THIRD PARTIES SECURITY

APPROVED BY

PRYSMIAN S.p.A BOARD OF DIRECTORS

June 10, 2025

Code: PO-IT-I&C-SEC012

prysmian

The planet's pathways

TABLE OF CONTENTS

1. PURPOSE & OBJECTIVE

The purpose of this document is to define the scope, the audience and the general principles to be applied in order to reduce Information and Cyber Security risks deriving from an incorrect management of Prysmian Group Third Parties and to ensure protection of confidentiality, integrity and availability of Group information exchanged and accessed by them.

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, involved in the selection, management and monitoring of Third Parties and related contracts and relationships.

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

While Third Parties are vital to many organization's operations, they can introduce Information Security risks that should be taken into account. Third Parties can handle Prysmian Group valuable and sensitive information, thus, if appropriate security measures related to the management of Third Parties are not implemented, the confidentiality, integrity and availability of Group information could be affected.

Since the secure management and maintenance of Prysmian Group data is transferred to Third Parties, their lack of appropriate protection measures could result in financial, reputational, operational and legal impacts for the Group.

Considering that cybercriminals increasingly target Third Parties as a vector to attack their customers or partners and regulators increasingly hold organizations liable for breaches of vendor-controlled data, the management of Information Security risks associated with Third Parties is a fundamental aspect for the Group. Information Security requirements should be taken into account during all the phases of the Procurement processes, from the selection of potential suppliers and the integration of specific Information Security clauses within the contracts to the proper management of agreements termination.

Third Parties Security practices must be carried out in accordance with the following general principles.

- Third Parties Security Management processes, procedures and instructions should be formalized, published, distributed and regularly reviewed in order to ensure the adoption of the appropriate Information Security controls within the Third Parties Management activities.
- Updated list of Prysmian Group Suppliers and other Third Parties should be maintained. The list should contain a "score" or a "ranking" of each supplier, evaluated based on the criticality of the service provided, on the type of information accessed and on the associated risk.

- Third Parties should have access only to that kind of data and information assets that are necessary for the provision of the service. For each Third Party, data and assets that have to be accessed within the provision of the service should be identified and the related access modalities should be carefully defined. This provides the basis for the analysis of the Third-Party risk profile.
- A risk-based approach should be employed in the identification of, selection of and relationship development with Suppliers and other Third Parties. A risk evaluation should be performed (e.g. by means of a risk assessment questionnaire) to identify the criticality of the Third Party for the Group based on predefined criteria such as the type of provision and the type of data processed. If some aspects of the provision or of the relationship change, the risk profile of the Third Party should be updated.
- Due diligence activities should be executed at least on Third Parties with a significant risk "rating" in order to evaluate the adequacy of Information Security safeguards they have adopted to protect the confidentiality, integrity and availability of the Group information. Due diligence activities should be performed prior the selection of a Third Party, to determine Information Security gaps to be addressed in order to establish an agreement, and during the course of the relationship. Furthermore, the Group should agree with Third Party the possibility to execute Information Security Audits or Technical Assessments on the Third-Party processes and systems that access or process Group information ("right to audit").
- Agreements with Third Parties should be formalized and signed only after careful considerations, considering the results of the risk evaluation and of the due diligence activities. If relevant gaps are identified, the inclusion of specific clauses within the agreement should be evaluated and the Third Party should guarantee to implement initiatives aimed at remediating these gaps. Prysmian Group should require Suppliers and other Third Parties to provide evidence that their operations and controls comply with contractual requirements and that identified gaps have been addressed.
- Suppliers and other Third Parties that access, process, store and communicate Group non-public information should be required to adhere to Group Information Security practices or communicate any situations where this adherence is not

achievable. Group expectations regarding Information Security practices that Suppliers shave to implement should be formalized with specific clauses or with Information Security requirements baselines to be included within the contract. Purchasing Orders should contain a summary or a reference to the above-mentioned Information Security requirements that Suppliers should meet.

- A reference individual of the Third Party should be designated and agreed as single point of contact for Information Security matters. Prysmian Group should interface with the appointed referent to discuss or report Information Security issues that could affect Group business and operations.
- Prysmian Group should specifically require Third Parties to protect, during the whole relationship and after the termination of any agreement, the confidentiality of Group information they access or process to provide the service. Confidentiality requirements could be formalized, for example, in a Non-Disclosure Agreement or in a contractual clause.
- Prysmian Group should specifically require Third Parties to protect, during the whole relationship and after the termination of any agreement, the Personal Information they process from unauthorized access and disclosure. Third Parties should perform any treatment, disclosure, transmission and retention of Personal Information in compliance with all applicable laws and regulations (e.g. GDPR). Privacy requirements could be formalized, for example, in a specific contractual annex or in a contractual clause.
- Prysmian Group should require its Third Parties to notify in a timely manner any Information Security incident occurred within their systems and perimeter that could affect Group information. Data breaches or Information Security events that could affect Prysmian Group business should be communicated according to applicable laws and regulations and contractual terms and they should be promptly investigated and solved by the Third Party jointly with the Group. Same notification and resolution should be ensured in case of detected and known vulnerabilities of Third Parties systems that could generate, if exploited, impacts on the confidentiality, availability, or integrity of Group information.
- Prysmian Group should guarantee the Information Security along its whole Supply Chain, requiring its Suppliers and other Third Parties to adopt Information Security

controls within their own Third Parties Management practices and, more in general, within their own Supply Chain.

- Service Levels, that indicates the minimum acceptable performance and availability level for the services provided, should be defined, agreed and formalized within agreements with the Suppliers. Suppliers should respect these Service Levels both in normal conditions and during disruptive events.
- Permitted disclosure of Prysmian Group information by Third Parties should be regulated, controlled and formalized. Third Parties should notify and consult Prysmian Group for any disclosure regarding Group data requested by public authorities or by law or needed for other cases, to evaluate potential negative effects.
- Relationship or agreement termination with a Third Party should be regulated within the agreement, in particular Information Security practices to be adopted upon termination should be agreed. Third Parties should be required to return or delete any Group information they have. If not possible, the confidentiality of this information should be ensured even after the termination of the relationship with the Third Party. Furthermore, Third Party user accounts and access privileges should be promptly removed or disabled.

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	07/09/2020	First release
1.1	10/10/2022	Revision and Update
1.2	10/06/2025	Change template and revision