Document Type: *Policy*

ABSTRACT

ICT Security Policy

Competent Structure: CIO

Date: December 2021

Version 6

Internal Use Only

illimity Bank S.p.A

SUMMARY

Document Type	Policy	
Structure Responsible for the Document	CIO	
Contacts	CIO: Filipe Teixeira Filipe.Teixeira@illimity.com	
	Head of Operations: Luca Dozio Luca.Dozio@illimity.com	
Structures Involved in the Process of Sharing the Present Version	Compliance & AML; HR & Organization	
Recipients of the Regulation	**Parent Company**	**Other Companies**
	illimity Bank S.p.A.	Entities of the Banking Group
Version approved by	Chief Executive Officer	
Date of approval	13/12/2021	
Date of validity	14/12/2021	

ABSTRACT

VERSIONS

Name of regulation and version	Main changes	Approving body and date
ICT Security Policy V.1	Drafting of the document.	Board of Directors, 27 February 2019
ICT Security Policy V.2	Addition of technical annex no. 1 – Rules for the use of ICT systems and instruments.	Head of Digital Operations, 24 June 2019
ICT Security Policy V.3	Revision of the Policy for the new Group perimeter.	Chief Executive Officer, 15 November 2019
ICT Security Policy V.4	Revision of the technical annex of the Policy in order to have greater detail on the possibility of using banking instruments; revision of certain references in the legislative and regulatory section; extension of details and guidelines on ICT security in the interaction with third parties in selecting products and project development.	Chief Executive Officer, 23 September 2020
ICT Security Policy V.5	Revision of the paragraph *"Management of Business Assets"* in order to have greater detail on the means of sending corporate data outside the Group.	Chief Executive Officer, 24 September 2021
ICT Security Policy V.6	Minor operational refinements, preparatory to the publication on the institutional website	Chief Executive Officer, 13 December 2021

ABSTRACT

Contents

ABSTRACT

ABSTRACT

1 PURPOSE AND SCOPE OF APPLICATION

The ICT Security Policy establishes the objectives of the ICT security management process adopted by the Banking Group, in line with the propensity to ICT risk determined at a corporate level, and describes the general security principles inherent in the management of the ICT system as well as the roles and responsibilities connected with the organisational and methodological framework of the delegated ICT management processes to ensure a suitable level of protection.

The Policy additionally establishes the guidelines adopted for communicating with, training and raising the awareness of the various classes of users in the Banking Group's staff.

The Policy consists of a set of objectives, security principles and practices that the Banking Group adopts and includes in its operating procedures in an ICT security ambit to ensure the control and/or governance of the Group's ICT system.

In accordance with the established full outsourcing model, the Banking Group determines the objectives of the ICT security management process adopted by the Group, the guidelines to be followed and the responsibilities and guiding principles for achieving and maintaining an adequate level of security for the Group's ICT system, in line with the propensity to business risk, in compliance with the minimum requirements established at a corporate level and with the relevant laws and regulations and national and international standards of reference.

This approach enables the Banking Group to be able to constantly:

- meet its customers' needs;
- create value for its shareholders over time;
- provide a quality service, characterising its actions with professionalism, expertise, an understanding of the needs of every customer and transparency;
- ensure rigorous compliance with laws and regulations;
- enhance the professional and personal development of staff;
- safeguard the Group's reputation and assets.

The aim of creating and implementing ICT security processes and procedures is to direct the structures involved towards achieving the following objectives:

- safeguarding the confidentiality of information, avoiding unauthorised consultation and dissemination;
- assuring the integrity of the information managed by the systems and other ICT resources used in its processing in order to ensure its accuracy and consistency;
- assuring the availability of the ICT resources to ensure continuity of the provision of ICT/electronic services in accordance with the methods and timing pre-established by the contractually defined SLAs;
- assuring conformity and compliance with ICT security laws, abiding by mandatory data protection legislation and regulations such as the GDPR and Circular no. 285 of the Bank of Italy;
- ensuring the authenticity and origin of the data and keeping track of updates (non repudiation);
- ensuring the security of the Group's ICT system on the basis of the results of the risk analysis.

1.1 SCOPE OF THE DOCUMENT

The ICT system is a strategic resource within the Banking Group's assets and in as in the case of "tangible" assets must be suitably protected from risks that may cause economic damage, harm to the banking Group's image and/or jeopardise the proper functioning of business operations.

The Chief Executive Officer and all the business structures must therefore contribute and assist in achieving and maintaining an adequate level of ICT security.

This ICT Security Policy provides guidelines on the security of the business's ICT system and accordingly represents the principle means of communicating and sharing corporate directives on the governance of the ICT System by establishing:

- general security principles and criteria which must be guaranteed and complied with in the ICT security management processes;
- guidelines for satisfying the obligations imposed by the external laws and regulations on ICT security matters to which the Group is subject;
- the roles, responsibilities and personnel involved in ICT security management.

The guidelines described in this document are applicable to all the entities of the illimity Banking Group subject to the management and coordination of the Parent Company illimity Bank S.p.A., for the parts of respective competence and depending on the nature of the activity performed by each individual subsidiary. Group companies are accordingly required to incorporate these guidelines and revise their internal rules and regulations in accordance with the Parent Company's indications.

1.2 ALIGNMENT WITH THE ICT RISK MANAGEMENT PROCESS

The risk management process adopted by the Banking Group periodically assesses the ICT risks to which it is exposed and enables security measures and controls designed to reduce these to be identified, in relation to the objectives listed in the previous paragraph. This ICT Security Policy also provides guidelines regarding the results of such process.

Business information must be protected by adopting all the security measures considered necessary for mitigating the risks identified by the specific risk analyses.

The structure of the processes and the strength of the controls is made commensurate to the results of the risk analysis process. All risks not adequately mitigated by protection mechanisms must be brought to the attention of the Bank's corporate bodies, the Head of the function designated to supervise ICT risks or the Operating Unit, depending on the relative level of risk.

The management of ICT security facilitates the proper management of ICT risks by way of a suitable management of processes such as change management, incident management and business continuity management, in order to identify threat vectors and the vulnerabilities of processes and systems.

1.3 GENERAL PRINCIPLES

The main principles underlying and directing the Banking Group's on security management are based on the following criteria:

- confidentiality – protection of data from uses that are unauthorised and/or not in line with the classification level of such (e.g. data access by unauthorised parties, unauthorised communication of data);
- integrity – protection of data from unauthorised or undesired activities (e.g. voluntary or involuntary unauthorised modification of information);
- availability – protection of data from possible events capable of reducing the Group's ability to make such data available (e.g. inability to reach systems);
- compliance – data management in compliance with industry sector laws and regulations on security;
- non repudiation – the assurance that the people or processes that have given rise to the information are actually those recognised by the identification mechanisms;
- verifiability – the assurance that on occurrence, and also at a later date, it will possible to reconstruct events connected with the use of the ICT system and data processing;
- least privilege – the principle that establishes that every user or system administrator is only granted the authorisation strictly necessary for performing his assigned duties;
- segregation of duties – the principle that establishes that particularly critical operations are performed through the cooperation of several users or system administrators with responsibilities formally distributed;
- need to know – the means of regulating logical access to networks, systems and data bases on the basis of effective operating needs;
- zero trust- management of the perimeter that envisages entry barriers decreases because participation in the Group's ICT structure based on the unique identification of the parties involved is strengthened.

ABSTRACT

2 GLOSSARY

Definitions	
Asset	Any item that has a value for the organisation.
Authentication	Procedure for verifying the identity of a user by a system or service.
Authorisation	Procedure verifying whether a customer or another internal or external person is entitled to perform a certain action, e.g. to transfer funds or access sensitive data.
Backup	The act of saving ICT flows (programme libraries, procedures and data archives) and creating reserve copies to ensure that their ICT content is in any case available in the event the originals are destroyed.
Bank	illimity Bank S.p.A. with registered office at Via Soperga 9, 20127 Milan, Italy.
Chief user	Corporate figure identified for each system or application and formally assuming the responsibility, representing users and acting as representative in relations with the functions in charge of development and technical management.
Critical component of the ICT system	System or application with respect to which an ICT security incident may jeopardise the proper and secure performance of operating functions that are important for the Bank, such as the effective completion of the duties of the corporate bodies and control functions.
Disaster recovery	The set of activities designed to ensure availability and reinstate critical processes and ICT services in case of system interruption.
Encryption	Process of converting information to a codified format (encoding) that cannot be interpreted without performing a process of reconversion to the original format. This process is performed by using algorithms and an encoding/decoding password known as a Key.
Group	The Bank and the subsidiaries forming part of the illimity Banking Group registered in the Roll of Banking Groups.
ICT resource	An ICT asset that assists in the reception, filing, processing, transmission and utilisation of the information managed by the intermediary.
ICT risk	Risk of suffering economic losses, loss of reputation or loss of market share due to the use of Information and Communication Technology – ICT. In the integrated representation of business risks for prudent purposes (ICAAP), this type of risk is considered, from certain aspects, to be one of the operational, reputation and strategic risks.
ICT security incident	Any event, or series of connected events, not planned by the Bank, which affects its ICT resources and which i) has or could have a negative impact on the integrity, availability, confidentiality, authenticity and/or continuity of the intermediary's services or processes; or ii) in any case entails the breach of or imminent threat of the breach of business regulations and practices concerning the security of information (e.g. cyber fraud, attacks through internet and malfunctioning and disservices).

Incident	Any event not forming part of the ordinary operation of services, which causes, or may cause, an interruption to or reduction in the quality of such and which corresponds to a change of state that has relevance to the Bank's business activities.
Management Body	The corporate body, or the members of such, responsible for or delegated to perform - pursuant to the Italian civil code or provisions of the bylaws – ordinary management duties, understood as the implementation of guidelines approved as part of exercising the function of strategic supervision. In the current model adopted by illimity, this body is identified in the Chief Executive Officer (hereinafter also CEO) who, as head of the internal structure, participates in the management function.
Norms	Rules, directives and standards which, consistent with the Security Policies, must be followed to achieve the previously established security objectives. These should be considered to be a direct extension of the Security Policies.
Organisational structures (or Structures)	The types of organisational structure of which illimity's Organisation Chart is composed in which the detailed responsibilities are assigned as described in the "Organisational Structure Regulation".
Outsourcer	An external party instructed to perform a process, a service or an activity of the Bank on the basis of specific contractual agreements.
Outsourcing	An agreement in any form between the Bank and a service provider on the basis of which the provider carries out a process, a service or an activity of the Bank.
Password	A word or string of characters by means of which the mechanism for the authentication of a user of the ICT system can be actioned (certain recognition).
Personal data	Information relating to an individual, identified or identifiable, also indirectly, by referring to any other information, including a personal identification number.
Processing	Any operation or set of operations, which can also be performed without the aid of electronic instruments, concerning the collection, recording, organisation, retention, consultation, processing, modification, selection, extraction, comparison, use, interconnection, blocking, communication, dissemination, erasure and destruction of data, even if not held in a data bank.
Risk analysis	The set of activities designed to identify the possible risks (attacks and vulnerability) to which a system may be exposed with the aim of identifying security countermeasures to protect such system.
Security Manuals/ Procedures/ Operating Instructions	These provide a detailed description of the operating methods to be followed to implement a security norm or directive.
Serious ICT security incident	An ICT security incident leading to at least one of the following consequences: • high economic losses or prolonged disservices for the intermediary, also as the result of repeated incidents of a lesser size; • key disservices concerning customers and other parties (e.g. payment intermediaries or infrastructures); an assessment of the seriousness takes into consideration the number of potentially involved customers or counterparties and the amount at risk;

	• the risk of affecting the Bank’s ability to comply with the conditions and requirements of the law or those prescribed by supervisory regulations; • reputational damage in the event the matter enters the public domain (for example through the media or press agencies).
Strategic Supervision Body	The corporate body which – pursuant to the Italian civil code or the provisions of the bylaws – has responsibility for directing business operations by, for example, examining and approving business or financial plans or strategic operations. This body is identified as the Board of Directors.
User	The person creating or using the information on the basis of authorisation to do so.

ABSTRACT

ABSTRACT

3 ROLES AND RESPONSIBILITIES

The preparation and upkeep of the ICT Security Policy involve the following Business Structures, which play an active role in the processes of directing, managing and controlling the security of the ICT System.

3.1 BOARD OF DIRECTORS

As the strategic supervisory body defined in Bank of Italy Circular no. 285, the Board of Directors is responsible for the direction and control of the ICT system. In this respect:

- it approves the development strategies of the ICT system;
- it approves this ICT Security Policy
- it approves the guidelines on selecting the personnel with technical functions and functions regarding the purchase of systems, software and services, including the use of outside suppliers[1];
- it fosters the development, sharing and updating of ICT know-how within the Group;
- it is informed on a timely basis in the event of serious problems for business activities caused by incidents or the malfunctioning of the ICT system;

With specific regard to its responsibility for supervising the analysis of the ICT risk, the board:

- approves the organisational and methodological framework for analysing ICT risk;
- approves the propensity to ICT risk;
- is informed on at least an annual basis about the ICT risk situation with respect to risk propensity.

3.2 CHIEF EXECUTIVE OFFICER

As the body with the management function, as determined by Bank of Italy Circular no. 285, the Chief Executive Officer has the duty of ensuring the completeness, adequacy, functionality and reliability of the ICT system. More specifically, he:

- establishes the organisational architecture of the ICT Structure ensuring that it corresponds over time to the determined strategies and models;
- establishes the organisational, methodological and procedural structure for the ICT risk analysis procedure, in conjunction with the business function delegated to manage risk;
- approves all the Banking Group's ICT documentation, also in connection with the procedures for service providers, ensuring consistency with ICT and business requirements as well as with business strategies;
- assesses, at least on an annual basis, the performance of the ICT function with respect to the set strategies and objectives, in cost/benefit terms or by using integrated performance measurement systems, taking the appropriate measures and initiatives for improvement;
- approves, at least on an annual basis, the assessment of the risk of critical items as well as the report on the adequacy and costs of ICT services, in this respect informing the body with a strategic supervision function;
- monitors the proper performance of the ICT services management and control processes and, in the event of any identified anomalies, puts appropriate corrective measures into practice;
- takes timely decisions with respect to serious ICT security incidents.

3.3 ICT FUNCTION

The organisational structure of the Banking Group's ICT function, which includes the function delegated to manage ICT security, is based on criteria of functionality, efficiency and security, determining duties and responsibilities by taking factors into account such as the complexity of the corporate structure, size, the sectors of activity and business and operational strategies. More specifically, the ICT function:

- follows the preparation and updating of the security policy and operating instructions;
- ensures consistency of security controls with the approved policies;
- participates in the design, realisation and maintenance of the data centre's security controls;
- participates in the design of the Bank's applications software;
- participates in the assessment of the ICT products supporting the Bank's processes;
- participates in the assessment of potential risk and the identification of security controls as part of the ICT risk analysis process;
- ensures the constant monitoring of the threats regarding the various ICT resources;
- follows the performance of the security tests carried out before a system enters production.

[1] In this respect see Bank of Italy Circular no. 285/2013, First Part, Title IV, Chapter VI.

In performing the above activities of its competence, the ICT function – by way of the function delegated to manage ICT security – involves the business control functions on a constant basis or when opportune.

3.4 RISK MANAGEMENT

The CRO plays an active role in the Bank's ICT security management process.

The assessment of ICT risks, based on the determination of appropriate continuous ICT flows within the Banking Group concerning changes in the operating context and the efficacy of the measures for protecting ICT resources, is preparatory to the identification of possible security measures to be introduced to mitigate/reduce ICT risks regarding the business assets analysed. Risk assessment is carried out at least on an annual basis and in any case in the event of significant changes.

The CRO is additionally responsible for conducting a risk analyses of service providers, meaning the process of monitoring third party risk, in order to produce a holistic and all-inclusive assessment of the Banking Group's exposure to ICT risk.

3.5 COMPLIANCE & AML

Compliance & AML constantly monitors the compliance of systems and processes with the relevant legislative and regulatory obligations for ICT, ensuring:

- assistance on technical and organisational matters from which non-compliance risk may arise, such as issues relating to the processing of personal data;
- consistency of the organisational structures with external laws and regulations for the parts relating to the ICT system;
- verification of the areas subject to legislative and regulatory requirements included in contracts with third parties and Group companies (including agreements outsourcing important essential functions and critical components of the ICT system).

3.6 INTERNAL AUDIT

In accordance with a risk-based, process-oriented approach, the Internal Audit structure performs procedures ("third level controls") designed to ensure an adequate coverage of the various applications, infrastructures and operating processes, including any outsourced components, as well as performing a regular assessment of the completeness, adequacy, functionality (in terms of efficiency and efficacy) and reliability of the internal control system.

3.7 ICT OUTSOURCERS AND PROVIDERS

The Bank uses the services of ICT outsourcers and providers, to which it has entrusted, in as-a-service mode, its Core Banking System, the cloud infrastructure and the various payment systems. The outsourcers and providers have identified, within their respective organisations, figures and structures designed to ensure the existence of controls over their ICT systems on the basis of the identified needs of the Banking Group. Relations with outsourcers/providers are based on agreements, also by formalising SLAs and KPIs, for the constant monitoring of the outsourced ICT components, and require compliance with the Banking Group's security policies.

4 GUIDELINES

4.1 ICT SECURITY POLICIES

The objective of the operating policies of the Banking Group on ICT security matters – as well as that of the present Policy – is the management and safeguarding of the Group's ICT System by ensuring that during their whole lifecycle, data and information are suitably protected, in compliance with legislative and regulatory requirements on personal data protection and the safeguarding of business assets.

To this end, the Banking Group regularly publishes and updates these policies[2], for which this present Policy provides directions, guidelines to be followed and objectives to be achieved. In particular, this Policy is updated on at least an annual basis and in any case on the introduction of, or significant variation in, reference legislation or regulations, security standards or the processes and technologies of the Banking Group. Continuous updating must be ensured as well as the resulting alignment between the Banking Group's regulations and any variation in, or introduction of, new processes by outsourcers.

ABSTRACT

[2] The Incident Management Policy and the Change Management Procedure are examples of this.

4.2 ORGANISATION OF ICT SECURITY

In order to ensure the sound management of ICT security, organisational controls are established together with the relative security frameworks and indicators to direct, control and monitor the measures set up to protect and safeguard the general principles discussed in paragraph 1.3.

The organisation of ICT security and the relative procedures/protection measures are subject to regular revision, possibly also by third parties, with the aim of ensuring the maintenance of suitable levels of efficiency and protection in the management of the Group's ICT system.

4.3 MANAGEMENT OF HUMAN RESOURCES

ICT Security Policies support Human Resources by including the following aspects:

- Determination of the obligations and rules of conduct to be followed when using the allocated credentials and business devices, which are communicated to new members of the Banking Group's staff (on starting work) by the HR & Organization function.
- Increase in the awareness and responsibility of all the Group's personnel and any third parties involved in business processes (advisors, providers, etc.) with respect to a proper and secure use of the ICT resources that constitute the Group's ICT System.
- Determination of the proper means of managing the processes for the cessation of the working relationship, arranging for the return/dismissal of the assets and the formal termination of the working relationship between the parties.
- Determination of, and support in, the management of the entire lifecycle of users and the relative credentials for accessing the Bank's ICT systems.
- Support in the organisation of staff training programmes on ICT security.

As part of their contractual obligations, all users (employees and external staff) accept and sign the terms and conditions on their responsibilities and those of the organisation regarding ICT security.

Staff are constantly trained and updated on security matters so that they may be aware of the main technological and organisational security measures introduced by the Banking Group.

This objective is achieved by providing training moments and rules for employees that direct their daily activities.

To this end, employees must attend the training courses provided that cover security matters, in order to be updated on the introduction of any new laws and regulations, so that they may understand the importance of ICT security and their responsibilities and the harm that an improper use of the Group's ICT system could cause to the Banking Group.

The responsibilities and obligations regarding the protection of business information are a fundamental part of the duties assigned to each person and also remain valid after the end of their contractual relationship, in this way ensuring the confidentiality of the information relating to the Banking Group.

Any breaches of the provisions of this ICT Security Policy must be brought to the attention of the employee's supervisor and by way of the internal whistleblowing procedure.

ABSTRACT

4.4 MANAGEMENT OF BUSINESS ASSETS

All ICT resources (hardware, software, procedures and data) belonging to the business organisation are catalogued and recorded, in this way making it easier to identify and recognise the persons responsible for the security of these resources.

In this respect, the tools developed with the user's ICT tools form part of the cataloguing and monitoring process[3].

[3] The development of applications directly under the responsibility of the operating and control units is subject to measures of an organisational and methodological nature designed to guarantee a level of security comparable with the applications developed by the ICT structure. A regular monitoring process catalogues the applications developed with the user's ICT tools and checks that these correspond to security policy, in particular if used in key activities such as the preparation of data used in the financial statements, in risk management and in management reporting, in order to limit operating risk.

The Banking Group has a process ensuring that all tools (physical and logical) are properly disposed of when they lose their operational value and that they are properly reallocated when the persons responsible leave their position in the organisation.

All information must be classified on the basis of its level of criticality and the effects resulting from a breach of such information's properties of confidentiality, integrity and availability, with the final objective being to identify and implement suitable protection measures.

Staff are required to follow the rules for the proper management and protection of business data and information as determined with respect to their classification. If it is necessary to share business information and send it outside the Group, staff must adopt the security measures for the transmission of the data which are established in the Data Classification Policy, using only the working tools certified by the Banking Group. Any exceptions to the envisaged means of transmission must be authorised by the ICT security function.

4.5 ACCESS MANAGEMENT AND CONTROL

The objective of this dominion is to regulate the means of access to the various system, network and application components managed and used by the Banking Group, consistent with the role performed by the user and in compliance with the established security measures, starting with risk analysis.

More specifically, the following objectives form part of this area:

- to ensure authorisation for access to the business systems, mediating between the needs dictated by working efficiency and those dictated by good security and privacy practice, which require that access should be limited only to operators who have a real need for such access for working purposes; more specifically, ensuring that access to confidential information is based on the need to know and the segregation of duties;
- to perform a regular check that the working needs justifying the authorisations for access to the systems are maintained and possibly arranging for these to be partially/wholly cancelled;
- to control the proper utilisation by users of the authorisation access received.

In particular, the lifecycle of users is managed by an appropriate identity governance process set up by the ICT security function which provides for the following activities at a macroscopic level:

- **creation of users** – the request to create a new user (the hiring of a new employee, needs of the Banking Group, etc.) is tracked and authorised by the authorised staff in charge. Each user must be associated with authorisation profiles characterising the position that he holds in the banking organisation;
- **change of profile** – a formal request is required for each change in the user's profile, which must be authorised by the staff in charge and contain an indication of the changes and the reasons for these (organisational variation, change of job responsibilities, etc.), including any writing, reading and modification rights to be withdrawn;
- **disabling of users** – credentials are disabled when the owner no longer needs to use them due to a change in his job responsibilities or in the case of a prolonged absence (for example in the event of maternity leave). The systems are configured to automatically deactivate authentication credentials if these are not used for a period exceeding 6 months;
- **management of applications profiles** – each user is assigned an authorisation profile in line with his job responsibilities in accordance with the established Model. Exceptions, which must be suitably documented, may be granted on the basis of a reasoned request;
- **monitoring and checking users and the allocated enabling profiles** – on a regular basis, and in any case at least annually, a review is carried out of users and their profiles to check their relevance, with specific attention being placed on any exceptions granted.

The general principles for authorisation for access to the systems is based on the following aspects:

- segregation of roles/duties;
- access only granted if strictly necessary to the performance of the duties allocated to each user or system administrator (least privilege);
- regulation of logical access to the systems on the basis of the need to know.

In addition, the following technical security measures exist when implementing the system of authentication to the Group's ICT system:

- password – the word or string of characters required for access to the systems is managed in accordance with international good practice, for example passwords may not contain the user's identification code or

ABSTRACT

name and must be changed on first use. It is the responsibility of the user to whom the access credentials have been assigned to ensure the confidentiality of the password and a use consistent with his job responsibilities;

- identification codes – the identification codes assigned to users are unique, personal and non-transferrable and may not be re-assigned.

The Banking Group also uses strong authentication solutions for all users (Multi-Factor Authentication) and Conditional Access systems; the Group's users may only access ICT instruments if they hold valid credentials, which are further validated by physical devices managed by the Group's ICT (laptop and mobile), which form part of the equipment assigned to all employees.

Specific procedures exist for technical users and/or those with administrative privileges as well as controls that satisfy the requirements of the Provision issued by the Italian Data Protection Authority "Prescribed measures and precautions for data controllers regarding processing performed with electronic instruments relating to the assignment of duties as system administrator – 27 November 2008".

For this type of user, a privileged access management system exists that provides for a workflow for approval in the case such users need their minimum privileges to be raised. The workflow for approval triggers a request to the ICT security function which assesses it and either accepts it or refuses it as a consequence.

4.6 PHYSICAL AND ENVIRONMENTAL SECURITY

In accordance with current legislation on workplace health and safety, premises intended to accommodate the technological resources used to provide ICT services are arranged so as to ensure suitable protection against the threat of natural, intentional or accidental events that may cause harm to persons and damage to business assets and/or jeopardise the proper, continuous functioning of the resources themselves.

To this end, processes and controls to be activated for physical access to the premises to prevent unauthorised access have been established, for example the keeping of a register of visitors entering and leaving the Bank's facilities. The involvement of third parties is essential for ensuring the Group is properly protected from potential events such as accidents, floods, etc..

The Banking Group is involved in providing suitable protection for its ICT systems, also through the use of physical security measures. This objective is pursued by:

- ensuring security of the physical areas and data centres;
- protecting ICT equipment;
- adopting processes for the destruction and secure elimination of instruments and information;
- having regulations on the retention and safeguarding of instruments at the user's disposal.

4.7 ENCRYPTION

Encryption is one of the tools used to ensure the security of the memorisation of data as well as for managing and communicating such data.

The use of encryption mechanisms such as secure communication protocols (for example HTTPS), or the management of certificates issued by an internal or external certification authority (CA) in order to protect critical business information, is governed by business processes that establish roles and responsibilities in this respect.

In particular, the functions managing the use of encryption keys and the functions involved in the control and establishment of the encryption standards to be used are segregated.

4.8 MANAGEMENT OF OPERATIONS

The objective of this dominion is to ensure that ICT services guarantee adequate levels of data confidentiality, integrity and availability and of all the principles listed in paragraph 1.3, in compliance with business requirements and current legislation, also if the management of the Banking Group's ICT component is outsourced to third parties.

The operating processes are appropriately formalised in specific procedures and/or operating instructions that establish roles and responsibilities, activities, controls and information flows.

All workstations with access to the Group's network are equipped with security mechanisms that reduce the risk of ICT/virus attacks, which could cause serious business losses.

The user must immediately inform the ICT security function in all cases when the security measures are not properly applied and/or the available tools turn out to be inadequate.

ABSTRACT

ABSTRACT

Despite the introduction of security measures, the user must utilise the services available (email, web, etc.) in a responsible manner and in accordance with internal regulations, avoiding the disclosure of business information. For example downloading files from the internet must be avoided as must opening or forwarding attachments to emails of doubtful origin, etc..

Business assets provided to users (for example computers, emails, mobile phones) must be used for work purposes only or for personal use as prescribed.

The installation of software that has not been authorised by the structure in charge of business software management is prohibited. Any ad hoc installation must be justified by business reasons and evaluated by the relevant heads of software management.

Backups enable the availability of the information and systems to be guaranteed even following ICT security incidents or calamities. The confidentiality, integrity and availability of the processed data is however ensured during all the stages envisaged by the backup management process.

As established by current laws and regulations (tracking of banking data, systems administrators, etc.) mechanisms for tracking access and critical operations are envisaged to ensure full compliance, guaranteeing the confidentiality, inalterability and availability of data in line with the requirements of the individual provisions.

Capacity management activities are established in order to understand future business requirements, the organisation's operations and the ICT infrastructure and to guarantee the performance and efficiency of the present and future capacity of the systems. In performing such activities, the Banking Group takes into account the requirements for business operations, the services provided and the ICT resources in order to implement an iterative process, in compliance with the Group's strategic plans, which tries to find the right balance between cost constraints and the organisation's needs.

The Banking Group carries out Vulnerability Assessments and Penetration Tests (VAs/PTs) of the Group's ICT system on a regular basis, delegating the performance of these to third parties under the Group's supervision, and in particular those regarding the systems considered the most critical for the business. The identification of the perimeter to be subjected to these activities is also established on the basis of an analysis of the ICT risk, which might detect critical matters in the Banking Group's systems. These activities make it possible to carry out a regular certification of the security of the systems, ensuring the introduction of effective countermeasures against the newly-identified threats and the management of the associated risk over time. Simultaneous with these checks, the Banking Group generates detailed reports containing the results of the tests and schedules any remediation action that may need to be taken.

4.9 COMMUNICATION SECURITY

Communication Security sets itself the aim of safeguarding the transmission of data on private and public telecommunications networks, with specific emphasis on the physical components (hardware devices), which constitute the network infrastructure used by the Banking Group. In order to minimise the risks that might jeopardise the integrity and availability of the data transmission functions, the main activities to be carried out are as follows:

- cataloguing and classification of the type of network;
- proper management of the components of the network infrastructure, with specific attention given to the aspects of capacity planning, business continuity, disaster recovery and ICT security;
- the formal specification of business rules that govern the conduct of internal/external staff when using and managing the network infrastructure utilised by the Banking Group.

In this respect, the main aspects to be taken into consideration are as follows:

- availability, modality and tools to ensure continuity in the provision of network services;
- monitoring, modality and tools to be used to control network traffic, with the aim of detecting any differences with the established means of operating;
- segregation of the telecommunications network, mechanisms to separate and filter traffic between internal sub-networks within the Group's perimeter;
- means and processes of transferring information inwards and outwards. In particular, information must be communicated through the use of secure protocols on the basis of criteria that ensure the confidentiality and integrity of the information transmitted and received by the Banking Group.

All staff are permitted to use the internet and corporate email. The Banking Group inspects internet traffic (also SSLs) in order to apply filters designed to increase protection from malware or prevent action that is potentially damaging to its reputation. Individual users are enabled for access to the present tools by way of the basic authorisations, following notification from the HR office that a person has been hired.

ABSTRACT

4.10 PURCHASE, DEVELOPMENT AND MAINTENANCE OF THE ICT SYSTEM

The aim of this dominion is to guarantee the production, purchase and maintenance of reliable and secure applications systems in terms of :

- the accuracy of the processing of the data managed by the application;
- controls on authorisation to use the functionalities and data of the application;
- safeguarding the integrity of the data stored in the application's archives;
- safeguarding the confidentiality of the managed data;
- tracking and historicisation of the data updates carried out;
- compliance of the data processing with tax law and other laws and regulations;
- prevention and minimisation of the business risks associated with the use of the application.

In this respect it is the responsibility of the Banking Group to require any third parties involved in the development and maintenance of software/hardware to follow established processes in line with the Group's security policies. In addition, the Banking Group controls the accuracy of the processes followed by checking the documentation produced and formally approving the activities of the development process (functional analyses, UAT test plan, passage into production, etc.).

4.11 SECURE DEVELOPMENT OF SOFTWARE

The software produced must be designed and developed in order to ensure maximum efficiency and effectiveness and a level of security consistent with the information processed and business objectives. As a result, the following general requirements must be taken into consideration:

- the secure development of the software must guarantee the confidentiality, availability and integrity of the information processed and managed, and must be compliant with the general principles listed in paragraph 1.3;
- the environments used to manage the lifecycle of the software (development tests, UATs, pre-production and production) must be kept separate from each other to the extent this is possible;
- the developed code must take account of all applicable laws and regulations, in particular those on personal data protection, fostering the principles of Security/Privacy by Design & by Default;
- best industry practice for the security of the development process (such as the OWASP top 10) must be encouraged;
- the staff involved in the design and development must be suitably trained and have a heightened awareness of ICT security matters.

4.12 SECURITY OF THIRD PARTIES

The ICT system must be managed – also when some of its components are managed by or entrusted to third parties – in compliance with the guidelines and security measures established in this ICT Security Policy. It is therefore fundamental to ensure that the requirements of this Policy on the outsourcing of business functions are included in any contracts or agreements.

The management and/or outsourcing of certain ICT services must provide for compliance with the security measures established by the Banking Group. For this purpose, minimum security requirements are established which must be followed in governing, from a contractual and operational standpoint, relations with third parties who, in order to provide the agreed services, need to access the Banking Group's ICT resources or process its data.

As guarantee of compliance with the security measures, specific audit procedures to be performed on the third party are prescribed within the contracts, formally requiring compliance with laws and regulations such as those on data protection; a Third Party Security Risk Score is drawn up based on the information collected from the provider, rating the adequacy of the security measures and the third party's attitude.

Business information must therefore also be protected in accordance with any contractual restrictions agreed with third parties that assist in any processing connected with the Group's ICT system, in compliance with the requirements of confidentiality, integrity and availability of the information and intellectual property.

4.13 MANAGEMENT OF ICT SECURITY INCIDENTS

The incident management process is the set of activities and tools that the Banking Group adopts to prevent incidents occurring concerning the services provided, or to identify and respond to them on a timely and effective basis, with the aim of safeguarding the corporate ICT systems, consistent with best industry practice and applicable laws and regulations, by performing the following activities:

ABSTRACT

- making a timely identification of any obstacles to, or breaches of, the proper functioning of the system and the relative causes;
- classifying security incidents using a structured methodology;
- identifying the way in which the security incident will be handled;
- establishing the means of dealing with security incidents, both of an internal nature (escalation) and external nature, by coordinating with ICT outsourcers and activating any communications with the Bank of Italy, insurance brokers, the authorities, the police force, etc.;
- reporting and sharing indicators with specialist groups for a rapid identification of any threats;
- gathering the information needed (evidence) for supporting any legal action;
- analysing the security incident, identifying any mistakes or weaknesses and the strategies to be adopted to deal with it, improving the timing of any action and the response to similar events in the future.

Any person coming into contact with the Group's ICT resources is responsible for reporting security events and incidents if they occur. Reporting, to be filed using a suitable ticketing tool, must be made to the person's direct supervisor who, if necessary, will activate the escalation process. Reports must contain the date and time the incident occurred, the ICT asset affected (application, database, PC, network component, etc.) and a description of the event.

Serious ICT security incidents are communicated on a timely basis to the Board of Directors, to the Bank of Italy and, where envisaged, to other supervisory authorities and/or the police, prior to the despatch of a summarised report containing a description of the incident and the disservices caused to internal users and customers. Any incidents regarding payment systems and personal data breaches must comply with the notification requirements of the specific laws and regulations of reference.

Further information can be found in the Incident Management Policy.

4.14 MANAGEMENT OF BUSINESS CONTINUITY

The Banking Group plans, implements and constantly updates all ICT security measures designed to ensure the continuity of ICT services, also in the case of catastrophic events.

The Business Continuity Plan establishes the parties involved, the strategies and the adopted solutions for continuity, setting itself the following objectives:

- to ensure staff are safeguarded;
- to comply with legislative and regulatory requirements;
- to minimise reaction time and the time needed to reinstate the processes considered vital for the business on the occurrence of critical events;
- to avoid the economic effects deriving from the shutdown or limit these to the greatest extent;
- to avoid the harm done to the Company's image or limit this to the greatest extent.

The plan is tested, controlled and revised on an annual basis, and/or in case of a structural change in the systems, also with the assistance of outsourcers.

ANNEXES

4.15 ANNEX 1: RELATED LEGISLATION AND REGULATIONS

INTERNAL RELATED REGULATIONS

illimity Way
Privacy Policy

EXTERNAL RELATED LEGISLATION AND REGULATIONS

Provisions for prudent supervision for banks - Circular no. 285 of the Bank of Italy of 17 December 2013 and subsequent amendments
Personal data protection code – Legislative Decree no. 196 of 30 June 2003 (Official Journal of 29 July 2003), supplemented by the amendments introduced by Legislative Decree no. 101 of 10 August 2008 on

“Provisions for the adaptation of national legislation to the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”
Guidelines of the Italian Data Protection Authority applying to the use of e-mails and the internet in the employment context (Official Journal no. 58 of 10 March 2007 and subsequent amendments)
Prescribed measures and precautions for data controllers regarding processing performed with electronic instruments relating to the assignment of duties as system administrator – 27 November 2008 (Official Journal no. 300 of 24 December 2008 and subsequent amendments)
Provisions on video-surveillance - 8 April 2010 (Official Journal no. 99 of 29 April 2010 and subsequent amendments)
Prescriptions on the circulation of information in a banking environment and tracking banking transactions (Provision no. 192 of the Italian Data Protection Authority of 12 May 2011, published in Official Journal no. 127 of 3 June 2011 and subsequent amendments)
Law no. 231 – Corporate Responsibility, Codes of Ethics and Responsibilities of Legal Persons pursuant to Legislative Decree no. 231/2001
Official Journal no. 99 of 29 April 2010 and subsequent amendments
Official Journal no. 127 of 3 June 2011 and subsequent amendments
Guidelines on biometric recognition and graphometric signatures (Initiation of consultation – Official Journal no. 118 of 23 May 2014 and subsequent amendments)
General Data Protection Regulation - Regulation (EU) 2016/679 (GDPR - Official Journal of the European Union of 4 May 2016, becoming effective on 25 May 2018, and subsequent amendments)
Payments Service Directive 2 - (EU) 2015/2366 (PSD2 – 13 January 2018) and legislative decrees incorporating this into Italian legislation – Legislative Decree no. 11 of 27 January 2010 – as well as regulatory technical standards and guidelines issued by the European Banking Authority (EBA).

ABSTRACT

4.16 ANNEX 2: REFERENCE STANDARDS AND METHODOLOGIES

Over time the international community has developed various methodologies, some of which have been ratified by standardisation bodies (BS, ISO/IEC, government bodies, etc.) and accordingly have become the standards of reference.

The most widespread standards, guidelines and best practices recognised by the international community have been taken into consideration to identify the requisites of a security management system that are closest to the specific technological, organisational and business context of the Banking Group, in order to have an authoritative and comprehensive point of reference, including when the ICT system is outsourced.

The following is a list of reference standards and methodologies on which this ICT Security Policy is based:

- ISO/IEC 27001:2017 - *Information technology - Security techniques - Information security management systems - Requirements*;
- ISO/IEC 27002:2013 - *Information technology - Security techniques - Code of practice for information security controls*;
- *The Standard of Good Practice for Information Security* - *June* 2014 - *Information Security Forum*;
- COBIT 2019 (*Governance, Control and Audit for Information and Related Topics*) from ISACF (*Information Systems Audit and Control Foundation*) and ITGI (*IT Governance Institute*);
- *Payment Card Industry Data Security Standard* (PCI DSS);
- NIST *Cybersecurity Framework* v1.1 - *National Institute of Standards and Technology*;
- SCF – *Secure Control Framework*.