ITALMOBILIARE
INVESTMENT HOLDING

Cyber Security Framework of Italmobiliare Group

Summary document

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

Sommario

The Cyber Security Framework

The Italmobiliare Group has adopted a Security Governance Framework consisting of a collection of documents designed to guide the main macro-domains of information security and cyber security. This Framework aims to define rules, measures, and principles applicable to all group companies, customizing them according to local and business-specific characteristics, while always remaining consistent with central principles and objectives.

The Framework provides a structured and comprehensive detailing of all policies, processes, technical, organizational, and behavioral rules necessary for the centralized and widespread management of information security and cyber security within the Italmobiliare Group, in accordance with best practices and in compliance with international standards and current regulations.

The program includes periodic reviews to ensure effectiveness, adaptability, and relevance. It has been developed to protect the information and assets of the group, minimizing economic, reputational, and legal risks while ensuring regulatory compliance.

The Framework currently consists of the following documents:

- Information Security Policy
- Glossary
- Information Security Regulation
- Regulation on Information Classification and Asset Management
- Regulation for ICT Supplier Management
- Regulation for Information Security Incident Management

Information Security Policy

The first document of the Framework is the "Information Security Policy".

This policy, in addition to introducing the Framework, defines its purpose, main guiding principles, objectives, and scope of application.

The "Information Security Policy" is presented in its entirety in the second part of this document.

Glossary

A comprehensive section of definitions clarifies all key terms: from asset and system administrator to data breach, malware, endpoint, ICT function, GDPR, security incidents, KPI/KSI, least privilege access, legal entity, threat, security measure, multi-factor authentication, penetration test, phishing, privacy, remote working, data controller, user, vulnerability, etc.

Information Security Regulation

The regulation highlights the role of information as a crucial asset and the management of security as an enabling factor for business. It also makes clear that compromising confidentiality, integrity, and availability (CIA) can have critical impacts.

The regulation establishes minimum security rules, adaptable by each group company according to its own specific needs, and it is inspired by international standards (ISO/IEC 27001/27002, NIST, National Cybersecurity Framework).

Areas of information security covered:

- Internal procedures and regulations
- Security organization
- Human resources
- Asset management
- Access control
- Encryption
- Physical and environmental security
- Operations security
- Communications security
- Acquisition, development, and maintenance of systems
- Supplier relations
- Incident management
- Business continuity
- Compliance

For ease of use, to further explore some of the topics listed above, the regulation relies on the following three in-depth documents:

- Regulation on Information Classification and Asset Management
- Regulation for ICT Supplier Management
- Regulation for Information Security Incident Management

The regulation is mandatory for all group-controlled companies and may be voluntarily adopted by affiliates.

The main measures contained in the regulation and related documents are described below.

Internal Information Security Procedures and Regulations

Each company must implement clear processes, roles, and responsibilities, maintain up-to-date documentation approved by management, and monitor it periodically. The effectiveness analysis of the adopted security measures must be tracked and periodically shared with the parent company.

Security Organization

Roles and responsibilities must be identified, conflicting activities segregated (request, approval, execution, control), contacts with authorities and interest groups defined, and constant intelligence on threats, both strategic, tactical, and operational, must be maintained.

Project Security

Information security must be considered from the design phase, identifying risks and requirements, including through collaboration with external suppliers, and including specific security clauses in contracts. If risks emerge, a specific protection plan must be prepared.

Remote Working

Security measures for remote work are detailed, including obligations, prohibitions, access and device management, restrictions on the use of unsecured networks, protection of information from unauthorized access, backups, access rights revocation, and asset return. Technical measures such as VPN, multi-factor authentication, antivirus, and encryption are listed.

Human Resources

Defines selection and screening processes for new hires, training obligations, and policy acceptance, confidentiality agreements. The HR function must ensure that all staff are trained and aware of good security practices, with channels for reporting violations. Responsibilities may continue even after termination of employment (e.g., post-relationship confidentiality agreements, information transfer).

Asset Management and Information Classification

Each company must register assets and associated information, defining requirements, restrictions, and access rights. The regulation details the lifecycle management of information (generation, classification, sharing, custody, archiving, destruction), indicating measures for each phase (password protection, secure custody, encryption, secure deletion).

Information Classification

A four-level taxonomy is proposed:

- Public: Intended for disclosure, no restrictions.
- Internal: Necessary for normal operations, where unauthorized disclosure would cause minor damage. Measures: access restricted to internal staff, use of company tools, credential protection, etc.
- Confidential: Critical information, where disclosure can cause significant damage. Stricter measures: authorized access, distribution list, secure storage, protected printing, prohibition of storage on unauthorized devices, encryption.
- Strictly Confidential: Of strategic/privileged relevance, where leaks can cause severe damage. Measures: sharing only with user list, secure company systems, tracking, confidentiality clauses, authorized maintenance.

Use of Corporate Assets

Defines behavioral rules and prohibitions for the use of assets and information, including: prohibition of unauthorized disclosure, sending illicit documents, disabling antivirus, installing unauthorized software, unauthorized use of social media and unapproved file sharing services.

Credentials and Passwords

Strict rules for assignment, use, choice, and renewal of passwords, obligation to change password in case of suspected compromise, strong authentication protection for strategic applications.

Communication Tools and DLP

Obligation to use only approved corporate tools, recommendation of DLP solutions, training on safe use of email and electronic collaboration services.

Malware Protection

Mandatory use of antivirus, antispam filters, firewalls, training on threat recognition, prohibition of opening suspicious emails/sites.

Permitted Software/Installation

Only authorized software and strict installation and update processes, prohibition of unauthorized installation of any kind of software.

Internet Access and Safe Browsing

Implementation of web filtering systems, awareness of damage risks and personal responsibilities.

Remote Access

Requirement to protect information through encryption, strong authentication, VPN, caution in using public networks.

Mobile Device Management, BYOD

Rules for configuration, inventory, remote management, backup, encryption of portable devices, prohibition of BYOD use unless explicitly authorized.

Social Networks and Artificial Intelligence

Rules for responsible use of company social networks, prohibiting the disclosure of confidential information. Recommendations on ethical and responsible use of AI, absolute prohibition of entering sensitive company data into non-approved AI solutions, obligation of human supervision.

Data Breach, Theft, Loss Management

Detailed procedures for reporting, response, evaluation, notification, and possible initiation of procedures required by GDPR and internal regulations.

Controls and Disciplinary Actions

Security monitoring systems are foreseen, in compliance with transparency and proportionality principles, and possible disciplinary actions in case of repeated or serious violation.

User Data Processing and Record Retention

Limited retention of processed data over time, in compliance with data retention criteria and privacy regulations.

Cybersecurity Awareness

Employee training and updates on security topics, simulated phishing campaigns, informational material.

Access Control

Definition of processes for regulating logical and physical access, identity management, periodic verification of access rights, management of privileged accounts, obligation of strong authentication and logging of key actions.

Encryption

Adoption of rules for encrypting devices and communication channels proportionate to the information's classification level, key management in line with best practices, and use of digital signatures for authenticity, integrity, and non-repudiation.

Physical and Environmental Security

Protection of the physical space of IT assets, physical access controls, monitoring of sensitive areas, protection against environmental threats and disasters, management of the security of off-site assets, and secure disposal of equipment.

Clean Desk and Clear Screen Policies

Policies for keeping desks clear and devices protected, secure storage of documents and removable media, protected printing, deletion of data from whiteboards and other display tools.

Operations Security

- Documented procedures for the safe and proper use of IT resources.
- Change and configuration management.
- Resource capacity management.
- Protection against malware and constant system updates.
- Backup procedures, testing, and safe storage of copies.
- Logging and monitoring of relevant events, system clock synchronization.
- Software installation performed only by authorized personnel.
- Technical vulnerability management through assessment and patch management.
- Secure information deletion and data masking for non-production/test environments.
- Prevention of data leakage through solutions like classification, DLP, firewall, antivirus, and IDS.

Communications Security

- Management and control of corporate networks, segregation through VLAN, use of firewalls and network access control.
- Secure management of network services, logging of service usage activities.
- Web filtering and awareness on responsible Internet use.
- Rules for transferring information (digital, physical, verbal).
- Confidentiality agreements to protect classified information.

Acquisition, Development, and Maintenance of Systems

- Definition of security requirements for applications and systems, determined through risk assessment.
- Application of Security by Design principles and separation of development/test/production environments.
- Management of secure development, including outsourcing, security testing, use of secure repositories, and consideration of data masking for test environments.

ICT Supplier Relations

The regulation governs the selection, contracting, monitoring, and review of ICT suppliers, including:

- Definition of roles and responsibilities (contact person, asset owner, privacy coordinator, etc.).
- Security requirements to be accepted by suppliers, extended throughout the ICT supply chain.
- Monitoring of relationship changes, compliance with security requirements even for cloud services.
- Supplier evaluation based on skills, certifications (ISO 27001, 27017, 27018, 27701, CSA STAR, etc.), business continuity management capacity, audit rights, ethical and sustainability requirements.
- Negotiation and formalization of contracts including rules for security incident prevention, data management, confidentiality standards, subcontracting management, audit rights, penalties, and termination rules (data return, secure deletion, etc.).

Information Security Incident Management

- Identification of a contact person and, if needed, an incident response group (with ICT and security expertise).
- Definition of internal rules, roles and responsibilities, and methods for the rapid reporting of security events.
- Method for evaluating and classifying incidents by priority and impact (Critical, High, Medium, Low), with a description of impact and urgency.

- Details of incident management phases: identification, analysis, classification, escalation, response and recovery, closure, and lessons learned.
- Incident tracking via Track Record including details such as date, description, actions taken, escalation, closure, root cause analysis.
- Confidential management of incident information, use of secure channels, responsibility of involved personnel, possible specific confidentiality agreements.
- Lessons learned from incidents and updating of policies and the knowledge base.

Business Continuity Security

Definition of requirements for business continuity, development and testing of Business Continuity plans, Disaster Recovery, redundancy of IT systems (multiple contracts, separate data centers, duplication of hardware components, etc.). Planning of ICT response and determination of RTO/RPO based on Business Impact Analysis.

Compliance and Audit

- Identification, updating, and compliance with legal, regulatory, statutory, and contractual requirements, including privacy and intellectual property.
- Protection of evidence and records, including the management of custody chains and record categorization.
- Processes for the protection of personal data (GDPR) and effective process communication to all relevant parties.
- Independent and internal audits of information security. Obligation of periodic compliance tests (vulnerability management and penetration tests).
- Protection of information systems during test and audit activities through appropriate tools, logging, and contractual compliance.

ITALMOBILIARE
INVESTMENT HOLDING

INFORMATION SECURITY POLICY

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

INFORMATION SECURITY POLICY

INDEX

Introduction

Italmobiliare S.p.A. (hereinafter "Italmobiliare" or "the Holding") has established a program of actions aimed at formalizing a Security Governance Framework, applicable both to Italmobiliare and its subsidiaries and affiliates (hereinafter collectively "the Italmobiliare Group" or "Group"), with the purpose of adequately protecting information and corporate assets. The objectives are to set out the basic rules and measures in the fields of information and cyber security to be observed in all activities carried out by the Legal Entities (hereinafter "LEs")[1] of the Group.

In this context, the Holding, in keeping with its governance role, defines the strategic direction, while each Group LE analyzes and contextualizes the established rules locally—potentially differing according to their relationship with the Holding (e.g., depending on whether they are a subsidiary or an affiliate) and specific business characteristics—providing periodic monitoring on the status of the Information Security System.

The Security Governance Framework is a set of documents aimed at addressing the macro-domains of security/cyber security (e.g., security objectives, asset management, information classification, user governance, secure development, ICT supplier management, incident management, business continuity, etc.). Each LE must adopt the guidelines contained therein, tailoring them to its own context but always respecting the principles and objectives outlined in the document.

To ensure its effectiveness, the framework may be subject to periodic review or updating.

COMMITMENTS

The function managing IT Services (ICT Function) in the various companies of the Group is committed to preserving the confidentiality, integrity, and availability of all physical and electronic information resources. Inadequate information security can lead to reputational damage, financial losses due to business interruptions or penalty payments, competitive disadvantage, as well as possible sanctions in relation to current regulations.

The information security requirements are intended as a mechanism to reduce the risks associated with information management to acceptable levels.

[1] Legal Entity, meaning the companies controlled by the Holding and the companies in which Italmobiliare owns shares

Purpose

This policy describes the objectives and general principles that the Group must adopt in handling information in order to support business needs and ensure compliance with legal or regulatory requirements and risk management choices. The document serves as a guiding regulation to support Information Security Management within the Group.

PRINCIPLES AND SECURITY REQUIREMENTS

In order to safeguard corporate assets, the policy provides for the adoption of the following **Security Requirements**:

1. **Confidentiality**: information must be available only to those who are authorized to access it.

2. **Integrity**: it is necessary to safeguard the completeness, accuracy, and compliance of the information throughout its entire lifecycle.

3. **Availability**: access to information and associated architectural elements must be ensured for authorized individuals whenever requested.

Furthermore, the following **Principles** are adopted:

4. **Need to Know**: access should be limited solely to information that the user needs in order to perform the tasks assigned to them.

5. **Segregation of Duties**: activities within a company process should be divided to prevent fraud or errors.

6. **Least Privilege Access**: it is necessary to grant the minimum set of privileges possible (access to systems and information) for the user's activities.

7. **Security by Design**: from the earliest design phases of a solution, as well as in all subsequent definition and implementation phases, potential vulnerabilities and security measures aimed at mitigating them must be considered.

8. **Security by Default**: the most secure security measures and configuration settings possible should be determined and chosen “by default.”

Objectives

Through the principles defined in the Security Governance Framework, this Information Security Policy is aimed at directing and providing tools to:

a. Support corporate strategy by making information security one of the key factors for business success;
b. Protect the Group's assets in their financial, physical, intellectual property, and reputational aspects, ensuring the availability, confidentiality, and integrity of managed information;
c. Comply with current regulations and security commitments established in contracts with third parties;
d. Ensure continuity of services through the application of established security procedures;
e. Ensure that employees, collaborators, and third parties are well informed about information security practices and aware of their responsibilities in this area;
f. Enable full knowledge of managed information and assess its criticality, to facilitate the implementation of appropriate levels of protection;
g. Guarantee secure access to information, company premises, and individual company facilities to prevent unauthorized or improperly authorized processing;
h. Prevent, classify, manage, and correctly communicate any anomalies, vulnerabilities, and incidents with impacts on the information system and the company's security levels.

APPLICATION SCOPE

This Policy applies to all processes and to all resources, both human and instrumental assets (including external ones), involved in the management of information handled by the Italmobiliare Group.

In particular, the recipients of this document are:

1. The management levels of the Group's companies, which adopt the Policy and ensure adequate commitment and the necessary resources to enable the effective implementation of the principles defined herein;
2. Group employees, who are responsible for implementing the provisions of this Policy within their respective areas of responsibility;
   - Employees of companies controlled by Italmobiliare Investment Holding, in a binding manner;
   - Employees of associated companies, in the form of strategic guidance / guidelines;
3. Third parties who, due to relationships with Group companies, may have access to the company's information assets.

Revisions

Issue date	Redacted	Verified	Approved	Issued
01/12/2023	Information Systems ITM	Information Systems ITM	Human Resources ITM	Human Resources ITM

Rev.	Rev. Date	Revision description