Information Security Policy

Introduction

At SAFETY IO, we are enthusiastic and committed about privacy and security as a matter of company culture. We deeply care about strict confidentiality, information security, and full compliance with all applicable privacy and data protection laws, in particular the GDPR. As part of this commitment, we decided to establish an Information Security Management System (ISMS) to govern customer data processing with high security standards that are in accordance with applicable laws and our commitment level to our customers.

Our management team has overall accountability and responsibility for information security and fully supports the information security objectives formulated in this policy and the concepts and measures derived and to be derived from it.

Furthermore, the management team encourages employees to stay abreast of SAFETY IO policies, potential threats, and their specific responsibilities by completing training programs on a regular basis. SAFETY IO's dedicated Security team owns the Information Security Management System and is responsible for reporting any issues and improvements to the management team.

References

- ISO/IEC 27001:2013 standard:
  - 5.2 Information security policy
  - 6.2 Information security objectives and planning to achieve them
- ISMS Manual

Policy Scope

This policy applies to all SAFETY IO employees, contractors, vendors and agents who have access to, possession of, or control of SAFETY IO's business information and technology assets, including access to SAFETY IO's network, cloud platform, communication systems, information systems, computing systems, workstations, mobile devices or other data access/storage devices.

SAFETY IO-owned or managed information includes, but is not limited to, data and/or information in any form, format, or on any type of media, including information processing, transfer, sharing, communications (verbal and written) and storage.

This policy addresses all aspects of information security including confidentiality, integrity, availability and privacy. The management team strongly supports the policy and scope and can be held accountable for its adoption and effectiveness across SAFETY IO.

All employees of SAFETY IO receive training on the information security management system and their duties to contribute to its effectiveness, focused on the policies, privacy and overall information security. Specialized staff receive training tailored for their respective roles and responsibilities. Therefore, all employees understand and support all of the relevant aspects of information security, privacy and availability.

As used in this Policy, "SAFETY IO" or "Company" refers to the Safety io GmbH within the scope of the ISMS.

Information Security Objectives

Objective 1: Customer trust and protection
Protect customer information in order to satisfy customer expectations and comply with relevant data privacy regulations, laws and contracts.

Objective 2: Availability and resilience of infrastructure
Ensure the availability and resilience of SAFETY IO´s infrastructure and assets providing customer services.

Objective 3: **Security culture**
Constantly educate all our employees about information security, the ISMS, and their role in protecting SAFETY IO and our customers.

Objective 4: Establishing ISMS in compliance with ISO 27001:2013
The ISMS complies with the ISO 27001:2013 standard and is regularly reviewed and continuously improved.

Information Security Organization

The Managing Director is the executive sponsor for information security and SAFETY IO´s Information Security Management System.

Managing Director and SAFETY IO Management Team are accountable for delivering services that meet customer needs and are in line with the information security objectives highlighted in this policy. They are also responsible for allocating appropriate resources for SAFETY IO to achieve these objectives, and for delegating the responsibility of implementing the ISMS to the Security Team.

The Security Team coordinates all activities related to implementation, operation and optimization of the ISMS in a way that supports SAFETY IO's business goals. The Security Team is responsible for delivering capabilities for all applicable security domains to support the security objectives in this policy.

The Security Team consists of the Operations Manager, the Security Specialist and a dedicated DevOps Engineer.

Roles and Responsibilities

Roles and responsibilities around SAFETY IO ISMS are defined in the ISMS Manual.

Information Security Management System

SAFETY IO has established and will maintain an Information Security Management System (ISMS) according to the above-mentioned information security objectives. SAFETY IO's business processes shall be organized, conducted, and controlled as part of the ISMS that effectively helps to reduce information security related risks.

Information security objectives will continue to be aligned with SAFETY IO's business goals and the ISMS is intended to be an enabling mechanism for information sharing, for electronic operations, Software as a Service and for reducing information-related risks to acceptable levels.

SAFETY IO's ISMS shall be developed to comply with the ISO/IEC 27001:2013 standard.

Implementation and Monitoring

The Security Team is responsible for the implementation of this Information Security Policy. The Security Team monitors the implementation of ISMS requirements to ensure uniform procedures and the fulfillment of the information security objectives.

Continuous Improvement

The effectiveness and efficiency of the ISMS will be regularly reviewed and evaluated. Furthermore, corrective measures will be identified, implemented, and verified to continuously improve the ISMS.

Policy Compliance

Noncompliance or violations of this policy, or its derived regulations, may lead to disciplinary measures.

Publication

This Information Security Policy and all its changes will be communicated throughout the company, so that the principles and values of this policy are understood and lived by every employee and interested parties.

Document Owner and Approval

The Security Specialist is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

This procedure was approved by the Managing Director and is issued on a version-controlled basis under his/her approval.

Berlin, 28 January 2021

_____

Managing Director