CLOUD SECURITY

APPROVED BY

PRYSMIAN S.p.A BOARD OF DIRECTORS

June 10, 2025

Code: PO-IT-I&C-SEC007

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 ensure protection of Prysmian Group information when treated and/or stored on the cloud or by a cloud provider. This document outlines the risks of cloud solutions and defines general principles to mitigate them.

The purpose of this document is to define the scope, the audience and general principles to ensure protection of Prysmian Group information when treated and/or stored on the cloud or by a cloud provider. This document outlines the risks of cloud solutions and defines general principles to mitigate them.

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

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.

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

Cloud computing is a model for enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. However, cloud computing impacts the organizational, operational, and technological approaches to data security, network security, and information security good practice.

Following paragraphs describe cloud service and deployment models, potential security risks associated with them and general principles to properly govern cloud service and providers.

5.1 CLOUD MODELS

There are three basic service models of cloud computing:

- Software as a Service (SaaS), the consumer is able to use the provider's applications running on a cloud infrastructure; the consumer does not manage or control the underlying cloud infrastructure;
- Platform as a Service (PaaS), the consumer is able to deploy onto the cloud infrastructure applications acquired or self-developed using programming languages, libraries and tools supported by the provider; the consumer does not manage or control the underlying cloud infrastructure but has control over the deployed applications and possibly configuration settings for the application-hosting environment;

- Infrastructure as a Service (Iaas), the consumer is provided with processing, storage, networks and other computing resources where he is able to deploy and run arbitrary software, which can include operating systems and applications; the consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage and deployed applications.

Cloud computing can be deployed according to the following four cloud deployment models:

- Private cloud, the cloud infrastructure is provisioned for exclusive use by a single organization, it may be owned, managed and operated by the organization, a third party or some combination of them;
- Community cloud, the cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns, it may be owned, managed and operated by one or more organizations in the community, a third party or some combination of them;
- Public cloud, the cloud infrastructure is provisioned for open use by the general public, it may be owned, managed and operated by a business, academic, government organization or some combination of them.
- Hybrid cloud, the cloud infrastructure is a composition of two or more distinct cloud infrastructures that remain unique entities but are bound together by standardized or proprietary technology.

5.2 POTENTIAL RISKS

Cloud computing services are not only exposed to existing security risks, but they are also subject to the emergent threats associated with multitenancy, outsourcing of the application and data, and virtualization.

The following are the most important cloud computing specific risks:

- Loss of governance: using cloud infrastructures, the control is necessarily ceded to the cloud provider on a number of issues which may affect security.

- Lock-in: it could be difficult to migrate from one provider to another or migrate data and services back to an in-house IT environment, especially if data, application and service portability is not enabled.
- Isolation failure: multi-tenancy and shared resources are representative characteristics of cloud computing. This risk category covers the failure of mechanisms aimed to separate storage, memory, routing between different tenants (e.g., so-called guest-hopping attacks).
- Compliance risks: it could happen that the compliance to industry standard or regulatory requirements cannot be ensured and it could happen that the provider cannot provide evidence of their own compliance with the relevant requirements or he does not permit audit by the cloud customer.
- Management interface compromise: customer management interfaces of public cloud providers are accessible through the Internet and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.
- Data protection: cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., between federated clouds.
- Insecure or incomplete data deletion: requests to delete cloud resources may not result in true wiping of the data. Adequate or timely data deletion may also be impossible either because several copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients. In the case of multiple tenancies and the reuse of hardware resources, this represents a higher risk to the customer than with dedicated hardware.
- Malicious insider: while usually less likely, the damage which may be caused by malicious insiders is often far greater. Cloud architectures necessitate certain roles which are extremely high-risk because with very high permissions (e.g., provider system administrators and managed security service providers).

5.3 GOVERNANCE PRINCIPLES

In order to address and manage potential risks and security challenges introduced by cloud technologies, the Group must manage cloud services and providers in accordance with the following general principles.

- Cloud services and deployment models must be in-depth analyzed in order to adopt a solution that meets the Group specific business needs while ensuring consistency with its risk management objectives. Prysmian Group must clearly define what services purchase from cloud providers and what activities perform internally.
- Cloud providers must be carefully selected considering offered services, professional certifications, any constraints (e.g. on the territorial distribution) but also their flexibility in defining contractual agreements.
- Security risk assessment must be performed in order to determine security risks associated to cloud services. Results of this activity allows the Group to make an informed decision about the adoption of cloud service. Due to the evolving nature of cloud and its providers also vendor risk should be included in the analysis (e.g. business survivability of providers, portability of data and applications, and interoperability of services).
- It must be negotiated the appropriate Service Level Agreement (SLA) and contractual obligations with the cloud provider thus ensuring that security requirements are contractually enforceable. It is important to understand the contractual responsibilities of each party, considering that the baseline expectations vary by the service model, with the customer having more control and responsibility in an IaaS model, and the provider having the dominant role for SaaS solutions.
- With respect to the additional complexities introduced by the cloud borderless and multitenant nature on compliance with laws and regulations, Prysmian Group must consider the impact of a distributed IT model, including the impact of cloud providers operating in different geographical locations and different legal jurisdictions. Any information processed, transmitted, stored, or viewed that is identified as Personal Identifiable Information or private information faces privacy

regulations worldwide that may vary from a country to another; moreover, many laws prohibit or restrict the transfer of information out of the country.

- A Data Security Lifecycle must be adopted for evaluating security exposures and defining cloud data security strategy that should be layered with information governance policies, and then enforced by key technologies such as encryption and specialized monitoring tools. If needed, the adoption of new data security techniques can be evaluated, such as data dispersion, a kind of algorithm capable of providing high availability and assurance for data stored in the cloud, by means of data fragmentation. Moreover, all sensitive data should be encrypted moving to or within the cloud at the network layer, or at nodes before network transmission (for all service and deployment models).
- Data must be protected from malicious individuals and virtual machine vulnerabilities and this must be done considering and defining new methods suitable for cloud-based architectures. Virtualization is one of the key elements of the cloud services, therefore Prysmian Group should identify which types of virtualization the cloud provider uses, if any, and verify the security measures adopted. Examples of these security measures are: segregation of virtual machines, encryption of data accessed by virtual machines, protection of any virtual machine image or template, management of backup and failover systems when the virtual machine images are deleted or wiped, implementation of firewall (inbound/outbound), Intrusion Prevention System, web application protection, antivirus, file integrity monitoring, and log monitoring, etc.

Moreover, regular web application penetration testing should be carried out and related remediation should be implemented to reduce identified vulnerabilities.

- Activities on company data must be subject to access control, monitoring and logging. Prysmian Group should evaluate the need to strengthen the current level of authentication by evaluating the implementation of strong authentication methods to access to the cloud applications. The existing identity and access management practices in place must be respected and identity integrity and audit must be preserved when moving data off-site and/or decoupling the pillars of the solution into web service architecture.

Cloud-based system must be continuously monitored according to the type of adopted service model in order to promptly detect suspicious events or changes from the normal behavior of systems and users.

- Secure Software Development Life Cycle (SSDLC) assumes increased importance when migrating and deploying applications in the cloud. The company should ensure that the best practices of application security, identity management, data management, and privacy are included to its development programs and throughout the lifecycle of the application. Prysmian Group must understand the characteristics of the cloud applications and the difference with traditional ones thus defining an application security assurance program that ensures - for the applications that have being migrated and/or developed and maintained in a cloud environment - adequate capability and capacity to design, develop, test and deploy secure applications. Configuration and change management must be auditable and verifiable.
- Portability and interoperability must be guaranteed. Interoperability is the requirement for the components of a cloud eco-system to work together to achieve their intended result. Interoperability mandates that those components should be replaceable by new or different components from different providers and continue to work, as should the exchange of data between systems. Portability is a key aspect to consider when selecting cloud providers since it can both help prevent vendor lock-in and deliver business benefits by allowing identical cloud deployments to occur in different cloud provider solutions, either for the purposes of disaster recovery or for the global deployment of a distributed single solution.
- Selected cloud providers must have Business Continuity and Disaster Recovery processes in place; if needed, specific certifications must be required and reviewed by Prysmian. Moreover, for critical applications, Prysmian Group should not depend on a singular service provider and should have a Disaster Recovery Plan in place that facilitates migration or failover if a supplier fails.

Prysmian Group must prevent data loss ensuring that data on cloud is backed up on regular basis and geographically distributed.

- Data centers and servers must be protected both logically and physically and onsite assessment should be performed periodically. Prysmian Group should ensure that the provider has adopted service management processes and practices to run their data centers and has adopted racking techniques that ensure agile and highly available resources inside the data center. The access to physical locations must be restricted and network equipment and telecommunications assets must be controlled by personnel appropriately placed in the cloud provider's organization.
- Prysmian Group must understand how the cloud-service provider defines events of interest versus security incidents and what events/incidents the provider reports to it and in which way.
  Cloud computing does not necessitate a new conceptual approach to incident response, rather it requires that the organization appropriately maps its incident response processes and programs to the specific operating environment it embraces.

  Moreover, it must be agreed and formalized the cloud provider support for incident analysis, with specific reference to the nature (content and format) of data he will supply for analysis purposes and the level of interaction between Prysmian and the provider incident response team. In particular, it must be determined whether available data for incident analysis satisfy legal requirements on forensic investigations that may be relevant to Prysmian.
  In order to facilitate the processing of events/incidents, Prysmian should require the set-up of proper communication paths to be utilized in case of incident occurrence and the adoption of open standards for communications.

- Removal of data from the cloud, due to expiry of contract or any other reason, should be covered in detail while setting up the Service Level Agreement (SLA) and contractual obligations. This should cover deletion of user accounts, migration or deletion of data from primary / redundant storage, transfer of keys, etc.
- Prysmian personnel in charge must monitor that all the established agreements are respected by the cloud provider, by defining and measuring specific metrics for the evaluation of performance.

- In order to detect potential issues in the management of cloud resources, providers and data stored, regular audit activities must be performed by independent entities. Due to the on-demand provisioning and multi-tenant aspects of cloud computing, traditional forms of audit and assessment may not be available or may be modified. For example, some providers restrict vulnerability assessments and penetration testing, while others limit availability of audit logs and activity monitoring. Moreover, Prysmian Group must define how to collect, store, and share compliance evidence (e.g., audit logs, activity reports, system configurations).

Several principles described above can be used to support the cloud provider selection by enabling the execution of meaningful due diligence evaluation of cloud services and providers.

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