BYLAWS OF PROVIDING MILLENET® INTERNET BANKING SERVICES FOR CORPORATE BANKING CLIENTS AT BANK MILLENNIUM S.A.

Chapter I
General Provisions

§ 1.

„Bylaws of Providing Millenet® Internet Banking Services for Corporate Banking Clients at Bank Millennium S.A.", herein from the Bylaws lay down the terms of providing Millenet® services at Bank Millennium S.A., herein from the „Bank".

§ 2.

1. The concepts used in the Bylaws denote:
   1) Client – being a resident or non-resident who concluded with the Bank the Bank Account Agreement/Framework Agreement on Bank Accounts and Services for Corporate Clients or Framework Agreement on Keeping Term Deposit Accounts for Corporate Clients Who Do Not Have a Settlement Account in Bank Millennium S.A. or Agreement for Providing Millenet® Internet Banking Services for Corporate Clients,
   2) Agreement – agreement concluded between the Bank and the Client on the basis of which the Bank provides the Millenet® interbank service,
   3) bank account – clearing account or term deposit account conducted by the Bank for the Client or settlement or loan deposit account,
   4) Millenet® service - Millenet® Internet banking service for companies, which provides access to banking services through electronic systems, operating under an Internet address indicated by the Bank and through mobile devices supporting transfer of data (e.g. mobile phones), equipped with software provided by the Bank, hereinafter "the Mobile Application",
   5) User – a User of the Millenet® service, a private person who uses the Millenet® service to perform activities, to which he was authorised by the Client, holding the Millekod, login and access password, optionally using SMS P@ssword, an electronic signature device, hardware token or Mobile P@ssword,
   6) hedging instruments – solutions enabling the Client to safely use the Millenet® service, in particular: Millekod, login, access password, login SMS P@ssword, TLS protocol, Mobile PIN,
   7) authorisation tool – technical solutions accepted by the Bank, in particular: authentication with SMS P@ssword, electronic signature, hardware token, Mobile P@ssword for authorising financial orders placed by the Client, administrative actions mentioned in § 14, instructions connected with ordering products or services as well as other orders and statements placed with the Bank,
   8) authorisation rules – defined by the Client on a form – configuration of the authorisation rules, combination of simultaneous authorisations made by the persons from the specific acceptance groups required for authorisation of individual types of instructions,
   9) Acceptance group – a group defined by letters (A, B, C, D, E, F, G) and designating authorisation options for financial and non-financial instructions of the User which are defined by the Client on a form - configuration of the authorisation rules,
   10) Millekod – Client ID number assigned by the Bank consisting of 8 digits which is used by the User in order to log on to Millenet® service,
   11) Joint Millekod – functionality in the Millenet® service, which permits using accounts belonging to various entities on the level of functionality of a single Millekod,
   12) Access password – password for logging on to Millenet®,
   13) login SMS P@ssword – single-use digital password, sent by the Bank to the mobile phone number defined by Millenet® service User as an additional logging security,
   14) SMS P@ssword – a single-use digital password sent by the Bank to the mobile telephone number defined by the User of the Millenet® service telephone number of the mobile phone used for confirming instructions,
   15) electronic signature – signature made up of a pair of electronic keys assigned to the User of the Millenet® service (public key and private key) equivalent to the manual signature,
   16) hardware token – electronic device with keyboard and display, generating on the grounds of User's data input the digital single-use passwords, used to confirm the financial and non-financial instructions placed,
   17) hardware token PIN– four-digit access code for the hardware token defined by the User before the first use of the device,
   18) single-use P@ssword for the hardware token – single-use six-digit password generated by the hardware token on the grounds of User's data input, used to authorise financial or non-financial instructions,
   19) chip card/USB token – hardware that is a carrier of Millenet® service – pair of digital keys, allocated to the User,
   20) PIN of the chip card / USB token – four-digit access code for chip card/USB token issued to the User with the device,
   21) Mobile P@ssword – an eight-digit password defined by the User in the Millenet® system, which is used for authorising orders placed via the Mobile Application,
   22) Mobile PIN – four digit identification number used for logging on to the Mobile Application,
   23) Protocol of receipt of a token/chip card – form defined by the Bank, containing data identifying the Millenet® User as well as information identifying the electronic signature keys carrier, issued to the User,
   24) Certificate activation protocol – form defined by the Bank, on which the User confirms registration in Millenet® of public key certificate and declares that it shall be used by him for placing the electronic signature,
   25) Protocol of receipt of a hardware token - form, defined by the Bank, containing the identification data of Millenet® User and information identifying the electronic device issued to the User with keyboard and display,
   26) information about authorising User / personal data of Millenet® User – form defined by the Bank, containing personal data of the Millenet® User with authority to authorise orders, which can contain the mobile phone number defined for SMS P@sswords,
   27) Users configuration – form defined by the Bank, on which the Client applies for creation of Users, providing them with access to accounts, products and system functionalities; if "transactional platform" is marked on the form, the Users' configuration form shall also be the "Users' List" in the meaning of the "Transactional Platform Agreement", hereinafter called the Platform Agreement,
   28) Configuration of authorisation rules – form defined by the Bank, on which rules for acceptance of orders and transactions in Millenet® are defined,
   29) Request to create a Common Millekod – form defined by the Bank, on which Clients request creation of a Common Millekod,
   30) Configuration of Users for Common Millekod - form defined by the Bank, on which Clients request creation of Users, granting to them access to accounts, products and system functionalities,
   31) Configuration of authorisation rules for Common Millekod - form defined by the Bank, on which Clients define rules for acceptance of orders and transactions in Millenet® for Common Millekod,
   32) session – access to Millenet® service established with the use of security instruments,
   33) edit Users right – authorises adding, modifying and deleting a User directly in Millenet® internet banking,
   34) User changes authorisation right – authorisation to approve in keeping with authorisation rules the activities performed under the "edit Users" right,

   Helpdesk – team that provides technical assistance for Millenet® on-line banking services at 0801632632 and 225984031 on business days between 8:00 – 18:00.
2. The concepts which are defined in the Bylaws have the meaning assigned in the "General Conditions of opening and maintaining bank accounts for Corporate Banking Clients in Bank Millennium S.A.", hereinafter referred to as the „General Conditions".
3. The Bank can assign to offered products and services commercial names specified in the price list.

Chapter II
Conditions of making available and using the Millenet® service

§ 3.

1. The condition of obtaining access to the Millenet@ service is:
   1) to sign the „Framework Agreement to Bank Accounts and Services for Corporate Clients" or „Agreement for Providing Millenet® Internet Banking Service for Corporate Clients" or "Framework Agreement on Keeping Term Deposit Accounts for Corporate Clients Who Do Not Have a Settlement Account in Bank Millennium S.A.";
   2) submitting at the Bank by the Client:
      a) Users' configuration,
      b) information about authorising User,
      c) copy of Personal Identity Card of each User,
      d) configuration of authorisation rules.
2. The Bank reserves the right to expand the functionality or resignation from conducting the Millenet® service, in particular in the case of changing the functionality of the Bank's IT systems.
3. The Millenet® service is provided 24 hours a day and 7 days a week, reserving section. 6.
4. The Bank can block access to the Millenet® service in connection with the necessity to conduct necessary maintenance works or for security reasons.
5. Millenet® provides the Client with access to the information delivered by the Bank for a period appropriate for preparation of this information and the way in which it is recorded supports its reproduction in an unchanged form. The Client may record and store information and communication on his own permanent data carrier.

§ 4.

1. MilleKod, login, access password, login SMS P@ssword and Mobile PIN identify the User in Millenet® and permit using the system in accordance with rights held.
2. In User configuration the Client defines a login for every User, the phone number, to which the access password for the first and next logins and authorisation tools, including Users' phone numbers that shall be used to receive SMS P@sswords.
3. The Bank submits to the Client Millekod number contacting over the phone one of the persons identified on the form – Users configuration.
4. Every User shall define his/her own access password promptly after the first logging on.
5. The Bank may cancel the demand for login SMS P@ssword for a period of up to 24 hours upon the User's telephone request made at the Helpdesk. Cancellation of the login SMS P@ssword for an indefinite time requires Client's written instruction.
6. Users who confirmed receipt of the device for electronic signature on the token/chip card receipt protocol, shall activate the electronic signature certificate and shall confirm activation by phone, calling to the Helpdesk phone numbers.
7. Users who generated electronic signature keys on a carrier, receipt of which they did not confirm on the token/chip card receipt protocol, shall print from the Millenet® system the certificate activation protocol and deliver it to the Bank. The Bank shall activate the electronic signature certificate after receiving the signed protocol.
8. Users who have confirmed collection of the hardware token on the hardware token receipt protocol may use it upon the Bank's approval of the document.
9. A User holding rights to use the Mobile Application:
   1) has the possibility, after logging on to the Millenet® system, to define an own eight-digit Mobile P@ssword, which is used for authorising orders in the Mobile Application,
   2) shall get the possibility to set up his own four-digit Mobile PIN number, used for logging on to the Mobile Application,
   3) has the possibility, after logging on to the Millenet® system, of obtaining the PUK number which number is used for unlocking Mobile PIN number.
10. The defined mobile phone number, to which passwords are sent for logging on is at the same time the number for contacting the User.
11. Three attempts to enter the incorrect:
    1) access password, login SMS P@ssword, Mobile PIN or Mobile P@ssword shall cause their blockage,
    2) SMS P@ssword shall cause blocking the possibility of placing selected orders.
12. Three consecutive attempts to enter the incorrect access password or login SMS P@ssword shall cause access to the Millenet® system to be locked. In such case the Client, using the rights mentioned in § 14 sect. 1, may unlock the User's access.

13. If none of the Users holds the rights, mentioned in § 14 sect. 1, the Client shall contact the Helpdesk or the Relationship Manager to unlock access.
14. Three consecutive attempts to enter the incorrect Mobile PIN number shall cause access to the Mobile Application to be locked. Access may be unlocked by entering the Mobile PUK number, which is available in Millenet®.
15. Three failed attempts at entering PIN for the hardware token results in launching the de-blocking process by displaying the code that should be entered upon logging to Millenet® service.
16. Three failed attempts at entering single-use password generated by hardware token results in impossibility of authorisation with this device.
17. Three failed attempts at entering PIN of the chip card/USB token results in a blockade of the device.
18. If authorisation tools are locked, the Client should promptly contact the Helpdesk or the Relationship Manager to have them unlocked or replaced.

§ 5.

1. Access to the "Millennium Forex Trader" system, to the extent stipulated in a separate agreement within the framework of Millenet®, shall be granted to Clients who have signed the Platform Agreement.
2. Access to the "Millennium Forex Trader" system may be granted only in written form after submitting to the Bank the form – Users' configuration.
3. Security instruments for logging on to the Millenet® system by a User who was identified on the Users' configuration form as the person authorised to make transactions through the transactional platform, constitute "Means of Authorisation" in the meaning of the Millennium Telecommunication Services sp. z o.o. Telecom Services Provision Regulations. This means that logging on by the a/m User to the Millenet® system is equivalent to logging on to the Millennium Forex Trader Transactional Platform.

§ 6.

1. Access to the Millenet® system is possible provided that the hardware and software used by the Client has been configured in keeping with the Bank's recommendations, in particular in keeping with the Millenet® System User Manual, which is available on the Bank's website.
2. Technical requirements concerning devices, which may be used to run the Mobile Application in Millenet® service, are available on the Bank's website.
3. The Client is required to use the software version indicated by the Bank in the current version of the Manual, mentioned in sect. 1.

§ 7.

1. Users should use security instruments and authorisation instruments appropriate for the Millenet® service in the manner ensuring the observance of their confidentiality and are obliged not to make them available to other persons.
2. If there are suspicions as to knowledge by unauthorised persons of security instruments and access to authorisation instruments the Client should immediately:
   1) change them or block the Millenet® service and next,
   2) contact the Helpdesk or the Relationship Manager in order to obtain new security instruments or authorisation instruments.

§ 8.

1. Personal data of the authorising User SMS P@ssword must be confirmed by this authorising User on the form - Authorising User Information / Personal Data of Millenet® User.
2. User's personal data and phone number applied in order to receive login SMS P@sswords must be given on a form – Users' configuration.
3. The Bank does not permit using the same mobile phone numbers by various Users under one Millekod.
4. Receipt by a Millenet® User eligible for authorising of a carrier of keys used for placing an electronic signature must be confirmed on the "Token/chip card receipt protocol".
5. Receipt of hardware token by Millenet® User entitled to authorisation must be confirmed with a protocol.
6. Personal data of authorising Users created by the Client in the Millenet® system must be confirmed on the Millenet® User's personal data form. The User acquires the right to authorise orders following positive verification of personal data by the Bank.
7. The Bank reserves the right for verifying the validity of authorisation instruments with which there were authorised instructions at any moment by executing instructions. In the case of a negative verification result the orders shall not be executed.
8. Setting up a Mobile P@ssword requires confirmation with an authorisation tool.
9. The Bank in accordance with the Client may allow the employment of other authorisation instruments than those enumerated in § 2 section 1 item 8.

§ 9.

1. In the Millenet® system the Client can grant Users rights concerning trade finance transactions. Access to trade finance services may be granted only in written form after submitting to the Bank the User configuration form and the authorisation rules configuration form.
2. Granting rights to documentary letters of credit the Client authorises the User to place with the Bank orders to issue, change, transfer a documentary letter of credit; orders to waive restrictions to documents; rejection of non-compliant documents presented under the documentary letter of credit; adding confirmation to the letter of credit; explaining or supplementing the text of mentioned orders/instructions as well as performing other actual or legal actions connected with processing of letters of credit.
3. Granting rights to bank guarantees the Client authorises the User to place with the Bank orders to issue, change a guarantee, reguarantee, Civil Law surety, aval, decision in principle to grant a guarantee or surety as well as performing other actual or legal actions connected with processing of.

§ 10.

1. As part of providing the Millenet® service the Client may apply for linking his accounts to the Millekod of another entity subject to its consent, under the Joint Millekod function. The combining results in the possibility of assigning access to accounts to Users of other entities which signed an „Application for Creating a Joint Millekod" and performed the configuration of Users under a joint Millekod with respect to the newly added accounts of a different entity (Users' configuration for Common Millekod) as well as configuration of authorisation rules for Common Millekod).
2. Functionality rights granted to a User under Common Millekod are valid for all entities assigned to this Millekod.
3. Changes regarding modification, adding and deleting Users, rights and accepting orders and operations in the Millenet® as part of Joint Millekod functionality are made by the Bank upon instructions from the Client submitted on a bank form or with use of the appropriate function in Millenet® by the authorised User/Users.
4. An authorised User is understood to mean a person/persons who hold the right to "edit Users" and "authorise User exchanges".
5. Fees and commissions connected with access to the Millenet® system, with authorisation tools etc. are collected from the Client's account, to the Millekod of which accounts of other entities have been linked.

Chapter III
Transfer of Instructions

§ 11.

1. Users authorise instructions in accordance with their rights and the principles defined by the Client in the document - configuration of the authorisation rules.
2. Authorisation is made by confirmation of the instruction with proper system function and an authorisation tool assigned to the User, i.e.:
   1) Entering the SMS P@ssword received on the mobile phone number provided earlier,
   2) Inserting chip card/USB token with active certificate and stating PIN to the reader/USB port,
   3) Inputting single-use digital password generated by the hardware token.

§ 12.

1. The Bank reserves the right to temporarily or permanently set a maximum daily value of financial instructions authorised with use of individual types of authentication instruments without prior notification of the Client.
2. In order to ensure the safety of funds on the bank account the Bank reserves the right to employ additional security procedures, e.g. confirming of submitted instructions under the telephone numbers indicated by the Client.
3. The daily transactions' limit in the amount of PLN 150,000 (or the equivalent of this amount in currency) is applied to instructions authorised by a single person with an SMS P@ssword.
4. The Bank may execute transactions exceeding the daily limit, mentioned in item 3, if the Client sends the transfer to a recipient's account, to which he had sent transfers earlier or after additional telephone verification with a person with powers to authorise transactions in the Millenet® system.
5. The Bank has the right not to execute instructions if it is impossible to obtain the confirmation of an instruction for any reason.
6. The Bank has the right to block access to the Millenet® service, in particular:
   1) in the case of using the service contrary to the provisions of the agreement with respect to using the Millenet® service
   2) suspicion of using the Millenet® service by unauthorised persons.

§ 13.

1. The orders and statements made by the Client by means of the Millenet® service within the duration of an established session are considered as meeting the requirements of written form and result in obligations and rights whose content is specified in communiques given in Millenet® system.
2. The Client shall be liable for using the Millenet® service and for the instructions placed through it.
3. The Client is obliged to control the state of implementation of the instruction placed by means of the Millenet® service.
4. The content of the instruction placed in the mode specified in item 1 shall be legally binding on all the Parties until the execution of the action.
5. Each ordering of a product or service of the Bank placed by means of the Millenet® service denotes the Client's adopting of the conditions of using a given banking product or service.

§ 14.

1. The administrative rights available in the Millenet® service, subject to § 10 section 3, enable in particular:
   1) creating new Users and granting to them rights to accounts and transactions,
   2) granting to Users with locked access password the statuses, which permit unlocking access,
   3) defining the profiles of the Millenet® Users necessary to carry out specific operation types and approval of the introduced changes,
   4) defining acceptance groups of Millenet® system Users, essential to approve specific types of transactions and operations in the Millenet system,
   5) enabling other Users of the Millenet® service to activate the Mobile Application.
2. In the case of assigning by the Client rights to the User of the Millenet® service for authorisation, the provisions of § 10 shall apply.
3. The right to authorise a change of authorisation rules in the Millenet® system may be granted to a User only by the Bank on the basis of written instructions submitted on a Users' configuration form.

§ 15.

Payment orders placed during a session debit the Client's bank account.

§ 16.

1. In case of ceasing performance of a transaction in the Millenet® system the session shall be automatically terminated when the period of inactivity exceeds a limit defined in the system.
2. In case of ceasing to give instructions during a session, use of the Millenet® system should be terminated in the appropriate manner.
3. A new session must be set up to use the Millenet® system again.

§ 17.

1. Within the functions available in the Millenet® service, the authorised Users may submit to the Bank the scans of the original documents required by the Bank within the Customer service.
2. The functionality of submitting documents via Millenet® cannot be used in case of the original documents:
   1) Which are signed bilaterally - by the Bank and the Client,
   2) Documents and statements signed by the Client or Bank, which constitute attachment or security for the agreement concluded between the Bank and the Client,
   3) Documents indispensable for authentication of proper representation of the persons signing the agreement for the Client (e.g. authorisation to represent the Client or authorisation to sign the agreement).

Chapter IV
Statements from the bank account

§ 18.

1. As part of the Millenet® service the Bank makes available to the Client the possibility of downloading bank statements.
2. The Client performs the configuration and establishes the frequency of generating the statements.
3. Configuration of certain types of statements may be made only by the Bank upon the Client's request.

Chapter V
Scope of the Bank's responsibility

§ 19.

As part of providing the Millenet® service the Bank shall be responsible for the timely and compliant with the content execution of the Client's instruction, reserving § 21.

§ 20.

The Bank undertakes to observe banking secrecy as to any information obtained from the Client in connection with the provided Millenet® service.

§ 21.

1. As part of the Millenet® service the Bank shall not be responsible for losses caused by the circumstances beyond the Bank's control, i.e. for:
   1) force majeure – covering e.g. natural disasters, riots, warfare,
   2) strikes,
   3) decisions of public authority agencies,
   4) suspended Millenet® service, for reasons beyond the Bank's control,
   5) submitting an instruction contrary to the binding provisions of law,
   6) releasing the authentication instruments to unauthorised persons,
   7) making available collateral instruments to unauthorised persons.

   and in other cases when in keeping with regulations liability cannot be attributed to the Bank.
2. The Bank shall not be responsible for errors resulting from software other than the one supplied by the Bank.
3. The Bank shall not be responsible:
   1) for the content of the instruction submitted by the Client received at the Bank as part of the Millenet® service,
   2) for the incorrect operation of the installed equipment and computer network employed by the User,
   3) on account of the User's employing the Millenet® service from the browsers other than recommended by the Bank,
   4) on account of an inappropriate security of the Client computer, in particular:
      a) not updating of the operational system,
      b) lack of antivirus software,
   5) on account of disclosure of P@sswords to third parties,
   6) for lack of access to the Mobile Application resulting in particular from inability to transfer data using this Application.

Chapter VI
Scope of the Client's Liability

§ 22.

The Client shall be fully liable for orders executed by the Bank as part of the Millenet® service provided by the Bank.

§ 23.

The Client shall be liable for effects of execution by the Bank of an order, if it was executed as worded.

§ 24.

The Client shall be fully liable for actions and omissions of the Users employing the Millenet® service.

§ 25.

1. The Client must inform the Users about the conditions of the Agreement necessary to execute the instruction as part of the Millenet® service.
2. The Client shall be responsible for proper use and observance of rules of security and confidentiality of identifiers and passwords for the Millenet® system as well as the authorisation tools in use.
3. The Client shall also promptly inform the Bank about any and all circumstances, in result of which his security instruments and authorisations may have been used by unauthorised persons.

Chapter VII
Millenet® service Fees and Commissions

§ 26.

The Bank shall charge fees and commissions for the service, in amounts and under rules stipulated in the price list.

Chapter VIII
Procedure and conditions for resigning from the Millenet® system

§ 27.

1. The agreement for providing the Millenet® service may be terminated in writing by each of the parties, at 30 days' notice or at parties' consent at each time.
2. The Agreement regarding the Millenet® service shall be terminated upon closing of the last settlement account/account for settlement of deposits in zloty, kept for the Client.
3. The Millenet® system agreement shall be terminated upon closing of the last current account in zloty, kept for the Client.

§ 28.

The Bank has the right to terminate the Agreement for important reasons which depending on the terminated scope of Agreement include:

1) making available of the Millekod, login or authorisation tools to other persons,
2) justified suspicion of committing an offence by the Client,
3) disclosing of the incompatibility with facts of information transferred to the Bank on documents and personal data,
4) lack of funds on the account for an uninterrupted period of 3 months for the coverage of fees and commissions due the Bank,
5) infringement of the terms of the Agreement or provisions of the Bylaws,
6) using the Millenet® service contrary to its application

Chapter IX
Final provisions

§ 29.

1. The mode and principles of lodging claims by the Client and processing claims by the Bank are stipulated in the General terms and conditions.
2. To the extent not regulated hereunder, the provisions of the General Conditions as well as generally binding legal regulations shall apply.

Warsaw, December 2015