Security Procedures
보안 절차

1. 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).

- CitiDirect BE® (including WorldLink®)
- CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
- Manual Initiated Funds Transfer ("MIFT")
- Interactive Voice Response ("IVR")
- Email/Fax/Mail/Messenger/Phone with the Bank
- Other local electronic connectivity channels

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:

A. Authentication Methods

B. Customer Responsibilities

C. Data Integrity and Secured Communications

D. Security Manager and Related Functions

1. 서문

계좌 및 서비스에 관한 기본 약관 (MAST)의 통신 섹션 (또는 기타 관련 계좌 약관)에 명시된 바와 같이, 본 보안 절차는 당행의 연결 채널에 대한 고객의 접속을 확인하고, 하기 서비스 또는 연결 채널(서비스 및 연결 채널 이용 가능 여부는 현지 마켓 별로 상이함)과 관련한 당행과 고객 간의 통신 출처를 검증하기 위한 목적으로 수립되었습니다.

- 씨티다이렉트 BE® (WorldLink® 포함)
- 씨티커넥트®
- 국제은행간 통신 협정("SWIFT")
- 수기이체 ("MIFT")
- 자동응답시스템("IVR")
- 당행과의 이메일/팩스/우편/메신저/전화
- 기타 현지 전자 연결 채널

본 보안 절차는 계좌 및 서비스에 관한 기본 약관(MAST)을 함께 참고해야 하며, 때때로 개정되어 전자 형식 또는 기타 방식(CitiDirect BE 상에 보안 절차 개정 내용 공지)을 통해 고객에게 안내될 수 있습니다. 법에 의해 달리 규정되지 않는 한, 고객이 보안 절차 개정 내용을 안내 받은 후 상기 명시된 서비스 또는 연결 채널을 계속해서 이용하는 경우, 고객이 보안 절차 개정 내용을 수용한 것으로 간주됩니다. 본 보안 절차의 목차는 아래와 같습니다.

A. 인증 방식

B. 고객의 책임

C. 데이터 무결성 및 보안 통신

D. 보안 관리자 및 관련 업무 기능

2. Authentication Methods

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 ve rification, 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.

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.

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

2. 인증 방식

본 보안 절차에는 사용자 ID/비밀번호, 디지털 인증서, 생체 인증 및 보안 토큰(하드웨어 또는 소프트웨어), 서명/날인 인증, 그리고/또는 상기 인증 방식과 관련 있는 기기 등과 같은 수단('보안 권한 정보'로 통칭)을 통해 일반적으로 고객 그리고/또는 고객이 승인한 사용자의 권한을 고유한 방식으로 확인하고 검증하는 특정 보안 인증 방식이 포함됩니다. 인증 방식 및 관련 보안 권한 정보를 이용하여 당행은 징구한 자료의 출처를 검증할 수 있습니다.

서비스 그리고/또는 연결채널에 접속하기 위한 인증 방식 관련 정보는 CitiDirect BE 로그인 도움 웹사이트에서 확인할 수 있습니다. 고객은 이용 가능한 인증 방식을 언제든지 선택할 수 있습니다. 서비스 또는 연결 채널 실행 중, 당행은 디폴트 인증 방식을 설정할 수 있으며, 고객은 다른 이용 가능한 인증 방식으로 언제든지 변경할 수 있습니다.

서비스 그리고/또는 연결채널에 접근하기 위해 다음의 인증 방식을 사용할 수 있습니다.

CitiDirect BE Authentication Methods CitiDirect BE 인증 방식	
Biometrics 생체인증	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. CitiDirect BE에 접속하고자, 사용자 고유 신체적 특징(예: 지문, 안면인식), 사용자의 모바일 기기 상에 설치된 생체인증 기술, 그리고 암호 기술을 이용하는 디지털 인증 방식. 사용자가 본 인증 방식을 선택하는 경우, 신체적 특징 데이터는 당행으로 전송되지 않습니다.

CitiDirect BE Authentication Methods CitiDirect BE 인증 방식	
Challenge Response Token 질의 응답 토큰	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. 4자리 PIN번호 인증 후 동적 패스워드를 생성하는 (i)모바일 애플리케이션 기반의 소프트 토큰(MobilePASS 등) 또는 (ii) 실물 토큰(SafeWord Card, Vasco등). CitiDirect BE 액세스 시, 시스템에서 질문을 생성하면 MobilePASS 앱에서 응답 비밀번호를 생성해 시스템에 입력합니다. 보안 패스워드와 결합 시, 본 인증 방식은 다중인증이 가능합니다.
One-Time Password Token 일회용 비밀번호 토큰	Either (i) a mobile application 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. 4자리 PIN번호 인증 후 동적 패스워드를 생성하는 (i)모바일 애플리케이션 기반의 소프트 토큰(MobilePASS 등) 또는 (ii) 실물 토큰(SafeWord Card, Vasco등). 시스템 액세스를 위해 동적 패스워드를 입력합니다.
Secure Password 보안 패스워드	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. 사용자는 시스템 접속을 위해 보안 패스워드를 입력합니다. 보통 보안 패스워드로 인해 사용자는 특정 정보만 조회할 수 있는 등 시스템 상에서 사용자의 권한이 제한됩니다. 질의 응답 토큰과 결합 시, 본 인증 방식은 다중인증이 가능합니다.
SMS One-Time Code SMS 일회용 코드	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. SMS를 통해 사용자에게 동적 패스워드가 전달됩니다. 사용자는 시스템 접속을 위해 해당 동적 패스워드 및 보안 패스워드를 입력합니다.
Voice One-Time Code 음성 일회용 코드	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. 자동 음성전화를 통해 사용자에게 동적 패스워드가 전달됩니다. 사용자는 시스템 접속을 위해 해당 동적 패스워드와 보안 패스워드를 입력합니다.

CitiDirect BE Authentication Methods CitiDirect BE 인증 방식	
Digital Certificates 디지털 인증서	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. 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. 디지털 인증서란 인증 받은 인증기관이 인증, 확인을 위해 발행하는 전자 인증서를 지칭합니다. 디지털 인증서는 법인(법인 인감), 개인(개인 증명서)으로 구분될 수 있습니다. 고객은 현지 법에 따라 본인을 대리하는 모든 개인 증명서 사용자들의 신원을 적절히 검증할 책임이 있습니다. 당행과 고객은 공공 인터넷 접속 및 비 보안 인터넷 접속을 통해 교환되는 모든 정보가 완전히 암호화되어 보호될 수 있도록, 승인 받은 자가 제공하는 디지털 인증서를 이용해야 합니다.

CitiConnect for Files Authentication Methods CitiConnect 파일 인증 방식	
Digital Certificates 디지털 인증서	See description above. 상기 설명 참조
IP Address Whitelist When Using CitiConnect CitiConnect 이용시 IP 주소 화이트리스트	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. Virtual Private Network(VPN) 등을 통해 당행이 수령하는 특정 인터넷 정보는 사전에 동의된 IP 주소를 이용하여 정보를 교환하는 당사자들에게 달려있습니다. 당행은 고객의 지정 IP 주소에서 발송되는 정보를 수령할 뿐이며, 반대의 경우도 마찬가지입니다. 또한, 당행은 고객의 지정 IP 주소로 정보를 전송할 뿐이며, 반대의 경우도 마찬가지입니다. 상기 디지털 인증서 방식과 함께 이용됩니다.

CitiConnect API Authentication Methods CitiConnect API 인증 방식	
Digital Certificates 디지털 인증서	See description above. 상기 설명 참조
IP Address Whitelist When Using CitiConnect CitiConnect 이용시 IP 주소 화이트리스트	See description above. 상기 설명 참조

CitiConnect for SWIFT Authentication Methods CitiConnect SWIFT 인증 방식	
Digital Certificates 디지털 인증서	See description above. Can be used in conjunction with SWIFT Authentication method below. 상기 설명 참조. 하기 SWIFT 인증 방식과 함께 이용 가능합니다.
SWIFT Authentication SWIFT 인증	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. 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. 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. SWIFT 네트워크를 통해 당행과 고객 간에 전송되는 정보(예: 계좌정보, 지급 주문, 주문 취소 또는 수정 지시 등)는 SWIFT 의 계약문서(일반 사항, FIN 서비스 상세설명 등을 포함하는 문서이며, 때때로 수정, 보완됨)에 정의되어 있거나 또는 SWIFT 가 수립한 기타 약관에서 명시하고 있는 절차를 이용하여 인증됩니다. 당행은 발송인 및 당행과 고객 간 전송되는 정보의 진위여부를 밝히기 위해 SWIFT 절차에 포함된 사항을 제외한 그 어떤 것도 이행할 의무가 없습니다. 당행은 SWIFT 시스템 에러 또는 지연에 대한 책임이 없습니다. 고객은 SWIFT 에서 명시하고, 요구하는 형식 및 유형으로 당행에 정보를 제공할 책임이 있습니다. SWIFT 시설을 통해 송, 수신된 정보 및 전송은 회원사 규정을 포함한 SWIFT 규정 대상이 됩니다. 고객은 SWIFT 메시지 전송 기준을 익히고, 이를 준수할 책임이 있습니다.

SWIFT Authentication Method SWIFT 인증 방식	
SWIFT Authentication (Direct Connection for Financial Institutions) SWIFT 인증 (금융기관 직접 접속)	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. SWIFT 네트워크를 통해 당행과 고객 간에 전송되는 정보(예: 계좌정보, 지급 주문, 주문 취소 또는 수정 지시 등)는 SWIFT 의 계약문서(일반 사항, FIN 서비스 상세 설명 등을 포함하는 문서이며, 때때로 수정, 보완됨)에 정의되어 있거나 또는 SWIFT 가 수립한 기타 약관에서 명시하고 있는 절차를 이용하여 인증됩니다. 당행은 발송인 및 당행과 고객 간 전송되는 정보의 진위여부를 밝히기 위해 SWIFT 절차에 포함된 사항을 제외한 그 어떤 것도 이행할 의무가 없습니다. 당행은 SWIFT 시스템 에러 또는 지연에 대한 책임이 없습니다. 고객은 SWIFT 에서 명시하고, 요구하는 형식 및 유형으로 당행에 정보를 제공할 책임이 있습니다. SWIFT 시설을 통해 송, 수신된 정보 및 전송은 회원사 규정을 포함한 SWIFT 규정 대상이 됩니다. 고객은 SWIFT 메시지 전송 기준을 익히고, 이를 준수할 책임이 있습니다.

Digital/Electronic Signature Authentication Methods for Electronic Document Submission 전자 문서 제출 관련 디지털/전자 서명 인증 방식	
Digital Signature 디지털 서명	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. 서명, 메시지, 소프트웨어 또는 디지털 문서 진위여부와 무결성 검증을 위해 디지털 인증서를 이용하는 전자 서명의 일종.
Electronic Signature 전자 서명	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. 서명을 하고자 하는 자가 이용하는 본인 고유의 전자 심볼이며, 계약서 또는 기타 기록에 첨부됩니다. 전자 서명은 단어, 문자, 숫자, 심볼, 웹사이트 상의 버튼 클릭, 팩스 업로드 또는 수기 서명 스캔, 터치스크린 상의 서명 또는 전자 방식을 통해 약관에 동의된 형식으로 만들어질 수 있습니다. 실제 사용자가 직접 만들게 되는 전자 서명은 데이터 메시지에 동의하는 자의 신원을 확인할 수 있고, 이러한 동의를 인증할 수 있는 데이터 메시지와 관련이 있거나, 실제 이러한 메시지에 첨부됩니다. 전자 서명은 위에서 설명하는 관련 인증 방식에 따라, 그리고 당행의 전자 채널을 통해 당행 앞 제출됩니다.

Manual Initiated Funds Transfer (MIFT) Authentication Method 수기 이체(MIFT: Manually Initiated Funds Transfer) 인증 방식	
MIFT Authentication 수기 이체 인증	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. 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. 수기 이체(이전 수기 이체 지시 수정, 회수, 취소 포함)는 팩스 또는 우편 혹은 CitiDirect BE 를 통해 이루어집니다. 모든 형식이 모든 국가에서 지원되지는 않습니다. 거래개시자는 규정에 의거 거래를 개시할 수 있는 권한이 있으며, 고객이 지정, 확인한 자입니다. 확인자는 당행이 재량에 따라 수기 이체 거래 개시 지시 확인을 위해 콜백 할 수 있도록 고객이 지정한 자입니다. 일부 국가의 경우, 휴대폰 번호를 콜백 번호로 허용하지 않습니다. 보다 상세한 내용은 Country Cash Management User Guide, Global Manual Transaction Authorization 또는 Universal Nomination Form 에서 확인할 수 있습니다. 수기 이체는 당행과의 거래 지시 연락을 위한 비상 시 대책으로 이용될 수 있습니다.

Mail, Fax, Email and Messenger Authentication Methods 우편, 팩스, 이메일 및 메신저 인증 방식	
Seal Image Verification 도장 날인 이미지 검증	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. MIFT 요청을 제외하고, 당행이 팩스, 우편, 이메일 또는 메신저를 통해 수령하는 정보는 고객의 권한 문서 또는 당행 앞 제시된 이와 유사한 문서 상에 포함된 도장 날인 이미지를 바탕으로 신중하게 검증, 분석됩니다.
Signature Verification 서명 검증	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. MIFT 요청을 제외하고, 당행이 팩스, 우편, 이메일 또는 메신저를 통해 수령하는 정보는 고객의 권한 문서 또는 당행 앞 제시된 이와 유사한 문서 상에 포함된 정보를 바탕으로 서명 검증됩니다.
Secure PDF 보안 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. 암호화된 이메일이 PDF 문서 형식으로 일반 메일함으로 전송되며 PDF 문서는 비밀번호를 입력하여 열 수 있습니다. 이메일 본문과 첨부 파일 모두 암호화됩니다. 비밀번호는 최초 보안 이메일을 수신하면 설정할 수 있습니다.
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. MTLS (Mandatory Transport Layer Security)는 당행과 고객 간 보안 이메일을 전송할 수 있는 연결을 만듭니다. 이 채널로 전송된 이메일은 연결이 만든 암호화된 TLS 터널을 통해 인터넷으로 전송됩니다.

Phone Authentication Methods 전화 인증 방식	
PIN	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. 전화를 통해 당행에 연락을 취하는 고객은 접속 권한 검증을 위해 PIN 을 입력해야 합니다.
Verification Questions 검증 질문	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. 전화를 통해 당행에 연락을 취하는 고객은 접속 권한 검증을 위해 검증 질문에 대한 올바른 답변을 당행 담당자에게 제시해야 합니다.

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

상기 제시된 인증 방식은 현지 마켓 별로 상이하게 이용될 수 있습니다.

3. Customer Responsibilities

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.

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.

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.

3.4 Safeguarding of Authentication Methods

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.

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.

3. 고객의 책임

3.1 권한 있는 사용자 신원 확인: 고객은 (i) 모든 서비스 및 연결 채널과 관련하여 법인 차원에서 고객을 대신하여 해당 계좌를 관리하는 모든 개인, 그리고 (ii)고객을 대신하여 고객의 계좌를 관리하도록 권한을 부여한 각각의 인물에 대한 신원을 확인할 책임이 있습니다.

3.2 고객은 고객 및/또는 사용자들에게 거래 한도를 설정하고, 설정된 모든 거래 한도를 모니터링하며, 이러한 거래 한도가 (a) 고객의 내부 규정 및 기타 권한, 부속 문서(예: 고객의 이사회 결의 사항, 은행 지침, 위임장 혹은 이에 상응하는 문서)에서 규정하는 한도를 초과하지 않고, (b) 모든 연결 채널과 사용자 권한에 적절히 반영되도록 할 책임이 있습니다.

3.3 특정 국가에서는 개인(그리고 이들의 보안 권한 정보)에게 특정 기능 수행을 위한 접속 권한을 부여하기 이전에 당행이 관련 자금세탁방지 규정에 따라 이들의 신원을 확인하도록 규정할 수 있습니다. 보다 자세한 내용을 확인하려면 CitiDirect BE 웹사이트를 방문하거나, 고객 서비스 담당자에게 문의하기 바랍니다.

3.4 인증 방식 보호

고객은 가장 높은 수준의 주의와 성실함을 다해 인증 방식과 보안 권한 정보를 보호하고, 보안 권한 정보 접속 및 배포가 고객이 승인한 자에 대해서만 이루어지도록 할 책임이 있습니다.

제 3자가 전송한 통신: 고객이 보안 권한 정보를 이용하여 제3자의 통신 정보가 법인으로부터 발송된 것으로 확인, 인증하고자 하는 경우, 고객은 통신 정보를 당행으로 전송할 때(고객을 대신하여 제3자가 관리하는 애플리케이션 그리고/또는 시스템을 통해 보안 권한 정보가 전송될 때 포함), 보안 권한 정보에 대한 완전한 통제권을 행사할 책임이 있습니다. 모든 경우에 있어서 당행은 (i) 전자 연결 채널을 통해 당행이 수령하는 통신 정보가 본 보안 절차를 준수하여 수령되고, 고객으로부터 발송된 것으로 인증되면, 이러한 통신 정보가 고객의 지시에 의한 정보인 것으로 간주하게 되며, (ii) 본 보안 절차에 따라 고객을 대신하여 당행이 수령한 모든 통신 정보에 대해 조치를 취할 수 있습니다.

4. Data Integrity and Secured Communications

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.

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.

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.

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.

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.

4. 데이터 무결성 및 보안 통신

4.1 고객은 (i) 본인이 인지하기에 반드시 안전한 통신 및 전송 시스템이 아니며, (ii) 당행의 통제 하에 있지 않을 수 있는 인터넷, 우편, 이메일 그리고/또는 팩스를 이용하여 당행에 데이터를 전송하고, 당행과 통신 정보를 교환하게 됩니다.

4.2 당행은 기밀 정보를 보호할 수 있고, 전자 전송 중 변경이 일어나지 않도록 하는 업계 선도의 암호화 방식(은행이 선정함)을 이용합니다.

4.3 기술적 오류 또는 누군가(승인된 자 혹은 승인 받지 않은 자)가 서비스, 연결 채널 또는 인증 방식에 부적절하게 혹은 사기 행위 가능성을 가지고 접속하거나 사용한 사실을 인지하게 되거나 이 같은 사실이 의심되는 경우, 고객은 즉시 은행에 통보해야 합니다. 승인된 자가 부적절하게 혹은 사기 행위 가능성을 가지고 접속하거나 사용한 경우, 고객은 해당 승인된 자의 당행 서비스 또는 연결 채널 접속 및 사용을 중단하기 위해 즉각적인 조치를 취해야 합니다.

4.4 고객이 고객 데이터 및 지시서의 포맷팅 및 인식을 위해 (당행 또는 제3자가 제공한) 암호화 소프트웨어 혹은 파일 포맷팅을 사용하고 당행과의 통신 내용에 의거하여 행동하는 경우, 고객은 해당 소프트웨어를 본래 설치 목적으로만 이용해야 합니다.

4.5 고객은 (i) 보안 권한 정보가 승인 받지 않은 상태로 또는 사기 행위를 위해 이용된다고 의심되는 경우 및/또는 (ii) 서비스 혹은 보안 권한 정보를 보호하기 위한 목적으로, 은행이 보안 권한 정보 이용이 필요한 서비스에 대한 사용자 접속을 중단 또는 거절할 수 있음을 수용합니다.

5. Security Manager and Related Functions

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:

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);

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;

5.3 Modifying payment authorization flows;

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

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

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.

5. 보안 관리자 및 관련 업무 기능

CitiDirect BE에서 접속가능한 애플리케이션(아래에서 언급하는 개인 인증서 제외)에 대해 당행은 고객이 "보안 관리자" 담당자를 지정할 것을 요구합니다. 보안 관리자의 담당 책임은 다음과 같습니다.

5.1 다음과 같은 업무를 포함, 사용자(보안 관리자 본인 포함) 접속 및 권한을 생성, 유지합니다: (a) 사용자 프로파일(보안 관리자 프로파일 포함)과 권한의 생성, 삭제 또는 수정(사용자 이름이 반드시 신원 확인 문서와 일치해야 함) (b) 다양한 사용자들이 이용할 수 있는 기능 및 데이터를 정의하는 접속 프로파일 작성 (c) 사용자 로그온 보안 권한 정보 활성화 및 비활성화 (d) 거래 한도 부여(참고: 본 한도는 당행에서 모니터하거나 검증하지 않음. 고객은 본 한도가 고객의 내부 규정 및 요건(고객의 이사회 또는 이에 상응하는 회의체에서 수립한 요건 등)을 준수하도록 모니터링 해야 함).

5.2 고객이 관리하는 라이브러리(기정의된 양식으로 된 지급건 및 수취인 라이브러리 등) 입력 정보를 생성, 수정 및 다른 사용자들에게 동일한 작업을 승인합니다.

5.3 지급승인 흐름표를 수정합니다.

5.4 고객의 사용자들에게 동적 패스워드 보안 권한 정보 또는 기타 시스템 접속 보안 권한 정보나 패스워드를 배정합니다.

5.5 보안 침해를 의심할 만한 이유가 있을 경우 이를 은행에 통지합니다.

주: 특정 마켓에서는 감독 요건 그리고/또는 운영 수용력으로 인해 보안 관리자의 역할과 책임은 다양하거나 적용 가능하지 않을 수 있습니다. 이러한 마켓에서는 당행이 고객을 대신하여 보안 관리자 역할을 수행하기 위해 추가 문서 및 기타 정보를 요구할 수 있습니다.

6. Use of CitiDirect BE by Security Managers

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.

6. 보안 관리자의 CitiDirect BE 이용

당행은 지시서의 입력 및 승인을 위해 2명의 개별 인력을 요구합니다. 따라서 최소 2명의 보안 관리자가 필요합니다. 보안 관리자의 업무 또는 커뮤니케이션 지원과 관련하여, 보안 관리자 2인은 서로 협력하여 연결 채널을 통해 지시서 그리고/또는 확인서를 발부할 수 있습니다. 당행은 보안 관리자 2인이 승인한 경우 해당 통신 정보를 수락, 실행하며, 이러한 통신 정보는 고객이 보낸 것으로 간주됩니다. 당행은 충분한 백업을 위해 최소 3명의 보안 관리자를 지정할 것을 권장합니다. 고객은 TTS 채널 온보딩 양식에 보안 관리자를 지정해야 합니다. 고객의 보안 관리자는 제3자 기관(예를 들어 고객의 계열사)이 범용 접근권 양식(또는 당행이 인정하는 기타 승인 양식)을 작성하여 고객에게 자사 계좌 접근권을 승인한 경우 추가 지정 절차 없이 해당 제3자 기관을 위한 보안 관리자 역할을 수행할 수 있으며 (해당 제 3자 기관의 계좌 사용자 지정 포함) 관련 모든 권한을 행사할 수 있습니다. 이는 관련 승인에서 명시하는 계좌에만 적용됩니다.

7. Use of CitiDirect BE by Security Officers (For Personal Certificates only)

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.

7. 보안 담당자의 CitiDirect BE 이용 (개인 인증서만 해당)

당행은 개인에 대한 디지털 인증서("개인 인증서") 관리를 위해 2명의 개별 인력을 요구합니다. 따라서 연결 채널 상의 통신 정보 진위 확인 및 승인을 위한 목적으로 사용자에 대한 개인 인증서를 발부, 제거하는 보안 담당자 2인이 필요합니다. 당행은 충분한 백업을 위해 최소 3명의 보안 관리자를 지정할 것을 권장합니다. 당행은 개인 인증서를 통해 승인된 모든 통신 정보를 수락, 실행하며, 이러한 통신 정보는 고객이 보낸 것으로 간주됩니다.