Table of content

PRESENTATION OF THE MANUAL

The management of World Travel Assist, understanding the importance of proper information management, has committed to implementing an information security management system, aiming to adopt a framework of trust in the exercise of its duties with the State and citizens, all within the strict compliance with laws, international standard **ISO NTC IEC 27001: 2013**, and in alignment with the entity's mission and vision.

For World Travel Assist, the protection of information seeks to reduce the risks posed to its assets, systematically identifying them to maintain a level of exposure that ensures the integrity, confidentiality, and availability of the information, in accordance with the needs of the different identified stakeholders.

In accordance with the above, this policy applies to the Entity as defined in the scope, its employees, third parties, trainees, interns, suppliers, and the general public, taking into account that the principles on which the development of actions or decision-making around the ISMS will be determined by the following premises:

- Minimize risk across all functions of the entity.
- Adhere to the principles of information security.
- Comply with administrative function principles.
- Maintain the trust of clients, partners, and employees.
- Support technological innovation.
- Protect technological assets.
- Establish policies, procedures, and instructions regarding information security.
- Strengthen the culture of information security among employees, third parties, trainees, interns, and clients of World Travel Assist.
- Ensure business continuity in the face of incidents.

World Travel Assist has decided to define, implement, maintain, and continuously improve an Information Security Management System, supported by clear guidelines, in alignment with business needs and regulatory requirements.

The following are the 12 security principles that support the ISMS of World Travel Assist:

- - Responsibilities related to information security will be defined, shared, published, and

accepted by each employee, supplier, business partner, or third party.

- - World Travel Assist will protect information generated, processed, or stored by business processes, its technological infrastructure, and assets from risks arising from access granted to third parties (e.g., suppliers or clients), or as a result of internal outsourcing services.
- - World Travel Assist will protect information created, processed, transmitted, or stored by its business processes to minimize financial, operational, or legal impacts due to incorrect use. This requires the application of controls according to the classification of its proprietary or custodial information.
- - World Travel Assist will protect its information from threats originating from personnel.
- - World Travel Assist will protect processing facilities and technological infrastructure that support its critical processes.
- - World Travel Assist will control the operation of its business processes, ensuring the security of technological resources and data networks.
- - World Travel Assist will implement access controls for information, systems, and network resources.
- - World Travel Assist will ensure that security is an integral part of the information systems' lifecycle.
- - World Travel Assist will ensure effective improvement of its security model through appropriate management of security events and associated weaknesses in information systems.
- - World Travel Assist will ensure the availability of its business processes and operational continuity based on the impact of potential events.
- - World Travel Assist will ensure compliance with established legal, regulatory, and contractual obligations.

NOTE:These policies will be reviewed and updated if necessary on a semi-annual basis or sooner if an event necessitates it.

1. OBJECTIVE

The purpose of this manual is to define a framework for the development of the information security management system, aimed at protecting information and its assets against unauthorized use, disclosure or revelation, modification, damage, or loss, and to ensure compliance with applicable regulations and laws for WORLD TRAVEL ASSIST LATAM S.A.S.

2. SCOPE OF THE INFORMATION SECURITY POLICY

This policy is applicable to the processes described in the process map of World Travel Assist Latam SAS, which must comply with this requirement regardless of having additional or more restrictive policies, to enhance information security. The scope of this policy also includes suppliers, clients, third parties, and all stakeholders.

Each of the organization's processes will implement this policy in their activities and must report their compliance to the improvement process for monitoring the information security management system.

The policy must be available on the WTA corporate website at [https://wtabyhas.com/](https://wtabyhas.com), as well as in a common company repository and disseminated within the organization's facilities.

3. DEFINITIONS

Asset: According to [ISO IEC 13335-1:2004], any item that has value to the organization. It is also understood as any information or system related to the handling of such information that has value to the organization. It refers to any asset containing information, which has value and is necessary for carrying out the mission and operational processes of DAPRE. Assets can be classified as follows:

Confidentiality Agreement: A document in which employees of WORLD TRAVEL ASSIST LATAM S.A.S or those provided by third parties express their commitment to maintaining the confidentiality of the company's information, agreeing not to disclose, use, or exploit confidential information accessed in the course of their duties within the company.

Applications: All software used for information management. For example: SIGEPRE.

Authentication: A process aimed at ensuring the identification of a person or system.

Authenticity: The property that ensures information assets are only available by verifying the identity of a subject or resource. It guarantees that the identity of a subject or resource is as claimed and applies to entities such as users, processes, and information systems.

Confidentiality: Access to information is restricted to authorized individuals only. According to [ISO IEC 13335-1:2004], "the characteristic/property by which information is not available or revealed to unauthorized individuals, entities, or processes."

Control: All policies, procedures, practices, and organizational structures designed to keep information security risks below the acceptable risk level. (Note: Control is also used as a synonym for safeguard.)

Data: Basic elements of information (in any format) generated, collected, managed, transmitted, and destroyed in DAPRE. For example: Word file “listado de personal.docx”.

Auxiliary Equipment: All assets that support information systems but do not fall under any of the previously defined types. For example: air conditioning, paper shredder.

Information: An organized set of data contained in any document generated, obtained, acquired, transformed, or controlled by the obligated subjects. It constitutes a significant asset, essential for the activities of an organization, and consequently requires adequate protection. Information can exist in many forms, such as printed or written on paper, stored electronically, transmitted via mail or electronic means, displayed in videos, or presented orally in conversations.

Facilities: All locations where information systems are housed. For example: Accounting Office.

Integrity: The maintenance of accuracy and completeness of information and its processing methods. According to [ISO IEC 13335-1:2004]: the property/characteristic of safeguarding the accuracy and completeness of assets.

Personnel: All staff of DAPRE, subcontracted personnel, clients, users, and generally, all those who have access in any way to DAPRE's information assets. For example: Pedro Pérez.

Security Policy: Definition establishing the commitment of management and the organization's

approach to information security management.

Business Continuity Plan: A plan designed to ensure the continuation of the entity's critical functions in the event of an unforeseen occurrence that threatens them.

Information Security: According to [ISO IEC 27002:2005]: The preservation of confidentiality, integrity, and availability of information; additionally, other properties such as authenticity, accountability, non-repudiation, traceability, and reliability may also be considered.

ISMS (Information Security Management System): According to [ISO IEC 27001:2013]: A global management system that, based on risk analysis, establishes, implements, operates, monitors, reviews, maintains, and improves information security. (Note: The management system includes an organizational structure, policies, activity planning, responsibilities, procedures, processes, and resources.)

Services: Both internal services, those provided by one part of the organization to another, and external services, those provided by the organization to clients and users. For example: Resume publication, vacation requests.

Technology: All equipment used to manage information and communications. For example: computers, phones, printers.

User: In this document, refers to executives, employees, contractors, third parties, and other collaborators duly authorized to use equipment, systems, or IT applications, and who are provided with a username and password.

Vulnerability: A weakness in an organization's information security that potentially allows a threat to affect an asset. According to [ISO IEC 13335-1:2004]: A weakness in an asset or set of assets that can be exploited by a threat.

1. INFORMATION SECURITY POLICY

"World Travel Assist provides the necessary resources to establish and operate an information security management system that sets the guidelines to ensure the confidentiality, integrity, and availability of corporate information and that of all stakeholders, located in the information systems and software that store, process, and transmit information from all our processes, meeting the requirements and expectations of our clients. The system aims to protect information through the implementation and evaluation of the effectiveness of treatment plans, actions, and maintenance of physical, organizational, personnel, and technological controls, and establishes the following objectives:

- Minimize the risks to which information assets are exposed.
- Establish a culture of information security within the company.
- Ensure compliance with current legal, contractual, and business requirements.
- Adopt the information security guidelines stipulated in this document.
- Establish disciplinary and/or legal actions in response to non-compliance with these policies."

1. MOBILE DEVICE USAGE POLICY

WORLD TRAVEL ASSIST LATAM S.A.S has defined the following conditions for managing mobile devices (smartphones, tablets, etc.) for both institutional and personal use:

The company provides mobile devices solely for business purposes for each company process, equipped with the necessary resources such as data plans and minutes to fulfill their respective functions.

The company will ensure that employees use the provided equipment responsibly, in accordance with the **DC-MPR-018 CORPORATE CELLULAR LINES AND EQUIPMENT POLICY .** These usage reviews are conducted by the Information Security Officer according to the review schedule, with findings documented in the **FO-MPR-020 ATTENTION CALL RECORDS** form.

Management has established the following list of personnel authorized to use personal mobile devices within the organization:

Process	Name of Authorized

	Director:
General Management	Sabrina Morales
Process Improvement	Carolina Jaramillo
Accounting	Carolina León
Customer Loyalty	Mariana Vega
Human Resources	Paula Cocomá
Claims	Erika Rengifo
Quality	Luisa Mejía
TPA and Insurance Reporting	Felipe Navarrete
Technology	Andrés Ramírez
Suppliers	Andrés Mejía
Occupational Safety and Health	Vanessa Restrepo
Reimbursements	Catalina Moribe
Operations	Julio Carvajal
Medical Department	David Ñañez
Training and Development	Steven Castaño
Digital Developments	Arturo Álvarez

1. NETWORK AND NETWORK RESOURCE ACCESS POLICY

The Technology Management of WORLD TRAVEL ASSIST LATAM S.A.S, responsible for the company's data networks and network resources, employs various logical access control mechanisms to ensure that they are protected against any unauthorized access.

The company's wireless networks use authentication methods to prevent unauthorized access, including the use of firewalls and the HOST document with listed domains to which access is restricted. Additionally, the use of the KASPERSKY platform and its blocking features are implemented. A detailed description of the network management procedure is found in the document **DC-ITS-003 NETWORK AND TECHNOLOGICAL PLATFORMS MANAGEMENT.**

Computers that wish to connect to the company's data networks must meet all the requirements and/or controls for authentication (User credentials), as outlined in the procedure **PR-ITS-009 CONFIGURATION OF EQUIPMENT FOR BUSINESS USE,** and may only perform functions for which they are authorized.

The connection of third parties or visitors to the company's networks will be carried out according to the procedure **PR-ITS-012 PROCEDURE FOR THIRD PARTY ACCESS TO WTA NETWORK.**

Recreational websites not related to the company's work activities are restricted; however, a separate network with captive portal access (GUEST network) is available. This network, separate from the public business IP, allows access to these sites for recreational purposes only during non-working hours (lunch breaks and respective rest periods).

1. USER ACCESS MANAGEMENT POLICY

WORLD TRAVEL ASSIST LATAM S.A.S has established privileges for logical access control for each user or group of users to the company's technological resources and information systems, ensuring that employees and third-party personnel have access only to the information necessary for the performance of their duties.

The Technology Management has established the procedure **PR-ITS-016 CREATION, MODIFICATION, AND DEACTIVATION OF USER ACCOUNTS**, which outlines the creation, modification, blocking, or deletion of user accounts for managing users on the company's data networks, technological resources, and information systems. These actions must be carried out promptly when employees leave the company, take leave, are promoted, or are reassigned.

1. USER ACCESS RESPONSIBILITY POLICY

The purpose of this policy is to define acceptable access and use of all computational equipment, services, information systems, and data networks of **WORLD TRAVEL ASSIST LATAM S.A.S**. These rules are aimed at protecting employees and the organization from inappropriate use of information, network services, and computing equipment. The company will promote these actions by continuously raising awareness and informing staff, in accordance with the ongoing training plan of the ISMS, as evidenced in the document **FO-MPR-022 INFORMATION SECURITY SYSTEM PLANNING 2024.**

All employees, including third parties, should have access only to the information necessary for the legitimate performance of their functions and activities within the organization. The

allocation of privileges and access to information assets (institutional email, software, applications, shared folders, etc.) must be based on the needs of the areas and approved by the asset owner. The senior management determines the categorization of information assets based on confidentiality in the document **DC-MPR-010 INVENTORY AND CLASSIFICATION MATRIX OF INFORMATION ASSETS,** which specifies the usage permissions for each asset and which process or position is authorized for access.

Access for external parties to the institution may only be granted with prior authorization from the owner of the information processing medium and the information owner. Third-party access accounts must have an expiration time specified, which must be monitored by the Technology Process and process leader as applicable.

Employees are responsible for the user ID and password assigned for their access to the WTAOPS and Communicator information systems and must not share this information with other employees or third parties under any circumstances. For access to communication tools such as Skype and Gmail accounts, users can obtain access through the Technology Process, which will be responsible for setting passwords on each device. Grounds for breaches of this responsibility are detailed in **DC-MPR-016 ANNEX SECURITY BREACHES.**

Note: This policy is expanded in the **DC-MPR-013 ACCESS CONTROL POLICY** established by senior management.

1. PASSWORD USAGE POLICY AT WORLD TRAVEL ASSIST

Personal Passwords:

The organization specifies that for the WTAOPS and Communicator information systems, initial passwords are set by the provider. However, upon first login, the user must change their password in accordance with the policy and actions for creating secure passwords outlined below.

All passwords for accessing the WTAOPS operating system and the company's Communicator system are personal and non-transferable. Each employee is responsible for their password and must ensure that their passwords are not seen or learned by other employees.

Policy and Actions for Creating Secure Passwords:

1. Use at least 8 characters: Passwords should be composed of a minimum of 8 characters.
2. Include digits, letters, and special characters: It is recommended to use a combination of digits, letters, and special characters in a password.
3. Alternate between uppercase and lowercase letters: It is advisable to alternate randomly between uppercase and lowercase letters, remembering which letters are uppercase and which are lowercase.
4. Choose a memorable password: Select a password that is easy to remember and preferably one that can be typed quickly without needing to look at the keyboard.
5. Regularly change passwords: Passwords should be changed regularly; the operating system requires a password change every 3 months.
6. Use punctuation if allowed: If the system permits, use punctuation marks such as: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~. For example: “Tr-.3Fre”.

Actions to Avoid in Secure Password Management:

1. Avoid Using the Same Password Across Multiple Systems: Each system or service should have a unique password. For example, use a different password for WTAOPS and Communicator.

2. Do Not Use Personal Information in Passwords: Avoid using personal information such as the user’s name, family names, birthdates, identification numbers, or phone numbers.

3. Avoid Simple Keyboard Sequences: Do not use basic keyboard sequences (e.g., “qwerty”, “asdf”) or common numeric sequences (e.g., “1234”, “98765”).

4. Do Not Repeat Characters: Avoid repeating the same characters in a password (e.g., “111222”).

5. Avoid Using Only Numbers or Letters: Do not limit your password to just numbers, uppercase letters, or lowercase letters.

6. Do Not Use the Username in the Password: The password should not include the username or any part of it.

7. Avoid Easily Deductible Data: Do not use easily deducible data such as nicknames, favorite actor names, or fictional characters.

8. Do Not Write Passwords Down: Avoid writing down passwords on paper or in documents that may be accessible. Also, do not store passwords in text files on computers or devices.

9. Avoid Dictionary Words: Do not use words found in dictionaries, as modern password-cracking tools often use dictionary attacks to guess passwords.

10. Do Not Send Passwords via Email or SMS: Never send passwords through email, SMS, or mention them in any communication.

11. Avoid Unsecure Computers: Do not write passwords on computers with unknown security levels or on public computers (e.g., libraries, internet cafés).

12. Change Default Passwords: Always change default passwords provided by developers for systems like WTAOPS and Communicator.

Shared Passwords Managed by Technology:

Considering that information is a high-value asset for the organization, senior management has established the following guidelines for managing shared passwords for internal communication tools like Skype and Gmail accounts:

1. Centralized Management:
- Passwords for internal communication tools (e.g., Skype, Gmail) must be created, managed, and controlled by the Technology department. This approach helps prevent potential damage and misuse by employees.

2. No Direct Access for Employees:
- No employee is authorized to change passwords for Skype or Gmail accounts. If a password change is necessary, employees must request it through their process leader, who will then forward the request to the Technology department.

3. Strictly Professional Use:
- Communication tools provided by the organization are for business use only. Employees are responsible for any personal information shared via these tools, and the organization will not be held liable for such disclosures.

4. Authority for Review:

- The Technology department has the authority to review or verify information transmitted through Skype or Gmail accounts if requested by the process leader or management. This measure is in place to ensure the secure handling of information and compliance with organizational policies.

These measures are designed to maintain the security of internal communication channels and protect sensitive information from unauthorized access or misuse.

Tools and IT Solutions:

To comply with the policy and actions for creating secure passwords, our Technology department uses the following tool for password generation: [LastPass Password Generator](https://www.lastpass.com/es/features/password-generator#generatorTool).

The organization has established the following controls for password management:

1. Password Change Frequency:
- Passwords must be changed every 3 months.

2. Responsible for Creation and Update:
- The Technology Analyst is responsible for creating and updating passwords.

3. Separate Passwords for Skype and Gmail Accounts:
- Different passwords will be used for Skype and Gmail accounts to enhance security.

4. Password Storage:
- Passwords will be stored on each device only by the Technology department. Any requests or needs related to password use will require intervention from the Technology team.

5. Random Password Audits:
- The Technology department will conduct random password reviews for each department on a monthly basis, and will record these reviews in the Technology CRM system.

Policy on Security and Maintenance of Institutional Equipment

To prevent loss, alteration, or damage to the company's technological resources, the Technology Department of WORLD TRAVEL ASSIST LATAM S.A.S has established the following mechanisms and strategies to protect their integrity, both within and outside company facilities:

1. Delivery Records:

- Generation of delivery records with signatures of responsibility from both the end user and the leader of the corresponding process. **[FO-ITS-016 Equipment Delivery and Receipt Record for Computing Devices or Work Tools].**

2. Initial Configuration:

- Initial configuration of equipment according to the procedure **PR-ITS-009 CONFIGURACIÓN DE EQUIPOS PARA USO EMPRESARIAL**, including the setup of passwords and access credentials.

3. Preventive and Corrective Maintenance:

- The Technology Department will perform preventive and corrective maintenance on computing equipment and mobile devices as outlined in procedure **PR-ITS-001 MANTENIMIENTO PREVENTIVO DE EQUIPOS E INFRAESTRUCTURA TECNOLÓGICA.**

4. Authorized Movements and Assignments:

- The Technology Department is the sole authority for handling the movement and assignment of technological resources. Therefore, any disposition by employees of the company's technological resources is prohibited.

5. Reporting Issues:

- In the event of hardware or software issues with a workstation or other technological resources, the responsible user must report the issue to the Technology Department for proper assistance. Users should not attempt to resolve the problem themselves.

Privacy and Personal Data Protection Policy

WORLD TRAVEL ASSIST LATAM S.A.S is committed to protecting the personal data of its beneficiaries, suppliers, and other third parties from whom it receives and manages information.

As the custodian of personal data collected through various channels, the company has established the following terms and conditions for the processing of such information, ensuring that stored data:

Use Limitation:

- Is used solely for the company's functions, in accordance with the current national legislation, Law 1581 of 2012.

- Non-Disclosure:

- Is not published, disclosed, or shared with unauthorized personnel or third parties.

- Non-Alteration or Deletion:

- Is not altered or deleted without the required authorization.

Authorization for Data Processing:

- Areas that process personal data of beneficiaries or end-users must obtain authorization for the processing of these data (signed Record Release Form) to collect, transfer, store, use, circulate, delete, share, update, and transmit personal data in the course of the company's activities.

Access Control:

- Departments that process personal data of beneficiaries, employees, suppliers, or other third parties must ensure that only individuals with a legitimate business need—i.e., information necessary for performing job functions—have access to such data.

Secure Storage Tools:

- The company employs the following secure information storage tools to protect personal data:

[Specific tools and methods should be listed here, detailing encryption practices, access controls, secure storage solutions, and any other relevant measures.]

This policy ensures that personal data is managed in a secure and compliant manner, reflecting the company's commitment to privacy and data protection.

- WTAOPS Operating System: client information, end users
- Local network storage units (securely shared): employee information, internal process documentation, suppliers

Access to these units (securely shared) is restricted to process-related personnel only, thereby ensuring that no unauthorized individuals interfere with the information. Client data is managed directly and securely on our information system servers.

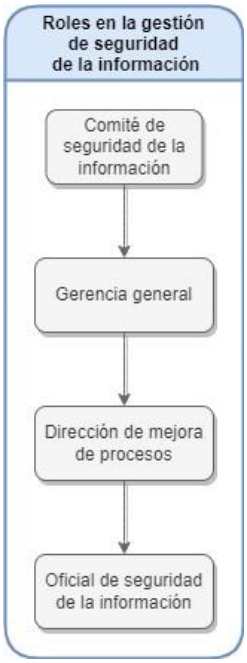
The organization establishes the **DC-MPR-022 PERSONAL DATA PROCESSING POLICY** to ensure compliance with Law 1581 of 2022.

1. INFORMATION SECURITY ORGANIZATIONAL STRUCTURE POLICY

In accordance with the commitment to the Information Security Management System, the company's management has pledged to allocate the necessary resources for the development and adherence to the Information Security Management System. Additionally, it has defined and established roles and responsibilities that encompass the operation, management, and administration of information security, as well as the existence of the Information Security Committee as outlined in its respective formation minutes.

Furthermore, management designates all process directors as responsible for adhering to the activities and policies of the system within their area, and for reporting any incidents to the Information Security Officer for the appropriate action plan.

The responsible officials designated by management are:



Position	Name	Responsibilities	Role / Function
Process Improvement Department	Carolina Jaramillo López	• Notify in a timely manner about changes and improvements made in your process that impact the management systems. • Actively participate in the organization's internal audit processes. • Take timely actions in response to nonconformities identified in the internal audit processes of the management systems. • Update the documentation of	• - Develop strategies that lead to the achievement of defined objectives. • - Create strategies that increase productivity and optimize resources. • - Manage business and information security risks to establish a risk analysis matrix

		your process with respect to the management system. • Direct the implementation and operation of the Information Security Management System (ISMS). • Comply with the general Information Security policy and the standards defined to meet the requirements of the Information Security Management System (ISMS). • Complete information security training.	with appropriate treatment. • - Coordinate internal audit activities and actions related to information security. • - Collaborate with other processes to apply organizational controls and information security controls. • - Review and evaluate management indicators related to security incident handling for presentation to senior management.
Information Security Officer	Brayan Moncada Hincapié	• -Maintain a comprehensive security policy. • - Develop, execute, and supervise information security strategies.	• - Implement and verify compliance with the security management system. • - Ensure adherence to security policies by all employees.

		• - Manage, handle, and monitor access control to the company's information. • - Enhance the information security culture. • - Properly use and manage the tools and equipment designated by the organization for performing duties. • -Comply with Occupational Health and Safety regulations and company-specific rules. • - Stay informed about industry developments and continually update knowledge to respond flexibly and efficiently to any cyber incidents affecting the company. • -Implement and monitor the information security training	• - Monitor security-related incidents. • - Guarantee maximum protection and privacy of corporate data and information. • - Oversee incident response planning and investigate security breaches. • - Coordinate the implementation of specific information security controls for new systems or services. • - Develop and execute information security training plans.

		plan.	

Information Security Committee		
Process	**Name**	**Role / Function**
Recursos Humanos	Cesar Lopez	• Support the implementation and operation of the Information Security Management System (ISMS). • Verify compliance with information security policie within each process. • Communicate all information related to the ISMS within each process. • Identify and share potential new risks related to information security.
Proveedores	Christian Rodas	
Calidad	Valentina Correa-Dana Ramos	
SG-SST	Sara Agudelo	
Customer	Paulina Jaramillo	
Médico	Manuel Ramirez	
Capacitación	Manuel Cuyato	
Reembolsos	Juan Manuel Betancurt	
Contabilidad	Laura Sánchez	
TPA	Jacobo Herrera	
Operaciones	Angela Gañan	

Users:

Users of the ISMS (Information Security Management System) are all organization employees and have the following responsibilities:

- - Adhere to information security policies
- - Report security incidents that threaten the confidentiality, integrity, or availability of information, or that indicate a violation of policies
- - Actively participate in all awareness and training campaigns related to the system
- - Support the development of internal and external audits of the system

Note: This policy is related to the **INFORMATION SECURITY COMMITTEE FORMATION MINUTES** and the **MN-MPR-002 INFORMATION SECURITY OFFICER JOB DESCRIPTION.**

Management of deviations and exclusions from the information security system:

Management conducts analysis and review of the controls in Annex A of NTC ISO 27001:2022. In compliance with the applicable organizational controls based on the organization's activities, the document **DC-MPR-017 STATEMENT OF APPLICABILITY i**s generated for managing deviations and exclusions.

1. SUPPLIER RELATIONS POLICY

Aware of the importance of maintaining the security of information and information processing services to which third parties or external entities have access, the company has established the following control mechanisms in contractual relationships to ensure that the information or services accessed or provided by suppliers or contractors meet information security standards.

Contractors, vendors, and/or suppliers must accept and sign the confidentiality agreement included in the contracts or agreements with suppliers and/or contractors. These agreements include a termination clause for non-compliance with information security policies. This information is managed according to procedure PR-RSC-002 Supplier Selection, Evaluation, and Reevaluation.

For this purpose, the organization establishes the following DC-MPR-020 SUPPLIER RELATIONS POLICY, which outlines the necessary information security guidelines.

2. CLEAN DESK AND SCREEN LOCK POLICY

The company has defined this policy with the objective of preventing unauthorized access, loss, and/or damage to information found at workstations, computing equipment, removable media, and document printing and scanning devices, during and outside of working hours:

- - All desks must remain clear and free of physical documents or removable media containing sensitive, restricted, or confidential information, except for the Human Resources, Accounting, and Occupational Health and Safety processes, as their duties require handling physical information. Printed reports containing sensitive, restricted, or

confidential information must be removed immediately from printers and either stored or promptly disposed of.

- - Only the Human Resources, Occupational Health and Safety, and Accounting departments are authorized to use printers, photocopiers, or scanners. Other departments requiring these services must request them through Human Resources.

- - Physical confidential information must be stored in lockable offices.

- - All computers must be locked when the workstation is unoccupied or unattended by pressing Windows + L. The Technology department is responsible for configuring equipment inactivity settings, and it is established that computers should be locked after one minute of inactivity.

- - The computer screen (desktop) must not display any files, except for shortcuts to necessary applications as described in procedure PR-ITS-009 CONFIGURATION OF EQUIPMENT FOR BUSINESS USE.

- - Eating at workstations is strictly prohibited.

3. PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

The physical security program for access to the facilities has been implemented to enhance the confidentiality, availability, and integrity of information through access controls and monitoring in office areas and facilities where restricted or confidential information or valuable technological assets reside. Specifically, the areas that represent the highest risk of information breach or unauthorized access are: Technology (server room or data center, technology office, and management office), electrical room - generator, Human Resources office (analysts and management), and Accounting office (analysts and management). Therefore, these areas are equipped with secure access methods, which may include biometric systems or locks. The following guidelines established by senior management are listed:

- - It is determined that the high-risk areas mentioned previously must remain locked when unoccupied. Access to these areas without the accompaniment or authorization of process personnel is prohibited.

- - Information storage media containing sensitive, restricted, or confidential data are kept

in the protected area of the technology process. This area has physical access control via biometric systems, to which only process personnel have direct access.

- - The organization's equipment is installed in secure environments, monitored in real-time via CCTV.
- - The organization mandates the use of fire-resistant paint for these rooms to ensure physical security and prevent fires.
- - It is determined that both entrances to the organization have reception and security services to control physical access only to authorized persons (employees and visitors).
- - Security cameras are installed throughout the organization and are monitored by the technology process.
- - Smoking is prohibited inside, at the reception, or on wooden tables within the organization. Smoking is only allowed outside the premises.
- - The EMERGENCY PREPAREDNESS, PREVENTION, AND RESPONSE PLAN, as well as the BUSINESS CONTINUITY PLAN (BCP), are established to address environmental, physical, or social threats.

Senior management conducts an analysis of the organization's physical location and determines that controls such as intrusion alarms, motion detectors, sound-sensitive sensors, external door alarms, and others are unnecessary. This decision is based on the fact that the company is located in a warehouse complex with private 24-hour security service and restricted access for unauthorized persons. Additionally, the company contracts exclusive private security services also 24 hours a day. It is important to note that the organization operates 24 hours a day, 365 days a year, and therefore is never completely unoccupied.

Physical Controls:

- - Electrical Room: Stores only UPS systems and distribution panels.
- - Generator: Properly enclosed and free from flammable materials in nearby areas.
- - Data Center: Stores only servers.

4. BUSINESS CONTINUITY MANAGEMENT POLICY

The company has conducted a detailed analysis of the various risks to business continuity. To address these risks, a document has been established outlining the guidelines to be followed in such cases. This document is the Business Continuity Plan (BCP).

5. INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

The organization has established the necessary guidelines for the proper management of potential incidents. These guidelines are outlined in the procedure for preventing and addressing incidents, **PR-MPR-011 INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE**. These guidelines have been communicated and shared with all employees across different processes within the organization to ensure timely reporting of incidents and to provide prompt treatment, generating an **FO-MPR-025 INFORMATION SECURITY INCIDENT REPORT.**

6. OBLIGATIONS OF COLLABORATORS

a. To maintain absolute confidentiality, even after the termination of the employment contract, regarding: procedures, methods, characteristics, client lists, security keys, supplies, software, databases of any kind, values of goods and services, technical, financial, economic, or commercial information of the contractor or its clients, and other information that WORLD TRAVEL ASSIST LATAM S.A.S uses in the development of its corporate purpose in relation to clients or third parties.

Paragraph One: Failure to comply with this obligation is not only grounds for termination of the employment relationship but may also lead to legal action against the employee for any material or immaterial damages caused, in addition to the enforcement of the penalty clause described later.

b. To refrain from engaging in unfair competition with WORLD TRAVEL ASSIST LATAM S.A.S. Therefore, the employee agrees not to use, even after the termination of the employment contract, for their own benefit or the benefit of third parties: client lists, databases of any kind, software, or procedures, secret keys, methods, characteristics, studies, statistics, projects, supplies used by WORLD TRAVEL ASSIST LATAM S.A.S both internally and externally in relation to its clients or third parties, and technical, financial,

economic, or commercial information of WORLD TRAVEL ASSIST LATAM S.A.S or its clients.

Paragraph Two: The employee is obligated to immediately return, upon termination of their contract, client lists, keys, databases, equipment, technical, financial, economic, or commercial information, and anything else that the employee has from WORLD TRAVEL ASSIST LATAM S.A.S and received for the performance of their duties.

Paragraph Three: Failure to comply with this obligation is not only grounds for termination of the employment relationship but may also lead to legal action against the employee for any material or immaterial damages caused, in addition to the enforcement of the penalty clause described later.

c. To adopt all necessary and appropriate precautions to safeguard the confidentiality of the information held by the employee from the company, including: client lists, databases of any kind, software, procedures, secret keys, methods, characteristics, studies, statistics, projects, supplies used by WORLD TRAVEL ASSIST LATAM S.A.S both internally and externally in relation to its clients or third parties, and technical, financial, economic, or commercial information of WORLD TRAVEL ASSIST LATAM S.A.S or its clients.

Paragraph Four:

The omission by the Employee in preventing the leakage of confidential or proprietary information of the company, such as client lists, databases of any kind, software, procedures, secret codes, methods, characteristics, studies, statistics, projects, supplies used by WORLD TRAVEL ASSIST LATAM S.A.S internally and externally with its clients or third parties, technical, financial, economic, or commercial information of WORLD TRAVEL ASSIST LATAM S.A.S or its clients, is grounds for dismissal with just cause, without prejudice to legal actions against them for the damages caused and the collection of penalties for non-compliance, in addition to the penalty clause for non-compliance.

19. PENALTIES FOR NON-COMPLIANCE

Besides being grounds for termination of the contractual relationship due to non-compliance with any of the special obligations the Employee has under this Confidentiality Agreement,

WORLD TRAVEL ASSIST LATAM S.A.S shall have the right to demand, as a Penalty Clause, the sum of ten (10) current legal monthly minimum wages, a penalty that may be enforced through executive proceedings. It is accepted that this clause and the entire agreement contained in this agreement constitute a clear, express, and enforceable obligation that grants executive merit under the terms of the Code of Civil Procedure, without prejudice to all legal actions to recover the damages caused to WORLD TRAVEL ASSIST LATAM S.A.S. Since the agreed penalty clause serves as a penalty or sanction, both the penalty and the compensation for damages may be demanded as applicable.

20. DURATION

This policy will remain in effect even if the employment relationship or any other type of relationship has ended, as non-compliance will cause damages to WORLD TRAVEL ASSIST LATAM S.A.S and will give the right to charge the stipulated penalty clause solely due to non-compliance, without prejudice to legal actions for the damages caused.

The senior management appoints the general management and the process improvement director to review and/or update the policies annually, or sooner if necessary.

21. APPROVAL

This policy manual is established and approved by the management on October 25, 2023.

X

Sabrina Morales
Gerente general

They are committed to the control and compliance with the policies.

X

Carolina Jaramillo López
Directora de mejora de procesos

X

Brayan Ramón Moncada Hincapié
Oficial de Seguridad de la información