УТВЕРЖДАЮ:
Председатель Правления
ПАО «НИКО-БАНК»
_____С.В. Сивелькина

Введено в действие с «20» ноября 2019 г.
Приказом № 776пр от 08.11.2019 г.

Правила работы системы «Интернет-Клиент» в ПАО «НИКО-БАНК»

1. Общие положения.

1.1. Настоящие Правила определяют порядок работы Клиента в рамках Системы «Интернет-Клиент», регулируют отношения, возникающие в связи с этим между Банком и Клиентом.
1.2. Термины, определения и сокращения:

Автоматизированное рабочее место по обмену электронными документами с использованием системы «Интернет-Клиент» (АРМ ИК) – комплекс программных и аппаратных средств, включая средства криптографической защиты информации, используемых Сторонами для обмена ЭД.

Администратор информационной безопасности Банка (Администратор ИБ) **–** работник, на которого возложены обязанности по регистрации и проверке ключей системы защиты информации в Банке.

Владелец сертификата ключа проверки электронной подписи (Владелец электронной подписи, Владелец ЭП) – лицо, которому выдан сертификат ключа проверки электронной подписи. Право владельца электронной подписи принадлежит лицам, имеющим полномочия на распоряжение находящимися на счете денежными средствами и указанным в принятой Банком карточке с образцами подписей и оттиска печати.

Вредоносный код – компьютерная программа, предназначенная для внедрения в автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование Банка и Клиента – пользователей систем дистанционного банковского обслуживания, приводящего к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче любой информации в электронном виде, а также к созданию условий для такого уничтожения, создания, копирования, блокирования, модификации и (или) передачи.

Договор - договор комплексного банковского обслуживания, заключенный между Банком и Клиентом.

Ключевая информация – Ключ электронной подписи, Ключ проверки электронной подписи. Плановое обновление ключевой информации производится не реже 1 раза в год. Плановая смена ключей ЭП производится без смены Владельца электронной подписи и типа носителя Ключевой информации.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с Ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Компрометация ключа электронной подписи – событие, определенное Владельцем электронной подписи как ознакомление неуполномоченным лицом (лицами) с его ключом электронной подписи, а также утрата (хищение) ключа электронной подписи, утрата (хищение) ключа электронной подписи с последующим его обнаружением. Компрометацией ключа, в частности, считаются следующие события: утрата, утрата с последующим обнаружением, несанкционированное копирование или подозрение на копирование, любые другие события, когда достоверно неизвестно, что произошло с носителем ключевой информации. Ключи считаются скомпрометированными и при увольнении (отстранении от занимаемой должности) ответственных исполнителей сторон, имеющих доступ к ключевой информации.

Мобильное приложение (NICO-BANK: Business-Online) - комплекс услуг, предоставленных Банком Клиенту и обеспечивающих возможность передачи между Банком и Клиентом электронных документов, подписанных электронной подписью, с использованием мобильных устройств.

Мобильное устройство - смартфон, планшет с актуальной версией операционной системы iOS или Android.

Ответственный работник Клиента – ответственный за подключение уполномоченное лицо, назначенное Клиентом для организации:

- процедуры генерации Ключевой информации;
- мер, необходимых для обеспечения безопасности при обмене ЭД;
- обмена ЭД с использованием АРМ ИК;
- взаимодействия с Банком по вопросам Ключевой информации и обмена ЭД.

Подлинность электронного документа (подлинность ЭД) – положительный результат проверки ЭП зарегистрированного Владельца электронной подписи, устанавливающий факт неизменности содержания ЭД, включая все его реквизиты.

Подтверждение достоверности ЭД – процедура проверки правильности ЭП, позволяющая установить факт неизменности содержания электронного документа, включая все его реквизиты.

Правила – настоящие Правила работы Системы «Интернет-Клиент».

Сертификат ключа проверки электронной подписи (Сертификат) – электронный документ или документ на бумажном носителе, выданный Банком и подтверждающий принадлежность Ключа проверки электронной подписи Владельцу электронной подписи.

Система «Интернет-Клиент» - совокупность программно-аппаратных средств, устанавливаемых на территории Клиента и Банка и согласованно эксплуатируемых Клиентом и Банком в соответствующих частях, а также организационных мероприятий, проводимых Клиентом и Банком, с целью предоставления Клиенту услуг в соответствии с настоящими Правилами. Система "Интернет-Клиент" состоит из подсистем обработки, хранения, защиты и передачи информации. Система «Интернет-Клиент» включает сервисы «Интернет-Клиент» и «Мобильный банк». Предоставление услуги на базе цифровой платформы Digital2Go от Компании BSS/платформа BS-Client от Компании BSS.

СКЗИ – средства криптографической защиты информации.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций – создание ЭП, проверка подлинности ЭП, создание Ключа электронной подписи и Ключа проверки электронной подписи.

Система управления ключевой информации – совокупность программно-аппаратных средств, ответственного подразделения Банка, работников ответственного подразделения Банка, выполняющих функции регистрации и сертификации Ключей проверки электронной подписи Клиента и Банка.

Уполномоченный работник Банка – работник Банка, взаимодействующий с Клиентом в рамках работы в Системе «Интернет-Клиент».

ФСТЭК - Федеральная служба по техническому и экспортному контролю.

Шифрование – криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому ЭД.

Электронный служебно-информационный документ (ЭСИД) – документ, в том числе и вложенный в виде отдельного файла, подписываемый ЭП, обеспечивающий обмен информацией с Банком (запросы, отчеты, другие документы) и имеющий равную юридическую силу с соответствующими документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати (при наличии), только при условии установления подлинности ЭСИД.

Электронный документ (ЭД) – электронный платежный документ и/или электронный служебно-информационный документ.

Электронный платежный документ (ЭПД) – документ, являющийся основанием для совершения операций по банковским счетам Клиента, открытым в Банке на основании Договора, подписанный ЭП и имеющий равную юридическую силу с распоряжениями на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати (при наличии), согласно заявленным образцам подписей и оттиска печати (при наличии), только при условии подтверждения подлинности ЭПД.

Электронное устройство – устройство Клиента, используемое в качестве удаленного рабочего места для целей дистанционного управления денежными средствами Клиента: персональный компьютер, ноутбук.

Электронная подпись (ЭП) – 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. По классификации Федерального закона от 06.04.2011 №63-ФЗ "Об электронной подписи" электронная подпись, используемая в Системе «Интернет-Клиент», относится к усиленной неквалифицированной электронной подписи.

PIN-код – пароль доступа к носителям Ключевой информации - USB-ключу eToken PRO/Рутокен ЭЦП 2.0, который служит для дополнительной защиты. Пароль может содержать знаки (цифры, буквы, символы) на английской раскладке на клавиатуре, и быть не менее 8 знаков.

1.3. Правила работы Системы «Интернет-Клиент» разработаны в соответствии с действующим законодательством Российской Федерации, в том числе с положениями нормативных актов ФСТЭК России, Федеральной службы безопасности, Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи» и других федеральных законов.

1.4. Настоящие Правила, включая все Приложения к ним, утверждаются Банком и размещаются на информационных стендах в структурных подразделениях Банка, в которых осуществляется обслуживание юридических лиц и индивидуальных предпринимателей, на официальном сайте Банка в сети Интернет по адресу www.nico-bank.ru.

1.5. Все изменения и дополнения в настоящие Правила и формы приложений к ним вносятся Банком в одностороннем порядке. Информация об изменении/дополнении настоящих Правил и Приложений к ним доводится Банком до сведения Клиентов посредством уведомления не менее чем за 10 (Десять) календарных дней до даты вступления в силу таких изменений/дополнений. Уведомление осуществляется путем размещения соответствующей информации на официальном сайте Банка в сети Интернет по адресу www.nico-bank.ru, на информационных стендах в структурных подразделениях Банка, в которых осуществляется обслуживание юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой, а также путем направления Банком Клиенту соответствующего сообщения по Системе «Интернет-Клиент».

1.6. Ознакомление Клиента с настоящими Правилами осуществляется до подключения Клиента к Системе «Интернет-Клиент».

1.7. Клиент присоединяется к настоящим Правилам путем подачи в Банк Заявления о присоединении к договору комплексного банковского обслуживания в ПАО «НИКО-БАНК путем заполнения соответствующих полей или заявления о присоединении, представленном в Приложении №1 к настоящим Правилам. С этого момента возникают права и обязанности Клиента и Банка по работе в Системе «Интернет-Клиент».

1.8. Присоединение к настоящим Правилам Клиентов, с которыми до 01.12.2019 Банком заключены Соглашения «Об обмене электронными документами при осуществлении расчетов с использованием системы «Интернет-Клиент», осуществляется путем подписания Клиентом Заявления о присоединении, форма которого представлена в Приложении № 1 к настоящим Правилам.

1.9. Требования, предусмотренные настоящими Правилами, относятся к технологиям, системам и средствам обработки, передачи и хранения ЭД и предназначены для Клиентов Банка, принимающих участие в обмене ЭД по Системе «Интернет-Клиент».

1.10. Безопасность технологии обработки ЭД обеспечивается созданием системы, включающей в себя комплекс технологических, организационных, аппаратных и программных мер и средств защиты на этапах подготовки, обработки, передачи и хранения ЭД.

1.11. Клиент обязуется соблюдать Рекомендации по обеспечению информационной безопасности при использовании Системы «Интернет-Клиент», представленные в Приложении №3 к настоящим Правилам.

1.12. Обязанности по администрированию программно-технических средств защиты ЭД рекомендуется возложить на одного из работников, эксплуатирующих данную подсистему, с внесением соответствующих изменений в его должностные обязанности (Ответственный работник Клиента).

Информация, содержащаяся в ключевых документах на бумажных, магнитных и других носителях для средств криптографической защиты, относится к информации ограниченного доступа.
1.13. Обмен электронными документами проводится через Систему «Интернет-Клиент», которая состоит из Центрального абонентского пункта - Банка и Абонентских пунктов – Клиентов, информационная безопасность документооборота осуществляется в соответствии с настоящими Правилами.
1.14. Абонентский пункт Банка передает и принимает документы с помощью Системы «Интернет-Клиент», работающей по каналам связи сети Интернет.
Использование других каналов связи для передачи электронных документов согласуется Сторонами отдельно.
Инициатором соединения для приема и передачи документов всегда является Клиент.
1.15. Для обслуживания Системы «Интернет-Клиент» Банк назначает ответственное лицо (Администратор системы «Интернет-Клиент» Банка). Администратор не должен иметь доступов к ЭП Владельцев, контактные телефоны: (3532) 34-90-90.
1.16. Функции Администратора Банка:

- отвечает за работу абонентского пункта в Системе «Интернет-Клиент»;
- участвует в процедуре проверки ЭП при решении конфликтных ситуаций;
- организует технический прием и передачу документов на абонентском пункте;
- по запросу Клиента обеспечивает консультационную поддержку персонала Клиента.

1.17. В рамках установочных работ Банк на основании предоставленных документов:

- производит регистрацию Клиента в Системе «Интернет-Клиент»;
- передает клиенту пакет документов в опечатанных конвертах: логин и пароль для входа в Систему «Интернет-Клиент», носители Ключевой информации eToken PRO/Rutoken и электронный автономный генератор одноразовых паролей eToken PASS.

1.18. Клиент в свою очередь самостоятельно производит настройку автоматизированного рабочего места и осуществляет вход в Систему «Интернет-Клиент» с помощью логина и пароля, которые Клиент получает или на бумажном носителе или по SMS (при наличии технической возможности).
1.19. Владелец ЭП производит при первом входе принудительную смену пароля для входа в Систему «Интернет-Клиент» на новый, известный только Владельцу ЭП пароль.
1.20 Ввод в эксплуатацию Системы «Интернет-Клиент» оформляется Актом о вводе в эксплуатацию системы электронного документооборота, подписанный Клиентом и Банком**.**

2. Порядок приема и передачи документов по Системе «Интернет-Клиент».

2.1. Клиент готовит электронное сообщение для передачи.
2.2. Клиент подписывает электронное сообщение своей ЭП. ЭП подтверждает авторство отправленного по Системе «Интернет-Клиент» документа и гарантирует его целостность, т.к. любое изменение в документе после его подписания сделает ЭП недействительной.
2.3. Клиент инициирует соединение с сервером Банка для передачи и приема электронных сообщений. Время обмена сообщениями определяется следующим образом:
2.2.1. Стороны признают в качестве единой шкалы времени при работе в Системе «Интернет-Клиент» Оренбургское поясное время (московское время плюс два часа). Контрольным является время системных часов аппаратных средств Банка.
2.3.2. Клиент осуществляет расходные операции по своему счету в пределах операционного времени Банка. Операционное время Банка устанавливается Общими правилами комплексного банковского обслуживания корпоративных клиентов в ПАО «НИКО-БАНК». Работа линии «Интернет-Клиент» по приему документов и их рассылка осуществляется в круглосуточном режиме, за исключением времени технологических перерывов, о которых Банк заблаговременно обязан любым способом предупредить Клиента.
2.3.3. Стороны считают, что моментом поступления информации принимающей Стороне в системе «Интернет-Клиент» является текущее время по системным часам принимающей Стороны в момент полного помещения информации на сервере принимающей стороны.
2.3.4. Платежные документы, поступившие в Банк по Системе «Интернет-Клиент» в течение операционного времени Банка, принимаются к исполнению текущим днем, поступившие в послеоперационное время Банка - следующим рабочим днем.

2.4. Основанием для принятия Банком переданного Клиентом по Системе «Интернет-Клиент» платежного документа является наличие и корректность ЭП, а также соответствие требованиям к оформлению платежных документов.
2.5. Банк формирует Клиенту электронное служебное сообщение о получении, прочтении и исполнении либо неисполнении платежного документа, которое Клиент получает в том же или при очередном сеансе связи с Банком.
2.6. По документам, оформленным с нарушением требований, в том числе с неверной ЭП, Клиенту по Системе «Интернет-Клиент» направляется электронное служебное сообщение с указанием причины, по которой платежный документ не принят.
В случае неполучения служебного сообщения о приеме/неприеме отправленного в Банк электронного документа в течение одного рабочего часа после отправки (с учетом режима работы Банка), Клиент может запросить разъяснения у ответственного работника Банка.
По отдельным платежным документам Банк может запросить дополнительное подтверждение или разъяснение. Подтверждение запрашивается по Системе «Интернет-Клиент» либо иным образом в день получения платежного документа. В этом случае платежный документ принимается к исполнению после получения требуемого подтверждения.

3. Носители ключевой информации и порядок обращения с ними.

3.1. В рамках работы Системы «Интернет-Клиент» для записи Ключевой информации используются тип носителя Ключевой информации USB-ключ eToken PRO/ Rutoken ЭЦП 2.0.
3.2. Носители Ключевой информации маркируются и учитываются в журнале, в котором указывается Ф.И.О. работника, сформировавшего Ключевую информацию (в том числе в случае формирования Ключевой информации Клиентом), дата формирования, вид содержащейся на нем информации, срок действия носителя Ключевой информации, перечень лиц, допущенных к работе с данным носителем, дата и причину вывода носителя из действия.
3.3. Создание Ключевой информации проводится на выделенном Электронном устройстве, программное обеспечение которого должно выполнять только функции, регламентированные технологическим процессом формирования криптографических ключей при отсутствии посторонних лиц. При этом электронное устройство размещается в отдельном, выделенном только для этой цели помещении.
3.4. Электронное устройство, вырабатывающее Ключевую информацию, должно быть оснащено программно-аппаратными системами защиты информации от несанкционированного доступа, имеющими сертификат ФСТЭК.
3.5. Доступ посторонних (неуполномоченных) лиц к носителям с Ключевой информацией должен быть исключен.
Не допускается:
- снимать несанкционированные копии с носителей Ключевой информации;
- знакомить с содержанием носителей Ключевой информации или передавать носители Ключевой информации лицам, в обязанности которых не входит работа в Системе «Интернет-Клиент» (в том числе не передавать носители IT-специалистам, обслуживающим АРМ ИК);
- выводить ключи электронной подписи /закрытые ключи шифрования на дисплей (монитор) или принтер;
- устанавливать носитель Ключевой информации в считывающее устройство АРМ ИК в режимах, не предусмотренных функционированием системы обработки и обмена ЭД, а также в другие Электронные устройства;
- записывать на носитель Ключевой информации постороннюю информацию.
3.6. Клиент обязан присоединять носитель Ключевой информации к АРМ ИК непосредственно перед началом работы в Системе «Интернет-Клиент», а по окончании работы извлекать носитель Ключевой информации из АРМ ИК. Во время работы с ключевыми документами необходимо исключить присутствие лиц, в функциональных обязанностях которых не предусмотрен доступ к ключевым документам.
Ключевая информация, принадлежащая ответственному исполнителю ЭП, хранятся владельцем ЭП в месте, недоступном для посторонних лиц (металлическом ящике или сейфе). Металлический ящик (сейф) должен надежно запираться и опечатываться (опломбироваться) печатью ответственного исполнителя. Использовать этот металлический ящик (сейф), опечатывать его и

вскрывать имеет право только лицо, уполномоченное для работы с данными ключевыми носителями. Допускается хранение ключевых документов в одном металлическом шкафу (сейфе) с другими документами ответственного исполнителя Клиента, но при этом отдельно от них и в упаковке, на которой указано, где эти ключевые документы используются.
Помещение, в котором размещается электронный идентификатор, должно быть оборудовано пожарной и охранной сигнализацией, решетками на окнах, дверьми с надежными замками.
3.7. В случае прекращения по тем или иным причинам полномочий работника Клиента, имевшего доступ к Системе «Интернет-Клиент», Клиенту необходимо незамедлительно известить об этом Банк, а также произвести смену паролей, перегенерацию закрытых ключей шифрования и ключей электронной подписи, бывших в распоряжении данного сотрудника.
3.8. Срок действия Ключевой информации – 1 год. После ввода в действие новых ключей ЭП / закрытых ключей шифрования недействительные (старые) ключи ЭП / закрытые ключи шифрования уничтожаются Клиентом самостоятельно с составлением акта. Ключи проверки ЭП / открытые ключи шифрования хранятся Клиентом в течение всего срока хранения ЭД, для подтверждения подлинности которых они могут быть использованы. Уничтожение ключей проверки ЭП / открытых ключей шифрования после истечения срока их хранения осуществляется Клиентом самостоятельно с составлением акта.
3.9. В случае если Банк производит генерацию (перегенерацию) ключа(ей) электронной подписи на носителях ключей информации - USB-ключ eToken PRO/ Rutoken, подготовку носителя для передачи Клиенту и т.д., Банк устанавливает по умолчанию PIN-код на USB-ключе eToken PRO/ Rutoken - 1234567890. Клиент обязан провести смену PIN-кода Владельца электронной подписи не позднее рабочего дня, следующего за днем получения Сертификата.
При неправильном вводе PIN–кода определенное количество раз подряд USB-ключ eToken PRO/ Rutoken блокируется. В этом случае Клиент может воспользоваться выданным паролем администратора ключевого носителя, который выдается клиенту в опечатанном конверте при передаче носителя eToken PRO/ Rutoken. Либо Клиент может обратиться в Банк для проведения процедуры перегенерации ключей ЭП.

4. **Правила парольной защиты.**

4.1. Клиент обязан установить пароли на учетные записи пользователей АРМ ИК.
4.2. Клиент обязан проводить полную плановую смену паролей пользователей АРМ ИК регулярно, не реже одного раза в 30 (Тридцать) дней.
4.3. Клиент обязан провести внеплановую полную смену паролей пользователей АРМ ИК в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) пользователя АРМ ИК.
4.4. В случае компрометации личного пароля одного из пользователей АРМ ИК Клиент обязан провести внеплановую полную смену паролей всех пользователей данного АРМ ИК.
4.5. Клиент не должен использовать функцию запоминания логина и пароля в браузерах.
4.6. Клиент не должен использовать одинаковые логин и пароль для доступа к различным системам.

5. Обеспечение информационной безопасности при подготовке, обработке и передаче ЭД.

5.1. На АРМ ИК рекомендуется устанавливать только лицензионное программное обеспечение. АРМ ИК в обязательном порядке должно быть оснащено средствами антивирусной защиты, а также желательно сертифицированные ФСТЭК программно-аппаратными системами защиты от несанкционированного доступа.
5.2. Конфиденциальность ЭД обеспечивается на основе использования средств криптографической защиты информации.
5.3. При эксплуатации СКЗИ необходимо соблюдать требования и рекомендации эксплуатационной документации на СКЗИ.
5.4. Клиент должен четко регламентировать порядок использования АРМ ИК, с которого осуществляется взаимодействие с Системой «Интернет-Клиент», в том числе список лиц и порядок доступа к АРМ ИК.

5.5. Не рекомендуется использовать на АРМ ИК средства удаленного (дистанционного) доступа, в том числе IT-специалистами для удалённой поддержки.
5.6. Не рекомендуется использовать АРМ ИК для доступа к посторонним сайтам сомнительного содержания.
5.7. Не рекомендуется устанавливать на АРМ ИК постороннее программное обеспечение, например, программы автоматического переключения раскладки клавиатуры, различные дополнения к браузерам и т.п. Программы данного вида могут передавать информацию о содержимом просматриваемых страниц посторонним лицам.
5.8. Не рекомендуется запускать на АРМ ИК программы, полученные из не заслуживающих доверия источников.
5.9. Клиент должен перед вводом своего логина и пароля убедиться, что установлено соединение с легальным сайтом Системы «Интернет-Клиент». Необходимо проверить правильность указания адреса сайта «http**s**://bk.nico-bank.ru»/ «http**s**://d2g.nico-bank.ru».
5.10. Клиент должен всегда правильно завершать сеанс работы в Системе «Интернет-Клиент», в обязательном порядке используя пункт меню «Выход».
5.11. Клиент не должен совершать доступ к Системе «Интернет-Клиент» с использованием постороннего АРМ ИК.
5.12. Клиент при подаче заявления на подключение Сервиса «Интернет-Клиент» по желанию может указать IP-адреса и MAC-адреса АРМ ИК на установку в Банке фильтра для АРМ ИК Клиента. Это позволит исключить возможность входа под вашим логином/паролем с АРМ злоумышленников.
5.13. В случае обнаружения подозрительных сайтов, доменные имена и стиль оформления которых сходны с именами и оформлением официальных сайтов ПАО «НИКО-БАНК» (например «n**l**k**o**-bank.ru», «nico-ban**c**.ru»), необходимо сообщить об этом в Банк любым из доступных способов связи.

6. **Требования и рекомендации по обеспечению информационной безопасности при использовании Мобильного приложения.**

6.1. Установку Мобильного приложения на Мобильное устройство Клиенту необходимо производить только по ссылкам, размещенным на официальном сайте Банка или в авторизованных магазинах приложений (App Store и Google Play). Обязательно убедитесь, что автором Мобильного приложения указан ПАО «НИКО-БАНК».
6.2. Клиенту необходимо установить на Мобильное устройство антивирус и своевременно его обновлять.
6.3. Клиенту необходимо своевременно устанавливать обновления безопасности операционной системы.
6.4. Клиенту необходимо установить парольную защиту на мобильном устройстве, использовать надежные пароли (как минимум 6 символов). Банк не рекомендует использовать легко подбираемые пароли, например: 123456, 111111 и т.д.
6.5. Для получения SMS с кодами подтверждения проводимых операций (при наличии технической возможности) Банк рекомендует Клиенту использовать другой мобильный телефон, не использующийся для работы с Мобильным приложением.
6.6. При получении сообщений на Мобильное устройство, содержащих ссылки или указания на установку приложений через SMS/MMS/E-mail, Банк не рекомендует Клиенту проходить по указанным в сообщении ссылкам.
6.7. Банк не рекомендует Клиенту входить в Мобильное приложение и осуществлять платежные операции в местах, где услуги Интернета являются общедоступными, и/или с использованием публичных беспроводных сетей (например: интернет-кафе, общественный транспорт и др.).
6.8. Клиенту необходимо завершать сеанс работы с Мобильным приложением, в обязательном порядке используя пункт меню «Выход».
6.9. При установке какого-либо нового приложения на мобильное устройство Клиенту необходимо обращать внимание на разрешения, которые требует приложение для своей работы, особенно на возможность доступа к SMS-сообщениям. Если разрешения вызывают подозрения или явно не соответствуют функционалу приложения, Банк рекомендует отказаться от его использования.

6.10. Банк не рекомендует Клиенту получать доступ к файловой системе своего Мобильного устройства (например, с помощью программы Jailbreaking или получение прав root для Android), так как это отключает защитные механизмы, заложенные производителем мобильной платформы.
6.11. Банк рекомендует Клиенту отключить в настройках Мобильного устройства возможность использования голосового помощника на заблокированном экране.

7. Правила антивирусной защиты АРМ ИК.

7.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).
7.2. Клиент должен производить регулярную антивирусную проверку и регулярное обновление антивирусных баз.
7.3. При возникновении подозрения на наличие вредоносного кода/компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) или обнаружении компьютерных вирусов антивирусом Клиентом незамедлительно должны быть приняты все меры по их удалению. После удаления вредоносного кода/компьютерного вируса Клиенту необходимо сменить пароль в Систему «Интернет-Клиент» и проконтролировать состояние банковского счёта.
7.4. В случае обнаружения вредоносного кода/компьютерного вируса Клиент должен предпринять все меры для прекращения любых операций с электронными документами с использованием ключей ЭП / закрытых ключей шифрования и произвести их смену. Категорически запрещается работать на АРМ ИК с платежными документами при наличии компьютерных вирусов.
7.5. Клиент должен незамедлительно обратиться в Банк в случае:
- подозрительной активности на АРМ ИК (самопроизвольное сворачивание или открывание окон, движение курсора, запуск различных программ и прочее) в период неактивности пользователя;
- появления каких-либо дополнительных окон или сообщений при попытке доступа в Систему «Интернет-Клиент» либо в процессе работы в Системе «Интернет-Клиент»;
- невозможности получения доступа к Системе «Интернет-Клиент» и т. д.
7.6. Банк не несет ответственность в случае финансовых убытков, понесенных Клиентом, в связи с нарушением и (или) ненадлежащим исполнением им требований по защите от вредоносного кода/компьютерного вируса клиентских АРМ ИК.

8. Риски, связанные с использованием ЭП.

8.1 Клиент должен понимать, что:
- существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети Интернет;
- существует вероятность атаки злоумышленников на оборудование, программное обеспечение и информационные ресурсы Клиента, подключенные/доступные в сети Интернет;
- гарантии по обеспечению информационной безопасности при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются;
- полностью исключить риск потери конфиденциальности, доступности и целостности информации передаваемой через вычислительные сети (в т.ч. через сеть Интернет, локально-вычислительные сети) невозможно, даже при выполнении всех требований и рекомендаций по информационной безопасности.
8.2. Банк фиксирует все действия, совершенные от имени Клиента в электронном журнале Системы «Интернет-Клиент». Содержимое журнала Системы «Интернет-Клиент» используется при разрешении спорных ситуаций и предоставляется по запросу правоохранительных органов в целях проведения расследования действий злоумышленников.
8.3. При несоблюдении настоящих Правил Клиент несет риски потери носителя Ключевой информации, раскрытия, искажения и несанкционированного использования ключей ЭП.
8.4. Вследствие несанкционированного использования злоумышленниками Ключевой информации возможно нанесение материального ущерба Клиенту или нанесение ущерба его деловой репутации.

8.5. В случае утраты Клиентом носителя Ключевой информации Банк не восстанавливает Ключи электронной подписи/шифрования. Информация Клиента, зашифрованная при помощи утерянного носителя Ключевой информации, восстановлению не подлежит.
8.6. При повторном получении Сертификата информация, зашифрованная с использованием старого носителя Ключевой информации, в случае его уничтожения восстановлению не подлежит.
8.7. Настоящие Правила определяют защитные меры по снижению рисков нарушения информационной безопасности при использовании Клиентом Системы «Интернет-Клиент».

9. Требования к программно-техническим средствам для электронного документооборота.

9.1. Банк предоставляет Клиенту следующие программные средства:
- Дистрибутив «ДБО BS-Client. Интернет Клиент»/Дистрибутив «ДБО **Digital2Go**. Интернет Клиент»
- Дистрибутив «eToken PKI Client»
- Дистрибутив «Панель управления Рутокен»
- Электронная документация по системе "Интернет - Клиент".

9.2. Требования к программно-техническим средствам (приобретаются Клиентом за собственный счет у третьих лиц):
- Персональный компьютер, поддерживающий работу текущей версии ИК или ноутбук;
- Антивирусная программа;
- Поддерживаемые ОС для стационарных компьютеров и ноутбуков:
  - Windows 7; 8 x86/x64; Windows 8.1 x86/x64; Windows 10
  - Windows Server 2008 x86, x64; 2008 R2; 2012; 2012 R2
- Браузеры:
  - Chrome.
  - Firefox
  - Интернет Explorer (IE 10-11)
  - Opera
  - Edge (Работу поддерживает в ограниченном объеме (недоступна подпись документов выданными ключами, только просмотр) по причине невозможности использования криптоплагина
  - Safari
- Наличие подключенного USB-интерфейса в персональном компьютере Клиента;
- Доступ в сеть Интернет;

9.3. Для работы Мобильного приложения необходимы смартфоны или планшеты с последней актуальной версией операционной системы Android или iOS.
9.4 Клиент обязуется не использовать в работе с Системой «Интернет-Клиент» нелицензионное программное обеспечение, и принимает на себя все неблагоприятные последствия неисполнения или ненадлежащего исполнения им обязанности по соблюдению данных требований.
9.5 Клиент обязуется поддерживать используемое программное обеспечение в актуальном состоянии, выполняя своевременную установку рекомендуемых поставщиком программного обеспечения обновлений и критичных исправлений.

10. Порядок разрешения разногласий при обмене ЭД в Системе «Интернет-Клиент».

10.1. Общие положения.

10.1.1. В данном разделе описан порядок разрешения спорных ситуаций между участниками Системы «Интернет-Клиент», связанных с подлинностью ЭД.
10.1.2. ЭД считается подлинным, если он был с одной стороны надлежащим образом оформлен, подписан и отослан, а с другой - получен, проверен и принят к исполнению по Системе «Интернет-Клиент» (в том числе с использованием Мобильного приложения).

Рассматриваются конфликтные ситуации трех типов:
1) Отказ Клиента от подписи ЭД;
2) Отказ Банка от факта получения ЭД;

3) Проверка подлинности ЭД.

10.1.3. В ходе разрешения конфликтной ситуации может возникать спор об актуальности используемой Ключевой информации между Клиентом и Банком. Ключ проверки ЭП считается актуальным и принадлежащим Клиенту, если он был зарегистрирован в Банке и в соответствии с Договором и Правилами, и действовал в момент, когда произошла конфликтная ситуация. В данном разделе описан также порядок разрешения спора об актуальности Ключ проверки ЭП Клиента.

10.1.4. Для рассмотрения спорных ситуаций по письменному заявлению одной из сторон создается экспертная комиссия. В заявлении должны быть указаны: название организации и ее банковские реквизиты; дата и номер ЭД, подлинность которого вызывает сомнения, или другие реквизиты, однозначно определяющие документ; предмет претензии. В комиссию со стороны Банка обязательно входят: Администратор ИБ и Администратор Банка. Комиссия состоит из 6 человек, ее членами являются в равном числе представители Банка и Клиента.

Замечание: до подачи заявления сторонам рекомендуется проверить, что причиной возникновения конфликтной ситуации не является нарушение целостности программного обеспечения.

10.1.5. Экспертная комиссия осуществляет свою работу в помещении Банка с использованием эталонной ПЭВМ (персональный компьютер, свободный от вирусов и программных закладок), эталонного программного обеспечения и ключевых носителей, участвующих в конфликтной ситуации сторон.

10.1.6. Эталонное оборудование и программное обеспечение предоставляется Банком.

10.1.7. Администратор Банка предоставляет:

- комплект программного обеспечения (операционная система, СЗИ) на машинном носителе информации;

- Ключ проверки ЭП пользователей, участвующих в конфликтной ситуации, на машинном носителе, для проверки подписей под электронными сообщениями, зарегистрированными в установленном порядке.

10.1.8. Клиент предоставляет свои электронные ключи на машинном носителе.

В присутствии членов экспертной комиссии Администратор Банка инсталлирует эталонное программное обеспечение на эталонную ПЭВМ, используя для этого комплекты инсталляционных носителей информации.

10.1.9. Экспертная комиссия убеждается в работоспособности компьютера и программного обеспечения.

10.1.10. Экспертная комиссия производит действия по разрешению конфликтной ситуации в соответствии с пунктом 10.2 настоящих Правил и принимает решение по вопросу подлинности ЭД.

10.1.11. Экспертная комиссия оформляет свое решение в виде акта, оформленного на бумаге и подписанного всеми членами экспертной комиссии.

10.1.12. Акт комиссии является окончательным и пересмотру не подлежит. Действия, вытекающие из него, являются обязательными для участников конфликтной ситуации.

10.1.13. Акт комиссии является основанием для предъявления претензий к лицам, виновным в возникновении конфликтной ситуации.

10.1.14. Акт комиссии может являться доказательством при дальнейшем разбирательстве конфликтной ситуации в судебных органах.

10.2. Порядок разрешения конфликтных ситуаций.

10.2.1. Отказ Клиента от подписи ЭД. Клиент утверждает, что принятый Банком ЭД не был отправлен или был отправлен, но позднее отозван, Банк отрицает это.

10.2.1.1. Убедиться, что ЭД действительно был принят в обработку. Если ЭД не был принят в обработку, прекратить рассмотрение конфликтной ситуации ввиду отсутствия предмета спора.

10.2.1.2. Получить от Банка копию спорного ЭД, заверенную Банком. В случае отказа Банка представить копию спорного ЭД конфликтная ситуация разрешается в пользу Клиента.

10.2.1.3. Проверить подписи Клиента ЭД в соответствии с разделом 10.2.4. настоящих Правил. Если подпись признается надлежащей, конфликтная ситуация разрешается в пользу Банка.

10.2.1.4. Если подпись надлежащая, а Клиент утверждает, что спорный ЭД был им отозван, Клиент предъявляет спорный ЭД, а также ЭД, свидетельствующий о факте отзыва спорного ЭД. При этом проверяется подпись ЭД, свидетельствующего о факте отзыва спорного ЭД, его принадлежность к спорному ЭД (а именно номер документа, реквизиты получателя, сумма документа) и сравнивается время выработки подписи спорного ЭД и ЭД, свидетельствующего о факте отзыва спорного ЭД. Если подпись под протоколом признается надлежащей, время обработки подписи, зафиксированное в ЭД, свидетельствующем о факте отзыва спорного ЭД, позднее времени обработки подписи спорного ЭД, но не позднее 17.00 часов, конфликтная ситуация разрешается в пользу Клиента.
10.2.1.5. В остальных случаях конфликтная ситуация разрешается в пользу Банка.
10.2.2. Отказ Банка от факта получения ЭД. Клиент утверждает, что посланный им ЭД был принят Банком, Банк отрицает это или утверждает, что данный ЭД был впоследствии отозван Клиентом.
10.2.2.1. Получить от Клиента спорный ЭД. В случае отказа Клиента предъявить спорный ЭД, прекратить рассмотрение конфликтной ситуации ввиду отсутствия предмета спора.
10.2.2.2. Проверить подпись Банка на ЭД в соответствии с разделом 10.2.4. Правил. Если подпись признается ненадлежащей, конфликтная ситуация разрешается в пользу Банка.
10.2.2.3. Если подпись признается надлежащей, Банк предъявляет полученный от Клиента ЭД, свидетельствующий о факте отзыва спорного ЭД. Клиентом проверяется соответствие ЭД, свидетельствующего о факте отзыва спорного ЭД, спорному ЭД. В случае несоответствия ЭД, свидетельствующего о факте отзыва спорного ЭД, спорному ЭД конфликтная ситуация разрешается в пользу Клиента. Если ЭД, свидетельствующий о факте отзыва спорного ЭД, соответствует спорному ЭД проверяются подписи Клиента этого ЭД в соответствии с разделом 10.2.4 Правил и сравнивается время выработки подписи ЭД, предъявленного Банком, и время выработки подписи спорного ЭД, предъявленного Клиентом. Если подпись ЭД, время обработки подписи ЭД, зафиксированное в документе, предъявленном Банком, позднее времени отработки подписи спорного ЭД, но не позднее 17.00 часов, конфликтная ситуация разрешается в пользу Банка.
10.2.2.4. В остальных случаях конфликтная ситуация разрешается в пользу Клиента.
10.2.3. Проверка подлинности ЭД. В данном разделе описана процедура разрешения конфликта, связанного с достоверностью принятого в проводку ЭД, т. е. его соответствие переданному Клиентом ЭД.
10.2.3.1. Получить от Банка копию принятого в обработку ЭД, заверенную Банком. В случае отказа Банка предъявить копию спорного ЭД, конфликтная ситуация разрешается в пользу Клиента.
10.2.3.2. Проверить соответствие содержания принятого ЭД переданному ЭД. В случае их полного совпадения конфликтная ситуация разрешается в пользу Банка.
10.2.3.3. В случае возникновения между сторонами конфликтной ситуации по факту приема Банком ЭД, получить от Клиента заверенную им копию спорного ЭД и соответствующий ему протокол. В случае его отказа предъявить спорный ЭД или протокол, конфликтная ситуация разрешается в пользу Банка.
10.2.3.4. Проверить подпись Банка на протоколе о приеме ЭД, предъявленного Клиентом, в соответствии с разделом 10.2.4 настоящих Правил. Если подпись ненадлежащая, конфликтная ситуация разрешается в пользу Банка.
10.2.3.5. Проверить соответствие протокола самому ЭД. В случае несоответствия протокола спорному ЭД, конфликтная ситуация разрешается в пользу Банка.
10.2.3.6. В остальных случаях конфликтная ситуация разрешается в пользу Клиента.
10.2.4. Порядок проверки корректности подписи ЭД. В данном разделе описана процедура проверки корректности ЭП на ЭД. Данная процедура используется при разрешении вопроса о подлинности ЭД или протоколов.
10.2.4.1. Произвести проверку соответствия файлов ключей проверки ЭП (сертификатов) Клиента, которые находятся у Клиента и в Банке в директории данного Клиента.
10.2.4.2. Проверить подпись на спорном ЭД, указанным стороной (с использованием ключа проверки ЭП Банка). Если подпись ненадлежащая, то принимается решение о некорректности подписи ЭД.
10.2.4.3. Если у одной из сторон возникают сомнения в принадлежности (актуальности) содержащегося ключа проверки ЭП, произвести процедуру разрешения конфликтной ситуации о

принадлежности (актуальности) ключа проверки ЭП в соответствии с разделом 10.2.5 настоящих Правил.

В случае, если ключ проверки ЭП признается не принадлежащим данной стороне, подпись ЭД признается ненадлежащей.

10.2.4.4. В остальных случаях принимается решение о надлежащей подписи ЭД.

10.2.5. Порядок проверки актуальности открытого ключа Клиента приведен в Таблице №1.

Таблица №1

Этап работы	Решение при положительном результате	Решение при отрицательном результате
Проверка действия ключей проверки ЭП (сертификатов) Клиента, предоставленных Банком на момент подписания спорного ЭД. Проверяется по дате отправки сообщения, распоряжению по Банку о дате ввода ключа в действие.	Ключ проверки ЭП Клиента действовал на момент подписания спорного ЭД. Далее выполняется 2 этап.	Ключ проверки ЭП Клиента не действовал на момент подписания спорного ЭД. Решение выносится в пользу Клиента.
Производится вывод на экран информации о ключе ЭП и сертификат ключа проверки ЭП Клиента.	Совпадение информации о ключе проверки ЭП и кодов сертификата ключа проверки ЭП в карточке регистрации и на экране компьютера. Решение выносится в пользу Банка.	Несовпадение информации о ключе проверки ЭП и кодов сертификата ключа проверки ЭП в карточке регистрации и на экране компьютера (не зарегистрирован или искажен файл ключа проверки ЭП Клиента у Банка). Решение выносится в пользу Клиента.

10.3. Порядок проведения работ по устранению причин возникновения конфликтной ситуации.

10.3.1. Если в результате выполнения работ по разбору конфликтной ситуации возникли подозрения о возможных несанкционированных действиях третьих лиц, в т.ч. некорректных или умышленных действиях персонала, имеющего доступ к программному и аппаратному обеспечению, на рабочем месте одной из сторон, а также в целях установления причин возникновения конфликтной ситуации и их устранения, данной стороной проводится соответствующее служебное расследование.

10.3.2. В этом случае создается внутренняя комиссия. Основными целями ее работы являются:

- установление причин возникновения конфликтных ситуаций;
- проверка на отсутствие специальных программных закладок, вирусных программ и других несанкционированных изменений программного и аппаратного обеспечения клиентского места, а именно выявление возможных несанкционированных действий на клиентском месте и установление причин, приведших к возможности несанкционированного доступа:
- проверка на отсутствие компрометации ключей;
- установление лиц, совершивших несанкционированные действия.

10.3.3. Комиссия проверяет:

- наличие, непрерывность и целостность протоколов регистрации событий систем телекоммуникаций, криптографической защиты и защиты от несанкционированного доступа и проводит их анализ и сопоставление между собой,
- условия эксплуатации программного обеспечения и клиентского места,
- наличие поддерживающих организационных мероприятий (ответственных должностных лиц, необходимых инструкций и правил, обеспечивающих выполнение требований эксплуатационной

документации на программное обеспечение и нормативных документов по защите) и их выполнение.
10.3.4. По результатам работы комиссии составляется протокол, отражающий выполнение требований Договора и Правил, по обеспечению безопасности на клиентском месте, результаты рассмотрения и анализа протоколов регистрации событий с выводами о возможных несанкционированных действиях и путях улучшения системы обеспечения безопасности работ. Выводы данного протокола доводятся до заинтересованных сторон.
10.3.5. При выявлении факта или подозрении в возможной компрометации секретных ключей подписи, проводится их экстренная смена.
10.3.6. При выявлении несанкционированных действий комиссией составляется план по устранению выявленных недостатков в системе безопасности, а также подготавливаются предложения по усилению мер и средств защиты.

11. Виды ЭД и требования по их оформлению.

11.1. Виды ЭД, направляемых Клиентом Банку:
- платежное поручение.
- служебная информация - запросы, сообщения и т.д. (сообщение в свободной форме).
- документы по валютному контролю (заявление на валютный перевод, поручения на покупку/продажу валюты, поручения на конверсию валюты, распоряжения на списание средств с транзитного валютного счета, обязательная продажа валюты, паспорта сделок по контрактам, паспорта сделок по кредитному договору, справка о валютных операциях, справка о подтверждающих документах, заявление на переоформление паспорта сделки, заявление о закрытии и/переводе паспорта сделки).

11.2. Виды ЭД, направляемых Банком Клиенту:
- выписка по счету за день.
- платежный документ (платежное поручение, банковский ордер, инкассовое поручение).
- служебная информация - запросы, сообщения и т.д. (сообщение в свободной форме).

11.3. Виды бумажных документов, используемых в дополнение к электронному документообороту между Банком и Клиентом:
- платежные ЭД Клиента, напечатанные в Банке, по которым выполнены операции (бумажные копии полученных ЭД, принятых к исполнению Банком);
- бумажные платежные документы, исполненные без использования Системы «Интернет-Клиент».

11.4. Требования по оформлению платежных ЭД:
11.4.1. Все ЭД должны содержать необходимые банковские реквизиты согласно требованиям действующего законодательства Российской Федерации, стандартам, принятым в банковской практике.
11.4.2. Все ЭД должны отвечать требованиям Системы «Интернет-Клиент», должны быть подписаны и зашифрованы Клиентом - пользователем системы «Интернет-Клиент», от которого поступает данный документ.

12. ПОРЯДОК ИНФОРМИРОВАНИЯ БАНКА КЛИЕНТОМ О КОМПРОМЕТАЦИИ КЛЮЧЕВОЙ ИНФОРМАЦИИ СИСТЕМЫ «ИНТЕРНЕТ-КЛИЕНТ».

12.1. В случае компрометации Ключевой информации либо если Клиент подозревает возможность возникновения подобных ситуаций, Клиент обязан незамедлительно уведомить об этом Банк по телефону. При обращении в Банк по телефону Клиент должен сообщить наименование Клиента, номер счета.
12.2. Уполномоченный сотрудник Банка перезванивает Клиенту на номер телефона, указанный в хранящемся в Банке досье Клиента.
12.3. Устное сообщение Клиента должно быть в обязательном порядке подтверждено письменным заявлением в течение одного рабочего дня после устного сообщения.

13. ОСОБЫЕ УСЛОВИЯ.

13.1. Банк имеет право направлять Клиенту по Системе «Интернет-Клиент», на номера мобильных телефонов и адреса электронной почты, представленные Клиентом Банку в рамках настоящих Правил, сообщения информационного и рекламного характера.
13.2. Банк имеет право проводить запись телефонных переговоров между уполномоченным сотрудником Банка и Клиентом.
13.3. Банк имеет право приостановить или прекратить использование Клиентом Системы «Интернет-Клиент» при нарушении Клиентом настоящих Правил и/или Договора.
13.4. Во всем, что прямо не предусмотрено настоящими Правилами и Приложениями к ним, Стороны руководствуются Договором, заключенным между Банком и Клиентом, а также действующим законодательством Российской Федерации.

Приложение №1
К Правилам работы системы
«Интернет-Клиент»
в ПАО «НИКО-БАНК»

Подлежит хранению в юр. деле №

В ПАО «НИКО-БАНК»

ЗАЯВЛЕНИЕ О ПРИСОЕДИНЕНИИ
К ОБЩИМ ПРАВИЛАМ КОМПЛЕКСНОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ
КОРПОРАТИВНЫХ КЛИЕНТОВ В ПАО «НИКО-БАНК»

_ V_ подается в целях подключения/отключения услуги к ранее открытому счету
____ подается в целях корректировки, изменения, дополнения ранее поданного заявления

Клиент	
Для юридических лиц: **полное и сокращенное наименование организации** ---------- ***Для физических лиц:*** **статус, фамилия, имя, отчество**	
ИНН Клиента	
ОГРН / ОГРНИП Клиента	
По законодательству Российской Федерации является	___ резидентом ___ нерезидентом

Клиент в соответствии со статьей 428 Гражданского кодекса Российской Федерации присоединяется к действующей редакции Общих правил комплексного банковского обслуживания корпоративных клиентов в ПАО «НИКО-БАНК» (далее, соответственно - Правила, Банк), путем подачи Банку Заявления о присоединении к Правилам (далее - Заявление). Клиент просит Банк рассматривать Заявление как оферту о заключении Договора комплексного банковского обслуживания (Далее-Договор) и совершить ее акцепт путем проставления Банком на Заявлении отметки об акцепте, и просит:

1. _ V__ Внести изменения в систему «Интернет-Клиент»

Клиент просит расторгнуть Соглашение об обмене электронными документами при осуществлении расчетов с использованием системы «Интернет-Клиент», заключенное между Клиентом и Банком ранее.

С даты подписания Клиентом настоящего Заявления о присоединении и заключения Договора комплексного банковского обслуживания Соглашение об обмене электронными документами при осуществлении расчетов с использованием системы «Интернет-Клиент», заключенное между Клиентом и Банком ранее, прекращает свое действие.

Дальнейшее использование системы «Интернет-Клиент» осуществляется Клиентом и Банком на основании Договора комплексного банковского обслуживания в соответствии с Общими правилами комплексного банковского обслуживания корпоративных клиентов в ПАО «НИКО-БАНК».

2. _V_ Подключить услугу «Сервис проверки компаний «Светофор» в Системе ДБО **___ Не подключать** **___ Отключить**	
Установить версию сервиса «Светофор»	**_V_** Режим **полной** версии сервиса **____** Режим **ограниченной** версии сервиса

Клиент подтверждает, что:

- ознакомился с Правилами, Порядками и Тарифами Банка, размещенными на Сайте Банка www.nico-bank.ru, понимает их текст, выражает свое согласие с ними и обязуется их выполнять;
- акцептованное Банком Заявление является документом, подтверждающим факт заключения Договора;
- обязуется знакомиться с Правилами, Порядками к Правилам и Тарифами Банка не реже, чем один раз в календарный месяц.
- уведомлен о том, что Банк вправе в одностороннем порядке вносить изменения и дополнения в Правила, Порядки к Правилам и Тарифы Банка в случаях и в порядке, установленных законодательством и Правилами, при условии уведомления Клиентов любым из способов, указанных в Правилах, не позднее, чем за 10 (Десять) календарных дней до вступления таких изменений/дополнений в силу.
- уведомлен относительно неприемлемости осуществления операций, обладающих признаками сомнительности, в соответствии с требованиями действующего законодательства в области противодействия легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма.

Настоящим Клиент подтверждает, что ознакомлен и согласен с Тарифами Банка.

_____ _____ _____

Должность руководителя, представителя по доверенности либо статус физического лица | *подпись* | *(фамилия, инициалы)*

М.П. « ____ »_____20___г.

Отметки Банка:

___ *Заявление принято. Личность подписавшего настоящее заявление удостоверена по документу, удостоверяющему личность. Подпись, проставленная в настоящем заявлении, соответствуют подписи, указанной в карточке с образцами подписей и оттиска печати Клиента.*

___ *Заявление получено по Системе «Интернет-Клиент». Заявление подписано электронной подписью, принадлежащей Клиенту.*

Сотрудник Банка: _____

(должность)

_____ _____ _____

(Фамилия, инициалы) | *(подпись)* | *(дата)*

Приложение 2
К Правилам работы системы
«Интернет-Клиент»
в ПАО «НИКО-БАНК»

АКТ
о вводе в эксплуатацию системы электронного документооборота

ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО «НОВЫЙ ИНВЕСТИЦИОННО-КОММЕРЧЕСКИЙ ОРЕНБУРГСКИЙ БАНК РАЗВИТИЯ ПРОМЫШЛЕННОСТИ», именуемый в дальнейшем «**Банк**», в лице _____, действующего на основании _____, с одной стороны, и

_____,
(Наименование организации)

именуемый в дальнейшем «**Клиент**», в лице _____,
действующего на основании
(Должность, Ф.И.О., уполномоченного представителя организации)

_____, с другой стороны и вместе именуемые **Стороны**, составили настоящий Акт о нижеследующем:

1. Банк предоставляет Клиенту следующие программные средства:
   - Дистрибутив «ДБО BS-Client. Интернет Клиент»/Дистрибутив «ДБО **Digital2Go**. Интернет Клиент»
   - Дистрибутив «eToken PKI Client»
   - Дистрибутив «Панель управления Рутокен»
   - Электронная документация по системе "Интернет - Клиент".
2. Банк и Клиент провели генерацию ключевой информации.
3. Клиент передал Банку в электронном виде ключи проверки ЭП и заполненные и заверенные подписью и печатью предприятия Акты признания открытого ключа (Сертификата).
4. Банк и Клиент провели пробные сеансы получения и передачи информации по Системе.
5. Банк провел ознакомительное обучение представителя Клиента эксплуатации системы.
6. Все платежные документы, переданные по Системе, в соответствии с условиями Соглашения приобретают юридическую силу с даты подписания настоящего Акта.

Настоящий Акт составлен в 2-х экземплярах по одному для каждой из сторон и является неотъемлемой частью договора комплексного банковского обслуживания в ПАО «НИКО-БАНК».

От Банка	От Клиента
_____/_____/	_____/_____/
М.П.	М.П
«____»_____20___г.	«____»_____20___г.

Приложение 3
К Правилам работы системы
«Интернет-Клиент»
в ПАО «НИКО-БАНК»

Рекомендации по обеспечению информационной безопасности при использовании системы «Интернет-Клиент».

Для обеспечения информационной безопасности при использовании системы дистанционного банковского обслуживания и сведению рисков мошенничества и, как следствие, финансовые потери к минимуму, необходимо быть предельно внимательными и следовать рекомендациям приведенным ниже.

Особенное внимание безопасности необходимо уделить тем клиентам с так называемым «домашним» компьютером, где выход в Интернет наиболее часто осуществляется без межсетевого экрана защиты и антивирусного программного обеспечения.

- Рекомендуется осуществлять работу в системе Дистанционного банковского обслуживания (ДБО) с использованием отдельной учетной записи в операционной системе компьютера, защищенной сложным паролем, известным только Вам. При возможности рекомендуется осуществлять доступ в ДБО с выделенного компьютера, используемого исключительно для работы с ДБО. Права пользователя в операционной системе компьютера должны быть минимально необходимыми, должна быть запрещена установка прикладного программного обеспечения за исключением необходимого для работы в ДБО. По возможности исключите посещение с данного компьютера сайтов сомнительного содержания и любых других потенциально опасных Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы и т.д.), а также чтение почты и открытие почтовых документов полученных из недостоверных источников;
- Соблюдайте правила безопасности при работе с ключевыми носителями:

- Необходимо сохранять в тайне закрытый (секретный) ключ электронной подписи. Не оставлять ключи в компьютере или на столе, если Вы покидаете свое рабочее место. По окончании работы ключи убирать в сейф. Не оставляйте без присмотра компьютер с активной ДБО;

- Уделите вопросу хранения ключей ДБО должное внимание. Помните, что наличие ключа позволяет заверить от Вашего имени документ и передать его на исполнение в Банк;

- Подключайте ключевой носитель к компьютеру только на время подписи документов. Не держите ключевые носители постоянно подключенными к компьютеру. Ни в коем случае не храните ключи на жестком диске компьютера;

- Постарайтесь внедрить использование для отправки документов двух подписей (2-х ключей);

- При компрометации или подозрения на компрометацию секретных ключей или компьютера, увольнения ответственного сотрудника или ИТ специалиста Вашей компании, который имел доступ к компьютеру или к секретным ключам, а также при истечении срока действия ключа с периодичностью, установленной договором на ДБО и правилами работы в системе незамедлительно сообщите в Банк для блокировки ключей и генерации новых.

- Рекомендуется избегать работы в ДБО с «недоверенных» компьютеров (в Интернет-кафе или другие общедоступные компьютеры, а так же «чужие» компьютеры временно используемые вами и т.п.). Крайне не желательно использование для работы в ДБО публичных беспроводных сетей (например, бесплатный Wi-Fi и т.п.);
- Соблюдайте правила безопасности при использовании паролей:

- Для работы в ДБО необходимо использовать только сложные пароли, удовлетворяющие следующим требованиям:

пароль должен иметь длину от 8 до 20 символов, в нем должно быть не менее двух цифр и двух букв, допускается использование букв латинского алфавита, цифр, знаков ! # $ % & ( ) * + - . / : ; < = > ? [\ .

пароль не должен содержать последовательности одинаковых символов и групп символов, легко угадываемые комбинации символов (dddddd, 333444555, qwerty, 12345, abc123 и т.п.)

пароль не должен содержать связанных с Вами данных (имена и даты рождения членов семьи, адреса, телефоны, часть номера вашей банковской карты и т.п.)

пароль не должен содержать словарных слов (passw0rd, football, shadow, sergey, natalia, русские слова, набранные в английской кодировке, например, Сергей – Cthutq).

пароль не должен совпадать с предыдущими паролями и не должен совпадать с именем входа.

пароль не должен быть копией или комбинаций паролей используемых Вами в других системах операционная система компьютера, электронная почта, развлекательный ресурсы в Интернет и т.п.);

- Никогда не сообщайте свой пароль третьим лицам, в том числе коллегам, родственникам и работникам Банка, вводите пароль только при работе в ДБО. Работник Банка не имеет права запрашивать у Вас пароль, даже если вы самостоятельно обратились в Банк. Вводите пароль только в ДБО, Банк никогда не отправляет сообщений с просьбой уточнить или предоставить пароль;

- Не записывайте свой пароль там, где доступ к нему могут получить третьи лица. Запрещается сохранять пароль на компьютере, мобильном устройстве, а так же на иных электронных носителях, доступ к которым могут получить третьи лица. Необходимо периодическое изменение пароля входа в систему.

- Рекомендуется постоянное использование системы антивирусного программного обеспечения (NOD32, AVP Kaspersky, Symantec AntiVirus и т.п.) на Ваших компьютерах. Необходимо использовать лицензионные программные продукты последних версий и постоянно обновлять антивирусные базы данных программных продуктов. Обновление антивирусных баз рекомендуется проводить в автоматическом режиме по мере их выпуска организацией-разработчиком. Необходимо обеспечить регулярные периодические проверки по поиску вирусов на автоматизированных рабочих местах используемых для ДБО.
- При поломке компьютера, с которого осуществляется работа по системе дистанционного банковского обслуживания, немедленно звоните в Банк и просите блокировать операции по системе;
- Остерегайтесь мошенничества:

- Банк никогда не связывается по телефону и не осуществляет рассылок сообщений по СМС или email с просьбой предоставить, подтвердить или уточнить Вашу личную информацию (пароли, логины, Ф.И.О., паспортные данные, номер мобильного телефона, на который приходят одноразовые пароли и другие личные данные). Не отвечайте на такие сообщения;

- При получении подозрительного сообщения якобы от имени Банка не отвечайте на него, не переходите по ссылкам указанным в подозрительном сообщении (даже если адрес похож на адрес сайта Банка). В сообщениях Банка никогда не будет просьбы зайти в ДБО по указанной в сообщении ссылке;

- При работе с ДБО обратите внимание на страницу входа и интерфейс, если вы заметите любые отличия, не заявленные ранее Банком, или возникнут иные причины для возникновения подозрений в том, что сайт поддельный, необходимо незамедлительно прекратить работу и обратиться в Банк по телефону техподдержки (никогда не связывайтесь по телефону указанному на подозрительной странице);

- Если вы самостоятельно связались с Банком, сотрудники могут уточнить у Вас персональную информацию, но не имеют права запрашивать у Вас пароль на вход в ДБО;

- Банк никогда не направляет сообщений о блокировке/разблокировке Вашей учетной записи в ДБО. Сотрудники Банка никогда не связываются по телефону, чтобы сообщить о недоступности ДБО вследствие проведения каких-либо регламентных работ. Если вы получили подозрительное сообщение от имени Банка, либо с Вами связались по телефону с одной из просьб, перечисленных в данном разделе, то рекомендуется сообщить о данном факте в Банк по телефону техподдержки (никогда не связывайтесь с Банком по телефону указанному в подозрительном сообщении);

- Обращайте внимание на появление подозрительной активности на Вашем компьютере, например, самопроизвольные движение курсора на экране, набор текста и т.п. Обращайте внимание на невозможность зайти на сайт ДБО, при том, что другие Интернет-сайты у Вас загружаются, а так же на невозможность войти в ДБО по причине несовпадения логина и пароля, при том, что они корректны. Обращайте внимание на «зависания» ДБО, при нормальной работе других Интернет сайтов. Данные факты могут свидетельствовать о заражении Вашего компьютера вредоносными

программами. Избегайте работы в ДБО с зараженных компьютеров, если на зараженном компьютере уже осуществлялась работа в ДБО, то незамедлительно заблокируйте Вашу учетную запись в ДБО. Вы можете сделать это, связавшись с Банком по телефону техподдержки.

- При эксплуатации средств защиты информации необходимо соблюдать рекомендации по обеспечению безопасности средств защиты информации.

В случае подозрения или обнаружения несанкционированного доступа в систему ДБО необходимо срочно позвонить в Банк, чтобы приостановить работу Вашей системы по следующим телефонам:

- с 8:00 – 19:30 по телефону 8 (3532) 34-90-90 – Служба технической поддержки;
- с 9:00 – 18:00 по телефону 8 (3532) 34-90-89 - Отдел по работе с юридическими лицами УКБ.