INFORMATION SECURITY

APPROVED BY

PRYSMIAN S.p.A BOARD OF DIRECTORS

April 09, 2025

Code: PO-IT-I&C-SEC001

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 Prysmian Group (hereinafter also "Group") is to recognizes that information, in its different forms (both digital and paper documents), is a critical asset and that its effective and efficient management and protection during all its lifecycle is significant for the business success.

The purpose of this Policy is to provide the direction to ensure the achievement of the Group information security objectives described in the Information Security Strategy.

This policy defines the general criteria to be followed for an effective information security management in order to mitigate information security risks and protect Group business processes and information.

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 policy is intended for all the personnel, internal and external, who manage the Group's information systems, facilities, communication networks, IT infrastructure and information.

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 OF INFORMATION SECURITY

The main purpose of information security is the protection of information assets and ICT systems elements from unauthorized access, use, disclosure, disruption, modification, or destruction, whether accidental or intentional, in order to guarantee the following core principles:

- Confidentiality, preventing information from being disclosed to unauthorized individuals, entities, or processes,
- Integrity, protecting information from malicious or accidental modification or manipulation ensuring the accuracy and completeness,
- Availability, ensuring that information is accessible and usable, when required, by authorized users, entities or processes.

The establishment, implementation and maintenance of a Group's information security management system aims to achieve the following objectives:

- protect the interest of the Group, shareholders, employees and third parties,
- ensure compliance with applicable laws and regulations,
- ensure a standard model for the Group information protection and management of related risks,

- guarantee a proper Group information protection and the continuity of business processes, based on the requested level of confidentiality, integrity, and availability,
- minimize business risks by preventing and reducing the impact of information security incidents.

Information Security objectives defined in the strategy are achieved by defining and adopting adequate security measures according to the following four security capabilities:

- Governance: ensure the Group has the right governance structures in place to enhance and maintain its preventive, detective and respond & recover security capabilities,
- Prevention: mitigate cyber exposure surface thanks to preparation and protection of the Group's assets,
- Detection: ensure the Group is aware of the internal and external threats and can pro-actively mitigate them,
- Response & Recovery: defend the Group against successful cyber-attacks and recover from generated impacts.

Adoption and continuous improvement of all the above capabilities allows to mitigate cybersecurity risk exposure by obtaining a good level of control on the Group's security.

6. GOVERNANCE

The governance capability aims to set the foundations of the Information Security Program, by defining criteria to be followed in order to properly govern the security posture of the Group.

6.1 ORGANIZATION ROLES & RESPONSIBILITIES

The protection of Group's assets (both tangible and intangible) is guaranteed by the effort of each involved individual or group. The Group's Information Security roles and responsibilities must be formally defined and clearly assigned and communicated to

involved actors in order to enable the achievement of the Group's information security goals.

Information security responsibilities must be defined according with applicable regulations and taking into consideration all the areas of the four information security capabilities (including governance, risk management, design, implementation, operation and monitoring of adopted security measures). For example, specific roles and responsibilities must be defined in order to promptly and effectively handle security incidents and emergency situation.

The definition and assignment of roles and responsibilities must be reviewed and updated when necessary.

6.2 CYBER RISK MANAGEMENT

In order to understand the Group exposure to cyber risks, specific information security risk assessments must be carried out. The information security risk assessment allows to identify applicable threats and existing vulnerabilities that could compromise the confidentiality, integrity and availability of the Group's information assets.

Identified and analyzed security risks must be prioritized and ranked according to defined risk evaluation criteria. Top risks should be properly treated by choosing the most suitable information security risk treatment option based on estimated implementation costs and expected benefits.

Results of this activity should be formalized providing a clear indication of top risks and details on the required actions to reduce them to the Group acceptable level.

Information security risk assessments must be performed at planned intervals or when significant changes are proposed or occur.

6.3 POLICIES & STANDARDS

Information security management is a process that involves everyone has access to the Group's information assets and it's based on the definition of behavioral and technological principles and requirements formalized in specific policies and standards.

To this aim, the Group must define a set of documents in order to formalize all the information security requirements needed to manage cyber security risks and to protect company's assets according to the information security strategy. This set of documents should be based on a well-structured framework and based on international security standards and best practices. Formalized documents should provide the security guidelines - with different levels of detail - to all involved parties, both internal and external, according to their responsibilities in the information security management process.

In order to pursue the continuous improvement of the information security management, security policies and standards must be kept updated to be in line with the information security strategy and policy, applicable regulations, and technological innovation. Security documents must be approved, published and archived in the Group's document repository that must be available to all involved parties who are authorized to access them.

Security policies and standards must be managed and controlled according to the Group operating procedure "Document and Record Management".

6.4 COMPLIANCE

All relevant legislative statutory, regulatory, contractual requirements regarding information security topics should be explicitly identified, documented and kept up to date for each country in which the Group conducts its business.

Prysmian Group must ensure the compliance with all the internal Information Security policies, standards and procedures and with all the applicable information security and industry regulations. Compliance must be ensured in all the countries where the Group conducts its business.

Privacy and protection of personally identifiable information should be ensured as required in relevant data privacy laws and regulations, where applicable.

6.5 SUPPLY CHAIN SECURITY

Risks associated with the whole supply chain must be properly identified and managed; relevant information security requirements must be established and agreed with each supplier that may access, process, store or communicate the Group's information.

Information security controls must be identified and mandated to specifically regulate supplier access to the Group's information and assets; these controls should include processes and procedures to be implemented by the Group itself as well as by the supplier.

The Group must regularly monitor, review and audit supplier service delivery in order to ensure that the information security terms and conditions of contractual agreements are met and that information security incidents and problems are timely and properly managed.

Moreover, changes to the services provided by suppliers, including existing information security policies, procedures and controls, should be managed, taking into account the criticality of business information, systems and processes involved and by performing a re-assessment of risks.

6.6 HUMAN RESOURCES SECURITY

Security controls performed by the Human Resources function allow to reduce the possibility to have a malicious insider in the Group. Human resources security must consider the whole professional life of both internal and external resources, from the engagement - to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered - to the change or termination of the employment / agreement.

Prior of the employment, background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Moreover, contractual agreements with employees, contractors and third parties must state their and the Group's responsibilities for information security.

6.7 TRAINING & AWARENESS

Information Security is a responsibility shared among managers, staff, IT professionals and all other users. For this reason, education and training must be spread among all the personnel of the Group, making everyone - at every level - aware of the cyber risk and of the importance of acting responsibly, avoiding behaviors that could cause damages to the Group and reacting effectively to security events.

The Group must define an information security awareness program to create and promote the security culture for the correct and secure management of information, processes and assets. The information security awareness program should be established in line with the Group's information security policies and relevant standards, taking into consideration the company's information to be protected and the controls that have been implemented to protect them. The awareness program should be planned to take into consideration the employees' roles in the organization, and, where relevant, the organization's expectation of the awareness of contractors. The activities in the awareness program should be scheduled over time, preferably regularly, so that the activities are repeated also to cover new employees. The awareness program should also be updated regularly in order to be aligned with organizational policies and standards and should be built on lessons learnt from information security incidents.

Moreover, specific training sessions must be organized for IT and technical staff in order to ensure a common knowledge of cyber risks, attack vectors and security solutions.
Both the awareness program and training effectiveness must be measured.

7. PREVENTION

The prevention capability aims to define, implement and operate security measures for the information protection, identity and access management, application and infrastructures protection to reduce the Group's exposure to cyber risks.

7.1 INFORMATION PROTECTION

Information assets must be protected by appropriate security measures according to the value they have for the Group. Information must be protected during the whole lifecycle, from its creation to its use, sharing, storage, archiving and destruction. According to the information level of criticality, suitable security measures must be adopted for each phase of the information lifecycle.

Prysmian Group must define and adopt a classification process that allows to define the level of sensitivity and criticality that information has for the Group, ensuring compliance with applicable regulations. According to this level, information handling rules (e.g., copy, storage, transmission, communication, disposal) must be properly defined.

Data loss prevention solutions should be implemented to validate whether sensitive information is securely stored, sent and used.

Moreover, the adoption of encryption solutions must be evaluated to protect information based on its sensitivity and exposure.

7.2 IDENTITY & ACCESS MANAGEMENT

Identity and access management solutions allow to govern access to the Group resources preventing unauthorized access to IT systems and services. Identity and access controls must be applied to both internal and external users.

Digital identities must be stored, reviewed and managed during all the time the user is in contact with the Group.

Prysmian Group must identify and implement authentication mechanisms in order to verify that an entity is who/what it claims to be. Access to all Group's information assets should be limited based on the principles of segregation of duties, need to know and least privileges. Users should only be provided with access to information and resources that they have been specifically authorized to use and that are necessary for the performance of their job.

The Group must identify the cases in which it's necessary to implement more stringent controls, such as strong authentication, if any.

A set of rights must be defined for different types of authenticated users. Only the necessary rights must be assigned to a user and these must be periodically reviewed and updated every time the user changes his company status.

7.3 APPLICATION PROTECTION

Security requirements must be considered within the software development process. The Group must define and integrate security controls in the design of mobile and desktop applications to ensure that security requirements intended to guarantee confidentiality, integrity and availability are totally fulfilled.

The implementation must be made using trusted tools and libraries and evaluating security impacts.

All the applications must be regularly tested from a security perspective during both the development phase and the operation.

7.4 INFRASTRUCTURE PROTECTION

Security requirements must be defined to protect the Group's infrastructure, from the network to systems, from ICS to mobile devices.

7.4.1 PHYSICAL SECURITY

Physical security must be designed and implemented to prevent unauthorized physical access, damage and interference to the Group's information and information processing facilities.

Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and appropriate entry controls must be adopted to ensure that only authorized personnel is allowed to access to critical areas.

The level of security measures related to the physical protection against natural disasters, malicious attack or accidents should be identified, designed and applied according to the results of a risk assessment.

7.4.2 PATCH & VULNERABILITY MANAGEMENT

Patch and vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities that exist within the Group systems, networks and applications.

Vulnerabilities are flaws that can be exploited by a malicious entity to gain greater access or privileges than it is authorized to have. Patch management addresses security flaws within a software and enhance and extend information systems functionalities as well.

The Group must design, implement and monitor a systematic, accountable, and documented security patch and vulnerability management process that guides system administrators to keep abreast of all the new patches and ensure proper deployment in a timely manner.

Moreover, patches and enterprise patching software must be tested before the deployment to all the Group.

7.4.3 MOBILE SECURITY

Mobile devices, such as smartphones and tablets, must be secured against a variety of threats.

The Group must evaluate security concerns inherent in mobile device use, for both organization-issued and personally owned mobile devices and define security requirements to be implemented to secure mobile devices throughout the whole lifecycle, from the initial configuration to the final disposal.

7.4.4 ICS/IoT SECURITY

Securing the Industrial Control Systems (ICS) and, the most modern Internet of Things (IoT), at both industrial and enterprise sites, is essential to the safe and reliable operation of modern industrial processes.

Security measures must be defined to restrict physical and logical access to the ICS network and devices, to protect individual ICS components from exploitation of related vulnerabilities, to manage information flows in secure and reliable layer, to restrict unauthorized modification of data, to detect and properly respond to security events and incidents, to maintain functionality during adverse conditions and to restore the system after an incident.

Defined security measures should cover the whole ICS lifecycle, from the architecture design to procurement, installation, maintenance, and decommissioning.

7.4.5 SYSTEM SECURITY

Mainframes and servers must be secured as well as workstations, laptops, and removable devices.

Prysmian Group must define and implement a hardening process to secure company systems by reducing their exposure to vulnerabilities.

Security requirements must be defined and approved to securely process, transmit & store information. Moreover, security baselines for specific information systems (servers, databases, workstations, laptops and removable devices) must be defined and adopted, and configuration management process must be established and maintained to control configuration baselines.

7.4.6 NETWORK SECURITY

Network security is aimed to protect information over the networks and supporting information processing facilities by adopting appropriate solutions to prevent and monitor unauthorized access and misuse of the IT resources.

The network, its components and provided services, must be protected from unauthorized access, even remotely, by defining appropriate configurations for the equipment, segregating networks according to specific access policies and installing devices to monitor and control the traffic.

Security mechanisms, service levels and management requirements of all the network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.

7.4.7 MALWARE PROTECTION

The Group infrastructure must be protected from malware though the implementation of prevention, detection, and recovery controls, and by providing an appropriate level of user awareness.

The Group must implement controls that prevent or detect the use of unauthorized software and the use of unknown or suspected malicious websites. Vulnerabilities that

could be exploited by malware should be identified and reduced. An anti-malware software must be installed, executed and updated on the Group's systems.

Security incident process should include detection and reaction of malware attacks.

8. DETECTION

The detection capability guides the Group in the recognition of internal and external threats. The organization has to be aware of a potential threat and its size in order to mitigate it.

8.1 CYBER THREAT MANAGEMENT

Cyber threats must be regularly identified and managed to protect the Group's systems, resources and people by monitoring the applicable cyber threats landscape.

Prysmian Group should perform cyber threat intelligence, gathering and sharing, internally and externally, information about threats, cyber criminals and their modus operandi. Internet, forums and groups should be monitored in order to detect attacks that could cause damage to the Group, in terms of security and reputation.

The readiness of the Group to response to a possible cyber-attack must be periodically tested and results must be analyzed.

8.2 SECURITY ANALYTICS

Security analytics solutions allow to timely detect security events and attacks by identifying anomalies or deviations from the usual behaviors of the Group networks, systems and users.

Prysmian Group must collect and analyze security events generated by the Group networks, hardware and applications; if possible and useful, monitoring, correlation and notifications of events should be performed in real time.

To enable security analytics, logging must be activated on each system, network and application in order to register performed activities.

9. RESPONSE & RECOVERY

The Group must promptly react and respond to a successful cyber-attack. This capability aims to improve the timeliness and effectiveness of the actions taken to reduce impacts generated by a security incident and to guarantee the continuity of business.

9.1 SECURITY INCIDENT RESPONSE

A security incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring services.

Prysmian Group must ensure a consistent and effective approach to the management of information security incidents that allows to classify a detected security event as an incident and to launch the defined response process.

This process must encompass the planning, coordination, and execution of appropriate mitigation and recovery strategies and actions. Management responsibilities and procedures must be established to ensure a quick, effective and orderly response to information security incidents and an escalation communication process must be defined and shared among all the interested parties.

Information which can serve as evidence must be identified, collected, acquired and preserved.

9.2 DIGITAL FORENSICS

The goal of cyber security forensics is to identify the main cause of a cyber security incident and to discover details regarding attack types, methodologies, and behaviors.

The Group must examine information systems and other resources prior and after a cyber-attack in order to understand vulnerabilities, voluntarily or involuntarily changes made to systems and other details. Appropriate methodologies and tools for security forensics should be used.

9.3 BUSINESS CONTINUITY & CRISIS MANAGEMENT

Business Continuity and Crisis Management Continuity Management encompasses planning and preparation to ensure that the Group can continue to operate in case of serious incidents or disasters and is able to recover to an operational state within a reasonably short period.

The organization must establish, document, implement and maintain processes, procedures and controls to ensure the required level of business continuity during an adverse situation.
Regular tests must be carried out to ensure that defined processes, procedures and controls are valid and effective during adverse situations.

10. POLICY UPDATE

This Information Security Policy must be periodically revised and updated, at least once a year or when significant changes occur (e.g., change of the organization, of the approach to security risk management and of the scope of security controls). The revision should be made considering the following aspects:

- Opportunity to improve adopted policy and address issues, in response to environmental, business, legal or technological changes,
- Versioning and changes controls,
- Approval of involved functions.

The revised and updated policy must be approved by management and shared with all the parties involved in the Group information security.

11. 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.

12. 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.

13. 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.

14. 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.**

a) "Document and Record Management" document
b) "Information Security Strategy" document

APPENDIX A – DEFINITIONS

Authentication – The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.

Authentication Mechanism – Hardware or software-based mechanisms that forces users, devices, or processes to prove their identity before accessing data on an information system.

Cyber Attack – An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Impact – The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Information Security – The protection of information and information systems from unauthorized access, use disclosure, disruption, modification, or destruction in order to guarantee confidentiality, integrity, and availability of information.

Information System – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Least Privilege – Users must be able to access only the information and resources that are necessary for its legitimate purpose.

Need to Know – The necessity for access to or knowledge of or possession of specific information required to carry out official duties.

Patch – An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Patch Management – The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

Risk – A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs, and the likelihood of occurrence.

Risk Assessment – The overall process of risk identification, risk analysis and risk evaluation.

Risk Criteria – The terms of reference against which the significance of risk is evaluated.

Risk Evaluation – The process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Security Incident – An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Security Requirements – Requirements levied on an information system that are derived from applicable laws, contractual agreements, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Segregation of Duties – Principle based on shared responsibilities of a key process that assigns the critical functions of that process to more than one person or department so that no single one is capable of performing or controlling it by himself.

Threat – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Source / Threat Agent – The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.

Vulnerability – The weakness of an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

APPENDIX B – DOCUMENT HISTORY

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

Version	Change Date	Major Changes
1	11/29/2017	First release
1.1	10/04/2022	Revision and add reference to NIST Special Publication 800-171
1.2	09/04/2025	Change document template to the standard