SECURITY AGREEMENT
PERSONAL DATA PROTECTION LAW 1581 OF 2012

Bogotá, Colombia, November 2018.

Hereby, **B&C Corporation** company legally registered and authorized under the laws of Colombia (hereinafter "**B&CC**" or "the company"), as the person in charge of processing personal data, whose files have been registered in the National Database Registry (RNBD) of the Superintendence of Industry and Commerce of Colombia (SIC), and in compliance with current regulations on data protection, in particular the provisions of Article 15 of the Political Constitution of Colombia ("habeas data"), Law 1581 of 2012, Decree 1377 of 2013 and other regulations that modified, added, complemented or developed it, approves to the present version of the internal policy on personal data processing (hereinafter the "Policy") , together with the technical and organizational procedures that develop it.

Table of Contents

1. INTRODUCTION

Article 17 of the statutory law 1581 of 2012 states:

"The Responsible for the processing must comply with the following duties, without prejudice to the other provisions provided for in this law and others that govern their activity (...)

K) Adopt an internal manual of policies and procedures to ensure proper compliance with this law and in particular, for the attention of inquiries and claims "

The purpose of this Security agreement is to describe and inform the controller about the use, destination and purpose of the processing of personal information and the rights that assist him, as well as the technical and organizational measures existing in **B&C Corporation**, (Hereinafter "**B&CC**" or the "Entity") , with regard to the security of archives, automated or non-automated, treatment centers, premises, equipment, systems, storage systems, programs and people involved in the processing of personal data, with the objective to guarantee the security, confidentiality and integrity of them and to avoid their alteration, loss, treatment or unauthorized access.

The Security agreement arises as an adaptation to the current provisions on personal data security, corresponding to Article 15 of the Political Constitution of Colombia ("habeas data"), Law 1581 of 2012, Decree 1377 of 2013 and other regulations that modify, add, complement or develop. The main provisions to the aforementioned law correspond to the following:

- Article 15 of the Political Constitution of Colombia ("habeas data")
- Law 1581 of 2012, by which general provisions for the protection of personal data are held. Adopted by the Congress of Colombia on October 17, 2012.
- Decree 1377 of 2013, by which law 1581 of 2012 is partially regulated and was approved by the President of the Republic of Colombia on 27 July 2013

This document includes all the measures, rules, procedures, and standards adopted by **B&CC**, aimed at guaranteeing the levels of security required by Law 1581 of 2012 and Decree 1377 of 2013, as well as a list of personal data, description of information systems and documents containing such data and systems that treat and identify the roles and responsibilities of personnel with access to them. This document and its annex procedures (available on the Intranet of B&C Corporation - https://www.bccorporation.org -) are written in compliance with the provisions of Law 1581 of 2012 and Decree 1377 of 2013 and they therefore include the necessary technical and organizational measures to guarantee the protection, confidentiality, integrity and availability of the resources affected by the provisions of the aforementioned regulation. Likewise, its purpose is to preserve honor, personal and family privacy and the full exercise of personal rights against its alteration, loss, treatment or unauthorized access.

It is therefore essential to define the measures, rules, policies and security procedures that allow obtaining and maintaining the level of information security appropriate to the criticality of the data and processes that are stored and managed at **B&CC**.

Persons with access to personal data and **B&CC** information systems must be aware of the need to preserve information and the consequences that inappropriate actions in this regard may cause the Entity. For this reason, personnel with access to personal data and information systems of **B&CC**, are periodically informed of all security regulations that affect the performance of their functions, as well as the consequences in case of non-compliance.

The security rules contained in this document affect all the organizational structures of **B&CC** and must be complied with and observed by all personnel with access to personal data and information systems of the Entity. Any violation of these measures, rules and procedures may entail disciplinary action consistent with the infraction, as well as appropriate legal actions.

In order to disseminate the knowledge of security standards, to which this document refers, a notification has been prepared and disseminated as established in Section 8 of this document.

This document must be permanently updated. Any relevant modification in the automated information systems or not, in the organization of these, or in the current provisions on the security of personal data will entail the revision of this document and, if applicable, its total or partial modification

2. DEFINITIONS

For the purposes of this document, the following definitions shall apply:

a) **Personal data**: Any information linked to or associated with one or several natural persons identified or identifiable.
b) **Sensitive data:** Data that affects the privacy of the owner or whose misuse can lead to discrimination.
c) **Database:** Organized set of personal data that is subject to treatment.
d) **Controller:** a natural person whose personal data is subject to processing by reason of a commercial or legal relationship with the company, be it a customer, supplier, employee, or any third party.
e) **Client:** Any person for whom the company provides a service or who has a contractual / obligational relationship.
f) **Provider:** Any natural or legal person that provides a service to the company, by virtue of a contractual / obligational relationship.
g) **Data processing**: Any operation, or set of operations, carried out on personal data, such as collection, storage, use, circulation, deletion, operations and technical procedures of an automated or non-automated nature, recording, processing, modification, consultation, blocking and cancellation, as well as the cessions of data resulting from communications, consultations, interconnections and transfers.
h) **Processor:** Natural or legal person, public or private, that by itself or in association with others, decide alone or jointly on the purpose on the basis of data and / or the processing of the data (The "processor").

i) **Responsible for the Treatment:** Natural or legal person, public or private, which by itself or in association with others, performs the processing of personal data, as the person in charge of the data (the "Security officer").

j) **Transfer:** It is when the Responsible and / or the person in charge of the processing of personal data, located in Colombia, sends the information or personal data to a receiver, who in turn is Responsible for the Treatment and is located inside or outside the country.

k) **Transmission:** Processing of personal data that involves the communication of the same within or outside the territory of Colombia when it has for its object the performance of a treatment by the Person in Charge on behalf of the Responsible.

l) **Treatment centers**: Within this concept are included the different resources (premises, equipment, systems, communications, etc.) that intervene in the processing of personal data.

m) **Backup**: Copy of the original data that is made in order to have a means of recovering them in case of loss

n) **Document:** All written, graphic, sound, image or any other kind of information that can be treated in an information system as a differentiated unit.

o) **File**: any organized set of personal data, whatever the form or modality of its creation, storage, organization and access.

p) **Non-automated database:** All data set organized personal non - automated and structured according to specific criteria relating to individuals, which allows access without disproportionate to their personal data efforts, whether one centralized, decentralized or dispersed functional or geographical form.

q) **Persons**: all those persons, belonging or not to the Company, who are involved in the processing and management of personal data.

r) **User profile**: authorized access to a group of users.

s) **Programs and applications**: list of applications that intervene in the processing of personal data of the Entity.

t) **Protected resource:** any component part of an information system, whether automated or not

u) **Responsible for Security**: person or persons to whom the person in charge of the file has formally assigned the function of coordinating and controlling the applicable security measures.

v) **Treatment systems**: Mode in which an information system is organized or used. By attending to the treatment system, the information systems can be automated, not automated or partially automated.

w) **User**: Subject or authorized process to access data or resources. The processes that allow access to data or resources without identification of a physical user will be considered users.

x) **Data protection laws:** means in relation to any Personal Data which is Processed in the performance of the Service Agreement, the General Data Protection Regulation (EU) 2016/679 ("GDPR") together with all implementing laws and any other applicable data protection, privacy laws or privacy regulations

y) **Sub processor**: means any data processor appointed by Processor to process Personal Data on behalf of the Controller;

For the rest of the terms used, it will be established in the definitions of Law 1581 of 2012, the decrees that regulate it, and the general policy of data processing of the company respectively.

3. SCOPE OF THE SECURITY AGREEMENT

This chapter determines the scope of application of this document with specification of the protected resources that support **B&CC's** information systems. Therefore, to determine the protected resources of the Company, the following components have been considered, defined in the previous section of this document:

- Personal data
- Non-automated database
- Document
- Programs and applications
- Treatment systems
- Data treatment
- Treatment centers
- People
- User profile
- Responsible for the treatment

These protected resources can be encompassed within three areas of applicability of the Security agreement:

- Legal Area: Determines the Legal Entity to which the measures described in this document apply.
- Personal Scope: Includes the protected resource defined as persons.
- Scope Material: Comprised of all those files, programs and applications that materialize them, as well as the treatment centers of the archives.

The scope of application therefore covers the systems that in some way participate in the storage or processing of **B&CC information**. In addition, the facilities that support the information systems are considered.

Legal area

This document will apply to B&C Corporation.

Personal environment

This Security agreement, including its attached procedures, is mandatory for all the Entity's personnel, including external personnel who provide services in the offices and facilities of **B&CC** and with access to personal data. Internal standards contained in Sections 3, 4, 5 and 6 of these documents are made known to all personnel of the entity in order to give due COMPLIANCE of obligation stated in Law 1581 of 2012.

The personnel in charge of handling files with personal data that provide their services through remote connections or the processing of files in their premises, will be responsible for compliance with security measures and aspects of a legal nature in the field of data protection, as set out in the corresponding contracts for treatment orders, and described in this Security agreement. Likewise, in Section 6 of this document, the functions and obligations of third parties with access to personal data are described in detail.

Material scope

It is applicable to all physical files that contain personal data held by **B&CC**. In Appendix 25, of this chapter, the list of these can be consulted. The measures established in it are mandatory for the management and for the employees of **B&CC**.

Applicable legislation:

- Article 15 of the Political Constitution of Colombia ("habeas data")
- Law 1581 of 2012, by which general provisions for the protection of personal data are held, approved by the Congress of the Republic of Colombia on October 17, 2012.
- Decree 1377 of 2013, by which Law 1581 of 2012 is partially regulated approved by the President of the Republic of Colombia on July 27 of 2013

4. SECURITY MEASURES APPLICABLE TO AUTOMATED FILES AND NON-AUTOMATED TREATMENT

Security measures contemplated in Article 19 of Decree 1377 of 2013 in accordance with the special categories provided in the Law 1581 of 2012, have been established based on the nature of the information processed. The nature of the information obliges to establish measures in accordance with its classification. Thus, it is considered:

"Sensitive data : Sensitive *data are those that affect the privacy of the Controller or whose improper use can generate discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership in unions , social organizations, human rights or that promotes the interests of any political party or that guarantees the rights and guarantees of opposition political parties as well as data related to health, sexual life and biometric data. "*

The Security Officer of each Database will supervise the development, for each of the existing files, in such a way that the name of the file, its structure, the level of security that corresponds to it, the departments or areas that have access, will be collected. to the information, as well as the detail of how much information is necessary for compliance with current legislation.

In order to give due compliance to the provisions of Article 15 of the Political Constitution of Colombia ("habeas data"), Law 1581 of 2012 and Decree 1377 of 2013, **B&CC** has established the following security measures, which must be known, accepted and respected by all the staff.

For the effective compliance of the security measures, it is necessary to comply with the policies established in Sections 4 and 5 of this document.

5. SECURITY MEASURES APPLICABLE TO FILES AND SYSTEMS AUTOMATED

5.1. BASIC LEVEL MEASURES

5.1.1. Identification and authentication

Given the importance of user access to information systems, **B&CC** has a mechanism that allows the unambiguous and personalized identification of all users who try to access information systems and verify that it is authorized.

The identification mechanism is based on the assignment of identifiers to each of the users who access the information systems.

The mechanism of user authentication to **B&CC** information systems is based on the existence of passwords. For some cases, confidential confirmation codes (signature).

In order to guarantee the confidentiality and integrity of the passwords, as well as the information resident in the Entity's information systems, which could be accessed through these passwords, allocation procedures have been defined and established. and storage of the keys that allow users to access the systems. These procedures require to change with a certain periodicity, always less than a year, the access passwords and while they are in force they are stored in an unintelligible way. The detail of the procedure for allocating, distributing and storing passwords is detailed in Annex 3 of this document.

The policies, rules and procedures that **B&CC** has in relation to this section of identification and authentication of users and assignment of access privileges can be found in Annex 2, Procedure of Identification and Authentication, of this document.

5.1.2. Access control

Given the importance of user access to information systems, **B&CC** has the necessary mechanisms to obtain an updated list of users and profiles that have authorized access to the Entity's information systems.

The subcontracted personnel that deals with files with personal data will have the same obligations and conditions as the employees of **B&CC**.

The logical and operative access of the users to the **B&CC** resources is allowed exclusively according to the needs derived from the professional activity they carry out. Additionally, there are mechanisms to prevent user access to resources with rights other than those authorized.

Solely and exclusively the personnel that manages the systems may grant, alter or cancel the authorized access to the data and resources, according to the criteria established by the person responsible or in charge of processing each of the personal files.

The policies, rules and procedures that **B&CC** has in relation to this section can be found in Annex 4 "Access Control Procedure" of this Document.

5.1.3. Temporary Files

Temporary files must meet the security level that corresponds to them according to the type of information they contain. In this way, they should be required the same security measures as the data files that will be generated throughout the life cycle of the processes.

Any temporary file (automated or non-automated) must be deleted or destroyed once it has ceased to be necessary for the purposes for which it was created.

The security procedures that allow **B&CC** to comply with the security level defined on the temporary files are described in Annex 5 "Procedure for handling temporary files" of this Document.

5.1.4. Management of Supports

B&CC has a procedure, as set out in Annex 6 "Management of media" of this document, by which it is possible to control the computer media and documents containing personal data through mechanisms that allow the identification and management of the inventory of these.

Additionally, **B&CC** has established the necessary mechanisms to guarantee that only authorized personnel have access to media containing information with personal data.

Support emails with attachments containing personal data that are managed by authorized personnel for the execution of their functions remains outside the process of inventory.

The exit of media that contains personal data outside the premises of the person responsible for the file will be conveniently authorized by **B&CC**. Also, in the transfer of the documentation that contains personal data all necessary measures will be established to avoid theft, loss or improper access to information during transport.

The policies, rules and procedures that **B&CC** has in relation to this section can be found in Annex 6 "Management of supports" of this Document.

As for the media that is going to be discarded or reused, the necessary measures will be taken to prevent any subsequent recovery of the information stored therein, prior to their being taken down in the inventory.

In the supports that are going to leave outside the premises of the Responsible of the File as a consequence of maintenance operations, the necessary measures will be taken to prevent any undue recovery of the information stored in them.

5.1.5. Backup

Considering **B&CC** information as a strategic asset for the organization, procedures have been defined for the making of backup copies and the recovery of personal data.

In these procedures are detailed the periodicity of these, the identification of the supports and the custody of these. Also, these procedures ensure the reconstruction of data in the state they were in at the time of loss or destruction of these occurs.

The Responsible for the Treatment or the Manager of the Treatment of each file, when this function is outsourced, will be responsible for verifying the definition, operation and correct application of the backup and recovery procedures, with a frequency of no more than six months.

Within the existing policies regarding the making of backup copies has been established the obligation to make a copy of weekly backup at least. This and other policies, rules and procedures are described in Annex 7 "Backup copies" of this document.

B&CC policies, standards, measures and procedures deemed necessary so that prior to the implementation or modification of information systems that address files with personal data tests are not made with actual data will be established, unless the level of security corresponding to the type of file processed is secured. If it is necessary to carry out tests with real data, a backup copy of the files with affected personal data will be previously made.

Annex 11 "Protection of real data in the testing environment" of this document describes the procedures followed in the Entity for the realization of tests.

5.1.6. Data processing outside the premises

On those occasions in which information is being processed outside the premises of the Security officer, this must be done after having the corresponding authorization to carry out the execution of said treatment.

In unusual cases of data processing outside the **B&CC** premises, it will be necessary to have the express authorization of the Security officer.

Additionally, it must be guaranteed that the security measures of the systems in which said information is going to be treated are adjusted to the measures corresponding to the type of information treated in accordance with or established by Law 1581 of 2012 and Decree 1377 of 2013.

The policies, rules and procedures that **B&CC** has in relation to this section can be found in Annex 12 "Processing of data outside the premises of the Entity" of this document.

5.1.7. Event log

Considering as a type of incident any anomaly that could affect the security of personal data, **B&CC** has established a procedure for the notification and management of such incidents.

This procedure allows recording of each notified incident the type and object, the moment in which it occurred, the person making the notification, who is notified, the status, priority and the effects derived from it, as well as the corrective measures applied for its resolution. In those cases, in which the determination of the moment in which it occurred is not possible, the moment of detection will be recorded.

In Annex 15 "Notification procedure, management and response to incidents" of this document, the procedure for notification, management and response to incidents is described in detail.

5.2. MEASUREMENTS OF AVERAGE LEVEL

5.2.1. Security officer

B&CC, as the Person in Charge of the Archives of personal data, will designate one or more Security Officers, responsible for coordinating and controlling the security measures defined in this document.

In no case is this designation of the Security Officer a delegation of responsibility that corresponds to **B&CC** as the legal entity responsible for the file.

In Section 7 of this Security agreement, a list of the functions of the Security Officer is included.

5.2.2. Audit

The information systems and data processing facilities will be subject periodically to an internal or external audit, in charge of verifying compliance with the Law 1581 of 2012 and Decree 1377 of 2013 and current procedures and instructions on data security.

The periodicity of these audits will be set by **B&CC** but will never be more than two years. Likewise, in the event of significant changes in the information systems, an extraordinary audit will be carried out after the completion of the change processes.

The audit reports resulting from the audits carried out by the auditors should discuss the adaptation to Law 1581 of 2012 and Decree 1377 of 2013 of the existing measures and controls in the Entity, identifying their deficiencies and proposing corrective or complementary measures. These reports must provide the necessary evidence (data, facts, observations, etc.) that supports the opinions reached and the proposed recommendations.

The audit reports will be analyzed by the competent Security Officer, who will raise the conclusions so that **B&CC**, adopts the appropriate corrective measures.

5.2.3. Identification and Authentication

For automated files with medium-level personal data, the user identification and authentication mechanism limit the possibility of repeatedly trying unauthorized access to information systems.

The policies, rules and procedures that **B&CC** has in relation to this section can be found in Annex 2 "User Identification and Authentication Procedure" of this document.

5.2.4. Physical Access Control

Solely and exclusively the authorized personnel may have access to the premises where the information systems with personal data are located.

Policies, standards and procedures that **B&CC** has in relation to this section can be found in Annex 9 "Physical Access Procedure control to the data center (PAP)" and Annex 10 "Procedure for Access Control of Buildings" of this document.

5.2.5. Management of Supports

In regards to the management of computer or other media that may contain personal data, the registration on entry and / or exit thereof, is managed and updated by the IT Systems Area , and must adapt to allow to know, directly or indirectly, the following information: type of support, the date and time of entry, the issuer, the number of media or documents, the type of information that contains the support, the shipping form and the person responsible for the reception and shipment that must be duly authorized.

The policies, rules and procedures that **B&CC** has in relation to this section can be found in Annex 6 "Management of supports and documents" of this document.

5.2.6. Event log

In the register of incidents existing in **B&CC,** the procedures performed to recover the data must be recorded, indicating the person who executed the process, the restored data and, where appropriate, the data that has been necessary to manually record in the recovery process.

Additionally, the express authorization of the Security officer for the execution of the data recovery procedures will be necessary.

Annex 15 "Notification procedure, management and response to incidents" of this document describes in detail the procedure for notification and management of existing incidents.

5.3. HIGH LEVEL MEASURES

5.3.1. Distribution of supports

The identification of the supports will be carried out using comprehensible labeling systems and following a nomenclature that allows the identification of personnel with authorized access to said supports and documents but is unknown and makes it difficult for other people to access it.

The distribution of media containing personal data will be done by encrypting said data or by using mechanisms that guarantee unintelligibility and non-manipulation of information during transport.

Likewise, portable devices will be encrypted when they are used for the processing of personal data outside **B&CC's** facilities. In those cases where it is not possible to encrypt the data, given the nature of the devices, it will be authorized by the Security officer to use them outside the premises, as well as analyzing the risks and needs of the use of the data. the same for the performance of the functions. In any case, the user will be responsible for monitoring and safeguarding said devices at all times.

5.3.2. Access Registry

- For those high-level files on which multiple accesses are made, that is, by several users, the access registry to personal data considered high level by its nature, will incorporate the following characteristics:

- For each access, the identification of the user, the date and time in which the access was made, the file accessed, the type of access and whether it has been authorized or denied will be saved.

- In the case of authorized access, the information that allows identification of the accessed record will be saved.

- The mechanisms that allow the registration of the detailed data in the two previous points will be under the direct control of the competent Security officer without being permissible, in any case, the deactivation of these.

- The minimum period of preservation of the access record will be two years.

- The responsible Security Officer will be responsible for making revisions, with a minimum monthly frequency, of the recorded control information, preparing a report of the revisions made and the problems detected.

The policies, rules and procedures that **B&CC** has in relation to this section can be found in Annex 13 "Register of access to high level files" of this document.

5.3.3. Backup and recovery

For data that, by its nature, is considered high level, the corresponding Backup copies will be made according to the criteria established by the Entity. Additionally, a copy of the backup and the recovery procedures of the data must be kept in a different place from the one in which the computer equipment that deals with them is found, complying in all cases with the security measures required in this document and in the Law 1581 of 2012 and Decree 1377 of 2013.

If the storage of an external backup copy is not possible (outside of the usual location of the computer systems), security measures will be guaranteed to guarantee the integrity of the copies and procedures during storage, in order to allow possible future recoveries.

5.3.4. Telecommunications

For those data that, by their nature, are considered high level, the transmission of these through telecommunications networks will be done by encrypting said data or using any other mechanism that ensures that the information is not intelligible or manipulated by third parties.

6. SECURITY MEASURES APPLICABLE TO DATABASES AND NON-AUTOMATED SYSTEMS

The policies, rules and procedures that **B&CC** has in relation to this section can be found in Annex 18 "Non-automated File Criteria" of this document.

6.1. BASIC LEVEL MEASURES

6.1.1. File criteria

The archives of the supports or documents will be made in files that guarantee the correct conservation of the documents, the location and consultation of the information and allow the exercise of the rights of opposition to the treatment, access, rectification, cancellation and opposition to the treatment.

6.1.2. Storage devices

The storage devices for documents that contain personal data will have mechanisms that hinder their opening.

For those cases in which the devices do not guarantee compliance with this rule, the Security officer will adopt measures that prevent access by unauthorized persons.

The policies, rules and procedures that **B&CC** has in relation to this section can be found in Annex 6 "Management of supports and documents" of this document.

6.1.3. Custody of supports

While the documentation with personal data is not stored in the storage devices because it is in the process of being reviewed or processed, either prior to or after its filing, the person who is in charge of it will keep these documents and prevent that it can be accessed by an unauthorized person.

The policies, rules and procedures that **B&CC** has in relation to this section can be found in Annex 17 "Custody of non-automated files" of this document.

6.2. MIDDLE LEVEL MEASURES

6.2.1. Responsible of Security

B&CC, as the Person in Charge of the Archives of personal data, will designate one or more Security officers, responsible for coordinating and controlling the security measures defined in this document.

In no case is this designation of the Security officer a delegation of responsibility, which corresponds to **B&CC** as the legal entity responsible for the file.

In Section 7 of this Security agreement, a list of the functions of the Security officer is included.

6.2.2. Audit

Information systems and data processing facilities will be periodically submitted to an internal or external audit, in charge of verifying compliance with Law 1581 of 2012 and Decree 1377 of 2013 in relation to current procedures and instructions on data safety.

The periodicity of these audits will be set by **B&CC** but will never be more than two years. Likewise, in case of significant changes in non-automated file storage systems, an extraordinary audit will be carried out after the completion of the change processes.

The audit reports resulting from the audits carried out by the auditors should explain the adequacy to the provisions of Law 1581 of 2012 and Decree 1377 of 2013 of the measures and controls in place at the Entity, identifying their deficiencies and proposing the measures corrective or complementary necessary. These reports must provide the necessary evidence (data, facts, observations, etc.) that supports the opinions reached and the proposed recommendations.

The audit reports will be analyzed by the competent Security officer, who will raise the conclusions so that **B&CC** adopts the appropriate corrective measures. These reports will be available to the Superintendence of Industry and Commerce.

6.3. HIGH LEVEL MEASURES

6.3.1. Storage of information

The cabinets, filing cabinets or other elements in which non-automated files can be stored with personal data are in areas where access is protected with access doors equipped with key-opening systems or another equivalent device. These areas remain closed when access to the documents included in the file is not required.

For those areas in which it is not possible to guarantee restricted access by means of mechanisms that impede free access, alternative measures will be established that guarantee restricted access to said areas only to personnel authorized to said files.

6.3.2. Copy or reproduction

The generation of copies or the reproduction of documents may only be carried out under the control of the authorized personnel in Annex 7 of this document.

For those cases in which copies are generated for the treatment of users with a temporary nature, once the processing of the information of the files or their copies has been made, the copies or reproductions that are no longer necessary will be destroyed so as to avoid access to the information contained in them or their subsequent recovery.

In annex 19 "Destruction of non-automated files" of this document, the procedure for the destruction of non-automated files containing personal data is specified.

In those cases where it is necessary to store the documents or their copies for a time, once they are used they will be stored according to the security criteria described in this document.

In annex 20 "Copy of non-automated files " of this document, the way to proceed is indicated in case of the need to make a copy of non-automated files.

6.3.3. Access to documentation

In the case of non-automated high-level files, **B&CC** will limit access to the documentation containing high-level personal data, only to personnel authorized for that purpose. In those cases, in which it is necessary to access by unauthorized third parties for this purpose, the necessary mechanisms to record such access will be established.

Likewise, in those cases in which it is necessary to access documents with high level personal data by multiple users, the necessary mechanisms will be established to identify the accesses made by each of the users.

Annex 21 "Accessing files not automated" of this document, the guidelines for access to information are described.

6.3.4. Transfer of documentation

Whenever the physical transfer of the documentation contained in a file is carried out, measures must be taken to prevent access or manipulation of the information subject to transfer.

7. RIGHTS, FUNCTIONS AND OBLIGATIONS OF USERS

7.1. GENERAL OBLIGATIONS

In order to comply with the provisions of Law 1581 of 2012 and Decree 1377 of 2013, **B&CC** imposes on its staff compliance with the obligations detailed below, which must be known, accepted and respected by all personnel.

The figures involved in the fulfillment of Rights, Functions and Obligations are those mentioned below:

- Responsible for the Treatment
- In charge of the treatment
- Controller of Information
- Security officer
- User

B&CC, within the Information *Security Standards* published on the Entity's Intranet, includes the guidelines that define the obligations and responsibilities of all persons with access to personal information in particular and the information systems that owns the Entity where this data is stored. These policies are mandatory for the entire organization. The Human Resources department will be in charge of informing the staff of the obligation in the fulfillment of these.

All **B& C** employees will comply with the regulations in force applicable at all times, as well as with the internal rules and procedures of the Entity related to the treatment and protection of personal data.

Any infraction of the aforementioned regulations must be communicated to the Regulatory Compliance area within the Compliance department through the Entity's complaints channel, following the usual internal channels. In case of existing normative conflicts, the hierarchical superior will go to him so that this one arranges what it comes to do, communicating the incident to the corresponding department.

Except in case of urgency, any action will be postponed in which one doubts about whether it can violate any regulation, whatever its rank.

All employees accept the obligations by signing these policies and procedures as defined in the procedure referenced in Annex 22 of this document.

7.1.1. Identification of responsible

The following have been assigned to identify **B&C Corporation**, related to Law 1581 of 2012 and Decree 1377 of 2013

In compliance with Law 1581 of 2012 and Decree 1377 of 2013, the controller authorizes the procesor to perform actions on their behalf under the legal, contractual and regulatory relationship that governs them.

Archive	**RESPONSABLE**
RESPONSABLE FOR THE FILE	B&C Corporation
RESPONSABLE FOR TREATMENT	Legal Manager
MANAGER OF THE TREATMENT	See Annex 25 " *Responsible for the treatment and provision of services" of this document.* B&C Corporation Processing of automated and non-automated files
RESPONSIBLE FOR SECURITY	Security Officer
CHARGERS OF GRANTING, ALTERING OR VOID ACCESS ON DATA AND RESOURCES	See procedure LOPD - 4 "*Access Control*" referenced in Annex 4 of this document. Support Department of B&C Corporation
IN CHARGE OF MANAGING THE NOTIFICATION, MANAGEMENT AND RESPONSE TO INCIDENTS	See procedure 15 - LOPD "Notification, management and response to incidents" referenced in Annex 5 of this document.

Archive PROVIDERS	**RESPONSABLE**
RESPONSIBLE FOR THE FILE	B&C Corporation
RESPONSIBLE FOR TREATMENT	Legal Manager
MANAGER OF THE TREATMENT	See Annex 25 " *Managers of treatment and provision of services" of this document.* Processing of automated and non-automated files
RESPONSIBLE FOR SECURITY	Security Officer
CHARGERS OF GRANTING, ALTERING OR VOID ACCESS ON DATA AND RESOURCES	See procedure LOPD - 4 "Access Control" referenced in Annex 4 of this document. Support Department of B&C Corporation
IN CHARGE OF MANAGING THE NOTIFICATION, MANAGEMENT AND RESPONSE TO INCIDENTS	See procedure 15 - LOPD "Notification, management and response to incidents" referenced in Annex 15 of this document.

Archive CLAIMS	**RESPONSABLE**
RESPONSIBLE FOR THE FILE	B&C Corporation
RESPONSIBLE FOR TREATMENT	Director of Customer Service
MANAGER OF THE TREATMENT	See Annex 25 " *Managers of treatment and provision of services" of this document.* Processing automated files
RESPONSIBLE FOR SECURITY	Director of Customer Service
RESPONSABLE OF GRANTING, ALTERING OR VOID ACCESS ON DATA AND RESOURCES	See procedure LOPD - 4 "Access Control" referenced in Annex 4 of this document. Support Department of B&C Corporation.
IN CHARGE OF MANAGING THE NOTIFICATION, MANAGEMENT AND RESPONSE TO INCIDENTS	See procedure 15 - LOPD "Notification, management and response to incidents" referenced in Annex 15 of this document.

7.1.2. Use and purpose of Personal Information.

Personal information will not be communicated to unauthorized persons. In case there is any requirement on the part of the person affected by the information, the appropriate measures will be taken, within the established in the operating procedures of the Entity to verify that the person requesting it is who they say they are. This information will not be sent by telephone or fax, unless expressly authorized by the interested party. The files of personal information will not be sent by unsafe means. The transmissions will be encrypted in accordance with the security levels required and using the tools provided for that purpose.

Personal information may not be used for purposes other than those for which it was collected. Additionally, it will not be used to reach a third or several, based on the analysis of this information.

The ability to access personal information does not imply authorization. No employee will access personal information that is not strictly necessary for their work. If any employee has access to personal information erroneously, they shall communicate this ability to access to the Support Department to make the appropriate corrections.

7.1.2.1. Personal data will be treated in order to:

a) Execute the corporate purpose of **B&C Corporation.**

b) Comply with the legal obligations of the company, due to the development of its commercial activity.

c) Manage data related to human resources, organizational analysis, development and management of performance reports of labor contracts, labor relations management, processing, management, payroll and compliance with legal obligations.

d) Manage the internal affairs of the company, including, but not limited to accounting, financial and management reports, calculation, presentation and payment of taxes, other records and compliance reports. This information includes personal data of directors and agents of the affiliates of the company.

e) Service and marketing: For the provision of customer services and marketing carried out with a network of customer base.

f) Perform the process of "Know your client - KYC", which consists of the set of procedures for the identification and acceptance of customers.

g) Comply with legal obligations, such as the recommendations of the "Financial Action Group" (FATF), the "Third American Directive" 2005/60 / EC, national laws on money laundering and financing of terrorism, financial services and compliance services tributary and opinion 14/2011 of Article 29 on the protection of data related to the prevention of money laundering and financing of terrorism of the "Working Group on Data Protection".

h) Manage the relationships of business partners: Those who belong to an international network or an international server of customer base. The business partners will also be the subcontractors that perform services to the clients.

i) Develop the business of the company: Analyzing the market of opportunities, the competition and the execution of strategies, to maintain and increase the market in the territories where **B&CC** develops operations.

j) Manage contractual services provided to the client, including, but not limited to, rates.

k) Process, manage and send the necessary information for the processing of payroll, payments, income, records, news and other requirements of the social security system according to Colombian legislation.

l) Negotiate with client prospects. The information obtained will not be used, sold or used for any other negotiation or object.

m) Pay contractual and extracontractual obligations.

n) Send information to governmental or judicial entities, by express request of the same.

o) Support external / internal audit processes.

p) Record the information of the employees and / or officials of the clients in the database of the company.

q) Record the information of the suppliers in the company's database.

r) Contact customers, employees and / or suppliers to send information related to contractual, commercial and legal relationships that may arise.

s) For purposes of security, prevention, investigation and prosecution of fraud.

t) Store the data that by any means and with the due authorization the company has collected.

u) Any other purpose that results in the development of the signing, negotiation and / or execution of the contract or any type of relationship, between the owner of the information and the company.

7.1.2.2. **B&C Corporation** will not sell, transfer or license the information received unless (i) there is express authorization of the Controller to do so and (ii) this is required and / or permitted by law.

7.1.2.3. **B&C Corporation** may subcontract to third parties for the processing of information. When the company effectively sub-contracts the processing of personal information with third parties, it will require said third parties to protect personal information with appropriate security measures, as well as prohibit the use of personal information for purposes other than those contracted and disclosure of such information. Personal information to third parties.

7.1.2.4. **B&C Corporation** may transfer and / or transmit the controller's information to other companies abroad for reasons of safety or administrative efficiency, in accordance with the authorizations of each of the Controllers.

7.1.2.5. When the place where the transfer and / or transmission of Data is to be located outside Colombia, the company will request the Delegation of Protection of Personal Data of the Superintendence of Industry and Commerce the declaration of conformity for the transfer of data.

7.1.2.6. Once the need for the processing of personal data ceases, they may be removed from the company's databases or archived in secure terms so that they are only disclosed when this is done in accordance with the law.

7.1.2.7. **Specific functions and obligations**

Every employee shall accept the obligations by signing said policies and procedures as defined in the "Notification and Disclosure" procedure, referenced in Annex 22 of this Document.

The functions and obligations of the intervening figures are described in the procedure "Personnel Functions and Obligations".

7.1.3. Update personal information

Once new personal information is received that modifies the existing one, it will be updated as soon as possible.

It is strictly forbidden the modification of personal information in a way that alters the actual data, whatever the reason for this action.

The information about personal data will be obtained through the procedures prescribed in the internal rules of the Entity. No information should be acquired by other means.

7.1.4. Compliance with indications from other departments.

All employees will comply punctually with the indications received from the departments on which they depend.

7.1.5. Obligations as processors.

a) Comply with and implement the rules of personal data protection and company policy.
b) Inform the client that from the beginning of the commercial relationship, information susceptible of protection will be collected and processed, and therefore must have the authorization of the controller of the information.
c) Request prior and express authorization of treatment of information to any person who for any contractual or extra-contractual relationship must provide sensitive data.
d) Keep updated the Data Processing Policy and make it known to its employees, customers and / or suppliers.

7.1.6. Obligations as Security Officer

a) Ask your clients – processors - the certification in which they claim to have obtained prior authorization from the Controllers of the information to treat it.
b) Ask clients, as processors for information, compliance with the rules of personal data protection.

7.1.7. Rights of the controller

In accordance with Article 8 of Law 1581 of 2012, the rights that assist the controllers of the information, in relation to their personal data are:

a) Know, update and rectify your personal data, within the legal parameters.
b) Request proof of the authorization granted by the Controller of the information to the company, as Responsible for the Treatment, except when expressly excepted as a requirement for the Treatment.
c) Request the company, as Responsible or Manager of the Treatment, information on the use that has been given to personal data.
d) Submit complaints for infractions to the provisions of the law and the rules that modify, add or complement, before the Superintendence of Industry and Commerce.
e) Revoke the authorization and / or request the deletion of data, when the Treatment does not respect the principles, rights and / or constitutional and legal guarantees; provided there is no legal obligation to preserve said data.
f) Free access exclusively to personal data that have been processed and know of the activities that are executed with your information on the occasion of such treatment.

Paragraph: The foregoing does not mean that access will be given to the processes developed in relation to the processing of personal data developed by the company.

7.1.8. Procedure for the Claims of the Controller

7.1.8.1. Contacts:

In case of questions about this Policy, or any concerns or complaints regarding the administration of this, please communicate through:

- **First name:** Alejandro Irirarte Yepez
- **E-Mail:** Legal@bccorporation.org
- **Address:** Carrera 8 # 12c-35 Oficina 402, Bogotá DC - Colombia
- **Tel.:** +57 319 658 6808
- **Area:** Legal

Requests for rectification, complaint, update, consultation, access or data subtraction, should be sent to:

- **Name:** Alejandro Irirarte Yepez
- **E-Mail:** Legal@bccorporation.org
- **Address:** Carrera 8 # 12c-35 Oficina 402, Bogotá DC - Colombia
- **Tel.:** +57 319 658 6808
- **Area:** Legal

7.1.8.2. Information Consultation Procedure

To make inquiries of information submitted to treatment by the company, the owner of said information must:

a) Send to the area in charge (indicated in point 7.1.8.1.) a written request, signed and notarized by the owner of the information or by the heir, with a copy of the identification document of the applicant.
b) In case the heir of the controller requests the information, they must attach a copy of the birth or marriage certificate, a public deed or an authentic copy of the judicial sentence, as applicable, together with the death certificate of the controller.
c) Applications or requests will be answered within a maximum term of ten (10) business days from the receipt of the request or request.
d) If for any reason the area in charge cannot attend the request or request, the interested party will be informed about the reasons for the delay and indicating the date on which the consultation will be attended. This date cannot exceed five (5) business days following the expiration of the first term.
e) If the application is incomplete, the interested party will be required within five (5) days after receipt of the request to correct the faults.
f) After two (2) months from the date of the request, without the applicant submitting the required information, it will be understood that he / she has withdrawn the request, as provided for in article 17 of law 1755 of 2015.

7.1.8.3. Claim Procedure

a) Submit to the area in charge (indicated in point 7.1.8.1.), the complaint or claim in writing, signed and notarized by the owner of the information or by the heir along with the copy of the personal identification of the applicant.
b) In the case of the heir of the owner who request the information they must attach a copy of the birth or marriage certificate, as appropriate, along with the death certificate of the owner.
c) If the claim is incomplete, the interested party will be required within five (5) days after receipt of the claim to correct the faults. After two (2) months from the date of the request, without the applicant submitting the required information, it shall be understood that the claim has been abandoned.
d) In the event that the person receiving the claim is not competent to resolve it, it will notify the corresponding party within a maximum period of two (2) business days and inform the interested party of the situation.
e) Once the complete claim has been received, the area in charge within the company will include in the database a legend that says "claim in process" and the reason for it , in a term not exceeding two (2) business days. This legend must be maintained until the claim is decided.
f) The maximum term for the area in charge of the company to handle the claim will be fifteen (15) business days counted from the day following the date of its receipt.
g) When the manager inside the company cannot attend the claim within said term, the interested party will be informed of the reasons for the delay and the date on which his claim will be handled, which in no case may exceed eight (8) business days. following the expiration of the first term.

8. CREATING, MODIFYING OR LOWERING FILES

8.1. CREATION OF NEW FILES

The creation of a new file must be requested by the director of the department who will be a user of. To do this, you will fill in the application form (see procedure *23 - LOPD - Creation, modification or deletion of files)* that will be sent to **B&CC's** Security officer and the Compliance department to evaluate the need to register a new file or modify one already existing in the General Registry of Data Protection of the Superintendence of Industry and Commerce. The Security officer of **B&CC** may assess together with the Security Officers of the archives existing if the newly created file can be included in any of the logical files already registered and it is only necessary to detail it in this document, its annexes and / or the procedures that develop them.

From these meetings or communications, the different Security officers will be informed of the existing files and the IT Systems department, in case it applies, the origin or inadmissibility of the creation of the new file or the inclusion in any of the files existing logics.

Later, if it is decided that this is a new file, it will be registered as new file in the General Data Protection Registry of the Superintendence of Industry and Commerce. This action will be developed by the Compliance Department, completing the requests of the Agency itself.

The security officer of the new file will fill the inner sheet provided by **B&CC** with the characteristics of the file and security measures that are applicable.

The person in charge of managing the registration of the files with the Superintendence of Industry and Commerce will be the Security officer of **B&CC.**

8.2. MODIFICATION OF THIS POLICY

This policy can be modified at any time, which is why it is recommended that the owners of the information periodically check the website www.bccorporation.org or through the intranet, where they will be notified of the change and the latest version of this policy or the mechanisms to obtain a copy of it will be made available.

9. DISCLOSURE PROCEDURE

The **B&CC** Security officer, as guarantor of the correct disclosure and compliance of the contents of the Security agreement, must communicate (through the HR department) to all employees with access to the **B&CC** information systems or to documentation with personal data, the existence of the Security agreement, the functions and obligations that users must carry out and the importance of their participation in the knowledge and compliance with the security standards detailed therein, to guarantee the protection and confidentiality of **B&CC** data**.**

For all the employees of **B&CC,** periodic training sessions will be held, with delivery of the instructions and reference material on security matters of the LOPD. Likewise, the completion of said courses and their successful completion will be verified. In this way, it is ensured that both former employees and new entrants know relevant principles and concepts in terms of data protection.

Additionally, for new employees, **B&CC** will require the reading and compliance of the confidentiality and data protection clauses by signing the offer letter or at the time of signing the employment contract.

10. PERMANENCE OF THE DATABASES:

The company will keep the personal data at least during the time that the special rules for each case establish it; In cases where the Law does not establish a conservation term, the company will store the information indefinitely.

11. CONFIDENTIALITY AND SECURITY

B&CC will maintain the confidentiality of the Personal Data and will instruct its personnel and the Sub processors. **B&CC** will implement the appropriate technical and organizational measures to guarantee a level of security of Personal Data appropriate to the risk required in accordance with the applicable Data Protection Laws and, when the processing refers to personal data of EU residents, it will take all the required measures in accordance with article 32 of the GDPR. When evaluating the appropriate level of security, **B&CC** must consider in particular the risks presented by the treatment in particular from destruction, loss, alteration, unauthorized disclosure or unauthorized access to the transmitted, stored or access personal data treated otherwise.

11.1. Impact evaluation of data protection

B&CC will provide reasonable assistance to the Client with any data protection impact assessment that is required in accordance with Article 35 of the GDPR and with any prior consultation with any Client Supervision Authority that is required in accordance with Article 36 of the GDPR, in each case in relation to the processing of personal data by **B&CC** on behalf of the client and taking into account the nature of the treatment and the information available to **B&CC.**

12. VALIDITY:

Version of this policy applies from the 01 of November of 201 8