Information Security Policy

Table of contents

1. Management Declaration 1
2. Information Security Goals and Initiatives 1
3. Information Security Management System (ISMS) 2
4. Information Security Initiatives 2
5. Responsibilities and Roles 3
6. Scope of Application 3
7. Maintenance and Updating 3

1. Management Declaration

Considering the importance of information security for company objectives, the Board of C&F S.A. establishes an Information Security Management System (ISMS) and introduces this Information Security Policy as the foundational document of ISMS, declaring their commitment and support for ensuring information security within the company. The Board owns the ISMS and directly oversees compliance with the principles set out in this policy and related documents. The Board confirms its leading role in ensuring information security by providing necessary and adequate measures to minimize risks within the ISMS. Ensuring information security means ensuring the confidentiality, integrity, and availability of processed information and data using appro-priate methods tailored to the level of risk while maintaining accountability, reliability, and transparency princi-ples.

The procedures outlined in this document are the objectives of the entire organization, understood as C&F S.A. and its subsidiaries and affiliates, and therefore apply to all employees, associates, contractors, and subcontractors. Each of them is obliged to adhere to this policy and meet all the requirements defined in it and derivative documents.

2. Information Security Goals and Initiatives

1. This policy has been established to ensure actions are taken to support the organization in achieving its busi-ness objectives, in particular:
    - Data entrusted to us by clients and own data, including personal data, are protected in a way that is expected and appropriate to their value;
    - Solutions and services delivered to clients do not generate unknown and unacceptable risks;
    - Actions remain compliant with legal regulations concerning information security, particularly re-garding data protection;
    - Knowledge and specific skills developed over years of the company's activity remain protected;
    - Frameworks of mechanisms have been defined to continuously measure and improve processes related to ensuring information security within the organization.

2. These goals are achieved through the following information security objectives:
    - Compliance with laws, regulations, and contractual requirements (compliance), protection of informational assets, particularly intellectual property rights, contractual information, and the company's image;
    - Achieving and maintaining an appropriately high level of security of assets, understood as ensuring the confidentiality, integrity, and availability of resources, and ensuring accountability for actions taken by employees, associates, and suppliers;
    - Ensuring business process continuity and appropriate response to security incidents;
    - Providing an appropriate level of knowledge regarding information security among employees and associates, and continuous education and building broad information security awareness.

3. Information Security Management System (ISMS)

To achieve ISMS objectives, the following assumptions are applied:

1. Adapting to the Company's context - ISMS must be adapted to the external and internal context of the Company, considering the operations carried out and their scale;
2. ISMS effectiveness - ISMS must ensure a high level of compliance and security effectiveness in relation to the established acceptable risk level;
3. ISMS efficiency - ISMS must ensure a high ratio of achieved results to the costs of its implementation and maintenance;
4. Ease of use and agility - ISMS must be based on minimal formal requirements, with security integrated into existing organizational processes, and system changes must adapt to dynamic market conditions.
5. The ISMS references the ISO27001:2022 standard and is based on a process approach and the Deming cycle (PDCA - Plan, Do, Check, Act). This approach includes the following actions:
    5.1. Preparation and implementation
    5.2. Operation and maintenance
    5.3. Business continuity management
    5.4. Changes and continuous improvement.
6. A key element of ISMS is the risk management process. The functioning of ISMS is regulated by separate information security documents.

4. Information Security Initiatives

The defined information security objectives within ISMS are achieved through the following initiatives:

1. Ensuring continuous leadership and support for the development and improvement of ISMS;
2. Appropriate ISMS structures and processes based on an integrated GRC (governance, risk, compliance) approach embedded in the internal organizational order of the Company;
3. Proper documentation of ISMS resulting from external requirements and internal needs;
4. Ongoing risk management to have adequate information for making informed management decisions and striving to reduce risk to acceptable levels while maintaining a cost-benefit balance;
5. Proper protection of information, particularly legally protected information and intellectual and property rights;
6. Ensuring an appropriate level of confidentiality, availability, and integrity of information in information systems and the reliability of IT systems;
7. Continuously raising awareness and engagement of employees in building a culture and standards of information security;
8. Periodic monitoring, reviews, and audits of ISMS.

5. Responsibilities and Roles

1. Each employee and associate of C&F S.A. is responsible for information security. Key roles in information security management are played by suppliers and subcontractors within the supply chain processes.
2. Each employee, associate, and supplier is responsible for adhering to the security principles arising from adopted ISMS solutions. Supervision and compliance with ISMS regulations and principles, including maintenance and improvement, are the responsibility of the Information Security Officer delegated by the Company's Management Board.
3. Each person listed in points 1-4 exercises due diligence to ensure that the actions performed within their role are unquestionable, documented, and adequately proven after their completion.

6. Scope of Application

1. This Information Security Policy document is superior to all documents concerning information security in the Company.
2. The principles outlined in this document and the entire ISMS apply to the following processes and areas of activity:

   2.1. Software development and maintenance services

   2.2. Consulting and data management analytics services

   This includes information in the form of paper documents, electronic documents, and other forms processed in computer systems and networks, whether owned or administered by the Company at its headquarters.
3. All employees, within the meaning of the Labor Code regulations, all cooperating persons, and others with access to information subject to protection, are required to familiarize themselves with the relevant lower-order documents and apply the principles defined.
4. The principles of this policy are obligatory, to an appropriate extent, for partners, suppliers, clients, and Company cooperators, subject to the proportionality principle for employees obliging them to manage third-party risk.

7. Maintenance and Updating

1. The Information Security Officer reports directly to the Chief Operating Officer.
2. The Information Security Officer is responsible, in particular, for achieving and maintaining an appropriate level of security, conducting risk analyses together with process and information owners, developing and updating ISMS documentation, building a culture of information security through educational programs, training, awareness-raising, and promotional activities, as well as supervising the implementation and assessing the effectiveness of safeguards and monitoring the effectiveness of ISMS.
3. The Information Security Policy will be verified and adjusted to ensure an appropriate level of security in line with changing internal and external context requirements, including business requirements.
4. This document will be updated in case of changes in regulations related to information security, including to ensure compliance with relevant external acts and regulators.