УТВЕРЖДЕНО

Правлением АО «Тагилбанк»

(протокол № 232 от 08.12.2017 г.)

Председатель правления

АО «Тагилбанк»

_____ **Л.Г. Пестова.**

ПОРЯДОК

дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей в АО «Тагилбанк»
с использованием доступа через информационно-телекоммуникационную сеть Интернет

(введен в действие с 21.12.2017 года
в соответствии с решением правления АО «Тагилбанк» от 08.12.2017 года № 232)

Нижний Тагил
2017 г.

Оглавление

1. Общие положения

1.1. «Порядок дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Тагилбанк» с использованием доступа через информационно-телекоммуникационную сеть «Интернет» (далее – «Порядок») устанавливает правила и условия, обязательные для исполнения юридическим лицом или индивидуальным предпринимателем (далее – Клиент) и АО «Тагилбанк» (далее – Банк), заключившими договор (в том числе любые дополнительные соглашения к нему) на использование систем «Дистанционного банковского обслуживания» (далее – ДБО). Порядок регулирует отношения сторон, возникающие в процессе оказания Банком услуг Клиенту по ДБО с использованием доступа через Интернет, порядок обмена электронными документами, в том числе по обеспечению информационной безопасности при обмене электронными документами.

1.2. Текст настоящего Порядка размещен на информационных стендах в месте нахождения Банка, в местах обслуживания Клиентов и на официальном сайте Банка в информационно-телекоммуникационной сети «Интернет».

Порядок может изменяться, дополняться Банком в одностороннем порядке и доводится до сведения Клиентов путем размещения на информационных стендах в месте нахождения Банка, в местах обслуживания Клиентов и на официальном сайте в информационно-телекоммуникационной сети «Интернет». При этом Банк обязан не менее чем за 10 (десять) календарных дней до даты введения в действие опубликовать изменения, дополнения, либо новую редакцию Порядка на официальном сайте Банка http://tagilbank.ru.

Моментом ознакомления Клиента с публично размещенным Порядком, любыми изменениями, дополнениями к нему, новыми редакциями считается момент, с которого эта информация была размещена на интернет-сайте Банка и в подразделениях Банка, обслуживающих Клиента.

1.3. Порядок и подписанное Клиентом заявление о присоединении к Порядку (Приложение № 5 к Порядку) в совокупности являются заключенным между Клиентом и Банком договором дистанционного банковского обслуживания с использованием доступа через Интернет (далее – Договор). Договор может быть заключен только при условии открытия Клиентом расчетного счета в АО «Тагилбанк».

1.4. Договор считается заключенным с момента получения Банком лично от Клиента Заявления о присоединении к Порядку (далее – Заявление). При этом Заявление должно быть:

- предоставлено Клиентом в Банк на бумажном носителе в 2-х экземплярах, по форме, установленной Банком;
- подписано Клиентом собственноручно (лично индивидуальным предпринимателем либо единоличным исполнительным органом юридического лица либо представителем Клиента по доверенности, при предъявлении документа, удостоверяющего личность);
- заполнено Клиентом надлежащим образом (сообщены достоверные сведения) и в полном объеме.

1.5. Один экземпляр Заявления остается в Банке, второй экземпляр с отметкой о принятии Банком передается Клиенту и является документом, подтверждающим факт заключения Договора.

1.6. Договор определяет условия и порядок предоставления Банком Клиенту услуг дистанционного банковского обслуживания с использованием доступа через Интернет.

1.7. Клиент вправе в любое время отказаться от ДБО, направив Банку заявление о расторжении Договора по форме, установленной Приложением № 7 к Порядку. Такое заявление должно быть подписано с соблюдением требований, указанных в пункте 1.4. Порядка.

1.8. Оказание Банком услуг ДБО в рамках Договора осуществляется в соответствии с тарифами на услуги, предоставляемыми АО «Тагилбанк» (далее – Тарифы). Банк вправе по решению Правления изменять, дополнять Тарифы в одностороннем порядке без согласования с Клиентами. Об изменениях в Тарифах Банк уведомляет Клиентов путем размещения соответствующих сообщений на информационных стендах в месте нахождения Банка, а также в местах обслуживания Клиентов и на официальном сайте в информационно-телекоммуникационной сети «Интернет» за 10 рабочих дней до ввода в действие изменений и(или) введения новых Тарифов. Тарифы становятся обязательными для сторон с момента введения их в действие.

1.9. Клиент обязан ежедневно любым доступным ему способом самостоятельно обращаться в Банк, в т.ч. на официальный сайт Банка в сети Интернет по адресу http://tagilbank.ru

для получения сведений о новой редакции, о внесенных изменениях и (или) дополнениях в Порядок, Договор и (или) Тарифы.

В случае несогласия Клиента с изменением, дополнением Порядка, Договора, Тарифов, и(или) их новыми редакциями Клиент имеет право расторгнуть Договор, письменно уведомив об этом Банк в соответствии с пунктом 1.7. Порядка.

В случае неполучения Банком до вступления в силу новых условий Договора, Порядка, Тарифов письменного уведомления о расторжении Договора, Банк считает это выражением согласия Клиента с изменениями условий Договора, Порядка, Тарифов.

1.10. В соответствии с Договором Банк в максимально короткие сроки уведомляет Клиента об операциях, совершаемых с использованием ДБО, способом, выбранным Клиентом для уведомления его об операциях по его банковскому счету (указывается в заявлении о присоединении к Порядку).

Обязанность Банка по направлению Клиенту уведомлений, предусмотренных Договором и действующим законодательством, считается исполненной при направлении уведомления в соответствии с имеющейся у Банка информацией для связи с Клиентом и в соответствии с выбранным Клиентом способом его информирования, указанным в Заявлении. Клиент считается уведомленным о совершенной операции с использованием систем ДБО с момента отправки Банком сообщения Клиенту независимо от факта получения/неполучения Клиентом сообщения.

Клиент согласен с тем, что стоимость услуг Банка по информированию о совершенных операциях с использованием систем ДБО устанавливается в соответствии с Тарифами Банка.

1.11. До заключения Договора Клиент ознакомлен:

- с настоящим Порядком (в редакции, действующей на момент заключения Договора, размещенной на информационных стендах в месте нахождения Банка, а также в местах обслуживания клиентов и на официальном сайте в информационно-телекоммуникационной сети «Интернет» http://tagilbank.ru);
- с размером вознаграждения Банка и порядком его взимания в соответствии с Тарифами, утвержденными Банком (размещены на информационных стендах в месте нахождения Банка, а также в местах обслуживания клиентов и на официальном сайте в информационно-телекоммуникационной сети «Интернет» http://tagilbank.ru);
- с информацией о наименовании и месте нахождения Банка, а также о номере его лицензии на осуществление банковских операций (сведения размещены на информационных стендах в месте нахождения Банка, а также в местах обслуживания клиентов и на официальном сайте в информационно-телекоммуникационной сети «Интернет» http://tagilbank.ru);
- с информацией о случаях повышенного риска использования ДБО (Приложение № 3 к Порядку);
- о способах направления Банку Клиентом уведомления об использовании ДБО без согласия Клиента.

1.12. Клиент уведомлен о том, что в случаях, установленных законодательными актами РФ, Банк обязан осуществлять списание денежных средств с банковских счетов Клиента без каких-либо поручений или распоряжений Клиента.

Клиент предоставляет Банку акцепт всех платежных требований (заранее данный акцепт) ко всем своим банковским счетам: а) для списания Банком ошибочно зачисленных на счет Клиента денежных средств; б) для списания Банком сумм комиссий, иных платежей в размере, порядке и случаях, установленных Тарифами; в) для списания сумм налогов, возникающих при исполнении Договора, уплата которых предусмотрена законодательством Российской Федерации; г) любую иную задолженность в случаях, предусмотренных отдельно заключаемыми договорами между Банком и Клиентом – кредитными договорами, договорами поручительства и др. Допускается частичное исполнение требований Банка на списание денежных средств со счета Клиента. Заранее данный акцепт (без ограничения суммы акцепта) действует со дня открытия счета Клиента по день его закрытия.

1.13. При отсутствии или недостаточности денежных средств на счете Клиента для списания Банком сумм любой задолженности в рамках Договора, погашения иной задолженности, в т.ч. по исполнительным документам, и(или) при наличии предусмотренных законодательством Российской Федерации ограничений по распоряжению денежными средствами на счете, Клиент предоставляет Банку право без дополнительных распоряжений (заранее дает акцепт) списывать указанные денежные средства с иных счетов Клиента в валюте Российской Федерации или иностранной валюте, открытых в Банке.

При необходимости списания денежных средств со счетов Клиента в валюте, отличной от валюты, в которой установлено обязательство, Клиент поручает Банку произвести за счет

Клиента конверсию/конвертацию валюты по курсу и на условиях, установленных Банком для совершения конверсионных операций на дату совершения операции, в счет погашения задолженности.

1.14. Порядок включает в себя следующие приложения, которые являются его неотъемлемой частью:

- Приложение № 1 – «Виды Электронных документов и требования к их оформлению»;
- Приложение № 2 – «Требования к программно-техническим средствам для проведения электронных расчетов»;
- Приложение № 3 – «Безопасность дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Тагилбанк» с использованием доступа через информационно-телекоммуникационную сеть «Интернет»;
- Приложение № 4 – «Порядок разбора конфликтных ситуаций, связанных с подлинностью электронных документов в Системе»;
- Приложение № 5 – «Заявление о присоединении к Порядку дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Тагилбанк» с использованием доступа через информационно-телекоммуникационную сеть «Интернет»;
- Приложение № 6 – «Уведомление об изменении сведений о клиенте»;
- Приложение № 7 – «Заявление о расторжении договора дистанционного банковского обслуживания с использованием доступа через информационно-телекоммуникационную сеть «Интернет»;
- Приложение № 8 – «Акт приема-передачи устройства USB-токен»;
- Приложение № 9 – «Заявление на внеплановую замену ключей и ключевого носителя»;
- Приложение № 10 – «Заявление о временном изменении режима при обслуживании с использованием системы дистанционного банковского обслуживания»;
- Приложение № 11 – «Заявление на подключение фильтрации по IP-адресам с использованием системы дистанционного банковского обслуживания»;
- Приложение № 12 – «Акт приема-передачи средства криптографической защиты информации».

1.15. Банк и Клиент признают используемую систему безопасности, определенную в Порядке, достаточной для защиты информации от несанкционированного доступа, а также для подтверждения авторства и подлинности электронных документов.

1.16. Банк имеет право отказать в выполнении распоряжения Клиента о совершении операции с использованием ДБО, по которой не предоставлены информация и документы по запросу Банка, предусмотренные Федеральным законом от 07.08.2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

1.17. Клиент обязуется письменно информировать Банк об изменении данных, указанных им в Заявлении, в течение 5 календарных дней с даты их изменения, а также предоставить в Банк документы, подтверждающие изменение этих данных.

1.18. Клиент обязан не реже одного раза в год предоставлять Банку (обновлять) информацию о себе, своих представителях, выгодоприобретателях: об изменениях места нахождения, состава участников/акционеров, величины уставного капитала, об изменении и наличии состава бенефициарных владельцев*****, предоставлять сведения об изменении их паспортных данных, о назначении и сроках полномочий представителей и их паспортных данных, номеров телефонов, электронного адреса.

** Бенефициарный владелец - физическое лицо, которое в конечном счёте прямо или косвенно (через третьих лиц) владеет (имеет преобладающее участие более 25 процентов в капитале) клиентом – юридическим лицом либо имеет возможность контролировать действия клиента.*

2. Основные термины и сокращения

В рамках Порядка используются следующие термины и сокращения.

Аутентификация – удостоверение правомочности обращения Клиента в Банк для совершения банковских операций по Счету.

Банк – акционерное общество «Тагилбанк», действующее на основании Устава, согласованного Центральным банком РФ 24 апреля 2015 года, регистрационный номер кредитной организации № 1635, свидетельство о государственной регистрации кредитной организации за № 1635, выдано Центральным банком РФ 30.12.1999 года, лицензия на

осуществление банковских операций выдана Центральным банком РФ 18 мая 2015 года за № 1635, ИНН 6623002060, КПП 662301001, ОГРН 1036605604078, место нахождения: Свердловская область, город Нижний Тагил, ул. Ломоносова, д. 2А.

Владелец сертификата ключа проверки электронной подписи – лицо, на имя которого выдан сертификат ключа проверки электронной подписи и которое владеет соответствующим закрытым ключом электронной подписи, позволяющим подписывать Электронные документы.

Дистанционное банковское обслуживание (ДБО) – предоставление Банком Клиенту банковских и информационных услуг с использованием систем «Интернет-банк».

Закрытый ключ электронной подписи – уникальная последовательность символов, известная владельцу сертификата ключа проверки электронной подписи и предназначенная для создания в Электронных документах электронной подписи с использованием средств электронной подписи.

Зарегистрированный ключ – открытый ключ электронной подписи абонента.

Зарегистрированный абонент – абонент систем «Интернет-банк», открытый ключ электронной подписи которого содержится в общем каталоге открытых ключей Центра регистрации ключей Банка.

Каталог открытых ключей – совокупность действующих открытых ключей электронной подписи абонентов сети, их идентификаторов и наименований.

Клиент – юридическое лицо или индивидуальный предприниматель, заключивший с Банком Договор или Дополнительное соглашение по обслуживанию систем «Интернет-банк».

Ключ электронной подписи (ключ ЭП) – уникальная последовательность символов, предназначенная для создания электронной подписи.

Компрометация закрытого ключа ЭП – событие, в результате которого закрытый ключ электронной подписи или его часть становятся известны или доступны постороннему лицу.

Открытый ключ электронной подписи – уникальная последовательность символов, соответствующая закрытому ключу электронной подписи, доступная пользователям информационной системы и предназначенная для подтверждения с использованием средств электронной подписи подлинности электронной цифровой подписи в Электронном документе.

Платежный электронный документ – Электронный документ, представляющий собой распоряжение Клиента на совершение операций по его банковскому счету, составленный в электронном виде, содержащий все предусмотренные законодательством РФ реквизиты. Платежный электронный документ, заверенный электронной подписью Клиента и являющийся основанием для совершения операций по счетам Клиента, открытым в Банке, имеет равную юридическую силу с расчетными документами, составленными на бумажных носителях и подписанными собственноручной подписью Клиента.

Подтверждение подлинности электронной подписи в Электронном документе – положительный результат проверки принадлежности электронной подписи под Электронным документом владельцу сертификата ключа подписи и отсутствия искажений в данном Электронном документе, с применением специальных средств электронной подписи и сертификата ключа подписи.

ПО - программное обеспечение.

Публичное размещение информации – размещение информации в головном офисе Банка, и его внутренних структурных подразделениях в местах доступных для Клиентов, а также на официальном сайте Банка в сети Интернет.

Сведения об открытом ключе (сертификате) абонента (ключа подписи) – распечатанная в виде отдельного документа полная информация о Клиенте, его идентификатор, открытый ключ. Подписывается Клиентом и заверяется их печатями.

Средство подтверждения – электронное или иное средство, используемое для подтверждения проведения операции или дополнительной Идентификации Клиента при получении от него Распоряжений.

Сертификат ключа проверки электронной подписи – Электронный документ или документ на бумажном носителе, выданный Центром регистрации ключей Банка и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Системы дистанционного банковского обслуживания – автоматизированные банковские системы, обеспечивающие формирование, передачу, регистрацию, исполнение и хранение Электронных Документов Клиентов, и проведение на их основе финансовых и иных операций.

Сообщение свободного формата – Электронный документ, содержащий сообщение и вложенный документ (при наличии).

Средства криптографической защиты информации (СКЗИ) - программные средства, реализующие алгоритмы криптографического преобразования информации и предназначенные для обеспечения ее конфиденциальности и (или) целостности.

Средства электронной подписи – шифровальные (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.

Стороны – Банк и Клиент, заключившие Договор.

Счет – банковский счет, открытый Клиенту в Банке.

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.

Электронная подпись (ЭП) – реквизит Электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием секретного ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе. ЭП является аналогом собственноручной подписи.

USB-токен – представляет собой компактное устройство с аппаратной реализацией российского стандарта электронной подписи (ЭП), шифрования и хеширования. USB-токен предназначен для генерации и защищенного хранения ключей шифрования и электронной подписи, выполнения шифрования и электронной подписи в самом устройстве, хранения цифровых сертификатов и иных данных. Аппаратная реализация криптографических алгоритмов (электронной подписи, хеш-функции и шифрования) внутри устройства обеспечивает конфиденциальность обрабатываемой информации при передаче и хранении, целостность обрабатываемой информации, а также подтверждение авторства посредством электронной подписи.

3. Порядок организации электронных расчетов

3.1. Электронные расчеты проводятся через Систему «Интернет-банк». Система состоит из Центрального абонентского пункта Банка и Рабочего места Клиента.

3.2. Рабочие места Клиента должны быть укомплектованы в соответствии с требованиями, указанными в Приложении № 2 к Порядку.

3.3. Клиент вправе указать определенный статический IP-адрес, с которого Клиентом будут осуществляться платежи и подтверждение Электронных документов (Приложение № 11 к настоящему Порядку). В этом случае вход с других Рабочих мест Клиента будет невозможен.

3.4. Для работы в Системе, при необходимости, назначаются ответственные лица Клиента – юридического лица, в чьи обязанности входит:

- в обязательном порядке выполнение требований информационной безопасности при работе с Системой;
- предварительная подготовка Электронных документов;
- своевременное и регулярное получение средствами Системы всей информации, передаваемой по Системе из Банка.

3.5. В случае делегирования полномочий по наложению ЭП на Электронные документы ответственное лицо Клиента отвечает за:

- хранение и использование закрытого ключа электронной подписи и средств подтверждения согласно раздела 5 Порядка;
- своевременное извещение Банка о случаях потери, возможного несанкционированного доступа к ключу ЭП и Средств подтверждения, компрометации ключа ЭП;
- участие в процедуре проверки ЭП при рассмотрении конфликтной ситуации.

3.6. Для обслуживания Системы Банк назначает ответственное лицо (администратора). Администратор Банка выполняет следующие функции:

- отвечает за работу Абонентского пункта Банка в Системе;
- участвует в процедуре проверки ЭП при рассмотрении конфликтных ситуаций;
- обеспечивает бесперебойное функционирование Абонентского пункта Банка;
- обеспечивает регулярную автоматическую обработку поступившей от Клиента по Системе информации и автоматическую передачу ее уполномоченному специалисту

Банка и своевременное размещение на интернет-сервере Системы всей необходимой информации по Системе;

- обеспечивает консультационную поддержку при установке и настройке программного обеспечения Системы Клиента.

3.7. Документы, отправляемые Клиентом по Системе через Интернет, передаются уполномоченному специалисту через Абонентский пункт Банка. Кроме того, Абонентский пункт Банка размещает всю необходимую справочную информацию и информацию по счету Клиента на интернет-сервере Системы, доступную при авторизации Клиента в Системе.

3.8. Клиент производит самостоятельную настройку Рабочего места согласно инструкции по установке, размещенной по адресу **https://ibank.tagilbank.ru.** При необходимости Клиент имеет право на бесплатные технические консультации по телефону.

3.9. Банк предоставляет в пользование Клиенту программное обеспечение системы ДБО, включая СКЗИ на срок действия заключаемого Договора.

Передача СКЗИ производится в офисе Банка уполномоченному лицу Клиента. При передаче оформляется Акт по форме, установленной Приложением №12. В случае передачи СКЗИ в формате аппаратного устройства (USB-токен) оформляется Акт по форме, установленной Приложением №8.

Клиент не вправе передавать, продавать, копировать или иным способом делать доступным третьим лицам полученное от Банка программное обеспечение либо иную информацию или сведения, связанные с заключенным Договором.

Клиент так же предупрежден, что он не вправе вывозить сертифицированные СКЗИ за пределы РФ без специального разрешения государственных контролирующих органов.

4. Генерация и регистрация ключей ЭП

4.1. Генерация и регистрация Ключей ЭП Клиента осуществляется в следующей последовательности:

4.1.1. Клиент путем обращения к серверу Системы по адресу **https://ibank.tagilbank.ru** самостоятельно осуществляет генерацию Ключей ЭП. В процессе генерации одновременно формируются Закрытый ключ ЭП, связанный с ним Открытый ключ ЭП и Сертификат открытого ключа ЭП.

4.1.2. Закрытый ключ ЭП создается и в последующем хранится только в памяти USB-токена или в файловом хранилище ключей ЭП.

4.1.3. Открытый ключ ЭП автоматически направляется по защищенному соединению сети Интернет в Банк и предварительно регистрируется.

4.1.4. Полученный в результате генерации Сертификат открытого ключа ЭП распечатывается Клиентом на бумажных носителях в количестве 2 (Двух) экземпляров и заверяется собственноручными подписями Владельца сертификата открытого ключа, руководителя Клиента (либо соответствующего Уполномоченного лица) и скрепляется печатью.

4.1.5. После надлежащего оформления, Сертификат открытого ключа ЭП в 2 (Двух) экземплярах направляется в Банк посредством личного обращения Клиента либо через его представителя наделенного соответствующими полномочиями.

4.1.6. Одновременно с Сертификатом открытого ключа ЭП в Банк предоставляются документы в отношении Уполномоченных лиц, указанных в нем, удостоверяющие их личности (оригиналы или нотариально заверенные копии), и документы, подтверждающие полномочия указанных лиц на подписание Электронных документов (оригиналы или заверенные в установленном Банком порядке копии с предоставлением оригиналов для сверки), если актуальные версии данных документов в Банк не представлялись ранее.

4.1.7. После получения Сертификата открытого ключа ЭП и документов указанных в п. 4.1.6. Порядка, Банк производит сверку предварительно зарегистрированного Открытого ключа ЭП переданного в Банк в электронном виде в момент генерации, с данными Открытого ключа ЭП указанного в представленном Сертификате открытого ключа ЭП. Помимо этого проверка производится в отношении идентификационных данных Клиента, паспортных данных Уполномоченных лиц Клиента и их полномочий (в части соответствия присвоенных прав подписей и сроков действия полномочий), а также соответствия собственноручных подписей Уполномоченных лиц Клиента.

4.1.8. При положительном результате проверки Банк регистрирует Открытый ключ ЭП в Каталоге открытых ключей Системы, после чего проставляет на 2 (Двух) экземплярах бумажных носителей Сертификата открытого Ключа ЭП дату приема, сроки действия Сертификата открытого Ключа ЭП, подпись уполномоченного лица Банка и скрепляет их печатью. После

заверения, Клиенту передается один экземпляр Сертификата открытого ключа ЭП, второй экземпляр остается на хранении в Банке.

4.1.9. Сертификат открытого ключа ЭП считается зарегистрированным, а соответствующие Ключи ЭП активированными, с даты, проставленной Банком на бумажных носителях Сертификата открытого ключа ЭП.

4.1.10. Сертификат открытого ключа ЭП (ключи ЭП) Клиента считается действующим в момент проверки ЭП при одновременном выполнении следующих условий:

- Сертификат открытого ключа ЭП зарегистрирован в Банке;
- срок действия Сертификата открытого ключа ЭП не истек;
- действие Сертификата открытого ключа ЭП не приостановлено и не отменено.

5. Хранение и использование ключей

5.1. В целях безопасности Клиент обязан хранить свои Ключи ЭП только на съемных носителях (при использовании файлового хранилища Ключей ЭП) или USB-токене.

5.2. В Банке хранятся только Открытые ключи Клиента.

5.3. Клиент берет на себя полную ответственность и обязуется самостоятельно обеспечить сохранность, неразглашение и нераспространение Ключей ЭП.

5.4. Срок действия Ключей ЭП определяется сроком полномочий владельца Сертификата открытого ключа ЭП, но не может превышать 1 (одного) года с даты начала действия Ключа ЭП.

5.5. По окончании срока действия Ключи ЭП подлежат обязательной перегенерации Клиентом в соответствии с п.4. Порядка, при этом прежние Ключи ЭП Клиента, по которым истек срок действия, считаются недействительными с даты, следующей за датой окончания срока их действия.

5.6. При утрате или компрометации Ключей ЭП Клиент обязан немедленно оповестить Банк по телефонам: **+7(3435) 977-000, +7(3435) 977-616, +7(3435) 977-619**, и незамедлительно направить в адрес Банка письменное уведомление в произвольной форме. Датой и временем получения Банком указанного уведомления Клиента считается: дата и время телефонного звонка Клиента по указанным номерам телефона; дата и время получения Банком письменного уведомления Клиента.

В случае компрометации Ключей ЭП работа Клиента в Системе приостанавливается до проведения внеплановой смены ключей ЭП Клиентом.

5.7. Клиент несет полную ответственность за соблюдение условий Порядка лицами, которых он назначает для работы в Системе и которым он передает Ключи ЭП.

5.8. В случае использования Клиентом USB-токена:

5.8.1. Закрытый ключ ЭП генерируется только внутри USB-токена и хранится в защищенной памяти USB-токена.

5.8.2. Формирование ЭП Клиента происходит в соответствии с «ГОСТ Р34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» непосредственно внутри SIM-карты USB-токена: на вход передается Электронный документ, на выходе - сформированная ЭП под данным документом.

5.8.3. Доступ ко всем криптографическим функциям USB-токена предоставляется только после ввода Клиентом корректного пароля Ключа ЭП, указанного при создании ключа. Для каждого Закрытого ключа ЭП применяется отдельный пароль, определяемый и устанавливаемый Клиентом самостоятельно.

5.8.4. В одном USB-токене допускается одновременно хранить секретные ключи:

- нескольких уполномоченных лиц одного корпоративного клиента;
- нескольких корпоративных клиентов.

5.8.5. Банк передает USB-токен (USB-токены) Клиенту по «Акту приема-передачи устройства USB-токен» (Приложение №8 к настоящему Порядку), подписанному Сторонами, после оплаты Клиентом соответствующей комиссии согласно Тарифам.

6. Порядок передачи и приема документов по Системе

6.1. Инициатором проведения всех расчетных операций и получения всей информации по Системе является Клиент.

6.2. Все справочники, шаблоны Электронных документов, сами Электронные документы после их сохранения, а также выписки и вся иная информация в Системе хранятся на интернет-

сервере Системы в Банке и доступны для работы Клиенту только во время проведения авторизованных сеансов связи с Банком через Интернет.

6.3. Вся информация, размещенная Банком на интернет-сервере Системы, в тот же момент становится доступной для Клиента при условии установления авторизованного сеанса связи с Банком по Системе.

6.4. Клиент устанавливает соединение с Интернет.

6.5. Клиент открывает сеанс связи с Банком через Интернет, защищенный подсистемой защиты Системы. При этом подсистема защиты Системы Клиента состоит из:

- Системы защиты интернет-трафика;
- Системы защиты информации;
- Системы сеансовых ключей.

6.6. В функции подсистемы защиты входят:

- аутентификация Клиента, в том числе посредством использования при входе в Систему сеансовых ключей;
- защита всех передаваемых и принимаемых в течение сеанса связи с Банком (через Интернет) сообщений по Системе, как на стороне Клиента, так и на стороне Банка;
- осуществление электронной подписи Электронных документов.

6.7. После аутентификации Клиент получает доступ к Системе и начинает работу с ней.

6.7.1. Клиент запрашивает и получает выписки, служебные сообщения, а также иную информацию, адресованную ему Банком, согласно Приложению № 1 к настоящему Порядку.

6.7.2. Клиент запрашивает и заполняет (редактирует) формы Электронных документов и справочников, а затем передает заполненные (отредактированные) формы в Банк, который осуществляет проверку правильности их заполнения и либо выдает служебные сообщения об ошибках, либо сохраняет переданные документы, записи справочников.

6.7.3. Клиент подписывает Электронные документы своей ЭП. ЭП подтверждает авторство отправленного по Системе документа и гарантирует его целостность, т.к. любое изменение в документе после его подписания сделает ЭП недействительной.

6.8. Основанием для принятия к исполнению Банком переданного Клиентом по системе платежного Электронного документа является аутентификация соединения Клиента согласно п.6.5 и п.6.6 Порядка, а также наличие и корректность ЭП Клиента в соответствии с п.6.7.3 Порядка, соответствие требованиям к оформлению платежных Электронных документов.

6.8.1. После получения платежного Электронного документа и проверки корректности ЭП и правильности оформления, уполномоченный специалист Банка проводит его по счету Клиента. При проведении валютной операции документ предварительно согласовывается с уполномоченным сотрудником службы финансового мониторинга и валютного контроля Банка.

6.8.2. Система автоматически отражает сведения о текущем состоянии документов в Банке (получении, приеме к исполнению и исполнении или неисполнении документа) посредством изменения статусов Электронных документов.

6.8.3. Информация по Электронным документам, поступившим в течение операционного времени и оформленным с нарушением требований, размещается Банком на интернет-сервере в Системе в день получения инструкции на исполнение документа с указанием причины, по которой не принят документ.

6.8.4. Информация по Электронным документам, поступившим по истечении операционного времени и оформленным с нарушением требований, размещается Банком на интернет-сервере в Системе на следующий рабочий день после получения инструкции на исполнение документа с указанием причины, по которой не принят документ.

6.9. В том случае, если статус Электронного документа не изменился в течение двух часов после отправки на исполнение при просмотре Клиентом данной информации во время сеансов связи (с учетом установленного режима работы Банка), Клиенту необходимо обратиться за разъяснениями к уполномоченному специалисту Банка.

6.10. По отдельным Электронным документам Банк может запросить дополнительное подтверждение или разъяснение. Подтверждение запрашивается по Системе, либо иным образом в день получения платежного Электронного документа. В этом случае Электронный документ принимается к исполнению после получения требуемого подтверждения.

7. Обязанности и права Сторон

7.1. Банк обязан:

7.1.1. Фиксировать направленные Клиенту и полученные от Клиента уведомления, а также хранить соответствующую информацию не менее 3 (трех) лет.

7.1.2. Обеспечить возможность направления ему Клиентом уведомления об утрате или компрометации Ключей ЭП в соответствии с п. 5.6. Порядка.

7.1.3. Информировать Клиента о совершении каждой операции с использованием ДБО путем направления Клиенту соответствующего уведомления согласно выбранного Клиентом способа его информирования:

- при предоставлении Клиентом данных своей электронной почты для таких уведомлений – на указанный Клиентом адрес электронной почты, либо
- при предоставлении Клиентом номера своего мобильного телефона для таких уведомлений – на указанный Клиентом номер мобильного телефона, либо
- при личном обращении Клиента к Банку – предоставление отчета на бумажном носителе.

Обязанность Банка по предоставлению Клиенту вышеуказанной информации считается исполненной надлежащим образом при направлении Банком уведомления в соответствии с имеющейся у Банка информации о способах и средствах связи с Клиентом, которые указаны Клиентом в Заявлении. При информировании Клиента о совершении операции с использованием ДБО несколькими способами (п.п. 7.1.3. Порядка) Банк считается выполнившим указанную обязанность с момента направления Клиенту уведомления о соответствующей операции с использованием ДБО хотя бы одним из способов, предусмотренных Порядком и указанным в Заявлении.

Если в качестве единственного способа информирования Банком о совершении каждой операции с использованием ДБО в рамках Порядка Клиент избрал способ – личное обращение к Банку для получения отчета на бумажном носителе, такой отчет предоставляется Банком незамедлительно по факту обращения Клиента. Клиент вправе ежедневно в рабочее время Банка обращаться для получения отчета. При этом Клиент самостоятельно определяет частоту и периодичность личного обращения к Банку для получения отчетов на бумажном носителе. В этом случае обязанность Банка по предоставлению Клиенту информации согласно настоящего пункта считается исполненной надлежащим образом в момент окончания каждого рабочего дня Банка; все риски, связанные с несвоевременным (по истечении одного рабочего дня с момента совершения каждой операции с использованием ДБО) обращением Клиента к Банку для получения отчета Клиент принимает на себя.

7.1.4. Предоставлять Клиенту документы и информацию, которые связаны с использованием Клиентом систем ДБО в следующем порядке: в письменном виде по запросу Клиента.

7.1.5. Исполнять полученные от Клиента Электронные документы в сроки и порядке, установленные действующим законодательством Российской Федерации, Договором банковского счета, с учетом условий настоящего Порядка, заключенным между Банком и Клиентом, действующими на момент поступления Электронного документа Тарифами Банка. А также сообщать Клиенту посредством системы ДБО об исполнении документов.

7.1.6. Оказывать Клиенту консультационные услуги по вопросам настройки клиентской части системы ДБО, приема (передачи) информации, технологии ее обработки в системе ДБО и использования средств защиты.

7.1.7. Незамедлительно, с момента получения уведомления о компрометации Ключей ЭП Клиента предпринять все меры для блокировки Открытых ключей ЭП соответствующих владельцев Ключей ЭП.

7.2. Клиент обязан:

7.2.1. Строго соблюдать все установленные Порядком меры безопасности при использовании систем ДБО, обеспечивать доступ к аппаратно-программным средствам системы ДБО только уполномоченных сотрудников.

7.2.2. Своевременно (в течение 5 календарных дней) письменно уведомлять Банк об изменении своих данных (Приложение № 6 к настоящему Порядку) и предоставлять Банку подтверждающие документы.

7.2.3. Незамедлительно уведомить Банк об утрате или компрометации Ключей ЭП в соответствии с пунктом 5.6. Порядка.

7.2.4. Уплачивать Банку комиссии и вознаграждение в размере, сроки и порядке в соответствии с Тарифами.

7.2.5. Для контроля операций с использованием ДБО самостоятельно проверять не реже чем 1 (один) раз в день свою электронную почту и SMS-сообщения, направленные на мобильный телефон, а также почтовую корреспонденцию – проверять наличие уведомлений Банка, прочитывать полученные уведомления.

7.2.6. Для ознакомления с возможными изменениями и (или) дополнениями в Порядок,

Договор, Тарифы, самостоятельно не реже 1 (одного) раза в день знакомиться с информацией, размещаемой Банком в актуальной редакции на официальном сайте в информационно-телекоммуникационной сети «Интернет».

7.2.7. Не осуществлять посредством ДБО незаконные финансовые операции, незаконную торговлю и любые другие операции в нарушение законодательства РФ.

7.2.8. Соблюдать условия настоящего Порядка.

7.2.9. Использовать полученные от Банка программно-технические средства только в целях, установленных настоящим Порядком, без права передачи, продажи или передачи иным образом третьим лицам. В случае нарушения установленных в отношении использования программного обеспечения запретов и ограничений Клиент несет перед Банком ответственность в соответствии с условиями настоящего Порядка.

7.2.10. Поддерживать актуальными системную дату и системное время на технических средствах, где установлено программное обеспечение клиентской части системы ДБО.

7.2.11. Своевременно устанавливать обновления системы ДБО, распространяемое Банком посредством носителей информации или рассылаемое по системе ДБО.

7.2.12. Предоставлять Банку по его требованию информацию, необходимую для исполнения Банком требований федерального закона от 07.08.2001 N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма".

7.2.13. За свой счет поддерживать в рабочем состоянии свои и полученные от Банка программно-технические средства, используемые для электронного документооборота в соответствии с заключенным Договором.

7.2.14. Не разглашать третьим лицам (за исключением случаев, прямо установленных действующим законодательством Российской Федерации или заключенным Договором) способы защиты информации и обеспечения безопасности при работе в системе ДБО, сохранять в тайне Закрытые ключи электронной подписи.

7.2.15. Немедленно информировать Банк обо всех случаях компрометации известных ему Ключей ЭП Банка, их утраты, хищения, несанкционированного использования, программно-технических средств, используемых для электронного документооборота в соответствии с настоящим Порядком.

7.3. Банк имеет право:

7.3.1. Прекратить предоставление услуг ДБО:

- в случае если в отношении Клиента имеются сведения об участии в террористической деятельности, полученные в соответствии с Федеральным законом от 07.08.2001 года (с изменениями) № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
- в случае отсутствия по месту нахождения Клиента его постоянно действующего органа управления, иного органа или лица, которые имеют право действовать от имени Клиента без доверенности;
- в случае наличия подозрений о том, что целью заключения Договора является совершение операций в целях легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма»;
- в случае выявления фактов допуска Клиентом к системе ДБО третьих лиц без письменного уведомления Клиентом Банка о данном факте;
- неисполнения или ненадлежащим исполнением Клиентом своих обязательств, предусмотренных Порядком;
- в случае поступления информации о зачислении на счет Клиента денежных средств, списанных в результате несанкционированного доступа к счетам других Клиентов (в том числе в других банках), а также любого несанкционированного доступа к счету;
- в иных случаях, предусмотренных действующим законодательством РФ.

7.3.2. В одностороннем порядке вносить изменения в настоящий Порядок, Договор, Тарифы, информируя об этом Клиента путем размещения соответствующей информации на информационных стендах в месте нахождения Банка, а также в местах обслуживания клиентов и на официальном сайте в информационно-телекоммуникационной сети «Интернет».

7.3.3. В одностороннем порядке приостановить с Клиентом обмен ЭД либо расторгнуть заключенный Договор ДБО в случаях и порядке, предусмотренных настоящим Порядком.

7.3.4. Требовать от Клиента замены ключей ЭП при проведении их плановой замены, увольнении работников Клиента, имеющих право доступа к системе ДБО, компрометации или подозрении на компрометацию криптографических ключей ЭП, нарушении правил безопасности

при эксплуатации системы ДБО, при смене лица, являющегося владельцем Сертификата (окончания срока его полномочий) в соответствии с карточкой с образцами подписей и оттиска печати, предоставленной в Банк.

7.4. Клиент имеет право:

7.4.1. Отказаться от использования ДБО в соответствии с п. 1.7. Порядка путем направления в Банк письменного заявления по форме Приложения № 7 к настоящему Порядку не менее чем за 3 (три) рабочих дня до даты, с которой Договор должен быть расторгнут.

7.4.2. Получать документы и информацию, которые связаны с использованием ДБО, в следующем порядке: в письменном виде по запросу Клиента.

7.4.3. Приостановить прием к исполнению распоряжений об осуществлении переводов денежных средств от своего имени.

7.4.4. Обращаться в Банк за разъяснениями по вопросам обмена Электронными документами и функционирования системы ДБО.

7.4.5. Обращаться в Банк для ограничения (приостановления) работы в системе ДБО путем направления в Банк письменного заявления по форме Приложения № 10 к настоящему Порядку.

7.4.6. Производить внеплановую замену ключей ЭП путем направления в Банк письменного заявления по форме Приложение № 9 к настоящему Порядку.

7.4.7. Обращаться в Банк для блокировки действующих Ключей ЭП.

7.4.8. Обращаться в Банк для изменения параметров обслуживания в системе ДБО.

7.4.9. Подавать в Банк для исполнения документы на бумажном носителе, при условии оформления в соответствующем порядке.

8. Оплата услуг Банка

8.1. Клиент оплачивает услуги Банка по подключению, выдаче цифрового сертификата по обслуживанию систем ДБО – в размере, установленном Тарифами, в следующем порядке: единовременно в день подписания Договора, путем бесспорного списания Банком инкассовым поручением денежных средств со счетов Клиента в Банке.

8.2. Клиент уплачивает Банку ежегодную абонентскую плату за обслуживание систем ДБО - в размере, установленном Тарифами, в следующем порядке: один раз в год в течение 10 рабочих дней с момента начала оплачиваемого периода (года обслуживания), путем бесспорного списания Банком инкассовым поручением денежных средств со счетов Клиента в Банке.

8.3. Клиент оплачивает услуги Банка по выезду сотрудника Банка к Клиенту по вопросам обслуживания систем ДБО – в размере, установленном Тарифами, в следующем порядке: в течение 5 рабочих дней со дня выставления Банком счета-фактуры согласно акта выполненных работ. Банк вправе списать денежные средства в оплату стоимости услуг, указанных в настоящем пункте, инкассовым поручением со счетов Клиента в Банке.

9. Ответственность сторон

9.1. Стороны несут ответственность за ненадлежащее исполнение своих обязанностей в соответствии с законодательством Российской Федерации и условиями Договора.

9.2. До момента направления Банку уведомления в соответствии с п. 5.6. настоящего Порядка, при условии направления Банком Клиенту уведомлений о совершении операций с использованием Системы согласно п.п. 7.1.3. настоящего Порядка, Клиент несет ответственность за все операции по его счету, совершенные с использованием Системы иными лицами с ведома или без ведома Клиента.

9.3. Банк не несет ответственности за сбои в работе почты, сети Интернет, сетей связи, возникшие по не зависящим от Банка причинам и повлекшие за собой несвоевременное получение или неполучение Клиентом любых уведомлений и сообщений Банка. Банк освобождается от имущественной ответственности в случае технических сбоев (отключение/повреждение электропитания и сетей связи, сбой программного обеспечения, базы данных Банка и др.), а также в иных ситуациях, находящихся вне сферы контроля Банка, повлекших за собой невыполнение Банком Порядка и Договора.

9.4. Банк не несет ответственности, в случае если информация о счетах Клиента, другая конфиденциальная информация о Клиенте, или о проведенных им операциях станет известной иным лицам в результате прослушивания или перехвата информации в каналах связи во время их использования.

9.5. Банк не несет ответственности за последствия совершения операций с использованием ДБО, совершенных неуполномоченными лицами, и в тех случаях, когда с использованием предусмотренных банковскими правилами и Договором процедур Банк не мог установить факта совершения операции с использованием ДБО неуполномоченными лицами.

9.6. Банк не несет ответственности за неисполнение или ненадлежащее исполнение своих обязательств по Договору, в случае если исполнение таких обязательств становится невозможно или затруднено, или задерживается ввиду возникновения форс-мажорных обстоятельств, что включает без ограничений принятие, опубликование или изменение в толковании или применении каких-либо законодательных или нормативных актов, решений и т.п. государственными или муниципальными органами Российской Федерации или других государств, Банком России, в результате которых исполнение Банком своих обязательств становится незаконным или неправомерным, а также саботаж, пожары, наводнения, взрывы, стихийные бедствия, гражданские волнения, забастовки и любые выступления работников, восстания, беспорядки, войны или действия правительств или любые другие обстоятельства, находящиеся вне разумного контроля Банка («обстоятельства непреодолимой силы»). Если стороны не достигнут письменного соглашения об обратном, при наступлении обстоятельств непреодолимой силы Банк вправе приостановить исполнение своих обязательств по Договору, которые попадают под действие обстоятельств непреодолимой силы до момента прекращения действия таких обстоятельств.

9.7. Банк не несет ответственности в случае невыполнения Клиентом Порядка и Договора. Банк не несет ответственности за убытки, возникшие в результате использования Клиентом программно-технических средств, не соответствующих требованиям, установленным Порядком, либо в результате проведения электронных расчетов на неисправном и не проверенном на отсутствие компьютерных вирусов персональном компьютере Клиента.

9.8. Банк несет ответственность за несоблюдение сроков подтверждения и проведения расчетных операций по счету Клиента на основании надлежащим образом оформленных, подписанных электронной подписью и своевременно доставленных Электронных документов Клиента в соответствии с действующим законодательством и договором банковского счета.

9.9. Любой Электронный Документ, полученный Банком по Системе, расшифрованный Банком, снабженный электронной подписью Клиента, и формально отвечающий другим требованиям настоящего Порядка и Договора и Дополнительных соглашений, в любом случае признается Электронным документом, исходящим от Клиента, что не допускает возможности отказа от его авторства со стороны Клиента ни при каких обстоятельствах.

9.10. Ответственность Банка перед Клиентом ограничивается документально подтвержденным реальным ущербом, возникшим у Клиента в результате неправомерных действий или бездействия Банка, действующего преднамеренно или с грубой неосторожностью. Ни при каких обстоятельствах Банк не несет ответственности перед Клиентом за какие-либо косвенные, побочные или случайные убытки или ущерб (в том числе упущенную выгоду), даже в случае, если он был уведомлен о возможности возникновения таких убытков или ущерба.

9.11. Банк несет ответственность перед Клиентом по возмещению последнему сумм операций, совершенных без согласия Клиента, в соответствии с требованиями ст. 9 Федерального закона от 27.06.2011 года № 161-ФЗ «О национальной платежной системе».

9.12. Клиент несет ответственность перед Банком за ущерб и расходы, понесенные Банком в результате нарушения Клиентом условий или положений Договора или законодательных актов.

9.13. Клиент несет ответственность за изменение своих платежных реквизитов в Электронных документах на несоответствующие представленным в Банк документам.

9.14. До момента направления Банку уведомления в соответствии с пунктом 5.6. Порядка, при условии направления Банком уведомлений о совершении операций с использованием ДБО, Клиент несет ответственность за все операции по его Счету с использованием ДБО, совершенные иными лицами с ведома или без ведома Клиента.

10. Порядок разрешения споров

10.1. Стороны обязуются урегулировать споры и претензии, возникающие в связи с исполнением Договора, путем переговоров. Процедура согласования разногласий по доказательствам тех или иных фактов проводится в соответствии с Приложением № 4 к Порядку.

10.2. При невозможности разрешения споров и разногласий путем переговоров, они разрешаются в Арбитражном суде Свердловской области в соответствии с действующим законодательством РФ.

11. Срок действия Договора и его расторжение

11.1. Договор действует без ограничения срока.

11.2. Стороны признают, что действие Договора прекращается в момент закрытия счета Клиента, указанного в Заявлении, а также при прекращении использования услуг Банка, предусмотренных Договором.

11.3. Клиент вправе в любой момент расторгнуть Договор, уведомив о данном намерении Банк в соответствии с пунктом 1.7. Порядка.

11.4. Договор может быть расторгнут на основании письменного соглашения сторон либо по иным основаниям, установленным действующим законодательством Российской Федерации.

11.5. Банк вправе в одностороннем порядке расторгнуть Договор в случаях, предусмотренных законодательством РФ.

11.6. Прекращение действия Договора не влечет прекращения обязанности Клиента погасить перед Банком имеющуюся задолженность по оплате услуг Банка по Договору.

12. Заключительные положения

12.1. Клиент соглашается с тем, что:

12.1.1. Банк имеет право направлять сообщения информационного характера (в том числе о наступлении сроков исполнения обязательств Клиента перед Банком по погашению задолженности, а также о возникновении просроченной задолженности по имеющимся перед Банком обязательствам) по месту нахождения Клиента, по адресу электронной почты либо по номерам телефонов, в том числе, по номерам телефонов сотовой связи, факсов, указанных Клиентом в Заявлении либо в иных документах, оформляемых в рамках Договора.

12.1.2. Банк имеет право на хранение и обработку, в том числе, автоматизированную, любой информации, относящейся к персональным данным Клиента/его представителей, в том числе, указанной в Заявлении Клиента и/или в иных документах в соответствии с Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных», включая сбор, систематизацию, накопление, хранение, уточнение, использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, предоставленных Банку в связи с заключением Договора в целях исполнения договорных обязательств, а также разработки Банком новых продуктов и услуг и информирования Клиента об этих продуктах и услугах, и все иные действия, предусмотренные Федеральным законом от 27.07.2006 года № 152-ФЗ «О персональных данных».

Согласие Клиента на обработку персональных данных действует в течение всего срока действия Договора, а также в течение 10 лет с даты прекращения действия Договора, после чего персональные данные подлежат уничтожению.

12.2. Клиент выражает согласие и уполномочивает Банк предоставлять полностью или частично персональные данные Клиента/его представителя и проводимых операциях по счетам Клиента третьей стороне, с которой у Банка заключено соглашение о конфиденциальности и неразглашении информации, в том числе для целей:

- осуществления связи с Клиентом для предоставления информации об исполнении Договора, для организации почтовых рассылок, рассылок SMS-сообщений и рассылок по электронной почте в адрес Клиента выписок по счетам, информации по кредитам, предложений (оферт) Банка, а также для передачи информационных и рекламных сообщений об услугах Банка: при этом Клиент несет все риски, связанные с тем, что направленные сообщения станут доступными третьим лицам;
- проведения стимулирующих мероприятий, в том числе лотерей, конкурсов, игр и иных рекламных акций, организуемых Банком и/или третьими лицами;
- осуществления телефонной связи с Клиентом, для предоставления Клиенту информации о результатах рассмотрения любых заявлений Клиента;
- осуществления взысканий просроченной задолженности перед Банком по Договору и/или любому иному заключенному с Банком соглашению, включая соглашения о кредитовании (кредитные договоры);
- организации улучшений программного обеспечения Банка;
- предоставления Банку услуг по хранению клиентских документов, созданию и хранению электронных копий указанных документов;
- передачи персональных данных Клиента оператору сотовой связи в целях обработки оператором сотовой связи переданных данных для дальнейшего информационного сопровождения исполнения Договора;

- передачи персональных данных Клиента сторонней организации, оказывающей услуги в целях заключения и исполнения заключенного между Клиентом и указанной организацией договора об оказании услуг.

12.3. Заключением Договора Клиент подтверждает следующее:

- Клиент ознакомлен и полностью понимает все условия Договора и Порядка, а также безусловно принимает эти условия и обязуется исполнять Договор;
- Клиент не заключает Договор под влиянием обмана, насилия, угрозы, под влиянием обстоятельств, вынуждающих его заключить Договор на крайне невыгодных для себя условиях;
- заключение Договора не ущемляет прав Клиента, правовые последствия заключения Договора Клиенту известны и понятны;
- Договор заключен Клиентом добровольно и осознанно, без какого-либо заблуждения или принуждения, в том числе со стороны Банка;
- при заключении Договора Клиент предоставил Банку достоверную информацию, необходимую для его идентификации. В случае изменения любой информации, указанной в Заявлении, Клиент обязуется своевременно (в течение 5 календарных дней) предоставить Банку обновленную информацию и подтверждающие документы.

Приложение № 1
к Порядку дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Тагилбанк» с использованием доступа через
информационно-телекоммуникационную сеть Интернет

ВИДЫ
Электронных Документов и требования к их оформлению

1. Виды Электронных Документов, направляемых Клиентом Банку:

1.1. Платежное поручение в валюте РФ.

1.2. Сообщение свободного формата.

2. Форматы Электронных Документов, направляемых Клиентом Банку:

2.1. Документы заполняются в порядке, определенном в экранной форме системы «Интернет-банк».

3. Виды Электронных Документов, направляемых Банком Клиенту:

3.1. Выписка из лицевого счета за период.

3.2. Оборотно-сальдовая ведомость за период.

3.3. Справочная и прочая информация из Банка (сообщение свободного формата).

4. Требования по оформлению платежных Электронных Документов, направляемых Клиентом Банку:

4.1. Все Электронные Документы должны содержать необходимые банковские реквизиты согласно требованиям действующего законодательства Российской Федерации и описанию системного комплекса «Интернет-банк», должны быть подписанными Клиентом системы «Интернет-банк», от которого поступает данный документ.

5. Требования по оформлению бумажных документов, используемых при электронных расчетах:

5.1. Все документы, полученные в Банке по системе «Интернет-банк» с верной электронной подписью и распечатанные на принтере, должны иметь отметку:

Получено по системе «Клиент-Банк». Заверено клиентом.

Приложение № 2
к Порядку дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Тагилбанк» с использованием доступа через
информационно-телекоммуникационную сеть Интернет

ТРЕБОВАНИЯ
к программно-техническим средствам для проведения электронных расчетов

1. Компьютер, минимальные и рекомендуемые параметры которого указаны ниже:

	Минимальные	Рекомендуемые
Процессор	Intel Celeron 600MHz	Intel Celeron 1GHz
Оперативная память	256 Mb	512 Mb
Операционная система	Windows XP/Vista/7/8/10, Linux, macOS 10.6 и выше	

Кроме вышеперечисленных требований рекомендуется наличие в компьютере пользователя USB-порта. Для хранения ключей ЭЦП рекомендуется использовать персональные криптопровайдеры — USB-токены, которые обеспечивают гарантированную защиту секретных ключей ЭЦП клиентов от хищений вредоносными программами.

Рекомендуется также наличие принтера, на котором будет распечатан Сертификат открытого ключа ЭЦП клиента.

2. Установленный на компьютере пользователя Web-браузер. В качестве Web-браузера рекомендуется использовать одну из следующих программ:
- Microsoft Internet Explorer 11;
- Mozilla Firefox 29 и выше;
- Google Chrome 36 и выше;
- Opera 13 и выше.

При необходимости установки на компьютере пользователя виртуальной Java-машины получите по адресу http://www.java.com/ru дистрибутив последней версии JRE для используемой операционной системы.

3. Доступ в Интернет. Рекомендуемая скорость соединения – 33,6 Кбит/сек и выше. В случае доступа в Интернет по телефонной коммутируемой линии необходимо наличие современного модема.

Приложение № 3
к Порядку дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Тагилбанк» с использованием доступа через
информационно-телекоммуникационную сеть Интернет

БЕЗОПАСНОСТЬ
дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Тагилбанк» с использованием доступа через Интернет

1. Система безопасности

1.1. Система безопасности включает в себя следование общим рекомендациям, систему ограничения доступа на рабочем месте участника Системы и систему обеспечения секретности и подлинности (защиты) информации, передаваемой по каналам связи.

2. Общие рекомендации

2.1. Не сохраняйте Ваш пароль в текстовых файлах на компьютере либо на других электронных носителях информации, т.к. при этом существует риск его кражи и компрометации.

2.2. При любых подозрениях компрометации пароля посторонними лицами (в т.ч. представившимися сотрудниками Банка), следует незамедлительно остановить работу и обратиться в Банк по любому из телефонов: +7(3435) 977-000, +7(3435) 977-616, +7(3435) 977-619.

2.3. Используйте современное антивирусное программное обеспечение и следите за его регулярным обновлением.

2.4. Регулярно выполняйте антивирусную проверку на своем компьютере для своевременного обнаружения вредоносных программ.

2.5. Своевременно устанавливайте обновления операционной системы своего компьютера, рекомендуемые компанией-производителем в целях устранения выявленных в нем уязвимостей.

2.6. Используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты Вашего компьютера – персональные межсетевые экраны, программы поиска шпионских компонент, программы защиты от “спам”-рассылок и пр.

2.7. Исключайте на ПК, на которых осуществляется подготовка и отправка документов в Банк, неконтролируемое использование систем удаленного управления ПК. Не привлекайте для администрирования и обслуживания данного ПК ИТ-персонал на условиях предоставления ему неконтролируемого удаленного доступа.

2.8. Исключайте посещение с ПК, на которых осуществляется подготовка и отправка документов в Банк, сайтов сомнительного содержания и любых других интернет-ресурсов непроизводственного характера (социальные и пиринговые сети, конференции и чаты, телефонные сервисы и т.п.), чтение почты и открытие почтовых вложений от недоверенных источников, установку и обновление любого ПО не с сайтов производителей. Настройками сетевого оборудования, корпоративных и персональных сетевых экранов выход в сеть Интернет ограничивайте “белым списком” со всех рабочих мест, на которых осуществляется подготовка, подписание и отправка платежных документов. В “белый список” должны включаться исключительно доверенные сайты и хосты самой организации, банков, налоговой службы, других государственных органов, необходимых в производственном процессе, серверы обновлений системного и антивирусного ПО.

3. Система ограничения доступа

3.1. Доступ к информации на абонентском пункте Клиента ограничен системой паролей при обращении к программному обеспечению абонентского пункта Клиента. При этом каждый сотрудник Клиента имеет свой собственный пароль для входа в Систему и свой индивидуальный код, которым отмечаются все произведенные им действия.

3.2. Банк не несет ответственности за разглашение сотрудниками Клиента их паролей, равно как и за модификации данных на абонентском месте Клиента несистемными средствами.

3.3. При регистрации клиента на Сервере Банка по запросу Системы Клиент проставляет кодовое (блокировочное) слово, по которому без проведения дополнительного расследования производится блокировка работы Клиента в Системе. Блокировка работы Клиента в Системе производится по устному запросу Клиента с обязательным указанием кодового слова. Для

отмены блокировки Клиенту необходимо предоставить в Банк письменное заявление с указанием причин отмены блокировки.

4. Защита информации, передаваемой по каналам связи

4.1. Система защиты информации, передаваемой по каналам связи, включает в себя подсистему обеспечения секретности информации и подсистему обеспечения ее подлинности.

4.2. Конфиденциальность данных обеспечивается защитой всех данных, передаваемых по каналам связи. Для защиты данных используется протокол TLS.

4.3. Каждая из сторон имеет свой набор из двух ключей - открытый ключ и закрытый ключ. Клиент хранит свой закрытый ключ на своем абонентском месте и несет полную ответственность за его секретность и конфиденциальность. С помощью этого ключа Клиент формирует ЭП под электронными документами, отправляемыми в Банк.

5. Обеспечение подлинности данных. Группы подписей под документами

5.1. Для обеспечения подлинности данных применяется ЭП. Все передаваемые Банку Клиентом или принимаемые Клиентом от Банка электронные документы могут иметь ЭП одного или более уполномоченных лиц соответствующих сторон, определяемых при регистрации на Сервере Банка.

Количество уполномоченных лиц не должно превышать 8 (восьми) человек. При этом следует учесть, что количество ЭП под каждым электронным документом должно соответствовать количеству имеющих право подписи лиц, определенных при регистрации на Сервере Банка.

5.2. Для подписи документа уполномоченными лицами соответствующих сторон используется двухключевой алгоритм. Алгоритм использует два ключа: секретный ключ, с помощью которого ставится подпись под документом, и открытый ключ, с помощью которого проверяется подпись под документом.

Каждому секретному ключу соответствует ровно один открытый ключ и наоборот. Построить секретный ключ, соответствующий заданному открытому, зная только этот открытый ключ, невозможно.

Зная открытый ключ, можно проверить правильность уже поставленной под документом с помощью соответствующего секретного ключа подписи, но невозможно правильно эту подпись поставить.

5.3. Для подписи документа уполномоченное лицо каждой из сторон использует свою личную ЭП, хранящуюся на носителе (в файловом хранилище ключей или USB-токене). Данное лицо несет полную ответственность за подлинность и конфиденциальность своей ЭП. В частности, все документы, подпись под которыми при проверке действительным открытым ключом ЭП лица является правильной, считаются подписанными этим лицом, даже если ЭП была поставлена другим лицом, получившим каким-либо образом доступ к ЭП этого лица.

5.4. Открытые ключи ЭП лиц с правом подписи хранятся у противоположной стороны и используются для проверки подписи под документами. ЭП под документом считается правильной, если проверка ЭП с помощью действовавшего на момент ее простановки ключа дает положительный результат. Проверка ЭП производится с помощью соответствующей утилиты Системы.

5.5. Стороны признают используемые в настоящей Системе электронные документы с правильной цифровой ЭП уполномоченных лиц организации юридически эквивалентными (аутентичными) бумажным документам с рукописными подписями уполномоченных лиц и печатью организации.

Приложение № 4
к Порядку дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Тагилбанк» с использованием доступа через
информационно-телекоммуникационную сеть Интернет

ПОРЯДОК
разбора конфликтных ситуаций,
связанных с подлинностью электронных документов в Системе

1. Банк рассматривает заявления Клиента, в том числе при возникновении споров, связанных с использованием Клиентом Системы, с подлинностью Электронного документа, а также предоставляет Клиенту возможность получать информацию о результатах рассмотрения заявлений, в том числе в письменной форме по требованию Клиента, в течение 30 календарных дней со дня получения таких заявлений, а также в течение 60 календарных дней со дня получения заявлений в случае использования электронного средства платежа для осуществления трансграничного перевода денежных средств.

2. Споры, не урегулированные путем переговоров, разрешаются в судебном порядке в соответствии с законодательством РФ.

3. В настоящем Приложении описан порядок разрешения конфликтов следующих типов:

- отказ Банка от факта получения Электронного документа (Клиент утверждает, что направленный им Электронный документ был принят Банком, Банк это отрицает);
- отказ Банка от Электронного документа (Клиент утверждает, что данный Электронный документ был принят им от Банка, Банк это отрицает);
- отказ Клиента от факта получения Электронного документа (Банк утверждает, что данный Электронный документ был получен Клиентом, Клиент это отрицает);
- отказ Клиента от документа (Клиент утверждает, что принятый к исполнению документ не направлялся им Банку, Банк это отрицает);
- проверка подлинности Электронного документа (Сторона утверждает, что принятый к исполнению Электронный документ не соответствует переданному).

4. В случае опротестования Клиентом операции, проведенной Банком от его имени и по его счету (далее – «спорная операция»), Клиент подает в Банк письменное заявление с изложением сути протеста и детальным описанием спорной операции, а также документы, имеющие отношение к предмету спора.

5. Для разрешения разногласий, заключающихся в оспаривании авторства и/или содержимого документа, совершенного в Системе «Интернет-банк», создается экспертная комиссия (далее – Комиссия). В состав Комиссии входят не менее 2 (двух) представителей Банка. Члены Комиссии от Банка назначаются приказом по Банку.

6. Клиент обязуется способствовать работе Комиссии и не допускать отказа от предоставления необходимых документов. Клиент обязуется предоставить Комиссии возможность ознакомления с условиями и порядком работы программных и аппаратных средств, используемых для обмена Электронными документами.

7. В ходе работы Комиссии Клиент и (или) Банк обязаны доказать, что обязательства, возложенные на какую-либо из сторон Договора, были исполнены надлежащим образом.

8. По итогам работы Комиссии Банк формирует в 2-х экземплярах Акт работы экспертной комиссии (далее – Акт) и направляет на имя Клиента письменный ответ на претензию с приложением одного экземпляра Акта, содержащий следующую информацию:

- фактические обстоятельства, послужившие основанием возникновения разногласий;
- техническая информация, полученная в процессе рассмотрения спорной ситуации (статистика доступа к Системе «Интернет-банк», записи журнала доступа за определенный период и т.д.);

– вывод о подлинности оспариваемого Электронного документа и его обоснование.

9. Если Клиент настаивает на том, что данный Электронный документ он не отправлял, Комиссия может вынести решение о компрометации доступа к Системе «Интернет-банк», что не снимает ответственности Клиента за данный Электронный документ.

10. Если проверка подлинности Электронного документа дает отрицательный результат, то Комиссией принимается решение о том, что Клиент не направлял Электронный документ Банку и не должен нести за него ответственность. В этом случае ответственность за Электронный документ несет Банк.

11. Акт, составленный Комиссией, является обязательным для Сторон и может служить доказательством при дальнейшем разбирательстве спора в суде. Все спорные вопросы, по которым стороны не достигли соглашения, а также отказ любой стороны от добровольного исполнения решения Комиссии, разрешаются в судебном порядке в соответствии с законодательством Российской Федерации в Арбитражном суде Свердловской области.

Приложение № 5
к Порядку дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Тагилбанк» с использованием доступа через
информационно-телекоммуникационную сеть Интернет

ЗАЯВЛЕНИЕ
о присоединении к Порядку дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Тагилбанк» с использованием доступа через Интернет

Настоящим Клиент_____
в лице _____,
действующего на основании _____:

- Заявляет о своем присоединении к «Порядку дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Тагилбанк» с использованием доступа через информационно-телекоммуникационную сеть Интернет» (далее – Порядок), ознакомлен с указанным Порядком.
- Просит подключить к дистанционному банковскому обслуживанию с использованием доступа через Интернет расчетный(е) счет(а) № _____
  _____
  _____
- Обязуется строго и безоговорочно соблюдать все требования Порядка, в том числе соблюдать режим ограниченного доступа к компьютеру, на котором установлено программное обеспечение Системы ДБО, исключить возможность несанкционированного доступа ко всем ключам ЭП, использовать и оперативно обновлять специализированное программное обеспечение для защиты информации – антивирусное программное обеспечение, персональные межсетевые экраны, средства защиты от несанкционированного доступа и пр.

_____
подпись

Актуальная информация для связи с Клиентом в соответствии с ч. 13 ст. 5 Федерального закона от 27.06.2011 года № 161-ФЗ «О национальной платежной системе»: *(указать адрес электронной почты, номер мобильного телефона, либо способ – личное обращение в банк для получения отчета на бумажном носителе)*
_____
_____

_____
подпись

Блокировочное слово: *(предназначено для аутентификации Клиента при телефонном звонке в Банк с целью временно блокировать работу в системе дистанционного банковского обслуживания.)*
_____

Подтверждаю достоверность и актуальность всех сведений о Клиенте, предоставленных при открытии вышеуказанного(ых) расчетного(ых) счета(ов). Гарантирую, что никаких изменений в предоставленных сведениях о Клиенте на дату подписания настоящего заявления не имеется. Обязуюсь ежедневно любым доступным мне способом самостоятельно обращаться в АО «Тагилбанк», в т.ч. на его официальный сайт в сети Интернет по адресу **http://tagilbank.ru** для получения сведений о новой редакции, о внесенных изменениях и (или) дополнениях в Порядок

_____
Подпись, фамилия и инициалы Клиента

м.п.

Заявление о присоединении получено, идентификация Клиента проведена, собственноручная подпись Клиента верна.
Дата принятия Заявления «_____»_____ 201___ г.
Должность, Ф.И.О. и подпись работника, принявшего Заявление:
_____
_____

Приложение № 6
к Порядку дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Тагилбанк» с использованием доступа через
информационно-телекоммуникационную сеть Интернет

УВЕДОМЛЕНИЕ
об изменении сведений о Клиенте

Настоящим Клиент_____
в лице_____,
действующего на основании _____, уведомляет банк об изменении следующих сведений о Клиенте: *(указать изменившиеся сведения – адрес/место нахождения, контактные телефоны, паспортные данные руководителя юридического лица или индивидуального предпринимателя, состав участников/акционеров юридического лица, величина уставного капитала юридического лица, изменения в составе бенефициарных владельцев, изменение их паспортных данных, сведения о назначении и сроках полномочий представителей и об их паспортных данных, изменение актуальной информация для связи с Клиентом в соответствии с ч. 13 ст. 5 Федерального закона от 27.06.2011 года № 161-ФЗ «О национальной платежной системе» или др.):*

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
Подпись, фамилия и инициалы Клиента

м.п.

Уведомление об изменении сведений получено, идентификация Клиента проведена, собственноручная подпись Клиента верна.

Дата принятия Уведомления «_____»_____ 201___ г.

Должность, Ф.И.О. и подпись работника, принявшего Уведомление:

_____
_____

Приложение № 7
к Порядку дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Тагилбанк» с использованием доступа через
информационно-телекоммуникационную сеть Интернет

ЗАЯВЛЕНИЕ
о расторжении Договора дистанционного банковского обслуживания с использованием доступа через информационно-телекоммуникационную сеть Интернет

Настоящим Клиент_____
в лице_____,
действующего на основании_____ в одностороннем порядке расторгает с ___.___.201___ года Договор дистанционного банковского обслуживания с использованием доступа через информационно-телекоммуникационную сеть Интернет, заключенный между Клиентом и АО «Тагилбанк».

_____

Подпись, фамилия и инициалы Клиента

м.п.

Заявление о расторжении Договора получено, идентификация Клиента проведена, собственноручная подпись Клиента верна.

Дата принятия Заявления «_____»_____ 201___ г.

Должность, Ф.И.О. и подпись работника, принявшего Заявление:

_____

_____

Приложение № 8
к Порядку дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Тагилбанк» с использованием доступа через
информационно-телекоммуникационную сеть Интернет

АКТ №_____
приема-передачи устройства USB-токен

«_____» _____ 201__ г. г. Нижний Тагил

Настоящим Актом подтверждается, что АО «Тагилбанк», именуемое в дальнейшем Банк, в лице _____,
действующего на основании _____ передал,
а _____,
именуемое в дальнейшем Клиент, в лице _____,
действующего на основании _____,
получил:

– устройство USB-токен, в количестве _____ штук,

с серийным номером №_____ с серийным номером №_____
с серийным номером №_____ с серийным номером №_____

для использования его/их в рамках «Порядка дистанционного банковского обслуживания юридических лиц и индивидуальных предпринимателей в АО «Тагилбанк» с использованием доступа через информационно-телекоммуникационную сеть Интернет» в качестве средства формирования и проверки электронной подписи.

Клиент подтверждает, что корпус переданного Устройства не имеет видимых признаков повреждения и взлома.

Клиент обязуется использовать и хранить USB-токен в соответствии правилами эксплуатации и хранения USB-токена.

Клиент согласен, что для использования USB-токена необходимо установить на своем рабочем месте (местах) драйвер USB-токен.

Клиент обязуется сформировать электронную подпись на USB-токен и предоставить в Банк Сертификат ключа проверки электронной подписи.

Настоящий акт составлен на 1 странице в двух экземплярах, имеющих одинаковую юридическую силу.

Руководитель организации Клиента

_____ / _____
(подпись) (Ф. И. О.)

М.П.

Уполномоченный представитель Банка

_____ / _____
(подпись) (Ф. И. О.)

М.П.

Администратор безопасности системы

_____ / _____
(подпись) (Ф. И. О.)

Приложение № 1
к Акту приема-передачи
устройства USB-токен

ПРАВИЛА
эксплуатации и хранения USB-токена

- Необходимо оберегать USB-токен от воздействия влаги и агрессивных сред сильных механических воздействий (падения с высоты, сотрясения, вибрации, ударов и т. п.), воздействия высоких и низких температур. При резкой смене температур (перемещении охлажденного USB-токен с мороза в теплое помещение) не рекомендуется использовать USB-токен в течение 3 часов во избежание повреждения USB-токена из-за сконденсированной на его электронной схеме влаги. Необходимо оберегать USB-токен от попадания на него прямых солнечных лучей;
- Недопустимо воздействие на USB-токен сильных магнитных, электрических или радиационных полей, высокого напряжения и статического электричества;
- При подключении USB-токена к компьютеру не прилагайте излишних усилий;
- USB-токен в нерабочее время необходимо всегда держать закрытым во избежание попадания на разъем USB-токена пыли, грязи, влаги и т. п. При засорении разъема токена нужно принять меры для его очистки. Для очистки корпуса и разъема используйте сухую ткань. Использование воды, растворителей и прочих жидкостей недопустимо. Не разбирайте USB-токен, это ведет к потере гарантии! В случае неисправности или неправильного функционирования USB-токена обращайтесь в Банк;
- Не передавайте USB-токен третьим лицам! Не сообщайте третьим лицам пароль от ключей электронной подписи! В случае утери (хищения) или повреждения USB-токена немедленно свяжитесь с банком;
- Ваш пароль от ключа электронной подписи не должен состоять из одних цифр. Безопасный пароль должен быть длиннее 6 знаков. Пароль должен содержать в себе строчные и прописные буквы, цифры и знаки препинания. Безопасный пароль не должен состоять из символов, находящихся на одной линии на клавиатуре. Пароль не должен быть значимым словом, которое можно легко подобрать или угадать.
- В связи с появлением вредоносного программного обеспечения, умеющего имитировать действия пользователя при создании и подписании электронной подписи платежного документа, настоятельно рекомендуется вставлять USB-токен в компьютер ТОЛЬКО на время работы в Системе «Интернет-банк» и ни в коем случае не оставлять его без присмотра!

Приложение № 9
к Порядку дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Тагилбанк» с использованием доступа через
информационно-телекоммуникационную сеть Интернет

ЗАЯВЛЕНИЕ
на внеплановую замену ключей и ключевого носителя

Настоящим Клиент_____
в лице_____,
действующего на основании _____, просит выполнить:

☐ внеплановую замену ключей электронной подписи в связи с _____
_____
_____

☐ замену ключевого носителя (USB-токена) и внеплановую замену ключей электронной подписи в связи с _____
_____
_____

☐ замену блокировочного слова *(указать новое)* «_____» в связи с
_____
_____

для системы «Интернет-банк».

_____
Подпись, фамилия и инициалы Клиента

м.п.

Заявление получено, идентификация Клиента проведена, собственноручная подпись Клиента верна.

Дата принятия Заявления «_____»_____ 201___ г.

Должность, Ф.И.О. и подпись работника, принявшего Заявление:
_____
_____

Приложение № 10
Порядку дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Тагилбанк» с использованием доступа через
информационно-телекоммуникационную сеть Интернет

ЗАЯВЛЕНИЕ
о временном изменении режима при обслуживании с использованием системы дистанционного банковского обслуживания

Настоящим Клиент _____
в лице _____,
действующего на основании _____, просит включить/отключить дистанционное банковское обслуживание с использованием доступа через информационно-телекоммуникационную сеть Интернет:

Включить		Отключить
☐	Режим временного ограничения обслуживания в Системе ДБО (вход в Систему и получение документов из Банка будет возможен, дебет счетов запрещен)	☐
☐	Режим приостановления обслуживания в Системе ДБО (работа в Системе будет заблокирована)	☐

_____
Подпись, фамилия и инициалы Клиента

м.п.

Заявление о временном изменении режима получено**,** идентификация Клиента проведена, собственноручная подпись Клиента верна.

Дата принятия Заявления «_____»_____ 201___ г.

Должность, Ф.И.О. и подпись работника, принявшего Заявление:
_____
_____

Приложение № 11
к Порядку дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Тагилбанк» с использованием доступа через
информационно-телекоммуникационную сеть Интернет

ЗАЯВЛЕНИЕ
на подключение фильтрации по IP-адресам с использованием системы дистанционного банковского обслуживания

Настоящим Клиент
_____ в лице
_____,
действующего на основании _____, просит включить/отключить фильтрацию по IP-адресам с использованием системы дистанционного банковского обслуживания с доступом через информационно-телекоммуникационную сеть Интернет для следующих IP адресов:

Включить	IP-адрес или диапазон IP-адресов (доступ к системе будет возможен только с этих IP адресов)	Отключить
☐		☐
☐		☐
☐		☐
☐		☐
☐		☐
☐		☐
☐		☐

_____
Подпись, фамилия и инициалы Клиента

м.п.

Заявление на подключение фильтрации по IP-адресам получено, изменения в списки IP-адресов, допущенных к работе в системе ДБО внесены, идентификация Клиента проведена, собственноручная подпись Клиента верна

Дата принятия Заявления «_____»_____ 201___ г.

Должность, Ф.И.О. и подпись работника, принявшего Заявление:
_____
_____

Приложение № 12
к Порядку дистанционного банковского обслуживания
юридических лиц и индивидуальных предпринимателей
в АО «Тагилбанк» с использованием доступа через
информационно-телекоммуникационную сеть Интернет

АКТ №_____
приема-передачи средства криптографической защиты информации

«_____» _____ 201__ г. г. Нижний Тагил

Настоящим Актом подтверждается, что АО «Тагилбанк», именуемое в дальнейшем Банк, в лице _____, действующего на основании _____ передал, а _____, именуем__ в дальнейшем Клиент, в лице _____, действующего на основании _____, получил:

Наименование средств защиты	Номер средства защиты	Отметка о получении
_____	№ _____	

Настоящий акт составлен на 1 странице в двух экземплярах, имеющих одинаковую юридическую силу.

Руководитель организации Клиента

_____ / _____
(подпись) (Ф. И. О.)

М.П.

Уполномоченный представитель Банка

_____ / _____
(подпись) (Ф. И. О.)

М.П.

Администратор безопасности системы

_____ / _____
(подпись) (Ф. И. О.)