SECURITY INCIDENT MANAGEMENT

APPROVED BY

PRYSMIAN S.p.A BOARD OF DIRECTORS

June 10, 2025

Code: PO-IT-I&C-SEC002

prysmian

The planet's pathways

TABLE OF CONTENTS

LEADERSHIP MESSAGE

Our strategy is "Connect to Lead". To lead the market with innovation, we must first and foremost protect the ideas and data that fuel it.

This vision is not just a slogan; it is, rather, the daily commitment of all Prysmian's people. The passion for our work, the drive for excellence, and the ability to act as one single, large team are the engine that allows us to connect the world, driving the energy transition and the digital transformation. Every day our dedication builds the foundations for a more sustainable and interconnected future.
In this global landscape, the value of information and the interoperability of systems have grown exponentially. For a manufacturing leader like us, this is not an abstract challenge. It means protecting the ingenuity we put into our products, the efficiency of our factories, and the data that allows us to serve our customers with trust.

This is why security is not the task of a few, but a responsibility that enables growth for all. Adopting secure behaviors is an act of professionalism and a fundamental ingredient of our daily work, essential for continuing to lead our industry successfully.

Massimo Battaini
Prysmian CEO

1. PURPOSE & OBJECTIVE

The purpose of this document is to define the scope, the audience and general principles to manage security incidents that could have impacts on information systems and on the Group's operations. General principles described in this policy must be applied in the related procedures and operating instructions.

This Policy is based upon the standards set by ISO 27001 series, NIST Cyber Security Framework and the applicable laws and regulations, including – but not limited to – the General Data Protection Regulation (GDPR)

2. POLICY OWNER

Information & Cyber Security Function owns this Policy and is responsible for periodically reviewing and updating it to ensure it accurately reflects organizational updates or legal and regulatory changes.

3. APPLICABILITY

This procedure is intended for all Prysmian Group users, including all employees, contractors, suppliers and visitors that are involved in the creation, classification or processing of the Group's Information, each for the specific area of responsibility.

4. YOUR RESPONSIBILITY AS EMPLOYEE

This Policy requires you to:

a) Read, understand, and comply with the requirements included in this Policy;
b) Comply with Prysmian's Code of Ethics and any other applicable policies or procedures;
c) Report immediately to the appropriate channels outlined in Section 6 of the **Helpline Policy** any alleged violation of this Policy, both if committed by a Prysmian employee or an external stakeholder;

d) Ask questions or report any concerns related to this Policy;

e) Complete assigned training related to this Policy when required.

5. GENERAL PRINCIPLES

Security incidents can damage the Group and its assets in terms of financial loss, brand reputation, compliance, data leakage, business interruption and safety. A security incident can occur at any time and the Group must be prepared to face and resolve it as soon as possible. To this aim, the Security Incident management process should enable a quick, effective and adequate response to security events in order to reduce damages to individuals or to the Group itself.

The Security Incident management process must be defined and implemented in accordance with applicable internal and external references and regulations, taking also into consideration the main information security national and international standards and best practices (e.g. ISO / IEC 27001, ISO/IEC 27035).
Moreover, it must be completely ensured the compliance with applicable external regulations concerning information security, including Privacy regulations, with particular reference to the requirements and actions to be adopted in case of security incidents that involve personal data.

The management of security incidents must be carried out in accordance with the following general principles.

- Security incidents must be promptly identified; all the users have the responsibility to timely report suspected security incidents to the function in charge, so that appropriate actions can be taken to minimize damages.
  An information security incident can be defined as an event or chain of events that compromise the confidentiality, integrity or availability of information. Examples of security incidents include:
    - Loss or theft of data or equipment on which data is stored,
    - Disclosure of confidential information to unauthorized individuals,
    - Hacking to computer systems,
    - Malware or other cyber security attack on systems or networks,
    - Breaches of physical security.

- Each security incident must be categorized according to a standardized taxonomy that identify the main categories of security threats and incidents.
- Security incidents must be classified based on a well-structured method that allows to identify a qualitative level of priority. The level of priority should be identified by estimating the level of criticality of affected resources and the level of impact of the occurred incident. To this aim, damages caused by the security incident need to be identified even if they are direct, indirect or consequential (those that remain even after the recovery, such as reputational damage).
- Security incidents must be in-depth analyzed and investigated to understand the nature of the occurred threat and related causes, typically natural, infrastructural, human factor (malicious or unintentional) and IT causes.
- Containment and recovery plans must be defined by the function in charge in order to minimize the impacts of the security incident.
- A security incident can be considered solved only when the status of the Group before the incident is completely recovered and restored; after that, the environment must be put under control for a defined range of time in order to ensure that the threat is really and definitively foiled.
- The Security Incident management process must include a learning phase aimed to gather a posteriori information that could be useful to improve the detection and resolution of similar future incidents.
- Details about information security incidents experienced (e.g. incident category, information affected and events leading up to incidents) should be recorded and maintained on a continuous basis, using a consistent approach.
- The effectiveness of the security incident management process must be regularly tested in order to assess the Group capability to response to security incidents.
- Appropriate awareness and training sessions must be performed to enable the adoption of the right behavior by the Group personnel and prevent the occurrence of negative events, and to make specialized personnel aware of their responsibilities and required actions.

6. CONSEQUENCES OF POLICY VIOLATION

As a Prysmian employee, you are agreeing to uphold our commitment to this Policy. Prysmian employees who violate this commitment or do not comply with this Policy shall be subject to disciplinary procedures, including possible dismissal, and any other legal action required to protect the interest and reputation of Prysmian, in line with the applicable legislation.

7. REPORTING A POLICY VIOLATION

All employees, contractors, and third-party users are required to report any suspected or actual violations of this Information Security Policy or any Security Incident immediately. All reports will be treated confidentially and investigated promptly. Ensuring the integrity and security of our information systems is a collective responsibility, and your cooperation is essential in maintaining a secure environment.

It is critical that potential violations are reported, internally, promptly as this may allow for immediate containment of any situation and prevention of an actual breach. Additionally, reporting is required to allow Prysmian to take the appropriate action, internally and externally, with regulatory reporting if it is required. Communication with the regulatory authority will be managed and coordinated by Corporate Affairs to protect the reputation and manage the liabilities of Prysmian.
As a Prysmian employee, you are required to report any Policy violation to:

a. **Cybersecurity@prysmian.com;** or
b. your Regional Compliance Team or the other designated subjects mentioned in Section 6.1 of the **Helpline Policy**.

Any form of retaliation, including threats and attempts of retaliation, is strictly prohibited. Prysmian is committed to ensuring that all employees are free to disclose any violation, either real or suspected, of the Prysmian's Company policy or procedure, to the extent they have reasonable grounds to believe that the matters reported are true. You will not be adversely impacted or retaliated upon in the workplace, either personally or professionally, for raising a valid and legitimate concern.

8. AUDIT, MONITORING AND CONTINUOUS IMPROVEMENT

The Owner of this Policy is responsible to perform periodic reviews and updates of this document, examining, in particular, revisions to be made based on internal organizational updates, changes to external legislation and best practices.

Using a risk-based approach, on a periodical basis the Information Security Function and the Internal Audit Department may perform, respectively, monitoring or audit activities aimed at verifying the correct enforcement of this Policy within the organization.

9. RELATED DOCUMENTS

The following Documents are related to this Policy and must be consulted by all Prysmian employees for further guidance. Part of such documents are available in the Ethics & Integrity Section of our **Company's Intranet** and are also publicly available within the correspondent Section of our **Corporate website.**

1. "Document and Record Management" document
2. "Information Security Strategy" document
3. "Information Security Policy" document

APPENDIX A – DOCUMENT HISTORY

The history of changes is shown below. The most recent changes are listed first.

Version	Date	Major Changes
1	11/29/2017	First release
1.1	10/04/2022	Revision and update
1.2	11/06/2025	Change template and revision