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) authorisation - expression of consent by the User for execution of a payment order or other transaction in Millenet,
   2) Client – entity 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.,
   3) Agreement – agreement concluded between the Bank and the Client on the basis of which the Bank provides the Millenet interbank Service,
   4) bank account – clearing account or term deposit account conducted by the Bank for the Client or settlement or loan deposit account,
   5) 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",
   6) eBOK Millennium Leasing website - internet module of the Customer Service System available on the Millennium Leasing website: www.millenniumleasing.pl. It is also available for Millenet Service Users after satisfaction of conditions stipulated in § 18 of the Bylaws. Using the eBOK service in Millenet environment by a Client involves the Bank's access to information resulting from conclusion and performance of a lease agreement, provided by Millennium Leasing in this service for the purpose of presentation in the system,
   7) 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 (whereas Clients who are sole traders or partners in civil-law companies may be simultaneously Users), holding the, login and Access password and using Millekod, SMS P@ssword, Hardware token, Hardware Token with reader or Mobile P@ssword,
   8) Hedging instruments – solutions enabling the User to safely use the Millenet Service, in particular: Millekod, login, Access password, login SMS P@ssword, Hardware token, Hardware token with reader TLS protocol, Mobile PIN,
   9) Authorisation tools – technical solutions provided by the Bank, SMS P@ssword, single-use P@ssword from a Hardware Token, single-use P@ssword from a Hardware Token with reader or Mobile P@ssword) for authorising Payment transactions ordered by the User, administrative actions mentioned in § 14, instructions connected with ordering products or Services as well as other orders and statements placed with the Bank,
   10) Authentication tools – provided by the Bank technical solutions, (Temporary Password provided by the Bank, SMS P@ssword, Single-use P@ssword from a Hardware Token or Hardware Token with reader used (depending on the message sent by the Bank) in Millenet service for Strong authentication and Authentication,
   11) 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,
   12) Acceptance group – a group defined by letters (A, B, C, D, E, F, G) and designating authorisation options for financial and non-financial instructions by the User which are defined by the Client on a form - configuration of the authorisation rules,
   13) 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,
   14) Joint Millekod – functionality in the Millenet Service, which permits using accounts belonging to various entities on the level of functionality of a single Millekod,
   15) Access password – password for logging on to Millenet,
   16) login SMSPassword – single-use digital password, sent by the Bank to the mobile phone number defined by Millenet Service User used for logging on to the Millenet Service as logging security,
   17) 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 authorisation the financial or non-financial instructions placed and for logging on to Millenet Service,
   18) Hardware token – electronic device with keyboard and display, generating on the grounds of User's data input the digital single-use passwords, used for authorisation the financial and non-financial instructions placed and for logging on to Millenet Service,
   19) Hardware Token with reader – electronic device with a keyboard, display and reader, generating digital single-use passwords on the basis of data of logging or of the authorised transaction, which the User sends to the device by means of scanning a graphic code containing the data,
   20) Hardware token PIN– four-digit Access code for the Hardware token defined by the User before the first use of the device,
   21) PIN of a Hardware Token with reader – a four to eight digit access code to the Hardware Token with reader, defined by the User during the first use of the device,
   22) single-use P@ssword from 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 and for logging on to Millenet,
   23) Single-use P@ssword from the Hardware Token with reader – single-use six-digit password generated by the Hardware token with reader on the basis of logon data or the authorised transaction, which the User sends to the device by means of scanning a graphic code containing the data, used for authorising financial or non-financial instructions as well as logging on to the Millenet Service,
   24) 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,
   25) Mobile PIN – four digit identification number used for logging on to the Mobile Application,
   26) Secure Envelope - a secure envelope, which contains a single-use temporary code, which is a factor of Strong Authentication, which contains a single-use temporary code for generating a Password for temporary access during the process of first logon. The Secure Envelope Code is valid 90 days from the moment of its assignment Secure Envelope to the User,
   27) Temporary Password - single-use temporary four-digit code, which is a factor of Strong Authentication, for generating an access Password during the process of first logon. The temporary password is valid 30 minutes from the moment of its generation and is set up by the User by means of contacting Helpdesk,
   28) Protocol of receipt of Secure Envelope - form, defined by the Bank, containing the identification data of Millenet User and information identifying the Secure Envelope issued to the User,
   29) Protocol of receipt of a Hardware token/ Hardware token with reader - 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 or an electronic device with keyboard, display and reader,
   30) 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,
   31) 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,
   32) Configuration of Authorisation rules – form defined by the Bank, on which rules for authorisation of payment orders and other transactions in Millenet are defined,
   33) Request to create a Common Millekod – form defined by the Bank, on which Clients request creation of a Common Millekod,
   34) 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,
   35) Configuration of Authorisation rules for Common Millekod - form defined by the Bank, on which Clients define rules for authorisation of payment orders and other transactions in Millenet for Common Millekod,
   36) Session – Access to Millenet Service established with the use of Hedging instruments,
   37) Edit Users right – authorises adding, modifying and deleting a User directly in Millenet internet banking,
   38) User changes authorisation right – authorisation to approve in keeping with Authorisation rules the activities performed under the "edit Users" right,
   39) Helpdesk – team that provides technical assistance for Millenet Service at 0801632632 and 225984031 on business days between 8:00 – 18:00,
   40) Millennium Leasing - Millennium Leasing sp. z o.o. having head office located in Warsaw at ul. Stanisława Żaryna 2A (02-593 Warszawa), entered into the Register of Entrepreneurs of the National Court Register maintained by Regional Court for the Capital City of Warsaw in Warsaw, KRS 13th Economic Division, under the number KRS 0000081821, with shareholders' equity of 48 195 000 PLN, REGON: 012015417, NIP: PL5260213126,
   41) Act – act on Payment Services,
   42) Provider – entity providing payment services on the grounds of the Act, including the Bank and service providers referred to in § 20,
   43) Payment account – account kept in favour of the Client and used for performing Payment transactions, whereas bank account is also construed as payment account, if this account is used for performing payment transactions as construed by the Act,
   44) Payment transaction – initiated by payer or recipient (as construed by the Act) deposit, transfer or withdrawal of cash,
   45) Authorisation – procedure allowing the Bank to verify User identity,
   46) Strong authentication – means Authentication ensuring protection of data confidentiality based on application of at least two elements that belong to a below category:
   47) knowledge (something exclusively the User knows),
   48) possession (something exclusively the User possesses),
   49) User's characteristics (something that characterises the User),
   50) which are an integral part of this authentication and are independent in a sense that breach of one of these does not weaken the credibility of the others,
   51) White List of VAT Taxpayers – an electronic list of entities registered as VAT taxpayers, kept by the Head of National Revenue Administration under art. 96b of the Act on Tax on Goods and Services (VAT), made available on the website of the Ministry of Finance.
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 defines the scope of services available in Millenet service.
3. The Millenet Service is provided 24 hours a day, 7 days a week, reserving section. 6.
4. The Bank can temporarily cease to provide the Millenet Service in connection with the necessity to conduct necessary maintenance works or for security reasons. In case of the need of temporary suspension of provision of Millenet service due to the necessary maintenance works, the Bank shall inform the Client about the planned unavailability of the Service and the duration of the downtime in an appropriate message visible before logging into the Service.
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, code from the Hardware token or Hardware token with reader and Mobile PIN authenticate the User in Millenet Service and permit using the system in accordance with rights held.
2. In User configuration the Client defines a login for every User, authentication tools and authorisation tools i.e.:
   1) Hardware token or Hardware token with reader for generating authorisation codes and/or
   2) number of mobile phone, to which the login SMSP@ssword, Access passwords for the subsequent logons as well as SMS passwords for authorising transactions will be sent by Bank.
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 with use of Strong Authentication during the first logon process.
5. Users who have confirmed collection of the Hardware token or Hardware token with reader on the Hardware token/Hardware token with reader receipt Protocol may use it upon the Bank's approval of the Protocol.
6. 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 authorisation 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.
7. The defined mobile phone number, to which SMS passwords are sent for logging on is at the same time the number for contacting the User.
8. Attempts to enter the incorrect:
   1) Access password, login SMS P@ssword, Mobile PIN may cause their blockage, of which the User shall be notified prior to setting up the blockage,
   2) SMS P@ssword or Mobile P@ssword may cause blocking the possibility of placing selected orders, of which the User shall be notified prior to setting up the blockage.
9. Consecutive attempts to enter the incorrect Hardware token code or Hardware token with reader code may cause Access to the Millenet system to be locked, of which the User shall be notified prior to setting up the blockage,.
   In such case the Client, using the rights mentioned in § 14 sect. 1, may unlock the User's Access.
10. 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.
11. Consecutive attempts to enter the incorrect Mobile PIN number may cause Access to the Mobile Application to be locked, of which the User shall be notified prior to setting up the blockage,. Access may be unlocked by entering the Mobile PUK number, which is available in Millenet.
12. Three failed attempts at entering PIN for the Hardware token results in launching the de-blocking process by showing on its display the code that should be entered upon logging to Millenet Service. If the Hardware token is a tool used for logging to Millenet, the Helpdesk should be contacted.
13. Triple entry of a wrong PIN number of the Hardware token with reader causes the need to perform an unblocking process by means of scanning the graphic code available after logging on to the Millenet Service. If the Hardware token with reader is a tool used for logging on to the Millenet Service, the Helpdesk must be contacted.
14. Three failed attempts at entering single-use password generated by Hardware token or Hardware token with reader results in impossibility of authorisation with this device.
15. Three failed attempts at entering single-use password provided in the Secure Envelope in case of consecutive attempts shall cause blocking of the possibility to use the code to set up an access Password.
16. Three failed attempts at entering single-use temporary Password, in case of consecutive attempts shall cause blocking of the possibility to use the code to set up an access Password.
17. If Authorisation tools or Authentication 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. Hedging 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 Hedging instruments, Authentication tools and Authorisation tools 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 Hedging instruments, Authentication tools or Access to Authorisation tools 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 Hedging instruments, Authentication tools or Authorisation tools.

§ 8.

1. Personal data of the authorising User 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 by Client 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 of Hardware token or Hardware token with reader by Millenet User entitled to authorisation must be confirmed with a protocol.
5. Receipt of the Secure Envelope must be confirmed with a Secure Envelope Receipt Protocol. The Bank may issue a Secure Envelope personally to the User identified in the application or to a person authorised to incur financial commitments on the Client's behalf, whose signature specimen is on the Signature Specimen Card submitted to the Client's account.
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 following positive verification of personal data by the Bank.
7. The Bank reserves the right for verifying the validity of Authorisation tools with which there were authorised at any moment by executing the Payment transaction or other orders in Millenet. 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 tools than those enumerated in § 2 section 1 item 9.

§ 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 in the amount as per the Service Price List for the Corporate Banking Clients.

Chapter III
Transfer of Instructions
§ 11.

1. Users perform authorisation in accordance with their rights and the principles defined by the Client in the document - configuration of the authorisation rules.
2. Strong User authentication is required, if the User gets access to his/her account online, initiates electronic Payment transaction, conducts through a remote channel an action that may imply a risk of fraud related to the performed payment services or other frauds as well as in case of services initiated by the Providers referred to in § 20. Each of the Authentication Tools used in the Strong Authentication mechanism must be set up and linked to the User.
3. 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) inputting single-use digital password generated by the Hardware token,
   3) inputting single-use digital password generated by the Hardware token with reader,
   4) entering the Mobile P@ssword.

§ 12.

1. 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 Payment transactions under the telephone numbers indicated by the Client.
2. 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 SMSP@ssword and Mobile P@ssword.
3. The Bank may execute transactions exceeding the daily limit, mentioned in item 2, if the Client orders the Payment transactions to a recipient's account, to which he had ordered Payment transactions earlier or after additional telephone verification with a person with powers to authorise in the Millenet system.
4. The Bank has the right not to execute a Payment transaction order if it is impossible to obtain the confirmation of an submitted transaction for any reason.
5. The Bank has the right to block Access to the Millenet Service:
   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,
   3) in case of suspicion or actual occurrence of any unauthorised transactions.
6. Promptly after blocking access to Millenet or the Mobile App the Bank shall contact the Client or User to clarify the situation.

§ 13.

1. The orders and statements made and authorised by the User 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 also by Users, including 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 takes place upon prior acceptance by the Client 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 authorise specific types of Payment transactions and other orders 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 transactions 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 desisting from performance of transactions in the Millenet system, in particular ceasing to give instructions during a Session, use of the Millenet system should be terminated by logging out.
3. A new Session must be set up to use the Millenet system again.

§ 17.

1. Using the functions available in Millenet service, authorised Users may submit to the Bank the following, required by the Bank for Customer Service:
   1) Documents / information prepared by the Client as:
      a) images of the original documents,
      b) unsigned information concerning the Client,
      c) documents in electronic form, bearing an appropriate qualified electronic signature,
   2) documents prepared by third entities / persons other than the Client, as images of original documents or documents in electronic form, bearing an appropriate qualified electronic signature.
2. Qualified electronic signature executed on the documents submitted to the Bank should fulfil the following conditions:
   a) Qualified signature should be issued by qualified supplier entered to the register of trust service suppliers kept by the National Bank of Poland or another supplier located in the territory of the European Union, who is on the European Union Trusted Lists (EUTL);
   b) The certificate should be up-to-date, not revoked, not cancelled as at the time of executing the signature on the document.

§ 18.

1. In the framework of access to Millenet Service Clients have the possibility of getting access to eBOK Millennium Leasing Service.
2. The terms and conditions of providing the eBOK Millennium Leasing Service by Millennium Leasing Sp. z o. o. are stipulated by "Bylaws on Provision of eBOK Millennium Leasing Sp. z o. o. service", hereinafter called "eBOK Bylaws".
3. Granting rights to eBOK Millennium Leasing Service at User Configuration is equivalent to submitting a user configuration form in Millennium Leasing in accordance with eBOK Bylaws.

§ 19.

1. In the Millenet Service the Bank provides the service of White List of VAT Taxpayers verification i.e. an automatic check whether the account, to which a payment is being made, is on the White List of VAT Taxpayers.
2. The White List of VAT Taxpayers Verification Service is performed by the Bank upon the client's demand.
3. The Bank performs the verification with observance of highest technological and security standards. Because the service is auxiliary to Millenet Service and verification of the White List of VAT Taxpayers is made with use of data provided by the Ministry of Finance, the Bank is not liable for non-compliance of the verification result, which will arise in result of errors or obsolescence included in the data made available by the Ministry of Finance.

Chapter IV
Initiated services by Providers
§ 20.

1. The User may use the following services initiated by the Providers:
   1) Payment transaction initiation service – means a service that consist in initiation of payment order by the Provider upon User's request from Payment account kept by the Bank. The service includes information about initiating and conducting a Payment Transaction, which is the same as information made available to a User if the User initiates a transaction directly;
   2) Account information access service – means an online service that consist in providing the User or the Provider consolidated information about at least one Payment account kept for the Client by the Bank.
      The service provides information on the Payment account and history of payment transactions, similar to the information presented in Millenet Service.
   3) Confirmation service for availability of funds on payment account – means online service that consists in initiating, upon the request of the Provider issuing card-based payment instrument, Bank's confirmation of availability on the Client's Payment Account of the amount necessary to perform Payment transaction executed on the basis of this card. Confirmation of fund availability does not mean their blocking on the Payment Account.
      Confirmation service for availability of funds on payment account is not applicable to Payment transactions initiated through card-based payment instruments on which electronic money is stored.
2. Services referred to in section 1, are available for Payment accounts in PLN and foreign currency.
3. Services of the Providers are available for the Users of Payment Accounts available online and require use of Hedging instruments available in Millenet Service.

§ 21.

1. The Bank executes the services initiated by the Providers exclusively on the grounds of the consents granted by the Users to the Providers or in case of the service indicated in § 20 section 1 item 3 – to the Bank and exclusively to the extent of these consents.
2. The Bank provides the User the set of consents, on the grounds of which the Providers' services are delivered and the Provider's data in the consent repository in Millenet on the grounds of User Configuration form.
3. The set of rights enabling a User to agree to provision of services initiated by Providers is defined in the User Configuration form.
4. On the grounds of the information about expressly consent of the User, supplied by the Providers, the Bank enables the Providers to perform the Payment transaction initiation service and the account information access service, based on the User Strong authentication applied in the relation between the Client and the Bank.
5. In connection with execution of the Providers' services Authentication Tools and Authorisation Tools are applied defined for the Millenet Service.
6. Subject to section 7, the User may, through the Millenet Service, withdraw the consent granted to the Bank and referred to in section 1 and may file an objection against the consents expressed to the Providers with immediate effect. Withdrawal of the consent and filing the objection means that every instruction received from the Provider after withdrawal of the consent or filing the objection, will be rejected by the Bank.
7. In case of the Payment transaction initiation service with current date, the User cannot cancel transaction after the Provider has been given consent for its initiation.
8. Every time, before execution of the instruction the Bank verifies whether the Provider holds proper authorisations defined in the Act.
9. In order to execute a one-off Payment transaction initiation service and one-off account information access service, the Bank presents the User a summary of the information submitted by the Provider information about the consents granted by the User and parameters of the requested service. Execution of the service is approved with use of Authorisation Tools available in Millenet Service, and in accordance with § 11 section 1.
10. In case of multiple account information access service, upon receiving such order, the Bank, before the first execution of the service, present the User a summary of the information about the consent granted, submitted by the Provider, and parameters of the requested service. Execution of the service may be approved with use of Authorisation Tools available in Millenet Service, and in accordance with § 11 section 1.
11. In case of the service of confirming availability of funds on Payment Account, the User grants the Bank a proper consent. Execution of the service is approved with use of Authorisation Tools available in Millenet Service, and in accordance with § 11 section 1.
12. The Bank may refuse to execute the Provider's service for justified causes related to suspected unauthorised action of the Provider.
13. The Bank informs the User about the refusal referred to in section 12 and its causes. The information, if possible, is communicated to the User before access refusal, however no later than on the business day following the day of such refusal, unless submission of the information is not advisable due to security reasons or is in breach of the law.
14. In case referred to in section 12, the Bank enables the Provider to provide the services immediately after discontinuation of the causes justifying the refusal.
15. Payment transaction initiation service is provided with the daily transaction limit set by the User.
16. The Bank does not collect any additional fees for the services initiated by the Providers, whereas Payment Orders are executed by the Bank in accordance with the principles defined in the General terms and conditions and the Price List.

Chapter V
Statements from the bank account
§ 22.

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 VI
Scope of the Bank's responsibility
§ 23.

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 § 25.

§ 24.

The Bank undertakes to observe banking secrecy as to any information obtained from the Client in connection with the

provided Millenet Service.

§ 25.

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 Authorisation tools and Authentication tools to unauthorised persons,
   7) making available Hedging 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) for the User's employing the Millenet Service from the browsers other than recommended by the Bank,
   4) for inadequate Client's computer security:
      a) no update of the operating system,
      b) no antivirus software,
   5) for disclosure of security instruments or authorisation tools to third party,
   6) for the damages caused by software not provided by the Bank,
   7) for lack of access to the Mobile Application resulting from inability to transfer data using this Application.

Chapter VII
Scope of the Client's Liability
§ 26.

The Client shall be liable for the effects of execution by the Bank of all the orders and instructions if they were executed as worded..

§ 27.

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

§ 28.

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 and the Authorisation tools in use.
3. The Client shall also promptly inform the Bank about any and all circumstances, in result of which his Hedging instruments, Authorisations tools and Authentication tools may have been used by unauthorised persons.

Chapter VIII
Millenet Service Fees and Commissions
§ 29.

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

Chapter IX
Procedure and conditions for resigning from the Millenet system
§ 30.

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. Termination of an agreement on provision of Millenet Service shall not cause loss of access to eBOK Millennium Leasing Service.
4. The procedure and conditions for resignation from the service of access to eBOK Millennium Leasing Service are stipulated in detail in eBOK Bylaws.
5. Resignation from access to eBOK Service does not mean termination of the Agreement on provision of Millenet Service.
6. The Millenet system agreement shall be terminated upon closing of the last current account in zloty, kept for the Client.

§ 31.

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, Access password, Authorisation tools or Authentication 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 X
Final provisions
§ 32.

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, 4 May 2020.