POLICY ON THE INFORMATION SECURITY MANAGEMENT SYSTEM

Company Mission

Sogin is the State owned company, 100% controlled by the Ministry of Economy and Finance, responsible for closing the fuel cycle, safely maintaining and dismantling Italian nuclear power plants and facilities, and managing radioactive waste (the so-called nuclear order).

Sogin is also tasked with siting, building and managing the National Repository and Technology Park (known as DNPT): a surface environmental infrastructure where all Italian radioactive waste, including that produced by industrial, research and nuclear medicine activities, can be stored safely.

Sogin builds on its experience and professional expertise also abroad, developing services for third parties in the fields of nuclear decommissioning and radioactive waste management

Information Security Management

In pursuing its mission, Sogin considers ensuring the IT security of its technological systems and organisational processes to be a priority. In this regard, it has invested in it as a strategic project and has decided to adopt an Information Security Management System compliant with the ISO/IEC 27001 standard.

The information security policy fosters management's commitment to protecting information through defined objectives, assigned responsibilities and appropriate information security measures, a commitment that is fundamental to the company's success and reputation and helps preserve the trust of the parties involved.

The information security policy is issued by Top Management, disseminated within the organisation and accessible to the relevant parties through internal and external communication channels. It is also periodically reviewed to ensure its suitability, adequacy and effectiveness on an ongoing basis.

Senior Management Commitment

Sogin is committed to complying with information security laws and regulations, minimising the risk of legal or administrative sanctions, significant losses or reputational damage. Furthermore, it is dedicated to meeting the corporate requirements established to ensure the protection and confidentiality of sensitive information.

The organisation also promotes information, training and awareness-raising among all parties involved regarding security requirements and the importance of following company guidelines to protect information. In this context, it recognises the importance of an effective security management system by its suppliers, ensuring that they handle information with the same level of security and care applied internally. For this reason, a rigorous third-party assessment and monitoring process is adopted to ensure compliance with applicable safety standards and regulatory obligations.

Management is committed to supporting, promoting and maintaining an Information Security Management System by providing the necessary resources to effectively implement security measures. It also promotes the continuous improvement of the Information Security Management System and periodically reviews it by assessing its effectiveness and efficiency.

Objectives

Ensuring information security is vital to prevent potential threats, such as cyber attacks or data breaches, which could jeopardise the integrity of the service and the trust of the parties concerned, as well as having potential impacts on public safety.

Sogin's Information Security Management System aims to enable, through the systematic identification, assessment and treatment of risks, the achievement of an adequate level of security in the management of information assets, in terms of:

- Confidentiality: access to information allowed only to authorised persons;
- Integrity: guaranteeing the accuracy and completeness of information and the processes used to handle and process it;
- Availability: accessibility of information, by authorised persons, when they need it;
- Authenticity: guaranteeing the certain attribution of information (non-repudiation);
- Compliance: ensuring that information processing complies with applicable national and supranational regulations.

Proper management of information security also offers a significant advantage, as it enables Sogin to achieve objectives it considers fundamental, namely compliance with laws, company policies and established security procedures, periodic monitoring of information security risks and, consequently, reduced exposure to incidents and security breaches.

In the current technological context, Sogin also aims to promote the responsible and conscious use of artificial intelligence technologies, ensuring that employees understand the potential, limitations and implications of these technologies.

Rome, November 2025

The Chief Executive Officer

Firmato digitalmente da: Gian Luca Artizzu
Organizzazione: SOGIN S.P.A.
Data: 19/11/2025 15:47:40