Online Banking - Online Access Agreement - Company / Sole Trader

Branch	Code

Account Details

Supporting Current Account Number: ☐☐☐☐☐☐☐☐☐☐☐☐

Power to Bind the Company: ☐ One Signature

☐ Two or more Signatures

Transactions Authorizations Rules: ☐ Standard (They are **pre-defined rules** to facilitate the process of accession)

☐ Customized (Forces the filling of the Attachment Rules)

Note: Under Standard Rules, the movement of funds can be made with one or more signatures, depending on the power to bind the Company / Sole Trader with one or more signatures, respectively, with a limit of € 50,000 total per transaction. The necessary signatures correspond to registered Users with the ability to move funds and administer the service. When choosing Standard Rules, the profile of users is limited to the following: access to all services (viewing, handling and service administration); viewing and preparation of operations, or just viewing. If these rules and profiles do not suit your needs you can choose Custom Rules, in which case you must fill and deliver the Attachment – Transaction Authorization Rules form to the Bank, along with this Contract and the Users profile.

Company Details / Sole Trader

Company Name / Name: _____

Tx Id Number: ☐☐☐☐☐☐☐☐☐ Share Capital: _____Euros

Adress: _____

Registered at the _____ Registry of Companies under the number_____

E-mail: _____ @ _____

Representative(s) that bind the Company / Sole Trader

Name: _____ Tax Id Number: ☐☐☐☐☐☐☐☐☐

Name: _____ Tax Id Number: ☐☐☐☐☐☐☐☐☐

Name: _____ Tax Id Number: ☐☐☐☐☐☐☐☐☐

Name: _____ Tax Id Number: ☐☐☐☐☐☐☐☐☐

Name: _____ Tax Id Number: ☐☐☐☐☐☐☐☐☐

User Registration Codes (To be completed by the Bank)

Identification Number: ☐☐☐☐☐☐☐☐ Registration Code: ☐☐☐☐☐☐☐☐☐☐☐☐☐☐

Mod. 10052092

Preliminary Conditions

1. By subscribing this agreement, the Client identified above recognises that he/she/it read in full and accepts the General Conditions for the use of Remote Communication Channels - Millennium bcp Companies (Bank), being bound by the rights and duties herein defined.
2. The Bank, better identified on the side text, is a credit institution registered in the special registry of Banco de Portugal under nr. 33, is a financial intermediary registered with Comissão do Mercado de Valores Mobiliários (CMVM), the Portuguese stock market regulator, under nr. 105, and is a tied insurance intermediary, under nr. 207074605 (date of registry: 26/06/2007). The Bank is authorised to sell as mediator Life and Non Life insurances of the insurance companies Ocidental - Companhia Portuguesa de Seguros de Vida, S.A., Ocidental - Companhia Portuguesa de Seguros, S.A. and Médis - Companhia Portuguesa de Seguros de Saúde, S.A. and also of Pensõesgere - Sociedade Gestora de Fundos de Pensões, S.A. (information and other registration details available at www.asf.com.pt).
3. Banco Comercial Português, S.A. is subject to supervision by the European Central Bank with registered office at Sonnemannstrasse 22, 60314 Frankfurt, Germany and of Banco de Portugal, with registered office at Rua do Ouro, 27 (1100-150 Lisbon), within the scope of the Single Supervision Mechanism, of the Securities Market Commission, headquartered at Av. da Liberdade, no. 252 (1056-801 Lisbon) and of the Supervision Authority for Insurance and Pension Funds, Av. Da República, n.º 76 (1600-205 Lisbon), within the scope of the specific competences of each of these Entities.

Scope

1. For the purposes of this contract, the following are considered remote communication channels between the Customer and the Bank:

a) Internet Channel – the Client's access to the Bank's website at www.millenniumbcp.pt;

b) Mobile Channel – the Client's access to the Bank using the Mobile App service;

c) Telephone Channel, hereinafter referred to as Contact Centre when it involves a call centre service – communication by phone established by initiative of the Client or of the Bank, including the phone contacts established through the Contact Centre (communications associated to the phone numbers 707502424 (domestic call) and +351707502424 (international call) or other numbers that may replace them that are disclosed by the Bank).

2. The remote communication means are remote communication channels granting the Client access to the Bank's services, available at any moment in those channels, the signature of legal acts or contracts within the scope of the bank relation established with the Bank as a credit institution and insurance agent, enabling access to the current account indicated above (Associated Account) for consulting, getting information and making operations, as well as disclosure and sale by the Bank and the subscription of financial products and services from a distance, including those related to payment services, securities and insurances.
3. For the purposes of the previous number, are legal acts or contracts signed within the scope of the bank relation and which may be available for remote access by the Client, all those concerning the processes for the opening, maintenance and closing of current accounts, payment services accounts, credit accounts and accounts for the registration and deposit of financial instruments, the use of those accounts as well as the processes for the subscription and execution of Life and Non-life insurances and the management of incidents, including, namely, the making of operations on insurances, the issue of powers of attorney, the issue of statements regarding personal data, the presentation of claims or other types of requests, the presentation of requests for statements, for information, for copies of bank statements or other documents, the issue of receipts, the subscription of contracts for the use of payment instruments, including payment instruments for online safe purchases and paperless transactions made with card, requests for access codes or for the use of internet services or payment instruments, the entering into contracts to acquire and request TPA's, the subscription of direct debits, the subscription of funds remittance services, the issue and revocation of payment orders, including of permanent or periodical ones, issue of purchase, sale or redemption orders involving financial instruments, even in the Stock exchange, the subscription or redemption of retail investment products and of investment products based on insurances, the request for cheques, the purchase and sale of currency, the making, reinforcement or settlement of term deposits based on insurances, the request for cheques, the making, reinforcement or settlement of term deposits, the subscription and resolution of rental safes, the engagement or management of credit, leasing, factoring, confirming, credits and documentary remittances operations and the issue of guarantees.
4. Thus, by using adequate computer and communication equipment, the natural persons indicated by the Client, hereinafter referred to as Users, will be able to access the Bank through remote channels and execute a number of transactions, namely consultation and / or use of accounts, in accordance with the powers defined by the Client.
5. For transfers and other transactions that involve the use of funds, the Client may customize transaction authorization rules through combinations of digital signature types (A, B, C or E) with a maximum of 5 combinations. All transactions involving the use of funds shall only be executed if the requirements in terms of amounts and combinations of digital signatures defined by the Client and accepted by the Bank are met.
6. Through the remote channels, the Customer may ask to purchase products or services with third party entities, under the terms of the agreement entered into between the latter and the Bank.
7. All agreements concluded through the remote communication channels are subordinated to these General Conditions and to the General and Specific Conditions applicable to the account opening agreement of the Associated current account and of other agreements entered into between the parties and with regard to each specific product or service provided, as well as to the Bank's pricing in effect, to the banking law and banking practice in general.

Risks associated with the remote communication channels

1. It is hereby explicitly agreed and accepted that, considering current knowledge and the technologies available, the Bank cannot guarantee that the Customer is completely safe against fraudulent actions of third parties targeting the Customer's account, being the latter bound to strictly follow the security recommendations issued by the Bank at all times, under the terms of the document ANNEX - RISKS AND SAFETY RULES, which is an integrant part of this Agreement and of the regular warnings issued by the Bank at www.millenniumbcp.pt, which the Client commits to read and fully obey.
2. The Bank is in charge of ensuring that its website, Mobile Banking services are reliable and that its servers and IT components are safe.
3. The Customer is responsible for the safety and reliability of the IT and communications equipment used to access

Mod. 10052092

the Bank through remote channels, namely computers, mobile phones and internet connections owned by him/her/it or under his/her/its care, under the terms of 3.4 and 3.5 below.

4. The Customer must possess computer and communication equipment with the appropriate characteristics to be able to access the Bank through remote channels, the security, maintenance and any modifications necessary to ensure permanent access to the Bank via this channel being his/her/its responsibility, in accordance with the technological innovations and changes that may be introduced and security recommendations published.
5. The minimum requirements in terms of equipment and communications necessary at any time to use each remote channel are described at www.millenniumbcp.pt, in the information spaces of each channel.

Users

1. The Client shall indicate, by completing and subscribing to this Agreement and its Annexes, rules for the authorization of transactions and Users Profile - and any addenda, which form an integral part thereof, the number and type of digital signatures required to authorize the transactions, as well as the ranges of amounts, and also defines, for each User, the profile in terms of services / functions to which they will have access, type of digital signature and accounts to be viewed / used by them.
2. The Client is entirely and exclusively responsible for defining the profile of Users, who may or may not be employees of the Client, for their selection, appointment and removal. The Client hereby acknowledges and accepts that the use, by the Users, of the services provided by the Bank, as well as the contracting of operations with the Bank by them, under the terms established under this agreement, shall always be taken in all cases and for all legal effects, as being done on behalf of the Client, sole counterparty to the Bank in this Agreement.
3. If the Client has funds and liabilities, namely current accounts, which are based in affiliated entities or associated with Grupo Banco Comercial Português, by subscribing to the terms of this Agreement, the Bank expressly authorizes the Bank to provide information corresponding to its financial assets and associated liabilities to current accounts or contracts that it wishes to view. Since it is possible to carry out transactions available in the remote communication channels at any moment, it also authorizes the Bank to take notice of them and inform the financial institutions where their resources or responsibilities are based.
4. The activation of the service will only take place upon reception and validation of the Agreement by the Bank and, whenever required, of its Annexes - Rules for the Authorization of Transactions and Users Profile - duly filled in and signed by the representatives with sufficient powers to bind the Client. In case the User is a Director or a Company Manager, or in the case of a Self-Employed Individual, if the individual is himself, has a Multichannel Access Code and joins or possess an Acquiring User, he / she may immediately check the accounts.
5. The Client should assign a maximum of three Users the responsibility for the management of the service, that is, to appoint them as Administrators of the Service. It is the responsibility of the Administrators of the Service, exclusively, to: change the accounts and services / functions to which they have access to, and the status (suspended / reactivated or removed) of the Users. The Service Administrator is not allowed to make changes to his own profile, as well as to the other Administrators of the Service, in which case a new registry should be made.
6. The changes arising from the previous point made by the Service Administrators become effective after the respective electronic signature authorization process has been completed.
7. The Client may proceed to designate new Users, making their registry and sending to the Bank the annex(s) - User Profile - duly signed with the Company's stamp. However, the Service Administrator shall have powers to substitute Users with the ability to consult and prepare transactions, but still obeying the authorization rules of transactions that are defined by the Client for this purpose.
8. For security reasons, the Bank is authorized to eliminate users who, for more than a year, have not accessed the services and it is up to the Client to ensure that there are enough users to keep the service running. Deleted Users may be retrieved at the request of a Service Administrator or by the Client.

Mobile App Service

1. In the Users registry, the Client may choose to grant powers for the Mobile App service, among other services, in the option " Nível de acesso a Serviços" (Service Access Level), as enshrined in the User Profile Annex of the User Contract.
2. The management of the Mobile Web service is carried out by the Users to whom the Client has granted access to the Mobile App service, using the option "Outros Serviços" (Other Services) on the website www.millenniumbcp.pt.
3. When the User subscribes to the Mobile App service he/she can set a maximum amount per transaction that will act as an additional security limit on the Mobile channel. This limit does not interfere with the company's authorization rules that are sovereign. You can change this amount, at any time, in the "Change limit per transaction" option.
4. The Mobile App service can be used on a variety of devices. In the process of installing the service on a new device, a new User Code can be assigned specifically to that device and it maintains the same conditions initially defined for the Mobile App service. Regardless of the use of the Mobile App service on various devices, the limit set for executing transactions is non-cumulative.
5. In case of loss, misplacement, theft, or misappropriation of the mobile phone where the M Empresas App is installed, the Client and / or the User should immediately inform the Bank so that the it can block access to that channel.
6. The Client and the User have sole responsibility for the use of the mobile device by third parties other than the latter.

Authentication Data

1. To have the possibility of accessing the Associated Account, resulting from this Agreement and subsequent consultation, requests for information, conveyance of orders or instructions or subscription of contracts , products and services mentioned in chapter 2 of this Contract, the Client must correctly use a set of authentication codes under the terms indicated in this Chapter and in the Annex Risks and Safety Rules, i.e. use of a digital signature which corresponds to the processing of data that can be construed as an individual right and exclusive to the Client and be used to authenticate him/her/it in the channels and ascertain the authorship of e-documents.
2. The customer will be given a User Code and a secret personal code - Password/Multichannel Access Code - which is essential to access the Internet and Mobile channels.
3. Access to the Associated Account through M Empresas App of the Mobile App Millennium service is made through the Secret Code (PIN) consisting of 4 digits, defined in the registration process.
4. As an alternative to the use of the Secret Code (PIN) for an effective access using the M Empresas App of the Mobile App Millennium service, the Client can choose to

Mod. 10052092

login with fingerprint (Touch ID) or facial recognition (Face ID), if the device provides these technologies.

5. For the entering into determined legal acts or contracts in remote channels, namely the carrying out of transactions that involve any kind of alteration to the Client's financial assets, a Digital Certificate may be required or any other alternative manner or means with equivalent or greater security conditions which the Bank provides.
6. The User Code, the Secret Personal Code (Password / Multichannel Access Code), the Digital Certificate and the PIN indicated in 6.3, are personal, confidential and non-transferable Authentication elements, and the User cannot allow third parties to use them, being bound to use them correctly, exclusively in person, on behalf of the Client. The Client is compelled to require Users and to ensure that they are bound, to observe the obligations contained in this clause,taking on all the consequences arising from their use and application and all risks resulting from their undue disclosure.
7. If in any situation, the Client has reason to believe that third parties are aware of the Authentication Data of a User, indicated in 6.4, it must immediately contact the Bank so that the codes are blocked.
8. At www.millenniumbcp.pt the User can, at any moment, change the Password / Multichannel Code and should do it regularly.

Convention on proof

1. The parties accept the legal equivalence of the Authentication Data to the Client's handwritten signatures.
2. The Bank will, in a legitimate manner, assume any access, information request, transmission of orders or instructions, signing of contracts or the entering into any legal acts or contracts through the use of the Authentication Data, as being made by the Client and the Bank will not be required to verify the user's ID in any other way.
3. The provisions mentioned in the previous number cannot be interpreted as a way to inhibit the Bank from obtaining the confirmation from the Customer of the orders or instructions received, including a written confirmation with a handwritten signature, nor damage the adoption of another way to formalize the banking transactions at the Bank's request or due to a legal requirement, or limits the acceptance of a determined type of instructions in view of amounts, number of orders or other criteria.
4. The orders and instructions that the Bank receives, as well as the agreements subscribed or the signing of any legal acts or businesses, provided that they are properly validated through the use of the Authentication Data or the Mobile Digital Key, enjoy full legal effect, the Bank remaining irrevocably legitimated to fulfil or execute them and effect the debits and credits arising from them, it being understood, in any case, that the Bank acts to comply with the orders and instructions given or the will exercised by the Client.
5. It is hereby expressly agreed between the Client and the Bank that, under the terms and for the purposes of article 3 (4) of Decree Law 290-D/99, of 2 August, the correct use of the Authentication Data given to the Customer shall have the same legal value as and serve as proof of the Customer's handwritten signature on paper.
6. The requirements of previous chapter and of this chapter also apply to the contracting of products or services with third party entities, as set out in nr. 2.5., the Bank acting, under this provision, on behalf of and in representation of those entities.

Processing Customer instructions

1. Without damaging the provisions of clause 10.1., the Client may give instructions to the Bank through the remote communication channels any time of the day, every day of the year.
2. The execution of the orders given by the Customer will be carried out in accordance with the conditions applicable to the type of remote channel, service or product requested.
3. The Bank may refrain from executing orders transmitted by the Client where they do not respect applicable statutory provisos or conflict with banking practices, when the account concerned does not have sufficient funds for the intended operation, or when any provision shown in this Contract (annexes and any addenda) is not fulfilled, particularly due to some irregularity in the process of transmitting and/or authorising the order in question that is not adequately remedied within 72 hours.
4. Once authorised and sent to the Bank for immediate processing, no alterations may be made, nor may the transmitted orders be cancelled via the remote channels.
5. Orders issued on non-working days shall be considered as being received on the next working day. The Customer must always heed the time limits set by the Bank for processing orders for the various products and services on the same day.
6. The "BancoMail" function of the internet channel does not obligate the Bank to execute the orders, unless this is expressly agreed.
7. Considering that the services or operations made available by the Bank through the remote communication channels are subject to interference, interruptions, disconnections, and other anomalies, namely as a consequence of malfunctions, overloads, line charges and energy failures, the Customer expressly acknowledges that no liability can be incurred by the Bank as to the potential or actual damages, including loss of profits, that may be borne directly or indirectly by the Customer pursuant to such events, in the extent that such interference, interruptions, disconnections and other anomalies had their origin in acts or omissions from third parties, including the entities that provide service licenses or are suppliers of the Bank and in services held and controlled by those third parties.

Operations recording

1. The Customer and the Bank agree that the computer recording of operations carried out under this Agreement, which may be viewed on screen and/or printed on paper, constitutes appropriate evidence of the orders given by the Customer.
2. Likewise, the Client expressly accepts that the combined statements and entries, the transaction slips and invoices are sent electronically, which may be viewed on screen and/or printed on paper.
3. The Bank undertakes to maintain the information it provides to the Customer via the Internet and Mobile channels permanently updated. However, the Bank's own accounting records shall always take precedence over this.

Suspension, blocked access and termination of the Agreement

1. It is hereby explicitly agreed that the Bank has the right to terminate this agreement, cancelling the service, or to suspend or block the service or the connection of the Client with the Bank, totally or partially, through the remote communication channels:

a) Whenever the Bank considers such is justified for safety or risk reasons or due to the suspicion of non-authorised or fraudulent use of those means:
b) If the Bank sees a significantly increased risk that the Client may be unable to fulfil its liability to pay;
c) The customer, in any way, interrupts its corporate activity, considerably reduces its solvency guarantees or presents a project for voluntary winding up;
d) The Client submits to insolvency or is required to submit its insolvency;
e) The Client applies for a Special Revitalization Process;
f) The authorization for the company to undertake its activities is revoked;

Mod. 10052092

g) Some measure of corrective intervention, provisional administration or resolution is applied;

h) An injunction is requested to suspend corporate resolutions or the Bank is given conflicting orders or instructions that are not adequately remedied or reveal a lack of cohesion or understanding between the members of the management body of the Client entity that, due to its severity and consequences may jeopardize the regularity of operations carried out through the remote channels;

i) For reasons of assistance, maintenance, repair or introduction of improvements to the internal data processing.

2. In such cases as those in the previous number, the Bank commits to immediately inform the Customer that the service has been blocked or cancelled, by means of automatic message or another quick means of communication, confirming such facts and the respective justification later on, within 5 days, in writing to the address indicated in the Associated Account or to the e-mail address previously provided by the Customer, in the Bank's records, except if the justification cannot be provided for objectively grounded safety reasons or if it is forbidden by other applicable legal requirements.
3. For security reasons, the User will be prevented from accessing Bank services through the Internet and Mobile, after three consecutive failed attempts to enter the respective User Code, Password /Multichannel Access Code.
4. Access may be reactivated through a new registry, a communication from the Client requesting the reactivation of the User, a direct request from the User at any branch of the Bank or a another equally safe method that the Bank may announce.
5. In the case of loss, theft or reproduction of the User Code, Password / Multichannel Access Code or in any situation indicating that unauthorised parties have accessed the service, and whenever the Client verifies the registration of any unauthorised transaction on the account, or the existence of errors or irregularities in the execution of operations, the Client shall promptly inform the Bank by the most expeditious means, confirming those facts in writing within a period not exceeding 5 days.
6. If the situation described above occurs and if the Bank objectively considers it to be appropriate, should it find evidence of irregularities or to protect the Client's assets, it shall block access to the accounts through the Internet and Mobile Remote Channels.
7. Blocking accesses according to the preceding paragraph will result in the automatic cancellation of the User Code, Password / Multichannel Access Code and termination of this Agreement, being the Bank obliged to immediately inform the Client of that event in accordance with item above.
8. The Client may at any time order the Bank to suspend the access of certain Users. When the Bank receives this communication by telephone, it shall immediately suspend the User, proceeding with the removal only upon receiving a written communication from the Client.
9. The Bank will eliminate the User's access on the first business day after the one when the written confirmation of the order, laid down in the previous point , is received and cannot be held liable for any damages until the moment of cancellation and, not being verified fraud or negligence due to the occurrence, the Client's liability shall cease.
10. The Bank, on its own initiative, will eliminate Users in the event of statutory changes, expiration of the mandates or definitive obstruction to the exercise of their functions.

Financial information

1. The financial information available through the Internet and Mobile channels, namely prices, indexes, news, studies or other, is provided by the Bank solely for information purposes and is drawn up by third parties which authorize the Bank to disclose it to Customers.
2. In spite of the careful selection made by the Bank concerning its sources of information, errors or omissions may not be detected by it; hence, the Bank cannot guaranty the accuracy of the disclosed information nor be deemed liable for the incorrect use or interpretation of such information.
3. The Client shall use the disclosed financial information at his/her own account and risk and will be exclusively responsible for the investment decisions made based on such information.

Service costs

1. The Client authorizes the Bank to debit the Related Account for costs related to services and operations carried out through the remote channels, including those related to the acquisition of goods or services from other suppliers on the Internet and Mobile App, giving permission to the bank to, in the event of insufficient balance and if it so wishes, but without being obliged to do so, debit the above mentioned account in the necessary amounts or to debit any other account that the Client is or will be holding with the Bank.
2. The operations that the Client carries out with the Bank using the Internet and the Mobile App, as well as any service fees that are due, are subject to the Bank's pricing in force at each moment. The Bank may, at any time, change its pricing. The Customer shall be informed of the changes introduced in the pricing by circular letter, message on the account statement, electronic mail or other appropriate means agreed by the parties. The amendments proposed by the Bank shall come into force after at least 30 days written notice is given to Client, and, should the Client not agree with the proposed amendments, they may state in writing their intention to terminate the contractual relationship within a maximum of 30 days of being informed by the Bank of the amendments, being assumed that it accepts the same them if it does not do that.
3. If the use of the Internet Channel by the Client relies on Digital Certificates, the Bank provides free certificates, up to a maximum of 5, valid for 1 year, which make it possible for 5 Users to register. If the Client wants more digital certificates, it must request them to the User Support Service, but bearing the corresponding costs.
4. The Customer shall bear no costs for contacts initiated by the Bank without prejudice to the price or charges due for the financial service engaged pursuant to each contact.

Processing Personal Data

1. The Bank shall process, or may process, personal data (any information regarding a natural person identified or identifiable) - namely data classified as personal data such as identification data, biographical data, data on account debit/credit entries and other financial data and data regarding risk assessment, for various purposes and data regarding the preference of their customers - for several purposes which may, or not, be directly associated to this Agreement: providing services for receiving deposits, granting loans, making payments and all other transactions banks are permitted to carry out, managing contracts, subcontracting of services including the processing of personal data, complying with tax obligations, reporting and providing information to public authorities, assessing risk, preventing fraud, operations security, credit assignment, marketing and direct marketing, managing communications and claims, assessing customer satisfaction, statistical and accounting processing, collections and litigation, preventing money laundering and terrorism financing, monitoring service quality and complying with the legal and regulatory obligations to which the Bank is subject.

Mod. 10052092

2. Moreover, the Bank is authorized to keep a digital record of the Customer codes and instructions transmitted by them, including telephone conversations under the scope of specialized telephone channels, for proving and ensuring the quality of the commercial transactions carried out between the Bank and the owners of the personal data, and may be used in court in the event of legal action.
3. The Bank may make the profiling of the customers based on their personal data, namely for the creation of customer risk profiles for example for granting credit, presenting proposals for other operations or evaluating the performance of the customer's profile.

4. The processing of some personal data may depend on the holder's prior consent. In the processing of data for direct marketing purposes, the personal data may be processed except if the holder expressly states that he/she does not such processing to be made.
5. The entities responsible for handling the data are the Bank, the joint ventures in which it takes part and companies controlled or partly owned by it, including the Bank's companies, branches and representation offices abroad, to which the Bank may convey the data gathered and registered.
6. Outsourcers, as well as suppliers or services license providers, including those with head office outside the European Union, may have access to the data collected and recorded by the Bank and process the data of the natural persons intervening in this agreement when and to the extent this is necessary to offer products or services sold by the Bank to the customer or to comply with the contract obligations set forth between the Bank and the customer, being those outsourcers bound by the bank secrecy duty as well as by the duty to strictly comply with the legislation and rules applicable to personal data processing under the exact same terms that bind the Bank.
7. Personal Data are stored for different periods of time, depending on the purpose for which they were collected and taking into account the following criteria: legal requirements for safekeeping information, necessity and minimizing the data processed based on the respective purposes. The Bank will erase or render anonymous the personal data of the customers when these are no longer necessary for the purposes for which they were collected and processed.
8. The rights of information, access, to rectification, to object, to erasure, to restriction of processing and to data portability are granted by law, pursuant to a written communication addressed to the Bank. The customer may, at any time, request any information to the Bank on the processing of his/her/its personal data.
9. The exercise of the rights mentioned above or any claim made by the company regarding the processing of his/her/its personal data may presented to the Bank, the respective Data Protection Officer or to the supervisory authority.
10. The account holders' information rights shall be complemented by other policies and documents which may be found in the several communication platforms of the Bank, particularly the Privacy Policy, the updated version of which can be found at any of the Bank's branches or at its website www.millenniumbcp.pt.

Amendment and early termination of the Agreement

1. The Bank shall communicate any amendments that affect this Contract by circular letter, message on the account statement or by another appropriate means with two months prior notice.
2. The proposed amendments shall be considered to have been accepted by the Customer if the Bank has not been notified of his/her/its non-acceptance before the date proposed for the same to come into effect, the Customer being entitled to immediately terminate this agreement free of charge on the grounds of such changes.
3. The Bank and the Customer may, at any time, terminate this Agreement with at least 10 days prior notice.
4. During the 10-day prior notice term, if the Customer fails to meet a proviso of this Agreement, the Bank shall not be obligated to execute new orders. Orders given prior to the termination notice and whose execution date falls after the termination of the Agreement shall expire automatically, unless the Bank is already bound to execute them before third parties.

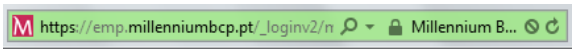
Final Provisions

1. This contract is governed by the Portuguese language, law and jurisdiction.
2. To judge all matters arising from this agreement, the courts of the district of Lisbon, Oporto and the Customer's domicile in Portugal are established as competent, expressly renouncing all others.
3. The Customer may submit complaints or grievances for actions or omissions by bodies and employees of the Bank to the Ombudsman, who will consider them after the necessary investigations have been conducted, and may issue recommendations to the Bank's Executive Committee. The recommendations issued by the Ombudsman are binding for the bodies and services, after approval by the Executive Committee. Questions should be submitted in writing for the attention of the Ombudsman, using the address shown for the purpose at www.millenniumbcp.pt.
4. The Client may also present his/her claims to Banco de Portugal. For that purpose it may choose to use the Complaints Book available at the Bank's branches. This Book will be delivered by the Bank immediately after being requested by the Client or the Client may access it by means of the Bank Client Portal where he/she may fill in and print the online claim form and send it by mail to the address of Banco de Portugal, as per instructions described in the above mentioned Portal.
5. Please be informed that the Bank has available a service that receives and extra-judicial handling of any claims that the Customers wish to present; For that purpose, the claims are to be sent to: Customer Care Centre via the number 707502424 and/or by e-mail to the address www.millenniumbcp.pt and/or in writing, the complaint being addressed to Avenida Avenida Professor Doutor Cavaco Silva (Tagus Park – Edifício 3), 2740-256 Porto Salvo.

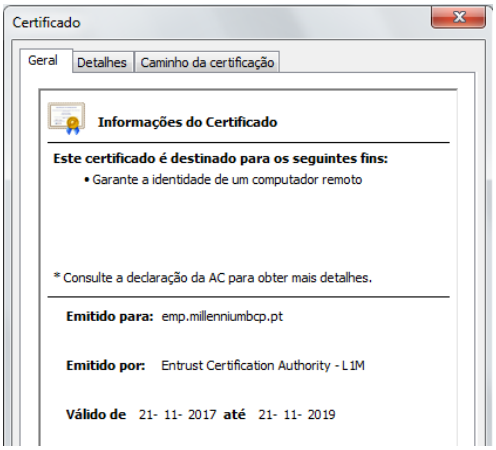
ANNEX - RISKS AND SAFETY RULES

I. Rules to access the internet website www.millenniumbcp.pt

1. Whenever you access your bank accounts online through Millennium bcp's website, please check if: (i) if the address starts with https://emp.millenniumbcp.pt/, (ii) if the address bar is green and (iii) if, at the end of the address bar, a lock is shown followed by "Millennium BCP" as shown:



In case of doubt, confirm the origin of the digital certificate - double click on the padlock - and check if it actually identifies Millennium bcp;



2. The access to the website www.millenniumbcp.pt can be made through:

Online Registration – The registration of the Company and respective User(s) is carried out on the Internet Website www.millenniumbcp.pt. In the access of the website www.millenniumbcp.pt the User Code, the Password and two (2) random digits of the tax identification document are requested (which will always be the same until the login is done successfully);

Registration at the branch – The registration of the Company and its User(s) is carried out at one of the Bank's branches. In the access of the website www.millenniumbcp.pt the User Code and two (3) random digits of the Multichannel Access Code are requested (which will always be the same until the login is done successfully);
Therefore, if additional information is requested it is an attempt to commit fraud and you should report it by calling 707 50 24 24. From abroad call +351 210 04 24 24. Personal assistance available every business day from 8 a.m. to 2 a.m. (GMT) and on non-business days from 10 a.m. to 24:00 (GMT).

3. To access the internet website www.millenniumbcp.pt we never requests your mobile phone number or the installation of software/security programmes.
4. Millennium bcp always sends e-mails with NO links. You should never open Millennium bcp's website through links on messages, search engines or even through your "Favourites". Always type in the complete address www.millenniumbcp.pt to avoid accessing untrustworthy pages, very similar to Millennium bcp's website, as well as the installation of malware in the equipment used to access Millennium bcp's website.
5. Millennium bcp never requests personal and/or confidential data, as for example the Password / Multichannel Access Code, mobile phone number, change of data, etc. by email or by any other mean.
6. You should carefully read the SMS received containing the Authentication Codes since the transaction data are identified in the text message. Never give to third parties the Authentication Codes received via SMS or via token.
7. Don't use obvious Password / Multichannel Access Codes (1234567; 1111111; date of birth; etc) to access the website www.millenniumbcp.pt. Periodically change your access codes to Millennium bcp using the option "Other Services » Personal data management: Change Password/Multichannel Access Code".
8. Define unique Access Codes for the Millennium bcp website www.millenniumbcp.pt and don't use them on other websites.
9. Never give third parties personal identification data that can be used for certification with the mobile phone operators, or User Codes, Multichannel Access Codes or other codes, namely authorisation codes received by SMS or Token.
10. You should also prevent third party access to the devices used for banking operations as well as to their components, such as SIM cards.
11. Should you suspect that your access codes have been compromised, please change them as soon as possible or request that they be blocked using the phone channel.
12. Should you find that your phone is inactive, please contact your operator immediately to ensure the correct functioning of the SIM card.
13. Protect your devices:
    - Install an anti-virus and update it regularly.
    - Use a firewall to filter Internet traffic in and out of your computer;
    - Pay attention to the security updates that credible software companies provide and install them according to the instructions given.
14. You should beware of any e-mail that requires "immediate action" or creates a sense of urgency, especially if it shows spelling errors or bad grammar and has attached executable files. Analyse the e-mails you receive before opening them, always confirming the source and the subject and, if still in doubt, check with the sender.
15. You should always read our Newsletters and the information we provide on security. Please feel free to suggest any security issue you would like to read about on our newsletter. Whenever you have doubts or if you need further information please contact us using the e-mail address empresas@millenniumbcp.pt or call 707 50 45 04. From abroad call +351 210 04 24 24. Personal assistance available every business day from 8 a.m. to 2 a.m. (GMT) and on non-business days from 10 a.m. to 24:00 (GMT).

II. Rules to access the Contact Centre service

1. The Bank's phone service for:

a) Support for Company's users is available by calling 707 50 45 04. From abroad call +351 210 04 24 24. The service is personalized and the User Code and / or the Tax Identification Number (TIN) of the Company / ENI are requested;
b) Further information is available by calling 707 50 24 24. From abroad call +351 210 05 24 24. The service is personalized and you will be asked to enter your current account number and 3 random positions of the Multichannel Access Code.

2. For maintenance of the accesses of the www.millenniumbcp.pt additional security information (personal or relationship with the Bank) may be requested.

III. Rules of Access to Mobile Service

1. Native apps for mobile phones available for Apple and Android TM devices.
2. Install the apps through the brand's official web stores (Apple Store, Play Store).
3. M Empresas App Registration

• **Registration at the branch:** After installing the M Empresas App, define the Security PIN, composed of 4 numbers. Afterwards, enter the User Code and request the SMS Code required for the App's registry.
Enter the requested 3 random positions of your multichannel code to validate the SMS request. Lastly, enter the code you received via SMS and validate it with 3 random positions of the Multichannel Access Code.
Millennium bcp will never, under no circumstance, request simultaneously more than 3 digits of your Multichannel Code.

• Online Registration: after installing the M Empresas App, define the Safety PIN composed of 4 numbers. Afterwards, enter the User Code and request the SMS Code. This request is validated by the Password you use for the companies website. Once confirmed, you will then receive the code by SMS, which you will have to confirm again with the Password.

1. Access to the M Empresas apps:

• Access authentication via the M Empresas App is done using the 4 number PIN, defined in the registration process, or through Touch / Face ID.

• Authentication via Touch/Face ID for access to the M Empresas App is done using the phone's existing fingerprint or face recognition authentication module.

• When you turn on the Touch/Face ID on the M Empresas App, the User should:

a. Guarantee that the only fingerprints/Facial ID recorded on your mobile device, belong to you.

b. Inform the Bank whenever you find that your Touch/Face ID authentication device was compromised, authorizing the Bank to immediately block access to the channel until the situation is solved.

• The mobile device's existing fingerprint/face recognition authentication module is not property or provided by the Bank, therefore the Bank cannot guarantee that access using this means of authentication is secure, nor can it be held liable for an eventual malfunction or inherent losses arising from the use of this authentication.

2. Making and confirming transactions

• Registration at the Branch: the M Empresas App will never ask you, simultaneously, more than 3 digits of the Multichannel Access Code to confirm transactions. Therefore, if additional information is requested it is an attempt to commit fraud and you should report it by calling 707 50 45 04. From abroad call +351 210 04 24 24.

• Online registration: when carrying out transactions, you will be asked to enter the password, the same used in the company's website.

I. Risks

1. Failure to comply with the recommendations on the use of distance communication means issued above may lead to the following risks for the users:

• Third parties may gain access to personal and confidential data;

• Third parties may execute transactions using the assets in the account and generate financial losses.

Signatures and Stamps

Date _____/_____/_____
Year Month Day

Customer

_____

_____

_____

_____

Signatures Verification
The signature of the Representative or Representatives that bind the Company match our files.

Date _____/ _____/ _____

Sign:_____

Banco Comercial Português, S.A.
(Bank's Authorized Signatures)

_____ _____

NUC _____ NUC _____