



CYBERSECURITY

Insight

TIM Group

2026 June



INDEX

1. Cybersecurity at the heart of our commitment to a reliable and secure digital environment ...	3
2. Our Cybersecurity Governance System	4
3. The Regulatory and Institutional Framework for Cybersecurity	6
4. Our Cybersecurity Policy	7
5. Our Cybersecurity Management System	9



1. Cybersecurity at the heart of our commitment to a reliable and secure digital environment

We are the leading telecommunications provider in Italy and among the leaders in Europe. This position gives us a unique perspective on cyber threats. Every day, we monitor and analyze hundreds of events to prevent or contain attacks, working tirelessly to protect the network infrastructure, data centers, cloud platforms, and digital services of the TIM Group and, of course, our customers.

We have specialized and coordinated internal units, such as network security, Cyber Security Operations Centers (Cyber SOC), and companies like Telsy. This ecosystem allows us to closely monitor the evolution of threats that indiscriminately affect citizens, businesses, and institutions.

We also monitor developments in the regulatory and institutional landscape regarding cybersecurity to understand how defenses are being strengthened and what measures are being introduced at the European and national levels to enhance our ability to prevent and counter the increasing frequency of attacks.

We believe in a digital world that is reliable and secure. That is why we are committed to fostering a genuine culture of cybersecurity, one that is accessible even to non-experts. For this reason, in 2025, we published the 2024 Cybersecurity Report in collaboration with the Cybersecurity Foundation, Italy's first nonprofit foundation dedicated to the digital realm.

In 2025, the TIM Group also strengthened its oversight of information security and data protection issues within its Internal Control and Risk Management System (SCIGR), integrating these aspects among the key ESG risks monitored by governance bodies and Enterprise Risk Management processes.



2. Our Cybersecurity Governance System

To ensure the protection of our infrastructure and the data we process from cybersecurity risks, we operate through a structured and consistent governance system, which establish individual responsibilities for information security for the entire workforce.

The Board of Directors is responsible for strategic direction and oversight, including in the areas of internal control and risk management. In this context, it defines the guidelines for the Internal Control System and verifies its adequacy, effectiveness, and proper functioning, ensuring that the company's main risks—including those related to cybersecurity and data protection—are properly identified, assessed, and managed over time. To this end, the Enterprise Risk Management model adopted enables risks to be identified, assessed, and managed in a consistent manner throughout the Group.

At the overall governance level, in carrying out its responsibilities for strategic direction and oversight—which extend to matters of control and risk management—TIM's Board of Directors has established an internal committee focused on controls and risks (the Control and Risk Committee). The Control and Risk Committee is a subcommittee of the Board composed solely of independent directors. The Committee performs investigative functions to support the Board in its assessments and decisions regarding the control and risk management system, to which it regularly reports on its activities.

In 2025, the Board of Directors further strengthened its oversight of ESG matters and information security risks, highlighting cybersecurity, data protection, and regulatory compliance as among the key risks being monitored. Its areas of responsibility also include risks related to cybersecurity and privacy—fields in which the Committee Chair has solid operational experience.

The Chief Executive Officer (CEO), in accordance with the Board of Directors' guidelines, is responsible for establishing and ensuring the proper functioning of the internal control



and risk management system. The CEO is also responsible for governance regarding information security and cybersecurity, including the management of related risks.

By delegation of the Board of Directors and with the approval of the Government Authority, the CEO holds exclusive authority as the Director for Security Organization, in accordance with the “Golden Power” regulations. These regulations require close collaboration with the government on issues related to the security of strategic communications infrastructure and mandate the strengthening of internal security controls.

In 2025, the Internal Control and Risk Management System was further consolidated through coordination among Enterprise functions.

In particular, the Chief Security Office, which is responsible for Physical and Cyber Security across the TIM Group, through the organizational units within his Department—which include Cyber Security and the Security Officer (FAS), ensures comprehensive oversight of security matters, in line with the Golden Power regulations and under delegation from the Board of Directors. The Chief Security Office serves as the single point of contact for all security-related issues, supervises measures for the prevention and mitigation of cyber risks, reports directly to the Chief Executive Officer, briefs the Control and Risk Committee, and acts as the liaison with Institutional Authorities.



3. The Regulatory and Institutional Framework for Cybersecurity

As a strategic operator for the country, TIM operates within a particularly complex national and European regulatory framework regarding cybersecurity, critical infrastructure security, digital resilience, and personal data protection.

The Golden Power decrees, introduced in 2017, establish specific obligations for companies operating in strategic sectors such as telecommunications, requiring the adoption of dedicated security and control measures and specific reporting obligations to the government authority.

Decree-Law 21/2022, issued in the context of the Ukraine crisis, further strengthened the special powers of the Presidency of the Council of Ministers and introduced more stringent requirements for the security of 5G networks, which are considered critical infrastructure of national interest.

The implementation of the measures provided for by the legislation is subject to review by a Monitoring Committee established within the Office of the Prime Minister, which is tasked with verifying compliance with regulatory obligations and, where necessary, imposing sanctions.

Starting in 2021, the regulatory framework was further consolidated with the implementation of Law 133/2019, which established the National Cybersecurity Perimeter (PSNC), aimed at ensuring high levels of protection for operators managing ICT services essential to national security, including TIM.

Another key development in the regulatory landscape is European Directive 2022/2555 (NIS2), which entered into force in January 2023 and will be applicable as of October 18, 2024. This directive significantly expands the scope of the regulations on the security of networks and information systems, covering both sectors previously governed by other



regulations and new entities, including data centers and Content Delivery Networks (CDNs).

The Directive introduces stricter requirements regarding cyber risk management, supply chain security, operational resilience, cybersecurity governance, and the management and reporting of cyber incidents, while maintaining the obligation to adopt security measures commensurate with the risk and introducing basic minimum requirements. In the event of non-compliance, penalties of up to 2% of annual revenue may be imposed. NIS2 also strengthens supervisory bodies and activities at the European level and collaboration among Member States, including through the sharing of experiences in combating cyber threats.

Regulatory developments in the areas of cybersecurity, digital resilience, and compliance represent one of the key elements considered in the Group's governance and risk management processes.

The National Cybersecurity Agency (ACN) also operates within this context, with the task of monitoring, coordinating, and strengthening the country's resilience in the face of evolving cyber threats. TIM also maintains constant and structured collaboration with institutions, participating through its specialized departments in working groups at institutional bodies, including the Prime Minister's Office, the Ministry of the Interior, and the Ministry of Defense.

4. Our Cybersecurity Policy

Information security is a central element of the TIM Group's governance model, and the related policy applies to all corporate functions, processes, technologies, and assets that process information on behalf of the Group.

The information security policy defines principles, objectives, roles, and responsibilities aimed at ensuring confidentiality, integrity, availability, and protection of corporate



information and personal data, promoting an approach focused on continuous improvement and formalizing management's commitment to compliance with security requirements.

During 2025, the Group further strengthened the integration between cyber risk management, ESG governance, and internal control systems, ensuring the full integration of information security processes into governance, internal control, and risk management systems.

The policy applies to all corporate assets and involves the entire Group workforce, which is called upon to actively contribute to achieving security objectives through conduct consistent with corporate policies and applicable regulatory requirements, as well as by implementing security measures within their purview.

Through its Information Security Policy, TIM is committed to:

- define processes, roles, and responsibilities related to information security;
- ensure a level of confidentiality, integrity, availability, and protection commensurate with the business value of the information and the potential losses resulting from security incidents;
- raise awareness and train staff on cybersecurity issues;
- monitor, analyze, and manage any incident—even a suspected one—related to information security;
- define specific cybersecurity requirements for suppliers and other external parties;
- promote the continuous improvement of information security systems through collaboration with national and international organizations and institutions and the sharing of methodologies and best practices.
- conduct analysis for defining, identifying and prioritizing vulnerabilities in computer systems, applications, and network infrastructures.



In its relationships with suppliers and partners, the Group establishes specific requirements and contractual clauses designed to ensure the protection of information and intellectual property, regulatory compliance, adequate security levels, incident management, and the ability to conduct audits and monitoring. These requirements also cover the adequacy of the skills of the personnel involved, business continuity plans, service levels, and related penalties, which are aligned with or more stringent than those established for customers.

5. Our Cybersecurity Management System

To achieve the objectives set forth in the information security policy, the TIM Group has adopted an Information Security Management System (ISMS) based on structured processes for prevention, monitoring, risk management, and continuous improvement.

The system includes:

- a business continuity plan dedicated to cybersecurity and integrated into the Group's broader business continuity system, designed to safeguard the operation of critical processes in the event of incidents that could compromise service delivery. The plan includes procedures to prevent potential threats, limit and mitigate their impact, and restore processes;
- activities to detect, analyze, and manage cybersecurity vulnerabilities, aimed at preventing and reducing security incidents;
- IT infrastructure assessments designed to evaluate its compliance with internal regulatory frameworks, applicable regulations, adopted standards, and implemented security requirements;
- third-party audits of the Information Security Management System. In this regard, it should be noted that the Group has obtained ISO 27001 certification (valid until 06/12/2026);
- training programs for all TIM Group personnel, designed to raise awareness of information security;



- an escalation process for managing reports of incidents, vulnerabilities, or suspicious activity, collected by Group personnel and handled by the relevant departments.

Throughout 2025, the Group further strengthened its corporate risk monitoring and reporting processes, ensuring regular information flows to top management, the Control and Risk Committee, and the Board of Directors, including with regard to cyber risks and the resilience of digital infrastructure.

Cybersecurity activities also include the continuous monitoring of security events and the timely management of incidents through preventive and corrective technical and organizational measures aimed at protecting personal data and information assets and countering cyber threats, process vulnerabilities, and cyberattacks, including DDoS attacks.

To support these activities, the Group provides information tools and awareness initiatives for employees, designed to promote informed behavior consistent with information security requirements.

The effectiveness of the measures adopted is verified through specific systemic and operational Key Performance Indicators (KPIs), periodic internal and external audits, and structured Impact Analysis & Risk Assessment processes designed to evaluate the impacts resulting from the loss or compromise of information and systems and to identify priorities for action.

During 2025, a total of 22 events were confirmed, classified as IT breaches.