GENERAL POLICY OF DATA SAFETY

1. INTRODUCTION

1.1. CYA understands that corporate information is an essential asset for its activities.

1.2. CYA understands that the handling of its information and/or that of its CUSTOMERS goes through different storage and communication media, which are vulnerable to external and internal factors that may compromise information security corporate.

1.3. CYA uses Risk Management, Vulnerability Management, Management of Incidents, Incident Response Plans and Awareness Campaigns so that the information protection objectives are achieved and establishes the use acceptable use of resources so that its employees and/or service providers able to perform their functions.

1.4. CYA uses mechanisms, tools and services from manufacturers worldwide recognized and certified in the most diverse security standards to support your Information Security strategy.

1.5. In this way, CYA establishes its General Information Security Policy, as integral part of its corporate management system, aligned with good practices and internationally accepted standards, with the aim of guaranteeing adequate levels of protection of CYA's and/or its CLIENTS' information.

2. PURPOSE

2.1. This policy is intended to establish guidelines and safety standards for the Information that allows CYA employees and/or service providers to adopt standards of safe behavior appropriate to CYA's goals and needs;

2.2. Provide guidance on the adoption of controls and processes to meet the requirements for information security;

2.3. Safeguard the information of CYA and/or its CLIENTS, guaranteeing requirements adequate standards of confidentiality, integrity, availability and privacy;

2.4. Prevent possible causes of incidents and CYA's legal liability;

2.5. Minimize the risks of financial losses, market share, CUSTOMERS or any other negative impact on CYA's business as a result of security flaws.

3. SCOPE

3.1. This policy applies to all CYA employees and/or service providers.

4. GUIDELINES

4.1. The objective of CYA's Information Security Management is to ensure the systematic and effective of all aspects related to information security, supporting critical business operations and minimizing identified risks and its possible impacts.

4.2. The Board of Directors and the Information Security Management Committee are committed to effective management of information security at CYA. In this way, they all reasonable steps to ensure that this policy is adequately communicated, understood and followed at all levels of the organization. Periodic reviews will be carried out to ensure its continued relevance and suitability for the needs of CYA.

4.3. It is CYA policy:

4.3.1. Develop, implement and fully follow policies, rules and procedures for information security, ensuring that the adequate requirements of confidentiality, integrity, availability and privacy of the CYA and its CUSTOMERS are affected through the adoption of controls against threats from both external and internal sources.

4.3.2. Make security policies, standards and procedures available to all parties interested and authorized.

4.3.3. Ensuring education and awareness of the practices adopted by the CYA of information security.

4.3.4. Fully meet applicable information security requirements or required by regulations, laws and/or contractual clauses.

4.3.5. Fully handle information security incidents, ensuring that they are properly recorded, classified, investigated, corrected, documented and, where necessary, communicating to the appropriate authorities.

4.3.6. Ensuring business continuity through adoption, deployment, testing and continuous improvement of incident response plans.

4.3.7. Continuously improve Information Security Management through definition and systematic review of security objectives at all levels of the Organization.

5. COMMUNICATION OF SECURITY INCIDENTS TO THE NATIONAL AUTHORITY OF DATA PROTECTION

CYA will communicate to the National Data Protection Authority (ANPD) and to the data subjects the occurrence of a security incident, which may entail a risk or material damage to the holders.

Said communication must be made within a reasonable period, as defined by the national authority, and must mention, at a minimum:

I. a description of the nature of the personal data affected;

II. information about the holders involved;

III. an indication of the technical and safety measures used for the data protection, observing commercial and industrial secrets;

IV. the risks related to the incident;

V. the cause of the incident;

SAW. the impact of the incident;

VII. the reasons for the delay, in the event that the communication has not been immediate; and

VIII. the measures that have been or will be adopted to reverse or mitigate the effects of the damage.

6. ROLES AND RESPONSIBILITIES

6.1. INFORMATION SECURITY MANAGEMENT COMMITTEE

6.1.1. It is the responsibility of the INFORMATION SECURITY MANAGEMENT COMMITTEE:

6.1.1.1. Analyze, review and propose the approval of related policies and standards information security;

6.1.1.2. Ensuring the availability of the necessary resources for an effective Information Security Management;

6.1.1.3. Ensuring that information security activities are carried out in accordance with the General Information Security Policy;

6.1.1.4. Promote the dissemination of Information Security Policies and take the necessary actions to disseminate a safety culture in the information in the CYA environment.

6.2. INFORMATION SECURITY DEPARTMENT

6.2.1. It is the responsibility of the Information Security department:

6.2.1.1. Conduct the management and operation of information security, having as based on this policy and other resolutions of the Security Management Committee of Information;

6.2.1.2. Support the Information Security Management Committee in its deliberations;

6.2.1.3. Prepare and propose to the Information Security Management Committee the information security standards and procedures, necessary to enforce the General Information Security Policy;

6.2.1.4. Identify and assess the main threats to information security, as well as propose and, when approved, implement corrective measures to reduce risk;

6.2.1.5. Take reasonable action to enforce the terms of this policy;

6.2.1.6. Manage information security incidents, ensuring proper treatment.

6.3. INFORMATION MANAGERS

6.3.1. It is the responsibility of Information Managers:

6.3.1.1. Manage the information generated or under the responsibility of your area business throughout its lifecycle, including creating, handling and disposal in accordance with the standards established by the CYA;

6.3.1.2. Periodically review the information generated or under the responsibility your business area, adjusting their classification according to required;

6.3.1.3. Authorize and review access to information and information systems under your responsibility;

6.3.1.4. Request the granting or revocation of access to information or systems information in accordance with the procedures adopted by the CYA.

6.4. HUMAN RESOURCES DEPARTMENT

6.4.1. It is the responsibility of the Human Resources department to:

6.4.1.1. Support the creation of the CYA code of ethics and conduct;

6.4.1.2. Assist in the dissemination of the Information Security culture;

6.4.1.3. Support the definition and execution of disciplinary actions applied by the CYA.

6.5. MANAGERS AND COORDINATORS

6.5.1. It is the responsibility of managers and coordinators:

6.5.1.1. Request the information technology team to grant access to new collaborators or collaborators who need new access according to changes in their work activities;

6.5.1.2. Have an exemplary posture in relation to information security, serving as a model of conduct for the employees under its management;

6.5.1.3. Assist in the dissemination of the Information Security culture.

6.6. LEGAL DEPARTMENT

6.6.1. It is the responsibility of the legal department:

6.6.1.1. Monitor any legal and/or regulatory changes;

6.6.1.2. Include in the contracts specific clauses related to the security of the information;

6.6.1.3. Take appropriate legal action in case of incidents;

6.6.1.4. Ensuring that the legal bases used in the processing of personal data comply with the legislation.

6.7. INFORMATION TECHNOLOGY

6.7.1. It is the responsibility of information technology management to:

6.7.1.1. Receive and review requests to create access accounts or provision of privileges for employees and/or service providers services;

6.7.1.2. Grant, when authorized, access to employees and/or service providers, as indicated by information managers;

6.7.1.3. Revoke, when requested, the access of employees and/or providers service, as indicated by the information managers;

6.7.1.4. Support the periodic review of the validity of access credentials of employees and/or service providers providing information about the privileges currently in effect on information assets/systems;

6.7.1.5. Perform end-of-life information disposal procedures of assets in the technological field, using good practices and techniques that render the original information unrecoverable;

6.7.1.6. Prepare and maintain an inventory of equipment provided by CYA to its employees for the performance of their activities in accordance with the standards defined by the Information Security Management;

6.7.1.7. Document and monitor all accounts as well as analyze activity suspicions reported by available tools;

6.7.1.8. Implement and maintain the security controls defined by Management Information Security in the technological field;

6.7.1.9. during shutdown

7. SANCTIONS AND PUNISHMENTS

7.1. Violations, even if by mere omission or unconsummated attempt, of this policy, as well as other safety standards and procedures may lead to measures applicable disciplinary measures, including:

- Orientation;
- Verbal Warning;
- Written notice;
- Suspension;
- Dismissal without just cause;
- Dismissal for just cause.

7.2. The disciplinary measure adopted must be reasonable and proportionate to the fault committed, being applied as soon as possible. A longer period is allowed for the application of measures when the lack requires verification of the facts and the due responsibilities.

Similar violations should receive similar sanctions.

8. OMISSIONS

8.1. Omissions will be evaluated by the Information Security Management Committee to further deliberation.

9. REVISIONS

9.1. This policy is reviewed on an annual basis or in accordance with the Committee's understanding. Information Security Manager.

10. TOP MANAGEMENT COMMITMENT

10.1. The CYA Board of Directors, upon approving this General Information Security Policy, establishes a commitment to the continuous improvement of procedures related to

with information security, always seeking to keep CYA in compliance with legal and regulatory norms on these topics, guided by the principles, concepts, values and practices adopted here, with the objective of ensuring the confidentiality, integrity and availability of data from or through CYA controlled and the information systems used by it, allowing the institution prevent, detect and reduce vulnerability to security-related incidents information and protect the fundamental rights of liberty and privacy and the free development of the personality of the natural person.

11. POLICY MANAGEMENT

11.1. The General Information Security Policy is approved by the Management Committee of Information Security, in conjunction with the CYA Board of Directors.

11.2. This policy was approved on March 12, 2021.