Security Procedures
Процедуры безопасности

1. Introduction
Introduction

These "Security Procedures", as referenced in the Communications section of the Master Account and Service Terms ("MAST") (or other applicable account terms and conditions), are designed to authenticate the Customer's log-on to the Bank's connectivity channels and to verify the origination of Communications between Bank and Customer in connection with the following Services or connectivity channels (the availability of which may vary across local markets).

Данные «процедуры безопасности», как они обозначена в разделе Коммуникация Условий обслуживания Основного Счета (Master Account and Service Terms) (или других применимых условий и положений), разработаны для аутентификации пользователей Клиента в каналах связи с Банком и для подтверждения источника запросов между Банком и Клиентом по следующим каналами сервисам (доступность может варьироваться в зависимости от региона).

- CitiDirect BE® (including WorldLink®)
  CitiDirect BE® (включая WorldLink®)
- CitiConnect®
  CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
  Общество всемирных межбанковских финансовых каналов связи ("SWIFT")
- Manual Initiated Funds Transfer ("MIFT")
  Взаимно инициированный денежный перевод ("MIFT")
- Interactive Voice Response ("IVR")
  Интерактивный голосовой ответ ("IVR")
- Email/Fax/Mail/Messenger/Phone with the Bank
  Коммуникация с банком по электронной почте, факсу, мессенджерам и телефону
- Other local electronic connectivity channels
  Другие электронные каналы

These Security Procedures are to be read together with the MAST and may be updated and advised to the Customer from time-to-time by electronic or other means, including but not limited to posting updates to the Security Procedures on CitiDirect BE. Unless otherwise provided by law, Customer's continued use of any of the above noted Services or connectivity channels after being advised of updated Security Procedures shall constitute Customer's acceptance of such updated Security Procedures. These Security Procedures cover the following:

Данные Процедуры безопасности следует использовать вместе с Условиями обслуживания Основного счета. В них могут быть вноситься изменения, о которых будет сообщено клиенту в сервисе CitiDirect BE, а также другими каналам, включая электронные. Использование Клиентом любых обозначенных выше сервисов после его уведомления о внесении в них изменении приравнивается к согласию клиента на данные изменения, если иное не требуется законодательно. К Процедурам безопасности относятся следующие темы:

2. Authentication Methods
Методы Аутентификации

The Security 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), seal/signature verification, 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.

Процедуры безопасности включают ряд методов («Методы Аутентификации»), которые используются для идентификации и Аутентификации Клиента, а также других пользователей, авторизированных Клиентом, и подтверждения его прав с помощью одного или нескольких механизмов, таких как пары пользовательского ID/пароля, электронных сертификатов, биометрии, токенов (распространяемых на электронных или физических носителях), печать, подпись и других способов, связанных с Методами аутентификации (совместно – «Полномочия»). Методы аутентификации и связанные полномочия позволяют Банку подтвердить источник запроса, полученного Банком.

More information regarding Authentication Methods for access to Services and/or connectivity channels may be accessed on the CitiDirect BE Login Help website. Customer may at any time select an available Authentication Method. During implementation of Services or connectivity channels, Bank may set-up a default Authentication Method, which Customer may change at any time to another available Authentication Method.

С более подробной информацией относительно Методов Аутентификации для доступа к сервисам и каналам связи можно ознакомиться на сайте помощи по входу в CitiDirect BE. Клиент может в любой момент выбрать доступный способ аутентификации. Во время первичного подключения Сервисов и каналов связи, Банк может установить один из методов по умолчанию, которые Клиент может изменить на любой другой доступный метод в любое время.

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

Следующие Методы Аутентификации доступны для сервисов и каналов связи:

CitiDirect BE Authentication Methods *CitiDirect BE Методы Аутентификации*	
Biometrics *Биометрические данные*	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. *Метод аутентификации, использующий физические свойства пользователя (отпечаток пальца, распознавание по лицу), распознаваемые с помощью средств, встроенных в мобильное устройство пользователя, и способов криптографии для получения доступа в систему CitiDirect BE. Физические данные пользователя не передаются в Банк при использовании данного способа аутентификации.*
Challenge Response Token *Метод Запрос-Ответ*	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. This authentication method, when combined with a secure password results in multifactor authentication. *Либо (а) электронный токен, генерируемый мобильным приложением (например, MobilePASS), либо (б) физический токен (например, SafeWord Card, Vasco), которые в каждом случае генерируют динамический пароль после аутентификации по ПИН-коду (например, 4-digit PIN). При доступе в систему CitiDirect BE, система генерирует код запроса, который вводится пользователем в соответствующий токен, токен в свою очередь генерирует код Ответа, впоследствии вводимый пользователем в систему. При использовании данного метода с безопасным паролем, пользователь может установить многофакторную аутентификацию.*
One-Time Password Token *Токен для одноразового пароля*	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. *Либо (а) электронный токен, генерируемый мобильным приложением (например, MobilePASS), либо (б) физический токен (например, SafeWord Card, Vasco), которые в каждом случае генерируют динамический пароль после аутентификации по ПИН-коду (например, 4-digit PIN). Динамический пароль вводится в систему для получения доступа.*
Secure Password *Безопасный пароль*	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. This authentication method, when combined with a challenge response token results in multifactor authentication. *Пользователь вводит свой безопасный пароль для доступа в систему. Безопасный пароль, как правило, ограничивает возможности пользователя в системе, например позволяя просматривать только определенную информацию. При использовании данного метода совместно с методом Запрос-Ответ, пользователь может установить многофакторную аутентификацию.*
SMS One-Time Code *Одноразовый код по СМС*	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. *Динамический пароль, который пользователь получает по СМС и вводит вместе с безопасным паролем для входа в систему.*

Voice One-Time Code *Одноразовый голосовой код*	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. *Динамический пароль, который пользователь получает автоматическим звонком и вводит вместе с безопасным паролем для входа в систему.*
Digital Certificates *Электронные сертификаты*	A digital certificate is an electronic identification issued by an approved certificate authority for authentication and authorization. Digital certificates may be attributed to corporate legal entities ("Corporate Seals") or individuals ("Personal Certificates"). The Customer is responsible for properly verifying the identity of all users of Personal Certificates acting on behalf of the Customer in accordance with local law. *Электронный сертификат является средством идентификации пользователя, выпускаемым одобренным сертифицирующим органом для авторизации и аутентификации пользователя в системе. Электронный сертификат может быть выпущен для юридических лиц («Корпоративная печать») и для физических лиц («Персональный сертификат»). Клиент несет ответственность за подобающую проверку личностей всех пользователей, получающих Персональный сертификат и действующих от лица клиента, в рамках законодательства.* The Bank and the Customer are required to use digital certificates provided by authorized persons, to ensure all Communications exchanged via a public Internet connection or an otherwise unsecure Internet connection are fully encrypted and protected. *Банк и Клиент обязаны использовать электронные сертификаты, предоставленные авторизованным на это лицом или компанией, для обеспечения безопасной и зашифрованной передачи запросов в систему Банка через Интернет.*

CitiConnect for Files Authentication Methods ***CitiConnect для файлов Методы аутентификации***	
Digital Certificates *Электронные сертификаты*	See description above. *Смотри описание выше*
IP Address Whitelist When Using CitiConnect *Список разрешенных IP адресов при использовании 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. Used in conjunction with Digital Certificate method above. *Некоторые интернет запросы, получаемые банком, например, через VPN, могут передаваться с определенных заранее IP-адресов. Банк будет принимать запросы от и передавать данные по тем IP-адресам, которые обозначены как принадлежащие Клиенту. Используется вместе с Электронным сертификатом, указанным выше.*

CitiConnect API Authentication Methods ***CitiConnect API Методы аутентификации***	
Digital Certificates *Электронные сертификаты*	See description above. *Смотри описание выше*

IP Address Whitelist When Using CitiConnect *Список разрешенных IP адресов при использовании CitiConnect*	See description above. *Смотри описание выше*

CitiConnect for SWIFT Authentication Methods *CitiConnect для SWIFT Методы аутентификации*	
Digital Certificates *Электронные сертификаты*	See description above. Can be used in conjunction with SWIFT Authentication method below. *Смотри описание выше. Могут использоваться вместе с методами аутентификации для SWIFT, обозначенными ниже.*
SWIFT Authentication *Аутентификация в 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. *Запросы, передаваемые между Банком и Клиентом через SWIFT, включая, но не ограничиваясь данными о счете, платежными поручениями и инструкции изменить или отменить платежное поручение, будут авторизованы с использованием процедур, обозначенных в контрактных документах SWIFT (которые могут быть дополнены или изменены). Под процедурами понимаются Общие условия и положения, документация сервиса FIN, а также другие соглашения, которые могут быть установлены SWIFT. Банк не обязуется выполнять какие-либо процедуры для аутентификации отправителя запросов, не обозначенные документацией SWIFT.* 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. *Банк не несет ответственности за ошибки и задержки в системе SWIFT. Клиент несет ответственность за предоставление Банку запросов по форме, требуемой и определяемой 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. *Запросы передаваемые и получаемые через SWIFT регулируются правилами системы, включая правила членства в системе SWIFT. Клиент должен ознакомиться и следовать стандартам подачи запросов через SWIFT.*

SWIFT Authentication Method *SWIFT Методы аутентификации*	
SWIFT Authentication (Direct Connection for Financial Institutions) *Аутентификация в SWIFT (Прямое подключение для финансовых учреждений)*	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. *Запросы, передаваемые между Банком и Клиентом через SWIFT, включая, но не ограничиваясь данными о счете, платежными поручениями и инструкции изменить или отменить платежное поручение, будут авторизованы с использованием процедур, обозначенных в контрактных документах SWIFT (которые могут быть дополнены или изменены). Под процедурами понимаются Общие условия и положения, документация сервиса FIN, а также другие соглашения, которые могут быть установлены SWIFT. Банк не обязуется выполнять какие-либо процедуры для аутентификации отправителя запросов, не обозначенные документацией SWIFT.* 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. *Банк не несет ответственности за ошибки и задержки в системе SWIFT. Клиент несет ответственность за предоставление Банку запросов по форме, требуемой и определяемой 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. *Запросы передаваемые и получаемые через SWIFT регулируются правилами системы, включая правила членства в системе SWIFT. Клиент должен ознакомиться и следовать стандартам подачи запросов через SWIFT.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission *Цифровая/Электронная подпись Методы аутентификации для подачи электронных документов*	
Digital Signature *Цифровая подпись*	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. *Тип электронной подписи, которая использует Электронный сертификат для валидации отправителя запроса и подтверждения целостности подписи, сообщения, программного обеспечения или цифрового документа.*

Electronic Signature *Электронная подпись*	An electronic symbol attached to a contract or other record, unique to and used by a person with an intent to sign. Electronic signatures can be established in the form of words, letters, numerals, symbols, click of a button on a website, upload of facsimile or scan of a physical signature, signing on a touchscreen, or agreeing to any terms and conditions by electronic means. Created under the sole control of the person using it, it is logically attached to or associated with a data message, capable of identifying the person who consents to the data message and certifying the person's consent. Such Electronic Signature would be submitted to the Bank through the Bank's electronic channels and in compliance with the associated Authentication Methods described above. *Электронный символ, прикрепляемый к контракту или другой записи. Может быть закреплен за и использоваться только за конкретным человеком. Электронная подпись может быть в виде слов, букв, цифр, символов, кнопки на сайте, факса или загрузки копии физической подписи, подпись на сенсорном экране и согласие с любыми условиями и соглашениями и в электронном виде. Создается под контролем человека, который будет использовать подпись, и передается вместе с сообщением и подтверждает согласие пользователя на передаваемое сообщение. Банк получает электронную подпись через электронные каналы Банка в соответствии с Методами аутентификации указанными выше.*

Manual Initiated Funds Transfer (MIFT) Authentication Method ***Взаимно инициированный денежный перевод (MIFT) Методы аутентификации***	
MIFT Authentication *MIFT аутентификация*	Manually Initiated Funds Transfer (MIFT), including amendments, recalls, or cancelations of previous manual instructions, may be made by fax or letter or upload to CitiDirect. Not all forms are supported in all countries. Initiators are persons designated by the Customer who are authorized to initiate transactions in accordance with restrictions, if any, are identified by the Customer. Confirmers are person designated by the Customer that Bank may call back, at its discretion, for confirmation of manually initiated instructions for funds transfers. *Взаимно инициированный денежный перевод, включая изменения и отмену инициированных ранее запросов возможно совершить по факсу, с помощью письма или через CitiDirect BE. Не все формы поддерживаются для всех стран. Инициатором может выступать пользователь, авторизованный Клиентом на совершение транзакций в соответствии с какими-либо ограничениями, которые также определяются Клиентом. Подтверждать транзакцию могут пользователи, определенные Клиентом, к которым Банк может обращаться по своему усмотрению для подтверждения транзакций инициированных вручную.* In certain countries, mobile telephone numbers are not accepted as call back numbers. Further details are provided in the applicable Country Cash Management User Guide, Global Manual Transaction Authorization or Universal Nomination Form. MIFT is to be used by the Customer as a contingency method to communicating instructions to the Bank. *В некоторых странах, номер мобильного телефона не принимается в качестве средства связи с пользователями, ответственными за подтверждение транзакции. Более подробная информация об этом содержится Cash Management User Guide для каждой конкретной страны, Глобальных процедурах авторизации взаимных транзакций и форме Универсального назначения пользователей. MIFT следует использовать в качестве запасного канала передачи запросов Банку.*

Mail, Fax, Email and Messenger Authentication Methods *Почта, факс, электронная почта и мессенджеры Методы аутентификации*	
Seal Image Verification *Подтверждение печати*	Correspondence received by the Bank via fax, mail, email or messenger, excluding MIFT requests, are verified and collated with due care based on the seal image contained in the Customer's authority document or similar document provided to the Bank. *Корреспонденция, получаемая Банком по факсу, почте, электронной почте или через мессенджер, исключая MIFT запросы, рассматриваются и подтверждаются с помощью печати, содержащейся на генеральных распоряжениях Клиента или других схожих формах.*
Signature Verification *Подтверждение подписи*	Correspondence received by the Bank via fax, mail email or messenger, excluding MIFT requests, are signature verified based on the information contained in the Customer's authority document or similar document provided to the Bank. *Корреспонденция, получаемая Банком по факсу, почте, электронной почте или через мессенджер, исключая MIFT запросы, рассматриваются и подтверждаются с помощью подписи, содержащейся на генеральных распоряжениях Клиента или других схожих формах*
Secure PDF *Безопасная передача 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. *Зашифрованные электронные письма доставляются в любой почтовый сервис в виде PDF документов, которые могут быть открыты паролем. Шифрованию подлежат и текст письма, и прикрепленные файлы. Пароль для документов может быть создан при получении первого зашифрованного письма.*
MTLS *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. *Обязательный безопасный канал передачи данных (Mandatory Transport Layer Security (MTLS)) создает защищенный и безопасный сервис обмена электронными письмами между Клиентом и Банком. Письма передаются через интернет по зашифрованному TLS каналу.*

Phone Authentication Methods *Телефон Методы аутентификации*	
PIN *PIN*	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. *Клиент, связываясь с банком по телефону, должен ввести ПИН-код и авторизовать доступ.*
Verification Questions *Секретный вопрос*	Customers contacting the Bank via phone are prompted by the Bank's service representatives to provide correct verbal responses to verification questions in order to validate authorized access. *Клиент, связываясь с банком по телефону, должен предоставить сотруднику Банка устный ответ на секретный вопрос для авторизации доступа.*

The availability of Authentication Methods described above varies based on local markets.

Доступность конкретных методов аутентификации может изменяться в зависимости от доступности в каждом регионе.

3. Customer Responsibilities
Ответственность Клиента

3.1 Identifying Authorized Users: Customer is responsible for identifying: (i) all individuals acting on the Account(s) on behalf of the Customer at an entity level for all Services and connectivity channels, and (ii) each person acting on behalf of the Customer being duly authorized by the Customer to act on the Customer's Account.

Идентификация авторизованных клиентов: Клиент несет ответственность за: (а) идентификацию всех физических лиц, совершающих действия со счетами, от лица Клиента во всех сервисах и каналах связи Банка, и (б) то, чтобы каждое лицо, совершающее действия по счетам от лица Клиента, было авторизовано надлежащим образом.

3.2 Customer is responsible for assigning and monitoring any transaction limits assigned to the Customer and/or its users and ensuring that these limits (a) do not exceed the limits as required by the Customer's internal policies and other authority and constitutive documents such as Customer's Board of Director resolutions, Bank Mandates, Power Of Attorney, or equivalent document, and (b) are properly reflected on all connectivity channels and user entitlements.

Клиент несет ответственность за назначение и мониторинг любых лимитов на транзакции, установленных Клиенту и/или его пользователям, убеждаясь в том, что эти лимиты (а) не превышают лимитов, установленных внутренними нормативами Клиента и другими предписаниями, как рекомендации Совета Директоров Клиента, требования Банка, доверенностями или эквивалентными документами, и (б) подобающим образом отражены во всех каналах связи с Банком и пользовательских юрисдикциях.

3.3 Certain jurisdictions may require individuals (and their corresponding Credentials) to be identified by the Bank in accordance with applicable AML legislation requirements before granting access to perform certain functions. Please contact your Customer Service Representative or visit the CitiDirect BE website for further information.

Некоторые юрисдикции могут требовать, чтобы пользователи (и их соответствующие полномочия) определялись банком в соответствии с установленными процедурами по противодействию отмыванию денежных средств, перед предоставлением им доступа к определенным функциям. Пожалуйста, свяжитесь с вашим представителем службы поддержки или посетите веб-сайт Citi Direct BE для получения более подробной информации.

3.4 Safeguarding of Authentication Methods

Защита методов аутентификации

The Customer is responsible for safeguarding the Authentication Methods and Credentials with the highest standard of care and diligence, and ensuring that access to and distribution of the Credentials are limited only to persons that have been authorized by the Customer.

Клиент несет ответственность за обеспечение высшей степени безопасности Методов Аутентификации и Полномочий для обеспечения того, чтобы доступ к соответствующим полномочиям был только у пользователей, авторизованных клиентом.

Communications sent by a third party: Where the Customer is using a Credential to identify and authenticate their Communications as originating from them as a legal entity, the Customer is responsible for exercising full control over the use of such Credentials when sending Communications to the Bank, including where such Communications are sent by applications and/or systems that are managed by a third party on behalf of the Customer. In all circumstances the Bank will (a) deem any Communication it receives through an electronic connectivity channel, that has been received by the Bank in compliance with these Security Procedures duly authenticated as originating from the Customer, as a Communication instructed by the Customer and (b) may act upon any Communication that it receives on behalf of the Customer in compliance with these Security Procedures.

Запросы от третьих лиц: Там, где Клиент использует Полномочия для идентификации и аутентификации запросов, исходящих от лица Клиента, он несет ответственность за обеспечение полного контроля за использованием таких Полномочий, включая случаи, когда соответствующий запрос был отправлен через канал или приложение, управляемое третьей стороной от лица Клиента. Во всех случаях Банк будет (а) полагать, что все запросы, полученные по электронным каналам после надлежащей аутентификации в соответствии с Процедурами безопасности, получены по указанию Клиента, и (б) действовать в соответствии с запросом, полученным от лица клиента в соответствии со всеми процедурами безопасности.

4. Data Integrity and Secured Communications
Целостность данных и безопасность обмена информацией

4.1 The Customer will be transmitting data to and otherwise exchanging Communications with the Bank, utilizing the internet, mail, email and/or fax which the Customer understands are not (i) necessarily secure communications and delivery systems, and (ii) under the Bank's control.

Клиент будет передавать и получать данные от Банка, используя интернет, почту, электронную почту и/или факс, осознавая, что (а) данные каналы не являются гарантированно безопасными, и (б) не находятся под контролем Банка.

4.2 The Bank, utilizes industry leading encryption methods (as determined by the Bank), which help to ensure that information is kept confidential and that it is not changed during electronic transit.

Банк использует ведущие системы шифрования (которые определяются непосредственно банком), что помогает сохранять данные конфиденциальными и неизменными в процессе электронной передачи.

4.3 If the Customer suspects or becomes aware of a technical failure or any improper or potentially fraudulent access to or use of the Bank's Services or connectivity channels or Authentication Methods by any person (whether an authorized person or not), the Customer shall promptly notify the Bank of such occurrence. In the event of improper or potentially fraudulent access or use by an authorized person, the Customer should take immediate actions to terminate such authorized person's access to and use of the Bank's Services or connectivity channels.

Если Клиент заподозрил или обнаружил техническую неисправность или нежелательный и, возможно, преступный доступ к банковским каналам связи или Методам аутентификации каким-либо лицом (авторизованным или нет), Клиенту надлежит немедленно уведомить об этом Банк. В случае нежелательного или потенциально преступного доступа к авторизованным лицом, Клиент должен немедленно предпринять действия по прекращению доступа данного лица к каналам связи с Банком.

4.4 If the Customer utilizes file formatting or encryption software (whether provided by the Bank or a third party) to support the formatting and recognition of the Customer's data and instructions and acts upon Communications with the Bank, the Customer will use such software solely for the purpose for which it has been installed.

Клиент использует программное обеспечение, предназначенное для составления сообщений или шифрования (предоставленное Банком или третьими сторонами) для поддержки заданного форматирования данных и обеспечения возможности распознавания данных на стороне Банк, а также обеспечения Коммуникации с Банком. Клиент будет использовать указанное программное обеспечение исключительно в целях с которыми оно было установлено.

4.5 The Customer accepts that the Bank may suspend or deny users' access to Services requiring the use of Credentials (i) in case of suspicion of unauthorized or fraudulent use of the Credentials and/or (ii) to safeguard the Services or Credentials.

Клиент соглашается на то: что Банк может приостановить или отказать в доступе к Сервисам, для доступа к которым требуется предоставить Полномочия, (а) в случае подозрения на неправомерное или преступной использование полномочий (б) для безопасности Сервисов и Полномочий.

5. Security Manager and Related Functions
Роль Менеджера безопасности и его функции

For applications accessible in CitiDirect BE (with the exception of Personal Certificates discussed below), the Bank requires the Customer to establish a "Security Manager" function. Security Managers are responsible for:

Для приложений, доступных в CitiDirect BE (кроме Персональных сертификатов, указанных ниже), Банк требует от Клиента назначения лиц, выполняющих роль Менеджера Безопасности. Менеджер Безопасности ответственен за:

5.1 Establishing and maintaining the access and entitlements of users (including Security Managers themselves) including activities such as to: (a) creating, deleting or modifying user Profiles (including Security Manager Profiles) and entitlement rights (Note that user name must align with supporting identification documents); (b) building access profiles that define the functions and data available to individual users; (c) enabling and disabling user log-on credentials; and (d) assigning transaction limits (Note these limits are not monitored or validated by the Bank and Customer should monitor these limits to ensure they are in compliance with the Customer's internal policies and requirements, including but not limited to, those established by the Customer's Board of Directors or equivalent);

Установление и поддержание доступа и прав всех пользователей, включая самого Менеджера безопасности, с помощью: (а) создания, удаления или изменения пользовательских профилей (включая профиль Менеджера безопасности) и прав доступа (Обратите внимание, что имя пользователя должно совпадать с именем, указанным в удостоверении личности); (б) создание профилей с перечнем функций и уровнем доступа для отдельных пользователей; (в) включение и отключение полномочий пользователей; (г) установление лимитов на транзакции (Обратите внимание, что Банк не контролирует данные лимиты и Клиент должен самостоятельно обеспечивать их соответствие внутренней политике компании, включая установленную Советом Директоров Клиента или иными документами);

5.2 Creating and modifying entries in Customer maintained libraries (such as preformatted payments and beneficiary libraries) and authorizing other users to do the same;

Создание и модификация записей в библиотеках Клиента (такие как шаблоны для транзакций и список бенефициаров), а также авторизация пользователей для создания и редактирования записей;

5.3 Modifying payment authorization flows;

Изменение потоков данных;

5.4 Allocating dynamic password credentials or other system access credentials or passwords to the Customer's users; and

Распределение методов получения динамического пароля и других полномочий между пользователями Клиента;

5.5 Notifying the Bank, if there is any reason to suspect that security has been compromised.

Уведомление Банка при возникновении подозрения на нарушение безопасности системы.

Please note: Security Manager roles and responsibilities may vary or not be applicable in certain markets due to regulatory requirements and/or operational capabilities. In such markets, the Bank may require additional documentation and other information from the Customer to perform Security Manager functions on behalf of the Customer.

Обратите внимание: Роль и обязанности Менеджера безопасности могут варьироваться или не быть применимы для некоторых юрисдикций из-за законодательных ограничений и/или операционных возможностей. В таких юрисдикциях Банк может потребовать дополнительные сведения для выполнения роли Менеджера безопасности от лица Клиента.

6. Use of CitiDirect BE by Security Managers
Использование CitiDirect BE Менеджером безопасности

The Bank requires two (2) separate individuals to input and authorize instructions; therefore, a minimum of two Security Managers are required. Any two Security Managers, acting in concert, are able to give instructions and/ or confirmations through the connectivity channels in relation to any Security Manager function or in connection with facilitating communications. Any such communications, when authorized by two Security Managers, will be accepted and acted on by the Bank and deemed to be given by the Customer. The Bank recommends the designation of at least three Security Managers to ensure adequate backup. The Customer shall designate Customer's Security Managers on the TTS Channels Onboarding Form. A Security Manager of the Customer may also act as the Security Manager for a third party entity (for instance, an affiliate of the Customer) and exercise all rights relating thereto (including the appointment of users for that third party entity's Account(s)), without any further designation, if that third party entity executes a Universal Access Authority form (or such other form of authorization acceptable to the Bank) granting the Customer access to its account(s). This only applies in relation to Account(s) covered under the relevant authorization.

Политика Банк предписывает назначение Клиентом двух (2) лиц, ответственных за ввод и исполнение инструкций; в связи с этим, необходимо утвердить, как минимум два Менеджера безопасности. Любые два Менеджера безопасности вместе могут делать запросы и/или давать подтверждения в рамках полномочий друг друга. Подобный запрос, подтвержденный двумя Менеджерами, будет обработан Банком, который будет считать, что запрос отправлен от лица Клиента. Банк рекомендует назначить минимум трех Менеджеров Безопасности, для обеспечения непрерывной работы в случае недееспособности одного из Менеджеров. Клиент должен указать данные назначаемого Менеджера в Форме для подключения к цифровым каналам. Менеджер безопасности клиента также может исполнять аналогичную роль для третьей стороны (например, для дочерней компании) и выполнять все обязанности (включая назначение доступа пользователей к счетам третьей стороны) без дополнительного уведомления, в случае если сторона имеет с Клиентом Договор универсального доступа (или другая форма, одобренная Банком). Это применимо только для счетов, указанных в соответствующем договоре.

7. Use of CitiDirect BE by Security Officers (For Personal Certificates only)
Использование CitiDirect BE Сотрудником по безопасности (Только для персональных сертификатов)

The Bank requires two (2) separate individuals to manage digital certificates attributed to individuals ("Personal Certificates"). Therefore, two Security Officers are required to assign and removal Personal Certificates to users, for the purpose of authenticating and authorizing Communications on the connectivity channels. The Bank recommends the designation of at least three Security Officers to ensure adequate backup. Any Communications authorized by Personal Certificates will be accepted and acted on by the Bank and deemed to be given by the Customer.

Политика Банк предписывает назначение Клиентом двух (2) лиц, ответственных за управление персональными сертификатами. Потому, необходимо утвердить двух Сотрудников по безопасности, которые бы авторизовали запрос в Банк на выдачу и отзыв персональных сертификатов. Банк рекомендует назначить минимум троих Сотрудников по Безопасности, для обеспечения непрерывной работы в случае недееспособности одного из Сотрудников. Любой запрос, авторизованный персональным сертификатом будет обработан Банком, который будет считать, что запрос отправлен от лица Клиента.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions