INFORMATION SECURITY POLICY
ACO CARIBE, S.A.

1. IDENTIFICATION

Quality	Controller[1]
Company name	ACO CARIBE, S.A.
Identification	RUC: 155713427-2-2021 D.V. 94
Address	P.H. Pacific Center, Punta Pacifica, Tower A, Office No. 2000, Telephone: 6671-2702
E-mail	rui.rebelo@aco.com

2. OBJECTIVE

This policy is prepared by **ACO CARIBE, S.A.** with the objective of adopting the necessary and conducive measures to provide security to personal data, avoiding or reducing the risk of adulteration, loss, queries, use or unauthorized or fraudulent access and to be faithful to the principles of loyalty, purpose, proportionality, truthfulness, accuracy, transparency, confidentiality, lawfulness and portability.

3. GENERAL CONTENT

The information security policy of **ACO CARIBE, S.A.** enshrines measures administrative, technical and human resources to implement the security management system information, seeking to establish a framework of trust in the exercise of their duties between **ACO CARIBE, S.A.** and its suppliers, customers, staff and related third parties, all framed in strict compliance with the laws.

4. BASIC STANDARDS

The rules under which this policy is issued is Law 81 of 2019, of March 26, 2019, created by the Assembly of Deputies of the Republic of Panama and published in the Official Gazette No. 28743-A and its regulation by means of Executive Decree No. 285 of May 28, 2021 published in Official Gazette No. 29296-A issued by the Ministry of the Presidency.

5. DATA PROTECTION PRINCIPLES

In accordance with Law 81 of 2019 regulated by Executive Decree No. 285 of May 28, 2021 establishes the following principles that will be applicable to all the databases:

---

[1] Law 81 of 2021. Article 4, Paragraph 17. Definitions. For the purposes of this law, the following definitions shall apply: (Data Controller: Natural or legal, public or private law, lucrative or not, responsible for the decisions related to the processing of the data and who determines the purposes, means and scope, as well as issues related to these).

a. **Principle of loyalty:** Personal data must be collected without deception or falsehood and without using fraudulent, unfair or illicit means.

b. **Principle of purpose:** The data controllers must collect data for specific and legitimate purposes. The data may not be used subsequently in a manner incompatible or different with such purposes. The further processing of personal data for research purposes, studies, surveys or knowledge of public interest, will not be considered incompatible with the purposes that motivated the collection.

The purposes of the processing of the data will determine the term of conservation of these, after which the data controller will delete or delete them of your files, records, databases, dossiers, or systems of information, or, as the case may be, will subject them to a anonymization. In order to determine the data retention period, the will resort to the applicable laws in each case and the responsibilities of all order that must be attended to by the data controller or custodian of the database. In the case of personal data relating to convictions for crimes, administrative infractions or disciplinary offenses will be attended to as provided for in Article 30 of Law 81 of 2019.

c. **Principle of proportionality:** To know which data are adequate, relevant and minimum necessary for the purpose pursued with the data processing, the data controllers and, where appropriate, the custodians of the database, will take into account the state of the technology, the nature, scope, context and purposes of the processing.

To this end, they will be able to carry out and document impact assessments on protection of personal data in order to minimize the data subject of treatment, to know the risks involved in the treatments and to adopt the necessary measures and guarantees to mitigate them. The supervisory authority may define those cases in which it is it is advisable to carry out an impact assessment and establish the guidelines or standards to be followed in its development. The data controllers and the custodians of the databases shall adopt organizational measures that regulate access to personal data in your entity, in accordance with this principle by allowing access to them only to employees or public officials who need it for the development of their functions and limiting it to the amount of data and the time necessary for it.

d. **Principle of truthfulness and accuracy:** The data controllers they will take the necessary measures to keep accurate and up-to-date the personal data in their possession, in such a way as not to alter the reality of these as required for the fulfillment of the purposes that motivated their treatment.

e. **Principle of transparency:** Any information or communication to the holder of the personal data relating to the processing of these must be in a simple and clear language and keep him/her informed of all the rights that he/she has as the owner of the data, as well as the possibility of exercising the rights ARCO.

f. **Principle of confidentiality:** All persons involved in the processing of personal data are obliged to keep secret or reserve with respect to these, even when they have terminated their relationship with the holder or responsible for the processing of the data, preventing the access or use not unauthorized.

g. **Principle of legality:** In order for the processing of personal data to be lawful, should be collected and treated based on some of the conditions of legality recognized by Law 81 of 2019 and in accordance with what is described in the third section of this Chapter.

h. **Principle of portability:** The data subject has the right to obtain from part of the controller a copy of the personal data of structured way in a generic and commonly used format.

6. SCOPE OF APPLICATION

The information security policy applies to personal information about which **ACO CARIBE, S.A.** carries out any treatment, especially the information that rests on the digital and physical databases of the company.

7. RECIPIENT

In accordance with the foregoing, this policy is addressed to **ACO CARIBE, S.A.** in accordance with the Data processing policy - June 2022- in particular to collaborators and third parties linked that have as a function or their activities are related to the treatment of personal data collected and / or stored by the company, it will be of mandatory compliance and will be an integral part of the employment contracts.

8. PURPOSES OF THE SECURITY MANAGEMENT SYSTEM OF THE INFORMATION

a. Establish group and individual responsibilities for safety of the information of the areas and officials of **ACO CARIBE, S.A.**

b. Protect the information generated, collected, stored and processed by **ACO CARIBE, S.A.**

c. Minimize financial, operational or legal impacts due to improper use of the personal information collected and stored in the databases of **ACO CARIBE, S.A.**

d. Implement controls for database access in order to ensure the due custody.

e. Detect security incidents early and timely reports to the National Authority for Transparency and Access to Information (ANTAI).

f. Ensure compliance with legal, regulatory obligations and contractual established.

9. RESPONSIBLE WITHIN ACO CARIBE, S.A.

The following officers have been appointed to this policy:

ACTIVITY	CHARGE / OFFICIAL
Approval of the policy	Manager
Implementation of the policy: **a.** Structure, design and administer the ways for the protection of information through the policy. **b.** Establish the necessary controls within the company that guarantee the protection of the information. **c.** You coordinate the required activities with the staff of the company. **d.** Record and update the information in the Database of company. The custodian of the Database is the only responsible in front of the the National Transparency and Access to Information (ANTAI) **e.** Review the contents of the contracts when it involves international data transmission or transfer of personal belongings. **f.** Include the policy in employment contracts and other contracts with related third parties. **g.** Accompany and assist the company in the attention of the visits and the requirements made by the National Transparency and Access to Information (ANTAI)	Manager
Publication of the General policy	Manager
Implementation of the General policy	Manager
Training and coaching on the policy: **a.** Initial training **b.** Periodic training	Manager
Monitoring and supervision of the policy: **a.** Control and update company databases. **b.** Follow-up in particular on the collection, storage, use, circulation and deletion or disposal end of personal information, including the requirements to obtain the authorization of the holders. **c.** Access and correction of personal data. **d.** Conservation and deletion of personal information and databases of data. **e.** Responsible use of information, including controls of security **f.** Inclusion of confidentiality agreements and clauses and information management. **g.** Response, management and follow-up to requests, complaints and high claims by the holders of the information.	Manager

h. Keep files, material and information organized related to this policy and the policy of treatment of the information. **i.** Security incident management.	
Update and revision of the General policy	Manager

10. INFORMATION PROCESSING POLICY

ACO CARIBE, S.A. has an information processing policy since June of 2022, attached to this document.

11. PERIODIC REVIEW

ACO CARIBE, S.A. will carry out periodic reviews of this policy, at least once annually in order to update it, evaluate it and verify the controls for the safety of the information through feedback from company officials, contractors and related third parties.

12. PUBLICATION:

This policy has been disseminated among the collaborators and other people of **ACO CARIBE, S.A.** in conjunction with the information processing policy once it was reviewed and approved for execution.

The document will be available for consultation on the internal server and physicallyit will be delivered to each of the company's employees, who will be an integral part of your employment contract and the provision of services, as applicable.

13. PERSONAL INFORMATION COLLECTED AND STORED BY ACO CARIBE, S.A.

ACO CARIBE, S.A. processes personal information as follows:

GROUP	INFORMATION COLLECTED
COLLABORATORS	Names, identification, contact details, beneficiaries, professional references, business references, information about level of education, work experience, bank certificate.
SUPPLIERS	Names, identification, contact details, bank certificate.
CUSTOMERS	Names, identification, contact details, bank certificate.
PARTNERS AND BOARD MEMBERS	Names, identification, contact details, bank certificate.
CONTRACTORS (Tax auditor, accountant, lawyer)	Names, identification, contact details, bank certificate.

14. PURPOSES OF THE PROCESSING OF INFORMATION

In line with the information processing policy, the purposes for which **ACO CARIBE, S.A.** collects, stores and accesses personal information are the following:

COLLABORATORS:

a. To process personal information for the proper handling of all processes related to Human Talent within **ACO CARIBE, S.A.,** as well as for the sending of information related to such processes, such as: Promote the verification and evaluation procedures of applicants in the processes of selection, control and monitoring of the recruitment, verification processes and consultation of the veracity of the information, personal and/or job references, background disciplinary and/or judicial proceedings or those related to restrictive lists of risks, prevention of money laundering, corruption and financing of terrorism.

Support and execution of the collective benefits derived from a employment contract, such as, but not limited to: the enrollment of the collaborator and his beneficiaries for the issuance of payroll releases o payment tickets, membership and payment of contributions to the comprehensive system of social security, inscription and / or updating of beneficiaries before the comprehensive social security system, payroll payment, courses of training and education, care of wellness activities, manage the occupational health and safety system in the exercise of the different work activities and/or any other type of direct related information and indirectly the fulfillment of obligations arising from the contract employment, civil or commercial contract and with the Human Talent Administration;

b. Allow auditors access to personal information and data or third parties engaged to carry out internal audit processes or external aspects of the activity carried out by **ACO CARIBE, S.A.**

c. To consult and update the information and personal data, at any time, in order to maintain the veracity of the information

d. Contract with third parties for the storage and/or processing of the information and personal data for the correct execution of the processes and own Human Talent procedure, under the safety standards and confidentiality to which we are obliged.

SUPPLIERS AND CUSTOMERS:

a. **ACO CARIBE, S.A.** may collect information and personal data from suppliers to effectively meet the obligations arising from the purchase of goods or contracting of services;

b. Communications and notifications related to the contract or business the legal framework that binds the parties;

c. Carry out evaluations and selection of potential suppliers;

d. Compliance with tax and legal aspects with government entities and regulatory;

e. Establish business relationships to acquire goods or services;

f. Control and payments for goods and services received;

g. Qualitative and quantitative assessments of service levels received from suppliers;

h. Communication of Policies and procedures on how to do business with suppliers;

i. Process of control and accounting registration of obligations contracted with provider;

j. Consultations, audits and reviews derived from the business relationship with the supplier;

k. Any other activity necessary for the effective fulfillment of the commercial relationship between the supplier and **ACO CARIBE, S.A.;**

l. Verification on risk lists or restrictive lists, public lists, disciplinary, fiscal and criminal records;

m. Financial analysis.

15. INFORMATION SECURITY MEASURES

a. The guidelines on the processing of information carried out by **ACO CARIBE, S.A.** they will be issued exclusively by the management.

b. **ACO CARIBE, S.A.** will develop and implement the information security policy according to the standards indicated in the current regulations.

c. In order to ensure the availability, integrity and confidentiality of the information, **ACO CARIBE, S.A.** will employ and distribute to its officers equipment and/or mobile devices with cryptographic controls.

d. **ACO CARIBE, S.A.** will develop and implement a policy on the use of mobile devices corporate, which includes the target, the recipients, identification of the devices delivered, determination of the uses of such devices, consequences of non-compliance, commitments of the officials and prohibitions.

e. **ACO CARIBE, S.A.** will carry out a procedure of identification, use, administration and responsibility for the personal information on which you make any treatment.

Identification of information: identification and/or updating of information by reviewing contracts, purchase and/or service orders with the customers, suppliers and contractors for the purpose of determining the information that is required for the execution of the respective contract.

Classification of information: classification of information according to the criticality, sensitivity and reserve thereof, following the definitions of the Law 81 of 2019 and Executive Decree No. 285 of May 28, 2021.

Use: in accordance with the purposes provided for in this policy and the treatment of information.

Administration: as indicated in the table of responsible officers in the implementation and application of this policy.

f. **ACO CARIBE, S.A.** will maintain digital backup copies of the information in order to ensure its completeness and avoiding unauthorized access, modifications or deletions authorized.

g. **ACO CARIBE, S.A.** will implement access controls to the equipment, devices and files where the personal information on which you make any treatment.

This way they are included: use of users and passwords on each computer; use of profiles, users and passwords for access to the cloud; use of keys to access to the physical file; restricted access to networks, applications and/or systems of company information; user and password management by part solely of the company's

manager, who may create, modify and delete the same and shall notify each officer that the users (ID) and passwords are personal and non-transferable and should not be borrowed, modified, deleted or shared.

h. Traceability: **ACO CARIBE, S.A.** will implement mechanisms that allow traceability of the actions that officials take on the databases where record the personal information.

i. Deletion of information: **ACO CARIBE, S.A.** will implement mechanisms that allow the deletion of personal information that rests on databases physical and digital data, such as the acquisition of paper shredding machines and digital information erasure procedures without storage of copy.

j. **ACO CARIBE, S.A.** will conduct internal audits periodically to ensure the implementation and application of this policy.

k. **ACO CARIBE, S.A.** will enter into confidentiality and traffic ban agreements of information with officials, suppliers, customers and contractors.

l. **ACO CARIBE, S.A.** will implement mechanisms that allow the management of incidents of information security that allows personal information to be identified filtered, modified or deleted, timely report to the people involved and to the Superintendence of Industry and Commerce, as well as the measures to reduce the risk created on personal information.

m. **ACO CARIBE, S.A.** will conduct trainings to its officials on the management of the personal information that the company manages in its capacity as Responsible of treatment and will evaluate workers who have a specific role in the activities described in this policy. For this, the person responsible for the database processing, shall appoint an officer to be responsible for the custody of the database, as stated in article 47 of the Decree Executive 285 of May 28, 2021.

n. **ACO CARIBE, S.A.** will implement mechanisms that allow timely response to requests, complaints and claims of the holders regarding any aspect of the treatment.

16. BREACH

Failure to comply with this information security policy will be considered serious breach of the duties of the collaborators and will be just cause to terminate the employment contract.

Likewise, in contracts for the provision of services or any other nature, the breach is grounds for unilateral termination with just cause and without result in any type of compensation and/or recognition for damages.

17. VALIDITY

This information security policy of **ACO CARIBE, S.A.** will enter into force as of its publication and promulgation in June 2022.