GENERAL BUSINESS CONDITIONS FOR ELECTRONIC BANKING SERVICES

EFFECTIVE AS OF 25th October, 2021

PREAMBULUM

These General Business Conditions are applicable to the electronic banking services that customers may use to access their bank accounts held with Citibank Europe plc Hungarian Branch Office.

1. Definitions

Unless otherwise expressly provided in these General Business Conditions for Electronic Banking Services (hereinafter EB Conditions), the expressions bellow shall have the following meanings:

Bank:	Citibank Europe plc Hungarian Branch Office acting on behalf of Citibank Europe plc;
Customer:	any legal entity or any other entity that has concluded an agreement with the Bank for the use of any Instrument and accepted these EB Conditions as binding;
EB HelpDesk:	the Bank's customer service established to facilitate software usage and help to solve possible software defects, available on +36 1 374 5518 phone number from 8.00 a.m. to 5.00 p.m. on working days and from 8.00 a.m. to 2.00 p.m. on Saturday working days;
User:	any adult having full legal capacity authorized on the required form valid at all times to execute the transactions described in Appendix 1. Section 3 and Appendix 2. Section 3., or use the service defined in Appendix 3. Section 2. of the EB Conditions in the name and on behalf of the Customer;
Services:	the electronic banking services available through the Instruments;
Account:	all payment accounts of the Customer kept with the Bank;
Citi:	the Bank and its affiliates;
CitiService:	the Bank's customer service established to offer customized, high-quality banking services to Corporate Clients. CitiService is available at +36 1 374 5000 phone number from 8.00 a.m. to 5.00 p.m. on working days and from 8.00 a.m. to 2.00 p.m. on Saturday working days.
CCB Customer Service:	the Bank's customer service established to offer customized, high-quality banking services to Commercial Banking Customers, available at + 36 1 288 8880 phone number from 8.00 a.m. to 5.00 p.m. from Mondays to Thursdays, from 8.00 a.m. to 4.00 p.m. on Fridays and from 8.00 a.m. to 2.00 p.m. on Saturday working days.

Remote Access Payment Instrument (Instrument):	integrity of hardware, software and processes (excluding bank cards) that enables the Customer to access the Services.

Authentication Methods

The Procedures include certain secure authentication methods ("Authentication Methods") which are used to uniquely identify and verify the authority of the Customer and/or any of its users authorized by the Customer typically through one or a combination of mechanisms such as user ID / password pairs, digital certificates, biometrics, security tokens (deployed via hardware or software) and/or devices associated with the Authentication Methods (collectively, the "Credentials"). Authentication Methods and associated Credentials allow the Bank to verify the origin of Communications received by the Bank.

The following Authentication Methods are available to access the services or connectivity channels:

Token: Challenge Response	Either (i) a mobile application based soft token (e.g. MobilePASS) or (ii) a physical token (e.g. SafeWord Card, Vasco), which in each case is used to generate a dynamic password after authenticating with a PIN (e.g. 4-digit PIN). When accessing CitiDirect BE, the system generates a challenge and a response passcode is generated by the utilized token and entered into the system.
Token: One Time Password	Either (i) a mobile application based soft token (e.g. MobilePASS); or (ii) a physical token (e.g. SafeWord Card, Vasco) that is used to generate a dynamic password after authenticating with a PIN (e.g. 4-digit PIN). This dynamic password is entered into the system to gain access.
SMS One-Time-Code	A dynamic password delivered to users via SMS, after which the user enters the dynamic password and a secure password to gain access to the system.
Voice One-Time-Code	A dynamic password delivered to users via an automated voice call, after which the user enters the dynamic password and a secure password to gain access to the system.
Digital Certificates	A digital certificate issued by an approved certificate authority that is used for authentication. Digital Certificates utilize a key storage mechanism and a corresponding PIN, and may be issued by IdenTrust, SWIFT (3SKey) or other agreed-upon providers. Digital Certificates may be attributed to individual users ("Personal Certificates") or to corporate legal entities ("Corporate Seals") for authentication purposes. Where connectivity channels support Communications using Corporate Seals, the Customer is responsible for properly verifying the identity of all individual Customer representatives acting on the Account on behalf of the Customer in accordance with local law.

	Any Communications received by the Bank via a public Internet connection (including but not limited to HTTPS, secure FTP or FTPS) or otherwise unsecure Internet connection, will require the Bank and the Customer to exchange approved digital certificates to ensure that both the connectivity channel and the messages exchanged are fully encrypted and protected.
Secure Password	A user enters his or her secure password to access the system. A secure password typically limits a user's capabilities on the system, for example, by only permitting that certain information be viewed by the user.
Biometrics Authentication	A digital authentication method that utilizes a user's unique physical traits, (such as a fingerprint and facial recognition), built-in biometric technology on the user's mobile device, and cryptographic techniques to gain access to CitiDirect BE. Physical trait data is not transferred to the Bank when the user selects this authentication method.
PIN for IVR (Interactive Voice Response)	Customers contacting the Bank via phone or email are prompted to enter a PIN or provide other information to validate authorized access.
MTLS	Mandatory Transport Layer Security (MTLS) creates what would be a secure, private email connection between the Bank and the Customer. Emails transmitted using this channel are sent over the Internet through an encrypted TLS tunnel created by the connection.
Secure PDF	Encrypted emails are delivered to a regular mailbox as PDF documents that are opened by entering a private password. Both the message body and any attached files are encrypted. A private password can be set up upon receipt of the first secure email received.
IP Address Whitelist When Using CitiConnect	Certain Internet communications received by the Bank, for example, via a Virtual Private Network (VPN), may also rely on the parties exchanging information using pre-agreed Internet Protocol (IP) addresses. The Bank will only accept communications originating from the Customer's designated IP address, and vice versa; and the Bank will only transmit Communications to the Customer's designated IP address, and vice versa.
SWIFT	Communications sent between the Bank and the Customer via the SWIFT network, including, but not limited to, account information, payment orders, and instructions to amend or cancel such orders, will be authenticated using procedures defined in SWIFT's Contractual Documentation (as amended or supplemented from time to time) which includes without limitation its General Terms and Conditions and FIN Service Description or as set forth in other terms and conditions that may be established by SWIFT. The Bank is not obliged to do anything other than what is contained in the SWIFT procedures to establish the sender and authenticity of these Communications.

The Bank is not responsible for any errors or delays in the SWIFT system. The Customer is responsible for providing Communications to the Bank in the format and type required and specified by SWIFT. Transmissions and Communications sent or received via SWIFT facilities are subject to SWIFT rules and regulations in effect, including membership rules. The Customer is responsible for being familiar with and conforming to SWIFT messaging standards.

To learn more about these Authentication Methods, refer to the Login Help page on CitiDirect BE at: (https://portal.citidirect.com/portalservices/forms/loginHelp.pser)

2. Remote Access Payment Instruments

Appendix of these EB Conditions defines the description and the technical requirements of the Remote Access Payment Instruments and the Services available through each type of Instrument.

Depending on the type of the Remote Access Payment Instrument the Customer uses, the Bank may require the use of SafeWord cards or MobilePASS by the Users. The conditions of the use of SafeWord cards and MobilePASS are stipulated in the Appendix 1 of these EB Conditions.

3. Responsibilities of the Customer and the User for protecting the Instrument from unauthorized access

The Customer and the User are obliged to take all necessary actions to prevent any unauthorized persons from accessing such software, hardware (with special regard but not limited to the SafeWord card or the Instrument operating the MobilePASS application), identification codes and IT systems associated with the use of the Instruments and operated by in the possession of the Customer and/or the User. The Customer is required to hold regular internal audits in order to determine whether the measures applied to protect the Instruments are sufficient or require development.

4. Reporting obligation of the Customer and the User

The User and the Customer shall promptly notify the Digital Client Support team of the Bank if they find or suspect that in the course of using the Services, unauthorized third parties may have gain/gained access to the Instrument or any related software, hardware (with special regard to the SafeWord card or the Instrument operating the MobilePASS application), identification codes or IT systems. The disablement requests can be reported by dialing + 36 1 374 5518 via phone on Monday-Friday between 8:30 – 17:00, on Saturdays business working days between 8:30 – 14:00 or in any other cases in written to DCS.Hungary@citi.com email address.
The reporting person via phone shall provide his/her personal identification details, the names of the Customer and the User and the place and time and the description of the event-giving rise to the reporting. If the reporting person is not aware of the exact location or time of the event, he/she has to report the assumed place and time. The reporting must be considered as an order for blocking the Instrument. The Bank shall notify the Customer without any delay if cooperation is required from the Customer for the disabling of the SafeWord card or the MobilePASS response code. In the case of a written application, the intention of blocking Safeword card and/or MobilePass must be indicated in the subject field.

5. Liability

5.1. The Customer shall be liable for the losses occurred due to fraud on the part of the Customer or the User or due to the willful or gross negligent breach of the obligations by the Customer or the User stipulated in Clauses 3 and 4 of these EB Conditions.

5.2. The Bank shall be liable for any losses occurred by the Customer due to unauthorized access following reporting pursuant to Paragraph 4 above.

5.3. The Customer accepts that any transaction executed by the Users shall qualify as an authorized transaction by the Customer.

5.4 Unless mandatory law provides otherwise, Customer is sole responsible for all consequences arising from the availability of MobilePASS application security features to third parties and assumes all risks deriving from such disclosure. The User is required to change the MobilePASS application password if suspects that unauthorized persons have been aware of it.

6. Blocking

The Bank reserves the right to block the SafeWord Card or the MobilePASS response code generation in case of suspicion on the unauthorized or fraudulent use of the Instrument or in order to protect the safety of the Instrument.

7. User rights

7.1. Any documentation, information, hardware, software and other instruments given to the Customer in relation to these EB Conditions constitute the Bank's sole property. The Customer possesses no right except non-exclusive user rights.

7.2 Any documentation, information, hardware, software related to the Instruments shall constitute the Bank's business secrets and may only be disclosed to third parties in any way if the Bank gives its prior written consent, in which consent the Bank shall also stipulate the exact range of the information that may be so disclosed.

8. Termination

8.1. Either party may, at any time terminate the use of any or all Instruments in writing with a 60-day notice period without giving any reason. The Customer's access to Instrument affected by the termination shall cease on the last day of the notice period.

8.2. Either party may terminate the use of any or all Instruments with immediate effect in writing if the other party commits a gross breach of these EB Conditions. The Bank is entitled to terminate the agreement on the use of any or all Instruments with immediate effect, especially but not limited to if:

(a) the Customer or the User does not fulfill any of his /her responsibilities stipulated in these EB Conditions;

(b) the Customer's financial or other circumstances considered being significant by the Bank in connection with these EB Conditions change disadvantageously;

(c) the Customer provides false information in respect of these EB Conditions;

(d) the SafeWord card is being used after blocking or outside the scope of validity or function; or

(e) the Customer or the User violates the rules concerning the use of the Instrument.

8.3. The Bank may suspend the use of the Instrument in the event of serious breach of these EB Conditions.

8.4. The use of software, hardware, codes and systems provided by the Bank in connection with the use of the Instrument after the effectiveness of the termination is prohibited.

9. Assignment, partial invalidity

9.1. The Customer may not assign any of its rights and may not transfer any of its obligations (hereinafter: Assignment) under these EB Conditions without the prior written approval of the Bank. The Bank may assign any of its rights and may transfer any of its obligations without the prior written approval of the Customer. Based on the Assignment the assignee will obtain the Bank's rights and obligations and the Bank will be free from any such obligations.

9.2. Should any part of the present EB Conditions be invalid or unenforceable, it shall not affect the validity and enforceability of the remainder of the present EB Conditions.

10. Fees and charges

The fees and charges applicable to the Services are included in the Part I. of the Bank's valid Commercial and/or Corporate List of Conditions / Pricing and Fee Schedules

11. General Business Conditions

In matters not dealt with in these EB Conditions, the Bank's General Business Conditions of Corporate Services shall apply.

Appendix 1
CitiDirect BE

1. CitiDirect electronic banking service

CitiDirect BE is a web-based electronic banking framework service, accessible through the internet. Available CitiDirect applications:

a) CitiDirect BE Desktop (including enhanced file upload possibility) means the CitiDirect BE electronic banking service provided by the Bank for the Client, available at https://portal.citidirect.com, through which the Client may communicate electronically with the Bank within its respective authorizations.

b) CitiDirect BE Mobile means the CitiDirect BE electronic banking service provided by the Bank for the Client, available at https://m.citidirect.com, optimized for access via mobile telephones or similar devices, through which the Client may communicate electronically with the Bank within its respective authorizations, whereas this service does not have to include all functionalities of the CitiDirect BE service.

c) CitiDirect BE App means application for supported mobile devices such as cell phones, provided by the Bank for the Client, and through which the Client may access to the electronic banking service CitiDirect BE and communicate electronically with the Bank within its respective authorizations, whereas this service does not have to include all functionalities of the CitiDirect BE service.

Besides the technical requirements stipulated in the next paragraph, SafeWord card or MobilePASS activation code is required for the access of CitiDirect. The Bank provides a SafeWord card or MobilePASS activation code to each User of the Customer.

A detailed description of usage of CitiDirect can be found in the CitiDirect Online Help, which is an online help function built in the CitiDirect software with search function to enhance software usage.

2. Technical requirements

Minimum technical requirements needed to use CitiDirect services can be found on the https://www.citidirect.com website.

Should the above-mentioned technical requirements change, the Bank will notify the Customer 30 days prior to such change. The Customer shall promptly meet the modified minimum requirements for CitiDirect usage. If the Customer does not fulfill the above requirements, the Bank is not responsible for any losses arising from the above.

3. Services available through CitiDirect

The following services are available for the Customer via CitiDirect:

a) may access information regarding the Account, may inquire balances, access information on transactions processed on the Account;

b) may download and save the list of all incoming and outgoing transactions effected on the Account;

c) may initiate payments within and out of Hungary in HUF or in foreign currency;

d) may give instruction for group transfers, prompt collection orders, direct debit orders;

e) may make deposit;

f) may provide information not constituting payment order, or may send letters to the Bank;

g) may initiate payments by way of a postal voucher;

h) may initiate GIRO transaction related EBUK Customs electronic message sending;

i) may receive the information defined in points a) and b) above in an encrypted e-mail.

In order to access the Service defined under i) the Customer's e-mail system must include any of the encrypting profiles supported by CitiDirect. The https://www.citidirect.com website contains the list of encrypting software supported by CitiDirect. The Bank does not accept any responsibility or liability for any of the encrypting profiles, mainly for their proper functioning. The Customer is directly responsible and liable for meeting copyright obligations in connection with and for any payable fees for the encrypting profiles.

4. PIN Code

For the use of services of CitiDirect the Bank shall make available a SafeWord card and a PIN code or MobilePASS activation code upon Customer decision for the Users of the Customer of which dynamic password is generated to access all the Services described in Paragraph 3 above. The Customer and the Users have to keep the PIN and MobilePASS activation code in secret.

The Bank is entitled to apply further login security conditions for the access of services or any specific functions on top of the PIN code and password generated by the MobilePASS activation code.

5. SafeWord Card and MobilePASS

The SafeWord card constitutes the Bank's property, is not transferable, may not be delivered to the possession of third parties, may not be tied up as security or lien, may not be deposited, may not be handed over to third parties.

The Customer is entitled to request the SafeWord Card to be delivered in inactive status. The condition to activate SafeWord card delivered in inactive status is that Customer provides a duly signed confirmation including the SafeWord card serial number on the receipt of the SafeWord card and relating PIN code in original. In case the Customer requests the delivery of the SafeWord Card in active status and by the receipt of the SafeWord card by any person at the postal address requested by Customer, all risks related to the receipt of the SafeWord card lies on the Customer.

The Customer shall be directly liable for ensuring that the Users are familiar with the rules of using and safekeeping of the SafeWord card and MobilePASS activation code, as well as with the rules of liability related thereto. The Customer shall have joint and several liabilities with the User for any losses, which are sustained by the Bank through the violation of these EB Conditions by the User.

The Customer shall be directly liable for the security and operation of the MobilePASS application.

The Bank is entitled to register any information generated by the use of SafeWord card and use it as proof in case of any dispute. The Bank provides detailed information on the user conditions of MobilePASS application at https://portal.citidirect.com.

6. Usage of CitiDirect

Based on the Customer's request the Bank provides access to its system enabling the Customer to use CitiDirect with the properly filled in and duly signed request form valid for all times by submitting to the Bank. The condition of using CitiDirect that the Bank has identified all the Users in accordance with the legal regulations in force at all times regarding the prevention of money laundering and both the Customer and the Users have provided all required information and gave all required declarations in connection with the above.

The Customer must provide all required information and give all declarations in connection with the identification to perform as per the legal regulations in force at all times on the prevention of money laundering.

The Bank shall be entitled to alter, suspend or terminate the CitiDirect services or the Customer's or the User's right to use the CitiDirect services at any time only for technical or security reasons, simultaneously notifying the Customer of the above. The Bank shall notify the Customer of any such circumstance by phone or at the next log-in to CitiDirect. The Bank shall not be liable for any damages or losses sustained by the Customer through the alteration, suspension or termination in question.

Appendix 2
File-based Payment Services

1. Description of File-based Payment Services

File-based payment Services are Instruments, using which the Customer sends its encrypted payment file through CitiDirect in the format supported by the Bank from its proprietary treasury system onto Citi's destination server using one of the connection methods supported by Citi (e.g. FTP, HTTPS, CitiConnect, CitiDirect). Citi processes the payment instructions automatically.

The encryption and identification methods used for File-based Payment Services are based on the Public Key Infrastructure (PKI).

The Bank excludes its liability for the damages resulting from the break, restructuring or any other modification of the files prior the acceptance of the Bank's system.

The Bank shall process the transactions received via File-based Payment Services according to the cut-off times.

The File-based Payment Services Agreements concluded with other Citi entities are not subject to these EB Conditions for Electronic Banking Services. The Bank excludes its liability for such agreements regarding the processing, charging and any conditions including cut-off times and any processing requests, complaints and claims thereof.

2. Technical requirements

The technical (software and hardware) requirements of File-based Payments Services depend on the actual solution Citi offers to the Customers. The Customer side technical specifications and requirements of File-based Payments Services solution are agreed between the Customer and Citi during the implantation and testing period. During the implementation and testing period, Citi provides the information necessary to use the File-based Payment Services to the Customer.

3. List of available File-based Payment Services

With the use of the CitiDirect File-based Payment Services the Customer:

(a) may initiate payments within and out of Hungary in HUF or in foreign currency

(b) may give instruction for group transfers, prompt collection orders, direct debit or postal voucher orders in HUF within Hungary.

4. Usage of File-based Payment Services

The condition of using CitiDirect that the Bank has identified all the Users in accordance with the legal regulations in force at all times regarding the prevention of money laundering and both the Customer and the Users have provided all required information and gave all required declarations in connection with the above.

The Customer must provide all required information and give all declarations in connection with the identification to perform as per the legal regulations in force at all times on the prevention of money laundering.

The Bank shall be entitled to alter, suspend or terminate the CitiDirect services or the Customer's or the User's right to use the CitiDirect services at any time only for technical or security reasons, simultaneously notifying the Customer of the above. The Bank shall not be liable for any damages or losses sustained by the Customer through the alteration, suspension or termination in question.