POL Information security policy

Company name	Zefi
Effective date	09/07/2025

Version history

Version	Date	Description	Author	Approved by
1	09/07/2025	-- N/D --	Alexandros Fokianos	Aurora Maggio

Purpose

The purpose of this policy is to declare and communicate Top Management's commitment to protecting the organization's information assets. This document defines the framework for establishing, implementing, maintaining, and continually improving the Information Security Management System (ISMS), with the aim of protecting the confidentiality, integrity, and availability of information and supporting the company's strategic objectives.

Table of contents

Field of Application

This policy outlines the framework and principles for managing information security at Zefi. It is designed to protect the confidentiality, integrity, and availability of all information assets, including customer data and the company's proprietary AI-powered platform. This document applies to all personnel, processes, information systems, and assets managed by or on behalf of Zefi.

Regulatory References

- ISO/IEC 27001:2022
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation - GDPR)

Terms and Definitions

- **Information Security** : The preservation of confidentiality, integrity, and availability of information.
- **Confidentiality** : The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity** : The property of accuracy and completeness of information.
- **Availability** : The property of being accessible and usable on demand by an authorized entity.

Roles and Responsibilities

- **Amministratore Unico** : The Sole Director holds ultimate responsibility for information security, including the approval of this policy and related subject-specific policies, ensuring that security objectives are established and met, and overseeing the implementation of security rules and controls.
- **Dipendente** : The Employee is responsible for adhering to all information security policies and procedures, using company assets in an acceptable manner, and promptly reporting any observed or suspected security events, weaknesses, or threats.
- **Fornitore** : The Supplier or Contractor is responsible for complying with Zefi's information security requirements as stipulated in their agreements, protecting any company information they access, and reporting any security incidents through the designated channels.

Information Security Objectives

Zefi is committed to protecting the confidentiality, integrity, and availability of its information assets, including data processed for its customers and the AI-powered platform itself. The information security objectives are established to support the company's strategic direction and to manage risks effectively.

The **Amministratore Unico** shall ensure that the following strategic objectives for information security are pursued:

- **Ensure Data Confidentiality** : To protect customer data and all sensitive company information from unauthorized access, ensuring that access is granted strictly on a need-to-know basis.
- **Maintain Information Integrity** : To safeguard the accuracy and completeness of information and processing methods, ensuring that the insights provided by the Zefi platform are reliable and based on unaltered data.
- **Guarantee Service Availability** : To ensure that the Zefi platform and associated information assets are accessible and usable when required by authorized personnel and clients, in line with service-level agreements.
- **Achieve and Maintain Compliance** : To comply with all applicable legal, statutory, regulatory, and contractual requirements related to information security, particularly concerning customer data from European and international clients.
- **Foster a Security-Aware Culture** : To promote a culture of security throughout the organization, ensuring that all personnel understand their security responsibilities.
- **Manage Security Incidents** : To ensure that information security events are detected, reported, and responded to in a timely and effective manner to minimize business impact.

These objectives shall be documented, monitored, and measured as defined in the "PRO Objectives and planning for their achievement" procedure. The **Amministratore Unico** shall review the objectives at planned intervals, as part of the activities described in the "PRO Management Review Process," to ensure their continued suitability and alignment with the company's context.

Fundamental Information Security Principles

Policy Framework

This policy establishes the management direction for information security in alignment with business requirements and relevant laws and regulations. It serves as the foundation for a comprehensive suite of subject-specific policies and procedures that collectively form the Information Security Management System (ISMS).

- The **Amministratore Unico** shall approve this policy and all subject-specific policies.
- All policies shall be published and communicated to all personnel (**Dipendente** , **Fornitore** , **Amministratore Unico**) and relevant external parties in accordance with the "PRO Documented information management procedure".

- All personnel are required to acknowledge their understanding of and agreement to comply with the information security policies, as managed through the "PRO Human resources management procedure".
- This policy and all associated policies shall be reviewed at least annually, or when significant changes occur, to ensure their ongoing suitability, adequacy, and effectiveness. This review is a formal part of the "PRO Management Review Process".
- Specific information security roles and responsibilities are assigned and documented in the "POL Information security roles and responsibilities policy".

Acceptable Use of Resources

All of Zefi's information, information systems, and associated resources are critical assets and shall be used in an ethical, secure, and acceptable manner.

- The rules for the acceptable use of information and associated resources are identified and implemented to protect Zefi's assets. These rules are further detailed in the "POL Operational security policy" and the "Code of conduct".
- Access to information and systems shall be granted based on the principle of least privilege and business need. The allocation and use of access rights are managed according to the "PRO Logical access control management procedure" and recorded in the "Register of users authorized to use the information".
- The **Amministratore Unico** is responsible for ensuring that rules for the acceptable use of resources are defined, documented, and implemented.

Shared Responsibility and Event Reporting

Information security is the responsibility of every member of the organization. All personnel have a duty to protect the information assets to which they have access.

- All personnel, including employees (**Dipendente**), contractors (**Fornitore**), and management (**Amministratore Unico**), shall immediately report any observed or suspected information security events, weaknesses, or threats.
- Reporting shall be performed through the official channels established in the "PRO Information security incident management procedure".
- All reported events shall be assessed and managed according to the "PRO Information security incident management procedure", with significant incidents recorded in the "MOD Log of information security incidents".

Protection of Workspaces and Assets

Zefi shall implement rules to reduce the risks of unauthorized access, loss, and damage to information and assets in workspaces and when used off-site.

- **Clear Desk** : Personnel shall ensure that sensitive or classified paper documents and removable storage media are not left unattended at their desks or in public areas. Such assets must be secured in appropriate locked storage when not in use, as detailed in the "PRO Physical and environmental security procedure".

- **Clear Screen** : All workstations and mobile devices must be secured when unattended.
  - Devices shall be configured to automatically lock the screen. The display must turn off after 2 minutes of inactivity when on battery power and after 5 minutes when connected to a power adapter.
  - A password shall be required immediately to unlock the device after the screen saver begins or the display is turned off.
- **Security of Off-site Assets** : Assets used outside of Zefi's premises, including during remote work or travel, must be protected with the same level of security as on-site assets. The **Amministratore Unico** shall ensure that appropriate security measures are implemented to protect off-site assets from unauthorized access, loss, or damage, as specified in the "POL Operational security policy".

Archiving and Updates

This document is managed as part of the Information Security Management System (ISMS). It shall be reviewed at least annually, or upon the occurrence of significant changes to the organization's context or risk landscape, to ensure its continued suitability and effectiveness. All updates and versions are archived in accordance with the "PRO Documented information management procedure".

Reference Documents

- PRO Objectives and planning for their achievement
- PRO Management Review Process
- PRO Documented information management procedure
- PRO Human resources management procedure
- POL Information security roles and responsibilities policy
- POL Operational security policy
- Code of conduct
- PRO Logical access control management procedure
- Register of users authorized to use the information
- PRO Information security incident management procedure
- MOD Log of information security incidents
- PRO Physical and environmental security procedure