INTESA SANPAOLO

GENERAL PRINCIPLES

Principles of Information Security

EFFECTIVE FROM
24/04/2024

TABLE OF CONTENTS

INTRODUCTION 3

1 MAIN RESPONSABILITIES 4

2 PRINCIPLES AND HIGH-LEVEL RULES OF INFORMATION SECURITY 5

2.1 General principles of information security 5

2.2 Rules of conduct 5

2.3 Operational and process rules 6

2.3.1 Access management 6

2.3.2 Tracking events 6

2.3.3 Maintenance 7

2.3.4 Protection of removable storage media 7

2.3.5 Configuration and change management 8

2.3.6 Life cycle of systems and applications 8

2.3.7 Network security 9

2.3.8 Encryption and data masking 9

2.3.9 Third party and cloud service management 9

2.3.10 Management of security incidents 10

2.3.11 Business continuity management 11

2.3.12 Preventing and managing service frauds 11

2.3.13 Personnel management 12

2.3.14 Physical security 12

INTRODUCTION

Intesa Sanpaolo Group (hereinafter the 'Group') attributes strategic value to the protection of the information, of the informative system and of the business processes, both in the operational management of the activities as well as in the development of new services and solutions.

Consequently, the Group adopts these “Principles of Information Security”, which define: (i) the main responsibilities related to management of the information security (ii) high-level principles and standards aimed at protecting the confidentiality, integrity and availability of data and information of the Companies of the Group, and (iii) requirements for personnel[1], processes and technology in relation to information security, recognising that personnel at all levels have responsibilities to ensure the Group's information security.

This document, which represents the information security policy required by the relevant legislation[2], shall be:

- approved by the Board of Directors of Intesa Sanpaolo, also acting as Parent Company, and must be implemented by all Companies of the Group, considering their own corporate and regulatory contexts;
- updated periodically in order to consider the evolution of the external and internal context and the results of the ICT and Security risk assessment process;
- communicated to all personnel;

Regarding employees, in the event of non-observance of the relevant provisions, appropriate disciplinary measures shall be taken in accordance with the law, contracts and internal regulations in force. Regarding non-employee staff, failure to satisfy the relevant regulatory provisions shall be assessed in accordance with the terms of the existing contractual relationship and may lead to the resolution of the contract.

[1] The term "personnel" refers to employees, agents, people on staff leasing contracts or on internships, as well as Intesa Sanpaolo Group companies’ collaborators, regardless of the contractual relationship with the individual Company and/or all those who, for any reason, are involved in the Intesa Sanpaolo Group's business processes, both in Italy and abroad.

[2] In particular, Bank of Italy Circular No. 285/2013 (Part One, Title IV, Chapter 4) and the European Banking Authority Guidelines on ICT and security risk management (EBA/GL/2019/04).

1 MAIN RESPONSABILITIES

Below are the main responsibilities of the structures that contribute in various ways to guarantee information security and play an active role in the processes of guidance/governance, management and of the Information System security control:

- the **Corporate Bodies** establish the risk tolerance and assume general responsibility for the direction and control of Information Security and the Information System in general, and ensure its completeness, adequacy and functionality in terms of effectiveness and efficiency;
- the **Cybersecurity Function**, the head of which is the **Information Security Officer**:
  - defines and implements, in line with corporate strategies and objectives, the guidelines for cybersecurity, business continuity and anti-customer fraud.
  - oversees the definition and implementation of the organisational and technological measures necessary to ensure an adequate level of protection in terms of cybersecurity, business continuity (also with a view to business resilience) and fraud against customers;
  - adopts the cybersecurity, business continuity and anti-fraud solutions and provides the related services, guaranteeing the agreed service levels and pursuing the continuous improvement of processes with a focus on increasing effectiveness and efficiency;
  - ensures integrated control of the attack surface, centralised management of vulnerabilities, related remediation plans and active monitoring of security events;
  - ensures, for the areas within its competence, the monitoring of associations[3] with sector bodies, judicial authorities and law enforcement agencies, guaranteeing information and involvement of corporate control functions.
- **Functions Developing information security solutions** provide the design, implementation and management of IT security infrastructures, and perform line controls (Level I);
- **Functions Developing IT solutions** maintain and evolve applications and implement and design technology infrastructures, and perform line controls (Level I);
- the **Corporate Control Functions** ensure specific control activities in their respective areas of competence. In particular:
  - The Risk Management Function ensures the assessment, control and measurement of the ICT and security risk profile and is responsible for the development and maintenance of the ICT risk management and control framework;
  - The Compliance Function ensures the control of the risk of non-compliance with ICT, Information Security, Business Continuity and Data Protection regulations;
  - The Internal Audit Function performs periodic ICT and Security Risk analyses and periodically assesses the completeness, adequacy, functionality and reliability of the system of internal controls and the security of the information system.

In general, **personnel** at all levels are responsible for ensuring information security by adhering to the Company's rules of conduct and regulations on information security.

The Parent Company Functions perform the role of guidance, coordination and control of the corresponding Functions of the Companies of the Group.

[3] Specifically for the Parent Company, the Information Security Officer has the task of ensuring, with regard to cybersecurity and the technical-specialist activities and aspects of competence, iterations and relations with AgID- The Agency for Digital Italy and ACN- National Authority for Cybersecurity.

2 PRINCIPLES AND HIGH-LEVEL RULES OF INFORMATION SECURITY

2.1 General principles of information security

In order to guarantee the information security, the Group:

- promotes the **dissemination of a security culture**, within its area of responsibility, through appropriate training and awareness initiatives, which are also essential to ensuring the incisiveness and effectiveness of the risk mitigation measures;
- operates with the objective of ensuring the **security** and **resilience** of the services provided over time, in line with technological innovation and legislation in the field, aiming at providing **increasingly secure services**;
- guarantees the identification and **adequate treatment of ICT and security risk**, according to a risk-based approach, which considers, where applicable, the criticality of systems, processes, functions as well as the relevance of the data processed and identifies appropriate **risk containment measures**, in order to protect the confidentiality, integrity and availability of the Group's and customers' data and information;
- provides **security by design** as an integral part of the new product/service/model creation process;
- guarantees the management of access rights to IT resources and their support systems on a need-to-know basis (**need-to-know** principle), including remote access;
- guarantees the allocation of the minimum access rights to IT resources strictly necessary for the performance of their tasks (principle of «**least privilege**»), in order to prevent unwarranted access to a wide range of data or the allocation of combinations of access rights that can be used to circumvent controls (principle of «**separation of duties**»);
- considers security as an **enabler for the creation of innovative services**, considering the usefulness of innovative security technologies and devices in mitigating risks arising from continuously evolving scenarios;
- assess the **security of the supply chain** with an approach that enables the identification of the risks and most appropriate measures and includes **supplier control and management** models, in line with those established for the Group;
- participates and contributes to **networks with financial institutions, regulatory bodies, trade associations and Italian, European and international entities** for the sharing and promotion of **best practices, initiatives and projects** aimed at increasing and strengthening security measures;
- manages **anomalies and incidents** of varied nature and severity in an appropriate manner to **avoid or reduce disruptions** and ensure a speedy **return to normal operations**;
- guarantees the continuous **monitoring and analysis** of both the **internal and external environment**, in order to identify timely new threats.

2.2 Rules of conduct

Below there is a list of the main rules that staff must respect in order to contribute to the control of information security risks:

- information must be classified according to its level of criticality in accordance with internal regulations and must be handled with the utmost diligence to safeguard its confidentiality, in compliance with the procedures adopted by the Group;
- the IT tools assigned by the Group should be considered as working tools; therefore, they must be used in a secure manner to ensure the confidentiality, integrity and availability of

data and in such a way as not to harm the Group's reputation. A similar conduct must be adopted in the event of authorization for work use of IT tools owned by the user;

- access credentials related to IT work tools must be managed securely;
- When using IT work tools, all necessary precautions must be taken to prevent unauthorised third parties from acquiring confidential information or sensitive data;
- IT work tools during transport must be stored appropriately with special care even when not in use;
- Company communication tools must only be used for purposes related to the performance of work;
- Internet browsing recognised by the user is a work tool and must be used exclusively for purposes related to the performance of work activities and in such a way as not to damage the reputation of the Group;
- suspected data violations must be promptly reported to the dedicated support structures, so that they can take the necessary action and report to the authorities;
- documents must be managed consistently with the classification levels of the information they contain, from drafting to archiving and/or eventual destruction with the support of specific tools;
- in the case of flexible work, individual agreements and the Group's guidelines on where and how the work can be performed must be followed;
- company information must only be processed using file sharing tools (cloud or collaboration services) authorized by the Company, which allow an efficient and secure working approach without using external data storage platforms such as cloud storage services.

We also refer to the “Cybersecurity Rules of Conduct with Adequate Information” and the “Cybersecurity Vademecum for Third Parties” (which is provided to all third parties operating on the Company's information systems).

2.3 Operational and process rules

2.3.1 Access management

Safeguards must guarantee to ensure (i) proper identification and authentication of users, system administrators, customers, (ii) automated procedures and devices and that access is permitted, with the appropriate authorization, only to the information and the systems necessary to carry out the assigned functions and duties.
In particular:

- processes and tools should be set up to define, create and manage access profiles and the rules concerning their assignment to users based on the profiling model adopted, the purpose is to authorise access only to the resources and information necessary to perform the assigned tasks;
- users, applications and devices must be identified and authenticated before allowing their access to the information system (local, remote, network);
- mechanisms should be in place to monitor access to systems and applications, proportionate to the functions and data they contain/manage.

2.3.2 Tracking events

Safeguards must guarantee to ensure the management of the entire lifecycle of logs, the protection of the information tracked, the retention period and the guaranteed traceability of the tracked events to the user that executed them.

In particular:

- events that need to be tracked by the IT system, or by one or more of its components, because they are significant/critical in ensuring regulatory compliance and the security of the IT system, should be identified and documented;
- the IT system should generate logs that contain the minimum information established to be necessary for the critical events identified;
- tracking information and tools should be protected based on log type and the information it contains, especially when personal data is processed;
- to verify the occurrence of unauthorized activities (e.g., unauthorised accesses) the logs collected should be subject to periodic reviews and analysis, at the intervals prescribed for each type of log and tracked event;
- procedures should be defined to ensure that the information contained in logs is only shared with third parties in a secure manner.

2.3.3 Maintenance

Safeguards must be in place to ensure proper maintenance of information system components in order to guarantee effective protection of information systems.
In particular:

- duties and responsibilities related to the maintenance of the systems and the components of the information system must be formally assigned, to ensure the effective control of the related activities, which must be appropriately documented;
- the maintenance of the components of the information system must be carried out in accordance with the manufacturer's technical specifications and Company regulations;
- periodic maintenance of the systems must be arranged, in accordance with the instructions of the suppliers of the various technological components and in line with the expected service levels;
- the remote maintenance of the components of the information system must be approved, monitored and protected;
- there must be an authorization process for the personnel tasked with conducting maintenance operations on the information system.

2.3.4 Protection of removable storage media

Adequate safeguards must guarantee to ensure the proper protection and management of storage media and the information contained in them.
In particular:

- duties and responsibilities related to the assignment, installation and management of removable storage media (both electronic and non-electronic) must be formally assigned;
- an authorisation process must be established to the assignment of IT equipment (PCs, laptops, tablets, etc.);
- only equipment and/or technological solutions assigned or otherwise authorised by the Company must be used;
- the storage media containing corporate information must be protected with cryptographic techniques based on of the classification of the information contained, and mechanisms must be used for the irreversible deletion of the data contained in the storage media, before re-using, disposing of or maintaining them in accordance with corporate regulations;
- the physical transportation of the storage media must use methods and appropriate devices for the level of classification of the information contained.

2.3.5 Configuration and change management

Adequate safeguards must guarantee to ensure the management of configurations and modification of the information system[4] (including hardware, software, firmware and related documentation) during the entire lifecycle of the components in relation to inventory management, hardening activities, and protection of environments.

In particular:

- duties and responsibilities for managing information system configurations should be formally assigned to ensure the effective monitoring of the related activities, which must be appropriately documented.
- an inventory of information system components must be formalised and maintained complete and up-to-date, with a level of granularity such as to allow for the assignment of responsibilities for individual components, taking into account the entire life cycle of the assets considered. A standard (baseline) configuration of the Company's information systems is also defined, documented and updated, including aspects related to network type, system components and their location at architectural and physical level, in order to guarantee proper configuration management;
- modification to the information system must be formalised, tracked, documented and approved. In addition, the possibility of reverting to the previous configuration must be guaranteed (e.g. via rollback plan, backup, etc.);
- procedures must be defined for emergency changes;
- mechanisms should be in place to govern the installation of software by users, periodically verifying compliance with the Company regulations;
- appropriate protection of environments (e.g. Development, Testing and Production) and related data must be ensured, starting with the separation of these environments;
- the integrity of all components of the corporate information system must be protected, including protection against malicious code, the use of tools to detect tampering and protection against spam, and solutions against APT (Advanced Persistent Threat) attacks;
- software and the related documentation should be used in compliance with the relevant agreements and in accordance with copyright laws, and their use should be tracked based on the predefined number of available licenses, to monitor the copy and distribution thereof.

2.3.6 Life cycle of systems and applications

Adequate safeguards must guarantee to ensure the integration of security into the life cycle of systems and applications.

In particular:

- the life cycle of information systems must be defined and managed in accordance with company rules and processes;
- duties and responsibilities must be formally assigned, in order to ensure the effective control of the related activities, which must be appropriately documented, protected and securely stored;
- a phase must be defined and implemented to identify and analyse the security requirements for both new applications and the applications subject to changes. These requirements must guide the choice of the security measures for the protection of the information managed by the systems and applications, the level of robustness referring to the classification of the data processed, from possible constraints related to compliance with regulations/standards and the risks identified;

[4] This also includes patch management and change management.

- in the phases of developing and changing the applications, in order to ensure their correct operation, the security aspects must be adequately monitored and documented. Specifically, security measures must be implemented and adopted for the secure development, based on best practices (for example, OWASP), including the security requirements identified during the design phase or on the basis of the risks analysis;
- a security testing phase must be implemented and provide the testing of applications and the verification of the adequacy of the implemented functionalities and new components, also regarding the security requirements defined in the design phase or deriving from corporate regulations and any regulatory and/or compliance requirements (e.g. PCI DSS);
- changes must first be checked, tested and approved before switching to production;
- specific protection measures must be defined for the correct, secure and verifiable management of the application operation phase, which includes a check that the safety measures are kept effective over time;
- procedures must be defined to dispose of systems, applications and networks in cases where these are no longer used, in a safe and compliant manner.

2.3.7 Network security

Adequate safeguards must guarantee to ensure the correct and secure design, configuration and management of networks.
In particular:

- duties and responsibilities related to the security of networks and the associated components (e.g., firewalls, DNS, DHCP, etc.) must be assigned, in order to ensure the effective control of the related activities, which must be appropriately documented.
- the design of the network infrastructure must be carried out guaranteeing that the segregation between different network environments is respected, and measures covering confidentiality, availability and integrity requirements must be implemented;
- the network infrastructure must be configured by adopting protection principles related to the elimination of any unnecessary functionality from network devices (hardening) and the periodic review of traffic control policies.

2.3.8 Encryption and data masking

Adequate safeguards must be guaranteed to ensure the correct use of encryption and data masking measures and techniques and also the adequate management of cryptographic keys.
In particular:

- duties and responsibilities related to the management of data encryption and masking solutions must be formally assigned to ensure the effective monitoring of the related activities, which must be appropriately documented;
- criteria for the use of cryptographic techniques to protect information must be defined, according to its level of classification, the security risk analysis and the fulfilments under the regulations in force. In fact, there is a secure management of encryption keys based on the duties, procedures, methods and rules defined, adopting adequate countermeasures to protect encryption keys from modifications, losses and destruction.

2.3.9 Third party and cloud service management

Adequate safeguards must be guaranteed to ensure that an acceptable level of protection of corporate assets and information, in terms of privacy, confidentiality, integrity and availability, is reserved for the management of third parties and cloud services.
In particular:

- duties and responsibilities for the management of third parties must be formally assigned - right from the stage of assessing/selecting third parties until the termination of the contract relationship - to ensure the effective monitoring of the related activities, which must be appropriately documented.
- the responsibilities, processes, tools and methods for the exchange of information with third parties must be formalised, evaluating the use of techniques that guarantee confidentiality, integrity and non-repudiation, in relation to the critical nature of the information processed.
- an assessment of suppliers[5] must be carried out before the stipulation of the contracts for the acquisition or outsourcing of systems, components or services. The assessment must cover the suppliers' IT security and Business Continuity processes and safeguards, their consistency/suitability with the principles and rules adopted by the Bank, and must take into account the complexity, criticality, or importance of the functions outsourced to third parties, risks, and potential impacts on activities concerning Business Continuity;
- specific security requirements must be contractually formalised according to the type of supply and the relative associated risks, and more generally, to the critical nature of the context;
- secure third-party management procedures must be defined for all the duration of the agreement, also aimed at periodically verifying the adequacy of the supply and compliance with the planned IT security and business continuity processes and measures;
- secure procedures need to be defined for the termination of relations with third parties in all circumstances (including the case of termination of the agreement due to its natural expiry or termination due to the supplier’s infringement of specific contract obligations). More specifically, it needs to be specified that the failed application or infringement of the security and business continuity clauses constitute a serious infringement of the contractual obligations and determines the Bank's right to terminate the contract;
- third parties must be made aware of the code of conduct to guarantee the security of data processed and to guarantee that activities rendered in the scope of the contract relationship are carried out correctly by inserting appropriate clauses within the contracts.

2.3.10 Management of security incidents

Adequate safeguards must be in place to ensure proper management of security incidents at all stages of the life cycle (monitoring, identification, analysis, containment, recovery and reporting) and also the maintenance of an archive must be in place, concerning the incidents that have occurred.
In particular:

- duties and responsibilities related to the management of security incidents (including cyber-attacks) must be formally assigned to ensure the effective monitoring of the related activities, which must be appropriately documented;
- processes for monitoring and reporting events[6], for triaging/classifying and notifying incidents to the competent authorities and, if necessary, to interested parties, should be defined and implemented;
- a security incident management process should be implemented and should include the activities necessary to contain the impacts, removal of the causes and restoration of normal operating conditions;

[5] In particular, in the case of outsourced services delivered according to innovative models (cloud computing).

[6] “Event” means a change of status that is relevant in managing an ICT service or any of its elements. An event may indicate a malfunction in an IT component and, consequently, may trigger the generation of an incident.

- a post-incident analysis process should be implemented after the formal resolution of the incident, to include the collection and inventorying of evidence, the analysis of the causes of the incident, the identification of improvement actions and the related archiving activities;
- training and awareness-raising programs should be arranged for the users of the information system, regarding security events and behaviors to be adopted before, during and after an event is detected.

2.3.11 Business continuity management

Safeguards must be in place to enable the Bank to cope with and manage the consequences of an unforeseen event with potentially high business impacts, and to ensure that critical processes are restored in a timeframe and manner that allows for the reduction of negative consequences on the operations.
In particular:

- tasks and responsibilities for the Business Continuity management - including the establishment of a Business Continuity Management process - must be formally assigned to ensure effective oversight of the activities, which must be properly documented;
- a methodology for Business Impact Analysis (BIA) of critical business events must be identified and implemented; in addition, Business Continuity solutions must be defined, developed, and carried out, and tests, audits and internal audit activities must be performed. This maintenance process must enable the continuous improvement of Business Continuity activities;
- a Business Continuity training and awareness program should be established that, starting with the current level of Business Continuity management, it must identify the needs in terms of targeted training/interventions.

2.3.12 Preventing and managing service frauds

Adequate safeguards must be ensured to guarantee (i) the management of frauds, (ii) the identification of the analysis and proper management of any behavior suspected to be fraudulent, and (iii) the activation of appropriate preventive countermeasures to limit the economic and reputational risks of Group Companies.
In particular:

- duties and responsibilities for fraud management should be assigned in order to ensure prevention and control of the related risk, identification of mitigation solutions and monitoring of their effectiveness, reporting, collaboration with other functions and external entities, and training and awareness-raising in this regard;
- fraud risk must be addressed through defined operational fraud prevention and management processes, through which the planning, implementation, management and monitoring of the solutions necessary for its adequate mitigation are ensured;
- a common methodology for directing fraud risk analysis activities shall be adopted within the Group; based on the assessment of impacts, a centrally coordinated risk management strategy shall be defined and adopted;
- the effectiveness of security countermeasures in place must be continuously monitored, including through automated indicators;
- the functions responsible for mitigating fraud risk must make use of continuous discussion and effective cooperation with other corporate functions placed in charge of governing risks on the information and values handled, as well as cooperation with other market participants, such as, for example, suppliers, industry associations, customer associations, external bodies, and authorities, including Supervisory Bodies and Law Enforcement Agencies;

- a training and awareness program on the subject must be established, in order to educate personnel about the prevention and detection of fraud; special activities having the same purposes, must also be carried out with respect to corporate customers.

2.3.13 Personnel management

Safeguards must guarantee to ensure that the personnel management process takes security aspects into account.
In particular:

- for the personnel, the adequacy of the candidate's personal and professional references must be verified, with respect to the position and the sensitivity of the information to be handled;
- the contracts must include clauses to protect the confidentiality, integrity and availability of the information, in order to prevent the disclosure, damage and unauthorized use of the information;
- regular training must be provided to the personnel, at least once a year, depending on their role and activity, training, and awareness initiatives on compliance with and the specific application of the related rules, in order to minimise the risks related to the handling of the information.

2.3.14 Physical security

The security of company buildings and sites must be guaranteed, preventing unauthorized access and generally ensuring an adequate level of security of physical resources.
In particular:

- physical security policies and operating procedures must be defined, documented and updated, including the definition and assignment of roles and responsibilities, in order to ensure an effective protection of Company assets and Information Assets;
- suitable control measures must be implemented to ensure that physical access to the common areas is recorded and granted to authorized personnel only. Different access methods must be defined based on the various types of users registered;
- technical physical protection measures to prevent unauthorized access must be in place in relation to the importance of the buildings and the criticality of the operations and systems located there.