Information Security Policy

Information Security Management System

ISMS_MPO_002-1.6

SORINT.lab S.p.A.
Via Zanica, 17 - 24050 Grassobbio (BG) - Italy | Tel +39 035 697 511 - Fax +39 035 697 590
C.F., N. REG. IMPR. BG 95164770166 | P. IVA 03419770163 - REA BG 376790 | CAP. SOC. € 1.262.500,00 i.v.

DOCUMENT INFORMATION

COPYRIGHT

CONTACTS

COMPANY	NAME	ROLE	EMAIL ADDRESS	PHONE
SORINT.lab	Emilio Tresoldi	CISO	emilio.tresoldi@sorint.com	

DOCUMENT REVIEW

VERSION	DATE	AUTHOR	APPROVED BY	ISSUED BY
1.0	2016/12/19	Emilio Tresoldi	Luca Pedrazzini	Luca Pedrazzini
1.1	2020/09/16	Emilio Tresoldi	Luca Pedrazzini	Luca Pedrazzini
1.2	2021/09/05	Emilio Tresoldi	Luca Pedrazzini	Luca Pedrazzini
1.3	2022/09/12	Emilio Tresoldi	Luca Pedrazzini	Luca Pedrazzini
1.4	12/03/2024	Mario Gandolfi	Luca Pedrazzini	Luca Pedrazzini
1.5	05/06/2024	Mario Gandolfi	Luca Pedrazzini	Luca Pedrazzini
1.6	29/11/2024	Mario Gandolfi	Luca Pedrazzini	Luca Pedrazzini

CHANGE HISTORY RECORD

VERSION	DATE	LAST MODIFIED
1.0	2016/12/19	First Version
1.1	2020/09/16	Update
1.2	2021/09/05	Confirmed
1.3	2022/09/12	Confirmed
1.4	12/03/2024	Update - Scope SORINT
1.5	05/06/2024	Update – email contacts 2.1
1.6	29/11/2024	Update – PCI DSS

REFERRAL DOCUMENTS

VERSION	DATE	DOCUMENT
NA	NA	NA

SUMMARY

1. INTRODUCTION

SORINT.lab recognizes the necessity of ensuring that its business operates smoothly and seamlessly to generate benefit for its customers, shareholders and other stakeholders.

In order to provide a seamless operating performance level, SORINT.lab has implemented an ISMS - Information Security Management System, in line with the International Standard for Information Security, ISO/IEC 27001:2022 and for Payment Card Industry Data Security Standard PCI DSS v4.0.1.

This information security policy is a fundamental part of SORINT.lab's set of checks and balances to ensure that information is protected effectively and to meet obligations to customers, shareholders, employees and suppliers.

Failure to comply with this policy could have a significant effect on the operation of the organization and result in financial loss, as well as an inability to provide critical service to customers. Anyone who violates this policy will be subject to disciplinary actions in accordance with labor laws and collective bargaining agreements. If a criminal offense has been committed further action may be taken.

If you do not understand the implications of this policy you can refer to the appropriate officials within SORINT.lab S.p.a.'s Information Security Management System (ISMS).

1.1. SCOPE

This policy shall apply in conjunction with other policies or procedures to any type of information of SORINT.lab S.p.a and all companies controlled by it henceforth referred to as SORINT, and its customers, to systems that have SORINT as their Owner (including in the cloud), and to all internal and third-party personnel working with the company including compliance with the PCI DSS standard.

1.2. OBJECTIVE

The purpose of the policy, supplemented by other policies and procedures, is to maintain the confidentiality, integrity, and availability of information and supporting systems and to provide clear and consistent instructions for all SORINT Business processes.

It also provides Management, direction and support to implement the Information Management System (ISMS) and ensure that operations and software development comply with the security rules identified by the company.

2. IMPLEMENTATION

It is the responsibility of SORINT management as a whole to ensure implementation and compliance with the requirements of the policy. SORINT's Chief Information Security Officer (CISO) is responsible for ensuring all necessary communications, training, and support to facilitate the implementation and monitoring of compliance with this policy.

Non-compliance or exceptions to this policy will be handled by the CISO and subject to approval, modification or appropriate remedial action plan.

2.1. HELP

For support or assistance, the NGMS can be contacted at the e-mail address: desk@sorint.com or at the wetalk “service_desk” channel. In addition, specific inquiries regarding ISMS procedures and policies can be directed to the CISO at: ciso@sorint.com.

2.2. REFERENCE

The policy can be read along with the High Level System Management policy, the latest version of which is on the corporate portal, along with all other existing policies.

3. INFORMATION SECURITY IN SORINT

Information must be protected from unwanted exposure (Confidentiality), corruption (Integrity), and service failure (Availability) in accordance with appropriate security measures and protection levels.

3.1. General Requirements

To ensure adequate protection of information assets Sorint defines the following:

- All business processes identify and classify information in terms of Confidentiality, Integrity, Availability.

- Sorint or its customers' information shall be processed and stored only by SORINT or authorized services.

- Information is processed and reviewed in compliance with legal, contractual and classification requirements.

- Information security requirements are defined in all projects, initiatives and software developments.

- Recruitment ensures that resources meet security requirements.

- Information security is a contractual requirement for all internal and third-party personnel.

- Possible risks associated with working with third parties are analyzed and appropriately managed.

- Installation, distribution and use of software is regulated by policies and procedures and subject to approval.

- Network connections are under policy regulation and subject to approval.

- Logical access to SORINT systems is tracked and regulated through access policy.

- Physical access to SORINT assets is restricted and regulated in accordance with asset classification requirements.

- Data backups are performed at a frequency appropriate to the data classification and are defined in the backup policy.

- SORINT's systems are operated and maintained in accordance with vendor recommendations.

SORINT resources shall not be used for inappropriate activities that are considered illegal, unethical, or that may be offensive.

3.2. Test and Development System

Software development processes must, in order to be efficient and effective:

- Ensure key security requirements related to software development

- Ensure that the resources involved in the development process are properly trained to conduct testing

- Ensure security requirements at all stages of the process (development, pre-production, production)

- Ensure "code ownership" and "intellectual property rights”

3.3. Responsibilities of Sorint Management

All levels of SORINT management must ensure that information security management is among their goals. All SORINT managers encourage staff to report vulnerabilities and critical issues.

3.4. RESPONSIBILITIES OF EMPLOYEES

SORINT expects all personnel to ensure the protection of information and to use the tools properly and securely. Failure to do so negatively affects company business and the achievement of targeted goals.

All employees and third parties are responsible for the confidentiality of Sorint and Sorint's customers' information that they handle and ensure its security:

- Complying with policies and procedures

- Properly implementing operating procedures

- Using only software approved by management

- Changing their passwords periodically and storing them securely

- Ensuring that terminals are locked when you are away from workstations

- Ensuring proper protection of tools outside the workplace

- Using email, social media and public networks in a professional manner

- Disposing of files and documentation appropriately according to defined rules and steps.

- By taking appropriate precautions against malware received via e-mail or any other media

- By not circumventing security controls and allowing for any checks required by those tasked with ensuring security

- Reporting through the appropriate channels information regarding security vulnerabilities or unlawful behavior by personnel.

4. RISK MANAGEMENT

All processes and areas of SORINT are subject to periodic assessment and timely risk management. Areas with a high risk are submitted to the Information Security Committee for analysis by the CISO (chief information security officer)

5. INFORMATION SECURITY REVIEW

A periodic review of the assets where information is held is conducted in a timely manner to determine the presence of any non-conformities or vulnerabilities. Management is responsible for the proper review and audit of assets.

6. PREVENTION, INVESTIGATION AND REPORTING

All office managers are responsible for preventing Security Incidents and reporting any violations of Policy and Procedures.

7. TRAINING RELATED TO INFORMATION SECURITY

Appropriate training related to the Information Security Management System is planned for all employees both at the time of hiring and throughout their carreer at Sorint to ensure that everyone understands security risks and the need to have preventative measures.

8. DOCUMENTATION REVIEW AND ISSUE

This security policy is formally issued by the Chief Information Security Officer (CISO) on behalf of SORINT's Executive Board.

The policy and the Security Information Management System (ISMS) are subject to regular review, at least once every 12 months, updates, and improvements resulting from changes in internal and external threats, business, and feedback from the ISMS.

The CISO ensures timely circulation of policies using communication tools available within the company, as well as training material. The latest versions of policies, procedures and operational guides can be found in the Information Security Management System area on the CLANn corporate portal.

9. RELATIONSHIP WITH OTHER POLICIES

The security policy is the basis for establishing other more detailed information security policies and procedures.

The complete set of documentation about Information Security can be found on the Clann corporate portal in the Information Security Systems area.