TERMS OF USE FOR THE R-ONLINE BIZNES INTERNET BANKING SYSTEM

Chapter 1
GENERAL PROVISIONS

Section 1

These Terms define the rules of providing Customer service by Raiffeisen Bank Polska S.A. via the R-Online Biznes Internet banking system and the Mobile Bank service for Corporate Customers.

Section 2

The terms used herein shall have the following meaning:

Account Terms The Terms of Opening and Maintaining Bank Accounts and Fixed-Term Deposit Accounts in Raiffeisen Bank Polska S.A. or the Terms of Bank Accounts, Fixed-Term Deposits and Debit Cards for Small Enterprises in Raiffeisen Bank Polska S.A., as referred to in the Agreement.

Agreement An agreement or a framework agreement regarding opening and maintenance of a bank account, including access and use of the System.

Authentication method SMS Password and/or electronic signature stored in the Cryptographic Device

Bank Raiffeisen Bank Polska S.A.

Cryptographic Devices Microprocessor smart card readers, microprocessor smart cards (provided optionally at the Customer's request) or USB tokens (a device connected, for the duration of the operations requiring a signature, including a Payment Order, directly to a USB port with an integrated microprocessor – functionally equivalent to a card and a reader in one device), used for authorizing the Customer's operations, including Payment Orders, for the Customers who have this authentication method in the System. Cryptographic devices are the sole storage medium for the Key for an Electronic Signature, approved for use by the Bank with the exception of situations individually agreed with the Customer. Storing the Key for Electronic Signature on a medium other than the Cryptographic Device bears the risk of operations, including Payment Orders and contractor particulars, being authorized by unauthorized persons for which the Customer bears full liability. Leaving the USB token in the port outside the time required to perform the operation causes the risk of operation authorization, including Payment Orders and recipient's information by persons not authorized by the Customer, for which the Customer shall be responsible.

Customer A customer indicated in the Terms and Conditions of Bank Accounts, having a bank account in the Bank.

Electronic Modification Orders Electronic orders regarding the entitlements and System configuration selected by the Customer, made in the System by the Users appointed by the Customer if such a service is provided by the Bank.

Electronic Signature A sequence of characters used for confirming the authenticity and integrity of a placed Payment Order as well as for verifying the identity of the User placing his or her signature.

Identification Verification of the User by the Bank by means of comparison with an identity document and listing its characteristic features, including full identification data such as first name, surname, address, personal identification number or date of birth for non-residents.

Identifier A sequence of characters specific for every Customer, ascribed by the Bank and used for logging in.

Internet Access Channels (IAC) IT access channels including: R-Online Biznes, described herein; R-Online, described in the Terms of Rendering Services by Raiffeisen Bank Polska S.A. via Electronic Access Channels for Personal Customers; R-Dealer, described in the Terms of Use for the R-Dealer Internet Trading Platform and the R-Dealer Mobile Functionality Available in the Mobile Bank for Personal Customers, or the Terms of Use for the R-Dealer Internet Trading Platform and the R-Dealer Mobile Functionality Available in the Mobile Bank for Friedrich Wilhelm Raiffeisen Private Banking Customers, enabling placing Orders or obtaining information about the account(s) or other Products and services available in particular channels via a web browser.

Key for Electronic Signature A key used together with the TPIN Code by the User to authorize all operations, including Payment Orders and contractor particulars. The User's private key.

Logging Password A sequence of characters established by the User, used for logging in to the System and the Mobile Bank.

Mobile Bank Mobile banking service enabling management of banking products made available by the Bank at a given moment with the use of a mobile device (e.g. a mobile telephone), servicing data transmission and equipped with the relevant software and operating system.

Notifications Service which makes it possible to receive notifications, including text messages concerning the use of the System.

One-time Password A sequence of characters established by the Bank, used for the first logging in to Internet Access Channels or logging in after unblocking.

Orders Written or telephone orders made by the Customer in conjunction with the access and use of the System. Written orders include:
- User Entitlement Form
- System Configuration Form
- Electronic System Configuration Form
- Appendix 1 / Annexe to the application for opening and maintaining a bank account for small enterprises in Raiffeisen Bank Polska S.A. or other regarding the R-Online Biznes system.

Payment Order A statement made by the User or recipient, ordering execution of a Payment Transaction.

Payment Order Authorization Confirmation of Payment Order placement by the User, i.e. consent for Payment Transaction execution in accordance with the provisions hereof.

Payment Services Act Act dated August 19, 2011 on Payment Services (Journal of Laws No. 199, item 1175, as amended) or any other substituting act and executive orders thereto.

Payment Transaction Payment, transfer or withdrawal of cash, initiated via the System, Internet Access

	Channels or the Mobile Bank by the User or recipient.
PIN Code	The User's personal identification number. A way of securing the Cryptographic Device.
Service	A service provided by the Service Technician within the scope of services offered to the Bank, covering Software installation and/or System training for the Customer.
Service Receipt Report	A document in which the Customer confirms System Service provision.
Service Technician	The Bank's employee, an employee working based on a mandate contract or an employee of a company cooperating with the Bank with regard to System implementation and the Service.
Software	Cryptographic device drivers, certificates and components provided by the Bank.
Start-up Password	A sequence of characters established by the Bank, used for the first logging in to Internet Access Channels or logging in after the unblocking of Internet Access Channels by the Bank.
Starter Pack	Identifier and Start-up Password used for the first logging in to the System or for logging in after unblocking the System by the Bank.
System	The R-Online Biznes Internet banking system. It is a set of cooperating IT devices and software, ensuring the storage, processing, sending and receipt through telecommunications connections of data constituting requests to provide banking services (including requests to provide information about the Customer's account and operations on this account) as well as the results of request management by the Bank.
System Consultant	Bank employee responsible for current support in the use of the System and technical support.
SMS Password	A unique string of characters set by the Bank to authorize operations, including Payment Orders and recipient's information, for the Customers who have this authentication method in the System, sent via a text message.
Table of Fees and Charges	The Table of Fees and Charges for Business Entities or the Table of Fees, Interest Rates and Charges for Small Enterprise Customers applied by the Bank, as referred to in the Agreement.
Terms	The Terms of Use of the R-Online Biznes Internet Banking System.
User	The Customer or an individual indicated by the Customer as the person authorized to use the System (including to execute Payment Transactions) and to collect Cryptographic Devices, order their installation and/or order trainings.
R-Connect	Service allows communication between financial accounting systems and Internet banking system R-Online Biznes, with the use of webservices.

Chapter 2
GENERAL TERMS AND CONDITIONS OF SYSTEM USE

Section 3

1. In order to be able to use the System, the Customer shall have one or more accounts in the Bank and shall satisfy the requirements included by the Bank on the https://moj.raiffeisenpolbank.com/wymagania-systemu website. The Bank shall render services connected with the System pursuant to the Agreement concluded with the Customer and Appendices thereto, according to the principles included therein as well as the principles included in these Terms.
2. Within the System, the Bank shall provide the Customer with the possibility to use selected services without affecting the Bank's right to change the scope of services and the scope of their use via the System.
3. The Mobile Bank service may be provided to every System User in accordance with the Orders. In order to be able to use the Mobile Bank service, the User shall activate the System. System entitlements shall be superior and transferable to the Mobile Bank service.
4. Within the System, the Bank shall provide the Customer with the possibility to use a Notification service. After each operation is performed in the System information about logging in and/or unsuccessful attempt to log in and/or blocking of access to the System and/or rejection of the order placed via the System and/or a transfer above a specific amount being sent shall be generated.

Section 4

1. The Customer shall be obliged to use the Software version recommended by the Bank and entered onto the reference list available on the Bank's website, in information resources and/or from the Bank's employees.
2. The Bank shall be obliged to provide the Customer with technical requirements without affecting the Bank's right to change these requirements through a relevant publication on the Bank's website, in information resources and/or by the Bank's employees.
3. The Customer shall follow the technical requirements and the rules of safe use of the System provided by the Bank.
4. The Customer shall be obliged to adjust his or her devices and Software to the requirements described in para. 2.
5. The Customer shall not be authorized to copy, waive, lend or release to third parties any parts of documentation and/or Software in any form without the Bank's prior written consent.
6. The Customer shall not be authorized to introduce any changes to documentation, Software and/or Cryptographic Devices and shall not amend, translate, decompile or interfere in them in any other manner. The Bank shall have exclusive rights to documentation, Software and Cryptographic Devices made available to the Customer.

Chapter 3
FEES AND CHARGES CONNECTED WITH SYSTEM PROVISION AND USE

Section 5

1. The Bank shall collect fees and charges in accordance with the Table of Fees and Charges applied by the Bank for the Service, usage, changes in the scope of System entitlements and configuration as well as operations executed via the System. The fees and charges shall be collected from the bank account indicated in the Agreement unless the parties agree otherwise.
2. The charge for using the System shall be collected for every commenced month of using the System, starting from the month following the month of signing the Agreement/Application.
3. The Customer shall be obliged to maintain a bank account balance adequate to cover the Bank's fees and charges in order to enable the Bank to execute its right to charge the bank account indicated by the Customer. In the case of a lack of funds on the indicated bank account, the Bank shall have the right to charge the indicated bank account also in

the event of insufficient funds (creating a debit) or to collect the fees and charges from other Customer's accounts held in the Bank.

4. The remaining fees and charges shall be collected by the Bank in accordance with the Agreement and/or other arrangements made by the Customer and the Bank.
5. For the Service outside the territory of the Republic of Poland, the Customer ordering the Bank to perform the Service shall be obliged to cover any additional costs incurred by the Bank immediately on the Bank's first request unless the parties agree otherwise in writing.
6. The Bank may demand reimbursement of all costs incurred in conjunction with its readiness and activities aimed at installing the Cryptographic Devices if installation fails due to reasons attributable to the Customer. The Customer shall be obliged to immediately reimburse all respective costs on the Bank's first request.
7. The Bank shall be the sole owner of the Cryptographic Devices made available to the Customer. The Customer shall be obliged to cover a one-time charge due to the use thereof (pursuant to the Table of Fees and Charges) and to return them on the Bank's request or on the date of terminating the Agreement or on the date of terminating a possible separate agreement for providing and using the System.
8. The Software and Cryptographic Devices made available by the Bank or acquired by the Customer himself or herself shall be maintained by the Customer at his or her own cost, whereby the Customer shall be liable for their proper use and storage.

Chapter 4
CONCLUSION OF THE AGREEMENT AND ORDER PLACEMENT

Section 6

1. The Customer shall be liable for specifying the scope of entitlements granted to particular Users through placing an Order in which the Customer indicates the accounts available in the System, the scope of entitlements and the individuals authorized to use the System.
2. The Customer shall authorize the Bank to obtain information necessary for taking a decision on signing the Order regarding changes to System configuration and entitlements.
3. Should the Customer fail to submit information necessary to execute the Order, the Bank reserves the right to refuse its execution.
4. The Bank shall be obliged to perform Identification of every System User with regard to whom the application for access or change of entitlements contains entitlements to make Payment Orders.
5. The Bank reserves the right to withhold an Order in the event of its incompleteness, ambiguous interpretation or non-performance of Identification with respect to a User entitled to make Payment Orders.
6. The Customer or the individual entitled by the Customer to use the System shall be able to make telephone Orders requesting the Starter Pack as well as training and cryptographic devices to be provided in accordance with section 7 para. 6. The User shall not be authorized to order the Starter Pack for another User.
7. The Bank shall be authorized to verify the Customer's identity or the identity of the individual indicated by the Customer based on the particulars included in the User Entitlement Form or the Electronic System Configuration Form, or Appendix 1 / Annexe to the application for opening and maintaining a bank account for small enterprises in Raiffeisen Bank Polska S.A.
8. All Orders in written form shall be signed by individuals authorized to make statements of will in the name of the Customer. Orders placed in a form other than a written form and approved by the Bank may be authorized in accordance with the Customer's prior written statement, signed by individuals authorized to make statements of will in the name of the Customer. All documents and Order forms shall be available for Customers on the Bank's website, in the Bank's registered office and/or from the Bank's employees.
9. The Bank reserves the right to amend the forms in order to present System functions currently offered to Customers.

Chapter 5
INSTALLATION OF CRYPTOGRAPHIC DEVICES, TRAINING AND SYSTEM MODIFICATIONS

Section 7

1. All activities within the Service shall be performed by the Customer subject to activities executed by the Service Technician pursuant to an Order made by the Customer and requesting the Bank to perform the Service.
2. The Bank may refuse the Service if:
   a) the Customer does not satisfy the requirements enlisted in the Terms and/or the document: System Requirements;
   b) there exist reasons preventing the Service in the Bank's opinion.
3. Should the Customer request the Bank to perform the Service, the Order shall be executed within 14 working days from the date of submitting the Agreement and the set of documents described in section 6 para. 1, correctly filled in and signed. The Bank shall not be liable for the failure to observe this term due to reasons not attributable to the Bank.
4. In the case of the Service ordered outside the Republic of Poland, the term indicated in section 7 para. 3 may be prolonged and the Bank shall inform the Customer thereof.
5. The term of performing the Service shall be agreed between the Customer and the Service Technician together with the technical and organizational conditions, confirmed by the Customer in the form of a signed confirmation of appointment (fax or electronic mail).
6. Prior to the established term of the Service, the Bank shall send at its own cost:
   - the Starter Pack to the mobile telephone number indicated in the User Entitlement Form or Appendix 1 / Annexe to the application for opening and maintaining a bank account for small enterprises in Raiffeisen Bank Polska S.A. in the form of a text message or to the mailing address of the Customer's User (indicated in the abovementioned forms) by conventional mail (registered priority mail) or by courier mail (at the Customer's cost), separately for every System User.
   - The Cryptographic Device shall be provided upon signing the Agreement by or for the Customer or sent by courier mail to the System User. The Customer or any other person authorized by the Customer shall be able to collect Cryptographic Devices in any of the Bank's Divisions based on a receipt protocol signed by or for the Customer.
7. The Service performed by the Service Technician may include:
   a) installation and configuration of Cryptographic Devices;
   b) general Customer training with regard to using the System;

   depending on the options declared by the Customer in a respective Order.
8. The Service shall be performed by the Service Technician on the computers indicated by the Customer and for indicated individuals.
9. The training with regard to the System shall be provided on a one-off basis for all requested Users by the Service Technician for the Customer.
10. Prior to commencing the Service on a specific computer stand, the User shall be obliged to make a spare copy of any

data stored thereon. The Bank shall not be liable for any possible data loss being the result of Cryptographic Device installation and the Customer waives the right to make any claims resulting therefrom.

11. In order to enable Service performance, the Customer shall be obliged to provide the Service Technician with access to devices listed in the document System Requirements as well as to the Customer's computer system administrator.
12. The Customer shall confirm Service performance and proper System functioning in the Service Receipt Report.

Section 8

1. The essential requirement for use the R-Connect service is having access to System.
2. The Bank ensure access to the R-Connect after duly completed and signed R-Connect Services Form.
3. Prices list for R-Connect is specified in the R-Connect Services Form.
4. Customer use the certificate authentication (in X.509 standard) required to sign an XML messages payments on its own and at their own expense.
5. Customer with access to Electronic Modyfications Orders in the System, can modify permissions and configuration for the R-Connect service.
6. Within the scope of R-Connect Services shall be applicable the provisions of System regulations.

Section 9

1. The scope of the User's entitlements in the System and the Mobile Bank service shall be established based on an appendix to the Agreement (Electronic System Configuration Form, System Configuration Form and/or User Entitlement Form or Appendix 1 / Annexe to the application for opening and maintaining a bank account for small enterprises in Raiffeisen Bank Polska S.A.) or the current Specimen Signature Card in accordance with the particulars included in these Orders.
2. The Customer may change the selected System entitlements and configuration:
   a) Individually via the System Users to whom the Customer granted the right to make Electronic Modification Orders. The Electronic Modification Orders shall become effective after their approval by the Users having the right to sign the Electronic Modification Orders.
   b) By making respective Orders in the Bank, containing the scope of changes, effective after their implementation by the Bank within 7 working days from the date of placing a given Order. The changes made in the System shall be reflected in the Mobile Bank service for all banking products serviced at a given moment within this service.
3. Amendments made by the Customer in the Specimen Signature Card shall not be transferred automatically to the System and shall be reported by the Customer in the form of a relevant Order.

Chapter 6
USE OF THE SYSTEM

Section 10

1. The Bank shall be entitled to provide information about the turnover and balance on the Customer's account and to execute all received Orders to the burden and to the benefit of the Customer's accounts via the System and the Mobile Bank Service if the Customer's request is confirmed by relevant passwords and User's entitlements in the System and/or the Mobile Bank service.
2. The Bank shall provide the Customer with electronic bank account statements with regard to the accounts indicated by the Customer in the Order unless technical reasons prevent the Bank from the provision thereof.
3. The Bank provides the Customer with SMS Passwords and sends them to authorize all operations, including Payment Orders and recipient's information, to the mobile phone number indicated in the User's Authorization Form or Appendix 1 / Annex to the Application for opening and maintaining an account for Small-sized Enterprises for the Customers who have this authentication method in the System.
4. The Bank provides the Customer with authentication methods that use SMS Passwords or Electronic Signature stored in the Cryptographic Device.
5. The Bank reserves the right to unilaterally request from the Customer a confirmation of Payment Orders and other operations made through the System by using the Electronic Signature and SMS Password, of which the Customer shall be notified via the System.
6. The Bank advises the Customer to use the System on a computer intended solely for this purpose, taking into account the rules described in § 18 par. 3

Section 11

1. Entering the System and the Mobile Bank service as well as using its functions requires the correct, unique User's Identifier and interrelated Logging Password. For the Mobile Bank service, the Identifier shall be entered only upon installation or reinstallation of the service on a mobile device.
2. The Start-up Passwords for the Users shall be delivered within the Starter Packs sent in accordance with section 7 para. 6.
3. Upon the first use of the System, the User, having successfully submitted the Starter Pack received in the form of a text message enter the One-time Password (the second text message from the Bank) as well as the User's date of birth, and then shall be obliged to change his or her Start-up Password from the Starter Pack to his or her own Logging Password.
4. The activation of a User who received the Start-up Password by conventional mail (registered priority mail or courier mail) shall be performed through calling the Bank, answering the System Consultant's verifying questions and changing the Start-up Password to the User's own Logging Password.
5. While initiating the Mobile Bank service, the User enters the Logging Password established for the Internet Access Channels and his or her date of birth, and then he or she shall set a Password to log in to the Mobile Bank . In the case of providing the User with access to a subsequent Internet Access Channel, the User shall receive a text message informing about the need to log in with the use of an already possessed Identifier and Logging Password.
6. Every User shall create the Key for Electronic Signature with the possibility to ask for technical assistance of the System Consultant. The User shall be obliged to store the Cryptographic Device and the PIN Code thereto in a secure location as well as not to disclose them to third parties and to insert the Cryptographic Device in the USB port only for the time needed to authorize the operation and to remove the Cryptographic Device from the USB port after all operations had been authorized, including Payment Orders and contractor particulars.
7. The Key for Electronic Signature in the System shall be activated automatically by the System User at the moment of its creation.

Section 12

1. In the case of three unsuccessful attempts to enter the Logging Password to the System, the User shall be automatically blocked, which prevents him or her from further use of the System. The User shall be able to make

three additional attempts to log in on the www.raiffeisenpolbank.com website and to unblock the Internet Access Channels upon successful logging in. Having made six incorrect logging attempts, the User shall be completely blocked and a new Starter Pack shall be provided.

2. The blocking of the Internet Access Channels shall not result in blocking the Mobile Bank service.
3. In the event of blocking access to the System as described in para. 1, the Customer may request unblocking and sending of a new Starter Pack through:
   a) placing a telephone Order via the System Consultant, after positive verification of the identity of the User making the Order;
   b) placing a written Order signed by individuals authorized to make statements of will in the name of the Customer.
4. The use of the Starter Pack shall lead to reactivation as described in section 10 para. 1 to 5.
5. The Bank shall have the right to immediately block the User's access to the System pursuant to:
   a) a telephone Order placed by the User to be blocked after positive verification of the User's identity;
   b) a telephone Order regarding blocking of another User, placed by any of the Customer's Users, after verification of identity. Unblocking shall require a written Order placed by the Customer and the generation of a new Starter Pack;
   c) a written Order to block the Customer's User or Users, signed by individuals authorized to make statements of will in the name of the Customer.
6. In the case of legitimate doubts as to the use of the System by authorized individuals only, the Bank may block these Users whom such doubts concern.
7. The blocking of access to the System, mentioned in section 11 para. 6, shall be valid for the User with regard to all the Customers in whose name the User acts.
8. Written or telephone Orders described herein shall be admitted within the Bank's working hours.

Section 13

1. In the case of any problems with using the System or the Mobile Bank service, the Customer shall contact the System Consultant.
2. Within the current assistance regarding the use of the System mentioned in para. 1, the Bank shall be obliged to provide the Customer with technical support consisting of the provision of advisory information concerning the functioning and proper use of the System. The telephone number and working hours of the System Consultants shall be published by the Bank on its website, in information resources and/or by the Bank's employees.
7. Technical support shall be limited to the System made available to the Customer. It shall not cover the System's working environment, i.e. computer hardware and installed software as well as electronic/Internet banking software installed and made available by other banks.
8. Should the Customer fail to ensure proper IT personnel when receiving telephone support, the Bank shall not be liable for any possible damage resulting therefrom. The IT personnel shall be responsible for supervising the process of System implementation and the Service. The Bank shall make every effort to prevent the aforesaid damage, ensuring Customer service by highly qualified technical personnel.

Chapter 7
PAYMENT ORDERS – TYPES AND TERMS OF PLACEMENT AND EXECUTION

Section 14

1. The Bank shall receive Order Payments placed by the Users via the System or the Mobile Bank service (if the Bank offers such a service) in the 24-hour cycle subject to intervals necessary to perform technical service of the System.
2. The Payment Orders placed in the Bank via the System (including: accounts, scope of entitlements and the Users indicated in the Orders) shall be treated by the Bank and the Customer with equal force as the Payment Orders placed in writing and signed in accordance with the Specimen Signature Card, submitted to the Bank.
3. The Payment Orders placed in the Bank via the System or the Mobile Bank service (if the Bank offers such a service) shall be treated by the parties to the agreement as a special form of legal activity. The parties shall recognize their effectiveness and shall give their consent to take evidence in order to prove the execution thereof.

Section 15

1. The Payment Orders which have been properly prepared and placed in the Bank shall be deemed accepted and subject to execution within the term declared by the Customer, taking into account the order processing time established by the Bank and communicated to the Customer in a manner proper for bank accounts serviced by the System or the Mobile Bank service. The aforesaid regards Payment Orders placed with a current or future execution date.
2. The Bank shall verify whether the received Payment Order is complete and correct as well as whether the funds collected on a given bank account enable the execution of the Payment Order. Those Payment Orders containing an error preventing their execution or not covered by an account balance shall not be executed.
3. The Bank shall not be liable for the execution of Payment Orders regardless of their incompleteness or erroneousness.

Section 16

1. The User's Payment Orders made in the System or the Mobile Bank service shall be identified by the Bank with the use of the User's Identifier, the Logging Password and the Electronic Signature and/or SMS Password.
2. The Customer or other Users shall be obliged to place Payment Orders via the System or the Mobile Bank service in accordance with the binding legal regulations, the System and Mobile Bank functions offered by the Bank, the recommendations of the Bank's employees and the binding terms and conditions established by the Bank.
3. The Bank reserves the right to perform telephone verification of a Payment Order prior to its execution.
4. The User shall be obliged to check on a regular basis the correct execution of Payment Orders placed in the Bank via the System and to immediately inform the Bank about any irregularities.
5. Every Payment Order placed and authorized in the System or the Mobile Bank service shall become irrevocable. The Bank's consent shall be necessary to cancel a Payment Order. The Bank may collect a charge determined in the Table of Fees and Charges (if such a charge exists) for any activities connected with cancelling a Payment Order.

Chapter 8
LIABILITY PRINCIPLES

Section 17

1. The Customer shall be the sole administrator of the Software and Cryptographic Devices. The Bank shall not be responsible for any results of activities performed by unauthorized individuals.
2. The Bank shall be the System Administrator. The first System Entitlements for the Customer shall be granted based on

written Orders delivered to the Bank and signed by individuals authorized to make statements of will in the name of the Customer. The System Entitlements may be modified in accordance with section 8 para. 2.

3. The Customer shall be fully liable for the Payment Orders placed by the Users. The Customer shall be fully liable for the Payment Orders executed in instances described in para. 4, even if such Orders are not authorized by the Users.
4. The Bank shall not be liable for the results of:
   a) disclosing or enabling third parties by the Customer to:
      - use the System,
      - use the Mobile Bank service,
      - acquire Identifiers (log ins), Logging Passwords, Starter Packs, Cryptographic Devices and the Key for Electronic Signature, answers to the User's verifying questions, documentation and/or Software and/or SMS Password;
   b) using the Keys for Electronic Signature without the dedicated Cryptographic Devices offered by the Bank;
   c) Payment Orders made in the System by persons not authorized by the Customer, as a result of leaving the USB token in the port.
   d) non-observance by the Customer (intentionally or unintentionally) of due diligence principles, obligations listed in Art. 42 of the Act on Payment Services or obligations included herein or in the Account Terms, including for the use of the System via a computer or another electronic device on which there is an active software breaching the System's security;
   e) damaging the Software and Cryptographic Devices as a result of their use contradictory to these Terms and/or the Bank's recommendations;
   f) lack of telecommunications connection between the Customer and the Bank, preventing the use of the System or the Mobile Bank service unless such lack of communication is caused by sole intentional fault of the Bank or by the Bank's gross negligence;
   g) an incorrect Payment Order placed by the Customer (any and all corrections of erroneous Payment Orders shall be settled directly by the Customer and the beneficiary);
   h) improper System or Mobile Bank service implementation, performed by the Customer;
   i) force majeure, including but not limited to strikes, natural disasters, riots, and acts of war;
   j) a decision taken by public authorities, a statutory act or an executive order to an act;
   k) intervals in the functioning of the Bank's IT systems, resulting from the need to perform necessary activities connected with their proper functioning, improvement, maintenance, data supply or security.
5. In the event of a System failure, the Bank shall act with due diligence to immediately remove it.
6. The Bank shall be liable only up to the actual amount of the Customer's financial loss.
7. The Terms of Considering Complaints in RBPL describe the procedure of filing and considering complaints. The terms are available in the Bank's Divisions and on the Bank's website.
8. Should the Customer submit a claim regarding the use of the System, the Bank shall have the right to inspect the Customer's operating environment and to secure data stored in this environment. The operating environment shall mean a virtual image used for contact with the Bank or in the lack of such an image a computer together with the attached disks.
9. Any claims of the Customer against the Bank due to unauthorized, unexecuted or improperly executed Payment Transactions shall expire after six months from the date of charging the account or from the date on which a given Payment Transaction should have been executed if the Customer fails to inform the Bank about such an event.

Section 18

1. The Customer shall be liable for any damage caused by:
   a) improper storage and use of the Identifiers (log ins), Logging Passwords, Starter Packs, Cryptographic Devices and the Key for Electronic Signature (including failure to remove the Cryptographic Device from the USB port after the transaction had been performed), answers to the User's verifying questions, documentation and/or Software;
   b) acquisition and use of passwords by unauthorized third parties, copying or releasing by the Customer (through granting usufruct, lease, resale or in other manner) of the Identifiers (log ins), Logging Passwords, Starter Packs, Cryptographic Devices with the Key for Electronic Signature, answers to the User's verifying questions, documentation and/or Software and/or SMS Password;
   c) incorrect or incomplete recording of data provided by the Customer;
   d) turning off the text message service turned on by the Bank notifying about a log in to the electronic banking system.
2. In the event of any damage to the Software and Cryptographic Devices for reasons attributable to the Customer, the Bank may request reimbursement of actual repair costs and shall be entitled to collect relevant charges in accordance with the Table of Fees and Charges.
3. The Customer shall be obliged to acquaint himself or herself with the security policy and security information displayed on the System's login page as well as published by the Bank on its website and in information resources on a regular basis.
4. The Customer shall be obliged to immediately pay damages to the Bank in conjunction with any costs, loss or expenses incurred by the Bank as well as with any claims lodged against the Bank due to the Customer's irregularities.
5. The parties shall not be liable for the results of force majeure or the activities of public authorities.

Chapter 9
FINAL PROVISIONS

Section 19

1. Except for the instances enlisted in section 14, the Bank may withhold the execution of Payment Orders in instances described in the Account Terms as well as in the case of legitimate doubts as to the use of the System by authorized individuals only.
2. The Bank shall be obliged to immediately inform the Customer about withholding and reasons for withholding operations via the System.
3. The Customer shall waive any claims with respect to the Bank due to withholding the Customer's Payment Orders in accordance with the provisions hereof.

Section 20

1. The Bank reserves the right to amend these Terms.
2. Any amendments to the Terms introduced during the term of the Agreement shall require the delivery of amended provisions to the Customer.
3. The delivery referred to in paragraph 2 may be executed also via the System.
4. Should the Customer lodge a written statement on non-acceptance of the amended provisions hereof within 14 days from receiving the above information, the Agreement shall be terminated after one month from the date of information delivery or earlier by mutual agreement of the parties.
5. In the event of lack of any statement on non-acceptance of the amended provisions hereof within the term determined in

para. 4, the amendments shall be deemed accepted by the Customer and binding for the parties.

6. The termination of the Agreement shall be subject to relevant provisions of the Account Terms.
7. The Bank reserves the right to withdraw in writing from the Agreement regarding an inactive User who has not logged into the system with the use of ID and Password for at least 6 months.
8. The withdrawal by the Bank referred to in section 7 shall be made in writing and sent by the Bank by registered letter to the correspondence address recently given by the Client to the Bank, and in case the letter is returned or if the correspondence address is the Bank's Branch Office – also to the address of the Client's headquarters, and shall come into force after 30 days from the date of issue by the Bank. The Client must inform the User(s) of the authorization to access the System being revoked.
9. On the date these Rules become effective, the Bank enables Users – via Internet access channels and the Mobile Bank service – access to information subject to banking secrecy, execution of Payment Transactions, and execution of Orders and Electronic Modification Orders referred to in § 9 clause 2 with respect to Banking Product agreements made with the Bank, as well as those made with Polbank EFG. S.A., to which the Bank is a legal successor.

Section 21

1. Subject to paragraph 2, to all matters not settled in the Agreement appropriate provisions of the Polish law and the Account Terms shall apply.
2. The parties exclude in whole the application of the following regulations:
   a) part 2 of the Act on Payment Services;
   b) Art. 34-37, Art. 45, Art. 46 para. 2-5 and Art. 47-48 of the Act on Payment Services;
   c) chapter 4 part 3 of the Act on Payment Services (excluding Art. 59) to Payment Transactions not included in Art. 53 para. 1 of the Act on Payment Services. In the case of Payment Transactions executed in the territory of one or more member states (within the meaning of the Act on Payment Services), the term mentioned in Art. 54 para. 1 of the Act on Payment Services shall not exceed 4 working days from the receipt of the Payment Order by the Bank.

Section 22

The Agreement shall be executed in the Polish language unless the parties agree otherwise.

Valid from , 21st July 2017