GRUPO SUPERVIELLE



Information Security Policy

Grupo Supervielle S.A.

September 14, 2023

TABLE OF CONTENTS

1. **INTRODUCTION** 3
2. **GOVERNANCE** 3
3. **SCOPE** 3
4. **EXTENSION TO THIRD PARTIES** 4
5. **INFORMATION SECURITY PRINCIPLES** 4
6. **OBLIGATIONS** 5
7. **INFORMATION SECURITY MANAGEMENT PROGRAM** 6
8. **ETHICS AND VALUES LINE** 7
9. **ANNEX - GLOSSARY** 8

1. INTRODUCTION

Grupo Supervielle S.A. recognizes information and the media that support it as a strategic asset; and defines, as its objective, to achieve the necessary security levels that guarantee its adequate protection, based on the Confidentiality, Integrity, Availability, Authentication, Authorization and Non-repudiation pillars.

This Corporate Information Security Policy is the highest level policy in this area. Underlying this, Grupo Supervielle S.A. establishes several global policies for the different functions related to the protection of information.

Grupo Supervielle S.A. companies are subject to certain laws, regulations and contractual obligations that provide controls for information security.

In order to ensure information assets protection, the company establishes principles governing the protection of data and information to avoid risks inherent in their processing, transmission, storage, and destruction. This is done to avoid its loss, disclosure, embezzlement, non-availability, undue destruction, repudiation, access and/or unauthorized modifications.

Likewise, the integral protection of data is privileged, regardless of the medium that contains it, promoting an environment of ethical and controlled management in order to guarantee regulatory compliance and a competitive advantage in the market.

Consequently, the need arises to inventory, classify, and protect information based on its criticality, degree of exposure and risk appetite, assigning responsible people according to the management instance in which they intervene, the resource used, and the type of information accessed.

2. GOVERNANCE

The Board of Directors of Grupo Supervielle S.A. will be the body in charge of reviewing and approving this policy considering the guidelines and/or recommendations of the Cybersecurity Committee.

It is the responsibility of Information Security to ensure compliance with this Policy and to keep it updated in order to faithfully reflect the established guidelines, reviewing it once a year or, in the face of relevant changes.

3. SCOPE

This policy applies to Grupo Supervielle S.A. and its related companies and the reference to Grupo Supervielle in this document will include each of its related companies.

Failure to comply may imply labor sanctions and, where appropriate, the termination of contracted personnel, or contracts with suppliers or consultants.

The Information Security Policy and all documentary content that originates from it, are mandatory for Grupo Supervielle S.A. and therefore applies to all permanent employees, temporarily hired, suppliers, consultants and other people who carry out activities in Grupo Supervielle S.A.

It includes the protection of information assets with regard to the security of information obtained, created, or maintained by users in any written, printed, or electronic medium and all processes related to activities carried out through technological components.

This includes information of clients, employees, and proprietary information of Grupo Supervielle S.A., such as data on its products, strategies, processes, and services.

Any exception to this Policy must be analyzed by the Cybersecurity Committee, which will provide its recommendations to the Operational Risk Management Committee to make decisions in line with the organization's risk appetite. Subsequently, it will inform the Ethics, Compliance and Corporate Governance Committee about the decisions made.

4. EXTENSION TO THIRD PARTIES

Employees and service providers directly contracted by Grupo Supervielle S.A. must formally adhere to a document in which they agree to act in accordance with this Information Security Policy.

Likewise, contracts must include a clause that ensures information confidentiality.

5. INFORMATION SECURITY PRINCIPLES

The Information Security Policy is governed by the following principles:

- **Confidentiality:** Information owned by Grupo Supervielle S.A. or in its custody must be protected at all times against unauthorized access.
- **Integrity:** Measures must be implemented to prevent unauthorized modification or destruction of information, whether accidentally or intentionally.
- **Availability**: Must ensure that required information is available in a timely manner to the people authorized to access said information.
- **Authentication:** The identity of each individual or process that accesses Grupo Supervielle S.A. information must be properly verified before access is allowed.
- **Authorization:** Access to information should be limited only to what is necessary to support authorized business functions.
- **Non-repudiation:** Provides necessary guarantees that undoubtedly ensure participation of sending and receiving parties.
- **Access by function:** Access to information must obey the principle of least privilege, through which users are granted the minimum levels (or permissions) necessary to perform their job duties.

- **Access control closed by default:** Linked to the previous principle. All accesses must be closed by default and opened (for a user) only when necessary.

- **Non-transferable access:** The assignment of access permissions must be made to individual users and is non-transferable, so that the responsibility for the actions exercised with the access granted is directly attributable to that user.

- **Segregation of duties:** No user should have full control of a critical business process or transaction.

- **Responsibility identification:** Systems and processes must be subject to controls that allow unauthorized access to be detected and the person responsible for the activity carried out in said system or process to be identified.

- **Information security strategy:** The definition and implementation of a strategy for the protection of information assets must be ensured.

- **Information classification:** All information, whether verbal, written, printed, or electronic, must be classified based on its confidentiality, integrity, and availability.

- **Information disclosure:** Information, whether verbal, written, printed or electronic, must be disclosed in accordance with the confidentiality requirements of such information.

- **Awareness:** All individuals with access to Grupo Supervielle information must understand their roles and responsibilities regarding management and protection of Grupo Supervielle information.

6. OBLIGATIONS

The Information Security department of Grupo Supervielle establishes the following main controls:

- Develop, maintain, and communicate this Policy, and supporting documentation.
- Keep the Board of Directors informed about the Information Security governance performance, high-level policies, its strategic projects, and all actions related to the mission, goals and objectives related to the Information Security governance.
- Identify and implement a risk management framework for the protection of information and establish the necessary controls to resolve them in an acceptable manner to support the business objectives of Grupo Supervielle S.A.
- Verify that information protection processes are adequate based on current commercial and regulatory requirements.
- Manage information security training and awareness programs.
- Manage and respond to information security events and incidents in a timely manner to reduce the impact on shareholders, customers, and business partners.
- Develop and publish information security standards and procedures necessary to maintain a safe, secure, and compliant operating environment.
- Conduct risk assessments to identify threats, vulnerabilities, and measures to mitigate risk.

- Contribute to identifying and implementing appropriate segregation of duties and functions to minimize overlapping authorization risks.
- Manage vulnerability assessments, penetration tests, code reviews and security systems tests.
- Ensure that its processes are in line with the three lines of defense model adopted by the entity, implementing those controls and security measures that allow the confidentiality, integrity, and availability of the information to be reasonably preserved.

Users in turn agree to:

- Treat Grupo Supervielle S.A. information, of clients and of the general public in an ethical and secret manner and in accordance with current legislation and internal regulations to avoid misuse and improper exposure.
- Use information in a transparent way and only for the purposes for which it was collected.
- Contribute to perform processes that allow the execution and control of a process or transaction from its creation to its conclusion to ensure division of functions.
- Only access information and resources that have been formally authorized.
- Identification as an employee in the systems must be unique, personal, and non-transferable and identifies them as responsible for actions carried out.
- Access granting must obey the criterion of least privilege, according to which users only access information resources that are essential for the full performance of their activities.
- The password works as an electronic signature and must be kept secret, its dissemination is prohibited.
- Document and reliably report those risks (whether the user is responsible or not) that affect the principles mentioned in item 5 of this document before the Information Security Department and the Operational Risk Management Department.
- Do not use for private purposes or transmit to other technologies, brands, methodologies, and any information belonging to Grupo Supervielle S.A., even if they have been obtained or developed by the same employee in their work environment.
- Only disseminate information classified as public when necessary, refraining from disseminating sensitive or internal information of Grupo Supervielle S.A., such as policies, information on security tools, standards, or internal regulations/procedures.
- Inform and work together with the Information Security Department in the evaluation of any tool, application, service and/or provider that may have an impact on any information asset of the entity, in order to determine its impact on the security posture, define the mitigating controls that are considered necessary and carry out the corresponding monitoring.

7. INFORMATION SECURITY MANAGEMENT PROGRAM

The Information Security Management Program (“PGSI”, according to its acronym in Spanish) is a set of disciplines arranged by Grupo Supervielle S.A. in order to ensure a centralized and uniform approach in the definition and application of the Corporate Information Security Policy.

These disciplines include:

Logical Access to Information Assets: Security must be managed on the different types of access (local and/or remote), and the secure authentication of users and profiles of all Grupo Supervielle S.A. personnel. Said security must be applied to all information assets (applications and approved technological platforms), both for productive and contingency environments.

Security Monitoring and Control: It is aimed at securing the processing platforms and IT operations, to mitigate possible security risks, in accordance with the defined security monitoring and control procedures. Information assets accesses and activities must be monitored periodically, reporting incidents or any anomaly detected to whom it corresponds, and proceeding to take the necessary actions for their resolution. Systems and technology services that Grupo Supervielle S.A. outsources must be controlled to ensure correct administration of assets information security managed by the providers.

Virus and Vulnerability Management: Its purpose is to protect Grupo Supervielle S.A. against malicious code and to establish standards and procedures for the detection and remediation of vulnerabilities.

Support, prevention and maintenance of architectures and secure development life cycle: It must be guaranteed that security aspects are considered in all phases of computer systems life cycle, for which it must be reasonably ensured that all computer applications to develop or acquire incorporate, according to their characteristics and scope, access control systems and mechanisms that guarantee information security and allow its correct management, administration, control and auditability with the purpose of preventing loss, modification or inappropriate use of data in computer applications and protect the confidentiality, availability, and integrity of information.

Observations Follow-up: Involves carrying out a correct and timely follow-up of action plans that could arise as a result of findings and/or observations made by the different control entities.

Security Incident Management: It consists of having a process for the attention, detection, analysis, control, treatment and mitigation and response - recovery of security incidents, and its correct communication to the parties involved, for continuous process improvements.

Information Security Awareness Plan: Seeks to promote a culture of compliance with the Information Security Policy, as well as the best practices in information security.

Information Security Risk Management: The previous highlights are linked to the correct management of Information Security risks, providing controls related to reference points that can be used to identify deficiencies in the design and implementation in the asset. Periodic reviews are carried out that derive action plans if required.

8. ETHICS AND VALUES LINE

Any breach of this policy may be reported to the Compliance Department or through the Ethics and Values Line:

0800-777-7813

www.eticagruposupervielle.lineaseticas.com.ar

User: Supervielle

Password: Supervielle

9. ANNEX - GLOSSARY

Asset: In relation to Information Security, it refers to any information or element related to its treatment (systems, supports, buildings, people) that have value for the Organization.

Approver: It is responsible for authorizing the request to add or change permissions of a user. When a user relates to a service provided by third parties or provided by a supplier, the approver will be the primary person responsible for the service in question.

Application or Application System: All programming development that processes data and runs on a technological platform to provide support to internal and external business processes.

Technological Components: Any service, product or application that is part of Grupo Supervielle S.A. IT environment, such as, but not limited to: applications, software, hardware, connectivity components, development tools, monitoring tools, security components and protocols.

Information Custodians: Refers to persons or third parties that handle Grupo Supervielle S.A. information.

Information Owners: Representatives of Business Units responsible for information confidentiality, integrity, and availability, and for defining system access, grouped into what is called "Group/Profile," also having the responsibility to periodically control and validate users assigned to them. When necessary, Information Security may designate Groups/Profiles Owners for the application system that so requires.

Information Owners must be designated by the Business Unit Manager. Information Owners must be employees of Grupo Supervielle S.A., and belong to the operational areas responsible for the management of said information. The Business Unit Manager also appoints a replacement, who has the same powers and responsibilities.

In the case of services provided by third parties or by a supplier, responsibility of the Information Owner falls on the Business Unit that owns the service in question.

Technological Components Owners: They are members of Information Technology (IT) designated by the IT Manager, with authority to request, create, maintain, and eliminate technological components. The Technological Components Owners must be effective employees of Grupo Supervielle S.A. The IT Manager also appoints a replacement, who has the same powers and responsibilities.

Users: All employees, contractors, suppliers, consultants, and other people who carry out activities in Grupo Supervielle S.A. and who have been granted access to its information and technological components.

Supervisors: Business Unit people with responsibility for its users or for the service, product, information, or system provided by the business unit or support unit.

Personal data: Information of any kind referring to determined or determinable natural persons or legal persons.

Sensitive personal data: Personal data that reveals racial and ethnic origin, political opinions, religious, philosophical, or moral convictions, union membership and information regarding health or sexual preferences.