Information Security Policy of BFF Bank S.p.A. and BFF Banking Group Abstract

Policy BOD approval date 19/12/20

Table of contents

Introduction

1. The Information Security Policy governs the responsibilities and modalities for the Management of Information Security adopted by *BFF Banking Group* (hereinafter the "Group"), in compliance with, but not limited to, the provisions set out primarily in Bank of Italy Circular 285/2013 (in particular the 40th update), ESMA Guidelines for Cloud Outsourcing, Regulation (EU) 2016/679 (GDPR) and EU Regulation 2022/2554 (DORA).
2. The principles governed by the Policy refferd are applicable to *BFF Bank* S.p.A. (the "Bank", the "Parent Company"), its Branches and Subsidiaries.
3. The Information Security Policy has also been drafted in compliance with the main provisions of (but not limited to):
   - Legislative Decree 27 January 2010, amended by Legislative Decree 218/17 transposing Directive (EU) 2015/2366 of 25 November 2015 (PSD2) and concerning payment services in the internal market;
   - Delegated Regulation (EU) 2018/389 of 27 November 2017 and subsequent amendments and supplements with regard to Strong customer authentication and common and secure open standards of communication;
   - Circular 285/13 (40 update);
   - regulation EU 2022/2554 (Digital Operational Resilience Act – DORA) and associated delegated Regulations, with particular regard to Delegated Regulation 2024/1774 (RTS on ICT risk management and security tool, methods, processes, policies), in order to protect the Group's Information Assets by defining guiding principles and general criteria, in line with the Group's Strategy and in compliance with current regulations, at the basis of an effective Information Security Management System (ISMS).

Policy approval and update

Detailed description about the process of reviewing, updating and approving this policy.

Definitions

This section lists and specifies the meanings attributed to certain technical or recurring terms in the policy, in order to avoid interpretative ambiguities and ensure terminological consistency.

Body policy introduction and objectives

1. Information is an essential asset for BFF Banking Group to provide its activities and as such needs to be adequately protected. The information managed concerns significant aspects such as transactions, contracts, confidential client and personnel data. Given their importance for the Business, the Policy details the technical and organisational security measures aimed at protecting information from unauthorised or accidental changes, loss and unauthorised disclosure.

2. The first and second level risk analysis is the basis of the Policy and is necessary in order to understand vulnerabilities and compliance violations, assess possible threats and prepare the necessary countermeasures. The objective is to manage risk to an acceptable level through the design, implementation and maintenance of
the Information Security Management System (ISMS) in line with the ICT and Security Risk, defined and approved by the Board of Directors in the context of the Risk Appetite Framework.

3. The Policy establishes the following principles to protect the company's Information Assets:

- confidentiality: all information is protected from improper access and is used only by authorized persons;
- integrity: each information is the one that was originally entered into the computer system or was modified in a legitimate way by authorised persons whose activities are tracked in the system;
- availability: availability of the information in relation to the requirements of continuity of service provision and compliance with the rules requiring its secure storage;
- authenticity: the information received corresponds to that generated by the person or entity that transmitted it;
- compliance: the processing of information is carried out in compliance with the laws in force, sector regulations and self-regulatory codes in the areas in which they are applicable;
- verifiability: events associated with the use of the information system and the processing of data can be reconstructed, if necessary and also ata distance of time;
- Accountability: each operation is attributable to persons (users or applications) who are univocally identifiable;
- non-repudiation: information is protected against false denial of receipt, transmission, creation, transport, delivery and receipt.
- agility: ability to replace information technology (ICT) within reasonable time and cost constraints in case of changes to the external environment or business requirements.

4. The Information Security Policy's objectives established by the Parent Company are:

i. ensuring that staff and collaborators have adequate knowledge and awareness of the problems connected with information security and of the technical and organisational rules adopted in the use of information systems, in order to enable them to acquire sufficient awareness of their own responsibility for the processing of such information;

ii. ensuring that all external suppliers are aware of the importance of information security for the Bank and comply with the adopted Security Policy;

iii. establishing guidelines for the application of standards, procedures and systems to realise the Information Security Management System (ISMS), in order to duly and adequately protect all Group's information assets and ICT resources, including software, hardware and servers, as well as all related physical infrastructures and components, such as premises, data processing centres and areas designated as sensitive, so as to ensure suitable levels of confidentiality, integrity and availability for all information assets and resources and adopt mitigation measures against risks, including damage and unauthorised access or use through security measures that are appropriate and proportionate to the criticality of processes and assets;

iv. assigning responsibilities to the appropriate levels of the company and Group organisation for the implementation of the guidelines described in this document, set out in appropriate operating procedures and internal regulations and ensuring alignment with the security objectives stated in the bank's operational and digital resilience strategy;

v. transposing the provisions of the prevailing regulations concerning ICT and security, including by using the Standards ISO 27001 "Information Security Management Systems - Requirements" and ISO 27002 "Code of practice for information security management" as support for the implementation of the Information Security Framework (ISMS) and compliance with the rules and regulations to which the Bank and the Group are subject;

vi. ensuring that staff, collaborators and suppliers, each to the extent of their competence, correctly apply the operating procedures and security measures established by the Bank to protect data, including personal and payment data, and resources.

All the Group's staff and, where applicable, third-party suppliers, must be made aware of and apply the internal regulations concerning the security of information, according to their remit. Moreover, all staff is required to report, using the applicable channels, anomalous conduct or facts which could represent a security breach.

Chap.1 - organizational aspects of security

Actors and roles

The company figures/functions involved in security management at the Parent Company are:

- Board of Directors;
- Chief Executive Officer;
- Security;
- ICT;
- Projects;
- Human Resources & Organization;
- Facilities;
- ICT and security risk control;
- Compliance & AML;
- DPO;
- Internal Audit.

For the purposes of the Policy, branches are considered part of the Parent Company.

The board of directors

The Board of Directors (BoD) is the body with strategic supervisory functions, responsible for the direction and control of the information system, with a view to the optimal use of technological resources in support of the Bank's strategic objectives and ICT strategy, in consideration of the reference sector evolution and in line with the evolution of the Bank's operations sectors, processes and organisation. In particular, in the context of the Information Security Policy, the BoD:

- Approves the Policy as well as the other corporate documents for the management and control of the IT system (i.e. the strategic guidance document, the ICT and security risk analysis methodology, the ICT function's organisational chart, the ICT adequacy and cost summary report, the IT risk situation summary report, the reports of the Internal Audit and other functions

responsible for security assessment).

- Approves and periodically reviews internal ICT audit plans, ICT audits and major changes thereto.
- Approves and periodically reviews the policy on the modalities to use the ICT services provided by the third-party ICT service provider. In case of full outsourcing of the information system, the Board of Directors, if it does not have the necessary internal expertise, may use external resources independent of the service provider.
- Establishes communication channels at company level enabling it to be duly informed about the following:
  - the agreements entered into with third-party ICT service providers on the use of such services;
  - possible related and important changes envisaged with regard to third-party ICT service providers;
  - the potential impact of such changes on essential or important functions subject to the agreements in question, including a summary of the analysis carried out to assess the impact of such changes, as well as at least serious operational and safety incidents and their impact, response and recovery measures and remedial actions.
- Approves the Bank's organizational and governance structure with reference to the information system, ICT and Security Risk Management and Business Continuity, ensuring the clear distinction of tasks and responsibilities of the Corporate Bodies and Functions.
- Establishes appropriate governance mechanisms to ensure effective and timely communication, cooperation and coordination between all ICT-related corporate functions.
- Takes ultimate responsibility for the Bank's IT risk management.
- Has overall responsibility for defining and approving the digital operational resilience strategy.
- Keeps actively up-to-date in terms of appropriate knowledge and skills to understand and assess IT risks and their impact on the financial entity's operations, including by undergoing specific training on a regular basis, commensurate with the IT risks managed.
- Allocates and periodically reviews adequate financial resources to meet the Bank's digital operational resilience needs with respect to all types of resources, including relevant ICT security awareness programmes and operational and digital resilience training activities, as well as ICT skills for all staff.
- Is informed:
  - at least once a year on the adequacy of the services supplied and on the support of these services to the evolution of the company's operations in relation to the costs incurred;
  - periodically on the application and adequacy of the action plans to implement the ICT strategy;
  - promptly in case of serious business problems deriving from incidents and malfunctions of the information system, and is updated on the impact, corrective measures and additional controls following such events;

- periodically, and where appropriate, on the launch and progress of ICT projects, considered individually or in aggregate and depending on their size and importance and the risks associated therewith.

- Ensures that the ICT and security risk governance and control system is constantly adequate, also in terms of qualitative and quantitative sizing of personnel and available financial resources, to the operational needs of the ICT Function and the processes for the management of ICT and Security Risks and for the implementation of the ICT strategy.
- Defines and approves the development strategies for the information system, based on the evolution of the reference sector and in accordance with strategic guidelines and the existing and structure of the operating sectors, processes and corporate organization; in this context approves the reference model for the architecture of the information system. Formalises the ICT strategy; by defining:
  - How the corporate ICT system should evolve to effectively support and contribute to the corporate strategy, including the organisational structure evolution, changes in ICT systems and key dependencies on third parties;
  - The ICT architecture planned evolution, including dependencies on third parties;
  - Clear information security objectives, especially with regard to ICT systems and services, personnel and processes.
- Takes into account the Bank's information security objectives when approving the information system's architectural reference model.
- Promotes the development, sharing and updating of Security Awareness knowledge within the company.
- Approves *(i)* action plans prepared by the Chief Executive Officer for the implementation of the ICT strategy, *(ii)* the information security Policy; *(iii)* the guidelines for the selection of staff with technical functions and the acquisition of ICT systems, software and services, including through the use of external suppliers and Outsourcing.

- With specific regard to the exercise of supervisory responsibility for ICT and Security Risk analysis and management, the Board of Directors:

- approves the reference organisational and methodological framework for the management of ICT and Security Risk, promoting the appropriate valuation of technological risk information within the ICT function and integration with risk measurement and management systems (in particular, operational, reputational and strategic). The reference framework is reviewed at least annually, also in light of the experience gained during its implementation and monitoring, with a view to continuous improvement;
- approves the ICT and Security Risk appetite, having regard to internal services and those offered to clients, in accordance with the risk objectives and risk appetite framework defined at corporate level;
- is informed, in a clear and timely manner, and in any case, at least annually, of the ICT and Security Risk situation with respect to the risk appetite, including the risk assessment outcomes;
- ensures that the ICT and security risk governance and control system is constantly adapted, also in terms of qualitative and quantitative staffing and available financial resources, to the operational needs of the ICT function and the ICT and security risk management processes and for the implementation of the ICT strategy.

The Chief Executive Officer

The Chief Executive Officer is the body with management functions, assuming the task of ensuring completeness, adequacy, functionality (in terms of effectiveness and efficiency) and reliability of the information system. Specifically, in the context of this document, the Chief Executive Officer:

a) defines the action plans containing the measures to be adopted to achieve the ICT strategy objectives, monitors and measures their effectiveness, and periodically reviews them to ensure their adequacy and consistency with the company strategy over time, informing the Board of Directors in this regard. Furthermore, it ensures that the content of the action plans approved by the Board of Directors is communicated to all relevant personnel, including third parties where appropriate;

b) defines the organisational structure of the ICT Corporate Function, ensuring the correct sizing of its resources (human and financial) over time, as well as compliance with the strategies and architectural models as defined by the Board of Directors;

c) defines the roles and responsibilities for the ICT Corporate Function and for the management of ICT and Security Risk, as well as for related business continuity activities;

d) defines the organisational, methodological and procedural framework for the ICT and Security

Risk management process, pursuing an appropriate level of liaison with the Risk Management Function for operational risk estimation processes;

e) ensures that all personnel, including personnel in key roles, receive adequate training in ICT and Security Risks and information security, at least once a year or more frequently if necessary; in this regard, it defines and approves an information security training and awareness plan;

f) approves ICT operations management procedures and processes, concerning resources and services that have not been outsourced, guaranteeing the effectiveness and efficiency of the system, as well as its overall completeness and consistency, with specific regard to a functional allocation of tasks and responsibilities, the soundness of controls, and the validity of methodological and procedural support;

g) approves data governance standards, change and incident management procedures (where appropriate, in conjunction with the service provider's procedures), and in general ICT operations management procedures and processes; approves, normally on an annual basis, the operational plan of IT initiatives, verifying their consistency with the information and automation needs of business lines as well as with corporate strategies;

h) assesses, at least annually, the ICT performance with respect to the strategies and objectives set, in terms of cost/benefit ratio or using integrated performance measurement systems, taking appropriate actions and initiatives for improvement;

i) approves, at least annually, the critical components' risk assessment (ICT and Security Risk Situation Summary Report), as well as the ICT services adequacy and costs report, informing, in this regard, the Board of Directors; in this context, it checks the overall ICT and Security Risk situation in relation to the defined risk appetite, having, for this purpose, appropriate Information Flows concerning, at least, the residual risk level for the various IT resources, the implementation status of risk mitigation measures, the evolution of threats associated with the use of ICT, as well as incidents recorded during the reference period;

j) monitors the smooth running of ICT services management and control processes and, if anomalies are detected, implements appropriate corrective actions;

k) makes timely decisions on serious operational or IT security incidents, of which it is promptly informed, and provides information to the Board of Directors in the event of serious problems for the company's business deriving from incidents and malfunctions, with specific reference to the impact, response and additional controls to be defined.

Security

The Security function cooperates with the ICT and security risk Control Function in drafting and updating the Policy. In particular, in the context of this document, the Security Area:

- Supervises the correct implementation and maintenance over time of the Information Security Management System at the Group level, ensuring consistency of security safeguards, defined and mapped by it, allocating responsibilities, with existing policies and procedures and tracking exceptions.
- Performs the IT risks technological assessment for identification and mitigation and cooperates in the risk monitoring activities carried out by the ICT and security risk Control Function, to which it provides the outcomes of the assessments performed (e.g.: VA/PT, specific security alert analyses, system and endpoint security status investigations, etc.).
- Handles relations with telecommunication operators and relevant service providers, as well as annually verifying with the Head of Business Continuity Management the validity of the ICT Business Continuity (including the response & recovery plans) and Disaster Recovery plan and updates them according to the outcomes of tests carried out while providing appropriate feedback on the results to the ICT departments, in order to achieve the operational and digital resilience objectives set out in the respective strategy. In this context, monitors the actual implementation of corrective measures that have been identified.
- Gives its opinion on the introduction of new services or tools for processing corporate information with regard to the suitability of security mechanisms, indicating possible additional requirements or specific security measures/tools to be adopted, monitoring their implementation.
- Defines and implements security tests on new services that are developed and carries out periodic scans and security tests on ICT resources, documenting results and monitoring recovery plans; plans and carries out threat-led penetration tests (TLPT), documenting results and monitoring recovery plans.
- Cooperates to the implementation of ICT projects by assessing possible security risks introduced and indicating possible additional requirements or specific security measures/tools to be adopted, and monitoring their implementation.
- In relation to the ongoing monitoring carried out on the areas of competence, reports possible emerging and relevant criticalities, threats or risks to the ICT and security risk Control Function.

- Informs the ICT and security risk Control Function of any activity or event that materially affects the Bank's risk profile, significant operational or security incidents, as well as any material changes to ICT systems and processes.
- Supports the Parent Company's Business Continuity Manager in carrying out the activities within his remit. Takes care of the implementation and monitors the KRIs defined by the ICT and security risk Control Function on an ongoing basis, reporting thereto on a quarterly basis.

ICT

The ICT function is responsible for carrying out information system operational processes in accordance with the security policies defined in this document and in compliance with the procedures defined within the ISMS. In particular, in the context of this document, the ICT O.U.:

- Adopts internal regulations with the aim of governing processes and activities in accordance with the provisions of this Policy.
- Ensures the application of the rules concerning the information system, i.e. in relation to information and communication technology resources, ensuring an adequate level of security to guarantee information protection.
- Is responsible for software developments and the selection and implementation of software packages created by third parties (including standard software purchased from the market). In these contexts, it adopts suitable processes and instruments for ensuring the quality and security of the code, as well as compliance with functional and non-functional requirements established in the design phases of the solution;
- Is responsible for the implementation of ICT projects, with the governance of architecture evolution and technological innovation as well as with information system management activities, in line with the Bank's operational and digital resilience strategy;
- Performs the security checks of competence documenting the results of these, and ensures the implementation of any corrective measures that are identified;
- Informs the ICT and security risk Control Function of any activities or events that materially affect the Bank's risk profile, significant operational or security incidents, and any material changes to ICT systems and processes.
- Involves the Security function in order to identify suitable security measures in the technological and architectural context under management.

- Ensures suitable supervision of ICT suppliers within its remit, in line with corporate Policies and the applicable regulations.
- Actively involves the ICT and security risk Control Function in projects/activities involving substantial changes to the information system (to the extent of its remit) and, in particular, in the risk control processes relating to such projects, supports the Security function in implementing technological measures according to the principles of this Policy and in relation to its areas of competence.

Project

The Project function is responsible for the management of information and communication technology projects and for defining the guidelines to be adopted within the context of the governance of projects, including for the purpose of ensuring greater integration between project activities, ICT and the business and the governance of this area in line with the security policies defined in this document. Specifically, in the context of this document, the function:

- Is responsible for project governance and control, with specific reference to the engagement of the Security and ICT functions, especially in the initial project demands assessment phase and during project implementation.
- Collects security-related evolutionary needs from business users or on the basis of indications from other involved functions.
- Plans and collects budget requirements to execute security activities.
- Governs and monitors ICT changes. To this end, it ensures that the projects, and in general all the initiatives within its remit, have correctly formalized the functional and non-functional requirements necessary for the completion of ICT projects, irrespectively of whether these are related to business initiatives; it also ensures that all project risks are identified and their mitigation is tracked, as set forth in the corporate procedures.
- Actively involves the ICT and security risk Control Function in projects/activities involving substantial changes to the information system (to the extent of its remit) and, in particular, in the risk control processes related to such projects.
- Oversees ongoing update activities of the register of ICT supplies, ensuring the completeness thereof.

Human Resources & Organization

In the context of this document, the Bank's Human Resources & Organisation function:

- prepares Awareness activities, supported by the Security, on the basis of the information security training and awareness plan and promotes awareness-raising and updating activities on security issues and related responsibilities through specific annual training programmes;
- during the personnel life cycle ensures the audit of reliability (backgorund check), Awareness and compliance with information security requirements by personnel.

Regulation & processes

Is responsible for mapping the documentation which makes up the Information Security Management System and for keeping this map updated, while stating the updating responsibilities.

Facilities

The Facilities function is responsible for physical security and governance and management aspects:

- defines the physical security rules with the coordination of Security;
- governs physical access and authorizations to the CED and backup vaults for both employees and external staff;
- takes appropriate security measures to protect buildings (e.g. video surveillance systems, alarm devices, etc.;
- constantly monitors access and regulates access of both internal staff (on the basis of the tasks performed) and external staff;
- carries out testing and periodic maintenance of intrusion detection systems;
- activates the incidents, weaknesses or defects reporting procedure in case of a malfunctioning of physical security measures.

ICT and Security Risk Control

The ICT and security risk control function is a second-level control function responsible for managing, supervising and monitoring ICT and Security Risks, as well as verifying adherence of ICT operations to the ICT and Security Risk Management System. Specifically, in the context of this document, the ICT and security risk Control Function:

- contributes to the definition of this Policy and is informed of any activity or event materially affecting the Bank's risk profile, significant operational or security incidents, as well as any substantial changes to ICT systems and processes;
- is actively involved in information system substantial change projects and, in particular, in the security risk control processes related to such projects;
- monitors the ICT and security risk trends through information in reports;
- in relation to the risks that are identified, suggests areas of improvement or corrective actions.

Compliance & AML

The Compliance & AML function verifies, for the profiles within its remit, that internal regulations are compliant with external regulations, identifying, where appropriate, areas for adjustment in relation to new and/or changed regulations.

Internal Audit

The Internal Audit function has the specialist skills necessary to perform its assurance tasks relating to the corporate information system (*ICT Audit*). In particular, in the context of this document, the Internal Audit Function:

- Assesses the adequacy, overall reliability and security of the ICT Audit information system, in accordance with the principle of proportionality, also in relation to the Bank's activities and organisational structure relating to ICT profiles, and any significant changes thereto, also expressing assessments on the main identifiable technological risks and the Bank's overall IT risk management.
- Reviews, at planned intervals or following significant changes, the safety management model to verify the adequacy of measures taken and to assess possible improvement measures.
- Has audits conducted on the implementation of ICT response and recovery plans;
- Conducts audits on the overall framework for the management of information risks.

Staff of the Bank and the Group

All staff of the Bank and the Group are required to comply with the principles of this document, Information Security Policy and related procedures in relation to their duties and responsibilities, as defined herein.

Upon the termination of their employment relationship, members of staff are required to return, in accordance with the procedures notified from time to time, the ICT resources assigned to them and the information assets in their possession belonging to the Bank or the Group.

For the purposes of security governance, the additional corporate policies and procedures specifically governing Privacy and personal data breach issues are described, inter alia, in the Group Policy for the Management of Personal Data Breaches, and in the Group Policy for the protection of data from the design stage through default protection procedures (Privacy by Design – Privacy by Default) which, where necessary, are linked to the processes defined in this Policy through appropriate specifications in the ISMS procedures (e.g. the principle of privacy by design in the design of ICT systems and services, and the management of data breaches as a particular category of security incidents). The specific rules concerning the security of payment services are instead included in the Information Security Policy. The Security function contributes to the definition of the necessary security measures and monitors that the security measures set out for each area are correctly and fully implemented when a service is introduced or changed.

For Subsidiaries the actors and roles involved in security management are, as the case may be:

- Boards of Directors*:* apply the Information Security Policy and information system development strategies, including operational and digital resilience strategies, to the extent of their remit; transpose the organisational and methodological framework for ICT and Security Risk management, *ICT* and Security Risk appetite and ICT and Security Risk analysis methodology approved by the Parent Company. The Parent Company's Board of Directors is responsible for allocating adequate financial resources for training and awareness plans, to meet the Bank's and the Group's digital operational resilience needs, to implement the Information Security Policy and information system development strategies. Furthermore, Group companies notify the Parent Company of their financial needs for initiatives in this area as part of the drafting and approval process of the Group's annual or multi-year budget; the Parent Company ensures that these resources are adequate to achieve the objectives.
- *Chief Executive Officers*: approve and monitor the procedures drawn up locally and their application, in line with the guidelines adopted by the Parent Company, relating to the Information Security Management System. The Parent Company's Regulation & Processes O.U. is in charge of monitoring the procedures issued by the Subsidiaries in order to verify compliance

with the Group's drafting standards.

- Compliance & AML function and, where present, the local contact persons: verify, according to their remit, the presence of any specific aspects of national/local law with regard to the issues in the Information Security Policy, for both the Bank and the Group.
- *Risk Management* / Compliance & AML functions and, where present, the local contact persons: transpose and adopt the reference organisational and methodological framework for the management of the Parent Company's ICT and Security Risk; view the outcomes of the Business Impact Analysis within their remit.
- *Internal Audit functions* and, where present, the local contact persons: perform assurance tasks pertaining to the corporate information system (ICT Audit) and are responsible for third level audit and control activities pertaining to security.
- *ICT functions* through the coordination and direction of the Parent Company's ICT: prepare ICT structures and processes in line with locally applicable regulations and the guidelines and procedures issued by the Parent Company; adopt the management strategies, policies and procedures defined by the Parent Company regarding ICT; where necessary, they adopt local procedures. Ensure that the development of corporate systems and applications complies with the guidelines on software and hardware architecture governance and development and change management defined by the Parent Company; manage and develop the implementations required in the context of Group ICT projects; transmit to the Parent Company's ICT and Security functions the information flows of competence, as defined by the Group regulations or upon request of the Control Functions. They monitor the regular performance of *ICT* services management and control processes and, in the event of anomalies detected, implement appropriate corrective actions; as regards serious operational or security incidents, provide timely information to the Parent Company's *ICT function* in order to initiate escalation activities deriving from serious information system operational or security incidents, according to the procedure defined by the Parent Company.

  Employees assigned to activities with privileged functions on information systems are identified as System Administrators by the Department's Privacy Coordinator.
- The BC (Business Continuity) Manager of the Parent Company presides over and coordinates the entire Business Continuity management cycle for the Group in accordance with the BCM methodology defined at Group level. He/she is in charge of drafting, reviewing and updating the BCM methodology at Group level, assisted by the Security Area, as well as of updating and verifying the Business Continuity plans.

Separation of duties

Detailed description about the measures in place to ensure and monitor compliance with the principle of Separation of Duties to ensure adequate segregation between execution and control responsibilities, in order to reduce the risks of unauthorized changes and misuse of information and information services.

Contacts with the authorities

This section outlines how the Bank's and Subsidiaries' internal regulations assign responsibilities for managing relations with public authorities, entities, regulatory bodies and telecommunication operators, etc.

Chap.2 - Scope of the information security management system

This Policy is intended to define general principles and rules of relevance to the Group, with respect to the following areas:

- Security as part of human resources management
- Management of company inventories
- Logical access control
- Cryptography
- Physical and environmental security
- Ict operations security management
- Security of telecommunication networks
- Acquisition, development and maintenance of information systems
- Relations with suppliers
- Operational or security incidents management
- Security aspects in business continuity management
- Compliance
- Specific rules for the security of payment services

Security as part of human resources management

Human Resources plays a fundamental role in safeguarding the organization by ensuring that every stage of the employee lifecycle supports a secure working environment. Detailed description about the measures in place to ensure this before, during, at the termination pr change of the employment.

Management of company inventories

This section outlines the principles and measures governing the identification, tracking, protection, and disposal of all organizational assets, during the whole asset lifecycle, in order of safeguarding organizational assets, further detailing Asset Classification Types and Responsibilities, Information classification and management, Assets use and protection.

Logical access control

Detailed description about the principles and mechanisms used to regulate access to the organization's information systems, applications, and data, specifically for managing the lifecycle of authentication credentials and authorisation profiles, from initial assignment, to management of changes, in correspondence with changes in the company role or needs, up to temporary deactivation or termination in the event of termination of the employment relationship. Through these controls, the policy ensures that information assets are accessible only to authorized individuals and that access is managed in a secure, controlled, and auditable manner.

Cryptography

Detailed description about the organization's requirements for the use, management and protection of cryptographic controls to safeguard the confidentiality, integrity, and authenticity of information, establishing the cryptographic mechanisms to be implemented in accordance with approved standards, using algorithms, key lengths, and protocols that meet recognized industry or regulatory requirements.

Physical and environmental security

Detailed description about the controls required to protect the organization's facilities, infrastructure, and physical assets against unauthorized access, environmental hazards, and operational disruptions, etc. preventing any damage resulting from natural events or from human intervention, whether deliberate or accidental, and in relation to the level of criticality attributed to the information managed.

ICT Operations Security Management

This section outlines the principles, responsibilities, and controls governing the secure, reliable and orderly operation of the organization's information and communication technology (ICT) environment, dealing with ICT operational processes and procedures management, ICT change management, segregation of operating and test environments, capacity and Performance management, protection from malicious software and security monitoring, information backup and availability of services and data, recording and monitoring of security events (log), systems security audit, Technical vulnerability management, etc.

Security of Telecommunication Networks

Detailed description about the controls required to protect the organization's network infrastructure and the information transmitted across it from unauthorized access, interception, disruption or manipulation, dealing with network segmentation, encryption, monitoring and intrusion detection, resilience and availability, etc.

Acquisition, development and maintenance of information systems

Detailed description about the requirements and controls that ensure information systems are planned, designed, implemented, and maintained in a secure and controlled manner throughout their entire lifecycle. It typically establishes that security must be integrated into all phases of system development, ranging from initial requirements analysis to deployment, maintenance, and eventual decommissioning.

Relations with suppliers

Detailed description about the measures in place to establish the security requirements governing the selection, engagement, monitoring, and management of third-party entities that provide goods or services to the organization, also taking into account the relevant regulatory provisions, in order to guarantee the security of assets and instruments used to process information accessible to suppliers and other third parties.

Operational or security incidents management

Detailed description about the measures in place for identifying, reporting, assessing, responding to, and resolving incidents that may impact the organization's operations or information security, taking into account the relevant regulatory provisions applicable. Through these measures, the policy ensures that operational and security incidents are managed consistently, efficiently, and in a way that minimizes their impact on the confidentiality, integrity, and availability of the organization's systems and data.

Security aspects in business continuity management

Detailed description about the measures in place to integrate information security considerations into the organization's business continuity and disaster recovery processes, dealing with compliance, governance and technological requirements; with the aim of ensuring that business continuity management maintains robust security protections during disruptive events, enabling the organization to recover operations in a secure, controlled and resilient manner.

Compliance

In order to minimize the risk of criminal or administrative sanctions, significant operational or economic losses, as well as reputational damage, specific measures are put in place to ensure compliance with the provisions of law, regulations, contractual obligations, internal policies and any other applicable requirement relating to information security.

Specific rules for the security of payment services

Detailed description about the security controls and operational requirements necessary to protect financial transactions, payment data, and the systems that support payment services; describing the measures in place to carry out specific risk assessments, control and mitigate risks related to payment services, define, implement and govern security measures in payment services.