



ҚАУІПСІЗДІК ПРОЦЕДУРАЛАРЫ (11-нұсқа)
ПРОЦЕДУРЫ БЕЗОПАСНОСТИ (версия 11)
SECURITY PROCEDURES (version 11)

Осы қауіпсіздік процедуралары («Процедуралар») 11-нұсқалы электронды құжаттармен алмасу ережесінің («Ереже») ажырамас бөлігі болып табылады.

Процедуралар ескіріп кетуі мүмкін. Жанартылған Процедуралар мен Ережені оқымас бұрын www.citibank.kz сайтынан «Клиенттер үшін» секциясынан алуға болады.

Жазбаша әріппен Ережеде пайдаланылатын терминдер Ереженің «Пайдаланылатын терминдер» бөлігінде айқындалған.

Настоящие процедуры безопасности («Процедуры») являются неотъемлемой частью правил обмена электронными документами («Правила») версии 11.

Процедуры могут быть устаревшими. Обновленные Процедуры и Правила перед прочтением необходимо получить на сайте www.citibank.kz в секции «Для клиентов».

Термины, используемые в Процедурах с прописной буквы, определены в части «Используемые термины» Правил.

These security procedures («Procedures») integrate rules of electronic documents exchange («Rules») version 11.

The Procedures may be old and therefore, require an update. The Client before learning the Procedures should receive the latest version of the Procedures and the Rules from www.citibank.kz site, «Customers Info» section.

The terms used begun with a capital letter here, have definition stipulated in the Rules in «Used Terms» section.

1 Клиенттің қаржылық операцияларының қауіпсіздігі/ Безопасность финансовых операций Клиента/ Security of Client Financial Operations

1.1 Жүйенің ең басты міндеттерінің бірі Жүйе арқылы Шоттарға қол жеткізген кезде Клиенттің қаржылық операцияларының қауіпсіздігін қамтамасыз ету болып табылады. Жүйеде қолданылатын алдыңғы қатарлы технологиялар мұндай қауіпсіздікті қамтамасыз етеді.

1.1 Одной из главных задач Системы является обеспечение безопасности финансовых операций Клиента при доступе к Счетам через Систему. Используемые в Системе передовые технологии обеспечивают такую безопасность.

1.1 One of the main goals of the System is security of Client financial operations during the Client access to Accounts through the System. The System has been designed based on the latest technologies providing strong security of such operations.

2 Жүйеге қол жеткізу қауіпсіздігі/ Безопасность доступа в Систему/ Security of the System Access

2.1 Жүйеге қол жеткізу қауіпсіздігі қос факторлы қол жеткізу моделін пайдаланумен қамтамасыз етіледі. Мұндай модель кезінде Пайдаланушылар Жүйеге қол жеткізу үшін бір мезгілде а) Картаны және б) Картаның ПИН кодын пайдалануы тиіс.

2.1 Безопасность доступа в Систему обеспечивается использованием двухфакторной модели доступа. При такой модели, Пользователи, для доступа в Систему, должны одновременно использовать: а) Карту и б) ПИН код для Карты.

2.1 Security of the System access bases on two-factor access model, requesting each User to use а) the Card and б) PIN code simultaneously for the access to the System.

2.2 Қос факторлы қол жеткізу моделі Пайдаланушылардың келесі талаптарды сақтауы талабымен Жүйеге тек уәкілетті Пайдаланушылардың ғана қол жеткізуіне кепілдік береді:

2.2 Двухфакторная модель доступа гарантирует доступ в Систему только уполномоченных Пользователей, при условии соблюдения Пользователями следующих требований:

2.2 Two-factor access model provides access to the System only for authorized Users, if Users fulfill next requirements below:

а) Банктен жаңа Картаны және бастапқы ПИН коды бар жабық конвертті алған кезде Пайдаланушы дереу ПИН кодты өзгертуі тиіс.

а) При получении из Банка новой Карты и закрытого конверта с первоначальным ПИН кодом, Пользователь должен незамедлительно изменить ПИН код.

а) After new Card and closed PIN mailer receipt from the Bank, the User must immediately change PIN code.

б) ПИН код қатаң құпиялы ақпарат болып табылады. Пайдаланушы Администраторлар мен Банк қызметкерлерін қоса алғанда, үшінші тұлғаларға ПИН кодты хабарламауы тиіс.

б) ПИН код является строго конфиденциальной информацией. Пользователь не должен сообщать ПИН код третьим лицам, включая Администраторов и сотрудников Банка.

б) PIN code is strictly confidential information. User must not disclose PIN code to 3rd parties including Administrators and the Banks employees.

в) Пайдаланушы оның ашылуын және кейіннен үшінші тұлғалардың пайдалануын алдын алу үшін ПИН кодты оқта-текте өзгертуі тиіс.

в) Пользователь должен периодически изменять ПИН код для предупреждения его раскрытия и последующего использования третьими лицами.

в) User must periodically change PIN code to prevent its disclosure and use by 3rd parties.

д) Пайдаланушы ПИН кодты ұмытпауы тиіс, өйткені ол қалпына келтірілмейді. ПИН код жоғалған кезде Пайдаланушы Администраторға хабарласуы тиіс, Администратор өз кезегінде Банкке Картаны ауыстыру үшін хабарласуы тиіс.

д) Пользователь не должен забывать ПИН код, так как он не подлежит восстановлению. При утере ПИН кода, Пользователь должен обратиться к Администратору; Администратор, в свою очередь, должен обратиться в Банк для замены Карты.

д) User must not forget PIN code, as the code is not the mater to restore. In case of the code loss, the User will contact Administrator; then the Administrator will request the Bank to replace the Card.

е) Пайдаланушы Администраторлар мен Банк қызметкерлерін қоса алғанда, үшінші тұлғаларға Картаны бермеуі; немесе Картаны үшінші тұлғаларға қолжетімді жерде сақтамауы тиіс.

е) Пользователь не должен передавать Карту третьим лицам, включая Администраторов и сотрудников Банка; или хранить Карту в месте, доступном для третьих лиц.

е) The User must not pass the Card to 3rd parties, including the Administrators and the Bank employees; User must keep the Card in a room secured against 3rd party access.

ф) Карта ұрланған, жоғалған немесе бүлінген жағдайда Пайдаланушы дереу Администраторға хабарласуы тиіс, Администратор өз кезегінде Банкке Картаны ауыстыру үшін дереу хабарласуы тиіс.

ф) При краже, утере или порче Карты, Пользователь должен незамедлительно обратиться к Администратору; Администратор, в свою очередь, должен незамедлительно обратиться в Банк для замены Карты.

ф) In case of the Card theft, loss or damage User will immediately contact Administrator; then the Administrator will immediately request the Bank to replace the Card.

г) Карта аккумуляторының қызмет ету мерзімі орташа 3 жыл құрайды және ол ауыстырылмайды. Аккумулятордың қызмет ету мерзімі өткеннен кейін Пайдаланушы аккумуляторды ауыстыруға әрекет жасамауы тиіс. Пайдаланушы Администраторға хабарласуы тиіс, Администратор өз кезегінде Банкке Картаны ауыстыру үшін хабарласуы тиіс.

г) Срок службы аккумулятора Карты составляет в среднем 3 года и не подлежит замене. При истечении срока службы аккумулятора, Пользователь не должен пытаться заменить аккумулятор. Пользователь должен обратиться к Администратору; Администратор, в свою очередь, должен обратиться в Банк для замены Карты.

г) Life time of the Card battery is approximately 3 years. After the battery expiration, the User should not try to replace the battery with new one. The User will contact the Administrator; then the Administrator will request the Bank to replace the Card.

h) Клиент әрбір Пайдаланушы үшін бір Картадан артық шығармауы тиіс.

h) Клиент должен выпускать не более одной Карты для каждого Пользователя.

h) The Client should not request more than one Card issue per the User.

і) Жүйеге қол жеткізуді тоқтату қажет болғанда, Пайдаланушы Администраторға хабарласуы тиіс, Администратор өз кезегінде Банкке Картаны Жүйеден алып тастау үшін хабарласуы тиіс. Банк растағаннан кейін Пайдаланушы оның Жүйеге қол жеткізуі шынымен тоқтағанына көз жеткізуі тиіс.

і) При необходимости в прекращении доступа к Системе, Пользователь должен обратиться к Администратору; Администратор, в свою очередь, должен обратиться в Банк для удаления Карты из Системы. После подтверждения Банком, Пользователь должен удостовериться, что его доступ в Систему действительно прекращен.

і) In case of need in User access termination, the User will contact the Administrator; then the Administrator will contact the Bank for the access termination. After the confirmation receipt from the Bank, the User will make sure that the access has been actually terminated.

3 Жүйені басқару қауіпсіздігі/ Безопасность администрирования Системы/ Security of the System Administration

3.1 Жүйенің баптауларын рұқсатпен өзгертудің кепілдігі Жүйенің баптауларын кез келген өзгерту кезінде екі Администратордың міндетті түрде бірлескен қатысуын талап ететін қос факторлы басқару моделін пайдаланумен қамтамасыз етіледі. Бір Администратор орындаған Жүйе баптауларының кез келген өзгеруі күшіне ену үшін міндетті түрде екінші Администратормен авторландыруы тиіс.

3.2 Клиент Жүйедегі Администраторлар мен Пайдаланушылардың барлық әрекеттері үшін өзіне жауапкершілік алады. Банк Администраторлар мен Пайдаланушылардың әрекеттері үшін, соның ішінде Жүйенің жұмыс істемей қалуына, Нұсқаулықтарды рұқсатсыз инициализацияға, Шоттар бойынша ақпаратқа және Жүйенің қосымша қызметтеріне қол жеткізуге әкеліп соқтырған әрекеттер үшін жауапкершілік көтермейді.

3.3 Қос факторлы басқару моделі Администратордың Жүйені және оның қосымша қызметтерін, Жүйенің ағымдағы баптауларын, Жүйеге қатысты Клиенттің Банкке талаптарды рәсімдеу процедураларын білуі, Администраторлардың Жүйені орындайтын баптауларының орындалу нәтижесін түсінуі талабымен Жүйенің Клиенттің талаптарына сәйкес келетініне кепілдік береді.

3.4 Администраторлар, бірлесіп әрекет ете отырып, келесі функцияларды орындайды:

а) CD0, CD1 және CD4 сұратуларының электронды банктік үлгі нысандарын рәсімдеп, оларды Банкке береді.

б) Банктен алынатын жаңа Карталар мен ПИН кодтары бар жабық конверттерді бөледі; Пайдаланушылар Карталарды алған кезде бастапқы ПИН кодтарды өзгерткендеріне көзін жеткізеді.

с) мына баптауды қоса алғанда, Жүйенің барлық баптауларын орындайды:

✓ Жүйе конфигурациясының; Нұсқаулықтарды жасау және қол қою нобайларының; Пайдаланушылардың және Администраторлардың өздерінің құқықтарының; анықтамалықтар мен кітапханалардың.

✓ Есептерді, хабарларды автоматты түрде жеткізілуін, Delphi есептерінің алынуын қоса алғанда, Жүйенің қосымша қызметтерінің.

д) Жүйеге үшінші тұлғалардың рұқсатсыз кіруін болдырмау мақсатымен Әкімшілер Пайдаланушылар Карталар мен ПИН кодтары бар хатқалталарды алуын дәлелдегенше Пайдаланушыларға Жүйеде құқықтар тағайындамаулары тиіс.

е) Пайдаланушылардың ақпараттық және техникалық қолдауын орындайды; Жүйенің басшылықтарын бөледі.

3.5 Банк Жүйені басқармайды.

3.6 Банк, Клиенттің сұратуы бойынша келесі функцияларды атқарады:

а) Пайдаланушылар үшін жаңа Карталарды шығарады.

б) Жаңа Пайдаланушылар оларды Жүйеге қосады; Пайдаланушыларды Жүйеден ажыратады.

с) Қосылған Пайдаланушылар үшін Карталарды ауыстырады.

д) Пайдаланушыларға Администратордың құқықтарын береді.

е) Басқарушының Клиент Шоттарына қол жеткізуді айқындайды.

3.1 Гарантия санкционированного изменения настроек Системы обеспечивается использованием двухфакторной модели администрирования, требующей обязательного совместного участия двух Администраторов при любых изменениях настроек Системы. Изменения, выполненные одним Администратором, для вступления в силу должны быть обязательно авторизованы вторым Администратором.

3.2 Клиент принимает на себя ответственность за все действия Администраторов и Пользователей в Системе. Банк не несет ответственности за действия Администраторов и Пользователей, включая действия, приведшие к неработоспособности Системы, несанкционированной инициации Инструкций, доступу к информации по Счетам или дополнительным услугам Системы.

3.3 Двухфакторная модель администрирования гарантирует соответствие Системы требованиям Клиента при условии знания Администраторами Системы и ее дополнительных услуг, текущих настроек Системы, процедуры оформления требований Клиента в Банк относительно Системы; понимания Администраторами результата выполнения всех выполняемых ими настроек Системы.

3.4 Администраторы, действуя сообща, выполняют следующие функции:

а) Оформляют и передают в Банк электронные банковские формы запроса CD0, CD1 и CD4.

б) Распределяют получаемые из Банка новые Карты и закрытые конверты с ПИН кодами; убеждаются, что Пользователи, при получении Карт, изменили первоначальные ПИН коды.

с) Выполняют все настройки Системы, включая настройку:

✓ Конфигурации Системы; схем создания и подписи Инструкций; прав Пользователей и самих Администраторов; справочников и библиотек.

✓ Дополнительных услуг Системы, включая автоматическую доставку отчетов, уведомления, получение отчетов Delphi.

д) Администраторы не должны назначать Пользователям права в Системе до момента подтверждения Пользователями факта получения Карт и конвертов с ПИН кодами, во избежание несанкционированного доступа в Систему третьих лиц.

е) Выполняют информационную и техническую поддержку Пользователей; распределяют руководства Системы.

3.5 Банк не выполняет администрирование Системы.

3.6 Банк, по запросу Клиента, выполняет следующие функции:

а) Выпуск новых Карт для Пользователей.

б) Подключение новых Пользователей к Системе; отключение Пользователей от Системы.

с) Замена Карт для подключенных Пользователей.

д) Назначение Пользователям прав Администратора.

е) Определение доступа Распорядителя к Счетам Клиента.

3.1 Security of the System administration bases on two-factor Administration model, requesting couple of Administrators acting together in all changes of the System. The changes, performed by 1st Administrator, require authorization by 2nd Administrator prior to the changes coming into effect.

3.2 The Client shall be bound by all actions of the Administrators and the Users in the System. Bank is not responsible for all actions of the Administrators and the Users, including actions led to state of the System not operability, unauthorized initiation of the Instructions, access to the Accounts information or additional services.

3.3 Two-factor Administration model guarantees that the System will work fully according to the Client needs, if the Administrators know the System and its' additional services, actual settings of the System, Client requests procedure related to the System; Administrators should understand further effect, which will appear from all System changes, performed by the Administrators.

3.4 The Administrators, acting together, perform following functions:

а) They prepare and pass to the Bank Electronic Banking forms CD0, CD1 and CD4.

б) They distribute new Cards and PIN mailers, received from the Bank, to the User; they make sure that Users changed their initial PIN codes after the Cards receipt.

с) They perform all System changes, including:

✓ Configuration of the System, Instructions initiation and authorization schemes; Users and Administrators rights; libraries.

✓ Configuration of the System additional services including automated files and report delivery, notifications, Delphi reports receipt.

д) Administrators should not entitle rights to Users until Users' confirmation of the Cards and PIN mailers receipt to prevent unauthorized System access of 3rd parties.

е) They perform information and technical support of the Users; they distribute System guides.

3.5 The Bank does not perform System administration.

3.6 The Bank, per Client requests, performs following functions:

а) New Cards issue for the Users.

б) New Users activation; User access termination.

с) Cards replacement for active Users.

д) Entitle administrative rights to the Users.

е) Set an access to Client Accounts for the Accessing Entity.