacks. Therefore, risk management processes are aligned to achieve a high level of security. Everyone within the organization has a role to play in improving the level of security. Blumatix understands that even small actions and decisions can impact security.

By adopting the ISO 27001 and ISO 27002 standards and embracing a proactive and risk-based approach to information security, Blumatix aims to effectively manage security risks, protect sensitive information, and continuously enhance the overall security posture of the organization.

Blumatix Intelligence GmbH
Schwarzstraße 48
5020 Salzburg
Tel: +43 662 243410
Mail: office@blumatix.com

The scope of the ISMS includes all hardware and software components, as well as interfaces, required for the development and provision of the Capture Service BLU DELTA (https://www.bludelta.ai/). These modules are offered to Blumatix customers for automated document processing. Specifically, it encompasses all components necessary to offer customers a AI-powered document processing service and enable the functionality of this service. Further details regarding the scope can be found in the document "43_D_ISMS_Application Scope of the ISMS_V1.0.0_confidential_final.docx".

NOTE: Our information security policy is supported by additional topic-specific guidelines that mandate the implementation of security measures. These guidelines are designed to address the needs of our target audience and cover security-relevant topics for us.

Responsibilities

Blumatix acknowledges that our business processes and organizational values can be threatened by various risks. We continuously identify and assess these threats to evaluate the associated risks.

Both management and employees share the responsibility for maintaining an appropriate level of security. Every individual within the company, regardless of their position or role, is accountable for information security. It is expected that individuals take proactive action in addressing identified security issues without waiting for explicit instructions.

To foster and enhance security awareness, relevant training measures are implemented. Employees and managers are encouraged to participate in these training sessions and actively contribute to them.

All employees are obligated to identify risks and contribute to their treatment. The management team serves as the point of contact for suggestions for improvement. It is imperative to comply with all existing and future guidelines aimed at achieving the security objectives.

By emphasizing shared responsibility, promoting security awareness, and fostering a proactive approach to risk management, Blumatix aims to ensure the ongoing protection and improvement of information security throughout the organization.

Procedure for Violations

Actions, which

- tarnish the reputation of Blumatix,
- cause actual or potential material or immaterial harm to Blumatix through a security breach,
- compromise the safety of employees, customers, partners, or the facilities and systems, as well as the information of Blumatix, or
- enable unauthorized access to information,

are considered violations of the provisions of this and other policies.

Such violations of policies, procedures, and other regulations can have significant negative consequences for Blumatix. Therefore, intentional and grossly negligent actions that constitute a violation may result in employment-related consequences. Additionally, such misconduct may also lead to criminal or civil legal actions being taken.

Management's obligation to provide resources for the ISMS

The necessary resources are understood in terms of providing personnel, materials, facilities, equipment, training, and time. The top management is committed to providing adequate resources to establish, implement, and maintain an ISMS. For example, a dedicated project team was established, which, together with external consultants, has been building and implementing the ISMS within the company since May 2021. In terms of maintenance and certification, a certification contract with the Austrian Computer Society has been concluded for a period of 3 years.

Scope of the document

The scope of the ISMS of Blumatix includes all employees and contractors of Blumatix, as well as other external parties who use Blumatix's facilities or information.

Enforcement and Communication

This document is approved by the Information Security Officer and will be enforced by the top management of Blumatix. It takes effect upon announcement and is applicable in its current published form. It must be followed and adhered to by all relevant parties.

RACI

R Kurt Berthold
A: Martin Loiperdinger
C: Martin Loiperdinger
I: All employees and interested parties of Blumatix are required to comply with this document.

Classification and Access

This internally created document is publicly available and can be accessed on the SharePoint under "5.1_5.2_Informationssicherheitspolitik_V1.0.5_public_final.docx".Überprüfung der Richtlinie

The next review of this policy by the Information Security Officer is scheduled for June 30, 2023.

Versions

Version #	date	Author	changes
0.1	04.08.2021	Berthold	document created
1.0.0	11.08.2021	Loiperdinger	document released
1.0.1	09.05.2022	Loiperdinger	Document renamed to 5.1_5.2_Information Security Policy_V1.0.1_public_final.docx This is the currently valid version as 9th of May, 2022
1.0.2	14.06.2022	Berthold	Document revised after Stage I Audit
1.0.3	21.06.2022	Loiperdinger	document content checked
1.0.4	21.06.2022	Loiperdinger	document released
1.0.5	21.06.2022	Loiperdinger	Document renamed from "öffentlich" to "public" and shared again.

Salzburg, 04.07.2022 Blumatix Intelligence GmbH, Martin Loiperdinger, CEO