ITALMOBILIARE
INVESTMENT HOLDING

GUIDELINES

Information Security
Cyber Security

2026

Italmobiliare S.p.A.
REGISTERED OFFICE:
Via Borgonuovo 20, Milan
www.italmobiliare.it

Table of Contents

Information Security

PURPOSE

These guidelines identify the objectives and general principles that inspire Italmobiliare S.p.A. for the processing and protection of information within its organization, with the aim of supporting business needs, promoting compliance with applicable legal and regulatory provisions and guiding corporate risk management choices according to criteria consistent with industry best practices.

An inadequate level of information security can in fact lead to reputational, economic and competitive impacts, also related to the shutdown of activities, the possible application of penalties or sanctions and, more generally, the failure to monitor current regulations.

Information security requirements are therefore aimed at reducing the risks associated with information management to acceptable levels.

This document is intended as a general reference for the management of Italmobiliare S.p.A. Information Security. The Group companies may consider the principles and best practices referred to therein within the scope of their organisational and decision-making autonomy; The definition, approval and implementation of the relevant measures remain the exclusive responsibility of the bodies of each company.

OBJECTIVES

These guidelines are intended to provide a reference for the adoption of tools, measures and behaviours aimed at:

- Support the corporate strategy, enhancing information security as an enabling factor for the business;
- Safeguard the assets of Italmobiliare S.p.A., including from a financial, physical, reputational and intellectual property point of view;
- Ensure the availability, confidentiality and integrity of the information processed;
- Ensure compliance with current legislation and commitments made to third parties;
- Promote the continuity of services through the application of adequate security procedures;
- Promote the awareness of employees, collaborators and third parties with respect to their respective responsibilities;
- Facilitate the correct classification and protection of the information managed;
- Ensure secure access to company information, offices and premises;
- Prevent, classify, manage and promptly communicate anomalies, vulnerabilities and incidents that may affect information systems or corporate security levels.

SECURITY PRINCIPLES AND REQUIREMENTS

In order to protect the company's assets, the guidelines refer to the following **Security Requirements** as reference points:

- **Confidentiality**: information should only be accessible to authorised persons.
- **Integrity**: It is good practice to safeguard the completeness, accuracy and compliance of information throughout its lifecycle.
- **Availability**: it is appropriate to encourage, for authorised parties and when necessary, access to the information and technological tools necessary to manage it, consult its content and ensure its continuity of use.

The guidelines also refer to the following **Principles** as useful references to guide organizational and technical choices:

- **Need to Know**: Access should be limited to only the information necessary to perform the assigned task.
- **Segregation of Duties**: It is advisable to divide activities within business processes in order to help prevent fraud or errors.
- **Least Privilege Access**: It is recommended to grant the minimum set of privileges necessary, in terms of access to systems and information, for the performance of user tasks.
- **Security by Design**: It is good practice to consider potential vulnerabilities and their mitigation measures from the design of solutions and processes, as well as in the subsequent definition and implementation phases.
- **Security by Default**: By default, you should adopt security measures and configurations that are appropriate to your risk level and consistent with the most secure options available.

Italmobiliare S.p.A., within its organisation, undertakes to preserve the confidentiality, integrity and availability of all physical and electronic information resources under its responsibility.

Cyber Security

The following are the elements of good practice in each area relevant to IT security that each Group company can draw inspiration from, as a non-binding reference, in defining its cyber security strategies according to industry best practices and ensuring full oversight of the obligations provided for by the relevant legislation in force.

INTERNAL INFORMATION SECURITY PROCEDURES AND REGULATIONS

Define and maintain clear information security processes, roles and responsibilities, supported by up-to-date documentation, preferably approved by the competent bodies and subject to periodic monitoring.

SECURITY ORGANIZATION

Promote the definition of clear roles and responsibilities, facilitating the separation of potentially conflicting activities, such as request, approval, execution and control. Where necessary, it is also necessary to identify contact persons for relations with competent authorities and interest groups, as well as to maintain continuous monitoring of relevant threats, through strategic, tactical and operational intelligence activities.

PROJECT SECURITY

Consider information security early in the design of solutions, processes, and initiatives, including through early identification of risks and definition of applicable security requirements. This approach can also be a useful reference for projects involving external suppliers, providing, where appropriate, specific contractual clauses on safety. If significant risks emerge, consider the preparation of a dedicated protection plan, aimed at defining mitigation measures, responsibilities and monitoring methods during the project.

REMOTE WORKING

Identify specific security measures for remote work, aimed at providing addresses on applicable obligations and prohibitions, secure ways of managing access, use of company devices, use of trusted networks and protection of information from unauthorized access. These measures may include, where applicable, the use of solutions such as VPN, encryption and multi-factor authentication, as well as appropriate safeguards for backup, the timely revocation of access rights and the return of company assets at the end of the relationship or when no longer needed.

HUMAN RESOURCES

Promote structured processes for the selection and screening of new hires, as well as training initiatives, acceptance of company policies and signing of applicable confidentiality agreements. The HR Function can play a guiding role in promoting staff training and awareness of good information security practices, also providing suitable channels for reporting any breaches. Responsibilities regarding confidentiality and protection of information may remain even after the termination of the employment relationship, in accordance with the provisions of the applicable agreements and provisions.

ASSET MANAGEMENT AND INFORMATION CLASSIFICATION

Promote the census of assets and the information associated with them, identifying requirements, restrictions and access rights for each one consistent with the relative criticality and with the applicable classification level. For each phase of the information life cycle, from generation to classification, sharing, custody, archiving and destruction, identify appropriate security measures, such as password protection, secure custody, encryption and secure deletion, in order to promote consistent and continuous monitoring of the information processed.

Below are some good practices for the definition of the main technical safeguards.

Classification of Information

Adopt a classification taxonomy articulated on several levels, defined according to the sensitivity of the information and the potential impact deriving from unauthorized access, use or disclosure. Public information is intended for dissemination and does not require any particular restrictions. Basic measures should be taken for internal information, such as limited access to internal personnel, the use of corporate tools, and credential protection. For sensitive information, due to its criticality, it is recommended to adopt more stringent measures, including authorized access, use of controlled distribution lists, secure storage, secure printing, limitation of storage on unapproved devices and encryption. Strictly confidential information, having strategic or privileged importance, can be managed with enhanced safeguards, such as sharing limited to specific user lists, use of secure company systems, access tracking, confidentiality clauses and authorized maintenance interventions.

Use of Company Assets

Define rules of conduct and specific indications for the use of company assets and information, in order to promote their correct, safe and consistent use with work purposes. In particular, provide for the limitation of the unauthorized disclosure of information, the sending or management of illegal documents, the deactivation of antivirus safeguards, the installation of unauthorized software, as well as the unauthorized use of social media and unapproved file sharing services.

Credentials and Passwords

Define rules for assigning, using, choosing, and renewing passwords, including appropriate complexity policies and management methods consistent with the level of risk associated with the accounts and systems involved. In addition, provide for the timely modification of passwords in the event of suspected compromise, as well as the use of strong authentication mechanisms for access to applications, systems or services of particular strategic importance.

Collaboration and Communication Tools

Prioritise the use of approved corporate tools for collaboration and communication activities, in order to promote adequate levels of security, control and protection of shared information. Promote training and awareness-raising activities on the secure use of e-mail and electronic collaboration services, also with reference to the risks associated with phishing, unauthorized sharing of information and improper use of available tools. Where appropriate, adopt Data Loss Prevention solutions, aimed at preventing unauthorized or accidental disclosure of company data and information.

Malware Protection

Implement protection measures against malware, including antivirus solutions, spam filters, firewalls, and training and awareness-raising activities aimed at strengthening users' ability to recognize threats, suspicious messages, and potentially malicious sites. Define guidelines for the management of untrusted communications, attachments or links, including, among other things, the recommendation not to open or interact with such content, in order to reduce the risk of infection, compromise of systems or unauthorized access to company information.

Allowed Software

Provide for the use of only authorized software, through controlled installation, configuration and update processes. In addition, limit the unauthorized installation of software of any kind, in order to reduce the risk of introducing unapproved applications, technical vulnerabilities or components that are potentially harmful to the security of corporate systems and information.

Internet Access and Safe Browsing

Evaluate the implementation of web filtering systems and other browsing control measures, in order to reduce exposure to malicious content, unreliable sites or uses that are not consistent with the company's purposes. Awareness-raising activities aimed at users are also suggested, aimed at raising awareness of the risks associated with Internet access, including possible damage to company systems and information, as well as any personal liability deriving from non-compliant behavior.

Remote access

Adopt specific security measures for remote access to protect corporate information when connecting to systems, applications, and services outside the corporate network. Such measures may include, where applicable, the use of encrypted channels, VPN solutions and strong authentication mechanisms, as well as guidance on the secure use of public or uncontrolled networks, in order to reduce the risk of unauthorized access, interception or compromise of the information processed.

Mobile Device Management

Define rules for mobile device configuration, inventory, and management, including, where applicable, remote management, backup, mobile device encryption, and corporate data protection measures. In addition, regulate the conditions and methods of any use of personal devices according to BYOD models, promoting adequate levels of security, control and separation between corporate and personal information.

Social Networks and Artificial Intelligence

Define rules for the responsible use of corporate social networks and artificial intelligence tools, in order to prevent the unauthorized disclosure of confidential information and encourage a use consistent with the principles of security, fairness and responsibility. In particular, avoid the insertion of sensitive or confidential corporate data into unapproved artificial intelligence solutions, while providing for an ethical and conscious use of such tools and appropriate forms of human supervision over the content generated or processed.

Data breach, theft, loss management

Define procedures for the management of data breaches, thefts and losses, in order to facilitate timely reporting of events, a coordinated response and a correct assessment of impacts. These procedures may govern the methods of reporting, the possible activation of the obligations provided for by the GDPR and internal regulations, as well as the involvement of the functions responsible for the management of risk analysis, communication and mitigation activities.

- **Controls and Disciplinary Actions**

Provide for security monitoring systems, in compliance with the principles of transparency, proportionality and minimisation, in order to detect any anomalous behaviour, violations or non-compliant use of company resources. In the event of serious or repeated violations of safety rules, the introduction of appropriate disciplinary actions may be considered, in accordance with the provisions of applicable legislation, employment contracts and internal regulations.

- **User data processing and Record Retention**

To retain user data for a limited period that is proportionate to the purposes of the processing, in compliance with the defined data retention criteria and the applicable legislation on the protection of personal data. In addition, provide for methods of management, archiving and deletion consistent with the principles of minimization, limitation of storage and security of the information processed.

- **Cybersecurity Awareness**

Provide periodic training, updating and awareness-raising activities aimed at employees on the main IT security issues, in order to strengthen risk awareness and promote behaviour consistent with company policies. Such activities can include simulated phishing campaigns, informational communications, in-depth materials and initiatives aimed at promoting the recognition of threats and the correct management of corporate information.

ACCESS CONTROL

Define structured processes for the management of logical and physical access, promoting the correct governance of digital identities, the assignment and periodic verification of access rights, as well as the supervision of privileged users. In addition, provide strong authentication mechanisms and relevant action tracking systems where applicable to help protect information, systems and corporate environments from unauthorized access.

ENCRYPTION

Define rules for the encryption of devices, information and communication channels, in proportion to the level of classification and criticality of the information processed. In addition, manage cryptographic keys according to recognized criteria, ensuring their protection, availability and control throughout their entire lifecycle. Finally, where necessary, the use of digital signatures or other equivalent mechanisms is recommended to promote authenticity, integrity and non-repudiation of relevant information and transactions.

PHYSICAL AND ENVIRONMENTAL SECURITY

Adopt physical and environmental security measures aimed at protecting IT assets and the spaces in which they are located, through physical access controls, monitoring of sensitive areas, Clean Desk and Clear Screen rules and safeguards against environmental threats, accidental events and disasters. Such measures may also govern, where applicable, the protection of off-site assets and the secure disposal of equipment, in order to help prevent unauthorized access, damage, loss of availability or undue exposure of information.

SECURITY OF OPERATIONS

Overseeing the security of operations through organizational and technical measures aimed at promoting the correct functioning, protection and continuity of IT resources. In particular, provide for formalized and updated operating procedures for the secure use of company resources, structured change and configuration management processes, continuous capacity monitoring activities, safeguards for malware protection and system updating, as well as backup, logging and monitoring procedures for relevant events. In addition, regulate the installation of software, the management of technical vulnerabilities, patch management, the secure deletion of information and the possible use of data masking techniques in non-production environments, finally evaluating the adoption of suitable measures to prevent data leakage through classification tools, DLP, firewalls, antivirus and intrusion detection systems.

COMMUNICATIONS SECURITY

Oversee the security of communications through technical and organizational measures aimed at protecting company networks, communication services and information transferred or shared. These measures can promote adequate levels of control, confidentiality and traceability, including, where applicable, the management and monitoring of corporate networks, logical segregation, the use of firewalls and network access control solutions, as well as safeguards for the secure management of network services. In addition, adopt web filtering tools, awareness-raising initiatives on the responsible use of the Internet, indications for the secure transfer of information in digital, physical or verbal format and specific confidentiality agreements for the protection of classified information.

SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE

Manage the acquisition, development, and maintenance of systems by integrating security requirements throughout the application and infrastructure lifecycle, from the analysis and definition of requirements to development, testing, release, maintenance, and evolution. In this context, identify security requirements based on a risk assessment, apply the principles of Security by Design from an early stage, and facilitate the separation of development, test, and production environments. In addition, regulate secure development through defined procedures, even when entrusted to external suppliers, providing, where appropriate, for security testing, the use of secure repositories and data protection measures in test environments, such as data masking techniques.

RELATIONS WITH ICT SUPPLIERS

Manage relationships with ICT suppliers through structured processes of selection, contractualization, monitoring and review, promoting a clear definition of roles and responsibilities, the acceptance of security requirements extended to the entire ICT supply chain and the periodic control of compliance with them, also with reference to cloud services. The assessment of suppliers can take into account skills, certifications, ability to ensure business continuity, right to audit, as well as ethical and sustainability requirements. In addition, regulate in the contracts the prevention and management of security incidents, the processing and protection of data, confidentiality obligations, the management of sub-supplies, the possible application of penalties and the methods of termination of the relationship, including the return of data and secure deletion.

INFORMATION SECURITY INCIDENT MANAGEMENT

Support the management of information security incidents with a structured process, aimed at facilitating the timely identification of events, the correct assessment of their severity and the coordination of response, recovery and closure activities. To this end, clearly identify the contact person for incident management and, where necessary, a dedicated response team, as well as define roles, responsibilities and methods for rapid reporting of incidents. Incidents can be assessed and classified according to priority and impact, managed according to predefined phases, tracked through special registers and treated with adequate levels of confidentiality, also through the use of secure channels and specific responsibilities for the personnel involved. Finally, the evidence collected and the lessons learned can be a useful reference for updating policies, procedures and knowledge bases, contributing to the continuous improvement of security safeguards.

SECURITY IN BUSINESS CONTINUITY

Define security and business continuity requirements aimed at promoting the resilience of ICT services and systems, based on business needs and the results of any Business Impact Analysis. To this end, periodically develop, maintain and test Business Continuity and Disaster Recovery plans, providing redundancy and resilience measures for IT systems, such as alternative contracts, separate data centers and duplication of critical components. ICT response planning may also include establishing consistent recovery objectives, such as RTOs and RPOs, as well as periodically verifying the effectiveness of the measures taken.

COMPLIANCE AND AUDIT

Manage compliance and audit activities through a coordinated set of measures aimed at facilitating compliance with applicable legal, regulatory, statutory and contractual requirements, as well as the proper protection of relevant evidence and records. In this context, overseeing the processes relating to the protection of personal data, privacy and intellectual property, ensuring that the operating methods are adequately defined, communicated and understood by the data subjects. In addition, provide for independent audits, internal controls and periodic compliance checks, including through vulnerability assessment and, where appropriate, penetration tests.

Scope

This document has been adopted by Italmobiliare S.p.A. with exclusive reference to its own organisation and applies only to its personnel, processes, information, assets, information and network systems, as well as to its suppliers. It is not binding on subsidiaries and investee companies and is only a tool for sharing general principles and best practices in the sector. Each Group company defines, approves and implements in full autonomy, through its own administrative bodies and structures, policies, measures and investments in the field of information security, and independently assesses the applicability of cybersecurity legislation (including Legislative Decree 138/2024, transposing Directive (EU) 2022/2555 – NIS 2), autonomously fulfilling the related obligations.

In particular, Italmobiliare S.p.A. does not take decisions, nor does it influence decisions, relating to the IT security risk management measures of the Group companies; does not own or manage the information and network systems of the Group companies; does not carry out IT security operations on their behalf, nor does it provide them with ICT or security services; it does not supervise or verify the IT security measures of its subsidiaries or investee companies and does not issue adjustment plans or corrective actions. Any information flows to and from Italmobiliare S.p.A. for corporate, financial or investment evaluation purposes do not entail powers of use, control or intervention in the field of IT security and do not affect the autonomy of the companies concerned.

In order to maintain its effectiveness over time and to align it with organisational, technological and regulatory developments, this document may be subject to periodic revision or updating. Revisions and updates to this document are effective only within the organization of Italmobiliare S.p.A.

Revisions

Issue date	Redacted	Verified	Approved	Issued
30 Jul 2026	Information System ITM	Information System ITM	Human Resources ITM	Human Resources ITM

Rev.	Rev. Date	Revision Description