INFORMATION SECURITY AND CYBERSECURITY POLICIES

Corficolombiana

Trabajamos e invertimos
en el progreso del país

TABLE OF CONTENTS

INFORMATION SECURITY AND CYBERSECURITY POLICIES

INTRODUCTION

The purpose of this document is to inform the officers of CORFICOLOMBIANA S.A., the Information Security and Cybersecurity Policy established for the protection of information.

This document includes the aspects that must be considered by all officers so that the information is accessed only by those who have a legitimate need to perform their business functions (Confidentiality); that it is protected against unauthorized modifications, made with or without intention (Integrity), that it is available when required (Availability), that it is used for the purposes it was obtained (Privacy) and that the events that occur when accessing the information are tracked (Auditability).

Therefore, CORFICOLOMBIANA S.A. officers must act considering the guidelines set forth in this document and those developed in the rules, standards and procedures, as they support the Information Security and Cybersecurity Policy, in the understanding that senior management is committed to supporting all activities necessary to achieve the goals and principles of information security, according to the responsibilities assigned within the organization in relation to this issue.

DEFINITIONS

- **Community**: The users of the business information.
- **Reliability**: The information must be appropriate for the administration of the Entity and the fulfillment of obligations.
- **Controls**: Safeguards based on devices or mechanisms that are required to comply with the requirements of a policy.
- **Effectiveness**: The relevant information must be pertinent and its delivery timely, correct and consistent.
- **Efficiency**: The processing and provision of information must be done with the best possible use of resources.
- I**nformation or Business Information**: It is all that regardless of its presentation, medium or format, in which it is created or used, serves to support business activities and decision making.

- **Internet**: It is the logical connection of multiple communication networks, which use as a standard the TCP/IP protocol to communicate and share data between these networks.

- **Community Member**: An individual who has limited and specific authority from the Information Responsible Party to view, modify, add, disclose or delete information.

- **Information Security and Cybersecurity Model**: Refers to the set of policies, procedures, standards, security rules, security features and topologies that ensure the protection of business information hosted in the technological infrastructure and cyberspace where the entity's services are established and/or provided through third parties.

- **Standard**: Set of rules required to implement the policies. The standards make specific mention of technologies, methodologies, application procedures and other factors involved and are mandatory.

- **Information Security and Cybersecurity Organization**: Organizational structure that supports Information Security and Cybersecurity, where roles and responsibilities of each of its members are defined.

- **Perimeters or secure areas**: An area or grouping within which a defined set of security policies and measures are applied to achieve a specific level of security. Areas or zones are used to group information assets with similar security requirements and risk levels, to ensure that each zone is properly separated from the others.

- **Policy**: It is a set of regulations and guidelines framed in the different legal and administrative instruments that govern a function, in this case Information Security and Cybersecurity.

- **Information Security and Cybersecurity Policy**: A document establishing the guidelines and directives related to the safe handling of information in CORFICOLOMBIANA S.A., which is hosted in the technological infrastructure and cyberspace where the services of the entity and/or those provided through third parties are established.

- **Procedure**: Specific operational steps that individuals must take to achieve the goals defined in the policies.

- **Information Resources**: Devices or elements that store data, such as: records, files, databases, equipment and proprietary software or licensed by CORFICOLOMBIANA S.A.

- **Information Responsible Party**: An individual or organizational unit that has responsibility for classifying and making control decisions regarding the use of its information.

- **Risk**: The probability of an information security event occurring that causes loss to CORFICOLOMBIANA S.A.

- **Information Security**: Protection of information against accidental or intentional unauthorized access, modification, destruction or publication.

- **Physical Security**: Protection of information processing equipment from physical damage, destruction or theft; also, personnel are protected from potentially harmful situations.

- **NTC-ISO/IEC 27001**: Security techniques. Information Security Management System (ISMS). Requirements.

- **Circular Letter 029/2014 - part I, Title II, chapter I (predecessor Circular Letters: 052/2008, Circular 022/2010 and 042/2012**: minimum safety and quality requirements for the performance of operations.

- **Circular Letter 014-038/2009**: Instructions on the review and adaptation of the Internal Control System (ICS).

- **NIST 800-53**: Provides a catalogue of security controls for all Federal Information Systems in the United States. Referenced by EC 007/2018 as one of the reference frameworks to be considered for cybersecurity risk management.

- **Cybersecurity**: The set of policies, security concepts, resources, security safeguards, guidelines, risk management methods, actions, research and development, training, best practices, insurance and technologies that can be used to prevent access, hindering, interception, damage, data breach, use of malware, theft of media and non-consensual transfer of computer assets, in order to protect financial consumers and entity assets in cyberspace.

- **Cyberspace**: Corresponds to a complex environment resulting from the interaction of people, software and services on the Internet, supported by technological devices and networks connected to the global network, owned by multiple owners with different operational and regulatory requirements.

- **Note**: For this document, cyberspace will be understood as the environment where the entity's services and those provided through third parties are established.

- **Cyberthreat**: Appearance of a potential or actual situation where an agent has the capacity to generate a cyber-attack against the population, the territory and the political organization of the State.

- **Cybernetics**: Science or discipline that studies the automatic mechanisms of communication and operation control or techniques of the connections of living beings and machines.

- **Cyber-attack**: Organized or premeditated action by one or more agents to cause damage or problems to a system through cyberspace.

- **Cyber-risk**: Possible negative outcomes associated with cyber-attacks.

- **Cybersecurity event**: Identified occurrence of the state of a system, service or network, indicating a possible violation of information security policy or safeguard failure or a previously unknown situation that may be relevant to security.

- S**IEM (Security Information and Event Management)**: Information system that provides real-time analysis of security alerts generated by applications, security devices and network elements. They are usually log centralization systems.

- **SOC (Security Operation Center)**: Entity or unit, where business information systems (websites, applications, databases, data centers, servers, networks, desktops and other devices) are monitored, evaluated and defended.

- **Vulnerability**: Weakness of an asset or control that can be exploited by a threat. All those threats that arise from the interaction of systems in cyberspace are taken into account.

- **Information at Rest**: Data stored on persistent storage devices (e.g., databases, data warehouses, spreadsheets, files, tapes, external backups, mobile devices, hard disks, among others).

- **Information in Transit**: Information that flows through the public network or is untrusted, such as the Internet and data traveling on a private network, such as a corporate or business local area network (LAN).

- **Critical Third Parties**: Third parties with whom the entity is linked and who can have a direct impact on the security of its information.

1. OBJECTIVE

Establish the guidelines and directives related to the safe handling of information, framed in international security standards (e.g. ISO 27001) and in standards of regulatory entities (Finance Superintendence -

Circular Letter 029/2014 - part I, Title II, chapter I, Circular Letter 014-038/2009, SIC – Law 1581/2012 and its regulatory decrees or subsequent that repeal or modify them).

This Information Security and Cybersecurity Policy is a statement of the policies, responsibilities and accepted conduct to protect the Business Information in CORFICOLOMBIANA S.A.

2. FUNDAMENTALS

2.1. Principles

CORFICOLOMBIANA S.A. has established as fundamental the following principles that support the Information Security and Cybersecurity Policy:

- Information is one of the most important assets of CORFICOLOMBIANA S.A. and therefore it must be used according to the requirements of the business and keeping quality criteria (Effectiveness, Efficiency and Reliability).

- The confidentiality of the Business Information, as well as that belonging to third parties, must be maintained, regardless of its medium or format.

- The Business Information must be preserved in its integrity, regardless of its temporary or permanent residence, or the form in which it is transmitted.

- Business Information must be available when required and by those authorized to use it; likewise, it must be presented in a timely manner when legal and regulatory requirements so require.

- The privacy of CORFICOLOMBIANA S.A.'s information must be preserved.

- The events that occur when accessing CORFICOLOMBIANA S.A.'s information must leave a trace and allow its sequence reconstruction, review and analysis.

2.2. General Objective

The main objective of the Information Security and Cybersecurity Policy is that CORFICOLOMBIANA S.A., protects itself against situations that represent a risk for the Confidentiality, Integrity, Availability, Privacy and Auditability of the information in the technological infrastructure and cyberspace where the services of the entity and/or those provided through third parties are established.

2.3. Specific Objectives

The specific objectives pursued by the Information Security and Cybersecurity Policy are:

- Establish the foundations for the development and implementation of the Information Security and Cybersecurity Model;
- Define the conduct to be followed with regard to access, use, management and administration of information resources found in local applications as well as those implemented in cyberspace;
- Establish and communicate responsibility for the use of information assets, which support business processes and systems that are implemented in the local technological infrastructure and the infrastructure established in cyberspace;
- Manage the information security and cybersecurity risks;
- Establish communication channels that allow the Presidency and the Board of Directors to be informed of the risks and inadequate use of information assets that may arise in the local technological infrastructure and the infrastructure established in cyberspace, and the actions taken for their mitigation and correction;
- Protect the image, interests and good name of CORFICOLOMBIANA S.A.
- Establish the conditions in the information management that allows CORFICOLOMBIANA S.A. to fulfill the regulatory framework demanded by the control entities that supervise it.

2.4. Organization of the Document

The document is essentially organized into two parts: The first part describes the general objective of the Information Security and Cybersecurity Policy, its characteristics, the responsible parties and how it should be developed, implemented and maintained. The second part develops individual Policies, which specify the conduct accepted by CORFICOLOMBIANA S.A. in the management of its information and the actions that must be taken to achieve the objectives of this Policy.

2.5. Scope

The Information Security and Cybersecurity Policy provides the guidelines required to implement a reliable and flexible Information Security and Cybersecurity Model, and defines the basic framework that

will guide the implementation of any rule, process, procedure, standard and/or action related to the Information Security and Cybersecurity.

This Information Security and Cybersecurity Policy applies to all levels of the organization: Users (which includes employees and shareholders), Customers, Third Parties (which includes suppliers and contractors), Control Entities and Related Entities[1]; which access, either internally or externally, any information asset regardless of its location. Additionally, this Policy applies to all information created, processed or used in support of the business, regardless of the media, format, presentation or location.

Declaration of Commitment

Corficolombiana and its Subordinate Entities are committed to the information security and cybersecurity policy, promoting a culture of compliance and control in accordance with the principles established by the information security and cybersecurity management system. Therefore, they must:

- Prevent damage to the image and reputation through the adoption and compliance with the information security and cybersecurity policy.
- Continuously promote a culture of information security and cybersecurity.
- Manage in a structured and strategic way the information security and cybersecurity risks associated with the business and their relationship with third parties.

Each employee, temporary officer and supplier is responsible for applying the criteria defined in this policy and for adjusting their actions in accordance with the corporate values and guidelines established with regard to information security and cybersecurity. They are also responsible for reporting incidents of which they may become aware.

2.6. Organization and Responsibilities

The administration of this Policy shall be the responsibility of those who within CORFICOLOMBIANA S.A. play the roles that make up the Information Security and Cybersecurity Organization (for further information, refer to the document “Information Security and Cybersecurity Organization Standards of Corporación Financiera Colombiana”).

[1] Throughout this document, the word “Community” shall collectively refer to all these individuals.

2.6.1. Information Security and Cybersecurity Committee

The party responsible for ensuring the planning, implementation and maintenance of the Information Security Policy; as well as the performance of the actions required to maintain the security levels established in the local technological infrastructure and in cyberspace.

Its members, powers, responsibilities and operation are described in the document referred to as Information Security and Cybersecurity Organization.

The Comptroller may attend as a guest, in its capacity as an evaluator of the internal control system, in the understanding that its presence allows it to have an updated knowledge of the activities carried out for the maintenance of the corporation's information security model and thus being able to request it in order to conduct selective evaluations on the subject.

2.6.2. Information Security and Cybersecurity Leader

The information security and cybersecurity leader will be responsible for issuing guidelines to ensure the implementation, improvements, maintenance, verification and compliance with the Information Security and Cybersecurity Policy and the means required to achieve it. One of these means is the preparation of an Information Security and Cybersecurity Model, which must ensure its proper development, maintenance and implementation. In addition, such officer shall represent CORFICOLOMBIANA S.A. internally and externally in all matters related to Information Security and Cybersecurity.

2.6.3. Computer Security and Cybersecurity

In accordance with the guidelines issued by the information security and cybersecurity area, it must effectively manage the information security and cybersecurity in the local technological infrastructure and the infrastructure established in cyberspace for the entity in order to keep the confidentiality, integrity and availability of the information, by securing, updating, identifying cyberthreats, remedying vulnerabilities, maintaining and monitoring the physical and logical elements necessary for the provision of the entity's services and those provided through third parties. The results of such management will be submitted to the board of directors every six months through the information security and cybersecurity area.

Its powers, responsibilities and operation are described in the document entitled "Information Security and Cybersecurity Organization".

2.6.4. Responsible Party for the Information

All officers of CORFICOLOMBIANA S.A. must be responsible for the confidentiality and preservation of the information. A Responsible Party for the Information means whoever requires the information in order to carry out its business and whoever has the responsibility for managing it and classifying it, according to the importance it has for its area. It must also ensure compliance with the Information Security and Cybersecurity Policy within its area and to be able to do so, it must know the value of its information, the users that must have access to it and the privileges for its use.

2.6.5. Community (Information Users)

They are the other subjects that use the information and are responsible for protecting the information assets of CORFICOLOMBIANA S.A. by means of compliance with the Information Security and Cybersecurity Policy. Likewise, they must be alert to identify and report any breach or lack of compliance with the established rules or procedures.

CORFICOLOMBIANA S.A. shall define the roles and responsibilities required to complete the definition of the Information Security and Cybersecurity Organization, always ensuring the segregation of tasks as a method to reduce risks in the misuse of information.

2.6.6. Lines of Defense

In order to adopt and maintain a strong culture of Information Security and Cybersecurity, the three lines of defense must take the lead according to the following definitions:

2.6.6.1. First Line of Defense

The first line of defense is made up of the areas of computer security and all the employees of Corficolombiana and its Subordinate Entities. The information security and cybersecurity policy recognizes the areas of computer security and other employees as responsible in the first place for identifying, evaluating, managing, monitoring and reporting the information security and cybersecurity risks and incidents inherent in security products, activities, processes and systems. Those who make up this line of defense must know their activities and processes, and have sufficient resources to effectively perform their tasks.

2.6.6.2. Second Line of Defense

This line of defense is made up of the areas of information security and cybersecurity or equivalent areas of each entity, which must establish the guidelines in this matter and continuously monitor the fulfillment

of all the obligations related to the Information Security and Cybersecurity Risk. The Information Security Officer may also perform the role of Risk Director, Compliance Officer or equivalent. This person responsible must present the management results directly to Senior Management or the Audit Committee. In the event of separation of tasks, the relationship between the abovementioned officers and their respective duties must be clearly defined and known. Likewise, he must have sufficient resources to effectively perform all his functions and play a central and proactive role in the Information Security Management System. To this end, he must be fully familiar with the policies and standards in force, their legal and regulatory requirements and the Information Security risks derived from the business, including specific Cybersecurity issues.

2.6.6.3. Third Line of Defense

The third line of defense plays an important role in independently assessing the management and controls of information security and cybersecurity risks, as well as systems policies, standards and procedures, reporting to the Audit Committee. The persons in charge of internal audits who must carry out these reviews must be competent and properly trained and not participate in the development, implementation and operation of the risk/control structure. This review can be performed by audit personnel or by personnel independent of the process or system being assessed, but it can also involve duly qualified external actors.

2.7. Compliance and Handling of Policy Violations

Compliance with the Information Security and Cybersecurity Policy with its respective rules is mandatory for the Community. Each member of the Community must understand its role, know and assume its responsibility regarding the risks in information security and cybersecurity and the protection of information assets of CORFICOLOMBIANA S.A. Any breach of this Policy that compromises the Confidentiality, Integrity, Availability, Privacy and/or Auditability of information, may result in a disciplinary action that may end up with the termination of the employment agreement and a possible initiation of a judicial process under national or international laws that apply.

The Information Security and Cybersecurity Policy is based on the best practices in information security and cybersecurity and is consistent with the national and international legislation, and therefore the necessary steps shall be taken, including the applicable disciplinary and/or legal measures to protect its assets and their use.

2.8. Management of the Policy and Change Procedure

The Information Security and Cybersecurity Policy must be preserved over time. Therefore, it is necessary to conduct an annual review or due to structural and regulatory changes that affect CORFICOLOMBIANA S.A. to ensure that it meets the changing needs of the business. The Official Information Security and

Cybersecurity Leader is responsible for this task and it must carry it out with the participation of the Information Security and Cybersecurity Committee. That is, due to the need of an addition or change in the Policy, the Information Security and Cybersecurity Leader will propose such changes and request approval from the Information Security and Cybersecurity Committee of CORFICOLOMBIANA S.A., for its subsequent submission to the Board of Directors.

Any member of the Community may identify the need to amend the Information Security and Cybersecurity Policy. Such concerns and suggestions should be communicated to the Information Security Official Director.

2.9. Exceptions to the Policy

There are no exceptions to this Policy.

2.10. Policy Implementation and Programming

The Information Security and Cybersecurity Policy involves the development and implementation of a vast Information Security and Cybersecurity program, integrated into the daily operation of CORFICOLOMBIANA S.A. An effective Information Security program is a continuous process, not an event. To achieve the objectives established in this document, this Policy anticipates and authorizes the development of norms, standards, detailed operating procedures and other administrative measures, which will be published for the knowledge of the officers; as well as the development or acquisition of software tools that help detect or prevent attacks against the systems where CORFICOLOMBIANA S.A. information resides, whether it is in local applications or in cyberspace.

3. INDIVIDUAL POLICIES

3.1. Information Security and Cybersecurity

THE BUSINESS INFORMATION IS A FUNDAMENTAL ASSET OF CORFICOLOMBIANA S.A. AND THEREFORE IT MUST BE PROTECTED

The information of CORFICOLOMBIANA S.A., regardless of its presentation, media or format in which it is created or used for the support of the business activities is classified as business information or information asset.

The business information security is the set of protection measures taken by CORFICOLOMBIANA S.A. against the disclosure, amendment, theft or accidental or malicious destruction of its information. Those protection measures are based on the relative value of the information and the risk of being compromised.

The information responsible parties are the parties responsible for ensuring that the business information has the appropriate protection to preserve the Confidentiality, Integrity, Availability, Privacy and Auditability of the information.

CORFICOLOMBIANA S.A. must have the necessary means to ensure that each member of the Community preserves and protects the information assets in a coherent and reliable manner. Any person attempting to disable, defeat or overcome any security control shall be subject to the corresponding disciplinary actions.

CORFICOLOMBIANA S.A. must have an organizational structure for the information security and cybersecurity that allows managing and controlling the provisions in the Security Information and Cybersecurity Model.

3.2. Intellectual Property

OWNERSHIP OF INFORMATION MUST BE MAINTAINED

Intellectual Property is defined as any patent, copyright, invention or information that is owned by CORFICOLOMBIANA S.A.

Any material developed while working for CORFICOLOMBIANA S.A. is deemed its intellectual property and of exclusive use thereof; therefore, it must be protected against any disclosure, discovery or use that damages the competitiveness of CORFICOLOMBIANA S.A.

3.3. Information Responsible Parties

EACH INFORMATION ASSET OF CORFICOLOMBIANA S.A. MUST HAVE A RESPONSIBLE PARTY THAT MUST ENSURE ITS SECURITY BASED ON THE RISKS TO WHICH IT IS EXPOSED

CORFICOLOMBIANA S.A. uses information to perform its activities. It is created and delivered to each member of the Community to be developed and comply with its respective goals within the business framework.

The information used by CORFICOLOMBIANA S.A. for the development of its business objectives must have a Responsible Party, who uses it in its area and who is responsible for its correct use. Thus, he makes the decisions required for the protection of his information and determines which are the users and their use privileges. The Vice-Presidents, Managers and other holders of the departments directly reporting to the Presidency or those delegated by them shall act as Information Responsible Parties in CORFICOLOMBIANA S.A.

3.4. Compliance with Regulations

CORFICOLOMBIANA S.A. MUST COMPLY WITH THE LOCAL AND INTERNATIONAL REGULATIONS ON INFORMATION SECURITY AND PRIVACY AND CYBERSECURITY

The Information Security and Cybersecurity Policy is in accordance with, and supports compliance with the local and international laws and regulations relative to privacy, Information Security and cybersecurity. Therefore, those requirements must be included in the development of the Information Security and Cybersecurity Model and specific actions must be established to permanently maintain CORFICOLOMBIANA aligned with those provisions. Examples of those provisions are the bank reserve, software licensing, circular letters from the Finance Superintendence and those resulting from international groups such as the Basel Committee on Financial Entities Supervision.

Likewise and in order to maintain a good security level, this Policy must be supported on the best information security and cybersecurity practices.

3.5. Risk Management in Information Security and Cybersecurity

THE INFORMATION SECURITY AND CYBERSECURITY RISKS TO WHICH THE INFORMATION OF CORFICOLOMBIANA S.A. IS EXPOSED MUST BE IDENTIFIED, ASSESSED AND MITIGATED IN ACCORDANCE WITH THEIR VALUE, LIKELIHOOD OF OCCURRENCE AND IMPACT ON THE BUSINESS

The business information must be protected based on its value and the risk of being compromised. Therefore, through the Committee on Information Security and Cybersecurity, an analysis of the business conditions before the information security and cybersecurity must be periodically performed to determine or update the relative value of information, the risk level to which it is exposed and the respective Responsible Party.

Once the risk level and the information value are established, each Responsible Party must perform a formal risk assessment for these to be identified, assessed and the necessary actions are applied to correct or mitigate them pursuant to the risk levels allowed by CORFICOLOMBIANA S.A.

Each user of the information must be aware of the reporting procedures for risks that may have an impact on the information security of CORFICOLOMBIANA S.A. and they are required to immediately report any suspicion or observation of an incident to the information security and cybersecurity.

3.6. Training and Creation of Culture in Information Security and Cybersecurity

CORFICOLOMBIANA S.A. MUST ESTABLISH A PERMANENT PROGRAM FOR THE CREATION OF CULTURE IN INFORMATION SECURITY AND CYBERSECURITY FOR USERS AND THIRD PARTIES

CORFICOLOMBIANA S.A. must have a permanent program that allows ensuring that the users and third parties are informed about their responsibilities in Information Security and Cybersecurity and the ongoing threats that jeopardize the information it handles.

The officers and third parties must be aware of the information security and cybersecurity procedures that must be applicable in addition to those required to perform their work function. As part of their training program, the new personnel must attend during the training period a conference on information security and cybersecurity requirements of CORFICOLOMBIANA S.A.

3.7. Security in Personnel

CORFICOLOMBIANA S.A. MUST PROVIDE THE NECESSARY MECHANISMS TO ENSURE THAT ITS EMPLOYEES COMPLY WITH THEIR RESPONSIBILITIES ON INFORMATION SECURITY AND CYBERSECURITY FROM ENTRY TO SEPARATION

The employees joining CORFICOLOMBIANA S.A. must follow a selection process and once they are engaged, they shall receive a copy of the document “Information Security and Cybersecurity Policy” for their knowledge and certification.

The employment agreements must include clauses that indicate the corresponding responsibilities for information security and cybersecurity and compliance with the code of conduct, informing the employees the consequences in case these are not followed or met.

A log per employee must be kept for its knowledge and understanding of the Information Security and Cybersecurity Policy, through the certification of this document and the other rules and procedures issued in that regard.

CORFICOLOMBIANA S.A. shall develop a suggestion management program for information security and cybersecurity, by means of which the employees shall report vulnerabilities and risks detected.

3.8. Third Parties Accessing Information of Corficolombiana S.A., Locally or Remotely, in the Local Application or Cyberspace

THIRD PARTIES LOCALLY OR REMOTELY USING INFORMATION OF CORFICOLOMBIANA S.A. MUST COMPLY WITH THE INFORMATION SECURITY AND CYBERSECURITY POLICY

The use of CORFICOLOMBIANA S.A. information by Third Parties, whether it is in local applications or in cyberspace and which can be locally or remotely accessed, must be formalized through agreements and/or clauses that enforce compliance with this Policy. The agreements must include the obligation to protect the information of CORFICOLOMBIANA S.A., the security requirements to mitigate the risks on the information and cybersecurity and the consequences to which they would be subject in case of breaching it.

Each relationship with a third party must have a high-level representative (such as Vice-President, Manager or its Delegates) inside CORFICOLOMBIANA S.A. that ensures the correct use and protection of the business information. In view of the foregoing, and given the characteristics of the businesses handled in CORFICOLOMBIANA S.A., where third parties furnish financial information for analysis and valuation processes, the respective confidentiality agreements shall be subscribed in order to ensure that the information furnished is kept in reserve.

3.9. Individual Identification and Authentication

ALL THE USERS ACCESSING THE INFORMATION OF CORFICOLOMBIANA S.A. MUST HAVE A MEANS OF IDENTIFICATION AND ACCESS MUST BE CONTROLLED THROUGH A PERSONAL AUTHENTICATION

Each user is responsible for its actions while using any information resource of CORFICOLOMBIANA S.A., whether local or in cyberspace. Therefore, the identity of each user of the computer resources shall be solely established and authenticated and it may be not shared.

The users of CORFICOLOMBIANA S.A. once created and once their authorizations are assigned in the Information System, may access the information through their user and authentication key. Depending on the information value and the risk level, CORFICOLOMBIANA S.A. shall define appropriate authentication means that may not be shared (such as the access key) and those authentication means contain confidential information that must not be disclosed or stored in places where they can be accessed by non-authorized persons.

3.10. Control and Management of Access to Local or Cyberspace Information

THE USE OF INFORMATION OF CORFICOLOMBIANA S.A. MUST BE CONTROLLED TO PREVENT NON-AUTHORIZED ACCESS. THE PRIVILEGES ON THE INFORMATION MUST BE MAINTAINED IN ACCORDANCE WITH THE BUSINESS NEEDS LIMITING ACCESS ONLY TO WHAT IS REQUIRED

Physical and logical access control mechanisms must be maintained to ensure that the information assets are kept locally protected and in cyberspace in a coherent manner with their value for the business and the risks of loss of Confidentiality, Integrity, Availability, Privacy and Auditability of information.

The access rights must not compromise the segregation of tasks and responsibilities. The access made locally and/or in cyberspace to the information of CORFICOLOMBIANA S.A. shall only be granted to authorized users, based on what is required to perform the tasks related to their responsibility. Access to the resources of CORFICOLOMBIANA S.A. must be restricted in all cases and it must be specifically given under the premises of need to know and less privilege as possible.

3.11. Information Classification

THE INFORMATION RESPONSIBLE PARTIES MUST CLASSIFY THE INFORMATION BASED ON ITS VALUE, SENSITIVITY, RISK OF LOSS OR COMMITMENT AND/OR LEGAL WITHHOLDING REQUIREMENTS

As well as other assets, not all the information has the same use or value and therefore, it requires different protection levels. Any information of CORFICOLOMBIANA S.A. shall be classified by the Information Responsible Party based on a high-level analysis of the impact to the business in information security and cybersecurity, that determines its relative value and risk level to which it is exposed.

According to the risks detected, the Information Responsible Party and the Information Security Leader shall determine the controls necessary to provide an appropriate and coherent information protection level in CORFICOLOMBIANA S.A., without regard to the means, format or place where it is placed. These controls must be applied and maintained during the life cycle of the information, since its creation, during its authorized use and until its appropriate disposal or destruction.

Therefore, it must no be assumed that others are protecting the information, since the officers of CORFICOLOMBIANA S.A. have the duty to take the necessary measures to protect the information.

According to the information classification and the risks to which it is exposed, encryption controls must be implemented during the transmission and storage processes.

3.12. Business Continuity

ALL THE INFORMATION RESOURCES AND RELATED PROCESSES, WHETHER LOCAL OR IN CYBERSPACE, MUST HAVE A BUSINESS CONTINUITY PLAN AND BE PREPARED FOR ATTACKS AGAINST INFORMATION SECURITY AND CYBERSECURITY. THE CONTINUITY OF THE INFORMATION SECURITY AND CYBERSECURITY MANAGEMENT IS KEPT DURING CONTINGENCY SITUATIONS

The information must be available for its authorized used when CORFICOLOMBIANA S.A. requires it in the performance of its regular tasks. For that reason, procedures must be periodically developed, documented, implemented and tested to ensure a reasonable and timely recovery of the critical information of CORFICOLOMBIANA S.A., both locally and in cyberspace, without reducing the security levels established. This must be independent from the technological means used by CORFICOLOMBIANA S.A. and the possibility that the information is damaged, destroyed or is unavailable during a period of time.

CORFICOLOMBIANA S.A. shall establish immediate reaction measures that allow detecting and mitigating the effects of information security and cybersecurity attacks such as those of denial of services and the entry of a non-authorized code. These measures shall be based on procedures and elements that allow keeping CORFICOLOMBIANA S.A. informed about the existence of these threats, detecting the attacks immediately and performing the subsequent actions.

3.13. Physical Security

ALL PHYSICAL AREAS OF THE BUSINESS MUST HAVE A SECURITY LEVEL IN ACCORDANCE WITH THE VALUE OF THE INFORMATION PROCESSED AND MANAGED IN THEM. CONFIDENTIAL OR SENSITIVE INFORMATION FOR THE BUSINESS MUST BE KEPT IN PLACES WITH RESTRICTED ACCESS WHEN NOT USED. ALL OFFICERS MUST COMPLY WITH THE GUIDELINES FOR THE PHYSICAL PROTECTION OF THE RESTRICTED OR SENSITIVE INFORMATION THEY USE

The physical areas built to support the entire operation of the business must be provided with adequate controls (for example: doors, locks, card readers, biometrics, among others) according to the value of the information they contain.

CORFICOLOMBIANA S.A. computer resources must be physically protected against unauthorized access and environmental risks to prevent exposure, damage or loss of assets and disruption of the business activities.

Information classified as confidential or restricted must not be left unattended or without control, so CORFICOLOMBIANA S.A. must develop a program that allows preventing information critical for the

business from being accessed without authorization, which includes the implementation and compliance with the Clean Desktop and Clean Screen guidelines.

3.14. Non-Repudiation

THE AUTHENTICITY OF A BUSINESS OR ELECTRONIC TRANSACTION MADE BY CORFICOLOMBIANA S.A. MUST BE ENSURED, WHETHER LOCALLY OR IN CYBERSPACE

CORFICOLOMBIANA S.A. is increasingly relying more on electronic means to carry out its business. Therefore, for any business or transaction made by these means, CORFICOLOMBIANA S.A. must ensure the authenticity of each party involved and prevent any of them from denying its participation (non-repudiation).

When performing electronic business either locally or in cyberspace, traces must be generated that allow CORFICOLOMBIANA S.A. to resolve conflicts when any party denies its participation. These must be generated, saved and accessed in accordance with the Policies and Standards regulating these aspects in CORFICOLOMBIANA S.A.

3.15. Alert Management

CORFICOLOMBIANA S.A. MUST BE IMMEDIATELY ALERTED ON THE EXISTENCE OF VIOLATIONS TO THE INFORMATION SECURITY AND CYBERSECURITY POLICY

Situations or actions that violate this Policy must be detected, recorded and reported to the Official Information Security Director immediately (alerts). An event and incident management program must be developed that prioritizes such alerts and resolves them according to the information criticality for CORFICOLOMBIANA S.A. Said program must include the definition of an immediate reaction organization, in order to address these and other situations that CORFICOLOMBIANA S.A. deems critical.

3.16. Auditability of Information Security and Cybersecurity Events

CORFICOLOMBIANA S.A. INFORMATION SECURITY AND CYBERSECURITY RECORDS MUST BE PERMANENTLY REVIEWED TO ENSURE COMPLIANCE WITH THE INFORMATION SECURITY AND CYBERSECURITY MODEL

The Information Responsible Party must define the events deemed critical (for example: failed access attempts to the information system, deletion or alteration of information, among others) and the respective information security and cybersecurity records that must be generated. Information security and cybersecurity records must be activated, stored and permanently reviewed, and unexpected situations

must be timely reported to the Responsible Parties, as well as to the required levels. The records and means that generate and manage them must be protected by controls that prevent modifications or unauthorized access, to preserve the integrity of the evidence.

3.17. Connectivity

ALL CONNECTIONS TO PUBLIC NETWORKS MUST BE AUTHENTICATED TO PREVENT INFORMATION FROM BEING DISCLOSED OR ALTERED

Connections to CORFICOLOMBIANA S.A. private network must be carried out in a secure manner to preserve the confidentiality, integrity, availability and privacy of the information transmitted on the network. Likewise, all exit access to cyberspace and other companies must be carried out on networks approved by CORFICOLOMBIANA S.A.

Community members who connect to the private network must comply with this policy before making the connection. This also applies to any current or future connection in CORFICOLOMBIANA S.A. network using public networks.

The approval of the Information Responsible Party is required to remotely access CORFICOLOMBIANA S.A. information and said accesses must comply with the Identification and Authentication Policy.

3.18. Use of Computer Resources of the Local Business and in Cyberspace, of Mobile Devices and Mobile Work

COMPUTER RESOURCES PROVIDED TO THE COMMUNITY LOCALLY AND IN CYBERSPACE ARE FOR THE EXCLUSIVE USE OF THE BUSINESS

CORFICOLOMBIANA S.A. computer resources both local and in cyberspace are exclusively for the business purposes and must be treated as assets dedicated to providing the tools to perform the required work. Community members who attempt to access information for which they do not have an authorized business requirement are violating this Policy.

In the use of CORFICOLOMBIANA S.A. information, privacy must not be assumed. So, when it is used, records of the activity performed could be created, which can be reviewed by CORFICOLOMBIANA S.A. as provided in the document containing the Information Security and Cybersecurity Standards, which must be known and accepted by all officers. If so, the corresponding procedures will be performed in accordance with CORFICOLOMBIANA S.A. regulations.

CORFICOLOMBIANA S.A. reserves the right to restrict access to any information when deemed convenient. Personnel selected by CORFICOLOMBIANA S.A. may use restricted-use technology such as network monitoring, operating data and information security events. No unauthorized hardware or software will be loaded, installed or activated in the computer resources, without prior formal authorization from the Information Security Leader or corporate manager of IT and administrative services.

To access CORFICOLOMBIANA S.A. information, both local and in cyberspace, through means such as mobile devices or mobile work, controls necessary to reduce risks arising from these practices must be implemented.

3.19. Information Security and Cybersecurity in System Management Processes

EACH SYSTEM MANAGEMENT PROCESS OF CORFICOLOMBIANA S.A. MUST COMPLY WITH THIS INFORMATION SECURITY AND CYBERSECURITY POLICY

Activities, standards and responsibilities in information security and cybersecurity must be included within each system management process of CORFICOLOMBIANA S.A., in order to achieve compliance with the Information Security and Cybersecurity Policy and Standards.

The IT development and innovation area must create and maintain a methodology that controls the complete cycle of development and safe maintenance of systems and infrastructure. Information security and cybersecurity requirements must be identified prior to the design and development of the information technology and cybersecurity systems. During development, these requirements must be included within the systems and if a modification is required, it must strictly comply with the requirements for secure development and information security and cybersecurity that have been previously established. The Security level of a system cannot be diminished, so the information and systems in production will not be used for development, testing or maintenance of applications.

The implementation of a new system or significant change to the existing ones must be reviewed by a risk assessment, which allows the detection of risks, location of appropriate controls that mitigate or delete them and the safe operation.

The performance of a technological change that does not consider the Information security and cybersecurity requirements, exposes CORFICOLOMBIANA S.A. to risks. Therefore, each technological change must ensure compliance with the Information Security and Cybersecurity Policy and its respective standards, and in case of exposing CORFICOLOMBIANA S.A. to an information security and/or cybersecurity risk, it must be identified, assessed, documented, assumed and controlled by the respective Information Responsible Party.

The problem Management process records, allocates, follows up and resolves situations (problems) that compromise the availability of the services that technology provides to the business. The sources of this process are the problems derived from situations that break or compromise the Information Security and Cybersecurity Policy. Therefore, all the information security and cybersecurity problems of CORFICOLOMBIANA S.A. must be managed by this process, which based on a subsequent analysis will determine if they correspond to violations, problems or vulnerabilities in information security and/or cybersecurity, leading to the procedures established for each case.

4. REFERENCE DOCUMENTS AND ANNEXES

“Information Security and Cybersecurity Organization Standards Corporación Financiera Colombiana”

Click the following link to electronically certify having read this document

http://intranet:90/Certificacion/consulta.asp

5. CHANGES AFTER THE CREATION OF THE POLICY

Date	Version	Nature of the Change
Dec-06/2006	1	Policy creation.
Jun-23/2010	2	Document update. Information Security Policy framed within international standards (ISO 27001) and standards of regulatory entities (Finance Superintendence - Circular 052/2007, Circulars 014-038/2009). Members of the Information Security Committee. (Approved in Board of Directors, Minutes 1673).
Jul-11/2012	3	External Circular 052/2007 is updated by the current External Circular 022/2010. External Circular 014/2009 is deleted, with External Circular 038/2009 being in force. (Approved in Board of Directors, Minutes 1726).
Dec-21/2012	4	The text of the Introduction to the Policy, approved by the Board of Directors, is updated as recorded in minutes No. 1738 dated December 19, 2012.
Jun-12/2013	5	The following position is updated: System and Operations Manager for Corporate Systems and Operations Manager, in accordance with the change to the Organizational Structure approved in minutes of the Board No. 1748 dated 05/29/2013.
May-06/2015	6	The document is updated to be aligned with the new version of ISO 27001:2013 and the new Information Security directives (e.g. Personal Data Protection Act).
Aug-03/2016	7	The compliance officer is included in the information security committee replacing the comptroller, because the information security area depends on the compliance area and not the internal control area.
Nov-14/20	8	The policy is updated, including that related to cybersecurity, in order to comply with the requirements of CE 007/2018 issued by the Finance Superintendence. Circulars 029/2014 part I, Title II, chapter I are included (Proceeding Circulars: 052/2008, Circular 022/2010 and 042/2012, and circular 022/2010 is removed. NIST 800-53, Cybersecurity, Cyberspace, Cyberthreat, Cybernetics, Cyber Risk, Cybersecurity Event, SIEM, SOC, Vulnerability, Information at Rest, Information in Transit, Critical Third Parties are included as new definitions. Numeral 2.6.3, responsibility acquired by computer security, is included. Approved by minutes 1887 of the board of directors held on November 14, 2018.
May-31/2021	9	Review, update and alignment with Grupo AVAL's Corporate Policy on Information Security and Cybersecurity, as follows: ❍ Point "2.5 SCOPE" of the "Declaration of Commitment", mentioning that CORFICOLOMBIANA and its Subordinate Entities are committed to the information security and cybersecurity policy, is included. ❍ Numeral "2.6 ORGANIZATION AND RESPONSIBILITIES" includes the concepts of the three lines of defense. ❍ Numeral "2.8 ADMINISTRATION OF THE POLICY AND PROCEDURE OF CHANGE" is amended in reference to the frequency to update the security policy. Approved by minutes 1947 of the board of directors held on May 26, 2021.

www.corficolombiana.com
www.investigaciones.corficolombiana.com

Corficolombiana S.A
@corficolombiana
Corficolombiana
Investigaciones Económicas Corficolombiana