Редакция №1 от «20» марта 2025 г.

РЕГЛАМЕНТ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ КРЕДИТНЫХ ОРГАНИЗАЦИЙ В АО «БАНК 131» С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ ДБО БИФИТ

Version No.1 of March, 20 2025

REGULATIONS ON REMOTE BANKING SERVICES FOR CREDIT INSTITUTIONS AT BANK 131 JSC USING THE BIFIT RBS

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем Регламенте дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ (далее - Регламент) используются термины и определения, указанные в Правилах открытия и ведения корреспондентских счетов в АО «Банк 131» (и приложениях к ним), далее – Правила, Условиях осуществления информационного взаимодействия с использованием Системы информационного обмена, далее – Условия, если иное не указано в настоящем Регламенте.

Заявление – заявление Клиента, выражающее волю и намерение последнего присоединиться к Регламенту. Форма заявления определена в Приложении №1 к Регламенту.

Компрометация Электронной подписи – наличие оснований полагать, что доверие к тому, что используемые ключи/средства Электронной подписи, Аутентификационные данные, Абонентский номер и/или сами Электронные подписи или их носители утрачены/доступны неуполномоченным лицам/могут быть использованы без согласия уполномоченных лиц. К событиям, связанным с Компрометацией Электронной подписи, относятся, включая, но не ограничиваясь, следующие:

- утрата функциональных ключевых носителей, с последующим обнаружением или без такового;
- нарушение правил хранения, использования и уничтожения (в том числе после окончания срока действия) ключа Электронной подписи (усиленной неквалифицированной);
- утеря, передача и/или предоставлением доступа неуполномоченным третьим лицам к аппаратным средствам (в том числе мобильным телефонам или иным) и/или SIM-карте с Абонентским номером, в том числе который используется для направления Одноразового пароля;
- наличие подозрений, что Ключ ЭП стал известен неуполномоченным третьим лицам;
- возникновение подозрений на утечку информации или ее искажение;
- несанкционированное копирование или подозрение на копирование Статического и/или Одноразового пароля, функционального ключевого носителя, аппаратного средства и/или SIM-карты с Абонентским номером;
- прекращение полномочий или увольнение уполномоченных лиц, имеющих доступ к Ключу ЭП и(или) системе ДБО БИФИТ;
- случаи, когда нельзя достоверно установить, что произошло с носителями, содержащими ключевую информацию (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в

1.TERMS AND DEFINITIONS

In these Regulations on Remote Banking Services for Credit Institutions at Bank 131 JSC using the BIFIT RBS (hereinafter referred to as the "Regulations"), the terms and definitions specified in the Rules for Opening and Maintaining Correspondent Accounts at Bank 131 JSC (and its appendices), hereinafter referred to as the "Rules," and the Terms of Information Interaction Using the Information Exchange System, hereinafter referred to as the "Terms," shall apply, unless otherwise stated in these Regulations.

Application – A Client's application expressing the will and intention of the latter to join the Regulations. The form of the application is defined in Appendix No. 1 to the Regulations.

Compromise of an Electronic Signature – The existence of grounds to believe that the trust in the electronic signature keys/tools, authentication data, subscriber number, and/or the electronic signatures themselves or their carriers has been compromised, lost, accessed by unauthorized persons, or may be used without the consent of authorized persons. Events related to the compromise of an electronic signature include, but are not limited to, the following:

- Loss of functional key carriers, with or without subsequent discovery;
- Violation of the rules for storage, use, and destruction (including after expiration) of the electronic signature key (enhanced unqualified);
- Loss, transfer, and/or provision of access to unauthorized third parties to hardware (including mobile phones or other devices) and/or SIM cards with a subscriber number, including those used for sending a One-Time Password;
- Suspicion that the Electronic Signature Key has become known to unauthorized third parties;
- Suspicion of information leakage or distortion;
- Unauthorized copying or suspicion of copying of Static and/or One-Time Passwords, functional key carriers, hardware, and/or SIM cards with a subscriber number;
- Termination of authority or dismissal of authorized persons with access to the Electronic Signature Key and/or the BIFIT RBS;
- Cases where it is impossible to reliably determine what happened to the carriers containing key information (including cases where the carrier has malfunctioned, and it cannot be conclusively disproven that this occurred as a result of unauthorized actions by third parties, or other types of disclosure of key information).

результате несанкционированных действий третьих лиц, другие виды разглашения ключевой информации).

Клиент - иностранный банк или кредитная организация (банк или небанковская кредитная организация), признанный(-ая) таковым(-ой) в соответствии с законодательством Российской Федерации, обладающий(-ая) полной право- и дееспособностью, обратившееся(-аяся) в Банк в собственных интересах для заключения с Банком Договора об открытии и порядке ведения корреспондентского счета на условиях Правил (далее также – Договор) и Соглашения об осуществлении информационного взаимодействия с использованием Системы информационного обмена – Системы ДБО БИФИТ.

Ключ Электронной подписи (Ключ ЭП) - уникальная последовательность символов, предназначенная для создания усиленной неквалифицированной Электронной подписи.

Ключ проверки Электронной подписи - уникальная последовательность символов, однозначно связанная с Ключом Электронной подписи и предназначенная для проверки подлинности усиленной неквалифицированной Электронной подписи.

Логин – уникальная последовательность символов, состоящая из латинских букв и цифр, которая позволяет Банку однозначно идентифицировать (установить) Уполномоченного Представителя Клиента при доступе и работе в Системе ДБО БИФИТ (применяется при использовании Облачной подписи).

Одноразовый пароль – уникальная последовательность числовых символов, предоставляемая Банком по запросу Уполномоченного Представителя Клиента посредством SMS- или PUSH-сообщения на Абонентский номер Клиента (Уполномоченного Представителя Клиента), введение которого требуется для дополнительной аутентификации при доступе в Систему ДБО БИФИТ и/или дополнительного подтверждения Электронных документов при использовании усиленной неквалифицированной Электронной подписи.

Ответственный работник – работник Банка, уполномоченный на проведение идентификации Клиента и его Уполномоченного Представителя, а также на прием от Клиента документов, в том числе Заявлений от Уполномоченных Представителей Клиента, в целях регистрации, предоставления доступа и использования Системы ДБО БИФИТ Клиентом и его уполномоченными Представителями.

Оператор ЭДО - оператор электронного документооборота, соответствующий требованиям, утвержденных Приказом ФНС России от 08.06.2021 N ЕД-7-26/546@ «Об утверждении Требований к оператору электронного документооборота», и осуществляющий деятельность по обеспечению электронного документооборота между Банком и Клиентом через систему ЭДО Оператора.

Client – A foreign bank or credit institution (bank or non-bank credit organization) recognized as such under the legislation of the Russian Federation, possessing full legal capacity and capacity, applying to the Bank in its own interests to conclude an Agreement with the Bank on the opening and maintenance of a correspondent account under the terms of the Rules (hereinafter also referred to as the "Agreement") and an Agreement on Information Interaction Using the Information Exchange System – the BIFIT RBS.

Electronic Signature Key (ES Key) – A unique sequence of characters intended for creating an enhanced unqualified electronic signature.

Electronic Signature Verification Key – A unique sequence of characters uniquely associated with the Electronic Signature Key and intended for verifying the authenticity of an enhanced unqualified electronic signature.

Login – A unique sequence of characters consisting of Latin letters and numbers, which allows the Bank to uniquely identify (establish) the Authorized Representative of the Client when accessing and working in the BIFIT RBS (used when using a Cloud Signature).

One-Time Password – A unique sequence of numeric characters provided by the Bank at the request of the Authorized Representative of the Client via SMS or PUSH message to the Client's (Authorized Representative's) subscriber number, which is required for additional authentication when accessing the BIFIT RBS and/or additional confirmation of Electronic Documents when using an enhanced unqualified electronic signature.

Responsible Employee – A Bank employee authorized to identify the Client and its Authorized Representative, as well as to accept documents from the Client, including Applications from the Authorized Representatives of the Client, for the purpose of registration, granting access, and use of the BIFIT RBS by the Client and its Authorized Representatives.

EDI Operator – An electronic document interchange operator that meets the requirements approved by Order No. ЕД-7-26/546@ of the Federal Tax Service of Russia dated June 8, 2021, "On Approval of Requirements for Electronic Document Interchange Operators," and carries out activities to ensure electronic document interchange between the Bank and the Client through the EDI Operator's system.

Static Password – A secret sequence of characters known only to the Authorized Representative of the Client. The Static Password is used to log in to the BIFIT RBS and ensures that the person accessing the system is the owner of the provided Login – the Authorized Representative of the Client. The Static Password is set by the Client during

Статический пароль – секретная последовательность символов, которая известна только Уполномоченному Представителю Клиента. Статический Пароль используется для входа в Систему ДБО БИФИТ и позволяет убедиться в том, что обратившееся лицо является владельцем представленного Логина – Уполномоченным Представителем Клиента. Статический пароль задается Клиентом при регистрации и применяется при использовании Облачной подписи.

Удостоверяющий центр - организационная структура Банка, предназначенная для управления единой инфраструктурой Ключей проверки Электронной подписи с целью обеспечения юридической значимости Электронных документов и контроля целостности информации, защищенной усиленной неквалифицированной Электронной подписью, осуществляющая функции по созданию и выдаче Сертификатов ключей проверки электронных подписей, а также иные функции, в соответствии с Регламентом и законодательством Российской Федерации.

Сертификат ключа проверки электронной подписи – документ на бумажном носителе и/или в электронном виде, выданный Удостоверяющим центром, с указанным в шестнадцатеричном виде Ключом проверки Электронной подписи Клиента, подтверждающий принадлежность Ключа проверки Электронной подписи владельцу Сертификата ключа проверки электронной подписи. Сертификат ключа проверки электронной подписи должен быть подписан его владельцем (Уполномоченным Представителем Клиента).

Уполномоченный Представитель Клиента/Уполномоченное лицо – лицо, действующее от имени Клиента в силу полномочий, предоставленных ему по доверенности, на основании распорядительного акта или на основании договора, закона, или акта государственного органа, или акта органа местного самоуправления, в том числе исполнительный орган Клиента (если применимо), надлежащим образом уполномоченное на совершение юридических действий от имени Клиента и обладающее всеми необходимыми полномочиями, разрешениями, согласиями, одобрениями на совершение соответствующих действий, указанное в Заявлении о заключении Договора или Заявлении о внесении изменений в условия Договора, Заявлении, а также в Сертификате ключа проверки электронной подписи (при использовании УНЭП), в том числе, имеющее право распоряжаться денежными средствами Клиента на Счете(-ах), или имеющее право на просмотр и получение Электронных документов, в том числе выписок по Счету (без права распоряжаться денежными средствами/совершения сделок от имени Клиента).

Владелец Сертификата ключа проверки электронной подписи – Уполномоченный Представитель Клиента.

registration and is used when using a Cloud Signature.

Certification Authority – An organizational structure of the Bank designed to manage a unified infrastructure of Electronic Signature Verification Keys to ensure the legal significance of Electronic Documents and control the integrity of information protected by an enhanced unqualified electronic signature, performing functions related to the creation and issuance of Electronic Signature Verification Key Certificates, as well as other functions in accordance with the Regulations and the legislation of the Russian Federation.

Electronic Signature Verification Key Certificate – A document on paper and/or in electronic form issued by the Certification Authority, indicating in hexadecimal form the Electronic Signature Verification Key of the Client, confirming the ownership of the Electronic Signature Verification Key by the holder of the Electronic Signature Verification Key Certificate. The Electronic Signature Verification Key Certificate must be signed by its holder (the Authorized Representative of the Client).

Authorized Representative of the Client/Authorized Person – A person acting on behalf of the Client by virtue of authority granted by a power of attorney, based on a directive, contract, law, or act of a state body or local government, including the executive body of the Client (if applicable), duly authorized to perform legal actions on behalf of the Client and possessing all necessary powers, permissions, consents, and approvals to perform the relevant actions, specified in the Application for concluding the Agreement or the Application for amending the terms of the Agreement, the Application, as well as in the Electronic Signature Verification Key Certificate (when using an enhanced unqualified electronic signature), including having the right to dispose of the Client's funds in the Account(s), or having the right to view and receive Electronic Documents, including account statements (without the right to dispose of funds/conduct transactions on behalf of the Client).

Holder of the Electronic Signature Verification Key Certificate – The Authorized Representative of the Client.

Electronic Signature – Information in electronic form that is attached to or otherwise associated with other information in electronic form (the information being signed) and that is used to identify the person signing the information.

Within the framework of these Regulations, the Parties use the following types of Electronic Signatures:

Enhanced Unqualified Electronic Signature (UES) – An electronic signature that:

- Is obtained as a result of cryptographic transformation of information using the Electronic Signature Key;

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

В рамках Регламента Стороны используют следующие виды Электронных подписей:

УНЭП (Усиленная неквалифицированная Электронная подпись) - Электронная подпись, которая:

- получена в результате криптографического преобразования информации с использованием Ключа Электронной подписи;
- позволяет определить лицо, подписавшее Электронный документ;
- позволяет обнаружить факт внесения изменений в Электронный документ после момента его подписания;
- создается с использованием средств электронной подписи.

Облачная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией, и которая используется для определения лица, подписывающего информацию, хранение ключей Облачной подписи и формирование подписи под документом выполняется на удаленном сервере Банка, а не на локальных устройствах Владельца подписи. Облачная подпись относится к УНЭП.

УКЭП (усиленная квалицированная электронная подпись) - Электронная подпись, которая соответствует всем признакам УНЭП и следующим дополнительным признакам:

1) Ключ проверки Электронной подписи указан в квалифицированном сертификате;

2) для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи» (далее – №63-ФЗ).

Далее по тексту совместно УНЭП, Облачная подпись и УКЭП именуются ЭП.

Настоящий Регламент предусматривает направление заявлений, сообщений, необходимых для получения (восстановления) доступа, изменения условий использования Системы ДБО БИФИТ с использованием УКЭП внешнего аккредитованного удостоверяющего центра. УКЭП внешнего аккредитованного удостоверяющего центра используется в рамках обмена электронными документами через Оператора ЭДО.

ФКН (Функциональный ключевой носитель) - персональное средство строгой аутентификации и хранения данных, аппаратно поддерживающее работу с Ключом Электронной подписи, позволяющее осуществлять механизм электронной подписи так, что Ключ Электронной подписи не покидает пределы носителя.

Средства электронной подписи - шифровальные

- Allows identification of the person signing the Electronic Document;
- Allows detection of changes made to the Electronic Document after the moment of its signing;
- Is created using electronic signature tools.

Cloud Signature – Information in electronic form that is attached to or otherwise associated with other information in electronic form (the information being signed) and that is used to identify the person signing the information. The storage of Cloud Signature keys and the generation of the signature under the document are performed on the Bank's remote server, not on the local devices of the Signature Holder. The Cloud Signature is a type of UES.

Enhanced Qualified Electronic Signature (QES) – An electronic signature that meets all the characteristics of UES and the following additional characteristics:

1. The Electronic Signature Verification Key is specified in a qualified certificate;
2. The creation and verification of the electronic signature are performed using electronic signature tools that have received confirmation of compliance with the requirements established by Federal Law No. 63-FZ dated April 6, 2011, "On Electronic Signature" (hereinafter referred to as No. 63-FZ).

Hereinafter, UES, Cloud Signature, and QES are collectively referred to as ES.

These Regulations provide for the submission of applications, notifications, and other documents necessary for obtaining (restoring) access or changing the terms of use of the BIFIT RBS using a QES issued by an external accredited certification authority. The QES of an external accredited certification authority is used within the framework of electronic document interchange through the EDI Operator.

Functional Key Carrier (FKC) – A personal means of strict authentication and data storage, hardware-supported for working with the Electronic Signature Key, allowing the implementation of the electronic signature mechanism so that the Electronic Signature Key does not leave the carrier.

Electronic Signature Tools – Cryptographic tools used to implement at least one of the following functions: creation of an electronic signature, verification of an electronic signature, creation of an Electronic Signature Key and an Electronic Signature Verification Key.

(криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание Ключа Электронной подписи и Ключа проверки Электронной подписи.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящий Регламент регулирует отношения возникшие в процессе оказания Банком услуг в рамках Соглашения об осуществлении информационного взаимодействия с использованием Системы информационного обмена – Системы ДБО БИФИТ (далее – Система ДБО БИФИТ), при подключении и использовании Клиентом и Уполномоченными Представителями Клиента Системы ДБО БИФИТ и является соглашением между Банком и Клиентом, определяющим порядок и условия взаимодействия при выпуске и использовании Электронной подписи в рамках указанной корпоративной информационной системы электронного документооборота.

2.2. Настоящий Регламент является неотъемлемой и составной частью Правил и Условий осуществления информационного взаимодействия с использованием Систем информационного обмена.

2.3. Для подключения Клиента и Уполномоченного Представителя Клиента к Системе ДБО и ее использования Уполномоченный Представитель Клиента должен присоединиться к Правилам и Условиям осуществления информационного взаимодействия с использованием Систем информационного обмена, а также к Регламенту путем подписания Заявления.

2.4. При регистрации Уполномоченного Представителя Клиента в реестрах Системы ДБО БИФИТ Уполномоченному Представителю Клиента присваивается регистрационный номер, который указывается в Заявлении такого лица, полученном Банком.

2.5. Обмен Электронными документами между Банком и Клиентом с использованием Системы ДБО БИФИТ осуществляется в рамках Правил (включая приложения к ним), приобретенных Клиентом продуктов и услуг Банка и их условий, а также иных заключенных между Банком и Клиентом сделок (если использование Системы ДБО БИФИТ предусмотрено ими), а также при условии, что

2.GENERAL PROVISIONS

2.1. These Regulations govern the relations arising in the process of the Bank providing services under the Agreement on Information Interaction Using the Information Exchange System – the BIFIT RBS (hereinafter referred to as the "BIFIT RBS"), during the connection and use of the BIFIT RBS by the Client and the Authorized Representatives of the Client. These Regulations constitute an agreement between the Bank and the Client, defining the procedure and terms of interaction for the issuance and use of Electronic Signatures within the specified corporate electronic document management system.

2.2. These Regulations are an integral part of the Rules and the Terms of Information Interaction Using Information Exchange Systems.

2.3. To connect the Client and the Authorized Representative of the Client to the BIFIT RBS and use it, the Authorized Representative of the Client must join the Rules and the Terms of Information Interaction Using Information Exchange Systems, as well as these Regulations, by signing an Application.

2.4. Upon registration of the Authorized Representative of the Client in the registers of the BIFIT RBS, the Authorized Representative of the Client is assigned a registration number, which is indicated in the Application of such person received by the Bank.

2.5. The exchange of Electronic Documents between the Bank and the Client using the BIFIT RBS is carried out within the framework of the Rules (including their appendices), the products and services of the Bank acquired by the Client and their terms, as well as other agreements concluded between the Bank and the Client (if the use of the BIFIT RBS is provided for therein), and provided that the Client's servicing can be carried out using the BIFIT RBS.

2.6. The Client acknowledges that the BIFIT RBS used is sufficient to ensure reliable and efficient operation

обслуживание Клиента может быть осуществлено с использованием Системы ДБО БИФИТ.

2.6. Клиент признает, что используемая Система ДБО БИФИТ является достаточной для обеспечения надежной и эффективной работы при приеме, передаче, обработке и хранении информации, а используемые средства защиты информации, обеспечивающие разграничение доступа, шифрование, контроль целостности и формирование ЭП, являются достаточными для защиты от несанкционированного доступа, подтверждения авторства и подлинности информации, содержащейся в получаемых ЭД, обеспечения целостности информации, условий неотказуемости, неизменности, достоверности, отсутствия искажений, а также разрешения спорных ситуаций при условии соблюдения Сторонами мер безопасности, в том числе обеспечения Клиентом надлежащей защиты Клиентской части Системы ДБО БИФИТ от несанкционированного доступа.

2.7. Подписание бланка Сертификата ключа проверки электронной подписи Клиентом означает взаимное признание Сторонами ЭП Клиента с момента регистрации ключа проверки ЭП Владельца Сертификата в Системе ДБО БИФИТ, формирования сертификата и подтверждает получение Сертификата ключа проверки электронной подписи на бумажном носителе и/или в электронном виде посредством Системы ДБО БИФИТ.

2.8. Клиент соглашается с тем, что Электронные документы Сторон, обмен которыми осуществляется в рамках Системы ДБО БИФИТ, признаются Электронными документами, подписанными УНЭП (Облачной подписью или Усиленной неквалифицированной Электронной подписью), и являются равнозначными документам на бумажных носителях, подписанными собственноручной подписью уполномоченного лица Стороны и скрепленными печатью такой Стороны (при наличии), в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

2.9. Одной Электронной подписью могут быть подписаны несколько связанных между собой Электронных документов (пакет Электронных документов). При подписании Электронной подписью пакета Электронных документов каждый из Электронных документов, входящих в этот пакет, считается подписанным Электронной подписью того вида, которой подписан пакет Электронных документов.

2.10. Стороны признают в качестве единой шкалы времени

in receiving, transmitting, processing, and storing information, and that the information security tools used, ensuring access control, encryption, integrity control, and the generation of Electronic Signatures, are sufficient to protect against unauthorized access, confirm authorship and authenticity of the information contained in the received Electronic Documents, ensure the integrity of information, conditions of non-repudiation, immutability, reliability, absence of distortions, and resolution of disputes, provided that the Parties comply with security measures, including the Client ensuring proper protection of the Client's part of the BIFIT RBS from unauthorized access.

2.7. The signing of the Electronic Signature Verification Key Certificate form by the Client means the mutual recognition by the Parties of the Client's Electronic Signature from the moment of registration of the Electronic Signature Verification Key of the Certificate Holder in the BIFIT RBS, the formation of the certificate, and confirms the receipt of the Electronic Signature Verification Key Certificate in paper form and/or electronically through the BIFIT RBS.

2.8. The Client agrees that the Electronic Documents of the Parties, exchanged within the framework of the BIFIT RBS, are recognized as Electronic Documents signed with an Enhanced Unqualified Electronic Signature (Cloud Signature or Enhanced Unqualified Electronic Signature) and are equivalent to paper documents signed by the handwritten signature of the authorized person of the Party and sealed with the seal of such Party (if applicable), in accordance with Federal Law No. 63-FZ dated April 6, 2011, "On Electronic Signature."

2.9. Several related Electronic Documents (a package of Electronic Documents) may be signed with one Electronic Signature. When signing a package of Electronic Documents with an Electronic Signature, each of the Electronic Documents included in this package is considered signed with the type of Electronic Signature used to sign the package of Electronic Documents.

2.10. The Parties recognize the local time at the location of the Bank's division servicing the Client as the unified time scale when working in the BIFIT RBS. The control time is the system clock time of the Bank's hardware.

2.11. The Client undertakes to ensure access to and work in the BIFIT RBS only for the Authorized

при работе в Системе ДБО БИФИТ местное время по месту расположения подразделения Банка, обслуживающего Клиента. Контрольным является время системных часов аппаратных средств Банка.

2.11. Клиент обязуется обеспечить допуск к работе и работу в Системе ДБО БИФИТ только Уполномоченных Представителей Клиента, с учетом ролей таких лиц при использовании Системы ДБО БИФИТ.

2.12. Клиент осознает повышенный риск несанкционированного использования Системы ДБО БИФИТ, включая компрометацию Ключей ЭП и несанкционированное удаленное управление Системой ДБО БИФИТ, при ненадлежащем соблюдении Клиентом мер безопасности.

2.13. Используя Систему ДБО БИФИТ, Клиент приобретает возможность:

- Формировать, подписывать Электронной подписью и направлять в Банк платежные (расчетные) документы, в соответствии с законодательством Российской Федерации, в том числе платежные поручения, в целях совершения операций по открытым в Банке Счетам Клиента;
- Формировать, подписывать Электронной подписью и направлять в Банк запросы на отзыв платежных (расчетных) документов, в том числе платежных поручений, ранее переданных в Банк;
- Получать от Банка выписки по Счету(-ам) в виде Электронных документов, содержащие информацию об операциях, совершенных по открытому(-ым) в Банке Счету(-ам) Клиента;
- Формировать, направлять и получать в/от Банка информацию свободного формата в виде Электронных документов (в том числе служебно-информационных сообщений), согласно функционально-техническим возможностям Системы ДБО БИФИТ;
- Формировать, подписывать Электронной подписью, направлять и получать в/от Банка Электронные документы, в соответствии с Правилами, Условиями, приобретенными Клиентом продуктами и услугами Банка, а также в соответствии с условиями отдельных заключенных Сторонами сделок (если использование Системы ДБО БИФИТ предусмотрено последними);
- Формировать, подписывать Электронной подписью и направлять в Банк заявления (если это предусмотрено Правилами и при наличии технической возможности);
- .

2.14. При получении Электронного документа Банк производит процедуры приема к исполнению,

Representatives of the Client, taking into account the roles of such persons when using the BIFIT RBS.

2.12. The Client acknowledges the increased risk of unauthorized use of the BIFIT RBS, including the compromise of Electronic Signature Keys and unauthorized remote control of the BIFIT RBS, in case of inadequate compliance by the Client with security measures.

2.13. By using the BIFIT RBS, the Client gains the ability to:

- Prepare, sign with an Electronic Signature, and send to the Bank payment (settlement) documents in accordance with the legislation of the Russian Federation, including payment orders, for the purpose of conducting transactions on the Client's Accounts opened with the Bank;
- Prepare, sign with an Electronic Signature, and send to the Bank requests to revoke payment (settlement) documents, including payment orders, previously submitted to the Bank;
- Receive from the Bank account statements in the form of Electronic Documents containing information on transactions conducted on the Client's Accounts opened with the Bank;
- Prepare, send, and receive from the Bank free-format information in the form of Electronic Documents (including service-information messages), in accordance with the functional and technical capabilities of the BIFIT RBS;
- Prepare, sign with an Electronic Signature, send, and receive from the Bank Electronic Documents in accordance with the Rules, Terms, products, and services acquired by the Client from the Bank, as well as in accordance with the terms of individual agreements concluded by the Parties (if the use of the BIFIT RBS is provided for therein);
- Prepare, sign with an Electronic Signature, and send to the Bank applications (if provided for by the Rules and if technically possible).

2.14. Upon receipt of an Electronic Document, the Bank performs procedures for acceptance for execution, revocation, return (cancellation) of the payment (settlement) document, in accordance with the Bank's rules, including verification of:

- The right to dispose of funds (verification of the Electronic Signature, request for additional confirmation for certain payments of the Client);
- Integrity control (immutability) of the payment order details;
- Structural control (verification of the established details and the maximum number of characters in

отзыва, возврата (аннулирования) платежного (расчетного) документа, в соответствии с Банковскими правилами, в том числе проверку:

- Права распоряжения денежными средствами (проверка ЭП, запрос по отдельным платежам Клиента дополнительного подтверждения);
- Контроль целостности (неизменности) реквизитов платежного поручения;
- Структурный контроль (проверка установленных реквизитов и максимального количества символов в реквизитах платежного поручения);
- Контроль значений реквизитов;
- Контроль достаточности денежных средств.

При выявлении отрицательного результата проверки любого из вышеуказанных обстоятельств полученный ЭД Системой ДБО БИФИТ не принимается и данный результат (Электронный документ) автоматически направляется Клиенту, а поручение, содержащееся в нем, Банком не исполняется.

2.15. При получении Электронного документа Банк производит проверку УНЭП или Облачной подписи. Проверка выполняется аппаратно-программным комплексом Банка в момент подписания Уполномоченным Представителем Клиента документов в Системе ДБО БИФИТ. При положительном результате проверки электронный документ переходит из статуса «Новый» в статус «На исполнении». При отрицательном результате проверки электронный документ переходит в статус «Отвергнут» Обеспечение проверки защищенного доступа к Системе ДБО БИФИТ достигается применением защищенного протокола SSL в процессе установления соединения между web-сервером банка и Клиентом. Для подтверждения подлинности web-сервера выполняется сравнение доменного имени загружаемого web-сервера с указанным в сертификате. Протокол SSL используется в форме протокола https (прикладной протокол http поверх криптографического протокола SSL).

2.16. Формат Электронных документов определяется функционально-техническими возможностями Системы ДБО БИФИТ, экранной формы клиентской части Системы ДБО БИФИТ. Каждый Электронный документ, направляемый Клиентом в Банк с использованием Системы ДБО БИФИТ, должен содержать Электронную подпись Уполномоченного Представителя Клиента. Электронная подпись Клиента, содержащаяся в Электронном документе Клиента, подтверждает авторство Уполномоченного Представителя Клиента и является средством проверки неизменности содержания Электронного документа, так как любое изменение Электронного документа, после его подписания Электронной подписью, нарушает целостность Электронной

the payment order details);

- Control of detail values;
- Control of the sufficiency of funds.

If a negative result of the verification of any of the above circumstances is identified, the Electronic Document received by the BIFIT RBS is not accepted, and this result (Electronic Document) is automatically sent to the Client, and the instruction contained therein is not executed by the Bank.

2.15. Upon receipt of an Electronic Document, the Bank verifies the Enhanced Unqualified Electronic Signature or Cloud Signature. The verification is performed by the Bank's hardware and software complex at the moment the Authorized Representative of the Client signs the documents in the BIFIT RBS. If the verification result is positive, the Electronic Document transitions from the status "New" to the status "In Process." If the verification result is negative, the Electronic Document transitions to the status "Rejected." Secure access to the BIFIT RBS is ensured by using the SSL protocol during the establishment of a connection between the Bank's web server and the Client. To confirm the authenticity of the web server, the domain name of the loaded web server is compared with the one specified in the certificate. The SSL protocol is used in the form of the HTTPS protocol (application protocol HTTP over the cryptographic protocol SSL).

2.16. The format of Electronic Documents is determined by the functional and technical capabilities of the BIFIT RBS and the screen form of the Client's part of the BIFIT RBS. Each Electronic Document sent by the Client to the Bank using the BIFIT RBS must contain the Electronic Signature of the Authorized Representative of the Client. The Electronic Signature of the Client contained in the Electronic Document of the Client confirms the authorship of the Authorized Representative of the Client and is a means of verifying the immutability of the content of the Electronic Document, as any change to the Electronic Document after its signing with the Electronic Signature violates the integrity of the Electronic Signature.

2.17. The Electronic Document must be signed with the Electronic Signature only by the Authorized Representatives of the Client who have the right to dispose of funds in the Account (for payment (settlement) Electronic Documents), the data of which are specified in the Application for concluding the Agreement/Application for amending the terms of the Agreement and the

подписи.

2.17. Электронный документ должен быть подписан Электронной подписью только Уполномоченных Представителей Клиента, имеющих право распоряжения денежными средствами на Счете (для платежных (расчетных) Электронных документов), данные о которых указаны в Заявлении о заключении Договора/Заявлении о внесении изменений в условия Договора и Заявлении. Если Электронный документ, должен быть подписан несколькими подписями Уполномоченных Представителей Клиента, в соответствии с Заявлением о заключении Договора/Заявлении о внесении изменений в условия Договора/Карточкой с образцами подписей и оттиском печати, и Соглашением о сочетании подписей к КОП, Электронный документ должен быть подписан каждым из Уполномоченных Представителей Клиента, согласно вышеуказанным документам, по одной Электронной подписи из первой и второй группы подписей.

2.18. Система ДБО БИФИТ автоматически отображает сведения о текущем этапе обработки Клиентом и/или Банком Электронного документа, посредством присвоения Электронному документу определенного статуса и его изменения.

2.19. Система присваивает Электронным документам следующие статусы:

- **«В картотеке»** - присваивается Электронному документу, если при обработке платежа на счете Клиента оказалось недостаточно средств для совершения операции.
- **«Новый»** - присваивается при создании и сохранении нового Электронного документа Клиентом.
- **«На исполнении»** - присваивается Электронному документу при прохождении процедуры приема к исполнению, в том числе при запросе Банком от Клиента подтверждения совершаемой операции в случае использования Облачной подписи.
- **«На обработке»** - присваивается Электронному документу после его принятия к исполнению Банком.
- **«Исполнен»** - присваивается Электронному документу после его исполнения Банком (в том числе после списания денежных средств со Счета Клиента на основании данного документа).
- **«Отвергнут»** - присваивается Электронному документу, если он не может быть принят к исполнению в Банке. Для уточнения причины необходимо обратиться в Банк любым доступным Клиенту способом.

2.20. Созданный и подписанный Электронной подписью Электронный документ Клиент отправляет в Банк с

Application. If the Electronic Document must be signed with several signatures of the Authorized Representatives of the Client, in accordance with the Application for concluding the Agreement/Application for amending the terms of the Agreement/Specimen Signature Card and Seal Impression, and the Agreement on the Combination of Signatures to the COP, the Electronic Document must be signed by each of the Authorized Representatives of the Client, according to the above documents, with one Electronic Signature from the first and second groups of signatures.

2.18. The BIFIT RBS automatically displays information about the current stage of processing of the Electronic Document by the Client and/or the Bank by assigning a certain status to the Electronic Document and changing it.

2.19. The System assigns the following statuses to Electronic Documents:

- "In File" – assigned to an Electronic Document if, during the processing of the payment, there were insufficient funds in the Client's Account to complete the transaction.
- **"New" –** assigned when a new Electronic Document is created and saved by the Client.
- **"In Process" –** assigned to an Electronic Document during the acceptance for execution procedure, including when the Bank requests confirmation from the Client for the transaction being performed in case of using a Cloud Signature.
- **"Under Processing" –** assigned to an Electronic Document after its acceptance for execution by the Bank.
- **"Executed" –** assigned to an Electronic Document after its execution by the Bank (including after the debiting of funds from the Client's Account based on this document).
- **"Rejected" –** assigned to an Electronic Document if it cannot be accepted for execution by the Bank. To clarify the reason, the Client must contact the Bank by any available means.

2.20. The Client sends the created and signed Electronic Document to the Bank using the BIFIT RBS.

2.21. The Bank verifies the Electronic Document received from the Client and accepts it for execution if the verification result is positive, including the positive result of all control procedures provided for in clauses 2.14 and 2.15 of these Regulations.

2.22. The verification result of the Electronic Document

использованием Системы ДБО БИФИТ.

2.21. Банк осуществляет проверку полученного от Клиента Электронного документа и принимает его к исполнению при условии положительного результата проверки, в том числе положительного результата всех процедур контроля, предусмотренных пунктом 2.14, 2.15 настоящего Регламента.

2.22. Результат проверки Электронного документа считается положительным, если он:

- Оформлен в соответствии с действующим законодательством Российской Федерации;
- Оформлен в соответствии с нормативными документами Банка России и требованиями Банка;
- Оформлен в соответствии с требованиями, установленными заключенными Сторонами сделками, в соответствии с Правилами, и настоящим Регламентом;
- Подписан надлежащей (надлежащими) Электронной(-ыми) подписью(-ями) Уполномоченного(-ых) Представителя(-ей) Клиента, имеющего(-их) право на распоряжение денежными средствами на Счете (для платежных (расчетных) Электронных документов), Электронные подписи прошли проверку в Банке.

2.23. Клиент может отозвать переданный в Банк Электронный документ, в соответствии с требованиями законодательства Российской Федерации, заключенных Сторонами сделок, правилами совершения операций, с использованием Системы ДБО БИФИТ. Отозваны могут быть только неисполненные Электронные документы, которые не дошли до статуса «Исполнен». Если запрос на отзыв исполнен, Электронному документу присваивается статус "Исполнен." В случае невозможности исполнения запроса на отзыв, Электронному документу вернется статус, в котором Электронный документ находился до обработки Банком запроса на отзыв.

2.24. Клиент самостоятельно контролирует (отслеживает) этапы и результаты обработки отправленных в Банк Электронных документов в соответствующих разделах Системы ДБО БИФИТ.

2.25. Банк и Клиент обмениваются по Системе ДБО БИФИТ следующими Электронными документами:

- платежные поручения;
- запросы на отзыв документа;
- выписки, содержащие информацию о движении средств по счетам;
- документы для совершения валютных операций (заявления на перевод иностранной валюты, распоряжения на покупку/продажу валюты и т.п.);
- документы валютного контроля;

is considered positive if it:

- Is prepared in accordance with the current legislation of the Russian Federation;
- Is prepared in accordance with the regulatory documents of the Central Bank of Russia and the requirements of the Bank;
- Is prepared in accordance with the requirements established by the agreements concluded by the Parties, in accordance with the Rules and these Regulations;
- Is signed with the proper Electronic Signature(s) of the Authorized Representative(s) of the Client who have the right to dispose of funds in the Account (for payment (settlement) Electronic Documents), and the Electronic Signatures have been verified by the Bank.

2.23. The Client may revoke an Electronic Document submitted to the Bank in accordance with the requirements of the legislation of the Russian Federation, agreements concluded by the Parties, and the rules for conducting transactions, using the BIFIT RBS. Only unexecuted Electronic Documents that have not reached the status "Executed" may be revoked. If the revocation request is executed, the Electronic Document is assigned the status "Executed." If the revocation request cannot be executed, the Electronic Document will return to the status it was in before the Bank processed the revocation request.

2.24. The Client independently monitors (tracks) the stages and results of processing of Electronic Documents sent to the Bank in the relevant sections of the BIFIT RBS.

2.25. The Bank and the Client exchange the following Electronic Documents through the BIFIT RBS:

- Payment orders;
- Requests to revoke documents;
- Statements containing information on the movement of funds in accounts;
- Documents for conducting foreign exchange transactions (applications for foreign currency transfers, orders for the purchase/sale of currency, etc.);
- Currency control documents;
- Application for opening an Account, Application for closing an Account, Application for amending the terms of the Agreement, Application for termination of the Agreement (if technically possible);
- Other payment (settlement) documents applicable within the framework of non-cash settlement forms provided for by the legislation of the Russian

- Заявление об открытии Счета, Заявление на закрытие Счета, Заявление о внесении изменений в условия Договора, Заявление о расторжении Договора (при наличии технической возможности);
- иные платежные (расчетные) документы, применимые в рамках предусмотренных законодательством Российской Федерации и заключенных между Сторонами сделок форм безналичных расчетов (в соответствии с функциональными и техническими возможностями Системы ДБО БИФИТ);
- произвольные документы (иные документы или письма, составленные в произвольной форме).

2.26. Уполномоченному Представителю Клиента может быть предоставлен доступ к Системе ДБО БИФИТ, с возможностью получения сведений о Клиенте, его операциях, открытых в Банке банковских счетах Клиента, с правом просмотра и получения Электронных документов, в том числе выписок по счетам. В случае предоставления Уполномоченному Представителю Клиента указанного доступа в Систему ДБО БИФИТ, последний не вправе совершать операции по Счету(-ам), в т.ч. распоряжаться денежными средствами, подписывать платежные (расчетные) Электронные документы. Клиент самостоятельно осуществляет контроль за соблюдением Уполномоченными Представителями Клиента ограничений полномочий последних, неся при этом ответственность перед Банком и иными третьим лицами, а также риск возникновения неблагоприятных последствий, в том числе имущественного характера, при ненадлежащем исполнении указанной обязанности и(или) ее неисполнении.

3. ПОРЯДОК ПОДКЛЮЧЕНИЯ КЛИЕНТА К СИСТЕМЕ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

3.1. Порядок регистрации Уполномоченного Представителя Клиента в Системе ДБО БИФИТ**:**

3.1.1 Под регистрацией Уполномоченного(-ых) Представителя(-ей) Клиента понимается внесение в реестры Системы ДБО БИФИТ регистрационной информации о таком лице(-ах), на основании Заявления о заключении Договора и(или) Заявления о внесении изменений в условия Договора и Заявления.
Подача Уполномоченным Представителем Клиента Заявления осуществляется каждым таким лицом, путем обращения к Ответственному работнику по юридическому

Federation and agreements concluded between the Parties (in accordance with the functional and technical capabilities of the BIFIT RBS);
- Arbitrary documents (other documents or letters prepared in free form).

2.26. The Authorized Representative of the Client may be granted access to the BIFIT RBS, with the ability to obtain information about the Client, its transactions, bank accounts opened with the Bank, with the right to view and receive Electronic Documents, including account statements. If the Authorized Representative of the Client is granted such access to the BIFIT RBS, the latter is not entitled to conduct transactions on the Account(s), including disposing of funds, signing payment (settlement) Electronic Documents. The Client independently monitors the compliance of the Authorized Representatives of the Client with the restrictions on their powers, bearing responsibility to the Bank and other third parties, as well as the risk of adverse consequences, including property consequences, in case of improper performance or non-performance of this obligation.

3. PROCEDURE FOR CONNECTING THE CLIENT TO THE REMOTE BANKING SERVICE SYSTEM

3.1. Procedure for Registering the Authorized Representative of the Client in the BIFIT RBS:

3.1.1. The registration of the Authorized Representative(s) of the Client refers to the entry of registration information about such person(s) into the registers of the BIFIT RBS, based on the Application for concluding the Agreement and/or the Application for amending the terms of the Agreement and the Application.
The submission of the Application by the Authorized Representative of the Client is carried out by each such person by contacting the

адресу Банка в течение Операционного времени Банка.

3.1.1.1.В Заявлении Уполномоченный Представитель клиента указывает специальную парольную фразу, которая в дальнейшем может быть использована для дополнительной идентификации Клиента.

3.1.2 Прохождение Уполномоченным Представителем Клиента самостоятельной предварительной регистрации в Системе ДБО БИФИТ требуется в случае, если Клиент не подключен к Системе ДБО БИФИТ.

3.1.3 При приеме Заявления Ответственный работник идентифицирует Уполномоченного Представителя Клиента, с использованием документов, удостоверяющих личность последнего (оригиналы или нотариально заверенные копии), и документов, подтверждающих полномочия указанных лиц на использование аналогов собственноручной подписи (Электронной подписи) от имени Клиента (оригиналы или заверенные в установленном Банком порядке копии с предоставлением оригиналов для сверки, если ранее данные документы в Банк не представлялись).

3.1.4 Заявление Уполномоченного Представителя Клиента принимается Ответственным работником после проведения Идентификации такого Представителя Клиента, о чем проставляется соответствующая отметка на Заявлении. Банк вправе отказать в приеме Заявления без объяснения причин такого отказа. Отказ в приеме Заявления влечет отказ в регистрации Уполномоченного Представителя Клиента в Системе ДБО БИФИТ.

3.1.5 При выборе Клиентом метода работы в Системе ДБО БИФИТ с использованием Облачной подписи или УНЭП Ответственный работник направляет на указанный в Заявлении о заключении Договора и(или) Заявлении о внесении изменений в условия Договора адрес электронной почты Уполномоченного Представителя Клиента ссылку для прохождения саморегистрации Клиента в Системе ДБО БИФИТ. Процесс саморегистрации описан в инструкции по работе с Системой ДБО БИФИТ, размещенной на сайте https://help.131.ru/

Responsible Employee at the legal address of the Bank during the Bank's operating hours.

3.1.1.1. In the Application, the Authorized Representative of the Client specifies a special passphrase, which may subsequently be used for additional identification of the Client.

3.1.2. Independent preliminary registration of the Authorized Representative of the Client in the BIFIT RBS is required if the Client is not connected to the BIFIT RBS.

3.1.3. When accepting the Application, the Responsible Employee identifies the Authorized Representative of the Client using identity documents (originals or notarized copies) and documents confirming the authority of such persons to use analogues of handwritten signatures (Electronic Signatures) on behalf of the Client (originals or copies certified in the manner established by the Bank, with the provision of originals for verification if such documents have not previously been submitted to the Bank).

3.1.4. The Application of the Authorized Representative of the Client is accepted by the Responsible Employee after the identification of such Representative of the Client, as indicated by the corresponding mark on the Application. The Bank has the right to refuse to accept the Application without explaining the reasons for such refusal. Refusal to accept the Application results in the refusal to register the Authorized Representative of the Client in the BIFIT RBS.

3.1.5. If the Client chooses the method of working in the BIFIT RBS using a Cloud Signature or an Enhanced Unqualified Electronic Signature (UES), the Responsible Employee sends a link for self-registration of the Client in the BIFIT RBS to the email address of the Authorized Representative of the Client specified in the Application for concluding the Agreement and/or the Application for amending the terms of the Agreement. The self-registration process is described in the instructions for working with the BIFIT RBS, available on the website: https://help.131.ru/.

3.1.5.1. The Electronic Signature Verification Key Certificate is stored in containers—separate files in a specific format on the Bank's internal servers. Each container is encrypted with a key created based on a password set by the owner of the Cloud Signature key.

3.2. If the Client chooses the method of working in the BIFIT RBS using an Enhanced Unqualified Electronic Signature (UES) stored on a Functional

3.1.5.1 Сертификат ключа проверки электронной подписи хранится в контейнерах – отдельных файлах в формате на внутренних серверах Банка. Каждый контейнер зашифрован ключом, созданным на основе пароля, установленного владельцем ключа Облачной подписи.

3.2. При выборе Клиентом метода работы в Системе ДБО БИФИТ с использованием УНЭП, хранящейся на ФКН, Ответственный работник передает должным образом упакованный ФКН Уполномоченному Представителю Клиента.

3.3. Факт передачи ФКН, а также целостность упаковки подтверждается собственноручной подписью Уполномоченного Представителя Клиента в Акте приема-передачи ФКН Системы ДБО БИФИТ. Форма Акта определяется Банком в Приложении №2 к настоящему Регламенту. В случае нарушения целостности упаковки ФКН Уполномоченный Представитель Клиента должен указать об этом в Акте. При отсутствии соответствующей отметки в Акте, Стороны определили считать целостность упаковки ФКН не нарушенной, а сам ФКН надлежащим образом полученным Уполномоченным Представителем Клиента.

3.4. Уполномоченный Представитель Клиента при использовании Системы ДБО БИФИТ и обмене Электронными документами через нее вправе использовать указанный в Заявлении метод работы (способ подписания Электронных документов, с учетом функциональных возможностей Системы ДБО БИФИТ) с использованием УНЭП. В рамках обмена Электронными документами с использованием Системы ДБО БИФИТ информационное взаимодействие между Банком и Клиентом осуществляется с использованием Электронных подписей, выпущенных в Системе ДБО БИФИТ.

3.5. Клиент (его Уполномоченный Представитель) считается подключенным к Системе ДБО БИФИТ, а Уполномоченный Представитель Клиента имеет возможность пользоваться Системой ДБО БИФИТ при наступлении следующих событий:

- при использовании Облачной подписи с момента саморегистрации Уполномоченного Представителя Клиента в Системе ДБО БИФИТ в порядке, предусмотренном п. 3.1.5 Регламента, и предоставлению Банком доступа Уполномоченному представителю Клиента в Систему ДБО БИФИТ.

Key Carrier (FKC), the Responsible Employee transfers the properly packaged FKC to the Authorized Representative of the Client.

3.3. The fact of transfer of the FKC, as well as the integrity of the packaging, is confirmed by the handwritten signature of the Authorized Representative of the Client in the Act of Acceptance and Transfer of the FKC of the BIFIT RBS. The form of the Act is determined by the Bank in Appendix No. 2 to these Regulations. If the integrity of the FKC packaging is violated, the Authorized Representative of the Client must indicate this in the Act. In the absence of such a note in the Act, the Parties agree to consider the integrity of the FKC packaging as not violated and the FKC as properly received by the Authorized Representative of the Client.

3.4. The Authorized Representative of the Client, when using the BIFIT RBS and exchanging Electronic Documents through it, has the right to use the method of work specified in the Application (method of signing Electronic Documents, taking into account the functional capabilities of the BIFIT RBS) using an Enhanced Unqualified Electronic Signature (UES). Within the framework of exchanging Electronic Documents using the BIFIT RBS, information interaction between the Bank and the Client is carried out using Electronic Signatures issued in the BIFIT RBS.

3.5. The Client (its Authorized Representative) is considered connected to the BIFIT RBS, and the Authorized Representative of the Client has the opportunity to use the BIFIT RBS upon the occurrence of the following events:

- When using a Cloud Signature, from the moment of self-registration of the Authorized Representative of the Client in the BIFIT RBS in the manner provided for in clause 3.1.5 of the Regulations, and the Bank's provision of access to the Authorized Representative of the Client to the BIFIT RBS. This condition applies to Authorized Representatives of the Client authorized to dispose of funds/conduct transactions (when using a Cloud Signature), as well as to Authorized Representatives of the Client authorized to view and receive Electronic Documents, including account statements (without the right to dispose of funds/conduct transactions on behalf of the Client);
- When using an Enhanced Unqualified Electronic Signature (UES) on an FKC, after receiving notification of the issuance of the Electronic Signature Verification Key Certificate and completion of the procedure for generating the

Указанное условие применяется в отношении Уполномоченных Представителей Клиента, наделенных правом распоряжаться денежными средствами/совершения сделок (при использовании Облачной подписи), а также в отношении Уполномоченных Представителей Клиента, наделенных полномочиями на просмотр и получение Электронных документов, в том числе выписок по Счету (без права распоряжаться денежными средствами/совершения сделок от имени Клиента);

- при использовании УНЭП на ФКН после получения уведомления о выпуске Сертификата ключа проверки Электронной подписи и завершения процедуры формирования Электронной подписи средствами Системы ДБО БИФИТ Уполномоченным Представителем Клиента.

3.6. По истечении срока полномочий Уполномоченного Представителя Клиента Банк блокирует доступ такого Уполномоченного Представителя Клиента к Системе ДБО БИФИТ.

3.7. Клиент вправе установить ограничения по параметрам операций, которые могут осуществляться Клиентом с использованием Системы ДБО БИФИТ в заявлении, форма которого определяется Банком и размещена на ресурсе https://131.ru/contracts и в офисе Банка. Прием заявления в Банк осуществляется с использованием Системы ДБО БИФИТ.

3.8. Одноразовый пароль автоматически генерируется Системой ДБО БИФИТ, в том числе в целях дополнительной аутентификации Уполномоченного Представителя Клиента при предоставлении ему доступа в Систему ДБО БИФИТ и/или дополнительного подтверждения Электронного документа. Уполномоченный Представитель Клиента должен ввести полученный Одноразовый пароль для прохождения процедуры аутентификации и/или дополнительного подтверждения Электронного документа.

3.9. Одноразовый пароль направляется Банком на Абонентский номер Уполномоченного Представителя Клиента, указанный в программно-аппаратном комплексе Банка на основании сведений, содержащихся в Заявлении о заключении Договора и(или) Заявлении о внесении изменений в условия Договора, Заявлении или Заявлении о смене Абонентского номера.

3.10. Порядок смены Логина и Статического пароля в Системе ДБО БИФИТ.

3.10.1 Уполномоченный Представитель Клиента

Electronic Signature by the Authorized Representative of the Client using the BIFIT RBS.

3.6. Upon the expiration of the authority of the Authorized Representative of the Client, the Bank blocks such Authorized Representative's access to the BIFIT RBS.

3.7. The Client has the right to set restrictions on the parameters of transactions that can be carried out by the Client using the BIFIT RBS in the Application, the form of which is determined by the Bank and is available on the resource https://131.ru/contracts and in the Bank's office. The acceptance of the Application by the Bank is carried out using the BIFIT RBS.

3.8. A One-Time Password is automatically generated by the BIFIT RBS, including for the purpose of additional authentication of the Authorized Representative of the Client when granting access to the BIFIT RBS and/or additional confirmation of the Electronic Document. The Authorized Representative of the Client must enter the received One-Time Password to complete the authentication procedure and/or additional confirmation of the Electronic Document.

3.9. The One-Time Password is sent by the Bank to the subscriber number of the Authorized Representative of the Client specified in the Bank's hardware and software complex based on the information contained in the Application for concluding the Agreement and/or the Application for amending the terms of the Agreement, the Application, or the Application for changing the Subscriber Number.

3.10. Procedure for Changing the Login and Static Password in the BIFIT RBS:

3.10.1. The Authorized Representative of the Client may independently change the Login and Static Password in the BIFIT RBS, except in the case of their loss. If the Static Password is lost, the Authorized Representative of the Client can independently request a link to reset the password on the authorization page of the BIFIT RBS, which will be sent to the email address specified in the Application for concluding the Agreement and/or the Application for amending the terms of the Agreement. If both the Static Password and Login are lost, the Authorized Representative of the Client must immediately contact the Bank to block access, in accordance with Section 8 of the Regulations. To restore access to the BIFIT RBS, the Authorized Representative of the Client may personally contact the Bank with an Application to

может самостоятельно изменить Логин и Статический пароль в Системе ДБО БИФИТ, за исключением случая их утраты. В случае утраты Статического пароля Уполномоченный Представитель Клиента на странице авторизации в Системе ДБО БИФИТ может самостоятельно запросить ссылку для восстановления пароля, которая будет направлена на указанный в Заявлении о заключении Договора и(или) Заявлении о внесении изменений в условия Договора адрес электронной почты. В случае утраты Статического пароля и Логина Уполномоченный Представитель Клиента обязан незамедлительно обратиться в Банк для блокирования доступа, в соответствии с разделом 8 Регламента. Для восстановления доступа в Систему ДБО БИФИТ Уполномоченный Представитель Клиента может лично обратиться в Банк с Заявлением о смене логина и/или пароля /разблокировке доступа в Системе ДБО БИФИТ, форма которого определяется Банком и размещена на ресурсе https://131.ru/contracts и в офисе Банка, и документом, удостоверяющим его личность, либо провести смену дистанционным способом.

3.10.2. Для дистанционной смены Логина и Статического пароля Уполномоченный Представитель Клиента должен направить в Банк с адреса электронной почты, указанного в Заявлении о заключении Договора и(или) Заявлении о внесении изменений в условия Договора, Заявлении, сканированную копию подписанного Заявления о смене логина и статического пароля по следующим контактным данным: dbo@131.ru. Для обработки Заявления о смене логина и статического пароля Ответственный работник Банка связывается с Уполномоченным Представителем Клиента с использованием контактных данных, указанных Уполномоченным Представителем Клиента в Заявлении о заключении Договора и(или) Заявлении о внесении изменений в условия Договора, Заявлении. При этом, Уполномоченный Представитель Клиента должен сообщить уполномоченному работнику Банка следующую информацию:

- свои идентификационные данные;
- специальную парольную фразу.

Аутентификация заявителя при подаче запроса на смену Логина и Статического пароля в Системе ДБО БИФИТ - Уполномоченного Представителя Клиента осуществляется по специальной парольной фразе, содержащейся в Заявлении. После успешной

change the Login and/or Password/unblock access to the BIFIT RBS, the form of which is determined by the Bank and is available on the resource https://131.ru/contracts and in the Bank's office, and provide an identity document, or carry out the change remotely.

3.10.2. For remote change of the Login and Static Password, the Authorized Representative of the Client must send to the Bank, from the email address specified in the Application for concluding the Agreement and/or the Application for amending the terms of the Agreement, the Application, a scanned copy of the signed Application to change the Login and Static Password to the following contact details: dbo@131.ru. To process the Application to change the Login and Static Password, the Responsible Employee of the Bank contacts the Authorized Representative of the Client using the contact details specified by the Authorized Representative of the Client in the Application for concluding the Agreement and/or the Application for amending the terms of the Agreement, the Application. In this case, the Authorized Representative of the Client must provide the authorized employee of the Bank with the following information:

- Their identification data;
- The special passphrase.

Authentication of the applicant when submitting a request to change the Login and Static Password in the BIFIT RBS—the Authorized Representative of the Client—is carried out based on the special passphrase contained in the Application. After successful authentication, the Responsible Employee of the Bank sends an invitation link for a video call to the contact details of the Authorized Representative of the Client for additional authentication. If the identification and authentication procedures are successfully completed, the Authorized Representative of the Client performs self-registration in the BIFIT RBS again in the manner provided for in clause 3.1.5 of the Regulations, and the Responsible Employee processes the Application in accordance with clause 3.1 of the Regulations.

3.11. Procedure for Changing the Subscriber Number Used to Receive the One-Time Password: 3.11.1. To change the Subscriber Number of the Authorized Representative of the Client used to receive the One-Time Password, such Authorized Representative of the Client must contact the Bank

аутентификации Ответственный работник Банка направляет на контактные данные Уполномоченного лица Клиента ссылку-приглашение на видеозвонок, в целях проведения дополнительной аутентификации. В случае проведения успешных процедур идентификации и аутентификации Уполномоченный Представитель Клиента производит повторную саморегистрацию в Системе ДБО БИФИТ в порядке, предусмотренном п. 3.1.5 Регламента, а Ответственный работник обрабатывает заявление, в соответствии с п. 3.1. Регламента.

3.11. Порядок смены Абонентского номера используемого для получения Одноразового пароля.

3.11.1. Для изменения Абонентского номера Уполномоченного Представителя Клиента, используемого для получения Одноразового пароля такой Уполномоченный Представитель Клиента должен обратиться в Банк и предоставить Заявление на изменение Абонентского номера с предоставлением удостоверяющих личность документов. Если Абонентский номер меняет Уполномоченный Представитель Клиента, уполномоченный подписывать договоры/заявления, он может подписать только Заявление на изменение Абонентского номера (Приложение №3 к настоящему Регламенту) БИФИТ», указав в нем, что подтверждает принадлежность ему Абонентского номера.

3.11.2. Для дистанционной смены Абонентского номера Уполномоченный Представитель Клиента направляет Заявление о смене Абонентского номера посредством Системы ДБО БИФИТ, выбрав необходимый шаблон документа. Заявление должно быть подписано УНЭП обратившегося Уполномоченного Представителя Клиента. Дистанционная смена Абонентского номера возможна при наличии полномочий Уполномоченного Представителя Клиента подписывать и подать в Банк документы, заявления, сообщения, необходимые для регистрации, получения доступа, изменения условий использования Системы ДБО БИФИТ. Дистанционная смена Абонентского номера невозможна в случае Компрометации Электронной подписи или подозрений на Компрометацию Электронной подписи.

3.11.3. Смена Абонентского номера Уполномоченного Представителя Клиента осуществляется только после положительного завершения проверки представленных сведений и документов. Банк вправе отказать Клиенту в смене Абонентского номера Уполномоченного

and provide an Application to change the Subscriber Number along with identity documents. If the Subscriber Number is being changed by the Authorized Representative of the Client authorized to sign agreements/applications, they may only sign the Application to change the Subscriber Number (Appendix No. 3 to these Regulations), indicating that they confirm the ownership of the Subscriber Number.

3.11.2. For remote change of the Subscriber Number, the Authorized Representative of the Client sends an Application to change the Subscriber Number through the BIFIT RBS by selecting the appropriate document template. The Application must be signed with an Enhanced Unqualified Electronic Signature (UES) of the Authorized Representative of the Client submitting the request. Remote change of the Subscriber Number is possible if the Authorized Representative of the Client has the authority to sign and submit to the Bank documents, applications, and notifications necessary for registration, access, and changes to the terms of use of the BIFIT RBS. Remote change of the Subscriber Number is not possible in case of compromise or suspicion of compromise of the Electronic Signature.

3.11.3. The change of the Subscriber Number of the Authorized Representative of the Client is carried out only after the successful completion of the verification of the submitted information and documents. The Bank has the right to refuse the Client to change the Subscriber Number of the Authorized Representative of the Client without explaining the reasons for such refusal.

3.12. If there is technical capability of the Bank and the Client, it is allowed to send the Application to change the Login and/or Static Password, the Application to change the Subscriber Number, the Application to open an Account, the Application to close an Account, the Application to amend the terms of the Agreement, and the Application to terminate the Agreement through the EDI Operator agreed with the Bank. In this case, the Application to change the Login and Static Password and the Application to change the Subscriber Number must be signed with an Enhanced Qualified Electronic Signature (QES) of the Authorized Representative of the Client specified in these applications. The Application to open an Account, the Application to close an Account, the Application to amend the terms of the Agreement, and the Application to terminate the Agreement

Представителя Клиента без объяснения причин такого отказа.

3.12. При наличии технической возможности Банка и Клиента допускается направление Заявления о смене логина и/или статического пароля, Заявления на изменение Абонентского номера, Заявления об открытии Счета, Заявления о закрытии Счета, Заявления о внесении изменений в условия Договора, Заявление о расторжении Договора через Оператора ЭДО, согласованную с Банком. В таком случае, Заявление о смене логина и статического пароля и Заявление на изменение Абонентского номера должны быть подписаны УКЭП Уполномоченного Представителя Клиента, указанного в этих заявлениях. Заявление Заявления об открытии Счета, Заявления о закрытии Счета, Заявления о внесении изменений в условия Договора, Заявление о расторжении Договора должно быть подписано УКЭП Уполномоченного Представителя Клиента и имеющего полномочия подписывать и подавать в Банк документы, заявления, сообщения, необходимые для регистрации, получения доступа, изменения условия использования Системы ДБО БИФИТ. В случае предоставления Клиентом через Оператора ЭДО Заявления о смене логина и/или статического пароля или Заявления на изменение Абонентского номера проводится идентификация и аутентификация Уполномоченного Представителя Клиента в соответствии с п.3.1.4 Регламента.

3.13. Для изменения специальной парольной фразы Уполномоченный Представитель Клиента должен лично обратиться в Банк с Заявлением в свободной форме с предоставлением удостоверяющих личность документов.

4. ПОРЯДОК ВЫПУСКА СЕРТИФИКАТОВ ПРОВЕРКИ КЛЮЧЕЙ ЭЛЕКТРОННОЙ ПОДПИСИ

4.1 Для получения Сертификата ключа проверки электронной подписи для работы в Системе ДБО БИФИТ и осуществления обмена Электронными документами с использованием УНЭП, каждый Уполномоченный Представитель Клиента, данные о котором указаны в Заявлении о заключении Договора и(или) Заявлении о внесении изменений в условия Договора и Заявлении, Карточке с образцами подписей (при её оформлении в соответствии с Правилами), прошедший Идентификацию у Ответственного работника Банка, должен лично:

must be signed with an Enhanced Qualified Electronic Signature (QES) of the Authorized Representative of the Client who has the authority to sign and submit to the Bank documents, applications, and notifications necessary for registration, access, and changes to the terms of use of the BIFIT RBS. If the Client submits the Application to change the Login and/or Static Password or the Application to change the Subscriber Number through the EDI Operator, the identification and authentication of the Authorized Representative of the Client are carried out in accordance with clause 3.1.4 of the Regulations.

3.13. To change the special passphrase, the Authorized Representative of the Client must personally contact the Bank with an Application in free form, providing identity documents.

4. PROCEDURE FOR ISSUING ELECTRONIC SIGNATURE VERIFICATION KEY CERTIFICATES

4.1. To obtain an Electronic Signature Verification Key Certificate for working in the BIFIT RBS and exchanging Electronic Documents using an Enhanced Unqualified Electronic Signature (UES), each Authorized Representative of the Client, whose details are specified in the Application for concluding the Agreement and/or the Application for amending the terms of the Agreement and the Application, the Specimen Signature Card (if issued in accordance with the Rules), and who has undergone identification by the Responsible Employee of the Bank, must personally:

- Create an Electronic Signature Verification Key

- создать с помощью средств Системы ДБО БИФИТ Сертификат ключа проверки электронной подписи, в электронном виде и на бумажном носителе;
- подписать и направить в Банк сканированную копию данного Сертификата на электронный почтовый ящик dbo@131.ru;
- предоставить в Банк данный Сертификат на бумажном носителе, заверенный собственноручной подписью такого Уполномоченного Представителя Клиента в течение 2 (Двух) рабочих дней, либо предоставить уникальный идентификатор, который присваивается почтовым отправлениям, выдаваемый транспортной компанией, осуществляющей отправку оригиналов документов, либо направить экземпляры документов посредством Оператора ЭДО.

Инструкция по подключению к Системе ДБО БИФИТ и генерации ключей УНЭП размещена на ресурсе https://help.131.ru/ и в офисе Банка. Сертификат ключа проверки электронной подписи в обязательном порядке должен содержать: полные ФИО Уполномоченного Представителя Клиента (владельца Сертификата ключа проверки электронной подписи), наименование Клиента, адрес местонахождения, уникальный номер сертификата ключа проверки электронной подписи, даты начала и окончания срока действия такого сертификата, уникальный ключ проверки электронной подписи, наименование используемого средства электронной подписи и (или) стандарты, требованиям которых соответствуют ключ электронной подписи и ключ проверки электронной подписи, наименование Удостоверяющего центра. В рамках настоящего Регламента и Сертификата ключа проверки ЭП уникальным номером сертификата является идентификатор ключа проверки ЭП, указанный в выданном Сертификате. Также в рамках настоящего Регламента и Сертификата ключа проверки ЭП наименованием Удостоверяющего центра является наименование Банка, указанное в выданном Сертификате. Не допускается внесение каких-либо изменений в Сертификат ключа проверки электронной подписи, сформированный с использованием средств Системы ДБО БИФИТ.

4.2 При поступлении в Банк запроса на активацию Сертификата ключа проверки электронной подписи в электронном виде, Ответственный работник Банка сверяет данные, содержащиеся в указанном запросе в электронном виде с данными, указанными в запросе, представленном Клиентом на электронный почтовый ящик dbo@131.ru.

4.3 При положительном результате проверки Банк обрабатывает поступивший запрос на активацию и осуществляет активацию Сертификата ключа проверки электронной подписи. При отрицательном результате проведенной проверки активация Сертификата ключа

Certificate, both in electronic form and on paper, using the tools of the BIFIT RBS;
- Sign and send a scanned copy of this Certificate to the Bank's email address: dbo@131.ru;
- Provide the Bank with this Certificate on paper, certified by the handwritten signature of such Authorized Representative of the Client, within 2 (two) business days, or provide a unique identifier assigned to the shipment by the transport company delivering the original documents, or send the documents via the EDI Operator.

The instructions for connecting to the BIFIT RBS and generating UES keys are available on the resource https://help.131.ru/ and in the Bank's office. The Electronic Signature Verification Key Certificate must contain the following mandatory information: the full name of the Authorized Representative of the Client (holder of the Electronic Signature Verification Key Certificate), the name of the Client, the address of the location, the unique number of the Electronic Signature Verification Key Certificate, the start and end dates of the validity of such certificate, the unique Electronic Signature Verification Key, the name of the electronic signature tool used and/or the standards to which the electronic signature key and the electronic signature verification key comply, and the name of the Certification Authority. Within the framework of these Regulations and the Electronic Signature Verification Key Certificate, the unique number of the certificate is the Electronic Signature Verification Key identifier specified in the issued Certificate. Also, within the framework of these Regulations and the Electronic Signature Verification Key Certificate, the name of the Certification Authority is the name of the Bank specified in the issued Certificate. No changes are allowed to the Electronic Signature Verification Key Certificate generated using the tools of the BIFIT RBS.

4.2. Upon receipt of a request for the activation of the Electronic Signature Verification Key Certificate in electronic form, the Responsible Employee of the Bank compares the data contained in the specified electronic request with the data indicated in the request submitted by the Client to the email address dbo@131.ru.

4.3. If the verification result is positive, the Bank processes the received activation request and activates the Electronic Signature Verification Key Certificate. If the verification result is negative, the activation of the Electronic Signature Verification Key Certificate is not carried out, and the Responsible Employee of the Bank informs the Client of this. The Bank has the right not to inform the Client/its

проверки электронной подписи не осуществляется, информация об этом передается Клиенту Ответственным работником Банка. Банк вправе не сообщать Клиенту/его Уполномоченному Представителю о причинах отказа в активации Сертификата ключа проверки электронной подписи.

4.4 Активация Сертификатов ключей проверки электронной подписи осуществляется исключительно на основании полученной Банком информации от Уполномоченного Представителя Клиента, которая содержит сведения, необходимые для идентификации владельца Сертификата ключа проверки электронной подписи, при условии выполнения положений 4.1. – 4.3. Регламента.

4.5 По окончании процедуры активации Сертификата ключа проверки электронной подписи, Уполномоченный Представитель Клиента получает возможность, используя программные средства Системы ДБО БИФИТ, завершить процедуру активации УНЭП и приступить к ее эксплуатации.

4.6 Каждому Уполномоченному Представителю Клиента необходимо отдельно создать Сертификат ключа проверки электронной подписи.

4.7 Сертификат ключа проверки электронной подписи подлежит отзыву Банком в случае:

- компрометации Электронной подписи владельца Сертификата ключа проверки электронной подписи, соответствующего данному сертификату;
- получения владельцем нового Сертификата ключа проверки электронной подписи.

Authorized Representative of the reasons for refusing to activate the Electronic Signature Verification Key Certificate.

4.4. Activation of Electronic Signature Verification Key Certificates is carried out solely on the basis of the information received by the Bank from the Authorized Representative of the Client, which contains the data necessary to identify the holder of the Electronic Signature Verification Key Certificate, provided that the provisions of clauses 4.1–4.3 of these Regulations are fulfilled.

4.5. Upon completion of the activation procedure for the Electronic Signature Verification Key Certificate, the Authorized Representative of the Client gains the ability, using the software tools of the BIFIT RBS, to complete the activation procedure for the UES and begin its use.

4.6. Each Authorized Representative of the Client must separately create an Electronic Signature Verification Key Certificate.

4.7. The Electronic Signature Verification Key Certificate is subject to revocation by the Bank in the following cases:

- Compromise of the Electronic Signature of the holder of the Electronic Signature Verification Key Certificate corresponding to this certificate;
- Receipt of a new Electronic Signature Verification Key Certificate by the holder.

5. ПОРЯДОК ИСПОЛЬЗОВАНИЯ ОБЛАЧНОЙ ПОДПИСИ

5.1. В качестве средства подтверждения Электронного документа, подписанного Облачной подписью, используется Логин, Статический пароль, а также идентификатор ключа облачной ЭП.

5.2. В целях направления Уполномоченным Представителем Клиента Банку Электронного документа, Уполномоченный Представитель Клиента следуя инструкциям в экранных формах веб-интерфейса Системы ДБО БИФИТ, используя функциональные кнопки, инициирует подписание соответствующего Электронного документа:

а) Уполномоченный Представитель Клиента вводит необходимые данные, которые запрашивает

5. PROCEDURE FOR USING THE CLOUD SIGNATURE

5.1 As a means of confirming an Electronic Document signed with a Cloud Signature, the Login, Static Password, and the Cloud Electronic Signature Key Identifier are used.

5.2. To send an Electronic Document to the Bank, the Authorized Representative of the Client, following the instructions in the screen forms of the web interface of the BIFIT RBS and using functional buttons, initiates the signing of the corresponding Electronic Document:

a) The Authorized Representative of the Client enters the necessary data requested by the BIFIT RBS interface, using functional buttons and input fields.

интерфейс Системы ДБО БИФИТ, используя функциональные кнопки и поля для ввода информации.

b) Перед подписанием Электронного документа Уполномоченный Представитель Клиента обязан ознакомиться с ним и быть согласным с его содержанием в полном объеме и в случае согласия с текстом сообщения подтвердить подписание Электронного документа. В случае несогласия с текстом сообщения Уполномоченный Представитель Клиента должен отказаться от подтверждения подписания Электронного документа.

c) Для подписания сформированного Электронного документа посредством интерфейса Системы ДБО БИФИТ, Уполномоченный Представитель Клиента инициирует процесс подписания Электронного документа после проверки его содержания, и направляет Банку посредством интерфейса Системы ДБО БИФИТ запрос на подписание Электронного документа, содержащий Электронный документ

d) на мобильное устройство Уполномоченного Представителя Клиента направляется СМС или PUSH-сообщение о необходимости подписания Электронного документа.

e) Далее Уполномоченный Представитель Клиента в случае согласия с текстом сообщения на экранной форме должен ввести полученный одноразовый код в соответствующее поле экранной формы. В случае несогласия Уполномоченный Представитель Клиента должен не осуществлять ввод одноразового кода в соответствующее поле, закрыв экранную форму.

f) Для подписания сформированного Электронного документа посредством Облачной подписи Уполномоченный Представитель Клиента нажимает соответствующую электронную кнопку в интерфейсе Системы ДБО БИФИТ.

g) С момента нажатия Уполномоченным Представителем Клиента специальной функциональной кнопки в интерфейсе Системы ДБО БИФИТ Электронный документ считается подписанным Клиентом и направленным в Банк.

h) Полученный Банком запрос из интерфейса Системы ДБО БИФИТ расценивается как обращение за контейнером, содержащим ключ Облачной подписи.

i) Уполномоченный Представитель Клиента обязан обеспечить отсутствие доступа третьих лиц к идентификатору и паролю от Облачной подписи.

j) Электронный документ считается подписанным Облачной подписью и подлинным (исходящим от Уполномоченного Представителя Клиента) при одновременном соблюдении следующих условий: (1)

b) Before signing the Electronic Document, the Authorized Representative of the Client must review it and agree with its content in full. If in agreement with the text of the message, the Authorized Representative of the Client confirms the signing of the Electronic Document. If not in agreement, the Authorized Representative of the Client must refuse to confirm the signing of the Electronic Document.

c) To sign the generated Electronic Document through the BIFIT RBS interface, the Authorized Representative of the Client initiates the signing process after verifying its content and sends a request to the Bank through the BIFIT RBS interface to sign the Electronic Document, containing the Electronic Document.

d) An SMS or PUSH notification is sent to the mobile device of the Authorized Representative of the Client, requesting the signing of the Electronic Document.

e) Next, if the Authorized Representative of the Client agrees with the text of the message on the screen form, they must enter the received one-time code in the corresponding field of the screen form. If they do not agree, the Authorized Representative of the Client must not enter the one-time code and should close the screen form.

f) To sign the generated Electronic Document using the Cloud Signature, the Authorized Representative of the Client presses the corresponding electronic button in the BIFIT RBS interface.

g) From the moment the Authorized Representative of the Client presses the special functional button in the BIFIT RBS interface, the Electronic Document is considered signed by the Client and sent to the Bank.

h) The request received by the Bank from the BIFIT RBS interface is regarded as a request for a container containing the Cloud Signature Key.

i) The Authorized Representative of the Client must ensure that third parties do not have access to the Cloud Signature identifier and password.

j) The Electronic Document is considered signed with the Cloud Signature and authentic (originating from the Authorized Representative of the Client) if the following conditions are simultaneously met: (1) the Electronic Document has been received by the Bank, (2) the Electronic Document contains the Electronic Signature of the Authorized Representative of the Client, the verification result of which matches the key identifier.

To change the Cloud Signature Key, the Authorized Representative of the Client must activate the Cloud Signature Key in accordance with clause 4.1 of these Regulations.

Электронный документ получен Банком, (2) Электронный документ содержит Электронную подпись Уполномоченного Представителя Клиента, результат проверки которой совпадает с идентификатором ключа.

Для смены ключа Облачной подписи Уполномоченному Представителю Клиента необходимо провести активацию ключа Облачной подписи в соответствии с п.4.1 настоящего Регламента.

5.3. Смена ключа Облачной подписи производится в случаях:

- Компрометации Облачной подписи;
- утраты Логина и Статического пароля;

6. ПОРЯДОК ПРОВЕДЕНИЯ ПЛАНОВОЙ СМЕНЫ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

6.1. При каждом входе в Систему ДБО БИФИТ за 30 (Тридцать) дней до окончания срока действия Сертификата ключа проверки Электронной подписи Система ДБО БИФИТ сообщает о скором его окончании.

6.2. До истечения срока действия Сертификатов ключей проверки Электронной подписи Уполномоченный Представитель Клиента имеет возможность провести плановую процедуру смены Ключей Электронной подписи с использованием Системы ДБО БИФИТ.

6.3. Уполномоченный Представитель Клиента формирует новый Ключ Электронной подписи и Сертификат ключа проверки электронной подписи. Сертификат подписывается действующим ключом Электронной подписи и направляется в Банк с использованием средств Системы ДБО БИФИТ.

6.4. При поступлении в Банк обновленного Сертификата ключа проверки электронной подписи в электронном виде Ответственный работник обрабатывает запрос на активацию. Заведомо, до истечения срока полномочий, Уполномоченный Представитель Клиента одновременно с запросом должен предоставить документы, подтверждающие его полномочия (продление).

6.5. Банк осуществляет активацию Сертификата ключа проверки электронной подписи. Банк вправе отказать в активации Сертификата ключа проверки

5.3. The Cloud Signature Key is changed in the following cases:

- Compromise of the Cloud Signature;
- Loss of the Login and Static Password.

6. PROCEDURE FOR THE SCHEDULED REPLACEMENT OF THE ELECTRONIC SIGNATURE VERIFICATION KEY CERTIFICATE

6.1. Upon each login to the BIFIT RBS, 30 (Thirty) days before the expiration of the Electronic Signature Verification Key Certificate, the BIFIT RBS notifies the user of its impending expiration.

6.2. Before the expiration of the Electronic Signature Verification Key Certificates, the Authorized Representative of the Client has the opportunity to carry out the scheduled procedure for replacing the Electronic Signature Keys using the BIFIT RBS.

6.3. The Authorized Representative of the Client generates a new Electronic Signature Key and an Electronic Signature Verification Key Certificate. The Certificate is signed with the current Electronic Signature Key and sent to the Bank using the tools of the BIFIT RBS.

6.4. Upon receipt of the updated Electronic Signature Verification Key Certificate in electronic form, the Responsible Employee processes the activation request. Prior to the expiration of the authority, the Authorized Representative of the Client must simultaneously provide documents confirming their authority (extension) along with the request.

6.5. The Bank activates the Electronic Signature Verification Key Certificate. The Bank has the right to refuse to activate the Electronic Signature Verification Key Certificate, the information about which was received using the BIFIT RBS, without

электронной подписи, информация о котором получена с использованием Системы ДБО БИФИТ, без объяснения причины. В случае отказа Банка в активации Сертификата ключа проверки электронной подписи, Уполномоченный Представитель Клиента вправе лично обратиться в Банк для выпуска такого сертификата, в порядке, указанном в разделе 4 Регламента. После получения Банком подписанных Сертификатов, такой сертификат размещается в Системе ДБО БИФИТ.

providing a reason. In case of the Bank's refusal to activate the Electronic Signature Verification Key Certificate, the Authorized Representative of the Client has the right to personally contact the Bank to issue such a certificate, in the manner specified in Section 4 of these Regulations. After the Bank receives the signed Certificates, such a certificate is placed in the BIFIT RBS.

6.6. Уполномоченный Представитель Клиента завершает процедуру смены Ключа Электронной подписи, используя средства Системы ДБО БИФИТ.

6.6. The Authorized Representative of the Client completes the procedure for replacing the Electronic Signature Key using the tools of the BIFIT RBS.

6.7. После завершения процедуры смены Ключа Электронной подписи Уполномоченный Представитель Клиента может использовать исключительно новый Ключ Электронной подписи.

6.7. After completing the procedure for replacing the Electronic Signature Key, the Authorized Representative of the Client may use only the new Electronic Signature Key.

7. ПОРЯДОК БЛОКИРОВКИ И ВОССТАНОВЛЕНИЯ ДОСТУПА К СИСТЕМЕ ДБО БИФИТ

7. PROCEDURE FOR BLOCKING AND RESTORING ACCESS TO THE BIFIT RBS

7.1. Основанием для блокировки доступа Клиента и/или его Уполномоченного Представителя к Системе ДБО БИФИТ являются:

7.1.1. Получение Банком от Уполномоченного Представителя Клиента Заявление о внесении изменений в условия Договора (содержащего сведения о смене Уполномоченного Представителя Клиента/изменении его данных/прекращении полномочий или иные сведения, порождающие сомнения Банка в возможности осуществления доступа и/или пользования Системой ДБО БИФИТ Уполномоченным Представителем Клиента), запроса о приостановлении доступа к Системе ДБО БИФИТ, с указанием причин такого приостановления;

7.1.2. Компрометация Электронной подписи и/или использование Электронной подписи без согласия Уполномоченного Представителя Клиента;

7.1.3. Замена Карточки с образцами подписей и оттиска печати и/или Соглашения о сочетании электронных подписей, при их оформлении в соответствии с Правилами;

7.1.4. Прекращение или изменение полномочий или данных Уполномоченного Представителя Клиента;

7.1.5. Смена Абонентского номера Уполномоченного Представителя Клиента;

7.1 The grounds for blocking the Client and/or its Authorized Representative's access to the BIFIT RBS are:

7.1.1. Receipt by the Bank of an Application from the Authorized Representative of the Client to amend the terms of the Agreement (containing information about the change of the Authorized Representative of the Client/change of their data/termination of authority or other information causing the Bank to doubt the possibility of access and/or use of the BIFIT RBS by the Authorized Representative of the Client), a request to suspend access to the BIFIT RBS, indicating the reasons for such suspension;

7.1.2. Compromise of the Electronic Signature and/or use of the Electronic Signature without the consent of the Authorized Representative of the Client;

7.1.3. Replacement of the Specimen Signature Card and/or the Agreement on the Combination of Electronic Signatures, if issued in accordance with the Rules;

7.1.4. Termination or change of the authority or data of the Authorized Representative of the Client;

7.1.5. Change of the Subscriber Number of the Authorized Representative of the Client;

7.1.6. Loss of Authentication Data, Static Password without signs of compromise of the Electronic Signature;

7.1.7. Failure to provide or provision of inaccurate

7.1.6. Утраты Аутентификационных данных, Статического пароля без признаков Компрометации Электронной подписи;

7.1.7. Непредставление или представление недостоверных сведений и документов, запрашиваемых Банком, в том числе в целях выполнения требований законодательства Российской Федерации и нормативных актов Банка России;

7.1.8. Выявление Банком операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, установленным Банком России или подозрений на их совершение;

7.1.9. Направление Клиентом Заявление о внесении изменений в условия Договора, в рамках которого происходит приостановление предоставления доступа к Системе ДБО БИФИТ.

7.2. При наступлении событий, указанных в пп. 7.1.3, 7.1.7, 7.1.8 доступ в Систему ДБО БИФИТ блокируется всем Уполномоченным Представителям Клиента.

7.3. Клиент вправе осуществить блокировку доступа к Системе ДБО БИФИТ, в случаях, не связанных с компрометацией, или подозрении на компрометацию Электронной подписи.

7.3.1. Порядок блокировки доступа к Системе ДБО БИФИТ дистанционным способом:
Для дистанционной блокировки доступа к Системе ДБО БИФИТ Уполномоченному Представителю Клиента необходимо обратиться в Банк с соответствующим запросом по следующим контактным данным: dbo@131.ru или с использованием Системы ДБО БИФИТ, с указанием данных Уполномоченного Представителя Клиента, позволяющих установить его личность. Для обработки запроса на дистанционную блокировку уполномоченный работник Банка связывается с Уполномоченным Представителем Клиента с использованием контактных данных такого лица, указанных Уполномоченным Представителем Клиента в Заявлении на Продукт и Заявлении, при этом, Уполномоченный Представитель Клиента должен сообщить уполномоченному работнику Банка сведения, необходимые для аутентификации Уполномоченного Представителя Клиента.

7.3.2. Порядок блокировки доступа к Системе ДБО БИФИТ при личном обращении Уполномоченного Представителя Клиента в Банк:

7.3.2.1. Уполномоченному Представителю Клиента необходимо обратиться непосредственно в офис Банка, по его юридическому адресу, с

information and documents requested by the Bank, including for the purpose of complying with the requirements of the legislation of the Russian Federation and regulatory acts of the Central Bank of Russia;

7.1.8. Identification by the Bank of a transaction corresponding to the signs of transferring funds without the voluntary consent of the Client, as established by the Central Bank of Russia, or suspicions of such actions;

7.1.9. Submission by the Client of an Application to amend the terms of the Agreement, within the framework of which access to the BIFIT RBS is suspended.

7.2. Upon the occurrence of the events specified in clauses 7.1.3, 7.1.7, and 7.1.8, access to the BIFIT RBS is blocked for all Authorized Representatives of the Client.

7.3. The Client has the right to block access to the BIFIT RBS in cases not related to compromise or suspicion of compromise of the Electronic Signature.

7.3.1. Procedure for blocking access to the BIFIT RBS remotely:
To block access to the BIFIT RBS remotely, the Authorized Representative of the Client must contact the Bank with a corresponding request at the following contact details: dbo@131.ru or using the BIFIT RBS, indicating the data of the Authorized Representative of the Client allowing their identification. To process the request for remote blocking, the authorized employee of the Bank contacts the Authorized Representative of the Client using the contact details of such person specified by the Authorized Representative of the Client in the Application for the Product and the Application, and the Authorized Representative of the Client must provide the authorized employee of the Bank with the information necessary for authentication.

7.3.2. Procedure for blocking access to the BIFIT RBS upon personal application of the Authorized Representative of the Client to the Bank:

7.3.2.1. The Authorized Representative of the Client must apply directly to the Bank's office at its legal address with a corresponding written application to block access to the BIFIT RBS, signed by such person. Simultaneously with the request, the Authorized Representative of the Client must provide identity documents and documents confirming their authority.

7.3.2.2. Submission of a request to block access to the BIFIT RBS by the Authorized Representative of the

соответствующим письменным заявлением о блокировании доступа к Системе ДБО БИФИТ, подписанным таким лицом. Одновременно с запросом Уполномоченный Представитель Клиента должен предоставить документы, удостоверяющие его личность и подтверждающие его полномочия.

7.3.2.2. Подача запроса на блокировку доступа к Системе ДБО БИФИТ Уполномоченного Представителя Клиента возможна только в течение Операционного времени Банка.

7.4. Блокировка доступа осуществляется незамедлительно после получения соответствующего запроса и аутентификации Уполномоченного Представителя Клиента Банком, при условии его получения Банком в Операционное время. В случае, если запрос был получен Банком за пределами Операционного времени, такой запрос будет обработан, а доступ к Системе ДБО БИФИТ заблокирован, в Операционное время ближайшего за датой получения такого запроса Банком Рабочего дня.

7.5. Порядок восстановления доступа к Системе ДБО БИФИТ:

В случае, если основанием для блокировки доступа к Системе ДБО БИФИТ послужили обстоятельства, указанные в п.7.1.2-7.1.6, 7.1.9 разблокировка возможна после получения Банком письменного обращения (Заявления о смене логина и/или статического пароля/разблокировку доступа в Системе ДБО БИФИТ) Уполномоченного Представителя Клиента при личном посещении офиса Банка. Форма такого заявления определяется Банком и размещена на ресурсе https://131.ru/contracts и в офисе Банка. Одновременно с обращением Уполномоченный Представитель Клиента должен предоставить документы, удостоверяющие его личность и подтверждающие его полномочия и:

a) При использовании УНЭП: проведенной процедуры внеплановой смены сертификата ключа проверки Электронной подписи в соответствии с разделом 10 Регламента;

b) При использовании Облачной подписи: смена Статического пароля Уполномоченного Представителя Клиента в соответствии с п.3.12 Регламента; смены Абонентского номера Уполномоченного Представителя Клиента в случае утери и/или прекращения доступа к нему.

7.6. В случае, если основанием для блокировки доступа к Системе ДБО БИФИТ послужили обстоятельства, указанные в п. 7.1.6 Регламента, разблокировка возможна в соответствии с п. 3.12 Регламента. Дистанционная разблокировка в соответствии с п.

Client is possible only during the Bank's operating hours.

7.4. Access is blocked immediately after receiving the corresponding request and authenticating the Authorized Representative of the Client by the Bank, provided that the request is received by the Bank during operating hours. If the request is received by the Bank outside operating hours, such a request will be processed, and access to the BIFIT RBS will be blocked during the operating hours of the nearest working day following the date of receipt of such request by the Bank.

7.5. Procedure for restoring access to the BIFIT RBS:

If the grounds for blocking access to the BIFIT RBS were the circumstances specified in clauses 7.1.2–7.1.6, 7.1.9, unblocking is possible after the Bank receives a written request (Application to change the Login and/or Static Password/unblock access to the BIFIT RBS) from the Authorized Representative of the Client upon personal visit to the Bank's office. The form of such an application is determined by the Bank and is available on the resource https://131.ru/contracts and in the Bank's office. Simultaneously with the request, the Authorized Representative of the Client must provide identity documents and documents confirming their authority and:

a) When using an Enhanced Unqualified Electronic Signature (UES): completion of the unscheduled replacement procedure for the Electronic Signature Verification Key Certificate in accordance with Section 10 of these Regulations;

b) When using a Cloud Signature: change of the Static Password of the Authorized Representative of the Client in accordance with clause 3.12 of these Regulations; change of the Subscriber Number of the Authorized Representative of the Client in case of loss and/or termination of access to it.

7.6. If the grounds for blocking access to the BIFIT RBS were the circumstances specified in clause 7.1.6 of these Regulations, unblocking is possible in accordance with clause 3.12 of these Regulations. Remote unblocking in accordance with clause 3.12 of these Regulations is possible if the Bank has no grounds to believe that the Electronic Document Confirmation Tools have become known to unauthorized third parties.

7.7. If the grounds for blocking access to the BIFIT RBS

3.12Регламента возможна при отсутствии у Банка оснований полагать, что Средства подтверждения Электронного документа стали известны неуполномоченным третьим лицам.

7.7. В случае, если основанием для блокировки доступа к Системе ДБО БИФИТ послужили обстоятельства, указанные в п.7.1.8 Регламента, разблокировка возможна после получения Банком от Клиента подтверждения распоряжения о совершении операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия Клиента, установленным Банком России, при отсутствии иных установленных законодательством Российской Федерации оснований.

7.8. В случае, если основанием для блокировки доступа к Системе ДБО БИФИТ послужили обстоятельства, указанные в п.7.1.7 Регламента, доступ к Системе ДБО БИФИТ возобновляется после представления сведений и документов, запрашиваемых Банком. Документы предоставляются Клиентом Ответственному работнику в офисе Банка по его юридическому адресу в течение Операционного времени Банка.

were the circumstances specified in clause 7.1.8 of these Regulations, unblocking is possible after the Bank receives confirmation from the Client of the order to perform a transaction corresponding to the signs of transferring funds without the voluntary consent of the Client, as established by the Central Bank of Russia, in the absence of other grounds established by the legislation of the Russian Federation.

7.8. If the grounds for blocking access to the BIFIT RBS were the circumstances specified in clause 7.1.7 of these Regulations, access to the BIFIT RBS is restored after the provision of the information and documents requested by the Bank. The documents are submitted by the Client to the Responsible Employee at the Bank's office at its legal address during the Bank's operating hours.

8. ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ КОМПРОМЕТАЦИИ ИЛИ ПОДОЗРЕНИИ НА КОМПРОМЕТАЦИЮ ЭЛЕКТРОННОЙ ПОДПИСИ

8.1. При выявлении одной из Сторон Компрометации Электронной подписи или ее признаков (подозрений), выявившая Сторона уведомляет об этом другую Сторону.

8.2. Банк уведомляет Клиента о наступлении указанных в п. 8.1 Регламента обстоятельствах любым доступным Банку способом, используя имеющиеся в распоряжении Банка контактные данные Клиента, ранее предоставленные Клиентом.

8.3. Клиент уведомляет Банк о наступлении указанных в п. 8.1 Регламента обстоятельствах любым из нижеперечисленных способов:

- Письменное Уведомление о компрометации на бумажном носителе (передается в офисе Банка);
- Сканированная копия письменного Уведомления о компрометации, переданная на электронный адрес Банка: dbo@131.ru. Клиент обязан представить в Банк оригинал

8.PROCEDURE FOR ACTIONS IN CASE OF COMPROMISE OR SUSPICION OF COMPROMISE OF THE ELECTRONIC SIGNATURE

8.1 If one of the Parties identifies a compromise of the Electronic Signature or signs (suspicions) thereof, the identifying Party notifies the other Party.

8.2. The Bank notifies the Client of the circumstances specified in clause 8.1 of these Regulations by any means available to the Bank, using the contact details of the Client previously provided by the Client and available to the Bank.

8.3. The Client notifies the Bank of the circumstances specified in clause 8.1 of these Regulations by any of the following methods:

- Written Notice of Compromise on paper (submitted at the Bank's office);
- Scanned copy of the written Notice of Compromise sent to the Bank's email address: dbo@131.ru. The Client is obliged to submit the original of such Notice of Compromise on paper to the Bank within 2

такого Уведомления о компрометации на бумажном носителе в течение 2 (Двух) Рабочих дней, либо предоставить уникальный идентификатор, который присваивается почтовым отправлениям, выдаваемый транспортной компанией, осуществляющей отправку оригиналов документов, либо направить экземпляры документов посредством Оператора ЭДО.

- Форма Уведомления о компрометации определяется Банком и является Приложением №4 к Регламенту.

8.4. С момента получения Банком уведомления Клиента или выявления Банком обстоятельств, указанных в п. 9.1 Регламента, доступ Клиента (его Уполномоченных Представителей) к Системе ДБО БИФИТ блокируется до момента разблокировки такого доступа. Клиент уведомлен и согласен, что Банк не несет ответственности, включая финансовую, за любой факт блокировки доступа Клиента и/или его Уполномоченных Представителей к Системе ДБО БИФИТ, в связи с тем, что действия Банка по блокировке доступа к Системе ДБО БИФИТ направлены на обеспечение сохранности средств на Счете, защиту интересов Клиента и недопущению мошеннических операций и практик.

8.5. С момента направления Клиентом Банку или получения Клиентом от Банка уведомления о наступлении указанных в п. 8.1 Регламента обстоятельствах, Клиент не вправе использовать скомпрометированную Электронную подпись (ее ключ и/или средства)/Аутентификационные данные/Абонентский номер. В случае любого использования Клиентом такой Электронной подписи/Аутентификационных данных/
Абонентского номера после наступления указанных в п. 8.1 Регламента обстоятельств, Клиент самостоятельно несет риск наступления неблагоприятных последствий для него, в том числе правовых и финансовых.

8.6. Разблокировка доступа к Системе ДБО БИФИТ осуществляется в соответствии с п. 8.5 Регламента при получении Банком Уведомления о компрометации на бумажном носителе.

(two) working days, or provide a unique identifier assigned to the shipment by the transport company delivering the original documents, or send the documents via the EDI Operator.

- The form of the Notice of Compromise is determined by the Bank and is Appendix No. 4 to these Regulations.

8.4. From the moment the Bank receives the Client's notification or identifies the circumstances specified in clause 8.1 of these Regulations, the Client's (its Authorized Representatives') access to the BIFIT RBS is blocked until such access is unblocked. The Client is notified and agrees that the Bank is not responsible, including financially, for any fact of blocking the Client's and/or its Authorized Representatives' access to the BIFIT RBS, as the Bank's actions to block access to the BIFIT RBS are aimed at ensuring the safety of funds in the Account, protecting the Client's interests, and preventing fraudulent transactions and practices.

8.5. From the moment the Client sends a notification to the Bank or receives a notification from the Bank about the occurrence of the circumstances specified in clause 8.1 of these Regulations, the Client is not entitled to use the compromised Electronic Signature (its key and/or tools)/Authentication Data/Subscriber Number. In case of any use by the Client of such Electronic Signature/Authentication Data/Subscriber Number after the occurrence of the circumstances specified in clause 8.1 of these Regulations, the Client independently bears the risk of adverse consequences, including legal and financial ones.

8.6. Unblocking access to the BIFIT RBS is carried out in accordance with clause 8.5 of these Regulations upon receipt by the Bank of the Notice of Compromise on paper.

9. ПОРЯДОК ПРОВЕДЕНИЯ ВНЕПЛАНОВОЙ СМЕНЫ СЕРТИФИКАТА КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ

9.1. Указанный раздел применяется в случае использования Клиентом (его Уполномоченными Представителями) УНЭП. Внеплановая смена Ключей Электронной подписи Уполномоченного Представителя Клиента и соответствующих им Сертификатов ключа проверки Электронной подписи выполняется в случае:

- установленного факта Компрометации Электронной подписи или подозрений на это;
- изменения регистрационных данных Уполномоченного Представителя Клиента;
- выхода из строя ФКН.
- Внесение сертификата ключа проверки в список отозванных сертификатов

9.2. После получения Банком Уведомления о компрометации Банк отзывает (аннулирует) Сертификат скомпрометированного ключа проверки электронной подписи.

9.3. Для активации нового ключа Электронной подписи и соответствующего ему Сертификата ключа проверки Электронной подписи Уполномоченный Представитель Клиента лично обращается в офис Банка с заявлением на выпуск Сертификата ключа проверки Электронной подписи в свободной форме и в указанном в разделе 4 настоящего Регламента порядке с предоставлением документов, удостоверяющих его личность и подтверждающие его полномочия.

9.PROCEDURE FOR UNSCHEDULED REPLACEMENT OF THE ELECTRONIC SIGNATURE VERIFICATION KEY CERTIFICATE

9.1 This section applies if the Client (its Authorized Representatives) uses an Enhanced Unqualified Electronic Signature (UES). The unscheduled replacement of the Electronic Signature Keys of the Authorized Representative of the Client and the corresponding Electronic Signature Verification Key Certificates is performed in the following cases:

- Established fact of compromise of the Electronic Signature or suspicion thereof;
- Change of registration data of the Authorized Representative of the Client;
- Malfunction of the Functional Key Carrier (FKC);
- Revocation of the Electronic Signature Verification Key Certificate.

9.2. After receiving the Notice of Compromise, the Bank revokes (cancels) the compromised Electronic Signature Verification Key Certificate.

9.3. To activate a new Electronic Signature Key and the corresponding Electronic Signature Verification Key Certificate, the Authorized Representative of the Client personally contacts the Bank's office with an application for the issuance of an Electronic Signature Verification Key Certificate in free form and in the manner specified in Section 4 of these Regulations, providing identity documents and documents confirming their authority.

10.ПОРЯДОК РАССМОТРЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

10.1. Процедура проверки подлинности Электронной подписи выполняется по инициативе Банка или Клиента. Под процедурой проверки подлинности Электронной подписи, при обмене между Банком и Клиентом Электронными документами с использованием Системы ДБО БИФИТ, подписанными Электронной подписью, понимается возникновение у Банка или Клиента сомнений, связанных с непризнанием авторства и (или) целостности Электронного документа, подписанного Электронной подписью Уполномоченного Представителя Клиента.

10.2. Стороны признают информацию, содержащуюся в

10. PROCEDURE FOR RESOLVING DISPUTES

10.1 The procedure for verifying the authenticity of the Electronic Signature is initiated by the Bank or the Client. The procedure for verifying the authenticity of the Electronic Signature, when exchanging Electronic Documents between the Bank and the Client using the BIFIT RBS, signed with an Electronic Signature, refers to the Bank or the Client having doubts regarding the authorship and/or integrity of the Electronic Document signed with the Electronic Signature of the Authorized Representative of the Client.

10.2. The Parties recognize that the information contained

программно-аппаратных средствах и системных журналах Банка, достаточной для проверки подлинности УНЭП и Облачной подписи в Электронном документе. Подтверждение подлинности Облачной подписи в Электронном документе осуществляется путем сопоставления данных, указанных Уполномоченным Представителем Клиента в настройках использования Облачной подписи в Системе ДБО БИФИТ, и данных, присвоенных оспариваемому Электронному документу в Системе ДБО БИФИТ, полученному Банком, а также информации в системных журналах Банка, в соответствии с процедурой, приведенной в п.11.12 Регламента.

10.3. Подтверждение подлинности УНЭП в Электронных документах осуществляется путем проверки соответствующим средством Электронной подписи с использованием Сертификата ключа проверки электронной подписи принадлежности такой Электронной подписи в Электронном документе Уполномоченному Представителю Клиента (владельцу сертификата) и отсутствия искажений в подписанном данной Электронной подписью Электронном документе, в соответствии с процедурой, приведенной в п.11.10 Регламента.

10.4. Процедура проверки подлинности Электронной подписи при обмене Электронным документами Клиентом и Банком с использованием Системы ДБО БИФИТ, в случае применения Клиентом УНЭП основывается на математических свойствах алгоритма Электронной подписи, реализованного в соответствии с актуальным стандартом Российской Федерации ГОСТ Р 34.10-2012, гарантирующего невозможность подделки значения УНЭП любым лицом, не обладающим ключом такой Электронной подписи. Итогом разрешения конфликтной ситуации является либо доказательство подлинности, целостности и авторства оспариваемого Электронного документа Клиенту (его Уполномоченному Представителю), либо установление факта приема Банком искаженного Электронного документа.

10.5. На случай возникновения споров Банк обеспечивает хранение в течение установленных законодательством Российской Федерации сроков в специальной базе данных Электронных документов в виде единиц хранения, каждая из которых включает данные Электронного документа, строки Электронной подписи с параметрами УНЭП, Сертификат ключа проверки электронной подписи Уполномоченного Представителя Клиента, использованный при создании УНЭП, историю настроек Системы ДБО БИФИТ для использования

in the Bank's hardware and software systems and system logs is sufficient to verify the authenticity of the Enhanced Unqualified Electronic Signature (UES) and the Cloud Signature in the Electronic Document. Confirmation of the authenticity of the Cloud Signature in the Electronic Document is carried out by comparing the data specified by the Authorized Representative of the Client in the settings for using the Cloud Signature in the BIFIT RBS and the data assigned to the disputed Electronic Document in the BIFIT RBS received by the Bank, as well as the information in the Bank's system logs, in accordance with the procedure set out in clause 11.12 of these Regulations.

10.3. Confirmation of the authenticity of the UES in Electronic Documents is carried out by verifying the corresponding Electronic Signature tool using the Electronic Signature Verification Key Certificate to confirm that such Electronic Signature in the Electronic Document belongs to the Authorized Representative of the Client (the certificate holder) and that there are no distortions in the Electronic Document signed with this Electronic Signature, in accordance with the procedure set out in clause 11.10 of these Regulations.

10.4. The procedure for verifying the authenticity of the Electronic Signature when exchanging Electronic Documents between the Client and the Bank using the BIFIT RBS, in the case of the Client using a UES, is based on the mathematical properties of the Electronic Signature algorithm implemented in accordance with the current Russian standard GOST R 34.10-2012, which guarantees the impossibility of forging the value of the UES by any person who does not possess the key of such Electronic Signature. The outcome of resolving a dispute is either proving the authenticity, integrity, and authorship of the disputed Electronic Document to the Client (its Authorized Representative) or establishing the fact that the Bank received a distorted Electronic Document.

10.5. In the event of disputes, the Bank ensures the storage of Electronic Documents in a special database for the periods established by the legislation of the Russian Federation. Each storage unit includes the data of the Electronic Document, the Electronic Signature lines with UES parameters, the Electronic Signature Verification Key Certificate of the Authorized Representative of the Client used to

Облачной подписи и УНЭП в системных журналах Банка, а так же данные Средств подтверждения Электронных документов, использованные при создании Облачной подписи и УНЭП в оспариваемом Электронном документе. Банк обеспечивает защиту данных от возможных искажений в процессе хранения. Банк обеспечивает хранение полученных Банком оригиналов Сертификатов ключей проверки электронной подписи Клиента.

10.6. В случае дистанционного обращения Уполномоченного Представителя Клиента для перевыпуска Сертификата ключа проверки электронной подписи Банк обеспечивает хранение полученного Банком подписанного Уполномоченным Представителя Клиента Сертификата ключа проверки электронной подписи в электронной форме.

10.7. Процедура проверки подлинности Электронной подписи при обмене Электронными документами с использованием Системы ДБО БИФИТ выполняется Согласительной комиссией, в состав которой входят надлежащим образом уполномоченные представители обеих Сторон (не менее двух человек от каждой стороны). По соглашению Сторон в состав комиссии может быть введен независимый эксперт.

10.8. В случае, если оспариваемый Электронный документ является частью пакета Электронных документов, то процедура проверки подписи осуществляется под пакетом Электронных документов, в состав, которого входит оспариваемый Электронный документ.

10.9. Порядок разрешения конфликтной ситуации.

10.9.1. В случае возникновения необходимости в проведении процедуры проверки подлинности Электронной подписи при обмене Электронными документами с использованием Системы ДБО БИФИТ, Уполномоченный Представитель Клиента представляет Банку письменное заявление, содержащее существо претензии с указанием на Электронный документ, который он оспаривает.

10.9.2. Банк и Клиент должны в течение не более пяти рабочих дней от даты приема Банком заявления Клиента сформировать Согласительную комиссию для его рассмотрения.

10.9.3. Согласительная комиссия должна закончить свою работу в течение 14 рабочих дней с момента ее создания.

10.9.4. Решение Согласительной комиссии принимается большинством голосов ее участников, оформляется актом и

create the UES, the history of BIFIT RBS settings for using the Cloud Signature and UES in the Bank's system logs, as well as the Electronic Document Confirmation Tools used to create the Cloud Signature and UES in the disputed Electronic Document. The Bank ensures the protection of data from possible distortions during storage. The Bank ensures the storage of the original Electronic Signature Verification Key Certificates of the Client received by the Bank.

10.6. In the case of a remote request by the Authorized Representative of the Client for the reissuance of an Electronic Signature Verification Key Certificate, the Bank ensures the storage of the Electronic Signature Verification Key Certificate signed by the Authorized Representative of the Client and received by the Bank in electronic form.

10.7. The procedure for verifying the authenticity of the Electronic Signature when exchanging Electronic Documents using the BIFIT RBS is carried out by a Conciliation Commission, which includes duly authorized representatives of both Parties (at least two persons from each side). By agreement of the Parties, an independent expert may be included in the commission.

10.8. If the disputed Electronic Document is part of a package of Electronic Documents, the signature verification procedure is carried out for the package of Electronic Documents, which includes the disputed Electronic Document.

10.9. Procedure for Resolving Disputes:

10.9.1. If it is necessary to verify the authenticity of the Electronic Signature when exchanging Electronic Documents using the BIFIT RBS, the Authorized Representative of the Client submits a written application to the Bank containing the essence of the claim and indicating the Electronic Document being disputed.

10.9.2. The Bank and the Client must, within no more than five working days from the date the Bank receives the Client's application, form a Conciliation Commission to review it.

10.9.3. The Conciliation Commission must complete its work within 14 working days from the date of its formation.

10.9.4. The decision of the Conciliation Commission is made by a majority vote of its members, documented in an act, and signed by all

подписывается всеми членами комиссии.

10.9.5. В случае, если Стороны не пришли к взаимному соглашению или в случае отказа от добровольного исполнения решения Согласительной комиссии, Стороны решают конфликтную ситуацию в судебном порядке.

10.10. Процедура проверки УНЭП.

10.10.1. Для проверки принадлежности Электронной подписи Уполномоченному Представителю Клиента и проверки отсутствия искажений в Электронном документе уполномоченным работником Банка из базы данных Банка извлекается файл Сертификата ключа проверки электронной подписи Уполномоченного Представителя Клиента - владельца Сертификата ключа проверки электронной подписи, использованный при создании УНЭП под оспариваемым Электронным документом.

10.10.2. Устанавливается принадлежность ключа проверки Электронной подписи, содержащегося в извлеченном файле, владельцу Сертификата ключа проверки электронной подписи по следующей процедуре:

- из базы данных извлекается первичный Сертификат ключа проверки электронной подписи Уполномоченного Представителя Клиента - владельца Сертификата ключа проверки электронной подписи. Устанавливается принадлежность ключа проверки Электронной подписи владельцу Сертификата ключа проверки электронной подписи, путем сравнения с ключом проверки Электронной подписи, указанному в Сертификате проверки ключа электронной подписи в бумажном виде, имеющимся в распоряжении Банка. Если соответствие не установлено, то принадлежность ключа Электронной подписи данному владельцу Сертификата ключа проверки электронной подписи – Клиенту/Уполномоченному Представителю Клиента не подтверждается;
- из базы данных извлекается последующий (при наличии такового) Сертификат ключа проверки электронной подписи Уполномоченного Представителя Клиента - владельца Сертификата ключа проверки электронной подписи и устанавливается факт его подписания первичным ключом Электронной подписи по содержанию Сертификата ключа проверки электронной подписи. В противном случае - принадлежность ключа данному Уполномоченному Представителю Клиента не подтверждается;
- вышеуказанные действия последовательно повторяются вплоть до проверки Сертификата ключа проверки электронной подписи владельца,

members of the commission.

10.9.5. If the Parties do not reach a mutual agreement or in case of refusal to voluntarily execute the decision of the Conciliation Commission, the Parties resolve the dispute in court.

10.10. Procedure for Verifying the UES:

10.10.1. To verify the ownership of the Electronic Signature by the Authorized Representative of the Client and the absence of distortions in the Electronic Document, the Bank's authorized employee extracts the Electronic Signature Verification Key Certificate file of the Authorized Representative of the Client—the holder of the Electronic Signature Verification Key Certificate—used to create the UES for the disputed Electronic Document from the Bank's database.

10.10.2. The ownership of the Electronic Signature Verification Key contained in the extracted file is established by the following procedure:

- The primary Electronic Signature Verification Key Certificate of the Authorized Representative of the Client—the holder of the Electronic Signature Verification Key Certificate—is extracted from the database. The ownership of the Electronic Signature Verification Key by the holder of the Electronic Signature Verification Key Certificate is established by comparing it with the Electronic Signature Verification Key specified in the paper version of the Electronic Signature Verification Key Certificate available to the Bank. If no match is found, the ownership of the Electronic Signature Key by the holder of the Electronic Signature Verification Key Certificate—the Client/Authorized Representative of the Client—is not confirmed;
- The subsequent (if any) Electronic Signature Verification Key Certificate of the Authorized Representative of the Client—the holder of the Electronic Signature Verification Key Certificate—is extracted from the database, and the fact of its signing with the primary Electronic Signature Key is established based on the content of the Electronic Signature Verification Key Certificate. Otherwise, the ownership of the key by this Authorized Representative of the Client is not confirmed;
- The above actions are sequentially repeated until the Electronic Signature Verification Key Certificate of the holder used to create the Electronic Signature for the disputed Electronic Document is verified. If the content of the

использованного для создания Электронной подписи под оспариваемым Электронным документом. Если из содержания Сертификата ключа проверки электронной подписи в базе данных не следует, что Сертификат проверен и подписан предыдущим Сертификатом ключа проверки электронной подписи соответствующего Уполномоченного Представителя Клиента - владельца Сертификата ключа проверки электронной подписи, принадлежность ключа Электронной подписи такому Уполномоченному Представителю Клиента не подтверждается. В противном случае - Ключ Электронной подписи признается принадлежащим указанному в его Сертификате ключа проверки электронной подписи Уполномоченному Представителю Клиента.

10.10.3. Устанавливается действительность Сертификата ключа проверки электронной подписи Уполномоченного Представителя Клиента - владельца Сертификата ключа проверки электронной подписи, на момент получения Банком оспариваемого Электронного документа. Сертификат ключа проверки электронной подписи является недействительным на момент получения Банком оспариваемого Электронного документа, если:

- срок действия Сертификата ключа проверки электронного документа истек;
- данный Сертификат ключа проверки электронной подписи был помещен в список отозванных сертификатов.

В противном случае, Сертификат ключа проверки электронной подписи Уполномоченного Представителя Клиента - владельца Сертификата ключа проверки электронной подписи признается действительным.

10.10.4. Устанавливается факт блокирования доступа владельцу Сертификата ключа проверки электронной подписи к Системе ДБО БИФИТ на момент получения Банком оспариваемого Электронного документа. В случае, если дата получения Банком Уведомления о компрометации ключа Электронной подписи и/или заявления на блокирование доступа в Систему ДБО БИФИТ Уполномоченному Представителю Клиента – владельцу Сертификата ключа проверки электронной подписи раньше даты получения Банком оспариваемого Электронного документа — такой

Electronic Signature Verification Key Certificate in the database does not indicate that the Certificate has been verified and signed by the previous Electronic Signature Verification Key Certificate of the corresponding Authorized Representative of the Client—the holder of the Electronic Signature Verification Key Certificate—the ownership of the Electronic Signature Key by such Authorized Representative of the Client is not confirmed. Otherwise, the Electronic Signature Key is recognized as belonging to the Authorized Representative of the Client specified in its Electronic Signature Verification Key Certificate.

10.10.3. The validity of the Electronic Signature Verification Key Certificate of the Authorized Representative of the Client—the holder of the Electronic Signature Verification Key Certificate—is established at the time the Bank received the disputed Electronic Document. The Electronic Signature Verification Key Certificate is invalid at the time the Bank received the disputed Electronic Document if:

- The validity period of the Electronic Signature Verification Key Certificate has expired;
- The Electronic Signature Verification Key Certificate has been placed in the list of revoked certificates.

Otherwise, the Electronic Signature Verification Key Certificate of the Authorized Representative of the Client—the holder of the Electronic Signature Verification Key Certificate—is recognized as valid.

10.10.4. The fact of blocking access to the BIFIT RBS for the holder of the Electronic Signature Verification Key Certificate at the time the Bank received the disputed Electronic Document is established. If the date the Bank received the Notice of Compromise of the Electronic Signature Key and/or the application to block access to the BIFIT RBS by the Authorized Representative of the Client—the holder of the Electronic Signature Verification Key Certificate—is earlier than the date the Bank received the disputed Electronic Document, such Electronic Document is recognized as invalid. Otherwise, or if it is established that the Bank did not receive the corresponding Notice of Compromise of the Electronic Signature Key and/or the application to block access to the BIFIT RBS by the Authorized Representative of the Client—the holder of the Electronic Signature Verification Key Certificate—

Электронный документ признается недействительным. В противном случае либо при установлении отсутствия факта получения Банком соответствующего Уведомления о компрометации ключа Электронной подписи и/или заявления на блокирование доступа в Систему ДБО БИФИТ Уполномоченному Представителю клиента – владельцу Сертификата ключа проверки электронной подписи оспариваемый Электронный документ признается действительным и корректным.

10.10.5. Проверка Электронной подписи оспариваемого Электронного документа производится в автоматическом режиме Системой ДБО БИФИТ. Протокол проверки УНЭП составляется и подписывается всеми членами Согласительной комиссии.

10.11. Процедура проверки Облачной подписи

10.11.1. Для проверки принадлежности Облачной подписи Уполномоченному Представителю Клиента и отсутствия искажений в Электронном документе из базы данных Банка уполномоченным работником Банка извлекается оспариваемое Электронное сообщение, файл подписи к оспариваемому Электронному сообщению и файл с идентификатором Облачной подписи.

10.11.1.1. Для разбора конфликтной ситуации используются эталонные программно-аппаратные средства Банка (Система ДБО БИФИТ). Используется специальное программное обеспечение, предназначенное для проверки Облачной подписи под Электронным документом.

10.11.1.2. Устанавливается принадлежность ключа проверки Облачной подписи, содержащегося в извлеченном файле, Уполномоченному Представителю Клиента по следующей процедуре: сравнивается номер ключа Облачной подписи, извлеченный из базы данных Банка, с номером ключа, указанного в Бланке Сертификата ключа проверки электронной подписи Клиента, хранящегося в досье Клиента, или в базе данных Банка. В случае, если принадлежность ключа установлена, Согласительная комиссия переходит к следующему этапу. При несовпадении информации оспариваемый документ признается некорректным.

10.11.1.3. Проверка Облачной подписи

the disputed Electronic Document is recognized as valid and correct.

10.10.5. The verification of the Electronic Signature of the disputed Electronic Document is carried out automatically by the BIFIT RBS. The UES verification protocol is drawn up and signed by all members of the Conciliation Commission.

10.11. Procedure for Verifying the Cloud Signature:

10.11.1. To verify the ownership of the Cloud Signature by the Authorized Representative of the Client and the absence of distortions in the Electronic Document, the Bank's authorized employee extracts the disputed Electronic Message, the signature file for the disputed Electronic Message, and the file with the Cloud Signature identifier from the Bank's database.

10.11.1.1. To resolve the dispute, the Bank's reference hardware and software tools (BIFIT RBS) are used. Special software designed to verify the Cloud Signature under the Electronic Document is used.

10.11.1.2. The ownership of the Cloud Signature Verification Key contained in the extracted file is established by the following procedure: the Cloud Signature Key number extracted from the Bank's database is compared with the key number specified in the Client's Electronic Signature Verification Key Certificate form stored in the Client's dossier or in the Bank's database. If the ownership of the key is established, the Conciliation Commission proceeds to the next stage. If the information does not match, the disputed document is recognized as incorrect.

10.11.1.3. The verification of the Cloud Signature of the disputed Electronic Document is carried out automatically by the BIFIT RBS. The UES verification protocol is drawn up and signed by all members of the Conciliation Commission.

10.12. Liability of the Parties in Case of Disputes Regarding Electronic Documents Signed with an Electronic Signature Exchanged Using the BIFIT RBS:

10.12.1. The Bank is not liable to the Client in the cases specified in the Rules (including their appendices), as well as when the Conciliation Commission establishes the following facts during the verification of the UES under the disputed Electronic Document:

- The Electronic Signature Verification Key in the

оспариваемого Электронного документа производится в автоматическом режиме Системой ДБО БИФИТ. Протокол проверки УНЭП составляется и подписывается всеми членами Согласительной комиссии.

10.12. Ответственность Сторон при оспаривании Электронных документов, подписанных Электронной подписью, обмен которыми осуществляется с использованием Системы ДБО БИФИТ.

10.12.1. Банк не несет ответственности перед Клиентом в случаях, указанных в Правилах (включая приложения к ним), а также при установлении Согласительной комиссией совокупности следующих фактов при проверке УНЭП под оспариваемым Электронным документом:

- ключ проверки Электронной подписи в оспариваемом Электронном документе принадлежит Уполномоченному Представителю Клиента - владельцу Сертификата ключа проверки электронной подписи;
- Сертификат ключа проверки электронной подписи Уполномоченного Представителя Клиента — владельца Сертификата ключа проверки электронной подписи был действителен на момент получения Банком оспариваемого Электронного документа;
- не установлен факт получения Банком от Клиента Уведомления о компрометации ключа Электронной подписи и/или заявления о блокировании доступа в Систему ДБО БИФИТ Уполномоченного Представителя Клиента, с использованием Средства подтверждения Электронного документа, которым был подписан оспариваемый Электронный документ, либо момент получения Банком Уведомления о компрометации ключа Электронной подписи и/или заявления на блокирование позже момента получения Банком оспариваемого Электронного документа.

10.12.2. Ответственность Банка наступает исключительно при наличии доказанной вины последнего и наличии прямой причинно-следственной связи между наступившими событиями, доказанной виной Банка и негативными для Клиента последствиями (ущербом). В любом случае, ни при каких обстоятельствах, Банк не возмещает Клиенту упущенную выгоду.

10.12.3. Клиент/Уполномоченный Представитель Клиента несут ответственность перед Банком во всех

disputed Electronic Document belongs to the Authorized Representative of the Client—the holder of the Electronic Signature Verification Key Certificate;

- The Electronic Signature Verification Key Certificate of the Authorized Representative of the Client—the holder of the Electronic Signature Verification Key Certificate—was valid at the time the Bank received the disputed Electronic Document;
- The Bank did not receive a Notice of Compromise of the Electronic Signature Key and/or an application to block access to the BIFIT RBS by the Authorized Representative of the Client using the Electronic Document Confirmation Tool with which the disputed Electronic Document was signed, or the moment the Bank received the Notice of Compromise of the Electronic Signature Key and/or the application to block access was later than the moment the Bank received the disputed Electronic Document.

10.12.2. The Bank's liability arises exclusively in the presence of proven fault on its part and a direct causal connection between the events that occurred, the proven fault of the Bank, and the negative consequences (damage) for the Client. In any case, under no circumstances does the Bank compensate the Client for lost profits.

10.12.3. The Client/Authorized Representative of the Client is liable to the Bank in all and any cases of non-fulfillment and/or improper fulfillment of the Rules (including their appendices), these Regulations, the provisions of the legislation of the Russian Federation, and the requirements of the Bank, and bears the risk of any legal and/or financial consequences, including adverse consequences for the Client, the Bank, and other persons related to such violation/improper performance.

и любых случаях невыполнения и/или ненадлежащего выполнения Правил (включая приложения к ним), Регламента, положений законодательства Российской Федерации и требований Банка, а также несут риск наступления любых правовых и/или финансовых последствий, в том числе неблагоприятных для Клиента, Банка, иных лиц, связанных с таким нарушением/ненадлежащим исполнением.

11.ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Регламент составлен на русском и английском языках. В случае возникновения противоречий приоритетным считается текст Регламента на русском языке.

11.2. Правоотношения Сторон, урегулированные Регламентом, а также любые иные правоотношения Сторон, связанные с выполнением Регламента, подлежат регулированию и толкованию в соответствии с законодательством Российской Федерации.

11.3. В случае, если любая из Сторон откажется от исполнения решения Согласительной комиссии, все споры и разногласия подлежат разрешению в соответствии с настоящим пунктом. Все споры, возникающие между Клиентом и Банком в рамках выполнения Регламента или в связи с ним, подлежат разрешению в соответствии с законодательством Российской Федерации путем переговоров, а в случае невозможности такого решения - в Арбитражном суде Республики Татарстан.
Клиент вправе обратиться в Банк с письменной претензией, подписанной Уполномоченным Представителем Клиента и скрепленной печатью последнего (при наличии) путем обращения в офис Банка, по его юридическому адресу. Письменный досудебный порядок урегулирования споров с Банком, в рамках настоящего Регламента, является обязательным. Срок ответа на досудебную претензию – 15 (пятнадцать) рабочих дней с даты ее получения Банком.

11.4. В случае изменения положений законодательства Российской Федерации, при которых положения Регламента входят в противоречие с положениями законодательства Российской Федерации, к таким правоотношениям Сторон подлежат применению положения законодательства Российской Федерации.

11. FINAL PROVISIONS

11.1 These Regulations are drawn up in Russian and English. In case of any discrepancies, the Russian text of the Regulations shall prevail.

11.2. The legal relations of the Parties governed by these Regulations, as well as any other legal relations of the Parties related to the implementation of these Regulations, shall be regulated and interpreted in accordance with the legislation of the Russian Federation.

11.3. If either Party refuses to comply with the decision of the Conciliation Commission, all disputes and disagreements shall be resolved in accordance with this clause. All disputes arising between the Client and the Bank in connection with or related to the implementation of these Regulations shall be resolved in accordance with the legislation of the Russian Federation through negotiations, and if such resolution is impossible, in the Arbitration Court of the Republic of Tatarstan.
The Client has the right to submit a written claim to the Bank, signed by the Authorized Representative of the Client and sealed by the latter (if applicable), by contacting the Bank’s office at its legal address. The pre-trial written procedure for resolving disputes with the Bank, within the framework of these Regulations, is mandatory. The response time to a pre-trial claim is 15 (fifteen) working days from the date of its receipt by the Bank.

11.4. In the event of changes in the provisions of the legislation of the Russian Federation, under which the provisions of these Regulations conflict with the provisions of the legislation of the Russian Federation, the provisions of the legislation of the Russian Federation shall apply to such legal relations of the Parties.

11.5. В случае признания какого-либо условия Регламента недействительным, это не влечет недействительности Регламента в целом и/или любых иных положений Регламента. Взамен недействительного положения к правоотношениям Сторон подлежат применению нормы законодательства Российской Федерации.

11.6. Банк вправе в одностороннем, внесудебном порядке вносить изменения в Регламент и/или приложения к нему. Изменения в Регламент вступают в силу и подлежат применению к правоотношениям Сторон по истечении 10 (Десяти) календарных дней с момента размещения таких изменений или новой редакции Регламента на ресурсе: https://131.ru/contracts или доведения до сведения Клиента таких изменений любым иным доступным Банку способом. До начала каждого взаимодействия с Банком с использованием Системы ДБО БИФИТ, в том числе направления в адрес Банка любого Электронного документа, а также не реже одного раза в 10 (Десять) календарных дней, Клиент и его Уполномоченные Представители обязаны знакомиться с Регламентом, а также изменениями в нем. Не ознакомление или несвоевременное ознакомление Клиента и/или его Уполномоченных Представителей с изменениями, внесенными в Регламент, не является основанием для их неприменения к правоотношениям Сторон. В случае несогласия Клиента с изменениями в Регламент, последний вправе расторгнуть Соглашение об осуществлении информационного взаимодействия с использованием Систем информационного обмена в рамках использования Системы ДБО БИФИТ ___, в порядке и на условиях, указанных в Правилах, если иное не указано в отдельном соглашении Сторон, письменно уведомив об этом Банк не позднее даты вступления таких изменений в силу, согласно Регламенту. В случае неполучения Банком, до вступления в силу изменений в Регламент письменного уведомления Клиента, изменения считаются безоговорочно принятыми Клиентом, заключение дополнительных соглашений Сторонами не требуется.

11.5. If any provision of these Regulations is declared invalid, this shall not invalidate the Regulations as a whole and/or any other provisions of these Regulations. In place of the invalid provision, the norms of the legislation of the Russian Federation shall apply to the legal relations of the Parties.

11.6. The Bank has the right to unilaterally and out of court amend these Regulations and/or its appendices. Amendments to these Regulations shall enter into force and apply to the legal relations of the Parties after 10 (ten) calendar days from the date of publication of such amendments or the new version of the Regulations on the resource: https://131.ru/contracts or notification of the Client of such amendments by any other means available to the Bank. Before each interaction with the Bank using the BIFIT RBS, including sending any Electronic Document to the Bank, as well as at least once every 10 (ten) calendar days, the Client and its Authorized Representatives are obliged to familiarize themselves with these Regulations and any amendments thereto. Failure to familiarize or untimely familiarization of the Client and/or its Authorized Representatives with amendments to these Regulations is not grounds for their non-application to the legal relations of the Parties. In case of the Client's disagreement with amendments to these Regulations, the Client has the right to terminate the Agreement on Information Interaction Using Information Exchange Systems within the framework of using the BIFIT RBS ___, in the manner and under the conditions specified in the Rules, unless otherwise provided in a separate agreement between the Parties, by notifying the Bank in writing no later than the date such amendments enter into force, in accordance with these Regulations. If the Bank does not receive written notification from the Client before the amendments to these Regulations enter into force, the amendments are considered unconditionally accepted by the Client, and no additional agreements between the Parties are required.

12.СПИСОК ПРИЛОЖЕНИЙ

12.1 Приложение №1 Заявление о присоединении к Регламенту дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ

12.2. **Приложение №2** Акт приема-передачи ФКН Системы ДБО БИФИТ

12.3. Приложение №3 Заявление о смене логина и статического пароля /разблокировку доступа в системе ДБО БИФИТ /смене Абонентского номера

12.4. Приложение №4 Уведомление о компрометации ключа Электронной подписи (прекращении действия средства подтверждения и(или) об утрате средства подтверждения, и (или) об использовании Системы ДБО БИФИТ без согласия Клиента)

12.5. Приложение №5 Инструкция по обеспечению информационной безопасности при работе в Системе ДБО БИФИТ

12.6. Приложение №6 Требования к программно-техническим средствам для проведения расчетных операций в электронной форме в Системе ДБО БИФИТ

12.7. Приложение №7 Заявление на установление ограничений по параметрам операций с использованием Системы дистанционного банковского обслуживания БИФИТ АО «Банк 131»

12.8. Приложение №8 Сертификат ключа проверки электронной подписи сотрудника клиента в системе "iBank" ДБО БИФИТ

12.LIST OF APPENDICES

12.1 Appendix No. 1: Application for Joining the Regulations on Remote Banking Services for Credit Institutions at Bank 131 JSC Using the BIFIT RBS.

12.2. Appendix No. 2: Act of Acceptance and Transfer of the Functional Key Carrier (FKC) of the BIFIT RBS.

12.3. Appendix No. 3: Application for Changing the Login and Static Password / Unblocking Access to the BIFIT RBS / Changing the Subscriber Number.

12.4. Appendix No. 4: Notice of Compromise of the Electronic Signature Key (Termination of the Confirmation Tool and/or Loss of the Confirmation Tool, and/or Unauthorized Use of the BIFIT RBS Without the Client's Consent).

12.5. Appendix No. 5: Information Security Guidelines for Working in the BIFIT RBS.

12.6. Appendix No. 6: Requirements for Software and Hardware for Conducting Settlement Operations in Electronic Form in the BIFIT RBS.

12.7. Appendix No.7: Application for Setting Restrictions on Transaction Parameters Using the BIFIT Remote Banking System of Bank 131 JSC.

12.8. Appendix No. 8: Electronic Signature Verification Key Certificate of the Client's Employee in the "iBank" BIFIT RBS.

Приложение №1 к Регламенту дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ

АО «Банк 131»
420012, РФ, Республика Татарстан,
г. Казань, ул. Некрасова, д. 38
ИНН/ОГРН 1655505780/1241600056390

_____ _____202_

Заявление[1] №_____

о присоединении к Регламенту дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ	
ФИО	
Серия и номер паспорта	
Орган и дата выдачи паспорта	
Действующий на основании _	
От имени Клиента	
ОГРН	
Адрес электронной почты[2]	
Абонентский номер[3]	

Настоящим сообщаю АО «Банк 131» что полностью и безусловно соглашаюсь с Регламентом дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ (далее – Регламент), ознакомлен и согласен с Регламентом, включая его приложения, и обязуюсь соблюдать все положения Регламента при использовании Системы ДБО БИФИТ (далее – Система ДБО БИФИТ).

Прошу зарегистрировать меня в Системе ДБО БИФИТ АО «Банк 131» и:
☐выдать ФКН Рутокен и выпустить Сертификат ключа проверки электронной подписи согласно разделу 4 Регламента;
☐ выдать Облачную подпись, выпустить Сертификат ключа проверки электронной подписи согласно разделу 4 Регламента и установить Абонентский номер, указанный в настоящем заявлении, для доступа в Систему ДБО БИФИТ
☐ ***(используется для Уполномоченных Представителей Клиента с правом просмотра)*** установить Абонентский номер, указанный в настоящем заявлении, для доступа в Систему ДБО БИФИТ, а также Одноразовых кодов для аутентификации.
☐Уведомления о совершенных операциях прошу направлять:

☐	*по адресу электронной почты*
☐	*на Абонентский номер*

Прошу установить следующую кодовую информацию:
вопрос:_____ ответ: _____

Настоящим подтверждаю, что указанные в настоящем заявлении Абонентский(-ие) номер (-а) и адрес электронной почты принадлежат исключительно и только мне, иные лица не имеют доступа к ним.
С Приложениями №6,7 к Регламенту ознакомлен и согласен, обязуюсь выполнять требования, указанные в них.

Уполномоченное лицо Клиента: _____ _____ *« ____» _____ 20 ___ г.*
(подпись) (расшифровка подписи)
МП

[1] Номер Заявления присваивается после регистрации Уполномоченного Представителя Клиента в реестрах Системы ДБО БИФИТ.
[2] Указывается адрес электронной почты уполномоченного лица. Поле обязательно для заполнения.
[3] Указывается Абонентский номер уполномоченного лица. Поле обязательно для заполнения.

Заполняется Банком

Идентификация Уполномоченного лица Клиента проведена, полномочия и документы проверены, Заявление зарегистрировано в Банке «____» _____ 20____ г.

_____ _____ _____ « ___» ___ 20 __ г.
(должность) (подпись) (расшифровка подписи.)

Отметка об исполнении:

Заявление выполнено, присвоен № _____ **:**

_____ _____ _____ « ___» ___ 20 __ г.
(должность) (подпись) (расшифровка подписи.)

Bank 131 JSC (Bank)
Nekrasova 38, Kazan, Republic of Tatarstan, 420012
INN/OGRN 1655505780/1241600056390

_____ _____202_

Application[1] No./ Заявление №_____

о присоединении к Регламенту дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ	**on joining the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs**
Full name / ФИО	
Passport series and number/Серия и номер паспорта	
Authority issued the passport and date of the issue/Орган и дата выдачи паспорта	
Acting on the basis of / Действующий на основании _	
On behalf of the Client / От имени Клиента	
Registration No. / Регистрационный №	
e-mail address/Адрес электронной почты[2]	
Subscriber Number/ Абонентский номер[3]	

Настоящим сообщаю АО «Банк 131» что полностью и безусловно соглашаюсь с Регламентом дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ (далее – Регламент), ознакомлен и согласен с Регламентом, включая его приложения, и обязуюсь соблюдать все положения Регламента при использовании Системы ДБО БИФИТ (далее – Система ДБО БИФИТ).

I hereby inform Bank 131 JSC that I fully and unconditionally agree with the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs (hereinafter referred to as the Regulations), have read and agree with the Regulations, including their annexes, and will comply with all the provisions of the Regulations when using the RBS system.

I hereby request to register me in the RBS System of Bank 131 JSC and:
/Прошу зарегистрировать меня в Системе ДБО БИФИТ АО «Банк 131» и:

☐ issue Rutoken FKM and issue an electronic signature verification key certificate in accordance with Section 4 of the Rules; / выдать ФКН Рутокен и выпустить Сертификат ключа проверки электронной подписи согласно разделу 4 Регламента;
☐ issue a Cloud Signature and set the Subscriber Number specified in this application to send a Login and a Temporary Password to access the RB System and activate the Cloud Signature key. / выдать Облачную подпись, выпустить Сертификат ключа проверки электронной подписи согласно разделу 4 Регламента и установить Абонентский номер, указанный в настоящем заявлении, для доступа в Систему ДБО БИФИТ
☐***(используется для Уполномоченных Представителей Клиента с правом просмотра)*** set the Subscriber number specified in this application for sending the Login and Temporary Password for access to the RBS System, as well as One-Time Codes for authentication/ установить Абонентский номер, указанный в настоящем заявлении, для доступа в Систему ДБО БИФИТ, а также Одноразовых кодов для аутентификации.
☐ I hereby request to send notifications of transactions/Уведомления о совершенных операциях прошу направлять:

☐ at e-mail address: / по адресу электронной почты

☐ to the Subscriber number: / на Абонентский номер

I hereby request to set the following code information
/ Прошу установить следующую кодовую информацию:

[1] The Application number is assigned after the Client's Authorized Person has been registered in the registers of the RBS System. / Номер Заявления присваивается после регистрации Уполномоченного Представителя Клиента в реестрах Системы ДБО БИФИТ.
[2] The e-mail address of the authorized person is indicated. Required field. / Указывается адрес электронной почты уполномоченного лица. Поле обязательно для заполнения.
[3] The subscriber number of the authorized person is indicated. Required field. / Указывается Абонентский номер уполномоченного лица. Поле обязательно для заполнения.

Question / вопрос: _____ _ answer / ответ: _____

Настоящим подтверждаю, что указанные в настоящем заявлении Абонентский номер и адрес электронной почты принадлежат исключительно и только мне, иные лица не имеют доступа к ним.
С Приложениями №6,7 к Регламенту ознакомлен и согласен, обязуюсь выполнять требования, указанные в них.

I hereby confirm that the Subscriber number and e-mail address specified in this application belong exclusively and only to me, other persons have no access to them.
I will comply with the requirements specified in Appendices No. 6, 7 to the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs have been read and agreed.

Authorized Representative of the Client:
/ Уполномоченное лицо Клиента: _____ _____ ____ _____ *20* ___ .
(signature) (printed)

Seal (if any)

To be filled in by the Bank / Заполняется Банком

Идентификация Уполномоченного лица Клиента проведена, полномочия и документы проверены, Заявление зарегистрировано в Банке «____» _____ 20____ г.

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Отметка об исполнении:
Заявление выполнено, присвоен № _____ **:**

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Приложение №2 к Регламенту дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ

АКТ № ___
приема-передачи ФКН Системы ДБО БИФИТ

г. Казань «___» _____20__ г.

АО «Банк 131», именуемое в дальнейшем Банк в лице _____, действующего(-ей) на основании _____ с одной стороны, и _____ , именуемый в дальнейшем «Клиент», в лице____ _____, действующего(-ей) на основании _____, с другой стороны, совместно именуемые – «Стороны», а по отдельности – «Сторона», в рамках Регламента дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ (далее – «Регламент») (заявление о присоединении №_____ от ___ _____ 20__ г.), составили настоящий Акт о нижеследующем:

Банком передан, а Клиентом принят Конверт с персональным (-и) отчуждаемым (-и) носителем (-ми), предназначенным (-ми) для хранения и использования усиленной неквалифицированной Электронной подписи (далее- ФКН), целостность которого не нарушена, с целью использования Системы ДБО БИФИТ в соответствии с Правилами открытия и ведения корреспондентских счетов в АО «Банк 131», Условиями осуществления информационного взаимодействия с использованием Системы информационного обмена и Регламентом с использованием Системы ДБО БИФИТ:

п/п	ФИО (Уполномоченного лица клиента)	ФКН
1.		электронный ключ Рутокен «Рутокен ЭЦП 2.0» №_____

Передал
АО «Банк 131»
420012, Республика Татарстан,
г. Казань, ул. Некрасова, д. 38
ИНН/ОГРН 1655505780/1241600056390

Принял
Наименование
Адрес
ИНН/ОГРН

от Банка: **от Клиента:**

_____ _____
(должность) (должность) М.П.

_____ _____ _____ _____
(подпись) (расшифровка подписи) (подпись) (расшифровка подписи)

Acceptance and Delivery Certificate No.
of FKM of the RBS System BIFIT /
АКТ № ___
приема-передачи ФКН Системы ДБО БИФИТ

Kazan _____20 _

АО «Банк 131», именуемое в дальнейшем Банк в лице _____,
Действующего(-ей) на основании _____
с одной стороны, и _____
именуемое в дальнейшем Клиент,
в лице _____,
действующего(-ей) на основании _____
с другой стороны, совместно именуемые – «Стороны», а по отдельности – «Сторона», в рамках Регламента дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ (далее - Регламент) (заявление о присоединении
№_____ от ___ _____ 20__ г.),
составили настоящий Акт о нижеследующем:

Bank 131 JSC, hereinafter referred to as the Bank represented by _____
acting under _____
on the one part, and _____
hereinafter referred to as the Client`s Authorized person
represented by _____
acting under _____
on the other part, referred together herein as Parties and individually as a Party, within the scope of the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs (Application on joining
No. _____ dated _____ _____20__), have drawn up this Act as follows:

Банком передан, а Клиентом принят Конверт с персональным (-и) отчуждаемым (-и) носителем (-ми), предназначенным (-ми) для хранения и использования усиленной неквалифицированной Электронной подписи (далее- ФКН), целостность которого не нарушена, с целью использования Системы ДБО БИФИТ в соответствии с Правилами открытия и ведения корреспондентских счетов в АО «Банк 131», Условиями осуществления информационного взаимодействия с использованием Системы информационного обмена и Регламентом с использованием Системы ДБО БИФИТ:

The Bank has transferred, and the Client has accepted an Envelope with the personal alienated carrier(s) intended for storage and use of the enhanced non-certified Electronic Signature (hereinafter referred to as the FKM), the integrity of which has not been violated, for the purpose of using the RBS system in accordance with the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs and the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC corporate clients:

n/a	Full name (Client`s Authorized person) / ФИО (Уполномоченного лица клиента)	FKM / ФКН
1.		Rutoken ES 2.0 electronic key No. ____

Transferred to
Bank 131 JSC (Bank)
Nekrasova 38, Kazan, Republic of Tatarstan, 420012
INN/OGRN 1655505780/1241600056390

from the Bank:

(title)

(signature)

Accepted
Name _____
Address _____
Reg. No._____

from the Client:

(title)

(signature)

Приложение №3 к Регламенту дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ

Заявление
о смене логина и статического пароля
/разблокировку доступа в системе ДБО БИФИТ/смене Абонентского номера

г. Казань **«___» _____20__ г.**

ФИО	
Серия и номер паспорта	
Орган и дата выдачи паспорта	
Действующий на основании _	
От имени Клиента	
ОГРН	
Адрес электронной почты[1]	
Абонентский номер[2]	

В соответствии с Регламентом дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ (далее - Система ДБО БИФИТ) прошу:

☐ – разблокировать доступ в Систему ДБО БИФИТ, с использованием ранее предоставленных данных для доступа (с условиями и причинами блокировки согласен, претензий к АО «Банк 131» не имею);

☐ - установить новый Абонентский номер для доступа в Систему ДБО БИФИТ, прохождения процедуры аутентификации и подписания Электронных документов при ее использовании, для указанных Уполномоченных лиц: +(___)_____;

☐Уведомления о совершенных операциях прошу направлять:

☐ по адресу электронной почты

☐ на Абонентский номер:

Настоящим подтверждаю, что указанный в настоящем заявлении Абонентский номер принадлежит исключительно и только мне, иные лица не имеют доступа к нему.

_____ /_____/«___» _____20___г /
(Подпись) (ФИО) (Дата)

М.П.

Заполняется Банком

Идентификация Уполномоченных лиц Клиента проведена, полномочия и документы проверены
Заявление зарегистрировано в Банке «____» _____ 20____ г.

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Работник Банка, проверивший ЭП:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Отметка об исполнении:
Ответственный работник Банка**:**
_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

[1] Укажите адрес электронной почты уполномоченного лица. Обязательное поле
[2] Укажите абонентский номер уполномоченного лица. Обязательное поле.

Заявление
о смене логина и статического пароля /разблокировку доступа в системе ДБО БИФИТ/смене Абонентского номера

Application
on login and static password change / unlocking RBS system BIFIT access / subscriber number of mobile communication change

Kazan ___ _____ **20**___

Full name / ФИО	
Passport series and number/Серия и номер паспорта	
Authority issued the passport and date of the issue/Орган и дата выдачи паспорта (если Орган отсутствует – указать только дату выдачи)	
Acting on the basis of / Действующий на основании	
On behalf of the Client / От имени Клиента	
Registration No. / Регистрационный №	
e-mail address/Адрес электронной почты[1]	
Subscriber Number/ Абонентский номер[2]	

В соответствии с Регламентом дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ (далее - Регламент) прошу:

In accordance with the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs, I hereby request to:

☐ - unblock access to the RBS System using previously provided access data (agree with the terms and ground for the blocking, no claims against Bank 131 JSC); / разблокировать доступ в Систему ДБО БИФИТ (далее – Система ДБО БИФИТ), с использованием ранее предоставленных данных для доступа (с условиями и причинами блокировки согласен, претензий к АО «Банк 131» не имею);

☐ - establish a new Subscriber number with its Login and Temporary password for access to the RBS System, for passing the procedure of authentication and confirmation of Electronic documents when using it, for the specified Authorized persons: /установить новый Абонентский номер для доступа в Систему ДБО БИФИТ, прохождения процедуры аутентификации и подтверждения Электронных документов при ее использовании, для указанных Уполномоченных лиц: + (___)_____;

☐ I hereby request to send notifications of transactions/Уведомления о совершенных операциях прошу направлять:

☐ at e-mail address: / по адресу электронной почты: _____.

☐ to the Subscriber number: / на Абонентский номер: + (____)_____.

I hereby confirm that the Subscriber number specified in this application belongs exclusively and only to me, other persons have no access to it.

Настоящим подтверждаю, что указанный в настоящем заявлении Абонентский номер принадлежит исключительно и только мне, иные лица не имеют доступа к нему.

_____/_____ /_____ _____202_ /
(Signature) (Full name) (Date)

Seal (if any)

To be filled in by the Bank / Заполняется Банком
Идентификация Уполномоченных лиц Клиента проведена, полномочия и документы проверены
Заявление зарегистрировано в Банке «____» _____ 20____ г.:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)
Работник Банка, проверивший ЭП:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

[1] The e-mail address of the authorized person is indicated. Required field.
[2] The subscriber number of the authorized person is indicated. Required field.

Отметка об исполнении:
Ответственный работник Банка**:**

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Приложение №4 к Регламенту дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ

УВЕДОМЛЕНИЕ
о компрометации ключа Электронной подписи
(прекращении действия средства подтверждения и(или) об утрате средства подтверждения, и (или) об использовании Системы ДБО БИФИТ без согласия Клиента)

г. Казань «_»_____20__г.

ФИО	
Серия и номер паспорта	
Орган и дата выдачи паспорта	
Действующий на основании _	
От имени Клиента	
ОГРН	

в соответствии с Регламентом дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ (далее - Регламент), настоящим уведомляю АО «Банк 131» о Компрометации Электронной подписи в связи с

_____
_____
_____
_____

(*дата Компрометации ЭП/утраты ЭСП и (или) его использования без согласия Клиента, обстоятельства такой компрометации/утраты и (или) такого использования, подтверждения (при наличии) такой компрометации/утраты и (или) такого использования*)

Прошу с «____» _____20__г. заблокировать указанные ниже Средства подтверждения, использовавшиеся в рамках Регламента согласно заявлению о присоединении № _____ от «__»_____ _____20__г., и остановить обработку Электронных документов, подписанных/подтвержденных указанными средствами:

☐Сертификаты ключей Электронной подписи:

№	Ф.И.О. владельца – Уполномоченного лица	Серийный номер Сертификата ключа Электронной подписи
1		

☐Облачная подпись

№	Ф.И.О. владельца-Уполномоченного лица	Абонентский номер мобильного устройства
1		

_____ /_____/«___» _____20___г /
(Подпись) (ФИО) (Дата)

М.П.

Заполняется Банком

Идентификация Уполномоченных лиц Клиента проведена, полномочия и документы проверены, Заявление зарегистрировано в Банке «____» _____:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Работник Банка, проверивший ЭП:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Отметка об исполнении:
Ответственный работник Банка**:**
_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

УВЕДОМЛЕНИЕ
о компрометации ключа Электронной подписи (прекращении действия средства подтверждения и(или) об утрате средства подтверждения и (или) об использовании Системы ДБО БИФИТ без согласия Клиента)

NOTICE
on compromising the key of the Electronic Signature (termination of the means of confirmation and/or loss of the means of confirmation and/or use of the RBS System BIFIT without the consent of the Client)

Kazan ___ _____20__

Full name / ФИО	
Passport series and number/Серия и номер паспорта	
Authority issued the passport and date of the issue/Орган и дата выдачи паспорта (если Орган выдачи отсутствует, то указать только дату выдачи)	
Acting on the basis of / Действующий на основании	
On behalf of the Client / От имени Клиента	
Registration No. / Регистрационный №	

в соответствии с Регламентом дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ (далее - Регламент), настоящим уведомляет АО «Банк 131» с использованием Системы ДБО БИФИТ о Компрометации Электронной подписи в связи с

In accordance with the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs hereby notifies Bank 131 JSC on the Electronic Signature Compromise in connection with

_____

_____

_____

_____

(дата Компрометации ЭП/утраты ЭСП и (или) его использования без согласия Клиента, обстоятельства такой компрометации/утраты и (или) такого использования, подтверждения (при наличии) такой компрометации/утраты и (или) такого использования)

(date of ES Compromising/Loss of ES and/or its use without the Client's consent, circumstances of such Compromising/Loss and/or such use, confirmation (if any) of such Compromising/Loss and/or such use)

Прошу заблокировать указанные ниже Средства подтверждения, использовавшиеся в рамках Регламента согласно заявлению о присоединении
№ _____ от «__»_____20__г.,
с «____» _____20__г.
и остановить обработку Электронных документов, подписанных/подтвержденных указанными средствами: Сертификаты ключей Электронной подписи, содержащие следующие ключи Электронной подписи:

I hereby request to block Means of Confirmation noted below that were used within the scope of the Regulations on Remote Banking Service in the 'Banking App' system for Bank 131 JSC Corporate Clients and individual entrepreneurs according to Application on joining

No. _____ dated _____20__
since ____ _____ 20__
and stop the Electronic Documents processing that were signed/confirmed by the mentioned means:
Electronic Signature Key Certificates containing the following Electronic Signature Keys:

☐Сертификаты ключей Электронной подписи/ Certificate of the electronic signature verification key:

№	Full name of the owner - Authorized person / Ф.И.О. владельца – Уполномоченного лица	Certificates of the electronic signature verification key Serial number / Серийный номер Сертификата ключа Электронной подписи
1		

☐Subscriber mobile phone number: / Абонентский номер мобильной связи:

№	Full name of the owner, the authorized person / Ф.И.О. владельца-Уполномоченного лица	Subscriber number of the mobile device / Абонентский номер мобильного устройства
1		

☐ Cloud Signature / Облачной подписи:

№	Full name of the owner - Authorized person /Ф.И.О. владельца-Уполномоченного лица	Subscriber number of the mobile device / Абонентский номер мобильного устройства
1		

_____/_____ /_____202_ /
(Signature) (Full name) (Date)

Seal (if any)

To be filled in by the Bank / Заполняется Банком

Идентификация Уполномоченных лиц Клиента проведена, полномочия и документы проверены, Заявление зарегистрировано в Банке «____» _____ 20____ г.
Работник Банка, принявший заявление:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)
Работник Банка, проверивший ЭП:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Отметка об исполнении:
Ответственный работник Банка**:**
_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Приложение №5 к Регламенту дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ

Инструкция по обеспечению информационной безопасности при работе в Системе ДБО БИФИТ

В целях обеспечения информационной безопасности при работе в Системе ДБО БИФИТ (далее – Система ДБО БИФИТ) АО «Банк 131», **Клиент обязан:**

1. При осуществлении доступа к Системе ДБО БИФИТ, удостовериться в правильности указанного адреса в адресной строке браузера (https://bank.131.ru/) и наличии значка защищенного соединения (замок), исключая выход на сайты, внешне маскирующиеся под Систему ДБО БИФИТ.
2. При использовании Облачной подписи и/или иного вида Электронной подписи внимательно проверять информацию об Операции, полученную в СМС-сообщении или в PUSH-сообщении.
3. Своевременно устанавливать доступные обновления операционной системы и приложений.
4. Не подвергать используемое устройство операциям повышения привилегий / взлома операционной системы устройства (jail-break, rooting).
5. Использовать антивирус для устройств, своевременно устанавливать на него обновления вирусных баз.
6. Никогда не передавать свое устройство и/или sim-карту третьим лицам.
7. Ключи Усиленной неквалифицированной Электронной подписи хранить только на ФКН в недоступном для посторонних и неуполномоченных лиц месте (запирающиеся персональный сейф, металлический шкаф).
8. Не снимать копии с ФКН, не передавать ФКН лицам, к ним не допущенным, не записывать на ФКН постороннюю информацию.
9. Не использовать в качестве Статического пароля:

- последовательность символов, состоящих из одних цифр (в том числе даты, номера телефонов, номера автомобилей и т.п.);
- последовательность повторяющихся букв или цифр;
- идущие подряд в раскладке клавиатуры или в алфавите символы;
- имена и фамилии;
- ИНН или другие реквизиты Клиента/Уполномоченного Представителя Клиента.

Требования к Статическому паролю:

– Длина пароля должна быть не менее 8 символов.
– В числе символов пароля должны присутствовать строчные и прописные буквы, цифры и специальные

Appendix 5 to the Regulations on Remote Banking Services for Credit organizations at Bank 131 JSC Using the Remote Banking System (RBS) BIFIT

Information security guidelines for working in the BIFIT RBS

To ensure information security when working in the BIFIT RBS (hereinafter referred to as the "BIFIT RBS") of Bank 131 JSC, the Client is obliged to:

1. When accessing the BIFIT RBS, ensure that the address in the browser's address bar is correct (https://bank.131.ru/) and that the secure connection icon (lock) is present, avoiding websites that mimic the BIFIT RBS.
2. When using a Cloud Signature and/or any other type of Electronic Signature, carefully verify the transaction information received in an SMS or PUSH notification.
3. Promptly install available updates for the operating system and applications.
4. Avoid performing operations to gain elevated privileges or hacking the device's operating system (jailbreak, rooting).
5. Use antivirus software for devices and promptly update its virus databases.
6. Never transfer your device and/or SIM card to third parties.
7. Store Enhanced Unqualified Electronic Signature (UES) keys only on a Functional Key Carrier (FKC) in a place inaccessible to unauthorized persons (e.g., a personal safe or metal cabinet).
8. Do not make copies of the FKC, do not transfer the FKC to unauthorized persons, and do not record unrelated information on the FKC.
9. Do not use the following as a Static Password:
    - A sequence of digits only (including dates, phone numbers, car numbers, etc.);
    - A sequence of repeating letters or numbers;
    - Consecutive characters on the keyboard or in the alphabet;
    - Names and surnames;
    - Taxpayer Identification Number (TIN) or other details of the Client/Authorized Representative of the Client.

Requirements for Static Passwords:

- The password length must be at least 8 characters.
- The password must include lowercase and

символы (!, ", #, $, %, &, ', (,), *, +, -, ., /, @, :, ;, <, =, >, ?, [, \,], ^, _, `, {, }, ~);
- Запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему, а также выбирать пароли, которые уже использовались ранее;
- Личный пароль Клиент не имеет права сообщать никому;
- При смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 4 символа;
- Срок действия пароля пользователя не более 1года (365 дней).
- Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).
- После 5-и неудачных попыток ввода пароля, учетная запись Клиента блокируется до выяснения причин ввода неправильного пароля.
- Строго запрещается записывать пароли на бумажных носителях или в текстовых файлах на рабочем месте, оставлять их в доступных третьим лицам местах, передавать неуполномоченным лицам.

Необходимо:

- Установить на персональном компьютере (ноутбуке) парольную защиту на вход в Операционную систему.
- Хранить пароль доступа к ключу УНЭП отдельно от ФКН.
- Подключать ФКН, содержащий ключ ЭП, только в момент использования Системы ДБО БИФИТ и подписания Электронных документов. Не оставлять ФКН, содержащий ключ ЭП, постоянно подключенным к компьютеру.
- Не использовать ФКН, содержащий ключ ЭП, для каких-либо других целей, в частности, не хранить на нём информацию произвольного содержания, не относящегося к работе с Системой ДБО БИФИТ.
- Не копировать содержимое ФКН, содержащего ключ ЭП, и не передавать его никому даже на короткое время.
- Закончив работу в Системе ДБО БИФИТ или прервав её (даже на несколько минут), извлечь ФКН, содержащий ключ УНЭП, и убрать его в недоступное другим лицам место.
- Применять на рабочем месте лицензионные средства защиты от вредоносного кода с возможностью автоматического обновления баз данных сигнатур вредоносного кода.
- Если в качестве компьютера для работы в Системе ДБО БИФИТ используется переносной компьютер (ноутбук), исключить его подключение к сетям общего доступа в местах свободного доступа в Интернет (офисные центры, кафе и пр.)

uppercase letters, numbers, and special characters (!, ", #, $, %, &, ', (,), *, +, -, ., /, @, :, ;, <, =, >, ?, [, ,], ^, _, `, {, }, ~);

- It is prohibited to use an "empty" password, the system login name, or previously used passwords;
- The Client must not disclose their personal password to anyone;
- When changing the password, the new combination of characters must differ from the previous one by at least 4 characters;
- The password validity period must not exceed 1 year (365 days);
- The password must not include easily guessable combinations of characters (names, surnames, workstation names, etc.) or common abbreviations (e.g., PC, LAN, USER, etc.);
- After 5 unsuccessful password attempts, the Client's account will be blocked until the reasons for the incorrect password entry are clarified;
- It is strictly prohibited to write passwords on paper or in text files at the workplace, leave them in places accessible to third parties, or disclose them to unauthorized persons.

Additional Requirements:

- Set password protection for the operating system on the personal computer (laptop).
- Store the password for accessing the UES key separately from the FKC.
- Connect the FKC containing the Electronic Signature key only when using the BIFIT RBS and signing Electronic Documents. Do not leave the FKC containing the Electronic Signature key permanently connected to the computer.
- Do not use the FKC containing the Electronic Signature key for any other purposes, particularly do not store arbitrary information unrelated to working with the BIFIT RBS on it.
- Do not copy the contents of the FKC containing the Electronic Signature key or transfer it to anyone, even temporarily.
- After finishing work in the BIFIT RBS or interrupting it (even for a few minutes), remove the FKC containing the UES key and store it in a place inaccessible to others.
- Use licensed anti-malware software with automatic updates for malware signature databases at the workplace.
- If a portable computer (laptop) is used for working in the BIFIT RBS, avoid connecting it to public networks in places with free Internet access (office centers, cafes, etc.).
- Continuously monitor payment (settlement) documents sent when working with the BIFIT RBS, as well as the status of settlement (bank)

– Осуществлять постоянный контроль отправляемых платежных (расчетных) документов при работе с Системой ДБО БИФИТ, а также за состоянием расчетных (банковских) счетов, операциям по ним и остаткам.
– В случае выявления признаков Компрометации ЭП или выявления вредоносного кода в компьютере, используемом для работы в Системе ДБО БИФИТ, необходимо немедленно уведомить Банк по телефонам: 8 (800) 100 13 10 с 9 часов 00 минут до 18 часов 00 минут (в рабочие дни), либо лично явиться в Банк с целью блокирования скомпрометированных ключей ЭП с последующей их заменой.

К событиям, связанным с Компрометацией Электронной подписи, в том числе, относятся:

– утрата ФКН, с последующим обнаружением или без такового;
– нарушение правил хранения, использования и уничтожения (в том числе после окончания срока действия) ключа УНЭП;
– утеря, передача и/или предоставлением доступа неуполномоченным третьим лицам к аппаратным средствам (в том числе мобильным телефонам или иным) и/или SIM-карте с Абонентским номером, в том числе который используется для направления Временного и/или Одноразового пароля;
– наличие подозрений, что Средства подтверждения Электронного документа стали известны неуполномоченным третьим лицам;
– возникновение подозрений на утечку информации или ее искажение;
– несанкционированное копирование или подозрение на копирование Временного, Статического пароля, функционального ключевого носителя, аппаратного средства и/или SIM-карты с Абонентским номером;
– несанкционированный доступ к адресу электронной почты, указанному в Заявлении;
– прекращение полномочий или увольнение Уполномоченных лиц, имеющих доступ к Средству подтверждения;
– случаи, когда нельзя достоверно установить, что произошло с ФКН (в том числе случаи, когда носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий третьих лиц, другие виды разглашения ключевой информации).

При обнаружении несанкционированных доступов в Систему ДБО БИФИТ, платежных и иных операций в Системе ДБО БИФИТ, Компрометации или подозрении на Компрометацию Электронной

accounts, transactions, and balances.
- In case of detecting signs of compromise of the Electronic Signature or malware on the computer used for working in the BIFIT RBS, immediately notify the Bank by phone: 8 (800) 100 13 10 from 9:00 AM to 6:00 PM (on business days), or personally visit the Bank to block the compromised Electronic Signature keys and replace them.

Events related to the compromise of the Electronic Signature include:

- Loss of the FKC, with or without subsequent discovery;
- Violation of the rules for storage, use, and destruction (including after expiration) of the UES key;
- Loss, transfer, and/or provision of access to unauthorized third parties to hardware (including mobile phones or other devices) and/or SIM cards with a subscriber number, including those used for sending Temporary and/or One-Time Passwords;
- Suspicions that the Electronic Document Confirmation Tools have become known to unauthorized third parties;
- Suspicions of information leakage or distortion;
- Unauthorized copying or suspicion of copying Temporary, Static Passwords, Functional Key Carriers, hardware, and/or SIM cards with a subscriber number;
- Unauthorized access to the email address specified in the Application;
- Termination of authority or dismissal of Authorized Persons with access to the Confirmation Tools;
- Cases where it is impossible to reliably determine what happened to the FKC (including cases where the carrier has malfunctioned, and it cannot be conclusively disproven that this occurred as a result of unauthorized actions by third parties, or other types of disclosure of key information).

If unauthorized access to the BIFIT RBS, payment, or other operations in the BIFIT RBS, or compromise or suspicion of compromise of the Electronic Signature is detected, immediately notify the Bank and send a "Notice of Compromise" in the manner established by the Regulations on Remote Banking Services for Credit Institutions at Bank 131 JSC using the BIFIT RBS, and file a corresponding report with law enforcement agencies.

Prohibitions:

подписи немедленно уведомить Банк и направить «Уведомление о компрометации» в порядке, установленном Регламентом дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ, а также обратиться с соответствующим заявлением в правоохранительные органы.

Запрещено восстанавливать работоспособность поврежденного компьютера до проведения технической экспертизы. Работу с Системой ДБО БИФИТ разрешено проводить только после новой установки операционной системы с форматированием жестких дисков и после смены всех ключей ЭП клиента.

Требования:

- Отключить возможность удаленного и терминального соединения к компьютерам, используемым для работы по Системе ДБО БИФИТ, заблокировать 3389 (RDP Remote desktop).
- Включить в операционной системе журнал безопасности Windows.
- Использовать только лицензионное программное обеспечение – операционные системы, средства защиты от вредоносного кода, офисные пакеты и т.д. (далее по тексту – ПО).
- Обеспечить возможность своевременного обновления системного и прикладного ПО.
- Доступ в помещение, где размещен компьютер с Системой ДБО БИФИТ, предоставлять только Уполномоченным лицам.
- Компьютер, с которого осуществляется подготовка и отправка Электронных документов в Банк, рекомендуется выделить в отдельный сегмент сети с обязательным исключением его из общей локальной сети клиента.
- Исключить доступ к компьютерам, используемым для работы в Системе ДБО БИФИТ, посторонних лиц и персонала, неуполномоченных на работу в Системе ДБО БИФИТ и/или обслуживание компьютеров.
- При обслуживании компьютера ИТ-сотрудниками обеспечивать контроль над выполняемыми ими действиями.
- Запрещено передавать логины и пароли третьим лицам в том числе иным Уполномоченным Представителям Клиента.

АО «Банк 131» не осуществляет рассылку электронных писем с просьбой прислать ключи Электронных подписей и/или пароль к Системе ДБО БИФИТ и никогда не запрашивает у Клиента эту информацию.

Банк не осуществляет звонков, рассылку сообщений по электронной почте, SMS-сообщений, или иными

- Do not restore the functionality of a damaged computer before conducting a technical examination. Work with the BIFIT RBS is permitted only after reinstalling the operating system with formatting of the hard drives and replacing all of the Client's Electronic Signature keys.

Requirements:

- Disable remote and terminal connections to computers used for working with the BIFIT RBS, block port 3389 (RDP Remote Desktop).
- Enable the Windows security log in the operating system.
- Use only licensed software—operating systems, anti-malware tools, office suites, etc. (hereinafter referred to as "Software").
- Ensure the ability to promptly update system and application software.
- Grant access to the room where the computer with the BIFIT RBS is located only to Authorized Persons.
- It is recommended to isolate the computer used for preparing and sending Electronic Documents to the Bank in a separate network segment, excluding it from the Client's general local network.
- Prohibit access to computers used for working in the BIFIT RBS by unauthorized persons and personnel not authorized to work in the BIFIT RBS or service the computers.
- When servicing the computer by IT staff, ensure control over their actions.
- It is prohibited to transfer logins and passwords to third parties, including other Authorized Representatives of the Client.

Important Notes:

Bank 131 JSC does not send emails requesting the submission of Electronic Signature keys and/or passwords for the BIFIT RBS and never requests this information from the Client.

The Bank does not make phone calls, send emails, SMS messages, or use other methods to request confidential information (passwords, code words, etc.). If such a request is received, under no circumstances should the Client disclose this information and must immediately report it to the Bank.

способами, с просьбой сообщить конфиденциальную информацию (пароли, кодовые слова, и пр.). При получении такого запроса ни при каких обстоятельствах Клиент не должен сообщать данную информацию и должен немедленно сообщить об этом в Банк.

Приложение №6 к Регламенту дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ

Требования к программно-техническим средствам для проведения расчетных операций в электронной форме с использованием Системы ДБО БИФИТ (далее – Система ДБО БИФИТ)

1. Требования к программно-техническим средствам (приобретаются Клиентом за собственный счет у третьих лиц):

1.1. При использовании УНЭП:

- Персональный компьютер с портом USB и предустановленной операционной системой (ОС) Windows 7 и выше, MacOS[1]

- Интернет-браузер актуальной версии: Chrome 47 и выше / Firefox 44.0 и выше / Internet Explorer 10 и выше / Opera 36 и выше / Safari 9 и выше;

- доступ в сеть Интернет;

- принтер.

1.2 При использовании Облачной подписи:

-устройство с iOS (три последние версии системы);

- устройство Android — с версии 5.0 и более поздние версии.

2. Для использования Системы ДБО БИФИТ с применением УНЭП необходим выделенный компьютер с предустановленной операционной системой семейства Microsoft Windows. Если, по желанию Клиента, установка Системы ДБО БИФИТ производится на компьютер с предустановленными ОС сторонних производителей, Банк не несет ответственности за работоспособность Системы ДБО БИФИТ.

При эксплуатации Системы ДБО БИФИТ **запрещается:**

- Установка программного обеспечения сторонних фирм, а также сознательное внесение изменений в файлы программного и информационного обеспечения Системы ДБО БИФИТ;
- Доступ к Системе ДБО БИФИТ неуполномоченных лиц;

При эксплуатации Системы ДБО БИФИТ Клиент обязан:

Appendix No. 6 to the Regulations on Remote Banking Services for Credit Institutions at Bank 131 JSC Using the BIFIT RBS

Requirements for Software and Hardware for Conducting Settlement Operations in Electronic Form Using the BIFIT RBS (hereinafter referred to as the "BIFIT RBS")

1. Requirements for Software and Hardware (purchased by the Client at their own expense from third parties):

1.1. When using an Enhanced Unqualified Electronic Signature (UES):

- A personal computer with a USB port and a pre-installed operating system (OS) Windows 7 or higher, MacOS;
- An up-to-date version of an internet browser: Chrome 47 and above / Firefox 44.0 and above / Internet Explorer 10 and above / Opera 36 and above / Safari 9 and above;
- Internet access;
- A printer.

1.2. When using a Cloud Signature:

- A device with iOS (the three latest versions of the system);
- A device with Android—version 5.0 and later versions.

2. To use the BIFIT RBS with a UES, a dedicated computer with a pre-installed Microsoft Windows operating system is required. If, at the Client's request, the BIFIT RBS is installed on a computer with pre-installed third-party operating systems, the Bank is not responsible for the functionality of the BIFIT RBS.

Prohibited Actions When Using the BIFIT RBS:

- Installation of third-party software, as well as intentional modification of the software and information files of the BIFIT RBS;
- Access to the BIFIT RBS by unauthorized persons.

Obligations of the Client When Using the BIFIT RBS:

- Use the BIFIT RBS only on a functional and virus-free personal computer (laptop);
- Prevent the computer with the installed BIFIT

[1] Инструкция по работе с MacOS размещена на официальном сайте Банка.

- Использовать систему ДБО БИФИТ только на исправном и проверенном на отсутствие компьютерных вирусов персональном компьютере (ноутбуке);
- Исключить возможность заражения компьютера с установленной Системой ДБО БИФИТ программными вирусами или другими вредоносными программами;
- Использовать только легальное и лицензионное программное обеспечение;
- Обеспечить техническую исправность оборудования, входящего в состав рабочего места Системы ДБО БИФИТ;
- Применять средства антивирусной защиты и обеспечить регулярное обновление антивирусных баз.

Необходимость резервного копирования рабочего места пользователя Системы ДБО БИФИТ определяет Клиент и при необходимости осуществляет его собственными силами.

RBS from being infected with computer viruses or other malicious programs;

- Use only legal and licensed software;
- Ensure the technical functionality of the equipment included in the BIFIT RBS workstation;
- Use antivirus protection tools and ensure regular updates of antivirus databases.

Backup Requirements:
The need for backup of the BIFIT RBS user workstation is determined by the Client and, if necessary, is carried out by the Client independently.

Приложение №7 к Регламенту дистанционного банковского обслуживания кредитных организаций в АО «Банк 131» с использованием Системы ДБО БИФИТ

Заявление № _____
на установление ограничений по параметрам операций с использованием Системы дистанционного банковского обслуживания БИФИТ АО «Банк 131» (далее – Система ДБО БИФИТ)

ФИО	
Серия и номер паспорта	
Орган и дата выдачи паспорта	
Действующий на основании	
От имени Клиента	
ОГРН	

В соответствии с условиями Соглашения об осуществлении информационного взаимодействия с использованием Систем информационного обмена – Системы ДБО БИФИТ прошу установить ограничения по параметрам Операций по Счету(-ам) №:
_____

☐	На максимальные лимиты на операции и за период в разрезе счетов/способов подписания Номер счета / Тип подписи (УНЭП/Облачная подпись) / Период (1 операция/1 день/1 неделя/1 месяц) / Максимальная сумма перевода денежных средств в валюте Счета	
☐	перечень разрешенных получателей денежных средств (указываются наименование, реквизиты получателей денежных средств)	1. Наименование получателя _____ Номер счета _____ БИК_____ ИНН(если есть)_____ 2. …
☐	разрешенный временной период для совершения операций (указывается временной период приема Распоряжений о переводе денежных средств в часовом поясе UTC+3)	
☐	страны, находясь в которых Клиент может совершать переводы денежных средств (используется определение географического расположения по IP адресу[1] устройства, с которого осуществляется доступ в Систему ДБО БИФИТ)	
☐	перечень разрешенных категорий операций	☐ Платеж по шаблону, сохраненному в Системе ДБО БИФИТ ☐ Внутренний платеж (счет получателя открыт в АО «Банк 131») ☐ Внешний платеж (счет получателя открыт в другой кредитной организации) ☐ Платежи в бюджет РФ ☐ Валютный перевод

_____/_____/«__»_____20___г /
(Подпись) (ФИО) (Дата)

М.П.

[1] При использовании VPN сервисов, или анонимайзеров будет определяться конечный IP адрес устройства, с которого будет осуществлён доступ в Систему ДБО БИФИТ, что может повлечь недоступность Системы ДБО БИФИТ.

Заполняется Банком

Заявление принял ___ часов____ минут «__» _____20__г.
Работник Банка, принявший заявление:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)
(расшифровка подписи.)

Работник Банка, проверивший ЭП:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)
(расшифровка подписи.)

Ограничения установлены «__» _____20__г. (проставляется дата установки ограничений).
Ответственный работник Банка**:**

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

Application No. _____ for
the establishment of restrictions on the parameters of operations
using the Remote Banking Service System of Bank 131 JSC

/Заявление № _____
на установление ограничений по параметрам операций
с использованием Системы дистанционного банковского обслуживания АО «Банк 131»

Full name / ФИО	
Passport series and number/Серия и номер паспорта	
Authority issued the passport and date of the issue/Орган и дата выдачи паспорта (если Орган выдачи отсутствует, то указать только дату выдачи)	
Acting on the basis of / Действующий на основании	
On behalf of the Client / От имени Клиента	
Registration No. / Регистрационный №	

In accordance with the terms of the RBS System Agreement, please set restrictions on the parameters of Operations on the Account (s) No.:_____

<table>
<tr><td>☐</td><td colspan="2">For the maximum limits on transactions and for the period in the context of accounts/signing methods / На максимальные лимиты на операции и за период в разрезе счетов/способов подписания
<table><tr><td>Account No.
Номер счета</td><td>Signature Type (SES / ENCES/ Mobile Signature)/
Тип подписи (УНЭП/Облачная подпись)</td><td>Period (1 operation/1 day/1 week/1 month)
/Период (1 операция/1 день/1 неделя/1 месяц)</td><td>Maximum amount of money transfer in the Account currency /
Максимальная сумма перевода денежных средств в валюте Счета</td></tr></table></td></tr>
<tr><td>☐</td><td>list of authorized recipients of funds (specify the name and details of the recipients of funds)
/ перечень разрешенных получателей денежных средств (указываются наименование, реквизиты получателей денежных средств)</td><td>1. Наименование получателя _____
Номер счета _____
БИК_____
ИНН(если есть)_____
2. …</td></tr>
<tr><td>☐</td><td>the allowed time period for making transactions (the time period for accepting Money transfer Orders in the UTC+3 time zone is specified) / разрешенный временной период для совершения операций (указывается временной период приема Распоряжений о переводе денежных средств в часовом поясе UTC+3)</td><td></td></tr>
<tr><td>☐</td><td>countries where the Client can make money transfers (the geographical location is determined by the IP address[1] of the device from which the RBO System is accessed) / страны, находясь в которых Клиент может совершать переводы денежных средств (используется определение географического расположения по IP адресу устройства, с которого осуществляется доступ в Систему ДБО БИФИТ)</td><td></td></tr>
<tr><td>☐</td><td>list of permitted categories of operations /</td><td>☐ Payment based on a template saved in the RBS System</td></tr>
</table>

[1] When using VPN services or anonymizers, the final IP address of the device from which access to the RBS is made will be determined. This may result in the unavailability of the RBS.

	перечень разрешенных категорий операций	/ Платеж по шаблону, сохраненному в Системе ДБО БИФИТ ☐ Internal payment (the recipient's account is opened with Bank 131 JSC) / Внутренний платеж (счет получателя открыт в АО «Банк 131») ☐ External payment (the recipient's account is opened with another credit institution) / Внешний платеж (счет получателя открыт в другой кредитной организации) ☐ Payments to the budget of the Russian Federation / Платежи в бюджет РФ ☐ Currency transfer / Валютный перевод

_____/_____ /_____202_ /
(Signature) (Full name) (Date)

Seal (if any)

To be filled in by the Bank / Заполняется Банком

Заявление принял ___ часов____ минут «__» _____20__г.
Работник Банка, принявший заявление:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)
(расшифровка подписи.)
Работник Банка, проверивший ЭП:

_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)
(расшифровка подписи.)

Ограничения установлены «__» _____20__г. (проставляется дата установки ограничений).
Ответственный работник Банка**:**
_____/_____/_____ «___» _____20___г
(должность) (подпись) (расшифровка подписи) (дата)

СЕРТИФИКАТ КЛЮЧА ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ СОТРУДНИКА КЛИЕНТА В СИСТЕМЕ ДБО "БИФИТ"

1. Наименование организации _____

_____

2. Место нахождения юр. лица _____

_____

3. ОГРН* _____ дата внесения в ЕГРЮЛ (ЕГРИП)* "____" _____ года

4. ИНН (КИО) _____ 5. КПП* _____

6. Тел. _____ 7. Факс* _____ 8. E-mail* _____

9. Сведения о владельце ключа

Фамилия, имя, отчество _____

Должность _____

Документ, удостоверяющий личность _____

_____

серия _____ номер _____ дата выдачи"____" января _____ года

кем выдан _____

код подразделения _____

10. Примечания* _____

* необязательно для заполнения

Настоящим подтверждаю согласие на обработку банком моих персональных данных _____

подпись

Ключ проверки ЭП сотрудника клиента (создан ___.___.202__ г.)

Идентификатор ключа проверки ЭП ***0000000000001 Идентификатор устройства ****000001

Наименование криптосредств СКЗИ "Рутокен ЭЦП 3.0 3220"

Алгоритм ГОСТ Р 34.10-2012 256 бит (1.2.643.7.1.1.1.1) ID набора параметров алгоритма 1.2.643.2.2.35.1

Представление ключа проверки ЭП в шестнадцатеричном виде

```
45 8B 4E 20 CF DA 8F 9C 7C AB 2A 16 39 08 44 80
17 E3 9A 82 26 B4 A4 0E 75 7E E9 7C E9 35 41 4F
6E 5C 95 35 81 A1 F5 71 62 8F 1F 43 14 EE 2B 79
D7 95 A8 BF F1 B3 01 B3 06 82 31 72 03 12 71 3F
```

Личная подпись владельца ключа проверки ЭП

Срок действия (заполняется банком):

с "____" _____ 20__г.

по "____" _____ 20__г.

Сертификат ключа проверки ЭП сотрудника клиента действует в рамках договора на обслуживание в системе "iBank" N___ от "__"_____20__ г.

Достоверность приведенных данных подтверждаю

Руководитель организации

_____/_____/

подпись Ф.И.О.

Оттиск печати

Уполномоченный представитель банка

_____/_____/

подпись Ф.И.О.

Оттиск печати Банка

Дата приема сертификата ключа проверки ЭП

"___"_____20__г.

Администратор безопасности системы

_____/_____/

подпись Ф.И.О.

Оттиск печати

Дата регистрации сертификата ключа проверки ЭП

"___"_____20__г.