LOGGING

APPROVED BY

PRYSMIAN S.p.A BOARD OF DIRECTORS

June 10, 2025

Code: PO-IT-I&C-SEC006

prysmian

The planet's pathways

TABLE OF CONTENTS

LEADERSHIP MESSAGE 2

1. *PURPOSE & OBJECTIVE* 3
2. *POLICY OWNER* 3
3. *APPLICABILITY* 3
4. *YOUR RESPONSIBILITY AS EMPLOYEE* 3
5. *GENERAL PRINCIPLES* 5
6. *CONSEQUENCES OF POLICY VIOLATION* 7
7. *REPORTING A POLICY VIOLATION* 7
8. *AUDIT, MONITORING AND CONTINUOUS IMPROVEMENT* 8
9. *RELATED DOCUMENTS* 9

APPENDIX A – DOCUMENT HISTORY 10

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 purpose of this document is to define the scope, the audience and general principles for the secure and effective collection and management of logs that can be produced by Prysmian Group's IT systems. 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)

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 administering the Group's systems and infrastructure components and for all the staff involved in log management 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

Systems and networks, while interacting with users or with other systems, record many kinds of events, from access to data transfer, and store them in a file named event log. There is a range of different event logs, such as transaction logs, activity logs, access logs, audit logs, and each one provides value to Prysmian Group thanks to the unique information stored in them. For example, log files can contain information useful to identify accesses to Prysmian Group's systems and platforms, modalities in which services and applications are used, state of Prysmian Group's resources in terms of integrity and availability, etc.
Specifically, event logging can support different key areas:

- Analysing threats: event logs can be used to analyse threats to system components such as attempting to modify system privileges, deleting critical files or downloading illegal material from a website. Periodical reviews and analysis of logs are beneficial for identifying security incidents, policy violations and fraudulent activities shortly after they have occurred, and for providing information useful for resolving such problems;
- Improving capacity planning: event logs can be used to help coordinate the effective utilisation of IT resources, thereby helping to ensure the availability of important system components;
- Supporting forensic investigation: event logs can be used to support forensic investigations and identify operational trends by determining unusual activity that have been performed and their duration;
- Complying with legislation and regulation: event logs can be used to help meet legal and regulatory mandates that lay down certain priorities such as the monitoring of system components and retention of data.

A key role in supporting an effective Information Security strategy is played by security event logging, which is the logging mechanism by which records of events are generated and stored for analysis of security breaches.

The collection and management of logs must be carried out in accordance with the following general principles.

- Prysmian Group must determine systems and system components on which event logging must be enabled (e.g. server, workstation, database, firewall, critical business applications, systems that are subject to legal or regulatory obligations).

For each identified log source, Prysmian Group must define which types of events must be logged (e.g. security-related, transaction, usage) and related attributes. Log sources must be configured so that they capture the necessary information in the desired format and locations.

Automatic mechanisms capable to report the presence of errors during the log generating phase must be considered.

- Because logs contain records of system and network security, their confidentiality and integrity must be protected from breaches and incidents. Log sources that are not properly secured (e.g. that use an insecure transport mechanism) are more susceptible to intentional or unintentional log configuration changes and log alteration. To this aim, unauthorized parties must not have access to log files and they must not be able to rename, delete or perform other file-level operations on log files. Unauthorized parties must also not be able to manipulate log source processes, executable files, configuration files or other components of the log sources and of the log management infrastructure that could affect logging activities. In general, Prysmian Group personnel, while using logs, must be mindful of the trustworthiness of each log source (e.g. particular attention must be paid to the accuracy of logs produced by hosts that have been attacked successfully).
- Availability of logs must be guaranteed. Prysmian Group must configure the size of the logs considering the constraints given from the specifications of the systems, in order to meet data retention and availability requirements. When the size limit is reached, the log might overwrite old data with new data or stop logging, both of which would cause a loss of log data availability. In order to prevent this situation, Prysmian Group must also define mechanisms for storing logs exceeding the storage capabilities of the systems (e.g. use other

supports, bigger in size, to store old data for the needed period of time or send log to central collection systems). Moreover, the log management process and capabilities must be robust enough to handle not only expected volumes of log data, but also peaks of data during extreme situations (e.g. widespread malware incident, penetration testing, vulnerability scans). Availability of the logs must be ensured also with the adoption of a backup policy.

- Logs must be reviewed and analyzed regularly (e.g. every week) with the goal of eventually gain an understanding of the baseline of typical log entries and detect potential anomalies in the normal operations of the systems. To this aim, Prysmian Group ensures that logs related to user activities are processed according to the applicable laws and regulations (e.g. Privacy law). During log analysis, relevant events that necessitate a fast response, such as incidents and operational problems, can be identified and eventually trigger the Security Incident Management process.
- For each log, or log category, Prysmian Group must determine a retention period, according to internal and external regulations and business requirements. At the end of the retention period, Prysmian Group must ensure that the archived logs are properly destroyed.
- Prysmian Group should adopt a centralized log management tool in order to facilitate log analysis, monitoring and backup activities.

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
4. "Security Incident Management Policy" document
5. "Security Incident Management Procedure" 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