

RULES AND REGULATIONS GOVERNING GRUPO BANCOLOMBIA'S CORPORATE ON-LINE BANKING CHANNEL AND ITS CORPORATE BANKING APP

In using the banking services or products offered by the entities that currently belong or should in the future belong to Grupo Bancolombia, both at home as well as abroad (Bancolombia Panamá, Bancolombia Cayman, Bancolombia Puerto Rico), these provided through its website www.grupobancolombia.com.co, the CLIENT accepts these Rules and Regulations for using Bancolombia's Online Banking Services that apply both to those provided via the Corporate On-Line Banking Channel as well as the Corporate Banking App, hereinafter referred to as the SERVICE, which shall be governed by the terms and conditions therein agreed upon. Taking into account that certain entities belonging to Grupo Bancolombia, hereinafter referred to as the GROUP, are located in different countries which in turn have different legislations, the CLIENT accepts beforehand that, in the event of any non-compliance or dispute, these Rules and Regulations shall be governed by the legislation corresponding to the country where the GROUP's entity is located and with which the CLIENT has commissioned the product or service, this being understood that each event of non-compliance or dispute shall be treated on the basis of each individual financial entity, and not as the entire group of entities. This includes, without being limited to, any e-commerce, intellectual property and bank secrecy law. The CLIENT hereby declares that he/she/it acknowledges that the SERVICE has been commissioned separately from an individual entity and not jointly from the GROUP's entities as a whole.

In accordance with the foregoing, these Rules and Regulations shall be governed by the following clauses:

CLAUSE ONE. All those clients who have requested and have had the service enabled via the Corporate On-Line Banking Channel or the Corporate Banking App (hereinafter referred to the Channels) may use said SERVICE. In order to access the SERVICE, the CLIENT must identify him/her/itself using, in addition to their user names and passwords, several additional security mechanisms implemented by the GROUP, such as digital and/or electronic signatures and/or tokens, soft tokens, and/or protected identity authentication measures by means of push notifications, and/or additional security measures that may be established, these hereinafter referred to as the AUTHENTICATION MECHANISMS, which are personal and non-transferable and must be used only by the User(s) to whom these have been assigned under the CLIENT's own responsibility.

2. Upon registering for the SERVICE, the CLIENT must indicate the names and ID documents of the legal representatives and/or the persons designated as primary users for the purpose of logging onto the Corporate On-Line Banking Channel or the Corporate Banking App, as well as any other user that may be enabled this based on the configuration of the primary or secondary users that the GROUP should so determine for each CLIENT. The AUTHENTICATION MECHANISMS that shall identify the CLIENT when engaging with the GROUP shall consist of one or more keys or passwords and/or a digital and/or electronic signature and/or a token, soft token, and/or any other additional security measures that may be established, according to the authentication method chosen.

3. The SERVICE shall allow the CLIENT to communicate directly via the Internet with the GROUP, in order to provide the CLIENT with information and / or to allow the CLIENT to carry out banking operations and transactions as determined or enabled by the GROUP. Said transactions shall be governed by the specific agreements entered into between the CLIENT and the entities that currently belong or that should in the future belong to the GROUP as well as by the Rules and Regulations governing the use of the respective product or service, or, failing that, by any applicable legislation and customary banking practice.

4. The CLIENT, through all of his/her/its primary users or secondary users, may perform all those acts, operations or transactions that the GROUP should enable via the Channels, providing said users are duly authorized to do so. They may, among other things, manage and request products or services, issue statements of contractual acceptance, consult account balances and movements, send and/or receive wire transfers, deposits and investments, payments, use loans and/or lines of credit that have

been previously approved by the GROUP, countermand orders, freezing accounts and other services enabled by the GROUP. The CLIENT, using the AUTHENTICATION MECHANISMS specifically established, shall be able to identify him/her/itself to the GROUP and perform the different operations or transactions made available at that moment. Likewise, the CLIENT may identify him/her/itself to third parties in accordance with the particular agreements that the GROUP has entered into with said third parties, and for which the AUTHENTICATION MECHANISMS shall serve as a means of identification when engaging with said third parties.

5. In order for the CLIENT to perform account checks, debits, transfers or any other transaction that has been enabled with regard to third party accounts, the GROUP must have previously obtained due authorization from the corresponding third party. It shall be understood that the GROUP may grant credits or overdrafts on the CLIENT's checking accounts, in the event that there are no funds available in said accounts. In this case, these credits shall be governed by the terms, interest rates and other conditions stipulated by the specific agreements that exist at the time said credit is granted as applicable for each entity that belongs or should in the future belong to the GROUP.

6. In order to access the SERVICE, the CLIENT must have in place the physical means to receive or transmit via the Internet the information herein provided. The CLIENT shall acquire and maintain at his/her/its own cost and expense all the communication means and equipment required to use the SERVICE, and the GROUP shall not be responsible for the availability or reliability of said means and equipment.

7. In order to use the SERVICE, the GROUP places at the CLIENT's disposal different options for determining the channel usage terms and conditions for the primary and secondary users.

As part of the channel's features, the CLIENT shall be able to define the **functions** and **privileges** for its primary and secondary users. **Functions** shall allow the CLIENT to define the type of operation or transaction that can be performed by the users, these consisting of both administrative and transactional functions. a) Administrative functions: allow administrative operations to be carried out, including, without being limited to, activating and configuring secondary users, managing approved workflows, among others. This type of function is always assigned to the primary users, whereas for secondary users this is an option to be defined by the primary user(s); b) Transactional functions: allow non-administrative operations to be carried out, including, without being limited to, checking account balances and movements, transferring funds and making payments, among others. **Privileges** allow for user capabilities to be defined with regard to performing transactions using the channel or service and include: a) Direct Implementation Privileges: that is to say the capability to perform an operation without the need for approval, whereby users granted this privilege can also approve operations prepared by other users; b) Approver Privileges: this being the capability to approve operations prepared by other users; c) Preparer Privileges: the capability to prepare operations that another user must approve; d) Preparer - Approver Privileges: the capability to prepare or complete certain transactions, however, a transaction cannot be executed from beginning to end by the same user; that is to say he or she can only prepare but not approve the same transaction, or he or she can also approve transactions initiated by another user.

8. The SERVICE enables the same types of functions and privileges that the primary users have, however, it is the CLIENT who defines whether secondary users may have the same or lesser privileges than the primary users. The CLIENT shall not be able to carry out operations enabled through the GROUP's channels (Corporate On-Line Banking Channel or Corporate Banking App) without complying with the established privileges, this without prejudice to the possibility of modifying these, after fulfilling the requirements established by the GROUP.

9. The GROUP, at its own discretion, may make available to the CLIENT additional security mechanisms such as tokens, soft tokens, digital tokens, push tokens or others, without these being limited to the foregoing, so as to be able to log onto and / or make use of the Corporate On-Line Banking Channel, the Corporate Banking App and the PSE payment service, as shall be notified to the CLIENT through the enabled channels or the website itself.

10. The Token is a personal and non-transferable physical device that generates unique dynamic keys and is considered to be an additional security measure that the GROUP may offer at its own absolute discretion, bearing in mind the CLIENT'S transactional privileges and the need to have an additional security mechanism for logging onto and/or using the Corporate On-Line Banking Channel, the Corporate Banking App and the PSE payment service This without prejudice to the possibility that the GROUP may offer other additional mechanisms such as a second authentication feature for accessing the SERVICE.

In this case, the following terms and conditions would apply to using the token:

10.1. Users who, according to their transactional privileges, require tokens as an additional security measure, must request and activate these using the channels and / or mechanisms that the GROUP shall have laid on for such purpose. Based on their transactional privileges and when accessing the channel, the GROUP shall inform the user(s) of the need to enter the dynamic key generated by the token, this in addition to the AUTHENTICATION **MECHANISMS** herein stipulated.

10.2. The CLIENT irrevocably authorizes the GROUP to deliver the tokens to any of the users registered with the GROUP, or to those who have been authorized in writing when first signing up for the SERVICE or whenever the CLIENT should so request via the channel. The user to whom the token has been assigned may request the Emergency Access Service as a contingency, once the GROUP has enabled this function, which shall allow the user to receive his/her token key, via the e-mail address he/she has registered for this purpose. This key shall enable the CLIENT to make use of the SERVICE. The Emergency Access Service shall have restricted use and be governed by the terms and conditions defined by the GROUP as published on the website www.grupobancolombia.com.co. Upon using the Emergency Access Service, it shall be understood that the CLIENT implicitly accepts the terms and conditions published on the aforementioned website. Since this is for use in a contingency situation only, the GROUP shall not be responsible for any delay in sending the key or should this not be received by the user given any malfunctions detected with the communication systems or equipment used by the user or by the GROUP.

10.3. The Token is personal and non-transferable and must be carried and used only by the CLIENT to whom it was assigned.

10.4. MODIFICATIONS TO THE SECURITY MECHANISM: The GROUP may limit, extend, modify or add to the terms and conditions for using the Token security mechanism by giving prior notice to the CLIENT using the e-mail address that the CLIENT has registered with the corresponding entity belonging to the GROUP or through any other means. Once this change has been announced, the CLIENT shall be entitled to either accept or terminate the amended agreement, within the following fifteen (15) calendar days; should the client fail to cancel the product and continues using the service, it shall be understood that the modifications thereby introduced shall have been duly accepted. The foregoing shall apply notwithstanding any additional security mechanisms that the BANK should introduce for which the CLIENT shall be duly notified beforehand.

11. The CLIENT may not transfer or be represented by third parties when it comes to exercising his/her/its rights and fulfilling his/her/its commitments thus obtained, and shall be responsible for the operations and / or transactions carried out by his/her/its designated employees, users or third parties. The GROUP shall not be responsible for any damages that the CLIENT may suffer due to failure to comply with the obligation hereby assumed. The CLIENT shall indemnify the GROUP for all expense and losses arising from or relating to the unauthorized use of the SERVICE by persons indirectly obtaining access to such or by the CLIENT.

12. The CLIENT shall henceforth accept as evidence of the operations and / or transactions carried out, the electronic records generated by each of the entities that belong or should in the future belong to the GROUP these in the name of the user using the established AUTHENTICATION MECHANISMS, acknowledging the veracity of these records, lists, tapes, bank statements, etc.

13. The GROUP shall endeavor to maintain the SERVICE available to the CLIENT twenty-four (24) hours a day 7 days a week, without prejudice to the specific operating and transactional limitations and restraints established by the GROUP. The GROUP shall process the information and operations whenever the CLIENT should activate the SERVICE through the respective user and

AUTHENTICATION MECHANISMS and / or any other additional assurances that are established, providing these are legally or conventionally possible. Notwithstanding the foregoing, the operations carried out based on the information provided during the day shall be subject to verification by the GROUP, and the CLIENT shall henceforth authorize any adjustment, debit or credit made to the respective accounts or credits in the light of the aforementioned verification, which in any case shall be justified. Should the CLIENT schedule any operations and / or transactions at a future date, the GROUP shall proceed to perform these as required and scheduled by the CLIENT, except for any limitations or restrictions that should be established beforehand.

14. The GROUP reserves the right to interrupt or suspend the SERVICE due to technical difficulties, security problems or disruptions with the telecommunications or electricity services, etc. Likewise, the GROUP may introduce limitations for the operations and / or transactions to be performed using the SERVICE. The GROUP may reject transactions or temporarily or permanently block the services or operations etc. in the following events: **1.** Any default in paying any obligation owing to the GROUP including commission payments relating to using the SERVICE; **2.** Irregularities when using any of the services. **3.** When required as a security measure to protect both the GROUP or the CLIENT against any irregularity or circumstance affecting the service. The cancellation of any banking service or product accessed through the SERVICE. The GROUP reserves the right to add, suspend and / or cancel any of the products offered to the CLIENT through the SERVICE.

15. The CLIENT undertakes to implement all those measures required to prevent its operations from being used as instruments for concealing, managing, investing or using in any way funds or other assets sourced from illicit activities or for the purpose of giving the appearance of legality to these activities.

The CLIENT, on the date when this document is signed, hereby declares that he/she/it is not aware of any investigations, accusations, sanctions or convictions by any competent domestic or foreign authority against either the CLIENT or his/her/its direct or indirect partners or shareholders holding more than a 10% stake in the CLIENT's share capital, or his/her/its legal representatives, senior management, employees in managerial positions or third parties for any action carried out on behalf of or mandated by the CLIENT, nor for the senior management personnel of the CLIENT's subsidiaries or affiliates in any jurisdiction, for the following events i) the alleged commission of crimes relating to asset laundering, including primary or core criminal offenses relating to corruption, or the financing of terrorism; ii) Conduct that is punishable based on administrative, disciplinary, fiscal or judicial law governing violations of any anti-corruption legislation. Furthermore, the CLIENT hereby declares not to have been included in any blacklists maintained by any domestic or foreign authority for the purpose of controlling asset laundering, the financing of terrorism and corruption, in any of their forms.

When the information provided by the CLIENT proves to be untrue, or if during the business relationship the CLIENT maintains with the GROUP, the latter becomes aware of the existence of any investigation, accusation, sanction or conviction against either the CLIENT or any of the natural or legal persons mentioned in the previous paragraph, these arising from any of the equally related events, the GROUP may consequently suspend the service provided, reject any further disbursement or the use of its products, temporarily or permanently block products, channels, services and unilaterally terminate the existing business relationship without this giving rise to the payment of any indemnity.

Should the CLIENT be unable to state that indicated in the second subsection, or that the existence of any of the situations described in said statement shows progress being made in the corresponding proceeding, the GROUP may resort to any of the faculties described in the third subsection of this clause.

16. The CLIENT agrees to the accounting cut-off times according to the type of operation or transaction performed internally by the entity belonging to or that should in the future belong to the GROUP and which shall be permitted by corresponding banking regulators, so as to determine the date on which the operations and / or transactions carried out by the CLIENT shall be recorded.

17. The CLIENT may request or self-manage the processing of the following unforeseen events through the channel, without these being limited to those listed, or said events having a permanent nature:

17.1. Security Changes: these relate to CLIENT Authentication, the AUTHENTICATION MECHANISMS and everything to do with protecting transactions carried out using the Channels.

17.2. Changes relating to authorizing the CLIENT's own products to a third party:

- Authorizing/deleting specific products

17.3. Changes relating to Channel performance:

- Changes to savings and/or checking account numbers for the purpose of collecting channel usage commissions
- Replacing primary users
- Restricting Channel access
- Enabling/disabling the visualization of the CLIENT's own products
- Restricting the use of the Corporate Banking App
- Cancelling the use of the Channel

17.4. Changes relating to transaction restrictions: these relate to the limitations on the amounts and timing (daily, monthly, half-yearly) of the transactions that the Main User (s) may place on the functions and privileges of the Secondary User(s).

The GROUP shall process these changes within a period of one (1) business day. Notwithstanding the foregoing, the GROUP shall not be obliged to comply with said deadline in all those cases in which the identity and documentary checks required to proceed with said request prove to be incomplete or erroneous and / or when the system is malfunctioning.

In the event that the CLIENT should request the change be implemented at the end of the business day, the term for complying with such shall begin on the following business day. The list stipulated in this clause is not exhaustive. The aforementioned changes, as well as the process for addressing these, may be modified by the GROUP and communicated to the CLIENT through the Channel and/or the different official communication media belonging to the GROUP.

18. Each entity that belongs or shall belong to the GROUP is entitled to establish and charge the CLIENT the rates and/or commissions it defines for using the different services, products or transactions offered, which may be set for or determined by the operation carried out and/or the length of the connect time and/or the number of users and/or the volume of the operations performed. The CLIENT shall be given prior notice of the foregoing through the GROUP's website and / or any other means and / or channel. Similarly, the GROUP, in the event that this option exists, shall charge the token and the Emergency Access Service at the defined rate and which shall be announced on the GROUP's website.

First paragraph: The CLIENT hereby authorizes the debiting of the amount corresponding to the value of the rate and/or commission charged from the CLIENT's accounts or deposits.

Second paragraph: The GROUP may readjust the rates to be charged as stipulated in these Rules and Regulations by giving prior notice to the CLIENT through the GROUP's website or by any other means or channel. Once the change is announced, the CLIENT may decide to accept or terminate the contract, within the following fifteen (15) calendar days; should the CLIENT fail to cancel the product, service or channel and continues to use such, it shall be understood that he/she/it accepts the modifications therein introduced.

19. Any complaint arising from the SERVICE or the related costs and expense must be made within thirty (30) days following the date on which the transaction subject to the complaint was carried out. Should the CLIENT fail to lodge a complaint within the aforementioned period, the transaction(s) in question shall be considered approved.

20. In addition to the obligations contained in these Rules and Regulations as well as in the contracts, agreements, rules or regulations governing each product or service offered by the entities belonging or should in the future belong to the GROUP, the CLIENT specifically undertakes to: a) Not allow third parties to use the SERVICE using the key and/or AUTHENTICATION MECHANISMS that may be established. b) Establish the necessary controls in order to prevent unauthorized third parties from using the SERVICE, without prejudice to the CLIENT's responsibility for such operations. The CLIENT is responsible for ensuring that the user supplying the minimum data required for foreign exchange transactions as well as confirming said transactions is duly authorized to perform said operations. c)

Following the recommendations established for using the SERVICE and maintaining the corresponding security measures. d) Maintaining in strict reserve the way the SERVICE is handled together with its functionalities and facilities. e) Informing the users in charge of operating the SERVICE of the respective usage terms and conditions as well as the security recommendations issued by the GROUP. f) In the event that there is a token option: 1) Complying with the usage terms and conditions of this same device as established in Paragraph 10 of these Rules and Regulations. 2) Delivering the token, under the CLIENT's own responsibility, to those users who, according to their assigned transaction privileges, require such as an additional security mechanism, which the GROUP shall have informed the CLIENT when handing over said device. 3) In the event of the token being lost or stolen, the CLIENT shall immediately block the lost or stolen token via the Corporate On-Line Banking Channel or the Telephone Help Line or the channel that the GROUP shall enable for said purpose, under penalty of the CLIENT becoming liable for failing to comply with this obligation. 4) Informing the users in charge of operating the Token, of the respective usage terms and conditions as well as the security recommendations issued by the GROUP. g) Complying with the security recommendations issued by the GROUP on its website. h) Reviewing the account movements made using the SERVICE and informing the respective bank belonging the GROUP of the transactions subject to the complaint.

21. The GROUP shall not be responsible, unless otherwise proven, for the following events, among others: a) An event of force majeure, a fortuitous or unforeseeable circumstance or a third-party act that could adversely affect the CLIENT in so far as preventing, delaying, deflecting or altering the CLIENT's capacity to perform operations and / or transactions. b). Technical problems, maintenance activities or the need to suspend the service as a result of an event of force majeure, a fortuitous or unforeseeable circumstance or a third-party act. c) The inability to perform any operation due to reasons attributable to THE CLIENT, such as a lack of or insufficient funds, inadequate handling of the system, omissions or insufficient information provided on the corresponding forms and applications, damage sustained by the systems, or any other reason beyond the control of the GROUP. d) Any inconvenience caused by the fact that any supplier of goods or services fails to update in a timely manner their billing databases, or because they have carried out updates using the wrong data and consequently payments cannot be made or are made out for the wrong value or scheduled for the wrong date e) Information published on external websites, links to which are featured on the GROUP's website; f) Any inability, delay or deficiency in transmitting the data or operations as requested using the devices used to access the Internet; malfunctions with the CLIENT's equipment, telephone networks and Internet connections as well as any other circumstance beyond the GROUP's control. g) Improper use of the SERVICE on the part of any person whether or not they have been duly authorized by the CLIENT. Consequently, the CLIENT shall be responsible for the operations carried out with each banking entity belonging to the GROUP using the SERVICE, without any additional requirement other than the operation being ordered through the SERVICE and using the access keys according to the terms and conditions laid out in these Rules and Regulations. h) Errors in the amounts paid, the obligation to be paid, the corresponding ID data, etc., since each banking entity belonging to the GROUP shall not be obliged to validate the payment information supplied by the CLIENT through the SERVICE. i) Acts, omissions or guarantees on the part of third parties such as suppliers, websites and any other person

22. In providing the SERVICE, the GROUP may use its own technological platform or that of a third party specifically designated for such purpose and said platform shall comply with all the required security standards. In this case, the CLIENT shall expressly authorize said third party to receive the information required for using the SERVICE for purposes that shall be strictly transactional.

23. These rules and regulations shall remain in force for an indefinite term. The GROUP may, at any time, cancel, modify, limit or add to the terms and conditions herein contained in these Rules and Regulations, giving due notice of such changes on its website or by any other means and or channel enabled for this purpose. Once the change has been announced, the CLIENT may decide to accept or terminate the contract, within the following period of fifteen (15) calendar days; should the CLIENT fail to communicate his/her/its intention to cancel the product, service and/or channel and continues to use such, it shall be understood that he/she/it accepts the modifications thereby introduced. Should the GROUP suspend, restrict or cancel the services provided to the CLIENT, this shall not give rise to any

liability or claim for damages on the part of the CLIENT or third parties. In the case of any discrepancy between the content of the printed version of these Rules and Regulations and that of the electronic version published on the related webpages, the latter version shall prevail.

24. The CLIENT shall register with the entities belonging or should in the future belong to the GROUP with whom he/she/it has contracted products or services, providing the respective registered place of business, telephone number and address, both physical and e-mail, and shall give notice of any subsequent change to said information. All notifications and correspondence sent by the GROUP to the addresses thus given shall be deemed to be entirely valid.

25. The CLIENT hereby acknowledges that all Software and any type of code used on the Website as well as by the Corporate Banking App shall remain the property of the GROUP and/or its suppliers, and is protected by the domestic legislation of all those countries where the GROUP is present along with international intellectual property treaties. Any reproduction or redistribution of such is expressly prohibited by law and may result in civil and criminal penalties. The intellectual property rights corresponding to the GROUP's web page(s) as well as other website screens shall belong to the GROUP's entities, except those that correspond to the GROUP's suppliers by virtue of an agreement. Consequently, any unauthorized use of the information, images, logos and other material provided on these webpages is strictly prohibited.

26. Data inquiries and technical reports other than those required for performing transactions and that the CLIENT should receive through the website, shall be considered as provided for information purposes only and not as any investment recommendation or suggestion implying investment advice that could be binding on the entities belonging or that should in the future belong to the GROUP.

27. The CLIENT who is a foreign exchange resident in Colombia shall be responsible for becoming acquainted with and complying with all those obligations contained in the Colombian Exchange Regime, with regard to all those foreign currency operations carried out using the SERVICE.

The CLIENT declares under oath that the information provided to BANCOLOMBIA S.A., hereinafter referred to as the BANK, in carrying out foreign exchange operations is true, complete, and up-to-date, and corresponds to the minimum foreign exchange data required by the competent foreign exchange authorities. The CLIENT understands and takes full responsibility for any falsehood or inconsistency in providing said information. At the same time, the CLIENT acknowledges and accepts that the BANK, in its capacity as a Forex Market Intermediary (Intermediario del Mercado Cambiario - IMC in Spanish), shall provide the competent administrative and sanctioning authorities with the minimum data thus provided, should this be required by said authorities.

Likewise, the CLIENT authorizes the BANK to acquire the corresponding foreign currency so as to be able to provide the amounts required for carrying out the foreign exchange operations in question. Likewise, the CLIENT hereby irrevocably authorizes the BANK, on his/her/its behalf, to complete all documents as required by the corresponding foreign exchange authorities with regard to the foreign exchange operation carried out.

Should the CLIENT be the holder of any account(s) with any of the foreign-based entities that belong or should in the future belong to the GROUP (Bancolombia Panama, Bancolombia Cayman, Bancolombia Puerto Rico and/or other foreign-based entity that should in the future belong to the GROUP), he/she/it shall abide by the following provisions governing all those operations and activities involving foreign exchange operations or any procedure before the Colombian Foreign Exchange authorities:

- The CLIENT shall be responsible for directly filing before Colombia's Central Bank (Banco de la República) the corresponding Clearing Accounts so that these be then registered via the BANK's On-Line Banking Channel, specifically in the "Foreign Exchange Declaration Tool" module. The BANK shall not be liable for any error made by the CLIENT when registering a Clearing Account via the BANK's On-Line Banking Channel, using the "Foreign Exchange Declaration Tool" module.
- The CLIENT may use the "Foreign Exchange Declaration Tool" module if he/she/it complies with the electronic requirements stipulated by Colombia's Central Bank for sending information via the

latter's website. Should the CLIENT not have such requirement at his/she/its disposal, he/she/it must request this directly from Colombia's Central Bank, prior to using this service.

- The CLIENT shall be responsible for filling out and submitting the Foreign Exchange Statements to Colombia's Central Bank (Banco de la República) and transmitting the exogenous exchange information to the Colombian Tax Authorities (DIAN) within the terms established in the foreign exchange regulations in force in Colombia. Likewise, the CLIENT shall be responsible for the quality of the information provided in its reports, the BANK, through the Corporate On-Line Banking Channel, the Corporate Banking App or the dedicated channel, shall only generate files that serve as input so that the CLIENT may draw up the corresponding report to be submitted to the Colombian Tax Authorities (DIAN), this based on the information that has been provided by the CLIENT on the Foreign Exchange Declarations that have been marked as having been transmitted to Colombia's Central Bank.
- The CLIENT is solely responsible for the information entered and provided through the "Foreign Exchange Declarations Tool" module for subsequently completing the Foreign Exchange Declarations and / or Forms.
- The CLIENT shall be responsible for filling out any additional documents that may not be available on the Corporate On-Line Banking Channel, specifically in the "Foreign Exchange Declarations Tool" module for Clearing Account purposes.
- Primary or Secondary Users using their assigned roles, may enable the option of filling out Foreign Exchange Declarations for other Users and in turn define the accounts based on which they can use the service.
- The CLIENT shall be responsible for the information provided to Colombia's Central Bank on their Foreign Exchange Declarations and Form No. 10.
- The BANK shall not be responsible for the content included in the Foreign Exchange Declarations filed through the Corporate On-Line Banking Channel using the "Foreign Exchange Declarations Tool" module, since the service provided through this on-line module is simply a means for filing and transmitting the aforementioned documents to Colombia's Central Bank.
- Form N° 10 titled "Registrations, Account Movements Report and/or Clearing Account Cancellations" shows the outflows and inflows presented with the clearing accounts. This form also serves as a Foreign Exchange Declaration for Imported Goods (formerly Form No. 1), for Exported Goods (formerly Form No. 2), and for Services, Transfers and Other Items (formerly Form No. 5). "The "Foreign Exchange Declaration Processing" module shall only generate the information pertaining to the operations that are ready to be transmitted.
- When Foreign Exchange Declarations are required in the case of Foreign Debt (formerly Form No. 3) as well as for International Investments (formerly Form No. 4), these must be filed with Colombia's Central Bank prior to Form No. 10, taking into account that stipulated in Chapter 8 of the External Regulatory Circular Letter DCIN-83 issued by Colombia's Central Bank.
- The filing service provided via the Corporate On-Line Banking Channel, specifically using the module "Foreign Exchange Declaration" tool offers the possibility of completing Form N°10, when there have been no movements in the Clearing Account during the entire term in which said form must be transmitted to Colombia's Central Bank. Should this option not be available, the CLIENT must manually fill out and submit Form No. 10 for said period.
- The reconciliation of the inflows and outflows of the Clearing Account for the term allowed for their transmission must correspond to the sum of all the inflows and outflows reported in Form No. 10 for said period. The CLIENT is responsible for performing the respective reconciliation.
- The CLIENT who has this service enabled, agrees with the BANK to complete and transmit Form N° 10 ten days prior to the date on which the corresponding term expires, as required by current foreign exchange rules and regulations, this in order to avoid late filings due to problems in generating the XML-PDF file and / or filings being rejected by Colombia's Central Bank.
- When the CLIENT generates the XML files for transmitting Foreign Exchange Declarations pertaining to External Debt (formerly Form N°3) and International Investments (formerly Form N°4),

he/she/it must save these under the name required for transmitting these using the Colombian Central Bank's website, this pursuant to that provided in the foreign exchange rules and regulations in force.

- Whenever problems arise with transmitting Foreign Exchange Declarations in the case of External Debt (formerly Form N°3), International Investments (formerly Form N°4), and/or Form No. 10, these to Colombia's Central Bank, and which are caused by difficulties in structuring the XML file, the CLIENT must contact the BANK's client service area or its foreign currency manager so as to obtain specialized advice in complying with the foreign exchange requirements regarding Clearing Accounts and/or provide a report on the anomaly detected while providing the file in question via e-mail, solely and exclusively, to the address provided by the client service personnel of the BANK'S Telephone Help Line. It is crucial that this situation be resolved before the deadline for transmitting the Form to Colombia's Central Bank.
- The CLIENT shall be solely responsible for transmitting this information on a timely basis, and consequently, the BANK is exempt from any responsibility for late filings of Form 10 with Colombia's Central Bank as well as for submitting exogenous exchange information to the Colombian Tax Authorities (DIAN).
- The CLIENT must proceed to manually complete the Foreign Exchange Declarations for subsequent transmission to Colombia's Central Bank as well as the files for directly reporting the required information to the Colombian tax authorities (DIAN) using the pre-validation tool, whenever technological difficulties are encountered with the "Foreign Exchange Declaration Tool" module which could entail the late filing of the documents in question.
- Notwithstanding the fact that the parties may introduce modifications by mutual consent, the BANK may limit, extend or modify the terms and conditions of the "Foreign Exchange Declaration Tool" module by giving prior notice to the CLIENT through the Corporate On-Line Banking Channel or the dedicated channel enabled for this purpose. After announcing the modification made, and should the CLIENT continue to use the service, it shall be understood that he/she/it accepts the modifications thereby introduced.
- The BANK shall not be responsible for any files containing the tax information to be reported to the Colombian tax authorities, that correspond to earlier versions than that currently in force.
- The CLIENT shall be responsible for safeguarding the documentation supporting the foreign exchange operations performed, as well as the Foreign Exchange Declarations, Forms and Formats for reporting exogenous exchange information.

Paragraph: The CLIENT who is NOT a foreign exchange resident in Colombia, must abide by the obligations and responsibilities imposed by the Colombian Foreign Exchange Regime, as pertaining to operations performed in Colombia and/or with foreign exchange residents in Colombia.

28. The CLIENT authorizes the entities that belong or should in the future belong to the GROUP, both in Colombia and abroad (Bancolombia Panama, Bancolombia Cayman, Bancolombia Puerto Rico), to collect and process his/her personal data, including sensitive data, so as to process or handle the data listed below as considered necessary and inherent to complying with applicable legislation, performing the financial operation, and offering and managing the products and/or services. In this sense, the CLIENT shall authorize the entities belonging to the GROUP to request, store, consult, share, transfer, inform, report, rectify, process, modify, update, clarify, withdraw or disclose, and generally-speaking use their personal data. The entities belonging to the GROUP are hereby authorized by the CLIENT to request and obtain information and documents relating to the CLIENT, whether from government entities or officials, private individuals or companies, public or private databases, both at home and abroad. In turn, the CLIENT offers prior, express and informed consent to the GROUP's entities for supplying or exchanging information relating to his/her/its personal data (including financial, commercial and credit information (present, past and future), together with their biometric data, as well as all that relating to his/her/its rights and obligations arising from any contract, agreement or operation that the CLIENT has entered into or performed or shall enter into or perform), with other banks or entities or

Information and Risk Operators, in accordance with the confidentiality and personal data treatment policies of those entities belonging to the GROUP in compliance with applicable domestic legislation as well as international standards. Likewise, the CLIENT authorizes each entity belonging to the GROUP with which the CLIENT has contracted the product or service in question, to share the information regarding its products and services, as contained in its databases or in documents or forms corresponding to each entity, with other entities that belong or should in the future belong to the GROUP, this in order to use the SERVICE, so that these entities can, in turn, use this information to offer them benefits, products and services, complying with all applicable rules and regulations, updating the CLIENT's information with said entities, measuring and managing their commercial and administrative performance, this on either an individual or consolidated level along with the different risks to which said entities are exposed, as well as to prevent the improper use of its products and services. The CLIENT agrees that, by using the SERVICE, his/her/its information, as held by each of the GROUP's entities, may be stored either in Colombia or in any other country, providing this complies with the data protection rules and regulations upheld by each of the GROUP's entities.

29. All that which is not strictly stipulated in these rules and regulations shall be prescribed in the contracts, agreements, rules or regulations that govern each product or service provided by the GROUP, as well as that stipulated by applicable legislation.

30. In the event of any modification being introduced to the terms and conditions of these Rules and Regulations, the CLIENT shall be given prior notice through the GROUP's website or any other means or channel enabled for this purpose. Once the change is announced, the CLIENT may decide to accept or terminate the contract, within the following period of fifteen (15) calendar days; should the CLIENT fail to cancel the product, service or channel and continues to use such, it shall be understood that he/she/it accepts the modifications thereby introduced.

31. The CLIENT declares that by accepting these Rules and Regulations, he/she/it accepts that all their products and services as contracted with the entities that belong or should in the future belong to the GROUP, both at home and abroad (Bancolombia Panamá, Bancolombia Cayman, Bancolombia Puerto Rico), shall be included in the SERVICE, providing these are compatible with this channel; and consequently the CLIENT acknowledges and accepts the terms and conditions contained in these Rules and Regulations with each separate entity belonging to the GROUP.

Once the CLIENT accepts the terms and conditions governing the SERVICE, he/she/it shall also be accepting its respective usage policies.

ANNEX: THIRD PARTY PAYMENTS (APPLICABLE TO CLIENTS OF BANCOLOMBIA S.A, ONLY)

This annex, as accepted by the CLIENT, lays out the terms and conditions under which BANCOLOMBIA S.A., hereinafter referred to as the BANK, shall provide its Third-Party Payment Service:

CLAUSE ONE PURPOSE: The BANK undertakes with the CLIENT to make the payment, in the form of Payroll Payments and / or Supplier Payments and / or Third-Party Payments, of all those amounts to be paid to private individuals or legal entities, hereinafter referred to as the THIRD PARTIES, as the CLIENT should so indicate, based on the instructions and schedules given by the latter. For the purposes of providing the service, the BANK shall debit the necessary amounts from the checking or savings account or from any deposit that the CLIENT holds with the BANK, or shall charge the CLIENT's credit card, *Credipago* account (line of revolving on-line credit) or any other means of payment that the BANK has enabled for subsequently depositing the amounts to be paid in the checking or savings accounts belonging to THIRD PARTIES, whether these hold accounts either with the BANK or with any other financial institution. The BANK may authorize payments to be made in cash and/or in the form of a cashier's check, and delivered to the payees or those authorized for such purpose, as the CLIENT shall indicate in the list of payments submitted. These payments shall be made at the BANK's facilities.

CLAUSE TWO: PAYMENT AUTHORIZATIONS: In order to provide the service governed by this annex, the CLIENT shall prepare and send to the BANK through the channels enabled for this purpose, and according to the terms and conditions laid out by the BANK, the list of the third-party payments to be made. This list of payments must contain, among other things, the following information: date to be sent, name of the CLIENT, account number or identification of the deposit to be debited, or the credit card or line of credit to be charged, according to the options enabled by THE BANK, as well as details of the payments required: number(s) of the checking or savings account(s) to be credited, ID document number and names of the THIRD PARTY beneficiaries of the payments to be made, as well as those authorized to claim cashier's checks if applicable, type of account, the financial entity with which the THIRD PARTY holds an account, value of each of the amounts to be credited and/or payments to be made, total value of the operation, number of payments.

PARAGRAPH. The CLIENT authorizes the BANK to modify the contents or technical specifications referred to in this clause, for which it shall give the CLIENT prior notice through its website or any other means and/or channels laid on for this purpose. Once the change has been announced, the CLIENT may decide to accept or terminate the contract, within the following period of fifteen (15) calendar days; should the client fail to cancel the product and continues to use this service, it shall be understood that he/she/it accepts the modifications thus introduced, in accordance with that stipulated in Article 854 of the Colombian Code of Commerce regarding tacit acceptance.

CLAUSE THREE. FUNDS USED TO MAKE PAYMENTS: The CLIENT must have sufficient funds available to make the requested payments. The BANK shall not assume any responsibility for payments that fail to be made, in the event the account to be debited lacks funds, or the account is cancelled, settled or garnished, the card is cancelled, or check deposits are being cleared or any other circumstance pointing to a lack of available funds, or for inconsistencies in the information provided for the accounts to be debited. The foregoing is without prejudice to the fact that in the case of a checking account, the BANK may grant an overdraft to the CLIENT or any other credit facility that the BANK may provide to the CLIENT pursuant to the agreements in effect at the time this is required.

CLAUSE FOUR. RESPONSIBILITY: The BANK assumes no responsibility to the CLIENT in the following events: 1. When the third-party payee accounts are settled or canceled or whether there exists another reason for not being able to make the requested payment. 2. Should payments be delayed or transactions be disrupted due to failures with communication systems, computer equipment or the power supply due to an event of force majeure, a fortuitous or unforeseeable circumstance or a third-party act. 3. Should the operations not be carried out due to an event of force majeure a fortuitous circumstance, the fault of the CLIENT, a situation caused by a third party, and, generally speaking any unforeseen situation. 4. When the CLIENT sends information containing errors with regard to the accounts to be credited or the value of the payments to be made, in such a way that said errors cause payments to be made in accounts different from those of the intended THIRD PARTIES or for different amounts. 5. When the CLIENT has authorized a cash payment and/or a cashier's check to a THIRD PARTY

and said payments are not claimed by the corresponding beneficiaries or those authorized to claim the cashier's check where applicable, this within the term agreed upon with the CLIENT. 6. When payments into accounts held with other financial institutions cannot be made due to circumstances attributable to the recipient institution or the entity serving as a network for transferring such payments.

CLAUSE FIVE. OBLIGATIONS ON THE PART OF THE CLIENT: In fulfilling that stipulated in this Annex, the CLIENT is obliged to: 1. Register the accounts of all those THIRD PARTIES who are beneficiaries of the payments to be made, this prior to when said payments are scheduled to be made and in accordance with the procedure established for such. 2. Provide the BANK with the information regarding the payment orders in the manner and according to the terms stipulated by the BANK. 3. Provide the BANK with all the information and clarifications required for performing the service and to make any modifications to the information thus provided when inconsistencies are detected, this within the term stipulated by the BANK. 4. Maintain the funds required to honor the payment orders. 5. Pay the BANK the commission charged for the Service, as well as any other type of expense, tax or encumbrance caused by performing said payment service. This commission shall be paid in

accordance with the agreed terms and conditions, regardless of whether the operation fails to be finalized due to reasons not attributable to the BANK. 6. In the event that the BANK authorizes THIRD PARTY Payments in the form of cashier's checks to be handed over at a branch office, the CLIENT undertakes to inform the BANK of the beneficiaries of the payments and those authorized to claim said checks, where applicable, in the corresponding payment file to be sent to the BANK. The BANK shall follow the instructions given by the CLIENT for handing over the cashier's checks to the beneficiaries authorized in the list of payments, at the CLIENT's own risk and responsibility.

CLAUSE SIX OBLIGATIONS ON THE PART OF THE BANK: In fulfilling that stipulated in this Annex, the BANK is obliged to: 1. Maintain in the BANK's system all those electronic records in support of the payments made to THIRD PARTIES, this during the term provided by law. Should the CLIENT request said records, the BANK shall cease to be responsible to the CLIENT for maintaining such documents as of the moment when these are handed over. 2. Provide the CLIENT with the corresponding payment information using any means. 3. Crediting the CLIENT's account or deposits with the amounts that could not be paid to THIRD PARTIES. Should the issued cashier's checks not be claimed by the beneficiaries or the authorized payees, where applicable, the BANK, after a period of one (1) month as of the date the respective check is issued, shall order the cancellation of this same, crediting the same funds from which they were taken, without prejudice to the payment of all costs and taxes that may be incurred.

CLAUSE SEVEN. COMMISSION: The CLIENT shall acknowledge a remuneration for the service provided by the BANK, this being the commission charged by the BANK when the service is provided, which may be modified by the BANK. Said commission shall be automatically debited from the account indicated in the service request. Should there be no available funds in the accounts assigned for said purpose, the BANK may debit any of the accounts or deposits that the CLIENT may hold with the BANK in accordance with the agreed conditions. The BANK shall provide the CLIENT with prior notice of the value of the commission to be charged and / or any modifications to be made to such through the BANK's website or in any other means or channel enabled for this purpose, and it shall be understood that the CLIENT accepts said commission in the event the service is not canceled and is continued to be used.

CLAUSE EIGHT. OPERATIONS CARRIED OUT: On the business day following the date on which the operations are carried out, the BANK shall make available to the CLIENT the details of the payments made together with those that were unsuccessful. Likewise, the BANK and the CLIENT may agree on an additional service, namely that the BANK notifies the THIRD PARTY of the payment made, in which case, the CLIENT shall be solely responsible for supplying the correct information as required for sending such notices.

CLAUSE NINE. DOMICILE: The parties shall establish the same domicile for performing this contract as that stated in the service request. Any change of address on the part of the CLIENT must be notified to the BANK in writing.

CLAUSE TEN: While this contract continues in full force and effect, the CLIENT agrees not to assign or endorse to third parties any obligation arising from such.

CLAUSE ELEVEN. MODIFICATIONS: Without prejudice to the possibility of the parties making modifications by mutual consent, the BANK may limit, expand or modify the terms and conditions of this service by giving prior notice of such modifications to the CLIENT through the BANK'S website or any other means or channels enabled for this purpose. Once the change has been announced, the CLIENT may decide to accept or terminate the contract, within the following period of fifteen (15) calendar days; should the client fail to cancel the product and continues to use this service, it shall be understood that he/she/it accepts the modifications thus introduced, in accordance with that stipulated in Article 854 of the Colombian Code of Commerce regarding tacit acceptance.

CLAUSE TWELVE. All expenses, taxes or levies accruing from the use and/or the performance or the provision of the payment service shall be borne by the CLIENT.

CLAUSE THIRTEEN DURATION: The service governed by this Annex shall be provided indefinitely, but either party may terminate said service at any time and without the need to give reasons for such, by providing written notice to the other party to be received no less than one month beforehand.

SECURITY RECOMMENDATIONS FOR THE GROUP'S CORPORATE ON-LINE BANKING CHANNEL AND THE CORPORATE BANKING APP

Notwithstanding the other security recommendations that the GROUP should establish and communicate by any means and / or channel enabled for this purpose, the CLIENT must take into account the following security information:

The GROUP has provided the necessary security mechanisms so that the clients of the Corporate On-Line Banking Channel and the Corporate Banking App may carry out their operations in a safe and secure manner. Each user shall be responsible for using these mechanisms appropriately and therefore users are bound to:

- Not to disclose or share User IDs and / or additional security measures that may be required for using the Corporate On-Line Banking Channel as well as the Corporate Banking App.
- Immediately block the token, or other applicable authentication mechanisms, should this be lost, stolen or otherwise suspected of being compromised.
- In the case that the token option and/or any channel security mechanism exists, this must be kept in a safe place, beyond the reach of unauthorized third parties.
- Permanently review and update all those users who are duly registered to access and / or perform operations on the Corporate On-Line Banking Channel as well as a Corporate Banking App.
- Eliminate all those users who are no longer employed by the CLIENT from the Corporate On-Line Banking Channel as well as a Corporate Banking App.
- Install and maintain the required updates on the computers used to access the GROUP's electronic services, along with security tools such as antivirus, antispyware, personal firewall and operating system updates using the latest security patches released by the manufacturer.
- Should the user have to leave the workstation from which he or she is accessing the Corporate On-Line Banking Channel and Corporate Banking App, he or she should log off to conclude the work session.
- It is the CLIENT's responsibility to validate with the beneficiary of a payment, the accuracy of the information regarding the recipient bank and product to be credited for the operation being performed. The CLIENT shall also be responsible for validating on an internal level, the veracity of any payment operation before this is carried out. In the case of any transaction to be performed we recommend checking the veracity of the information internally with several of the CLIENT's officers and/or using various means (e-mail, mobile phone, landline). The BANK shall not be responsible for scams or other fraudulent activities, in which the client voluntarily carries out the operation.

The GROUP also recommends taking into account the following:

- Always log onto the Corporate On-Line Banking Channel by typing www.grupobancolombia.com
- Avoid accessing the Corporate On-Line Banking Channel using equipment located in public places such as Internet cafes and university facilities.
- Avoid accessing the Corporate On-Line Banking Channel using WIFI connections located in public places such as hotels, airports, restaurants, warehouses, among others.
- Remember that the Corporate On-Line Banking Channel offers different types of channel management tasks and privileges.
- We advise you to use dual mechanisms that allow for greater control over how your operations are handled.
- Memorize passwords and do not write these down anywhere. This is the password for accessing the Corporate On-Line Banking Channel and Corporate Banking App. Upon entering your password, ensure that this is not being observed by unauthorized persons.

- Structure your passwords taking into account different combination of letters, numbers and special characters. Do not include dates of birth, ID numbers, addresses or phone numbers.
- For secret questions, define answers that are not easy for others to decipher.
- Directly report to the GROUP any malfunctioning of the token, when applicable. Do not allow third parties or unauthorized personnel to repair a malfunctioning token.
- Frequently check the security section of www.grupobancolombia.com.
- Periodically review the movements of your banking products.
- Do not download or install programs from unknown sources on the computers used to access the Corporate On-Line Banking Channel, they may contain hidden programs or viruses that could compromise your information and your money.
- If you receive an email attachment, check the validity of the sender before opening. If an email appears to be suspicious, refrain from opening the attachments.
- Do not respond to e-mails or mobile phone messages that request your personal and/or financial information. Report these situations to the GROUP's Customer Care Service so as to obtain more information on how to proceed.
- Consult an IT expert regarding your concerns and best security practices, seeking technical support for securing your computers and information.
- The users of the Corporate On-Line Banking Channel must not be "Local Administrator" users, that is to say, they must not be authorized to install programs on the machine on which financial transactions are performed. This prevents the improper installation of malicious software designed to capture your information.
- If you see that the mouse or computer moves or performs operations only while using the channel, turn off the system and report it to a technical expert. It may well be that a malicious program (application) has been installed controlling your system and using it to make transactions via the channel.

SECURITY RECOMMENDATIONS FOR THE CORPORATE BANKING APP

- Keep the keypad on your mobile phone blocked, do not leave your mobile phone unattended, or lend it to strangers, and do not lend your SIM card for testing purposes.
- Use a non-obvious mobile phone password and do not share it. If your SIM card has a password, make use of it.
- In the event that your mobile phone is lost or stolen, immediately contact your operator and disable your number, also inform the entity with which you have acquired financial services.
- If you are used to installing or downloading applications(programs) on your mobile phone, do so only from reliable familiar sites that ensure absence of malicious programs (malware, spyware, virus), validate the conditions of use before accepting the installation.
- Do not browse unknown sites using your mobile phone. You could be prone to similar attacks as those targeting PCs.
- If your mobile phone requires maintenance or upgrades, never provide maintenance staff with your access codes or passwords. Also, check that no programs or applications other than those you normally use have been installed.
- Do not enable the Bluetooth ports by default. Only do so to connect to the devices used with your mobile phone. Configure an authentication process for these ports to prevent strangers from connecting up with your phone without your knowledge.
- If you use WIFI connections on your mobile phone, use secure protocols (WPA, WPA2) and do not connect up to unknown networks. Do not keep the WIFI connection active.
- Never store access passwords or keys on mobile phones or store financial services on mobile phone directories or files therein contained. If required, make use of data encryption programs.

- If your mobile phone has additional security options (in the case of blackberry, iOS or Android systems, high-end and some mid-range devices) make use of these while finding out more about the functionalities thereby provided.
- If you are used to backing up your mobile software and the data therein stored, do so on a tried and tested work station (PC) and make sure that only you have access to this information.
- Use programs to protect your mobile phone, should these be available Today there are antivirus and similar solutions for certain equipment.

In witness whereof, the parties have accepted the terms and conditions contained in this Application for Electronic Services, Rules and Regulations of the Corporate On-Line Banking Channel and the Bancolumbia Corporate Banking App and Third-Party Payment Annex, by affixing their signatures hereto on ___ day _____ month, 20____.

The guidelines established by each entity belonging or that should in the future belong to the GROUP for the handling and treatment of the client's personal data can be consulted at any time on the website of each of the GROUP's entities.