Principles of action of the corporate information security policy

[December 2023]

Version control

Version	Date	Control
1	April 2023	✓ Initial version
2	21/12/2023	✓ Alignment with the Corporate Information Security Policy

Contents

1 Introduction

1.1 Background

Information and communication technologies (ICT) are currently a key resource for the development and operation of banking services. ICT is not only an enabler in the strategies of the institutions and is part of almost all banking processes and distribution channels, but also executes automated controls over the core business information.

Information security must be established around a set of measures and procedures aimed at safeguarding the CaixaBank Group's ("the Group") information and promoting the will to:

- Ensure adequate protection of information, deploying security measures that the Group must adopt to adequately protect itself against threats and risks that could impact the confidentiality, integrity and availability of its systems, information assets or resources.
- Systematise the management of information security in such a way as to assist in making appropriate risk-based decisions in situations related to the preservation of information security.
- Establish a Group-wide information security function through responsibilities and roles.

1.2 Objective

The Group, aware of the importance of security in the processing of information for the entire Group, its customers, suppliers and, in general, all the institutions with which it has a relationship, considers it essential to establish the type of treatment to be given to the information it manages, throughout its life cycle and in order to guarantee its confidentiality, integrity and availability.

The purpose of the Corporate Information Security Policy (hereinafter "the Policy") is to set out the corporate principles on which the actions to be taken in the field of information security should be based, all of which are aimed at:

- Define the technical and organisational measures necessary to mitigate the Group's information security risk.
- Ensure the evaluation of information security decisions to preserve the balance between profitability and risks.
- Maintain appropriate management of this risk, in line with the Risk Appetite Framework, the outcome of which should be within the medium-low risk profile determined by the Board of Directors for the Group.
- Comply with regulatory requirements and supervisory expectations.

The Policy referred to in these Principles is updated in line with current regulatory references and best practices in information security management, both nationally and internationally.

2 *Scope of application*

The Policy referred to in these Principles is of a corporate nature and is aligned with the Corporate Technology Risk Management Policy. Its scope includes CaixaBank and all its subsidiaries (those in which the parent company exercises a controlling position).

3 General principles of information security

The Group's priority objectives include ensuring transparency, independence and good governance in order to safeguard the interests and trust of all stakeholders.

The general principles are fundamental guidelines related to information security and should always be present in any activity related to information and systems owned by the Group. The general principles are listed below:

a) Strategic alignment. The approach to information security shall at all times be aligned with the Group's strategic objectives.

b) Risk management. Through integration with the corporate risk management framework, risks shall be identified, monitored and treated to bring them within acceptable levels as defined by the Group.

c) Proportionality. The deployment of protection, detection and recovery measures shall be proportional to the risks, their criticality, the value of the information and the cost of the security measures defined.

d) Multi-layered security measures. There shall be a protection strategy consisting of several layers of security of organisational, logical and physical origin, arranged in such a way that when one fails, it allows time for an adequate reaction to materialised incidents, reduces the likelihood that the system as a whole can be compromised and minimises the ultimate impact on systems and information.

e) Fundamental characteristics of information security. Due to the strategic nature of the Group's information and the mission to achieve business objectives, it is necessary to ensure its protection based on the pillars of confidentiality, integrity and availability. The confidentiality of information must be guaranteed according to its categorisation, so that only authorised users have access to it. The integrity of the information must be ensured, guaranteeing that the data have not been manipulated and are therefore reliable. Finally, the availability of the information must be guaranteed, which is the ability to remain accessible in the location, at the time and in the manner required by authorised users.

   Likewise, and due to legal and ethical requirements, the Group must protect in these terms the information under its responsibility relating to customers, third parties and official bodies.

f) Delivering value and continuous improvement. Through continuous monitoring and the development of reviews and tests for the assessment of risks and controls, their effectiveness will be measured to optimise security investments and expenditure. Continuous monitoring will enable the capture of emerging security risks, whether driven by technological developments or by the Group's own evolution.

g) Default security of systems. Systems and their data shall be designed and configured to ensure a sufficient degree of security in line with strategic business objectives, maintaining their security throughout their life cycle.

h) Management of human and technical resources. The information security process should be considered as a process made up of people, technical, material and organisational elements. Staff using systems and information shall be trained and made aware of their information security duties and obligations arising from this policy. Such personnel shall apply the security principles in the performance of their duties.

i) Professionalism. The team in charge of managing information security shall be duly qualified and trained for the performance of their functions, under a process of continuous updating and training in the matter.

j) Classification of information and assets. Information assets shall be classified on the basis of information security criteria and assigned according to the functions to be performed and appropriate security measures applied.

k) Information security criticality. The development, implementation and maintenance of the Policy requires the formalisation of criteria for categorising the Group's assets in order to identify those with the highest priority when dealing with information security. To this end, the information security aspects and criteria to be considered, equally and without exception, in all Group companies within the scope of this Policy shall be established at corporate level. The Information Security Committee shall specifically approve a definition of criticality from the perspective of information security, so as to identify the most critical assets, with the first lines of defence being responsible for classifying existing assets.

l) User management, privileges, segregation and delegation of duties. Risks arising from lack of segregation of duties or incompatibilities of functions with specific roles and single-person dependency or overloading of critical functions shall be minimised. Processes shall also be established for appropriate user management.

m) Information security management at suppliers. When contracting suppliers, it must be ensured that the requirements arising from corporate policies and frameworks for relations with suppliers are transferred at both the contractual and training levels. The main requirements are: (1) comply with applicable information security legislation at all times in the territories in or from which the supplier provides services to the Group and encourage free market practices, as well as regularly review and improve governance practices; (2) put in place measures to prevent and avoid as far as possible that the Group's information and systems can be used for unlawful conduct and review them regularly, actively cooperate with regulators and law enforcement agencies and report all suspicious activities that are detected; and (3) encourage responsible security practices among suppliers and their supply chain, through contractual clauses and the implementation of monitoring mechanisms.

n) Security incidents. Mechanisms shall be established to detect and react to security incidents that may compromise the Group's information systems or assets. These procedures shall cover detection mechanisms, classification criteria, analysis and resolution procedures and communication to interested parties, ensuring the appropriate recording of the operational event when appropriate.

o) Disciplinary sanctions and non-compliance. In the labour sphere, non-compliance with the Security Policy may be considered a breach of the duty of good contractual faith, punishable by the disciplinary measures provided for in the labour laws and regulations in force at any given time, and without prejudice to the compensation for damages that the Group may claim from them.

3 Governance framework

The pillars on which the Group’s information security risk governance framework is based are as follows:

- Compliance with the principles contained in the Policy referred to in these Principles by the companies of the Group within its scope of application.
- Corporate supervision of the parent company.
- Alignment of strategies among the companies of the Group, and in turn alignment with best practices, supervisory expectations and current regulations.
- Maximum involvement of the governing and management bodies of the Group companies.
- Internal control framework based on the Three Lines of Defence model, which guarantees strict segregation of functions and the existence of several layers of independent control.

The Policy referred to in these Principles shall be subject to review by the Board of Directors.

4 Information and reporting framework

The establishment of an appropriate information framework is fundamental to the management of information security risks.

The main objectives of the reporting framework are:

- Provide the Governing Bodies and Senior Management with accurate, clear and sufficient information sufficiently in advance to facilitate decision-making and to verify that they are operating within the established risk tolerance.
- Keep shareholders and the Group's stakeholders informed in the area of information security.
- Provide the heads of the different areas, especially the management and control areas, with the necessary data to be able to control compliance with the strategy defined for the Group in relation to security.
- Satisfy the information requirements of the supervisory bodies.

Information shall be provided to the Governing Bodies on a regular basis. In addition, at the request of the Governing Bodies, they shall be provided with any monograph or information requested on an ad hoc or recurring basis in relation to cybersecurity in the Group.