BACKUP AND RESTORE

APPROVED BY

PRYSMIAN S.p.A BOARD OF DIRECTORS

February 02, 2026

Code: PO-IT-I&C-SEC004

prysmian

The planet's pathways

TABLE OF CONTENTS

1. PURPOSE & OBJECTIVE

The purpose of this document is to define the scope, the audience and general principles to reduce the risk of business data loss by ensuring that, in the event of an emergency (e.g. accidental delete, system failure, intentional or unintentional corruption/destruction of data, or disaster), business essential information or software can be restored within defined timescales. 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) and the Digital Operational Resilience ACT (DORA) 2022/2554.

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 defining backup business requirements and performing backup and restore activities.

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 based on its relevance for the Group, reducing any data loss risk that could jeopardize business continuity. To this aim, backup ensures data and systems storage on alternative devices allowing their restoration in case of an emergency within critical timescales (i.e. the timescale beyond which the unavailability of information would be unacceptable to the organisation).

Moreover, an effective backup and restore management strategy can also support the Group in meeting requirements for archiving important business information and meeting legal, regulatory and contractual requirements for document retention.

Backup and restore management must be carried out in accordance with the following general principles.

- Prysmian Group must identify the backup scope taking into consideration data and software that are relevant for the business and that should be recovered in case of an emergency (e.g. file server, email server, web servers, database, domain controllers). Backup scope should be determined taking into consideration also the criticality of the information and the level of confidentiality of the data.
- For each system or data set in the backup scope, depending on business requirements, it must be defined the backup frequency (e.g. daily, weekly, monthly) and a schedule backup window to execute backup procedures without interfere with business activities. Backup frequency should be determined taking into consideration the maximum amount of acceptable data loss for the business, calculated from the last successful backup, the criticality of the information or the level of confidentiality of the data.
- For each system or data set in the backup scope, it must be defined a backup retention period during which backup are stored and available to recovery. The retention period should be determined in accordance with business needs and applicable compliance constraints (e.g. regulations, contracts, etc.).

- For each system or data set in the backup scope, depending on business requirements, it must be identified the critical timescale for restoring information, taking into account the type of information to backup and where it is stored, legal, regulatory and contractual requirements (e.g. the handling of personally identifiable information (PII), document retention and customer information), business continuity plans and related arrangements. When defining the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) for each function, particularly for Prysmian Riassicurazioni S.p.A. it is essential to consider whether the data is linked to a Critical or Important Function (CIF), as well as the potential impact on overall market efficiency.
- Depending on the type and amount of data to be backed up, backup frequency, retention periods and recovery timescales set by business, the Group must determine the type of media to use for storing (e.g. backup appliance, magnetic tape systems, hard disks, optical storage). Secure disposal of backup media should be performed if it is physically damaged or exceeded the average lifecycle indicated by the support provider. Before the expiration of the data retention time, the Group should consider the ability to reuse the backup media for new storage.
- According to the criticality of data, time consuming to restore, technological capabilities and constraints on data retention and availability, personnel in charge must establish the appropriate type of backup: full, differential, incremental, or a combination of the previous ones. While the full type backup all files regardless of when they were last modified or backed up; differential/incremental types backup all files that have changes since the last successful incremental or full backup.

  Moreover, it must be defined an execution mode (online or offline) to perform the backup activity in accordance with the typology of the particular information and the criticality of business process. At the end of each backup run, the successful completion of the operation must be verified by checking that no malfunctions have occurred.
- .Backup systems and their associated restoration and recovery procedures shall be established, activated, and periodically tested in accordance with defined policies,

ensuring that the security of network and information systems, and the availability, authenticity, integrity, and confidentiality of data, are not compromised.

- Periodic recovery and backup tests must be performed to verify the integrity and availability of the backup and to verify the adequacy of the recovery times with respect to business needs. Specifically, backup testing should be periodically performed for the following purposes:
    - continuously ensure the availability of data.
    - verify that backup was successful.
    - check and correct errors, if any.
    - monitor the duration of the backup job.
    - optimize backup performance where possible.
- During recovery from ICT-related incidents, and when reconstructing data from external stakeholders, comprehensive checks and reconciliations must be performed to ensure the highest level of data integrity and consistency across all systems (wherever applicable).
- More than one copy of backup should be created and should not be in same place as the original data. Ideally, the Group should have a copy in another location, at sufficient distance away to escape any damage from a disaster (e.g. a fire or flood). Backup media should be stored offsite in a secure, environmentally controlled facility. When selecting the offsite location, distance, ease of accessibility to backup media, physical storage limitations, and the contract terms should be taken into account by the Group.
- At least for Prysmian Riassicurazioni S.p.A, the secondary processing site must be geographically distinct from the primary site to mitigate shared risks, capable of ensuring the continuity of critical or important functions in line with recovery objectives, and immediately accessible to staff in the event of primary site unavailability.
- Backups should be protected from loss, damage and unauthorized access, as well as the original data. Specifically:
    - backup media (e.g., DVDs, magnetic tapes, computer disks) must be stored in accordance with manufacturer specifications.

- backup media should be clearly labelled and located in a locked, fireproof computer media safe on-site, to enable important information to be restored quickly.
- backup should be protected from accidental overwriting.
- physical and logical access to backups must be restricted to a limited number of authorized individuals (e.g. through the use of access control software, physical locks and keys);
- details about data backed up, the date and time of the backup, the backup media used and its physical location should be recorded in a log (or equivalent);

Additionally, at least for Prysmian Riassicurazioni S.p.A.:

- Backups shall be stored on ICT systems that are both physically and logically segregated from the source ICT environment. These ICT systems must be securely protected against unauthorized access and any form of ICT corruption and must enable the timely restoration of services using data and system backups as required. This requirement applies in particular to Prysmian Riassicurazioni S.p.A., in alignment with the DORA Regulation.
- Redundant ICT capacity must be ensured, with resources, capabilities and functions that are adequate to support and sustain business needs

Moreover, the Group should consider including encryption in its backup strategy, including backup media that goes offsite for storage, to secure data that could be lost or stolen in route or at alternative site.

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
1.3	02/02/2026	DORA Regulation update