TORRE DE CALI
PLAZA HOTEL

PERSONAL DATA PROCESSING POLICY

TABLE OF CONTENTS

TORRE DE CALI
PLAZA HOTEL

TORRE DE CALI
PLAZA HOTEL

1. LEGAL BASIS AND SCOPE OF APPLICATION

The information processing policy is developed in compliance with Articles 15 and 20 of the Political Constitution, as well as based on Articles 17(k) and 18(f) of Statutory Law 1581 of 2012, which establishes general provisions for the Protection of Personal Data (LEPD). Additionally, it complies with Article 2.2.2.25.1.1, Section 1, Chapter 25 of Decree 1074 of 2015, which partially regulates Law 1581 of 2012.

This policy shall apply to all personal data recorded in databases that are subject to processing by the Data Controller.

1.1. Scope

This document applies to all personal data or any other type of information used or stored in the databases and files of HOTEL T.C. S.A.S., respecting the criteria for obtaining, collecting, using, processing, managing, exchanging, transferring, and transmitting personal data, and establishing the obligations and guidelines of HOTEL T.C. S.A.S. for the administration and processing of personal data stored in its databases and files.
This Manual applies to all processes of HOTEL T.C. S.A.S. that must perform data processing (public data, semi-private data, private data, sensitive data, and data of children and adolescents), acting as Data Controller and Data Processor.

1.2. Applicable Regulations

- Political Constitution of Colombia
- Law 1581 of 2012 Decree 1074 of 2015, Chapters 25 and 26, which compile the following decrees:
  • Decree 1377 of 2013
  • Decree 886 of 2014
- Law 1266 of 2008 (“General Provisions for Habeas Data”).
- Administrative acts issued by the Superintendence of Industry and Commerce.

2. DEFINITIONS

The following definitions are established in Article 3 of the LEPD and Article 2.2.2.25.1.3, Section 1, Chapter 25 of Decree 1074 of 2015 (Article 3 of Decree 1377 of 2013).

TORRE DE CALI
PLAZA HOTEL

2.1. Authorization

Prior, express, and informed consent of the Data Subject to carry out the processing of personal data.

2.2. Database

An organized set of personal data that is subject to processing, belonging to a common context and systematically stored for later use.

2.3. Personal Data

Any information associated with or that may be linked to one or more identified or identifiable natural persons. These data are classified as public, semi-private, private, and sensitive.

2.3.1. Public Data

Data that is not semi-private, private, or sensitive. Public data includes, among others, information related to civil status, profession or trade, and the status of merchant or public servant. Public data may be contained in public records, public documents, official gazettes and bulletins, and final judicial decisions not subject to confidentiality.

2.3.2. Semi-private Data

Data that is neither intimate, reserved, nor public, and whose knowledge or disclosure may interest not only the Data Subject but also a specific sector, group of people, or society in general, such as databases containing financial, credit, commercial, service-related information and information from third countries.

2.3.3. Private Data

Personal data of intimate or reserved nature that is of exclusive interest to the Data Subject and whose processing requires prior, informed, and express authorization. Examples include: personal telephone numbers and email addresses; employment data; administrative or criminal infractions; data managed by tax authorities, financial institutions, social security entities; solvency or credit data; data used to assess personality; data managed by electronic communications service operators, among others.

2.3.4. Sensitive Data

Data that affects the Data Subject's privacy or whose misuse may lead to discrimination, such as information revealing racial or ethnic origin, political orientation, religious or philosophical beliefs,

membership in unions or social or human rights organizations, or data relating to health, sexual life, or biometric data.

2.4. Data Processor

A natural or legal person, public or private, who processes personal data on behalf of the Data Controller.

2.5. Data Controller

A natural or legal person, public or private, who, alone or in association with others, decides on the database and/or the processing of the data.

2.6. Database Administrator

A collaborator responsible for controlling and coordinating the correct application of data processing policies once data is stored in a specific database, and for implementing the instructions issued by the Data Controller and the Data Protection Officer.

2.7. Data Protection Officer

The natural person responsible for coordinating the implementation of the legal framework for personal data protection and for handling Data Subjects' requests regarding their rights established in Law 1581 of 2012.

2.8. Data Subject

A natural person whose personal data is subject to processing.

2.9. Processing

Any operation or set of operations performed on personal data, such as collection, storage, use, circulation, or deletion.

2.10. Privacy Notice

A verbal or written communication issued by the Data Controller to the Data Subject informing them of the applicable information processing policies, how to access them, and the purposes of the processing.

2.11. Transfer

Occurs when the Data Controller and/or Data Processor in Colombia sends personal data to a recipient who, in turn, acts as a Data Controller inside or outside the country.

TORRE DE CALI
PLAZA HOTEL

2.12. Transmission

Processing of personal data involving the communication of such data within or outside Colombia for the purpose of carrying out processing on behalf of the Data Controller.

1. PRINCIPLES OF DATA PROTECTION

Article 4 of the LEPD establishes principles for the processing of personal data that must be applied harmoniously and comprehensively in the development, interpretation, and application of the Law. The legal principles of data protection are as follows:

3.1. Principle of Legality:
Data processing is a regulated activity that must comply with the provisions of the LEPD, Decree 1377 of 2013 compiled in Chapter 25 of Decree 1074 of 2015 and other provisions that develop it.

3.2. Principle of Purpose:
The processing must be for a legitimate purpose in accordance with the Constitution and the Law, which must be communicated to the Data Subject.

3.3. Principle of Freedom:
The processing of personal data may only be carried out with the prior, express, and informed consent of the data subject. Personal data may not be obtained or disclosed without prior authorization, or in the absence of a legal or judicial mandate that overrides the requirement for consent. The processing of data requires the prior and informed authorization of the data subject by any means that allows for subsequent verification.

3.4. Principle of Truthfulness or Quality:
The information processed must be truthful, complete, accurate, up-to-date, verifiable, and understandable. The processing of partial, incomplete, fragmented, or misleading data is prohibited.

3.5. Principle of transparency:
The processing of personal data must guarantee the data subject's right to obtain information from the data controller or the data processor, at any time and without restriction, regarding the existence of data concerning him or her. When requesting authorization from the data subject, the data controller must clearly and expressly inform them of the following, keeping proof of compliance with this obligation:

- The processing to which your data will be subjected and the purpose of the processing.
- The optional nature of the Holder's response to questions asked when they deal with sensitive data or data of children or adolescents.
- The rights you have as the Owner.
- The identification, physical address, email address and telephone number of the data controller.

3.6. Principle of Restricted Access and Circulation:
The processing of personal data is subject to the limitations arising from the nature of the data, the provisions of the LEPD (Law on the Protection of Personal Data), and the Constitution. In this regard,

processing may only be carried out by persons authorized by the Data Subject and/or by persons authorized by law. Personal data, except for public information, may not be available on the Internet or other means of mass dissemination or communication, unless access is technically controllable to ensure restricted access only to Data Subjects or authorized third parties in accordance with the law.

3.7. Safety Principle:

Information processed by the Data Controller or Data Processor must be handled with the necessary technical, human, and administrative measures to ensure the security of the records, preventing their alteration, loss, unauthorized or fraudulent access, use, or disclosure. The Data Controller is responsible for implementing the corresponding security measures and making them known to all personnel who have direct or indirect access to the data. Users accessing the Data Controller's information systems must be aware of and comply with the security rules and measures applicable to their roles. These rules and security measures are set out in PL-02 Internal Security Policies, which are mandatory for all users and company personnel. Any modifications to the rules and measures regarding personal data security made by the Data Controller must be communicated to users.

3.8. Principle of Confidentiality:

All persons involved in the processing of personal data that is not of a public nature are obliged to guarantee the confidentiality of the information, even after their relationship with any of the tasks that comprise the processing has ended, and may only supply or communicate personal data when it corresponds to the development of the activities authorized in the LEPD and in the terms thereof.

2. AUTHORIZATION FOR THE USE OF PERSONAL DATA

In accordance with Article 9 of the LEPD (Law on the Protection of Personal Data), the processing of personal data requires the authorization of the Data Subject, except in the cases expressly indicated in the regulations governing the protection of personal data. Prior to and/or at the time of collecting personal data, HOTEL T.C. S.A.S. will request the Data Subject's authorization to collect and process said data, indicating the purpose for which the data is requested, using automated, written, or oral technical means that allow for the preservation of proof of authorization and/or the unequivocal conduct described in Article 2.2.2.25.2.2, Section 2 of Chapter 25 of Decree 1074 of 2015.

The Holder's authorization will not be required when it comes to:

- Information required by a public or administrative entity in the exercise of its legal functions or by court order.
- Data of a public nature.
- Cases of medical or health emergencies.
- Processing of information authorized by law for historical, statistical or scientific purposes.

- Data related to the Civil Registry of people.

3. REQUEST FOR AUTHORIZATION FROM THE PERSONAL DATA SUBJECT

Authorization for the use and/or processing of data will be managed by HOTEL T.C. S.A.S., through mechanisms that guarantee its subsequent consultation and the manifestation of the will of the Owner through the following means:

- In writing.
- Orally.
- Through automated channels.
- Through unequivocal conduct of the holder that reasonably allows the conclusion that he granted the authorization.

HOTEL T.C. S.A.S., in advance and/or at the time of collecting personal data, will clearly and expressly inform the Data Subject of the following:

a) The treatment to which your personal data will be subjected and its purpose;
b) The optional nature of the response to the questions asked, when these deal with sensitive data or with the data of girls, boys and adolescents;
c) The rights you have as the Owner;
d) The identification, physical or electronic address and telephone number HOTEL T.C. S.A.S..

4. DATA CONTROLLER

The entity responsible for processing the databases covered by this policy is HOTEL T.C. S.A.S., whose contact details are as follows:

- Address: AV DE LAS AMERICAS 18N 26, CALI - VALLE DEL CAUCA
- Email: protecciondatos@hoteltorredecali.com
- Telephone: 6533535 – 0

5. DATA PROCESSING AND PURPOSES

HOTEL T.C. S.A.S., in the course of its business activities, processes personal data relating to natural persons, which is contained in and processed in databases for legitimate purposes, in compliance with the Constitution and the Law. The processing of personal data includes collection, storage, use, circulation, and deletion. Data processing will be subject to the purposes authorized by the Data Subject, the contractual obligations between the parties, and any applicable legal obligations.

He Annex 2 PL-01 Purposes of DatabasesIt contains information relating to the different databases under the responsibility of the company and the purposes assigned to each of them for processing.

6. DATABASE VALIDITY

Personal data incorporated into the databases will be valid for the period necessary to fulfill the purposes for which its processing was authorized and the special rules that regulate the matter, the current rules related to the storage period will also be taken into account.

7. RIGHTS OF THE HOLDER(S)

In accordance with Article 8 of the LEPD, Article 2.2.2.25.4.1, Section 4, Chapter 25 of Decree 1074 of 2015 (Articles 21 and 22 of Decree 1377 of 2013), data subjects may exercise a series of rights in relation to the processing of their personal data. The data subject shall have the following rights:

a) To know, update and rectify your personal data before the Data Controllers or Data Processors. This right may be exercised, among others, with respect to partial, inaccurate, incomplete, fragmented, misleading data, or data whose processing is expressly prohibited or has not been authorized;
b) Request proof of the authorization granted to the Data Controller except when expressly exempted as a requirement for processing, in accordance with the provisions of Article 10 of this law;
c) To be informed by the Data Controller or the Data Processor, upon request, regarding the use that has been made of your personal data;
d) To file complaints with the Superintendency of Industry and Commerce for violations of the provisions of this law and other regulations that modify, add to or complement it;
e) Revoke authorization and/or request the deletion of data when the Processing does not respect constitutional and legal principles, rights, and guarantees. Revocation and/or deletion will proceed when the Superintendency of Industry and Commerce has determined that the Controller or Processor has engaged in conduct contrary to the law and the Constitution;
f) Access free of charge to your personal data that has been processed.

These rights may be exercised by the following persons.

1. By the Holder, who must sufficiently prove his identity through the various means made available to him by the Responsible Party.
2. By their successors, who must prove such status.
3. By the representative and/or attorney of the Holder, after accreditation of the representation or power of attorney.
4. By stipulation in favor of another and for another.

The rights of children or adolescents will be exercised by the persons who are authorized to represent them.

9.1. Right of access or consultation

This refers to the right of the Data Subject to be informed by the controller, upon request, regarding the origin, use and purpose given to their personal data.

9.2. Rights to file complaints and claims

The Law distinguishes four types of claims:

- *Correction claim:*the right of the Holder to have those partial, inaccurate, incomplete, fragmented, misleading data updated, rectified or modified, or those whose processing is expressly prohibited or has not been authorized.
- *Claim for deletion:*the right of the Data Subject to have data deleted that is inadequate, excessive or does not respect constitutional and legal principles, rights and guarantees.
- *Revocation claim:*the right of the Holder to revoke the authorization previously given for the processing of his personal data.
- *Infringement claim:*the right of the Data Subject to request that the non-compliance with the regulations on Data Protection be remedied.

9.3. Right to request proof of the authorization granted to the Data Controller

Except when expressly exempted as a requirement for processing in accordance with the provisions of Article 10 of the LEPD.

9.4. Right to file complaints with the Superintendency of Industry and Commerce for violations

The Data Subject or successor may only submit the request (complaint) to the SIC – Superintendency of Industry and Commerce, once the consultation or claim process before the Data Controller or Data Processor has been exhausted.

8. PROCESSING OF MINORS' DATA

HOTEL T.C. S.A.S., in accordance with Article 7 of Law 1581 of 2012, processes personal data of children and adolescents within the framework of the criteria indicated in Article 2.2.2.25.2.9, Section 2 of Chapter

25 of Decree 1074 of 2015 (Article 12 of Decree 1377 of 2013), observing the following parameters and requirements:

1. That the use of the data responds to and respects the best interests of children and adolescents.
2. That the use of the data ensures respect for the fundamental rights of the minor.

Once the above requirements have been met, HOTEL T.C. S.A.S. will request authorization from the child's legal representative, after the child has exercised their right to be heard. The child's opinion will be considered, taking into account their maturity, autonomy, and capacity to understand the matter. As the Data Controller and/or Processor, HOTEL T.C. S.A.S. will ensure the proper use of children's and adolescents' data, applying the principles and obligations established in Law 1581 of 2012 and its implementing regulations. Furthermore, HOTEL T.C. S.A.S. will identify any sensitive data collected or stored in order to enhance the security and handling of the information.

9. DUTIES AS DATA CONTROLLER

HOTEL T.C. S.A.S., as the Data Controller, will fulfill the following duties, without prejudice to the other provisions of this law and other laws governing its activity:

11.1. Facing the Head:

a) To guarantee the Holder, at all times, the full and effective exercise of the right of habeas data;
b) Request and keep, under the conditions provided for in this law, a copy of the respective authorization granted by the Holder;
c) Inform the Data Subject properly about the purpose of the collection and the rights they have by virtue of the authorization granted;
d) To process inquiries and claims made in accordance with the terms set forth in this law;
e) Inform the Data Subject, upon request, about the use given to their data;

11.2. In front of the Manager:

a) Ensure that the information provided to the Data Processor is truthful, complete, accurate, up-to-date, verifiable and understandable;
b) Update the information, promptly communicating to the Data Controller all changes regarding the data previously provided and take other necessary measures to ensure that the information provided to the Data Controller remains up to date;
c) Correct the information when it is incorrect and communicate the relevant information to the Data Controller;
d) Inform the Data Controller when certain information is under discussion by the Data Subject, once the complaint has been filed and the respective process has not been completed;
e) Provide the Data Processor, as applicable, only with data whose processing has been previously authorized in accordance with the provisions of this law;

f) Require the Data Processor at all times to respect the security and privacy conditions of the Data Subject's information;

11.3. In relation to principles and other obligations:

a) Observe the principles of legality, purpose, freedom, quality, truthfulness, transparency, access and restricted circulation, security and confidentiality
b) Adopt an internal manual of policies and procedures to ensure proper compliance with this law and, in particular, to address inquiries and complaints;
c) Inform the data protection authority when security code violations occur and there are risks in the management of the information of the Data Subjects.
d) Comply with the instructions and requirements issued by the Superintendency of Industry and Commerce.
e) To keep the information under the necessary security conditions to prevent its alteration, loss, consultation, use or unauthorized or fraudulent access;

10. DUTIES AS DATA PROCESSOR

HOTEL T.C. S.A.S., as the Data Processor, will fulfill the following duties, without prejudice to the other provisions of this law and other laws governing its activity:

a) To guarantee the Holder, at all times, the full and effective exercise of the right of habeas data;
b) To keep the information under the necessary security conditions to prevent its alteration, loss, consultation, use or unauthorized or fraudulent access;
c) To promptly update, rectify or delete data in accordance with the terms of this law;
d) Update the information reported by the Data Controllers within five (5) business days from the date of receipt;
e) To process inquiries and complaints made by the Holders in accordance with the terms set out in this law;
f) Adopt an internal manual of policies and procedures to ensure proper compliance with this law and, in particular, to address inquiries and complaints from Data Subjects;
g) Register in the database the legend “claim in process” in the manner regulated in this law;
h) Insert the legend “information under judicial discussion” into the database once notified by the competent authority about legal proceedings related to the quality of the personal data;
i) Refrain from circulating information that is being disputed by the Owner and whose blocking has been ordered by the Superintendency of Industry and Commerce;
j) Allow access to information only to those people who are authorized to access it;
k) Inform the Superintendency of Industry and Commerce when violations of security codes occur and there are risks in the management of the information of the Holders;
l) Comply with the instructions and requirements issued by the Superintendency of Industry and Commerce.

TORRE DE CALI
PLAZA HOTEL

11. ATTENTION DATA SUBJECTS

To address requests, inquiries, and complaints regarding personal data protection, HOTEL T.C. S.A.S. has appointed a Data Protection Officer. Data subjects may submit their requests or inquiries through the following channels:
Email: protecciondatos@hoteltorredecali.com
Address: AV DE LAS AMERICAS 18N 26, CALI - VALLE DEL CAUCA.
Telephone numbers: 6533535 - 0

12. PROCEDURES FOR EXERCISING THE RIGHTS OF THE DATA SUBJECT

14.1. Right of access or consultation

HOTEL T.C. S.A.S. will guarantee the Holder the consultation of their personal data free of charge in the following cases (Article 2.2.2.25.4.2. section 4 chapter 25 of Decree 1074 of 2015):

1. At least once every calendar month.
2. Whenever there are substantial modifications to the information processing policies that warrant new consultations.

For inquiries exceeding one per calendar month, HOTEL T.C. S.A.S. may charge the Data Subject for shipping, reproduction, and, where applicable, document certification costs. Reproduction costs may not exceed the cost of recovering the corresponding materials. HOTEL T.C. S.A.S. will provide the Superintendency of Industry and Commerce with supporting documentation for these expenses upon request.

The Data Subject may exercise their right to access or consult their data by sending a written request to HOTEL T.C. S.A.S. via email to protecciondatos@hoteltorredecali.com, indicating "Exercise of the right of access or consultation" in the subject line, or by mail to AV DE LAS AMERICAS 18N 26, CALI - VALLE DEL CAUCA. The request must contain the following information:

- Name and surname of the Holder.
- Photocopy of the Citizenship Card of the Holder and, where applicable, of the person who represents him, as well as the document accrediting such representation.
- Petition specifying the request for access or consultation.
- Address for notifications, date and signature of the applicant.
- Supporting documents for the request made, where applicable.

The Data Subject may choose one of the following methods of querying the database to receive the requested information:

- Screen display.
- In writing, with a copy or photocopy sent by certified or non-certified mail.
- Email or other electronic means.
- Another system suitable to the database configuration or the nature of the processing, offered by HOTEL T.C. S.A.S.

Once the request is received, HOTEL T.C. S.A.S. will resolve the consultation request within a maximum period of ten (10) business days from the date of receipt. If it is not possible to address the consultation within this period, the interested party will be informed, stating the reasons for the delay and indicating the date on which their consultation will be addressed, which in no case may exceed five (5) business days following the expiration of the initial period. These timeframes are established in Article 14 of the LEPD.

Once the consultation process has been exhausted, the Holder or successor may file a complaint with the Superintendency of Industry and Commerce.

14.2. Rights to complain and make claims

The Data Subject may exercise their rights regarding their data by submitting a written request to HOTEL T.C. S.A.S., either by email to protecciondatos@hoteltorredecali.com, indicating "Exercise of the right of access or consultation" in the subject line, or by mail to AV DE LAS AMERICAS 18N 26, CALI - VALLE DEL CAUCA. The request must contain the following information:

- Name and surname of the Holder.
- Photocopy of the Citizenship Card of the Holder and, where applicable, of the person who represents him, as well as the document accrediting such representation.
- Description of the facts and request specifying the request for correction, deletion, revocation or infringement.
- Address for notifications, date and signature of the applicant.

- Supporting documents for the request made that you wish to use, where applicable.

If the claim is incomplete, the interested party will be required to correct the deficiencies within five (5) days of receiving the claim. If the applicant fails to submit the required information within two (2) months of the date of the request, it will be understood that they have withdrawn the claim.

Once the complete claim is received, a note stating "claim in process" and the reason for the claim will be added to the database within no more than two (2) business days. This note must remain until the claim is resolved.

HOTEL T.C. S.A.S. will resolve the claim within a maximum period of fifteen (15) business days from the date of receipt. If it is not possible to address the claim within this period, the interested party will be informed of the reasons for the delay and the date on which their claim will be addressed, which in no case may exceed eight (8) business days following the expiration of the first period.
Once the claim process has been exhausted, the Holder or successor may file a complaint with the Superintendency of Industry and Commerce.

14.3. Authorized to receive information

HOTEL T.C. S.A.S. will provide the information of the Holders of its databases to the following persons authorized or empowered to receive it, in accordance with article 13 of Law 1581 of 2012:

- To the Holders, their successors or their legal representatives;
- To public or administrative entities in the exercise of their legal functions or by court order;
- To third parties authorized by the Owner or by law.

14.3.1. Verification of the ability to request or receive information

To process a request for consultation or complaint, the applicant must provide the following documents to prove their ownership or the authority to receive the required information, according to the following cases:

- Holder: Copy of identity document.
- Successor: Identity document, civil registry of death of the Holder, document that proves the capacity in which he/she acts and copy of the identity document of the Holder.
- Legal representative and/or attorney: Valid identity document, document that proves the capacity in which he/she acts (Power of Attorney) and copy of the identity document of the Holder.

TORRE DE CALI
PLAZA HOTEL

13. DATA PROCESSING IN VIDEO SURVEILLANCE SYSTEMS

HOTEL T.C. S.A.S. will inform individuals about the existence of video surveillance systems by posting visible notices accessible to all users and installed in the areas under video surveillance, primarily at entrances to and within the monitored premises. These notices will inform users who the Data Controller is, the purposes of the data processing, the rights of the data subject, the channels available to exercise those rights, and where the Data Processing Policy is published.
Furthermore, it will retain the images only for the time strictly necessary to fulfill the purpose and will register the database that stores the images in the National Database Registry, unless the Processing consists only of the reproduction or broadcasting of images in real time.
Access to and disclosure of the images will be restricted to persons authorized by the Data Subject and/or at the request of an authority acting within its functions. Consequently, the disclosure of the collected information will be controlled and consistent with the purpose established by the Data Controller.

14. SECURITY MEASURES

HOTEL T.C. S.A.S., in order to comply with the security principle enshrined in article 4 literal g) of the LEPD, has implemented the necessary technical, human and administrative measures to guarantee the security of the records, preventing their alteration, loss, consultation, use or unauthorized or fraudulent access.

Furthermore, HOTEL T.C. S.A.S., through the signing of the corresponding transmission contracts, has required the data processors with whom it works to implement the necessary security measures to guarantee the security and confidentiality of information in the processing of personal data.

The following are the security measures implemented by HOTEL T.C. S.A.S., which are included and developed inyour PL-02 Internal Security Policies (Tables I, II, III and IV).

TABLE I: Common security measures for all types of data (public, private, confidential, restricted) and databases (automated, non-automated)	
Document and media management	1. Measures to prevent unauthorized access to or recovery of data that has been discarded, deleted, or destroyed. 2. Restricted access to the location where the data is stored. 3. Authorization from the person responsible for managing the databases for the release of documents or media by physical or electronic means. 4. Labeling or identification system for the type of information. 5. Inventory of supports.

TORRE DE CALI
PLAZA HOTEL

Access control	1. User access limited to the data necessary for the performance of their duties. 2. Updated list of users and authorized access. 3. Mechanisms to prevent access to data with rights other than those authorized. 4. Granting, alteration, or cancellation of permits by authorized personnel
Incidents	1. Incident log: type of incident, time it occurred, sender of the notification, recipient of the notification, effects and corrective measures. 2. Incident notification and management procedure.
Personal	1. Definition of the functions and obligations of users with access to the data. 2. Definition of the control functions and authorizations delegated by the data controller. 3. Disclosurebetween the staff of the rules and the consequences of non-compliance.
Internal Security Manual	1. Preparation and implementation of the mandatory manual for staff. 2. Minimum content: scope of application, security measures and procedures, functions and obligations of personnel, description of databases, incident procedure, identification of data processors.

TABLE II: Common security measures for all types of data (public, private, confidential, restricted) according to the type of databases	
Non-automated databases	
Archive	1. Documentation archive following procedures that guarantee proper preservation, location and consultation, allowing the exercise of the rights of the Holders.
Document storage	1. Storage devices with mechanisms that prevent access by unauthorized persons.
Document custody	1. Duty of diligence and custody of documents by the person in charge during their review or processing.
Automated databases	
Identification and authentication	1. Personalized user identification to access information systems and verification of their authorization. 2. Identification and authentication mechanisms; Passwords: assignment and expiration.
Telecommunications	1. Access to data through secure networks.

TABLE III: Security measures for private data according to the type of databases
Non-automated databases

TORRE DE CALI PLAZA HOTEL

Audit	1. Regular audit (internal or external) every two months. 2. Extraordinary audit due to substantial modifications in information systems. 3. Report on the detection of deficiencies and proposal of corrections. 4. Analysis and conclusions of the security officer and the data controller.
Security Officer	1. Appointment of one or more Database Administrators. 2. Designation of one or more persons in charge of the control and coordination of the measures of the Internal Security Manual. 3. Prohibition of delegation of the Data Controller's responsibility to the Database administrators.
Internal Security Manual	1. Periodic compliance checks.
Automated databases	
Document and media management	1. Record of entry and exit of documents and media: date, sender and receiver, number, type of information, method of delivery, person responsible for receipt or delivery.
Access control	1. Access control to the place or places where the information systems are located.
Identification and authentication	1. Mechanism to limit the number of repeated unauthorized access attempts. 2. Data encryption mechanisms for transmission.
Incidents	1. Record of data recovery procedures, person performing them, data restored, and data recorded manually. 2. Authorization from the data controller for the execution of the recovery procedures.

TABLE IV: Security measures for sensitive data according to the type of databases

Non-automated databases	
Access control	1. Access for authorized personnel only. 2. Access identification mechanism. 3. Log of unauthorized user access. 4. Destruction that prevents access to or recovery of the data.
Document storage	1. Filing cabinets, cupboards or others located in access areas protected by locks or other measures. 2. Measures to prevent access to or manipulation of physically stored documents.
Automated databases	
Access control	1. Confidential labeling system.
Identification and authentication	1. Data encryption mechanisms for transmission and storage.

Document storage	1. Access log: user, time, database accessed, access type, record accessed 2. Access log control by the security officer. Monthly report.
Telecommunications	1. Access and transmission of data through secure electronic networks. 2. Data transmission using encrypted networks (VPN).

15. COOKIES O WEB BUGS

HOTEL T.C. S.A.S. may collect personal information from its Users while they use the Website, the Application, or Linked Pages (Landing Pages). Users may choose to store this personal information on the website, the application, or the linked portal (Landing Page) to facilitate transactions and services provided by HOTEL T.C. S.A.S. and/or its linked portals (Landing Pages). Therefore, HOTEL T.C. S.A.S. uses various tracking and data collection technologies, such as first-party and third-party cookies. This analytics tool helps website and application owners understand how visitors interact with their properties. This tool may use a set of cookies to collect information and provide website usage statistics without personally identifying visitors to Google.

This information allows us to understand your browsing patterns and offer you personalized services. HOTEL T.C. S.A.S. may use these technologies to authenticate you, to remember your preferences for using the website, the application, and linked pages (Landing Pages), to present offers that may be of interest to you and to facilitate transactions, to analyze the use of the website, the application, or linked pages and their services, to use it in aggregate or combine it with the personal information we have, and to share it with authorized entities.

If a user does not want their personal information collected through cookies, they can change their preferences in their web browser. However, it is important to note that if a web browser does not accept cookies, some features of the website, application, and/or linked pages (landing pages) may not be available or may not function correctly. You can allow, block, or delete cookies installed on your device by configuring your browser settings as follows:

- Chrome: https://support.google.com/accounts/answer/61416?co=GENIE.Platform%3DDesktop&hl=es
- Microsoft Edge: https://support.microsoft.com/es-es/microsoft-edge/permitir-temporalmente-las-cookies-y-los-datos-del-sitio-en-microsoft-edge-597f04f2-c0ce-f08c-7c2b-541086362bd2
- Firefox: https://support.mozilla.org/es/kb/habilitar-y-deshabilitar-cookies-sitios-web-rastrear-preferencias
- Safari: https://support.apple.com/es-es/HT201265

16. SECURITY INCIDENT NOTIFICATION, MANAGEMENT AND RESPONSE PROTOCOL

HOTEL T.C. S.A.S. has an incident reporting procedure for communication and notification among employees, the personal data protection officer, data processors, data subjects, the oversight and control body, as well as judicial bodies: for the management and response to security incidents from the moment they are detected in order to be evaluated and manage the identified vulnerabilities, ensuring that the systems, networks, and applications are sufficiently secure.

All users and those responsible for managing databases, as well as any person involved in the collection, storage, use, circulation, or any processing or consultation of databases, must know the procedure to follow in case of security incidents to guarantee the confidentiality, availability, and integrity of the information contained in the databases under their responsibility.

Some examples of security incidents are: failure of security systems that allows access to personal data to unauthorized persons, the unauthorized attempt to remove a document or media, the loss of data or the total or partial destruction of media, the change of physical location of databases, knowledge of passwords by third parties, modification of data by unauthorized personnel, among others.

In the event of a security incident, the response team or committee will take the following criteria into account:

Strategy to identify, contain and mitigate security incidents.

- Implement measures to contain and reverse the impact that the security incident may have.
- Properly assess the security incident and its impact on the data subjects.
- Verify the legal or contractual requirements with service providers associated with the security incident.
- Determine the level of risk to the Data Subjects and notify the occurrence.
- Verify the roles and responsibilities of the personnel responsible for the operation of the affected information or data.

Timeline for security incident management.

Apply the procedure for handling security incidents, in accordance with parameters that allow for proper management and impact mitigation. Verify, based on the security incident assessment, the need to notify entities such as: the Attorney General's Office, the Office of the Inspector General, the Anti-Kidnapping and Extortion Unit (Gaula), the National Police, the Financial Superintendency of Colombia, the Police Cyber Center, colCERT; the Police CSIRT, the Asobancaria CSIRT, the Sectoral CSIRT, among others.

Security incident report progress

Monitor the management process by setting deadlines, evaluating its progress, and identifying potential conflict points that may arise in handling the security incident.

Security incident response assessment

Once the security incident has been managed and controlled, the response team should review the actions taken to contain it and make the necessary adjustments to implement an improvement plan.

Actions implemented and improvement plans

Establish the necessary actions to mitigate the impact of the security incident and prevent it from happening again, through corrective and preventive actions, as well as improvement plans that the response team must adopt.

Documentation and reporting to the oversight and control body

Document the information related to the security incident in an internal record, as well as prepare a report with supporting documentation of the actions taken, which must be submitted to the Superintendency of Industry and Commerce, through the RNBD within 15 business days after the incident was detected.

Revision

Evaluate the causes of the security incident and the success of its management to assess the effectiveness of the controls and actions implemented. Document the lessons learned for future reference.

17. MANAGEMENT OF RISKS ASSOCIATED WITH DATA PROCESSING

HOTEL T.C. S.A.S. has identified risks related to the processing of personal data and established controls to mitigate their causes through the implementation of PL-02 Internal Security Policies. Therefore, it will establish a risk management system, along with the necessary tools, indicators, and resources for its administration, when the organizational structure, internal processes and procedures, the number of databases, and the types of personal data processed by the organization are considered to be exposed to frequent or high-impact events or situations that affect the proper provision of the service or threaten the information of the data subjects.

The risk management system will identify sources such as technology, human resources, infrastructure, and processes that require protection, their vulnerabilities, and threats in order to assess their level of risk. Therefore, to guarantee the protection of personal data, the type or group of internal and external individuals and the different levels of access authorization will be considered. Likewise, the possibility of any type of event or action that could cause damage (material or immaterial) will be observed, such as:

- Criminality: Understood as actions, caused by human intervention, that violate the law and are penalized by it.
- Events of physical origin: Understood as natural and technical events, as well as events indirectly caused by human intervention.

- Negligence and institutional decisions: These are understood as the actions, decisions, or omissions of individuals who have power and influence over the system. At the same time, they are the least predictable threats because they are directly related to human behavior.

HOTEL T.C. S.A.S. in the risk management program will implement protection measures to avoid or minimize damage in the event that a threat materializes.

18. DELIVERY OF PERSONAL DATA TO THE AUTHORITIES

When a public or administrative entity, acting within its legal functions or by court order, requests HOTEL T.C. S.A.S. to access and/or provide personal data contained in any of its databases, the legality of the request and the relevance of the requested data to the purpose stated by the authority will be verified. Upon delivery, a record will be drawn up indicating the details of the requesting entity and the characteristics of the personal information requested, specifying the obligation to guarantee the rights of the data subject, both to the official making the request, the person receiving it, and the requesting entity.

19. INTERNATIONAL TRANSFER AND TRANSMISSION OF PERSONAL DATA

HOTEL T.C. S.A.S. will transfer personal data to countries that provide adequate levels of data protection. A country is considered to offer an adequate level of data protection when it complies with the standards established by the Superintendency of Industry and Commerce on this matter, which in no case may be lower than those required by Law 1581 of 2012. This prohibition will not apply when it involves:

- Information regarding which the Holder has given his express and unequivocal authorization for the transfer.
- Exchange of medical data, when required by the treatment of the Holder for reasons of health or public hygiene.
- Bank or stock market transfers, in accordance with the legislation applicable to them.
- Transfers agreed within the framework of international treaties to which the Republic of Colombia is a party, based on the principle of reciprocity.
- Transfers necessary for the execution of a contract between the Data Subject and the controller, or for the execution of pre-contractual measures provided that the Data Subject has given his or her consent.
- Transfers legally required for the safeguarding of the public interest, or for the recognition, exercise or defense of a right in a judicial process.

In cases where the transfer of data is necessary and the destination country is not on the list of countries considered as safe ports indicated by the Superintendency of Industry and Commerce, a declaration of

conformity relating to the approval for the international transfer of personal data must be obtained from the same entity.

International transfers of personal data between HOTEL T.C. S.A.S. and a data processor, enabling the processor to carry out processing on behalf of the controller, will not require notification to the data subject or their consent, provided a personal data transfer agreement exists. This personal data transfer agreement must be signed between the controller and the processor to define the scope of personal data processing under their control and responsibility, as well as the activities the processor will perform on behalf of the controller and the processor's obligations to the data subject. Additionally, the processor must comply with the following obligations and apply the data protection regulations in force in Colombia.

1. To process, on behalf of the Responsible Party, personal data in accordance with the principles that protect them.
2. Safeguard the security of databases containing personal data.
3. Maintain confidentiality regarding the processing of personal data.

The above conditions set for international data transmissions will also apply to national data transmissions.

20. BIOMETRIC DATA PROCESSING

Biometric data stored in databases is collected and processed strictly for security purposes, to verify personal identity and control access for employees, customers, and visitors. Biometric identification mechanisms capture, process, and store information related to, among other things, people's physical characteristics (fingerprints, voice recognition, and facial features) in order to establish or "authenticate" the identity of each individual.

The administration of biometric databases is carried out with technical security measures that guarantee due compliance with the principles and obligations derived from the Statutory Law on Data Protection, also ensuring the confidentiality and privacy of the information of the owners.

21. NATIONAL DATABASE REGISTRY – RNBD

The deadline for registering databases in the RNBD will be that established by law. Furthermore, in accordance with Article 12 of Decree 886 of 2014, Data Controllers must register their databases in the National Database Registry on the date the Superintendency of Industry and Commerce enables said registry, in accordance with the instructions issued by that entity. Databases created after that deadline must be registered within two (2) months following their creation.

TORRE DE CALI
PLAZA HOTEL

22. INFORMATION SECURITY AND PERSONAL DATA

Compliance with the regulatory framework for Personal Data Protection, and the security, privacy, and/or confidentiality of information stored in databases, is of vital importance to HOTEL T.C. S.A.S. Therefore, we have established information security policies, guidelines, procedures, and standards, which may change at any time to adapt to new regulations and the needs of HOTEL T.C. S.A.S., with the objective of protecting and preserving the integrity, confidentiality, and availability of personal information and data.

Likewise, we guarantee that in the collection, storage, use and/or processing, destruction or elimination of the information provided, we rely on technological security tools and implement security practices that include: transmission and storage of sensitive information through secure mechanisms, use of secure protocols, securing technological components, restricting access to information only to authorized personnel, information backup, secure software development practices, among others.

In the event that it becomes necessary to provide information to a third party due to a contractual relationship, we sign a data transfer agreement to guarantee the confidentiality and security of the information, as well as compliance with this Data Processing Policy, the information security policies and manuals, and the protocols for addressing data subjects established by HOTEL T.C. S.A.S. In all cases, we are committed to the protection, care, security, and preservation of the confidentiality, integrity, and privacy of the stored data.

23. DOCUMENT MANAGEMENT

Documents containing personal data must be easily retrievable. Therefore, the location of each document, both physical and digital, must be documented. These storage locations must be inspected frequently, and their preservation must be guaranteed by defining the storage medium and conditions, taking into account environmental conditions, storage locations, and risks to which they are exposed, among other factors. The document retention period is determined based on applicable legal requirements; otherwise, each organization defines it according to its needs. Likewise, the final disposition of the documents must be clearly defined, specifying whether they are recycled, reused, preserved, digitized, or other options.

Documents related to the protection of personal data must be prepared by personnel or an entity competent to do so; likewise, the organization must be the one to review and approve all documents and record it in the document approval box.

In order to be easily traceable, the documents must be coded, updated and modified by the responsible personnel. This modification will be carried out whenever necessary. For the elimination of a document, there must be a justification for it described in the history which is located at the bottom of all documents.

Both physical and digital documents containing personal data must be protected from external or internal agents who may alter their content, following the guidelines described in PL-02 Internal Security Policies

The distribution of documents containing personal data will be carried out by the data controller, who will document the evidence of said distribution, specifying, among other things, the type of document and the identification of the person to whom the information was delivered.

A person responsible for ensuring the confidentiality of the personal data of the data subjects must be designated. This person will be responsible for safeguarding documents, ensuring their physical and digital protection, preventing alterations to the information, and ensuring that documents leaving their custody are identified and easily traceable.

24. VALIDITY

This Policy update will be effective from 2025-03-26. The databases under the responsibility of HOTEL T.C. S.A.S. will be processed for the time that is reasonable and necessary for the purpose for which the data is collected and in accordance with the authorization granted by the Owners of the personal data.