Information Security Policy

(Public Information (P) – 2025 01)

Hydra iT

Hydra iT ISO

(P)

Information Security Policy

DOCUMENT HISTORY

Version	Creation/Revision	Date	Description of changes	Type of change (major or minor)
1	Luis Boutto	20-01-2025	Initial document	
1	Raquel Gomes	05-12-2025	Translation	
1	Francisco Cancela	09-12-2025	Translation Revision	

DOCUMENT VALIDITY

Approval	Date	Comments
Administration	03-02-2025	

Hydra iT ISO

(P)

Information Security Policy

TABLE OF CONTENTS

Contents

Information Security Policy

1. GOALS

1.1 General Goal

Define a framework to ensure the complete protection of Hydra iT's data and technological resources through the implementation of policies, security controls, and best practices that minimize cybersecurity risks, ensure regulatory compliance, and promote a safe and reliable work environment for all users.

1.2 Specific Goals

- ✓ **Establish access controls and permission management:** Define and enforce access policies based on the principle of least privilege, ensuring that users can only access the information and functionality necessary for their role.
- ✓ **Develop a security incident response plan:** Establish a clear and effective plan for identifying, containing, and mitigating security incidents, as well as for data recovery and service continuity.
- ✓ **Promote cybersecurity training and awareness:** Design ongoing training programs for users, focusing on preventing common threats such as phishing and secure information handling.
- ✓ **Commitment to continuous improvement:** Ensure the effectiveness of information security processes, in accordance with ISO/IEC 27001, promoting data protection and risk management in a sustainable manner.
- ✓ **Comply with applicable rules and regulations:** Align Hydra iT's security policies with legal and regulatory requirements, ensuring compliance and avoiding penalties.
- ✓ **Establish a robust data backup and recovery system:** Implement regular backup procedures and disaster recovery plans to ensure the availability and protection of critical data in the event of incidents.

2. SCOPE

This policy applies to all employees, subcontractors, partners, and any other person who has access to the organization's information systems. It covers all systems, networks, devices, applications, and data that are owned by or under the control of the organization.

3. INFORMATION AND INFORMATION SECURITY

Information is the most valuable asset for organizations. For this reason, Hydra iT assumes responsibility for ensuring that both its data and that of the customers it manages are managed in accordance with the following fundamental principles:

- ✓ **Confidentiality**: Information must be protected against unauthorized access. Only authorized people should have access to information based on their roles and responsibilities.
- ✓ **Integrity**: Data and systems must be accurate and protected against unauthorized or unintentional modification. Information integrity is essential for making reliable decisions.
- ✓ **Availability**: Information and systems must be available to authorized users when needed.

4. INFORMATION SECURITY POLICY

The protection of business partners' information and personal data under Hydra iT's responsibility, in a manner consistent with professional, ethical, legal, regulatory, and contractual requirements, is one of the Company's highest priorities and something that is considered fundamental to its success. The loss or misappropriation of personal information or data can have serious legal, financial, and/or reputational consequences, and Hydra iT is committed to safeguarding the privacy, confidentiality, integrity, and availability of its information or that of its business partners, whether it is in physical, digital, or intellectual form.

5. RESPONSABILITIES

To ensure the effectiveness of the Information Security Management System (ISMS), it is crucial that each level of the organization understands and assumes its specific responsibilities. The following describes the functions and obligations of the various roles, from senior management to employees, ensuring an integrated and consistent approach to protecting information assets.

- ✓ **Management**: Responsible for providing leadership, support, and resources to implement and maintain the ISMS. They must ensure that the policy is reviewed periodically and adjusted as necessary.
- ✓ **Information Security Officer (ISO)**: The ISO is responsible for developing, implementing, maintaining, and managing the ISMS, ensuring compliance with the security policy throughout the organization.
- ✓ **Directors and Team Managers**: Department supervisors or coordinators are responsible for ensuring the effective application of information security policies within their teams. They must monitor compliance with guidelines, promote security training, and report incidents or non-compliance.
- ✓ **Employees and Subcontractors**: All employees and contractors must comply with this policy and associated security procedures. Any violation of the policy must be reported immediately.

All employees, as well as third parties, who may in any way interact with information from partners, employees, and Hydra iT itself, are required to comply with and enforce all information security standards, and must promptly report to the RSI any event that may cause, or has caused, a breach of privacy or information security via email to servicedesk@hydra.pt.

Employees and third parties may be held liable in the event of non-compliance with the information security policies and standards established by Hydra iT.

Information Security Policy

6. MAINTENANCE

The Information Security Policy shall be reviewed whenever necessary and, mandatorily, at least once a year, to ensure that it remains appropriate for Hydra iT and shall be communicated to all employees.