DATA CLASSIFICATION

APPROVED BY

PRYSMIAN S.p.A BOARD OF DIRECTORS

April 09, 2025

Code: PO-IT-I&C-SEC010

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 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 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

Information is a strategic resource and a fundamental asset for the business and the success of the Prysmian Group, therefore it must be protected and managed based on its relevance for the Group, considering the highly competitive and internationally wide context in which it operates.

The correct classification of the Information is a fundamental pre-requirement to determine the adequate level of protection and the necessary security measures, aimed at effectively minimizing threats and guaranteeing the protection of the fundamental properties of Information Security: confidentiality, integrity and availability.

Data classification and management must be carried out in accordance with the following general principles.

- Prysmian Group Information must be classified based on defined criteria that consider the level of risk associated with an inadequate Information management.
- Criteria for Information classification must be based on the value of Information for the business. To this aim, criteria for classification must privilege more the principle of confidentiality than integrity and availability, in order to give more importance to the damage caused to the Group in case of unauthorized disclosure of Information.

- According to the "need to know" principle, access to Information must be guaranteed only to those individuals that need it in order to perform their job, in line with their responsibilities.
- According to the "segregation of duty" principle, the roles of control are separated from operational roles, hence the level of classification, distribution and scope of the permissions are granted by the individual who has the role of Information Owner.
- Information must be adequately protected during its whole lifecycle by adopting security measures commensurate with the assigned classification level. To this aim, Prysmian Group must identify a set of appropriate organizational, procedural and technical security measures for each Information classification level to be put in place and maintained. Defined security measures and controls must be properly adopted by involved parties during storage, processing, distribution activities and during any other permitted use of the Information.
- Classification levels and related security measures must be integrated and consistent with those defined in other standards or in specific regulations (e.g. local laws such as Italian Privacy Law). In fact, for specific categories of Information, national and international regulations and standards could require additional security measures in order to ensure their appropriate protection. In this case, the Group overall protection system must take into consideration the combination of the two sets of security measures, adopting the more restrictive security measures in case of overlap (principle of increased security).

6. ROLES & RESPONSIBILITIES

The following table describes the roles involved in the data classification process and their responsibilities:

Role	Responsibilities
Information Owner	• Assess and define the classification level of the Information that will be processed by the users according to the criteria described in this policy. • Manage the Information during its whole lifecycle, evaluating and performing any potential reclassification. • Identify the users entitled to access and process the Information. • Identify the operations that can be performed on the Information. • Evaluate the actual need for Information availability and, if necessary, decide for its disposal. • Report any observed or suspected disclosure to the LSA as defined in the Security Incident Management Procedure. • If needed, Information Owner activities can be performed by an authorized delegate.
Users	• Process the Information only for the defined purposes and according to their job duties and responsibilities. • Properly manage Information according to the defined classification level. • Report any observed or suspected misuse of Prysmian Group Information to the Information

	Owner as quickly as possible, in order to prevent Information Security incidents. • Report any observed or suspected disclosure to the LSA as defined in the Security Incident Management Procedure.
ICT Personnel	• Prepare, make available and maintain the technical tools and equipment needed to support the proper and timely classification of Prysmian Group Information and to adequately protect it. • Implement the IT security measures to adequately protect the Information, according to the assigned level of classification. • Report any observed or suspected disclosure to the LSA as defined in the Security Incident Management Procedure.
Security Personnel	• Support all involved actors in the proper application of all the classification principles and guidelines, during the whole Information lifecycle. • According to the assigned level of classification. • Verify the effectiveness of security measures designed to protect Information in accordance with its classification level. • Support definition and adoption of the proper tools and equipment to adequately protect the Information. • Report any observed or suspected disclosure to the LSA as defined in the Security Incident Management Procedure.
Human Resources	• Ensure that all involved actors are aware of the relevance and importance of Information

	classification through communication and awareness campaigns. • Communicate to the Group the importance of properly classifying Information and conforming to this Data Classification Policy.

Table 1: Roles and responsibilities

7. INFORMATION TO BE CLASSIFIED

This policy defines the criteria to assign classification levels to any form of Information created and processed by Prysmian Group, regardless of the type of Information and where and how it is stored, aggregated and transmitted.

Particularly, Information classification criteria described in this policy must be applied to any form of Information, regardless:

- How it is created:
  - Manually created – the Information is created or modified manually (e.g. emails, Word documents, physical archives);
  - Automatically created – the Information is produced by an electronic system (e.g. automatic emails, system reports).
- How it is structured:
  - Structured – the Information has a well-defined structure (e.g. ERP systems, database);
  - Unstructured – the Information is not organized with a structure (e.g. emails, hand-written notes).
- How it is processed:
  - Digital format – the Information is stored, transmitted, visualized or processed with electronic tools (e.g. applications, files, database, email);
  - Non-Digital format:
    - Physical format – the Information is represented on a directly usable physical medium (e.g. printed documents, hand-written notes);

- **Oral format** – the Information is represented under oral form (e.g. speech, conversations).

8. INFORMATION LIFECYCLE

Information must be properly managed during its whole lifecycle, from creation to disposal, as its value changes over time. Information lifecycle is composed by the following phases:

A. **Creation** – The Information is created;
B. **Classification** – The Information is classified based on the defined criteria;
C. **Usage –** The user uses and elaborates the Information;
D. **Transmission –** The Information is distributed to its recipients;
E. **Storage –** The Information is stored on the appropriate support;
F. **Disposal** – The Information is properly eliminated.

If needed, **Reclassification** can be performed by the Information Owner.

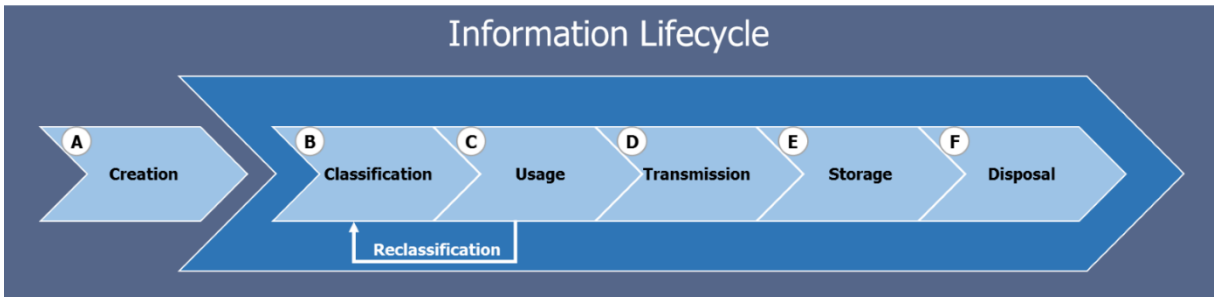

Figure 1: Information lifecycle

A. CREATION

During the creation phase, the Information, eventually acquired from internal or external sources, is subject to analysis, synthesis, and verification and, where applicable, consolidated into a corporate document (paper or electronic). During this phase, the document must be accessible only by the working groups entitled for the drafting and verification activities, in accordance with their duties, and by the Information Owner.

B. CLASSIFICATION

The Information Owner has the responsibility to determine the level of classification according to the principles set out later in this document and to ensure that all Information is properly labelled.

C. USAGE

During this phase, the Information, regardless of its form, is processed (and if needed, duplicated) by the users (Prysmian Group employees or third parties) in accordance with their job responsibilities and duties. The personnel must apply all the necessary security measures defined for the classification level assigned to the Information they are using.

The Information Owner should ensure that the Information is not misused and that the number of copies of it is limited and restricted to the needs of the business. Any copy must be compliant to the security measures provided for the Master Copy (original one) in accordance with its classification level.

When the content of a document is modified or altered, a new Information is created and the classification process must be executed from the beginning because the new document created could correspond to a classification level different from the original one. If a document is created merging two or more documents (completely or partially), the assigned classification level is the higher one among the levels of the documents used for the merger.

D. TRANSMISSION

The transmission phase comprises all the distribution and transmission activities from the Information Owner to its recipients (subjects that will use the Information). The transmission must be performed following the security measures defined for the classification level of the Information, using the appropriate channels and modalities, both for digital and non-digital formats.

E. STORAGE

In this phase, the Information is stored on an electronical or physical support. Defined security measures must be put in place based on the classification level of the Information (e.g. minimum security measures as specified in D.Lgs. 196/2003, Annex B).

Each user is responsible for the Information under his control and he must not leave documents or devices where Information is stored unattended, especially when the Information is confidential or higher.

F. DISPOSAL

Information can be disposed when no longer useful for the company or when required by law.

If the Information is no longer considered business relevant, the Information Owner has to ensure its proper disposal and, if necessary, its destruction, together with any further produced copies. Adopted disposal modalities must be adequate to the Information classification level.

G. RECLASSIFICATION

Reclassification is performed whether any change in the business relevance and sensitivity of the Information occurs (e.g. reserved documents on the acquisition of a third party voluntarily disclosed once the abovementioned acquisition has occurred, changes in the existing legislation concerning data privacy, etc.).

The Information Owner is the only subject authorized to modify the Information classification level, following the classification model described in the following paragraph of this policy.

9. INFORMATION CLASSIFICATION LEVELS

To classify the Information, it is necessary to evaluate and understand the risk that Prysmian Group has to manage in case of loss of data confidentiality, data disclosure, breaches, etc.

Particularly, Prysmian Group has defined the following classification levels (sorted by progressively less restrictive confidentiality requirements):

- CONFIDENTIAL RESTRICTED – This is the highest classification level and identifies extremely confidential and business critical Information. The unauthorized disclosure outside of permitted distribution scope, loss,

tampering or misuse represent a serious risk, in some cases irreversible, for the Group itself, its employees or third parties.

- CONFIDENTIAL – This level identifies highly sensitive Prysmian Group Information. An unauthorized access or release of this kind of Information poses a medium risk on the Group and its stakeholders.
- INTERNAL – This level identifies Information that does not belong to the previous levels and whose unauthorized access poses a low risk on the Group.
- PUBLIC – The unauthorized disclosure of the Information outside Prysmian Group does not pose any risk. Information of this kind is accessible to all users with no restrictions and/or publicly disclosed by the Group.

Any Prysmian Group Information, regardless of its classification level, can be shared and transmitted outside the Group, as long as the third party is included in the distribution list and the transmission is performed applying the defined security measures.

10. MODEL FOR INFORMATION CLASSIFICATION

The Information classification model is based on "quick tests" that can support the Information Owner in the risk evaluation process. By answering these questions, the Information Owner is lead to the identification of the proper Information classification level.

The following table provides, for each classification level, the related "quick test" and examples of Information.

Level	Quick test	Examples
Confidential Restricted	• An Information is "Confidential Restricted" if the answer to at least one of the following questions is "yes": • Would an individual external to Prysmian Group pay for this Information?	• Information concerning a highly significant and consistent part of Prysmian Group's business and / or research and development activities

	• Is the Information related to the future strategy or to the marketing plan? • Could this Information influence a potential purchase of a customer? • Could the diffusion of this Information have impacts on the price of the shares? • Do regulations that require the non-disclosure of this Information to third parties exist (e.g. Privacy regulations)? • Is the Information related to business or legal investigations? • Is the Information protected with Confidentiality / Non-Disclosure Agreements?	• Key strategies and long-term instructions • Information which is crucial for the technical and/or economic success of a product or technology • Documents containing sensitive employees' data (e.g. medical data, religion, ethnicity) • Legal proceedings in progress, legal investigations • Changes in the organizational structure (e.g. mergers, acquisitions, joint ventures, partnerships)
Confidential	• An Information is "Confidential" if the answer to at least one of the following questions is "yes": • Is the Information relevant for the press? • Can the diffusion of this Information outside the company endanger the position of a company member? • Should I worry about this Information being visible to someone else, as in the case I	• Information concerning the business and/or research and development activities of Prysmian entities • Future products programs (e.g. objectives, launch dates) • Short-term business plans and budgets • Information about customer and suppliers (contractual or financial relations, offers, quality evaluations)

	leave it unattended in a meeting room or someone collect it from my desk?	• Documents containing common employees' data (birth dates, addresses) • Information which could affect the technical and/or economic success of a product • Information concerning methodologies or processes
Internal	An Information is "Internal" if: • The Information does not belong to "Confidential Restricted" or "Confidential" categories. • No authorized Prysmian Group entity (e.g. Communications, Public Relations) has specified that this Information can be disclosed.	• Sales handbooks • Procedure handbook • Organization charts • Internal telephone and email directories
Public	An Information is "Public" if: • The Information does not belong to "Confidential Restricted", "Confidential" or "Internal" categories. • An authorized Prysmian Group entity (e.g. Communications, Public Relations) has specified that this Information can be disclosed. • Contractual, legal or any other form of public disclosure obligation of Information exist.	• Marketing material • Products and services brochures • Jobs alerts poster on the corporate website • Press releases

Table 2: Data classification model and examples

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.**

1. "Rule governing the classification, control and protection of Information" document
2. "Document and Record Management" document
3. "Information Security Strategy" document
4. "Information Security Policy" document
5. "Data Handling Security Guidelines" document
6. "Security Incident Management Procedure" document

APPENDIX A – DEFINITIONS

Availability – It is the capacity to ensure that Information is accessible and usable, when required, by authorized users, entities or processes.

Confidentiality - It is the capacity to prevent Information from being disclosed to unauthorized individuals, entities or processes.

Digital Information – Information represented by processing electronic content expressed through text, image or movie. The term digital indicates that this representation is of numeric type and assumes discrete numeric values.

Information – Any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audio-visual.

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 Security Measures – Set of measure designed to protect the Information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, availability and non-repudiation.

Integrity – It is the capacity to protect Information from malicious or accidental modification or manipulation ensuring its accuracy and completeness.

Need To Know – It is the principle that ensures user only accesses the Information strictly necessary to carry out his own activities, according to the assigned tasks and responsibilities.

Non–Digital Information – Information represented in any other format (e.g., paper, voice) different from the digital one.

APPENDIX B – DOCUMENT HISTORY

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

Version	Date	Major Changes
1	02/01/2018	First release
1.1	10/04/2022	Revision and update
1.2	09/04/2025	Change template and Revision