China Three Gorges Latam

# DATA PROTECTION POLICY

CTGL-LC-PO-006

Approved: ECM 39th 20241025

Version 1
10-25-2024

## Contents

## Chapter 1 General Provisions

### 1. Introduction

This document contains the Information Security Policy (the "Policy") applicable to: i) CTG Colombia Holding S.A.S; ii) Talasa Conexión S.A.S E.S.P; and iii) Talasa ProjectCo S.A.S. E.S.P (hereinafter referred to as the "Companies"). The Policy outlines the guidelines and principles applicable to the Companies' operations regarding the handling of personal and non-personal information.

The objective of this document is to define the organizational structure, general responsibilities, and obligations of employees and third parties, with the goal of mitigating the risks associated with the management of the Companies' information.

The Companies are aware of the threats that information faces today, as well as the consequences of failing to implement appropriate information security measures. Therefore, this Policy aims to develop the **Information Security Management System** (ISMS) for the Companies and to comply with the standards set forth by applicable regulations.

### 2. Scope

This Policy is mandatory for all employees of the Companies and third parties (suppliers and contractors) who provide services or have any relationship with the Companies (hereinafter, "Personnel"). The Policy will come into force upon publication.

## Chapter 2 Principles

This Policy achieves its objectives by adhering to the following principles, which will also apply to other documents and procedures implemented within the Companies. These principles complement the general principles for the processing of personal data as established by applicable regulations and the Companies' Data Processing Policy:

### 1. Confidentiality Principle

Refers to the set of procedures and technological and human measures implemented by the Companies to keep information secure and prevent unauthorized access, modification, consultation, or deletion. In practice, it involves the implementation of controls to regulate and prevent access to data by unauthorized personnel or third parties.

### 2. Integrity Principle

Consists of ensuring that the information used by the Companies has not been tampered with or altered by an unauthorized individual and, therefore, is reliable. Necessary systems must be implemented to ensure that the information stored in the company's systems complies with this principle and that unauthorized copies of the information are not stored.



Printed copies of this document are considered uncontrolled documents

### 3. Accessibility or Availability Principle

Ensures that systems, applications, and data will be available when needed by Personnel members or authorized third parties. Systems will be in place to ensure the preservation of systems and timely access to information.

### 4. Information Quality Principle

Refers to the requirement that the information used by the Companies must be truthful, complete, accurate, up-to-date, verifiable, and understandable. The use of partial, incomplete, fragmented, or misleading information or data is prohibited.

### 5. Security Principle

The Companies' information must be handled with the necessary technical, human, and administrative measures to secure records and mitigate associated risks.

### 6. Information Minimization Principle

It refers to the fact that, for the sake of efficiency in managing the required information, the amount of data collected will be reduced, as deemed appropriate and without affecting the operations and processes of the Companies. The use of data will be limited based on factors such as the authorization given by the data subjects, the purposes communicated to them, the retention period of the data, the number of people with access to the information, and the operations for which the data will be used.

## Chapter 3 Regulatory Framework

- Colombian Political Constitution: Article 15.
- Law 527 of 1999: Defines and regulates access to and use of data messages, electronic commerce, and digital signatures, and establishes certification entities.
- Law 1266 of 2008: Establishes general provisions for Habeas Data and regulates the management of personal data in databases, particularly financial, credit, commercial, service, and foreign country data.
- Law 1581 of 2012: Establishes general provisions for the protection of personal data.
- Decree 1377 of 2013: Partially regulates Law 1581 of 2012.
- Title V of the Unified Circular of the Superintendence of Industry and Commerce.
- Decree 886 of 2014: Regulates the National Registry of Databases.
- Decree 1074 of 2015: Issues the Regulatory Decree of the Commerce, Industry, and Tourism Sector. Partially regulates Law 1581 of 2012 and provides instructions on the National Registry of Databases (Articles 25 and 26).
- Decree 1078 of 2015: Issues the Single Regulatory Decree for the Information and Communication Technologies Sector.
- CONPES 3701 of 2011: Cybersecurity and Cyberdefense Policy Guidelines.
- CONPES 3854 of 2016: National Digital Security Policy.
- Colombian Technical Standard NTC-ISO/IEC 27001.



Printed copies of this document are considered uncontrolled documents

## Chapter 4 Information Security

**1.** General Information Security and Confidentiality Guidelines

The Companies have established the following main guidelines or pillars to maintain the security and confidentiality of their information:

- Timely identification of potential risks to the Companies' information security systems.
- Continuous development of the Companies' Information Security Management System, innovating in physical and technological controls.
- Raising awareness among Personnel about the importance of maintaining information security.
- Communicating this Policy, as well as the rules, procedures, and complementary documents on information security, to all Personnel.

**2.** Specific Security and Privacy Measures Adopted by the Companies

- **Classification of the Companies' Information:** The Companies have established the following parameters for classifying their information:
- **Public Information:** Information declared as public knowledge and available from publicly accessible sources without restrictions. This information can be shared with third parties, employees, or anyone without causing harm to others or business processes.
- **Internal Use Information**: Information used by the Companies to carry out assigned tasks, which cannot be shared with third parties without the asset owner's authorization.
- **Confidential Information**: Information used only by specific Personnel members to perform their tasks and cannot be accessed or known by other areas or employees of the Companies. Personal information of any data subject, for which the Companies act as data controllers, will be considered Confidential Information.

## Chapter5 Management of Company Assets

The Companies will manage and safeguard information assets that contain personal data, considered key assets, in accordance with document retention schedules. A responsible individual is assigned to each asset to manage it based on the company's needs, ensuring the confidentiality and security of the information.

Additionally, controls have been established to ensure that these assets are used in accordance with this Policy, and in the event of a change in responsibility, the asset will be formally handed over to the relevant area, which will verify the status of the information

## Chapter 6 Internal Organization

Procedures and rules for information security adopted by the Companies concerning their internal organization:

- The Companies have an Information Technology area.



Printed copies of this document are considered uncontrolled documents

- The Companies, through their internal areas, will maintain regular contact with Personnel involved in information security and privacy matters to develop and update the Companies' Information Management System.
- The Companies' information assets may only be managed by the person or area responsible for them, in accordance with established guidelines, thus reducing potential risks or accidental or intentional modifications to the information.
- The Companies will conduct information security training for all employees.

## Chapter 7 Personal Data Security

The Companies are committed to the proper handling of information and data related to individuals involved in their operations, including employees, investors, suppliers, and other third parties associated with the Companies. To this end, they have established a Data Processing Policy in accordance with the legal mandates of Law 1581 of 2012 and its complementary regulations. These documents apply to all data processing operations carried out in the databases under the Companies' control. Additionally, the Companies will follow the following parameters regarding the processing of Personal Data to ensure the confidentiality and security of their physical or automated databases:

- Strict compliance with Law 1581 of 2012, its regulatory decree 1377 of 2013, and other applicable personal data protection regulations in Colombia.
- Obtain the prior, express, and informed consent of data subjects for data processing.
- Guarantee the exercise of data subjects' rights, respond to their queries and claims promptly and effectively, and provide detailed information about the processing carried out.
- Notify the relevant authorities, within the time frame provided in current regulations, in the event of a possible personal data security incident.
- Train all Personnel on the proper handling of personal data in compliance with applicable regulations.

The Companies have implemented specific security controls to protect Personal Data, such as access controls via user and password to the applications containing databases or information assets (Data Room and/or SharePoint), ensuring that unauthorized users cannot access an application.

## Chapter 8 Human Resources

Las Compañías han definido los siguientes controles dirigidos específicamente a sus miembros de recursos humanos, en relación con la seguridad de la información:

### 1. Personal Onboarding

- The Companies have established a background check checklist for hiring Personnel.
- Personnel must sign confidentiality and non-disclosure agreements for the Companies' confidential information, making them binding.
- All new Personnel receive training and are permanently made aware of this Policy.

### 2. Personnel Offboarding



Printed copies of this document are considered uncontrolled documents

- Any offboarding notice must be immediately communicated to the administrative department so that it can deactivate all equipment, systems, access, and/or permissions assigned to the employee.
- A backup copy of the email inbox will be created once the employment relationship with the Companies ends.
- All access to information systems must be deactivated.
- Any authentication badge that identifies the individual as a Personnel member of the Companies must be returned.

## Chapter 9 Media management

Even though the Companies have tools that allow scanning all removable media connected to a device belonging to the Companies, the responsibility for this scan currently lies with each member of the Companies' Personnel, who must take sufficient measures to protect the information of the Companies contained in removable media. If there is unauthorized or fraudulent access, or the media is lost, Personnel members must immediately notify the Companies' administrative department.

## Chapter 10 Security Incident Management

The Companies have implemented security incident management for potential information security incidents. The following parameters have been established:

- Security Incident Definition: A security incident is defined as unauthorized access, attempt, use, disclosure, modification, or destruction of information (personal or otherwise); disruption of the normal operation of networks, systems, or IT resources; or a violation of a security measure implemented by the Companies.
- Incident Notification: Incident notifications allow a systematic response, minimizing recurrence, facilitating quick and efficient recovery, minimizing information loss, service interruption, and addressing legal aspects that may arise.
- Notification Process: Any user, third party, or contractor who suspects a security incident must notify the first point of contact defined by the Companies, which is the administrative department, through any communication channel (email). The initial point of contact will analyse if the reported incident is an information security incident or related to internal IT infrastructure issues (or non-reportable incidents). If there is suspicion of a personal data security incident, it will be immediately reported to the legal department and external advisors for a preliminary analysis to determine the extent and whether to notify the Superintendence of Industry and Commerce within the timeframes established by law.
- Containment: The goal is to detect the incident and prevent it from spreading further damage to the information or IT architecture. To facilitate this task, the Companies must have a pre-defined containment strategy, allowing quick decision-making, such as shutting down systems, disconnecting networks, or disabling services.
- Containment Strategy: The containment strategy varies depending on the type of incident, and criteria must be well-documented for quick and effective decision-making. Some base criteria include:
    - Forensic Criteria
    - Potential damage and asset theft
    - Evidence preservation needs



Printed copies of this document are considered uncontrolled documents

  - Service availability
  - Time and resources to implement the strategy
  - Effectiveness of the strategy (partial or total containment)
  - Duration of the solution
- Eradication and Recovery: After the incident has been contained, the next step is to eradicate and eliminate any traces left by the incident, such as malicious code, followed by recovery through system and service restoration. The IT administrator or their equivalent must restore the affected systems and harden the systems to prevent similar future incidents.

## Chapter 11 Vulnerability controls

The Companies review vulnerabilities in their information systems and have adopted the following specific measures to control technical vulnerabilities:

- The Companies monitor the use of SharePoint and corporate tools by personnel for work-related tasks and functions.
- The Companies track permissions granted to external providers when they need access to the Companies' systems or technological infrastructure.
- Each area within the Companies that deals with external providers potentially handling Company information must request the constant presence of the Companies' administrative department to ensure this Policy is communicated.

## Chapter 12 Access control

The Companies understand the current need to implement access controls to their information systems that provide effective and dynamic protection, taking into account the associated risks. Therefore, they have implemented the following measures:

- The Companies provide access to their networks to all members of staff, manage password changes, and update permissions and access to networks and various applications. Additionally, they update access to applications and websites to prevent access to prohibited pages or to avoid falling victim to activities such as phishing or similar threats.
- The Companies require periodic modification of the password for the wireless network, especially concerning the visitor network.
- The Companies use two-factor authentication, which allows for the confirmation of the identity of individuals accessing the Companies' tools, thereby preventing unauthorized access.
- The Companies generate strategies for centralizing authentication and manage access for all users through corporate email. Thus, when access to the centralized system is blocked, it also blocks access to the platforms that use corporate email.

## Chapter 13 User Controls

The Companies have defined the following tools to control the creation and use of user accounts:

- The Companies will grant users access that is requested and authorized by their immediate supervisor, department director, or contract supervisor in the case of contractors.
- User accounts created for Personnel members cannot have administrative permissions.



Printed copies of this document are considered uncontrolled documents

- The username and password assigned to Personnel members are personal and non-transferable.
- Once an employee's contract with the Companies ends, the HR officer or contract supervisor must notify the relevant department to ensure that access and email accounts are closed upon contract termination

## Chapter 14 Physical Security Controls

The Companies have implemented the following measures to protect their assets and/or information stored on physical equipment within the Companies' perimeter:

- The Companies have an access control system for their facilities.
- The security personnel at the building where the facilities are located establish mechanisms to inspect and examine the items brought in by visitors.

## Chapter 15 Physical Security Controls

The Companies have defined a scheme for the secure backup and restoration of the Companies' information. This ensures the security backup of email information and the proper storage of corporate information for the pertinent retention period.

## Chapter 16 Remote Information Access

The Companies have implemented the following controls to protect the security of their information when Personnel work remotely:

The Companies use technological tools such as DataRoom and SharePoint to remotely access the devices assigned to Personnel members, in order to monitor their performance, ensure information security, and provide remote support to these users.

All information managed by the Companies and accessed remotely must only be used to fulfill job responsibilities or contractual obligations.

## Chapter 17 Information Security Review

The Companies have defined a constant review process for their information security measures as follows:

- The Companies will conduct periodic internal audits to ensure the proper functioning of the Information Security Management System, specifically regarding controls, policies, and procedures.
- Process leaders must ensure that all security tools within their areas of responsibility are properly implemented, in compliance with security policies and standards; in cases of non-compliance, corrective actions will be evaluated and proposed.
- The Companies will review compliance with this Policy and will involve the executive management to determine if documents such as the Information Processing Policy are effectively implemented by all Personnel members.



Printed copies of this document are considered uncontrolled documents

Additionally, the company has established the policy CTGL-AD-IT-PO-001 Cybersecurity Incident Emergency Management to outline technological security guidelines

## Chapter 18 Regulatory compliance

The Companies must ensure the identification, documentation, and compliance with legislation related to Information Security. The administrative department, supported by various members, must identify, document, and keep updated the legal, regulatory, or contractual requirements applicable to the Companies and related to information security. Without exception, all Personnel members must be familiar with and adopt this Policy, as well as the responsibilities that arise from their job functions.

## Chapter 19 Supplementary provisions

This Policy is prepared in accordance with the procedures involved in the Companies' daily operations, which are constantly changing. For this reason, the Policy is subject to adjustments and modifications that will be made as required, incorporating new processes, tools, and operational changes in the Companies. It is the obligation of all Personnel members to stay updated with this Policy and its associated processes in order to perform their duties adequately.

This Policy has been reviewed by the legal department and finally approved by the Executive Committee.



Printed copies of this document are considered uncontrolled documents