HARDENING

APPROVED BY

PRYSMIAN S.p.A BOARD OF DIRECTORS

June 10, 2025

Code: PO-IT-I&C-SEC005

prysmian

The planet's pathways

TABLE OF CONTENTS

1. PURPOSE & OBJECTIVE

The correct classification of the Information is an important prerequisite to determine appropriate levels of protection and to apply appropriate security countermeasures, designed to effectively contrast threats on the Information and to ensure the protection of the fundamental Information security properties: confidentiality, integrity and availability.

The purpose of this document is to define core principles, main roles and responsibilities and the model for data classification, aimed at guaranteeing the proper security level for the 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, in charge of maintaining and updating IT infrastructure, networks, systems and other technological assets.

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

Common security threats, such as exploit of software bugs, unauthorized accesses to information and resources and Denial-of-Service attacks can endanger Prysmian Group's IT systems and infrastructure availability, integrity and confidentiality. The adoption of a hardening policy enable the Group to mitigate and contrast common security threats.

Hardening and patching activities allow the Group to improve the overall security level of IT systems and resources by removing common security vulnerabilities. These activities are applicable to all IT systems and system components among them:

- Computers,
- Servers,
- Mobile devices,
- Application software,
- Peripherals,
- Network devices,
- Databases,
- ICS/SCADA systems.

Hardening and vulnerability management activities must be carried out in accordance with the following general principles.

- An inventory of Prysmian Group IT assets and resources, materials and applications, must be created and maintained. The asset list is useful to keep under control the status and configuration of the assets. The list should contain,

for each resource, information about the owner of the resource, the level of criticality, the configuration and other information.

- Systems and applications must be carefully configured in order to prevent misuse and abuse of functionality from authorized and unauthorized individuals. Components that are not going to be used in a particular installation or required by the planned system functions should be removed or uninstalled from the system in order to reduce its exposure to security threats.

Furthermore, Prysmian Group should define and adopt security baselines for all its main systems in order to identify the minimum set of security configurations to apply and securely handle exceptions, when needed. Standard pre-determined systems' configurations aligned with the security baseline can be included in standard builds to be used in case of new installations (often referred as "image").

- Network devices and firewalls settings must be appropriately managed. Firewalls rules must filter incoming and outgoing traffic, allowing only traffic from and to approved sources, destinations, addresses and ports (e.g. incoming traffic cannot reach directly a host on an internal network). A careful traffic filtering / firewall configuration helps in detecting and preventing attacks.
- Hardening of IT resources includes access control in order to prevent misuse and abuse of assets or unauthorized access to information. Mechanisms that regulate who can access and what he can do must be defined to ensure that only authorized individuals gain access to business applications, information systems, networks and computing devices, that individual accountability is assured and to provide authorized users with access privileges that are sufficient to enable them to perform their duties. To this aim, hardening includes also management of system and built-in accounts that must be properly secured (when possible, disabled).
- Security functionalities of Prysmian Group assets must be segregated and accessible only by authorized people. The employees should not be able to modify intentionally or unintentionally the security settings, configurations, rules and measures of company's systems.

- System and software configurations, security mechanisms and measures, IT architectures and services, network infrastructures and any other kind of IT technologies in use at Prysmian Group should be designed and implemented with the least complexity possible. Resources that are configured, designed and maintained in a clear and simple way are more robust to anomalies, easier to secure and protect and their vulnerabilities can be identified and located faster and with less effort.
- Only the software approved by Prysmian Group can be installed on devices, computers and other assets. This is the software required for employees to perform their business activity, any other software should not be installed on Prysmian Group devices (exceptions must be requested to the IT and Security Departments). If applications not used by the employees are installed, they should be removed and their communication channels with other applications should be closed in order to reduce the vulnerability surface.
- Prysmian Group must install, maintain and keep up to date antivirus and anti-malware software on each computing system and device of its IT infrastructure in order to timely and effectively detect and respond to malicious software threats.
- A structured process must be put in place to deal with vulnerabilities and patches. The process should bring to remediation and patching of vulnerabilities with the appropriate timing and security measures: security patches and other kinds of patches and updates should be applied to secure the Group computing environment (exceptions must be properly requested and motivated and validated by the competent function). The security status of Prysmian Group resources and infrastructure must be regularly monitored in order to actively identify threats. To this aim, Prysmian Group must perform periodical vulnerability analysis in order to detect potential vulnerabilities in its computing environment and implement remediation as soon as possible. Vulnerability analysis should be performed also after security alerts and notifications from suppliers and vendors.

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	10/06/2025	Change template and revision