

ДОГОВОР о порядке использования системы «Клиент-Банк»

г. _____

«___» _____ 20__ г.

Банк «Йошкар-Ола» (публичное акционерное общество), именуемый в дальнейшем «Банк», в лице _____, действующей на основании _____, с одной стороны, и _____, именуемое в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой стороны (Банк и Клиент, упоминаемые одновременно, далее именуются «Стороны») заключили настоящий Договор о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА.

1.1. Предметом настоящего Договора является порядок приема и передачи документов в электронном виде с применением системы «Клиент-Банк».

2. ОСНОВНЫЕ ТЕРМИНЫ.

Для целей настоящего Договора используются следующие понятия:

2.1. **Система «Клиент-Банк»** – совокупность программно-аппаратных средств, устанавливаемых на территории Клиента и Банка, и согласовано эксплуатируемых Клиентом и Банком в соответствующих частях, а также организационных мероприятий, проводимых Клиентом и Банком, с целью предоставления Клиенту услуг по настоящему Договору.

2.2. **Аутентификация электронного сообщения** – процесс проверки сообщения, позволяющий установить, что сообщение исходит из указанного источника, и не было изменено при передаче.

2.3. **Код аутентификации электронного сообщения** – уникальная последовательность байт, формируемая Клиентом для аутентичности электронного документа. Код аутентификации (далее – КА) позволяет гарантированно удостовериться целостность электронного документа и идентифицировать его отправителя.

2.4. **Электронное сообщение** (далее – ЭС) – документ, обеспечивающий обмен информацией (запросы, отчеты, реестры, ведомости, выписки из счетов, Заявление о выдаче кредита, Срочное обязательство, Подтверждение, содержащее существенные условия депозитной сделки, и т.п.), при совершении расчетов и/или проведении операций по счету Клиента, являющийся основанием для совершения операций в том числе по счету(-ам) Клиента, подписанный (защищенный) соответствующими кодами аутентификации и имеющий равную юридическую силу с документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц Клиента и заверенными оттиском печати Клиента.

2.5. **АРМ Клиента** – совокупность аппаратных средств Клиента и программное обеспечение системы «Клиент-Банк», установленное на рабочем месте Клиента, предназначенное для подготовки и обработки отправляемых/получаемых ЭС.

2.6. **Кредитный договор** – Кредитный договор, Договор об открытии кредитной линии, Договор об открытии невозобновляемой кредитной линии, заключенный Клиентом с Банком.

2.7. **Заявление о выдаче кредита** – документ, на основании которого осуществляется предоставление Банком Клиенту кредита (текущего кредита (транша) в рамках заключенного Кредитного договора.

2.8. **Срочное обязательство** - документ, которым оформляются сроки и размер платежа по кредиту (текущему кредиту (траншу), получаемому Клиентом в рамках заключенного Кредитного договора.

2.9. **Персональный платежный лимит** – ограничение суммы денежных средств установленное клиентом, в пределах которого, могут быть осуществлены операции по банковскому счету клиента.

3. ОБЩИЕ УСЛОВИЯ ДОГОВОРА.

3.1. В соответствии с условиями настоящего Договора при использовании системы «Клиент-Банк» предусматривается прием и передача в электронном виде документов, связанных с:

- проведением операций по счету Клиента в Банке согласно договору банковского счета;
- передачей Клиенту информации о платежах физических лиц принятых Банком в его пользу;
- подписанием Заявления о выдаче кредита и Срочного обязательства, предоставлением Клиенту кредитов (текущих кредитов (траншей) по Кредитному договору, направлением писем, претензий и иной корреспонденции по Кредитному договору;
- осуществлением Клиентом платежей в погашение кредитных обязательств перед Банком;
- совершением депозитной сделки.

Электронные сообщения пересылаются по системе «Клиент-Банк» и исполняются без их представления на бумажном носителе. При этом стороны признают, что получение ЭС, заверенных КА, юридически равнозначно получению соответствующих документов на бумажном носителе (независимо от того, существуют такие документы на бумажном носителе или нет), заверенных печатью и подписью единоличного исполнительного органа (управляющего, руководителя управляющей организации).

3.2. В целях обмена ЭС, в том числе для совершения операций по счетам клиентов, Стороны используют разработанную Банком «Йошкар-Ола» (ПАО) систему «Клиент-Банк». Владельцем исключительных прав на программный продукт АРМ Клиента является Банк. Банк гарантирует, что владеет и пользуется программным обеспечением на законных основаниях и имеет право передавать его третьим лицам. В качестве средства обмена информацией и ЭС Клиент использует телекоммуникационные каналы связи или сеть Интернет.

3.3. Банк предоставляет Клиенту программную часть системы «Клиент-Банк», оказывает Клиенту помощь в установке системы «Клиент-Банк» и обучает персонал Клиента работе с ней. Банк оказывает консультативную помощь Клиенту по всем вопросам работы с системой на протяжении срока действия настоящего Договора.

3.4. Стороны обязаны за собственный счет поддерживать в рабочем состоянии свои программно-технические средства, используемые при передаче электронных сообщений и информации в соответствии с настоящим Договором.

3.5. Стороны обязуются обеспечивать конфиденциальность информации, передаваемой и получаемой по системе «Клиент-Банк».

3.6. Стороны несут ответственность за действия лиц, имеющих доступ к системам передачи информации в рамках настоящего Договора.

3.7. При возникновении в процессе эксплуатации программных и технических средств неполадок, сбоев и других проблем Клиент информирует об этом Банк в письменной форме. В случае невозможности оперативного устранения указанных неполадок обмен документами между Сторонами осуществляется на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц Клиента и заверенными оттиском печати Клиента.

3.8. К настоящему Договору прилагается «Регламент использования АРМ «Клиента» (Приложение №1), который является неотъемлемой частью настоящего Договора.

«Регламент использования АРМ «Клиента» определяет:

- общие требования обеспечения информационной безопасности при обработке и обмене электронными сообщениями между Банком и Клиентом;
- спецификацию (рекомендуемую конфигурацию) АРМ Клиента;
- требования к организации парольной защиты АРМ Клиента;
- требования к организации антивирусной защиты АРМ Клиента;
- порядок установки системы «Клиент-Банк» и порядок обмена КА;
- порядок обмена электронными сообщениями;
- действия в случае компрометации КА.

4. ПРАВА И ОБЯЗАННОСТИ БАНКА.

4.1. Банк обязан по требованию Клиента блокировать в системе «Клиент-Банк» существующие активные КА Клиента и зарегистрировать новые КА Клиента.

4.2. Банк обязан по телефонному звонку Клиента после произношения Клиентом кодового слова, впредь до письменного уведомления, временно блокировать работу Клиента в системе «Клиент-Банк».

4.3. Банк обязуется осуществлять обработку и исполнение ЭС полученных до 16 часов 00 минут по Московскому времени в рабочие дни текущим операционным днем. ЭС, полученные Банком, после 16 часов 00 минут Московского времени или в нерабочее время, обрабатываются Банком на следующий рабочий день.

4.4. После получения ЭС Банк проверяет его, оперативно устанавливает и обновляет статус каждого ЭС в соответствии с текущим состоянием процесса обработки ЭС. По каждому ЭС Клиента, сформированному средствами системы «Клиент-Банк», с корректными КА, Банк направляет по системе «Клиент-Банк» уведомление о результатах его обработки путем изменения информации о документе, доступной Клиенту, в виде изменения статуса этого документа, либо сообщение об отказе исполнения ЭС с указанием причины.

4.5. Банк не исполняет запросы на изменение или удаление ранее переданного ЭС, если этот ЭС имеет статус «На исполнении»/«Исполнен».

4.6. Банк обязуется выдавать Клиенту в электронном виде выписку с банковского счета, содержащую все операции, проведенные по счету в течение дня, а также суммы входящего и исходящего остатков по счету в течение дня.

4.7. Банк обязуется уведомлять Клиента о поступивших распоряжениях о переводе денежных средств по системе «Клиент-Банк» посредством установки соответствующего статуса документа и сообщения о принятии распоряжения к исполнению в системе «Клиент-Банк». Банк обязуется уведомлять Клиента о поступивших распоряжениях о переводе денежных средств путем направления СМС-сообщения на номер мобильного телефона, указанный Клиентом в заявлении на подключение услуги СМС-информирования. В случае отсутствия возражений от Клиента о переводе денежных средств в течение 30 минут, Банк исполняет распоряжение.

4.8. При установлении клиентом Персонального платежного лимита Банк обязуется перед отправкой поступивших распоряжений о переводе денежных средств по системе «Клиент-Банк» на исполнение осуществлять контроль суммы ЭС на предмет соответствия персональному платежному лимиту. Не прошедшие контроль ЭС не принимаются Банком к исполнению. О непринятии к исполнению ЭС Клиенту направляется сообщение с указанием даты и причины отказа в обработке ЭС - превышение персонального платежного лимита. Уведомление направляется не позднее окончания операционного дня. Клиент может отказаться от ранее установленного Персонального платежного лимита.

4.9. При подключении услуги СМС-подтверждение Банк обязуется перед отправкой поступивших распоряжений о переводе денежных средств по системе «Клиент-Банк» на исполнение запрашивать дополнительное подтверждение распоряжений в форме одноразового пароля на номер указанного в заявлении мобильного телефона. Клиент может отказаться от ранее подключенной услуги СМС-подтверждения заполнив заявление на отключение услуги СМС-подтверждение в системе «Клиент-Банк».

4.10. Банк обязуется информировать Клиента о совершенных по его счету операциях, а также о возвращении (аннулировании) распоряжений, путем направления соответствующих сообщений в системе «Клиент-Банк». Банк подтверждает исполнение распоряжений, переданных по Системе «Клиент-Банк», путем проставления штампа Банка об исполнении с указанием даты и Ф.И.О. ответственного исполнителя Банка на распечатанной копии электронного документа.

4.11. Банк обязуется в соответствии с п. 3.6 ст. 8 Федерального закона № 161-ФЗ информировать Клиента:

- о приостановлении приема к исполнению распоряжения Клиента на два дня в случае выявления им операции, соответствующей признакам осуществления перевода денежных средств без добровольного согласия клиента;

- о рекомендациях по снижению рисков повторного осуществления перевода денежных средств без добровольного согласия клиента;

- о возможности Клиента подтвердить распоряжение не позднее одного дня, следующего за днем приостановления Банком приема к исполнению указанного распоряжения или о возможности совершения Клиентом повторной операции, содержащей те же реквизиты получателя (плательщика) и ту же сумму перевода (далее - повторная операция).

4.12. Банк обязуется направлять информацию обо всех случаях и (или) попытках осуществления переводов денежных средств без добровольного согласия клиента в соответствии с Указанием Банка России от 19.08.2024 № 6828-У «О порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами электронных платформ в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без добровольного согласия клиента, форме и порядке получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, порядке запроса и получения Банком России у них информации о переводах денежных средств, связанных с переводами денежных средств без добровольного согласия клиента, в отношении которых от федерального органа исполнительной власти в сфере внутренних дел получены сведения о совершенных противоправных действиях в соответствии с частью 8 статьи 27 Федерального закона № 161-ФЗ, а также о порядке реализации ими мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия клиента».

4.13. Банк имеет право изменять формат электронных документов, передаваемых по системе «Клиент-Банк», с предварительным уведомлением об этом Клиента за три рабочих дня до предполагаемой даты введения в действие нового формата.

4.14. Банк имеет право производить замену подсистем обработки, хранения, защиты и передачи информации системы «Клиент-Банк» без согласия Клиента. Банк обязан уведомить об этом Клиента не менее чем за 10 календарных дней, а Клиент обязан в соответствующий срок получить у Банка или приобрести за свой счет и ввести в эксплуатацию необходимые программно-технические средства.

4.15. Банк имеет право приостанавливать работу Клиента в системе «Клиент-Банк» в случае:

- нарушений со стороны Клиента «Регламента использования АРМ «Клиента»;
- приостановления операций по счету в случаях, предусмотренных законодательством Российской Федерации;
- наложения ареста на денежные средства, находящиеся на счете Клиента;
- образования картотеки распоряжений, не исполненных в срок из-за отсутствия или недостаточности денежных средств на счете клиента;
- выявления в деятельности Клиента случаев и (или) попыток осуществления переводов денежных средств без согласия Клиента;
- выявления совпадений в операциях Клиента с полученной Банком от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента;
- нарушений со стороны Клиента «Регламента использования АРМ «Клиента».

4.16. В случае отсутствия оборотов по счету Клиента более одного года Банк имеет право отключить Клиента от системы «Клиент-Банк» и расторгнуть договор в одностороннем порядке. Банк обязан уведомить об этом Клиента не менее чем за 10 календарных дней.

4.17. В случаях компьютерных вирусных или аналогичных угроз Банк вправе приостановить обслуживание системы «Клиент-Банк» с уведомлением Клиента по контактному телефону о вирусном инциденте и возобновить работу после уведомления Клиента о ликвидации вирусного инцидента.

4.18. Банк не несет ответственности за убытки, понесенные Клиентом, которые явились следствием:

- допуска к АРМ Клиента лиц, не являющихся ответственными за его обслуживание;
- несанкционированного доступа к АРМ Клиента;

- несоблюдения «Регламента использования АРМ «Клиента».

4.19. Обо всех случаях приостановления работы Клиента в системе «Клиент-Банк» Банк обязан информировать Клиента в течение одного банковского дня путем передачи уведомления по Системе «Клиент-Банк».

4.20. При наличии сбоев в передаче электронной информации, возникших в результате неисправности линий связи, отключения или перебоев в линиях электропитания, неисправности аппаратных средств Сторон, а также в случаях, предусмотренных пунктом 4.11 настоящего Договора, обмен документами осуществляется в порядке, предусмотренном пунктом 3.7 настоящего Договора.

5. ПРАВА И ОБЯЗАННОСТИ КЛИЕНТА.

5.1. Клиент обязан выделить и оборудовать рабочее место для установки АРМ Клиента в соответствии с техническими требованиями, указанными в разделе 3 «Регламента использования АРМ «Клиента».

5.2. Клиент обязан допускать к эксплуатации системы «Клиент-Банк» только сотрудников, имеющих соответствующую подготовку, и в своей работе руководствоваться «Регламентом использования АРМ «Клиента».

5.3. Клиент обязан обеспечивать сохранность и целостность программного комплекса системы «Клиент-Банк», сохранять конфиденциальность и подлинность КА, хранить в секрете и не передавать третьим лицам пароль и КА Клиента, используемые в системе «Клиент-Банк».

5.4. Клиент обязан незамедлительно уведомить Банк обо всех случаях компрометации КА и об обнаружении попытки несанкционированного доступа к системе «Клиент-Банк».

5.5. Клиент обязан формировать электронные сообщения в системе «Клиент-Банк» и направлять их в Банк в соответствии с графиком обслуживания клиентов.

Клиент обязан контролировать доставку электронных сообщений в Банк и результаты их обработки, контролировать соответствие суммы платежа и остатка на начало операционного дня на своем счете в Банке и осуществлять платежи только в пределах этого остатка, за исключением случаев предоставления Банком овердрафта по счету Клиента, условия которого определяются отдельным договором.

В случае установления расхождений Клиент обязан извещать Банк до 10:00 часов следующего рабочего дня об отрицательных результатах выверки. Неполучение Банком от Клиента извещения об отрицательных результатах выверки в указанный срок является подтверждением Клиентом правильности исполнения электронного документа.

5.6. Клиент обязан по требованию Банка сгенерировать новые КА Клиента и зарегистрировать новый КА Клиента в Банке.

5.7. Клиент обязан не вносить какие-либо изменения в установленное у него программное обеспечение системы «Клиент-Банк», а также не устанавливать, не продавать, не сдавать в аренду и не передавать третьим лицам данное программное обеспечение.

5.8. Клиент обязан хранить сообщения, заверенные КА, в течение срока, установленного действующим законодательством РФ и нормативными актами Банка России, но не менее 5 лет.

5.9. Клиент имеет право уведомить Банк о направленном распоряжении и (или) о временном блокировании в системе «Клиент-Банк» по телефону с произношением кодового слова в порядке, предусмотренном «Регламентом использования АРМ «Клиента».

5.9.1. При использовании системы «Клиент-Банк» без согласия клиента Клиент обязан направить в Банк уведомление о неправомерном использовании системы «Клиент-Банк» в письменном виде незамедлительно после обнаружения факта утраты электронного средства платежа и (или) его использования без согласия клиента после получения от Банка уведомления в соответствии с пунктом 4.7 настоящего Договора. На уведомлении о неправомерном использовании системы «Клиент-Банк» сотрудником Банка указывается дата и время получения уведомления.

5.10. Клиент обязан незамедлительно уведомить Банк об изменении по любым основаниям ранее предоставленных Банку номеров телефонов.

5.11. Клиент имеет право отказаться от получения СМС-сообщений, предусмотренных п. 4.7 настоящего Договора. Отказ должен быть оформлен в письменном виде и представлен в Банк.

5.12. Клиент имеет право отказаться от услуги СМС-подтверждение, предусмотренной п. 4.8 настоящего Договора. Отказ должен быть оформлен в письменном виде и представлен в Банк.

5.13. Клиент имеет право досрочно прекратить действие своих КА, потребовать от Банка заблокировать эти КА, генерировать новые КА с последующей регистрацией в Банке.

5.14. Клиент имеет право представить Банку информацию о подтверждении распоряжения Клиента или совершить повторную операцию в случае приостановления Банком приема к исполнению распоряжения Клиента в соответствии с п. 3.4 ст. 8 Федерального закона № 161-ФЗ.

6. ПОРЯДОК ОПЛАТЫ УСЛУГ.

6.1. Клиент обязуется оплатить установку Системы в день оказания услуги в размере, установленном Тарифами по рублевому расчетно-кассовому обслуживанию юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся частной практикой (адвокатов, нотариусов) в головном офисе и в дополнительных офисах Банка «Йошкар-Ола» (ПАО) (далее - Тарифы Банка).

6.2. В случае повторной установки Системы по требованию Клиента, Клиент оплачивает повторную установку системы «Клиент-Банк» в размере, установленном Тарифами Банка.

6.3. Доступ в Систему предоставляется Клиенту после оплаты им услуг Банка в порядке, предусмотренном настоящим разделом.

6.4. Если у Клиента нет действующего банковского счета, открытого в Банке, комиссия оплачивается Клиентом в течение 10 рабочих дней с момента предъявления Банком счета на оплату.

6.5. Размер и порядок удержания комиссионного вознаграждения за пользование Системой устанавливаются Тарифами Банка.

6.6. Банк имеет право в одностороннем порядке вводить новые Тарифы, вносить изменения в действующие Тарифы Банка, устанавливать и изменять порядок обслуживания Клиента. Информация об изменении Тарифов Банка и условиях обслуживания доводится до Клиента путем размещения соответствующих уведомлений в подразделениях Банка, на официальном сайте Банка www.olabank.ru, оповещения Клиента через Систему, а также иными способами по выбору Банка не позднее, чем за 10 (десять) рабочих дней до даты их фактического вступления в силу.

6.7. Оплата услуг за обслуживание в Системе, указанных в Тарифах Банка, производится путем списания денежных средств с банковского счета Клиента на условиях заранее данного акцепта. Клиент дает акцепт Банку на списание денежных средств с банковского счета Клиента за установку (повторную установку) системы «Клиент-Банк» (заранее данный акцепт).

7. ОТВЕТСТВЕННОСТЬ СТОРОН.

7.1. За неисполнение или ненадлежащее исполнение обязательств по настоящему Договору Стороны несут ответственность в соответствии с действующим законодательством РФ.

7.2. Сторона не несет ответственности за убытки, возникшие вследствие разглашения другой Стороной КА третьим лицам, вне зависимости от причин.

7.3. Банк не несет ответственности за частичное или полное невыполнение обязательств по исполнению Клиентом «Регламента использования АРМ «Клиента».

7.4. Банк не несет ответственности за правомерность и правильность надлежащим образом оформленного Клиентом ЭС, а также за убытки, понесенные Клиентом вследствие отказов и несвоевременных действий лиц, в пользу которых осуществляется расчетная операция по поручению Клиента.

7.5. Банк не несет ответственности за неполадки и сбои, возникающие в процессе эксплуатации программных и технических средств в результате неисправности линий связи, отключения или перебоев в линиях электропитания, неисправности, возникшие ввиду несовместимости аппаратных, электронно-информационных средств и систем, используемых Клиентом и т.д.

8. ФОРС-МАЖОР.

8.1. Стороны освобождаются от ответственности за полное или частичное неисполнение каких-либо обязательств, вытекающих из условий настоящего Договора, если это неисполнение явилось следствием возникших после его заключения обстоятельств непреодолимой силы, которые стороны не могли ни предвидеть, ни предотвратить своими силами.

8.2. К обстоятельствам непреодолимой силы относятся события, на которые Сторона не может оказывать влияния и за возникновение которых не несет ответственности, например: наводнение, пожар, землетрясение, другие стихийные бедствия, повреждения линий связи, забастовки, состояние войны, правительственные постановления или распоряжения государственных органов, препятствующие выполнению условий настоящего Договора.

8.3. Срок исполнения обязательств по настоящему Договору переносится соразмерно времени, в течение которого такие обстоятельства будут действовать.

8.4. Если указанные обстоятельства будут продолжаться более 30 календарных дней, то каждая из сторон имеет право отказаться от дальнейшего исполнения обязательств по настоящему Договору, и в этом случае ни одна из сторон не будет иметь права на возмещение возможных убытков.

8.5. Сторона, у которой возникли обстоятельства непреодолимой силы, должна в письменной форме сообщить другой Стороне о наступлении и прекращении таких обстоятельств.

9. ПОРЯДОК РАССМОТРЕНИЯ СПОРОВ.

9.1. В случае возникновения между Сторонами споров и конфликтных ситуаций по поводу авторства и подлинности ЭС создается экспертная комиссия, которая проводит их рассмотрение и разрешение.

9.2. Оспаривающая Сторона направляет другой Стороне обоснованную претензию в письменном виде. Другая Сторона рассматривает и дает ответ на претензию в письменном виде в течение 10 дней со дня получения претензии.

В ответе на претензию указываются по два представителя Стороны - члены экспертной комиссии.

9.3. Экспертная комиссия создается Сторонами в течение 3 рабочих дней со дня получения оспаривающей Стороной ответа на претензию с отказом в ее признании. Оспаривающая Сторона обязана в трехдневный срок уведомить о своих двух представителях - членах экспертной комиссии.

9.4. Экспертная комиссия состоит из четырех членов (по два представителя от каждой стороны).

Члены комиссии в течение 2 рабочих дней со дня ее создания избирают из своего состава председателя экспертной комиссии.

9.5. Стороны обязаны в течение 2 рабочих дней со дня утверждения председателя экспертной комиссии представить комиссии необходимые материалы.

9.6. Экспертная комиссия проводит рассмотрение споров и конфликтных ситуаций с использованием эталонных программно-технических средств и принимает решение в течение 3 рабочих дней со дня представления Сторонами необходимых материалов.

9.7. Решение экспертной комиссии принимается единогласно в письменном виде и подписывается всеми членами комиссии.

9.8. Стороны признают решения экспертной комиссии окончательными и обязуются действовать в соответствии с ними. Срок исполнения решения экспертной комиссии - 3 рабочих дня с момента вынесения решения.

9.9. В случае возникновения разногласий между членами комиссии при принятии решения комиссией составляется заключение с подробным изложением мнений членов комиссии, после чего Стороны действуют в порядке, установленном п. 9.10 настоящего Договора.

9.10. В случае неисполнения решения экспертной комиссии, а также, если возникшие по настоящему Договору разногласия между Сторонами не удалось урегулировать путем переговоров и с помощью экспертной комиссии, споры подлежат рассмотрению в Арбитражном суде Республики Марий Эл.

9.11. При разрешении споров и конфликтных ситуаций Стороны руководствуются действующим законодательством РФ.

10. СРОК ДЕЙСТВИЯ И ПОРЯДОК РАСТОРЖЕНИЯ ДОГОВОРА.

10.1. Настоящий Договор заключается на неопределенный срок и вступает в силу с момента его подписания Сторонами. Договор составлен в двух экземплярах, причем оба экземпляра имеют одинаковую юридическую силу.

10.2. Все изменения и дополнения к настоящему Договору действительны лишь в том случае, если они совершены в письменной форме, подписаны уполномоченными на то лицами сторон и являются его неотъемлемой частью.

10.3. Стороны вправе расторгнуть настоящий Договор в одностороннем порядке. Сторона, изъявившая желание расторгнуть Договор, обязана выполнить перед другой Стороной все обязательства, вытекающие из условий настоящего Договора, после чего направляет другой Стороне письменное уведомление о своем намерении расторгнуть Договор. Договор считается расторгнутым по истечении одного месяца с даты получения Стороной вышеуказанного уведомления, при условии отсутствия у нее претензий к Стороне, направившей уведомление.

11. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ.

11.1. К настоящему Договору прилагается «Регламент использования АРМ «Клиента», который является неотъемлемой частью настоящего Договора.

12. ЮРИДИЧЕСКИЕ АДРЕСА, ПЛАТЕЖНЫЕ РЕКВИЗИТЫ И ПОДПИСИ СТОРОН.

БАНК	КЛИЕНТ
Банк «Йошкар-Ола» (ПАО)	
424006, Республика Марий Эл, г. Йошкар-Ола, ул. Панфилова, д.39г к/с 30101810845372202906 в ОКЦ № 1 Волго-Вятского ГУ Банка России, БИК 042202906, ИНН 1215059221.	Адрес: р/с ИНН/КПП
_____	_____
М.П.	М.П.

РЕГЛАМЕНТ ИСПОЛЬЗОВАНИЯ АРМ «КЛИЕНТА» для клиентов Банка «Йошкар-Ола» (ПАО) при обработке и обмене электронными сообщениями.

1. ОБЩИЕ ПОЛОЖЕНИЯ.

- 1.1. Настоящий Регламент использования АРМ Клиента разработан с целью обеспечения информационной безопасности при обработке и обмене электронными сообщениями между Банком «Йошкар-Ола» (ПАО) и Клиентами.
- 1.2. Регламент разработан в соответствии с требованиями Положения Банка России от 24.09.2020 № 732-П «О платежной системе Банка России» и Положения Банка России от 17.08.2023 № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».
- 1.3. Подготовленная клиентами платежная информация, на основании которой совершаются расчетные, учетные и кассовые операции, предназначена для внутреннего использования в организации и может быть передана иным организациям только в соответствии с действующим законодательством РФ.
- 1.4. Указанная информация относится к категории строгой отчетности. Ограничительные пометки (грифы) «Для служебного пользования», «Конфиденциально» или «Банковская тайна» на документы, содержащие данную информацию, не проставляются.
- 1.5. Безопасность информации, отнесенной к банковской тайне, обеспечивается в соответствии со статьей 26 Федерального закона от 02.12.1990 № 395-1 «О банках и банковской деятельности».
- 1.6. Стороны признают в качестве единой шкалы времени при работе с системой «Клиент-Банк» Московское поясное время.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

Для целей настоящего Регламента используются следующие понятия:

- 2.1. **Автоматизированная банковская система (далее АБС)** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая банковскую информационную технологию.
- 2.2. **Аутентификация электронного сообщения** – процесс проверки сообщения, позволяющий установить, что сообщение исходит из указанного источника и не было изменено при передаче.
- 2.3. **Код аутентификации электронного сообщения** – уникальная последовательность байт, формируемая Клиентом для аутентичности электронного документа. Код аутентификации (далее КА) позволяет гарантированно удостовериться целостность электронного документа и аутентифицировать его отправителя.
- 2.4. **Корректный КА** – код аутентификации документа Клиента, сформированный с использованием секретного ключа Клиента, дающий положительный результат ее проверки с открытым ключом Клиента.
- 2.5. **Секретный код Клиента** – код (последовательность байт), генерируемый Клиентом с использованием средств системы «Клиент-Банк», и предназначенный для формирования Клиентом кода аутентификации электронных документов.
- 2.6. **Открытый код Клиента** – код (последовательность байт), зависящий от секретного кода Клиента, генерируемый Клиентом с использованием средств системы «Клиент-Банк», и предназначенный для проверки Банком корректности электронных документов, сформированных Клиентом.
- 2.7. **Сертификат открытого кода КА Клиента** – бумажный документ с представленным в шестнадцатеричном виде открытым кодом Клиента, датой начала и окончания действия

открытого кода Клиента, заверенный подписью руководителя и имеющий оттиск печати клиента.

2.8. **Активный открытый код КА Клиента** – открытый код КА Клиента, зарегистрированный Банком в системе «Клиент-Банк», и используемый Клиентом в текущее время для работы в системе «Клиент-Банк».

2.9. **Компрометация кода** – несанкционированный доступ посторонних лиц к секретному коду.

2.10. **Блокировочное слово** – уникальное слово, определяемое Клиентом при регистрации в системе «Клиент-Банк», для блокирования работы системы «Клиент-Банк» по телефонному звонку в Банк.

2.11. **Код активации** – последовательность символов, формируемая при первом запуске системы «Клиент-Банк», необходимый для активации Банком системы «Клиент-Банк».

2.12. **Регистрационный код** – файл, формируемый Банком на основе Кода активации, переданного Клиентом Банку, необходимый для запуска системы «Клиент-Банк».

3. СПЕЦИФИКАЦИЯ НА РАБОЧЕЕ МЕСТО АРМ КЛИЕНТА.

3.1. Характеристики компьютера (далее ПЭВМ) необходимые для полноценной работы АРМ Клиента:

- операционная система: Windows7, Windows8, Windows10, Windows11;
- лицензионные средства антивирусной защиты;
- подключение к сети Интернет.

3.2. На данной ПЭВМ должен проводиться ежедневный антивирусный контроль установленного программного обеспечения и обеспечиваться возможность автоматического регулярного обновления антивирусных баз.

3.3. Порядок доступа в помещения, технологический процесс обработки и обмена ЭС с использованием средств защиты информации должен быть регламентирован и обеспечен инструктивными и методическими материалами организацией, использующей АРМ Клиента.

3.4. Для обеспечения защиты указанных помещений должны быть реализованы следующие меры:

- на входные двери должны быть установлены замки, гарантирующие надежную защиту помещений в нерабочее время, а для контроля за входом в помещения должны быть установлены автоматические замки (электронные, кодовые и т.п.) или другие средства современных систем контроля и регистрации доступа;
- помещения должны быть оборудованы сигнализацией и по окончании рабочего дня опечатываться и сдаваться под охрану.

4. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ АРМ КЛИЕНТА.

4.1. У Клиента должен быть разработан комплекс мер, обеспечивающих управление парольной защитой АРМ Клиента. Должен быть определен порядок формирования и смены паролей.

4.2. Личные пароли должны выбираться пользователями автоматизированной системы самостоятельно, с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@ # \$ & * % и т.п.);
- пароль не должен включать в себя легковычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения;
- при смене пароля новое значение должно отличаться от предыдущего не менее, чем в 6 позициях.

4.3. Личный пароль пользователь не имеет права сообщать никому.

4.4. Владельцы паролей должны быть ознакомлены под роспись с требованиями к структуре паролей и предупреждены об ответственности за использование паролей, несоответствующих данным требованиям, а также за разглашение парольной информации.

4.5. Полная плановая смена паролей входа на ПЭВМ, локальную вычислительную сеть (далее - ЛВС) должна проводиться регулярно, не реже одного раза в квартал.

4.6. Внеплановая смена (удаление) личного пароля любого пользователя

автоматизированной системы в случае прекращения его полномочий (увольнение, либо переход на другую работу внутри участка системы электронных расчетов) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.

4.7. Внеплановая смена паролей всех пользователей должна проводиться в случае прекращения полномочий (увольнении, переход на другую работу внутри организации и другие обстоятельства) администраторов информационной безопасности и других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению автоматизированной системой, либо полномочия по управлению подсистемой защиты информации данной автоматизированной системы, а значит, кроме личного пароля им, могли быть известны пароли других пользователей системы.

4.8. В случае компрометации личного пароля хотя бы одного пользователя автоматизированной системы должны быть немедленно приняты меры в соответствии с п. 4.6 или п. 4.7 настоящего Регламента в зависимости от полномочий владельца скомпрометированного пароля.

5. ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ.

5.1. В организации должны применяться только официально приобретенные средства антивирусной защиты. Установка и регулярное обновление средств антивирусной защиты на автоматизированных рабочих местах и серверах должны осуществляться администраторами безопасности организации.

Лучшей практикой является автоматическая установка обновлений антивирусного программного обеспечения.

5.2. При обеспечении антивирусной защиты в организации должны быть разработаны и введены в действие инструкции по антивирусной защите. Особое внимание должно быть уделено антивирусной фильтрации интернет трафика.

Лучшей практикой является построение эшелонированной централизованной системы антивирусной защиты, предусматривающей использование средств антивирусной защиты различных производителей и их отдельную установку на рабочих станциях, серверах и межсетевых экранах.

5.3. В ПЭВМ и ЛВС не допускается присутствие и использование программного обеспечения и данных, не связанных с выполнением конкретных технологических процессов организации.

5.4. Устанавливаемое или изменяемое программное обеспечение должно быть предварительно проверено на отсутствие вирусов. После установки или изменении программного обеспечения должна быть выполнена антивирусная проверка.

5.5. При обнаружении компьютерного вируса необходимо принять меры по устранению последствий вирусной атаки, проинформировать руководство и приостановить при необходимости работу (на период устранения последствий вирусной атаки).

5.6. Отключение или необновление антивирусных средств не допускается. Установка и обновление антивирусных средств в организации должны контролироваться представителями подразделений (лицами) в организации, ответственными за обеспечение информационной безопасности.

5.7. Ответственность за выполнение требований инструкции по антивирусной защите должна быть возложена на руководителя функционального подразделения организации, а обязанности по выполнению мер антивирусной защиты должны быть возложены на каждого сотрудника организации, имеющего доступ к ПЭВМ и/или ЛВС.

6. ОБЩИЕ ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ РЕСУРСОВ СЕТИ ИНТЕРНЕТ.

6.1. В организациях, осуществляющих дистанционное банковское обслуживание, в связи с повышенными рисками информационной безопасности при взаимодействии с сетью Интернет обязательно должны применяться соответствующие средства защиты информации (межсетевые экраны, антивирусные средства, и прочее), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии.

6.2. В организациях наличие банковской информации на ПЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме on-line, определяется бизнес-целями организации. При этом необходимо учитывать высокую вероятность несанкционированного доступа, потери и искажения данной информации. Хорошей практикой является практика, когда ПЭВМ, с помощью которых осуществляется взаимодействие с сетью Интернет в режиме on-line, не содержат никакой защищаемой информации.

7. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

7.1. Для установки системы «Клиент-Банк» Клиент получает необходимое установочное программное обеспечение, логин и пароль для первого входа в систему, а также первоначальное блокировочное слово. Установка системы производится во взаимодействии со специалистами Банка. Клиент вправе заменить блокировочное слово, сообщив его специалистам Банка.

7.2. После установки программного обеспечения производятся следующие действия:

- в подсистеме «Регистрация клиента, получение ключей» Клиент генерирует два типа кода (без права аутентификации и с правом аутентификации финансовых документов, передаваемых в Банк). Открытые части кода передаются Банку. Секретные части кода хранятся у Клиента в безопасном месте. Банк на основе открытой части кода Клиента создает сертификат и отправляет сертификат Клиенту. Клиент на основе закрытой части кода и полученного сертификата создает хранилище кодов и сохраняет его в безопасном месте.
- при первом запуске система «Клиент-Банк» вырабатывает уникальный Код активации, который необходимо сообщить Банку. Банк регистрирует Код активации Клиента, формирует Регистрационный ключ и передает его Клиенту. После этого система «Клиент-Банк» на стороне Клиента считается активированной.
- уполномоченные представители сторон подписывают:

- два экземпляра Акта сдачи-приемки автоматизированного рабочего места Клиента (Приложение №1);

- два экземпляра сертификата открытого ключа КА Клиента;

Первые экземпляры Актов передаются Клиенту, вторые - хранятся в Банке.

7.3. Для повышения уровня безопасности при эксплуатации АРМ «Клиента» хорошей практикой является реализация процедуры мониторинга, регистрирующего все значимые события, состоявшиеся в процессе обмена ЭС, и все инциденты.

7.4. При смене кода Клиент производит следующие действия:

- извещает Банк о том, что Клиент желает сгенерировать новый код КА Клиента (при этом сообщает блокировочное слово).
- генерирует новые коды КА.
- отправляет открытую часть кода в Банк. Начиная с даты активации новых кодов, документы подписанные старыми кодами считаются недействительными.

7.5. По окончании рабочего дня, а также вне времени составления и обмена ЭС носители с КА должны храниться в сейфах. Хранение носителей ключевой информации осуществляется ответственным лицом в опечатанном им сейфе (контейнере, пенале). Доступ неуполномоченных лиц к носителям ключевой информации должен быть исключен.

7.6. После ввода в действие новых КА старые должны быть уничтожены в сроки, определенные в соответствующих документах. Если срок не установлен, то КА должен быть уничтожен не позднее 10 суток после вывода из действия. Факт уничтожения оформляется в соответствующих журналах или актом. Носители КА, после уничтожения на них ключевой информации и очистки путем полного форматирования, могут быть использованы в дальнейшей работе без ограничений.

7.7. Не допускается:

- несанкционированно изготавливать копии КА;
- знакомить с содержанием КА или передавать информационные носители с КА лицам, к ним не допущенным;
- выводить КА на дисплей (монитор) ПЭВМ или принтер;

- устанавливать носитель с КА в считывающее устройство (дисковод) ПЭВМ, задействованных в обработке ЭС, в режимах, не предусмотренных функционированием системы обработки и обмена ЭС с Банком, а также в другие ПЭВМ;
- передавать носитель с ключевой информацией лицу, не допущенному к работе с ней;
- записывать на ключевой носитель постороннюю информацию.

7.8. В случае увольнения или перехода в другое подразделение (на другую должность), изменения функциональных обязанностей ответственного лица, имеющего доступ к ключевым носителям (КА и шифрования), должна быть проведена смена ключей.

8. ПОРЯДОК ОБМЕНА ЭЛЕКТРОННЫМИ СООБЩЕНИЯМИ.

8.1. Отправка документов Клиентом осуществляется в следующей последовательности:

- формирование электронных сообщений (ЭС) средствами АРМ Клиент или импорт документа из сторонних систем, поддерживающих формат выгрузки 1С «Бухгалтерия»;
- формирование кода аутентификации электронного сообщения (КА ЭС);
- передача ЭС по каналам связи.

8.2. Прием документов Банком:

- расшифровка и проверка подлинности КА отправляющей стороны и правильности оформления каждого документа.

8.3. Клиент имеет право, позвонив в Банк, и произнеся блокировочное слово, впредь до письменного уведомления, временно заблокировать свою работу в системе «Клиент-Банк».

9. ДЕЙСТВИЯ В СЛУЧАЕ КОМПРОМЕТАЦИИ КА.

9.1. В случае компрометации (нарушение правил безопасности хранения и использования КА, в результате которой возникла вероятность несанкционированного ее применения) немедленно прекращается обмен информацией на скомпрометировавших КА с уведомлением сторон о данном событии.

9.2. При компрометации или подозрении в компрометации секретных КА сторона обязана уведомить об этом другую сторону и немедленно прекратить отправку электронных документов до выяснения обстоятельств.

9.3. К событиям, связанным с компрометацией относятся:

- утрата носителей с КА;
- утрата носителей с КА с последующим обнаружением;
- увольнение ответственного лица, имеющего доступ к КА;
- возникновение подозрений на утечку информации или ее искажение;
- не проходит проверка подписи под входящими или исходящими сообщениями;
- нарушение печати на сейфе (пенале, контейнере) с КА.

Первые три события должны трактоваться как безусловная компрометация действующих КА. Три следующих события требуют специального рассмотрения в каждом конкретном случае.

9.4. По факту компрометации проводится служебное расследование, результаты которого отражаются в акте.

9.5. После приостановки обмена электронными документами по обстоятельствам, изложенным в п. 9.1 настоящего Регламента, для возобновления обмена ЭС стороны повторно формируют КА в порядке, изложенном в разделе 7 настоящего Регламента.

ПОДПИСИ СТОРОН.

БАНК

Банк «Йошкар-Ола» (ПАО)

424006, Республика Марий Эл,
г. Йошкар-Ола, ул. Панфилова, д.39г
к/с 30101810845372202906
в ОКЦ № 1 Волго-Вятского ГУ Банка России,
БИК 042202906, ИНН 1215059221

КЛИЕНТ

Адрес:
р/с
ИНН/КПП

м.п.

м.п.

АКТ СДАЧИ-ПРИЕМКИ
АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА КЛИЕНТА

г. Йошкар-Ола

«__» _____ 20__ г.

Банк «Йошкар-Ола» (ПАО), именуемый в дальнейшем Исполнитель, в лице _____, действующей на основании _____, с одной стороны, и _____, именуемый в дальнейшем Заказчик, в лице _____, действующего на основании _____, с другой стороны, составили настоящий Акт в том, что «__» _____ 20__ г. Исполнитель установил, а Заказчик принял программно-технический комплекс «Клиент-Банк», включающий в себя средства защиты информации и комплект документации «РЕГЛАМЕНТ ИСПОЛЬЗОВАНИЯ АРМ «КЛИЕНТА». Помещения, в которых размещаются технические средства обработки и передачи электронных платежных документов с использованием средства криптографической защиты информации, соответствуют требованиям.

Стороны претензий друг к другу не имеют.

От Исполнителя

От Заказчика
