SPECIAL CONDITIONS FOR USAGE OF ELECTRONIC/MOBILE BANKING FOR COMPANIES

I. GENERAL PROVISIONS

1. The rights and obligations of the e-banking Users shall be governed by way of these Special Conditions for usage of electronic/mobile banking for companies (hereinafter referred to as: the Special Conditions), CUT-OFF Time Plan For Payment Accounts For Companies, the Tariff for general banking services for Corporative clients, Tariff for general banking services for SME clients (hereinafter referred to as: the Tariffs for general banking services), which are integral parts of the User Framework Contract.
2. E-banking/mobile banking system use is a service provided by the Bank to its Clients only, i.e. to the companies holding an account with the Bank, which includes e-banking/mobile banking services.
3. The information in respect of the offer of Electronic Channel products and the services that the User may provide by using certain e-banking products is available at the Bank's sub-branches and on its webpage www.unicreditbank.rs
4. For each contracted e-banking/mobile banking product, the Bank will enable the User to have access to all necessary information in respect of using the selected product as well as use all services stated in the Product Use Contract and these Special Conditions.
5. By filing the Application, the Client acknowledges to be conversant and agrees with the provisions of these Special Conditions, accepting them in full.
6. The User shall be responsible for all information necessary for proper and secure operation of the agreed e-banking/mobile banking product furnished to the Bank, and is obliged to notify the Bank of any change thereof (e.g. phone number, mobile phone number and model, e-mail address, etc.).
7. To be able to use certain e-banking/mobile banking products, the User must ensure appropriate computer infrastructure (for mobile banking appropriate mobile device). Technical requirements for using certain products are available on the Bank's webpage www.unicreditbank.rs and/or at the Bank's business network. The User is obliged, subject to the technical requirements of individual e-banking products, to notify the Bank of the type of equipment the User uses in order to ensure proper operation of the product.
8. These Special Conditions shall govern the conditions for and manners of using the Bank's electronic payment instruments, and the rights, obligations and responsibilities for their contracting and using of companies (hereinafter referred to as: the Users), private individuals authorised to use electronic payment instruments on behalf of companies (hereinafter referred to as: the End-Users) and the Bank.
9. The information that the Bank forwards to the User or End-User of an e-banking product shall have the same value as the documents sent by mail by the Bank and may replace them.

GLOSSARY

Certain terms used herein shall have the following meanings:

1. **User** a business entity, corporation that contracts with the Bank usage of some of the electronic banking/mobile banking products;
2. **End-User (Authorisee)** is a private individual authorised by the User for using a particular e-banking/mobile banking product for and on behalf of the User;
3. **Username** is a unique set of alphanumeric characters constituting one of the elements by which the End-User is identified in the registration process for an e-banking/mBanking service;
4. **Signatory** is the End-User who owns the device storing the electronic authorisation, and acts for the User based on the granted authorities;
5. User Manual is a written document, describing the registration process and the use of e-banking/mobile banking products for the User and/or End-User..

6. Unlock Code/Password is a code/password used to unlock smartcards or USB Flash Drives in the event when a smartcard or USB Flash Drive is locked due to successive entries of a wrong PIN; In case of a locked token it is necessary for the Client to comply with the procedures for sending the locked token PIN to the Bank, the Bank to comply with the procedures for sending the unlock PIN to the Client in order to unlock the token.
7. **Encryption** is a process transforming information into a format readable only by the intended recipient.
8. **Decryption** is a process by which the recipient makes the encrypted information readable.
9. **Electronic Channels** are means and forms of electronic communication enabling use and/or contracting certain banking and non-banking services without any simultaneous physical presence of the End-User and the Bank's employee in the same place, and they include a network of services made available by the Bank to the User: online banking (BusinessNet Professional), E-banking (Multicash, Halcom, Office Banking, European gate, mobile banking), SWIFT Net, as well as connection through other Electronic Channels made available by the Bank to the User;
10. **Smartcard and USB Flash Drive** are certified cryptographic devices for secure electronic certificate storage;
11. **Certificate** is a set of data in electronic form which is attached to or logically associated with an electronic document serving for the e-banking service user identification;
12. **Electronic Signature** is a set of data in electronic form, which is attached to or logically associated with an electronic document serving for the signer identification;
13. **Qualified Electronic Signature** is an electronic signature reliably guaranteeing the signer's identity and electronic document integrity and disabling any subsequent denial of responsibility for the contents thereof, and which meets the conditions stipulated in the Electronic Signature Act;
14. **Activation code** – array of letters and numbers that bank delivers to customers in order to activate mobile application or mobile token. Activation code is unique code, for ome time use, and its use is limited by time.
15. **QR code (Quick Response)** - standardised two-dimensional label which represents a two-dimensional barcode based on the ISO 18004.

II. TYPE AND SCOPE OF SERVICES, SECURITY SYSTEM

1. Bank provides the Users with the following type of electronic/mobile banking:

- Global Web Solution (**hereinafter referred to as GWS**)- online electronic banking system (**BusinessNet Professional)**
- HAL e-bank system for electronic banking (hereinafter: **HAL e-bank**)
- MultiCash system for electronic banking (hereinafter: **MultiCash**)
- European gate
- SWIFT MT940/942
- Mobile banking – system for electronic banking via mobile device (hereinafter:**mBiznis**) for companies

2. **BusinessNet Professional** is an online e-banking application and a product of Unicredit Bank. This application uses the one-time password token mechanism to access the system and sign orders. To provide the Clients with a high information security level, BUSINESSNET PROFESSIONAL uses three levels of protection: personal identification, one-time password token identification and SSL encryption.

2.1. **Token** is an electronic device received on initiating the use of the BusinessNet Professional e-banking tool. The User will be asked their personal identification by entering their PIN code, and a one-time password will generate based on the PIN code (a four-digit combination of numbers created by the User at their own discretion for the purpose of signing in in future), token serial number and its unique key. Generation algorithm with the bank server is the trade secret. Token authentication is another protection layer, in the place, which is focus of few companies.

2.2. **Mobile token** (hereinafter:mToken) within mBiznis application that can be installed on mobile device, there is possibility of using software token – application that after entering PIN code generates one time password which identifies User of direct channel. During activation of Mobile token application, the user is going to be asked for personal identification as well as activated code after which the User will be enabled

to create its own PIN code. In this way, the application allows users to use mobile device/tablet as token. End user uses mToken for authentication and signing of payment orders in BusinessNet Proffesional

2.3. **SSL PROTOCOL** is a 128-bit key Encryption as the industry standard in secure online communications. It is used by 99% of major web presentations such as banks, companies dealing in online investments, stock-exchange transactions or commerce.

2.4. **Username** is a unique set of alphanumeric characters constituting one of the elements by which the End-User is identified in the registration process for the BusinessNet Professional service; The Client shall be asked only to be personally identified (username) and to prove their identity (token), thereafter the system access is allowed.

2.5. **BusinessNet Professional** International user is a user who has access to accounts of several Unicredit Group Bank Members using the BusinessNet Professional e-banking product. That is how the Client is enabled to use one token for transactions with all accounts opened at Unicredit Group Bank Members.

3. **HAL e-Bank** is a software product of Halcom Informatika d.d. Ljubljana, named HAL e-bank. In addition to standard HALCOM e-bank application releases, UniCredit Bank Srbija a.d. offers the variations thereof: Corporate E-bank, Personal E-bank, B2B; Hal-Ebank B2B enables connection between the Client's Information System and the Bank's Information System without user intervention, automatically at certain time intervals as specified. To ensure secure e-banking with the Bank, HAL e-bank has introduced two types of security instruments as follows:

3.1. HALCOM certificate embedded in the smartcard or USB key is an electronic, identification instrument enabling the End-User to work with the User's current accounts opened at the Bank. The End-User rights to the User's current accounts needs to be specified in the E-Banking Application. Use of a digital certificate disables false personation i.e. ensures a reliable authentication of the End-User.A Qualified Electronic Certificate is an electronic certificate issued by a certification authority in charge of issuing qualified electronic certificates (HALCOM in this case) containing statutory required information. Qualified Electronic Certificates confirm the link between the User's public cryptographic key and the End-User's identity who has signed the electronic document. The Qualified Electronic Certificates and related private cryptographic keys are used for a qualified electronic signature of files or messages and the user authentication. A Qualified Electronic Signature is an electronic signature which meets statutory requirements and which reliably guarantees the signer's identity, electronic document integrity and disables any subsequent denial of responsibility for the contents thereof. The User shall accept the digital certificate as the exclusive verification of their identity when using the HAL e-bank services, without the right to subsequent denial based on the approved Application and the Application for End-User Digital Certificate, the Smartcards are handed to the Client by Halcom AD Beograd, at the premises of Halcom AD Beograd or by courier. Exceptionally, the Client may take over a smartcard in the bank's premises, only if it is not the qualified certificate in question. Smartcards are issued with the defined validity of a digital certificate, and following the expiry thereof, the validity thereof must be renewed. When issuing a new card, the User shall authorize the End-User to work with their accounts by sending a new Application.In the event of revoking-cancelling the rights of use of a smartcard of certain End-Users, it is necessary that the Bank be furnished with the written Application for cancelling the certificate and use of the HAL e-bank service for the specific End-User.

3.2. WEB Username enables the User to access the WEB HAL e-bank system (hereinafter referred to as: WEB e-banking). This system is an upgrade of HAL e-bank and serves for the End-User access via web browsers. WEB e-b@nking End-Users with authorities to sign orders may remotely sign orders using web browsers, WEB username and related password, smartcard and smartcard reader. The End-Users with the right to access WEB e-b@nking authorized to view the statement may follow the turnover and statement of the company accounts by using only a web browser, username and password. WEB Username enables the End-User to access accounts based on the authorities

stated in the User's initial Application via the WEB HAL e-bank application.Based on the approved Application requesting issuance of a WEB Username for a specific End-User, the Bank shall hand over the WEB Username and WEB password to the End-User, i.e. the person

authorized therefor by the User. The handover of the WEB Username and WEB password shall take place at the Bank's premises.In the event of revoking-cancelling the right of use of the WEB Username for the End-User, the User needs to furnish the Bank with the signed Application for revoking-cancelling the right of use of the WEB Username.In the event of revoking-cancelling the right of use of a smartcard for an End-User, the right of use of the WEB Username shall be automatically terminated if issued to the person in question. The Application for revoking-cancelling the right of use needs to be furnished to the Bank in writing.

4. **MultiCash** system for e-banking is e-banking software produced by Omikron Systemhouse, Cologne, Germany. To ensure secure e-banking MultiCash use following security instruments:

   4.1. **BPD file** is a security mechanism in the form of a file stored on a specific data carrier, which in combination with the Electronic Signature enables the End-User to work with the User current accounts opened at the Bank. The End-User rights to the User's current accounts are specified in the Application. The BPD file and Electronic Signature disables false personation, i.e. ensures the reliable End-User authentication.

   4.2. **Electronic Signature (ES key pair)** is a security mechanism in the form of a file stored on a specific data carrier. Electronic Signature i.e. ES key pair is created by the User in their MultiCash application. By using BPD file and the communication code and following creation of the ES key pair, the User is obliged to set up the initial connection to the Bank's server and send the information in respect of their public key of the ES key pair generated.The private key of the ES key pair is secured with a secret password entered by the End-User while generating the ES key pair. The password for the ES key pair is known only to the End-User who is the owner of the ES key pairs for signing. On initial connection, the MultiCash application prints out a document containing a printout of the User's public key (User Initialisation Script) which needs to be signed by the End-User and furnished to the Bank in order for the End-User's Electronic Signature to be approved for use in the MultiCash system. The User shall accept the BPD file and ES key pair as an exclusive confirmation of their identity when using the MultiCash e-banking system services, without the right of subsequent denial.Following approval of the Application, the Bank shall issue the BPD file to the End-User, i.e. the person authorized therefor by the User.If the User wishes to revoke (cancel) the right of use of the MultiCash system for a specific End-User, it is necessary that they submit the written Application for cancelling the use of the MultiCash e-banking system services for that person, thereafter the Bank will cancel the rights to the MultiCash system. MultiCash system, technically allows User to administrate rights to other End Users which are not determen with Request for E-banking activation. Local users administration is fully explained in Users manual. Responsibility for the proper administration of these End Users is entirely at the User. The Bank bears no responsibility in the event of erroneous setting of these local End users orders as well as for the possible misuse of rights that are granted locally

5. **European gate**, a product by Unicredit Group enabling the Users to access all UniCredit banks (presently in 19 countries) through a single access point. This order routing and conversion platform enables processing of various national formats of payment orders as well as the international formats such as SAP Idoc, UN/EDIFACT or S.W.I.F.T Messages (e.g. MT101).

6. **SWIFT MT940/942** messages enabling the statement of accounts and interim turnover of accounts sending / receiving via SWIFT network.

7. **Mobile banking (mBiznis)** represents electronic communication between the User and the Bank via an application that is installed on a mobile phone or tablet, which enables him/her quick and efficient implementation of banking services without having obligation to go to Bank's branch UniCredit mobile

banking applications are predict measures to ensure secure electronic business with the Bank, such as the creation of a PIN code by the User (which is thus known only to him), the necessity of entering personal identification and activation code, while activating applications and creatingits PIN code. The application is copy-protected and protected from instaling it on other phones, as the link and activation code for installing applications can be used only once (once). It is not possible to install the same application, which is linked to the same account on two different mobile devices.

By downloading mBusiness application for mobile banking, software token is installed as well that guarantees complete work safety. The activation code represents a special identification number, which serves for activation the service and after that is not usable for further usage.

The following services are available through M Banking (mBiznis) application:

- executing of payment orders in domestic payment system
- internal transfer within personal accounts
- inquiry into the balance of the account, in real time
- request for payment at the point of sale
- availability overview of the list of exchange rates
- account balance and transactions on all accounts (including loans)
- account balance for debit and credit cards (data, transactions),
- conversion of foreign currencies into dinars at the Bank's buying exchange rate,
- receiving useful information (information on current offers, various notifications)
- setup the application (change of PIN code, language, font, etc.)
- as well as any additional services that the Bank will develop within the mobile banking application, about which customers will be informed via agreed channels of communication

8. **E-statement** is service of UniCredit that provides receipt of statements and other forms of information related to business relation between customer and the Bank by using pre-agreed mail address of the customer.

In terms of payment services by using chosen E-banking system User can perform payments, currency conversion, review the reports or other services depend of product capabilities, by contracting usage of the service with the Bank. The agreed scope of services related to the specified service can be subsequently changed with the use of already existing security instruments.

III. CONTRACTING OF USE, OBLIGATIONS AND RESPONSIBILITIES OF CONTRACTING PARTIES.

The condition for entering into the Contract is that the User opens a current account at the Bank to be able to use some of the e-banking payment instrument products. The User may agree the use of one or several e-banking products. To agree individual e-banking products, the User is obliged to furnish the Bank with the correctly filled in and signed Application relevant for contracting the direct channel. By certifying the Application for contracting an e-banking product the User acknowledges to be conversant with the General Business Conditions and other rules applicable therewith, and compliant with the application thereof. By submitting

(signing) the Application, the Applicant/User acknowledges to be conversant and compliant with all the provisions of these SC for usage of electronic banking, accepting them in full, as well as the General Business Conditions, which jointly have the power of a contract.

The User must designate one or several End-Users, who will use the agreed e-banking product on behalf of the User. Various types of authorities may be selected for a specific End-User. Any selection, change and revocation of End-User authorities shall be based on furnishing the correctly filled in Applications for a single or several e-banking products, submitted to the Bank by the User as stipulated for each e-banking product. The Bank is authorized to refuse entering into the Contract without any explanation. If the Client fails to perform the obligations contained herein, which they accepted by signing the Application, the Bank shall reserve the right to unilaterally terminate provision of the e-banking system services by way of the Notice. The User may cancel further use of the e-banking system in writing only. All debits accrued prior to the day of cancelling the use of the e-banking system, periodical costs related to the period when the cancellation occurred, as well as costs and interests, if any, arising from debit shall be incurred by the Client.

1. BusinessNet Professional

Contracting Of Use

The User shall be enabled to use BusinessNet Professional following submission of the signed E-Banking Request, opting for this type of service, legibly filled in and signed by an authorized signer. By way of this Request, the User shall authorize certain private individuals to work in BUSINESSNET PROFESSIONAL, define account access, and state the type of authorities for the persons by account. The User shall accept the full responsibility for the accuracy of entered information. Bank introduces the User how to access to BusinessNet Proffesional application via Personal identification and PIN code. User selects personal identification and enters into the Request.

Obligations and Responsibilities of Contracting Parties

The User undertakes, while working with the BUSINESSNET PROFESSIONAL system, to fully comply with the applicable laws and instructions for use for this software product.

The User is obliged to keep and shall cause the End-User to safeguard the token and keep the PIN code confidential in order to prevent them from coming in possession of other party. From time to time or if the End-User suspects or finds that a party has learned of their PIN, it is recommendable that the PIN be changed. It may be changed at any time as described in the Instructions for Use.

The User shall incur the full damage due to any loss, unauthorized or inadequate use of the token.

The User shall be responsible for the accuracy of all information furnished to the Bank and is obliged to report any change therein. If the Bank independently learns that the End-User information is inaccurate or changed, it may cancel further use of the BUSINESSNET PROFESSIONAL services, with a subsequent notice to the User.

The User is obliged, on the computers, which they will use to approach Business Net, to provide a licensed, properly configured operating system. If the Client, following the initial use of uses BusinessNet Proffesional on the non-licensed computer, non-configured or untested applications, the Bank shall not be responsible for any failure in execution of orders or other consequences, if any.

The User is required to provide the appropriate mobile device that is able to support the mBusiness and mToken application, if he/she wants to arrange this service. If User does not provide a suitable mobile device, he/she will not be able to use the service, and all the responsibility and all the costs bears alone.

The User cannot use Token – hardware device and mToken at the same time. In accordance with the specified, he/she must choose one of these two options in Request. If the User uses Token – hardware device, and wants to use mToken and fulfil conditions from the previous paragraph. He/she is obliged to return Token – hardware device to the Bank or to pay fee in the case of the lost Token – hardware device.

2. HAL e-bank

Contracting Of Use

To activate the HAL e-bank service, the User shall furnish the Bank with the following documents filled in and signed:

i. Request for E-Banking, opting for this type of service, by way of which the User authorizes certain private individuals – End-Users, defines account access, and states the type of authorities for the persons by account.
ii. General Order Form for issuing qualified personal digital certificates for a company
iii. Copy of the User's identity card i.e. the statement that the End-User's personal information furnished by the User is accurate

Based on the approved Request for E-banking and General order form. Halcom AD in their premises or via mail service will deliver smart cards. Bank can only deliver plain digital certificates, not qualified.

Based on approved Request for E-Banking for WEB user name for certain End User, Bank will deliver WEB user name and password to End User or to other person authorized by User.

Obligations and Responsibilities of Contracting Parties

The User undertakes, while working with the HAL e-bank system, to fully comply with the applicable laws and instructions for use for this software product.

The User is obliged to safeguard and shall cause the End-User to safeguard smartcards as well as keep the PIN confidential in order to prevent them from coming in possession of other party. If the End-User suspects or finds that a party has learned of their PIN it may be changed at any time as described in the Instructions for Use.

The User is obliged to safeguard the PUK code, capable of unblocking a smartcard and entering a new PIN code if it is blocked following three unsuccessful entries of the PIN code. In the event of loss of the PUK code, the blocked card is impossible to unlock and a new one needs to be issued. The Bank shall not be responsible therefor.

The User shall incur the full damage due to any loss, unauthorized or inadequate use of the card.

The Client shall be responsible for the accuracy of all information furnished to the Bank and is obliged to report any change therein. If the Bank independently learns that the End-User information is inaccurate or changed, it may cancel further use of the HAL e-bank services, with a subsequent notice to the Client.

Any copying of the Digital Certificate is prohibited. The Client shall incur any damage due to copying or attempted copying.

The User is obliged, on the computers where they will use the HAL e-bank services, properly configured operating system (minimum Windows 7 and up in case of the single user version of HAL e-bank). If the Client, following the initial use of the HAL e-bank services, uses on the same computer any non-licenced, non-configured or untested applications, the Bank shall not be responsible for any failure in execution of orders or other consequences, if any..

Users who have ordered the installation and training for HAL e-bank at their business premises following receipt of the Bank's notice that conditions have been created for the installation of the HAL e-bank system are obliged within 15 days to arrange the software installation by phone or by email to: e-banking@unicreditgroup.rs or by calling the technical support on: (+381 11) 3028 624. The Users, who have the HAL e-bank package for independent installation, after receipt of the Bank's notice, are obliged within 30 days of the notice to take over the HAL e-bank package at a UniCredit Bank's sub-branch.

If the User abandons the use of the HAL e-bank / MultiCash system service prior to the completed implementation of the system itself, following the notice by the Bank that the technical conditions have created for implementation of some of the electronic services, as described in detail in the wording hereof, the Bank may charge the User the penalty agreed in accordance with the Tariff for general banking services for Corporative clients. The Bank is entitled to retain the assets it collected at the time of filing the Application.

3. MultiCash

Contracting Of Use

To activate this e-banking service, the User is obliged to furnish the Bank with the following documents filled in and signed:

i. Request for E-Banking, by way of which the Client opts for this type of e-banking service and lists the persons authorized for working therein, as well as the accounts they will access.

ii. Copy of the User's identity card i.e. the statement that the End-User's personal information furnished by the User is accurate

Obligations and Responsibilities of Contracting Parties

The User undertakes, while working with the MultiCash e-banking system, to fully comply with the applicable laws and instructions for use for this software product.

The User is obliged to safeguard and shall cause the End-User to safeguard the Electronic Signature and the Electronic Signature password as well as the password to access the MultiCash application and the password for communication with the Bank to prevent them from coming in possession of other party. If the User suspects or finds that a party has learned of one of the foregoing passwords, it may be changed at any time as described in the instructions for use of the MultiCash software.

The User shall incur all the damage due to any loss, unauthorized or inadequate use of security instruments: the BPD file and Electronic Signature..

The User is obliged, while using the MultiCash services, to comply with the Rules and abide by the User Instructions, which is an integral part of the MultiCash programme.

The User shall be responsible for the accuracy of all information furnished to the Bank and is obliged to report any change therein. If the Bank independently learns that the End-User information is inaccurate or changed, it may cancel further use of the MultiCash services, with a subsequent notice to the User..

Any copying of the Electronic Signature and BPD file is prohibited. Any damage due to copying or attempted copying shall be incurred by the Client.

The User needs to provide on the computers where it will use the MultiCash services a licensed, properly configured operating system (minimum Windows 2000 Service pack III). If the User, following the initial use of the MultiCash services, uses on the same computer any non-licensed, non-configured or untested applications, the Bank shall not be responsible for any failure in execution of orders or other consequences, if any..

The Users who have ordered the installation and training for MultiCash at their business premises following receipt of the Bank's notice that conditions have been created for the installation of the MultiCash system are obliged within 15 days to arrange the software installation by phone or by email to: e-banking@unicreditgroup.rs or by calling the technical support on: (+381 11) 3028 624.

If the User abandons the use of the HAL e-bank / MultiCash system service prior to the completed implementation of the system itself, following the notice by the Bank that the technical conditions have created for implementation of some of the electronic services, as described in detail in the wording hereof, the Bank may charge the User the penalty agreed in accordance with the Tariff for general banking services for Corporative clients. The Bank is entitled to retain the assets it collected at the time of filing the Application.

4. MT 940, MT101

Contracting Of Use

To activate this e-banking service, the User is obliged to furnish the Bank with the filled in and signed Authorisation to Execute MT Messages. The User, an international client, may also activate this service directly through Bank Austria by signing the document entitled Unique Service Level Agreement For MT101 only.

The Bank is authorized to refuse completion of MT Messages if with the required SWIFT user from whose SWIFT address MT message is initiated cannot be approved by the RMA (Relationship Management Application).

The User-related information, stated in the Application for contracting e-banking products as last received by the Bank, shall be deemed accurate and applied to all other Contracts previously entered into by the User with the Bank in respect of use of the selected product.

5. Mobile banking

Contracting Of Use

The User is enabled to use BusinessNet Professional following submission of the signed E-Banking Request, opting for this type of service, legibly filled in and signed by an authorized signer. By way of this Request, the User shall authorize certain private individuals to work in MBiznis, define account access, and state the type of authorities for the persons by account. The User is accepting the full responsibility for the accuracy of entered information.

Obligations and Responsibilities of Contracting Parties

The User undertakes to fully comply with the applicable laws and instructions for use for this software product while working with the mBiznis system.

The User is obliged to keep and shall cause the End-User to keep the PIN code confidential in order to prevent them from coming in possession of other party. From time to time or if the End-User suspects or finds that a party has learned of their PIN, it is recommendable to change the PIN. PIN can be change at any time as described in the Instructions for Use.

The User shall incur the full damage due to any loss, unauthorized or inadequate use of the mtoken or mBiznis application.

The User shall be responsible for the accuracy of all information furnished to the Bank and is obliged to report any change therein. If the Bank independently learns that the End-User information is inaccurate or changed, it may cancel further use of the mBiznis services, with a subsequent notice to the User.

The User is required to provide the appropriate mobile device that is able to support the mBusiness and mToken application, if he/she wants to arrange this service. If User does not provide a suitable mobile device, he/she will not be able to use the service, and all the responsibility and all the costs bears alone.

Bank’s responsibility

The Bank will process the Application, in accordance with all the applicable contracts and rules entered into by the User with the Bank or accepted by the User, as well as in accordance with all applicable regulation.

The Bank is obliged to make computer-based records of all User's actions. Computer-based records are retained in accordance with applicable laws.

The Bank shall reserve the right to change the content or part of the content of the BUSINESSNET PROFESSIONAL / HAL e-bank / MultiCash/mBiznis system available to the User, without a prior notice. The Bank to the User will communicate any change of the content or part of the content of BUSINESSNET PROFESSIONAL / HAL e-bank / MultiCash/mBiznis and the instructions will be delivered accordingly.

The Bank shall not be accountable for any interferences in telecommunications and tele- transmission services offered by third parties, or any errors or damage arisen therefrom.

The Bank is obliged to furnish the User with the Instructions for Use of BUSINESSNET PROFESSIONAL/ HAL e-bank and MultiCash system.

6. E statement service

The User gets the ability to use E-statement service by submitting an appropriate Request, and which defines the email address to which the Bank will carry out account statements and other information regarding the business relationship between the User and the Bank.

IV. EXECUTION OF PAYMENT TRANSACTIONS

1. Any payment transactions for the execution of which the consent has been given in one of the foregoing ways is authorized and deemed the indisputable proof of the User identity. The fact that the Bank has recorded, as the use of a payment instrument, the use of identification and verification instruments accessed to by a personalized security instrument shall be sufficient to prove that the User, i.e. End-User has authorized the payment transaction in question, whereby the User assumes the responsibility for the executed transaction in question.
2. The Bank will, upon receiving a payment order, via the same channel the order has been received, deliver to the User a message of successful receipt of the order. The message of successful receipt of a payment order shall not imply that the order will be executed, but only that it has been received by the Bank.
3. The Bank shall execute correct payment orders within timelines set out in the General Business Conditions and the Cut-off time plan for payment accounts, applicable at the time of executing the payment transaction.
4. The payment orders sent to the Bank by any of the electronic payment instruments before the execution value date may be cancelled by the User and/or End-User until the execution date set out in the then applicable Cut-off time plan for payment accounts. The payment orders may be cancelled by using the same channel enabling filing and cancelling a payment order, as well as in writing at the Bank's sub-branches in accordance with the General Conditions for providing payment services.
5. Bank may refuse order execution in accordance with the General Conditions for providing payment services.
6. The Bank shall not be responsible for any failed execution of a payment transaction or improper execution thereof by electronic instruments, occurring due to incorrectly entered information in the User's i.e. End-User's order.

V. EXECUTION OF INSTANT PAYMENT TRANSFER AT POINT OF SALE

1. The Bank offers to its customers with whom it has contracted the use of the Mobile Banking service, the possibility of executing domestic payment transactions at the point of sale by using instant transfer . Payers have two ways of initiation of instant transfers:
    a) by presenting payers data through QR code
    b) by downloading data about the merchant from the code
2. The Bank shall, immediately after receiving the authorized instant transfer order, execute it in the shortest possible time if the conditions for execution of the order are fulfilled within the available funds on the account.
3. The Bank shall, immediately after the execution of instant transfer order, provide via a mobile banking message information on the amount and currency of the executed payment request, as well as the reference mark identifying the payment transaction at the point of sale. The Bank shall inform the Payers in the same way in case of refusal of instant transfer.
4. It is not possible to recall instant transfer payment based on the Request for payment at the point of sale. Users have possibility to initiate a refund request based on payment at the point of sale. Upon receipt of the Refund Request from the point of sale at the point of sale, the Bank shall proceed to the execution of all necessary checks whether the payment request at the point of sale has been properly executed. If, based on the

preformed checks, it has been established that there is a basis for repayment, the Bank shall initiate a request for a refund to the account of the beneficiary.

VI. DISABLING E-BANKING ACCESS, LOSS AND BLOCKADE OF SECURITY

1. Any loss, theft, suspicion of abuse, or abuse of identification and verification instruments, certificates stored on an identification and verification instrument, or personalised security features, knowledge or suspicion that an unauthorized party has learned of a personalised security feature, knowledge or suspicion that an unauthorised party has accessed an agreed channel must be forthwith reported by the User or End-User to the Bank, requesting that the e-banking access be blocked. The Bank shall act accordingly on the User report and the End-User report alike.
2. The report of loss or theft of an identification and verification instrument where the certificate is stored shall be the basis to revoke the certificate. The Bank is obliged to revoke the certificate upon receipt of the report.
3. The Bank will, even without any User's or End-User's report, automatically disable access to an e-banking product if the personalised security feature has been successively entered unsuccessfully as many times as stated in the User Manual for individual products.
4. The Bank is authorised, without any User's or End-User's report, to disable access to certain or all e-banking products in the following instances:
   i. in case of suspicion of unauthorised use or abuse of identification and verification instruments or personalised security features
   ii. if an e-banking product is being used for fraud or abuse.
5. The Bank shall notify the User and End-User beforehand of an intended blocking of access and/or inability to use a particular e-banking service, as well as of the reasons therefor, unless giving such notice is contrary to objectively justifiable security reasons, or against the law. The Bank is not obliged to notify the User and End-User beforehand of blocking the e-banking access in the event of unsuccessful entry of the personalised security feature, or expiry of the certificate stored on the End-User's identification instrument. The notice of inability to use e-banking products or a particular service available through E-banking shall be sent by the Bank to the User and End-User by any other means available.
6. All the payment orders received by the Bank prior to revocation of the certificate or blocking of an e-banking product access will be executed.
7. The Bank may, upon giving a notice no later than 24 hours beforehand, disable the use of agreed e-banking products in the event of changes and upgrades to the Bank's information system, including its information security system, or in the event of changes and upgrades to e-banking products. The notice of a temporary inability to use e-banking products shall be sent by the Bank to the User and End-User through the same e-banking product, by publishing it on the Bank's webpage or by other means available.

BusinessNet Professional/mBusiness

The Client/User is obliged to report any loss or theft of the token immediately to the Bank on (+381 11) 3028 624 or by e-mail on: gws@unicreditgroup.rs

Based on the received notice of the token loss or theft, any further use of the token for disposing of assets in the accounts held with the Bank will be disabled upon receipt of the notice during the working hours of the Technical Support, namely Monday-Friday, 09.00h - 17.00h. In addition, the User is obliged within 2 business days to notify i.e. confirm to the Bank, the token loss or theft. The permanently blocked token may not be unblocked, and the User shall incur the costs of re-issuance of the token. The User will incur consequences of abuse, if any, of the lost or stolen token.

HAL e-bank system

The Client/User is obliged to report any loss or theft of the smartcard immediately to the Bank on (+381 11) 3028 624 or by e-mail to: e-banking@unicreditgroup.rs. Based on the received notice of the card loss or theft, any further use of the smartcard for disposing of assets in the accounts held with the Bank will be disabled upon receipt of the notice during the working hours of the Technical Support, namely Monday-Friday, 09.00h - 17.00h. In addition, the User is obliged within 2 business days to notify i.e. confirm to the Bank, in writing, the card loss or theft. The permanently blocked card may not be unblocked, and the User shall incur the costs of re-issuance of the card. The User will incur consequences of abuse, if any, of the lost or stolen card. If the User blocks the smartcard, unblocking is possible if the User has information on the PUK and PIN codes, which they were handed together with the smartcard for the HAL e-bank use and the User shall incur any costs arisen therefrom.

The Bank shall order a card on the written request of the User's authorised person to Halcom AD Beograd.

VII. SAFEGUARDING OF PERSONAL AND CONFIDENTIAL INFORMATION

The Bank shall keep confidential all information, facts and circumstances of individual Users at its disposal. The User agrees that all information furnished to the Bank or learned by the Bank during entering and performing the Contract may be processed and used by the Bank to create a client base, prevent money laundering and terrorist financing, search and detect payment operations frauds, resolve complaints and make entries into documentation, which occurs with a view to exercising the rights and performing the obligations under the Contract. The Bank is obliged to treat the foregoing information in accordance with its legal obligation to keep confidential any information it has learned while doing business with the User, ensuring the confidential treatment thereof and the full protection of the banking secret by all parties who will be allowed access to protected information, as well as the use thereof for legal purposes, in no manner that could be deemed contrary to reasonably assumed interests of the contracting parties.

VIII. FINAL PROVISIONS

The Client agrees that the Bank is entitled to change the Special Conditions, fees and costs of the use of the GWS / HAL e-bank / MultiCash e-banking, without the Client's explicit consent. The Bank is obliged to furnish the Client with proposed amendments in writing no later than two months prior to the proposed effective date thereof. The Client may agree that the proposed amendments produce legal effect prior to the proposed effective date. It shall be deemed that the Client has agreed to the proposed amendments if, before the effective date, the Client has not notified the Bank in writing that they disagree with the proposal. If the Client disagrees with the proposed amendments, they are entitled, prior to the effective date thereof, to terminate the Framework Contract free of charge.

If the Client fails to perform the obligations contained herein, which they accepted by signing the Application, the Bank shall reserve the right to unilaterally terminate provision of the e-banking system services by way of the Notice.

In the event of a dispute, the Commercial Court in Belgrade shall have jurisdiction.
These Special Conditions for usage of electronic banking shall have the character of a legally binding document.
The provisions of these Special Conditions shall enter into force upon date of its adoption by the Board of Directors, and shall apply from 1st of February 2020.

Supervisory board of UniCredit Bank Srbija JSC Belgrade