Утверждены
Решением единственного
участника №
ТОО SredaPay (СредаПэй)»
(Решение от 18/06/2024 г.)

ПРАВИЛА

осуществления деятельности платежной организации

ТОО «SredaPay (СредаПэй)»

Содержание:

1. Общие положения.

1.1. Настоящие Правила платежной организации ТОО «SredaPay (СредаПэй)» (далее по тексту «Правила SredaPay», «настоящие Правила SredaPay»), определяют порядок, процедуру и условия, обеспечивающие осуществление платежных операций в системе «SredaPay (СредаПэй)» (далее по тексту «Система) и устанавливают общие требования к порядку оказания следующих платежных услуг:

- услуги по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам.

Правила SredaPay разработаны в соответствии с Законом Республики Казахстан «О платежах и платежных системах» от 26 июля 2016 года (далее - Закон о платежах), Правилами организации деятельности платежных организаций, утвержденными постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 215,, Уставом ТОО «SredaPay (СредаПэй)» и определяют порядок организации деятельности ТОО «SredaPay (СредаПэй)» в качестве Платежной организации.

1.2. Настоящие Правила SredaPay разработаны, утверждены высшим органом управления платежной организации «SredaPay (СредаПэй)» и обязательны для исполнения всеми участниками, осуществляющими платежи в Системе SredaPay. Каждый из Участников подтверждает и гарантирует, что обладает всеми правами и полномочиями, необходимыми и достаточными для присоединения к настоящим Правилам и исполнения обязательств в соответствии со всеми их условиями.

1.4. Порядок заключения договоров с физическими лицами на оказание платежных услуг осуществляется в строгом соответствии с Гражданским Кодексом Республики Казахстан предусмотренном в части 5 ст. 395 и считается заключенным с момента совершения действий, предусмотренных в публичной оферте, по использованию Системы и размещенной на официальном веб-сайте платежной организации ТОО «SredaPay (СредаПэй)»: www.sredapay.kz.

2. Термины и определения, применяемые в настоящих правилах.

2.1. **Оператор** – ТОО «SredaPay (СредаПэй)», осуществляющее управление Платежной организацией и обеспечивающее ее функционирование, включая осуществление сбора, обработки и передачи информации, формируемой при осуществлении операций в Системе.
2.2. **Система по учету платежей (Система)** — аппаратно-программный комплекс, а также связанные с ним средства и ресурсы, используемые Оператором Системы для предоставления Сервисов.
2.3. **Участники Системы/Участники** - Оператор Системы, Мерчант, Отправитель, Банк.
2.4. **Мерчант** – юридическое лицо или физическое лицо, осуществляющее деятельность без образования юридического лица (индивидуальный предприниматель), в соответствии с регулирующим законодательством, обеспечивающее оформление и выполнение Заказа Клиентов и в пользу которого Клиент осуществляет платеж в счет оплаты за поставляемый Товар, выполненные Работы, оказанные Услуги и заключившей отдельный договор с платежной организацией.
2.5. **Отправитель/Клиент** – физическое или юридическое лицо, оформившее Заказ на получение Товара, Работ, Услуг от Мерчанта с использованием Сервиса приема платежей Системы.
2.6. **Банк** – осуществляющий прием и выплаты денежных средств Мерчантам, при осуществлении операций покупки товаров или услуг Держателями карт на сайте Мерчанта с использованием Платежных карт (их реквизитов) на условиях Договора интернет – эквайринга;
2.7. **Оферта -** договор с физическими, юридическими лицами на оказание платежных услуг размещённом на официальном сайте платежной организации и считающейся заключенным при одобрении Клиентом в совершении платежной организацией платежных услуг.

2.8. **Безопасность/процедуры безопасности -** комплекс необходимых мер и программно-технических средств защиты информации, предназначенных для удостоверения прав владельцев, (клиентов платежной организации) платежных карт на использование платежных карт и обнаружения ошибок и/или изменений в содержании передаваемых и получаемых электронных сообщений при использовании платежных карт.
2.9. **Авторизация** – разрешение Оператором на проведение владельцем платежных карт операций с использованием этих платежных карт в платежной организации, включая предоставление доступа в его личный кабинет. Процедура прохождения авторизации устанавливается Оператором.
2.10. **Аутентификация** – установленные Оператором и доведенные до Клиентов/Участников Платежной организации процедуры и комплекс мер для подтверждения подлинности, и правильности составления электронных сообщений, а также для установления факта передачи электронного сообщения непосредственно Участником Платежной организации, указанным в качестве отправителя.
2.11. **Бесперебойность функционирования Платежной организации** – комплексное свойство Платежной организации, обозначающее ее способность предупреждать нарушения надлежащего функционирования и способность восстанавливать надлежащее функционирование в случае его нарушения.
2.12. **Логин** – уникальная последовательность символов, обозначающая условное имя Клиента в Платежной организации и используемая в целях его авторизации для доступа в личный кабинет в Платежной организации.
2.13. **Пароль** – уникальная последовательность символов, известная только Клиенту, предназначенная для доступа к услугам Платежной организации.
2.14. **Личный кабинет** – персональный раздел Клиентов Системе на интернет-ресурсе Платежной организации, посредством которого Клиент имеет доступ к информации по всем операциям, осуществленным в Системе, предусмотренными настоящими Правилами и заключенными договорами. Перечень предоставляемых услуг посредством личного кабинета Клиента устанавливается Оператором.
2.15. **Идентификация** – процедура, предусмотренная настоящими Правилами, заключающаяся в установлении личности Клиента на основании предоставленного им Оператору документа, удостоверяющего личность, и иных необходимых для проведения идентификации документов, требуемых настоящими Правилами, и регистрации Клиента в Платежной организации с внесением в Платежную организацию его персональных данных.
2.16. **Заявление на идентификацию** – заявление физического лица на идентификацию в Платежной организации, составленное по установленной Банком форме, подлежащее заполнению Участником Платежной организации - физическим лицом в целях прохождения идентификации согласно настоящим Правилам и содержащее условие о заключении между Банком и Участником Платежной организации - физическим лицом соответствующего договора, согласно условиям Оферты.
2.17. **Операционное поручение** – поручение, сформированное Клиентом в адрес Оператора, содержащее необходимую и достаточную информацию для осуществления платежа в Платежной Системе.

3. Описание платежных услуг, оказываемых Платежной организацией.

3.1. Услуги по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам, оказываются Платежной организацией на основании договоров, заключенных с банком/ банками второго уровня и Платежной организацией и обеспечивает прием платежей инициированных, с использованием платежных карт с указанием реквизитов назначения соответствующего платежа и бенефициара соответствующего платежа с последующим обеспечением передачи Платежной организацией реквизитов по платежу для его исполнения в адрес соответствующего банка, а банк в свою очередь исполняет указание клиента, переданное через платежную организацию в электронной форме и перечисляет платеж бенефициару.

4. Порядок и сроки оказание платежных услуг клиентам Платежной организацией.

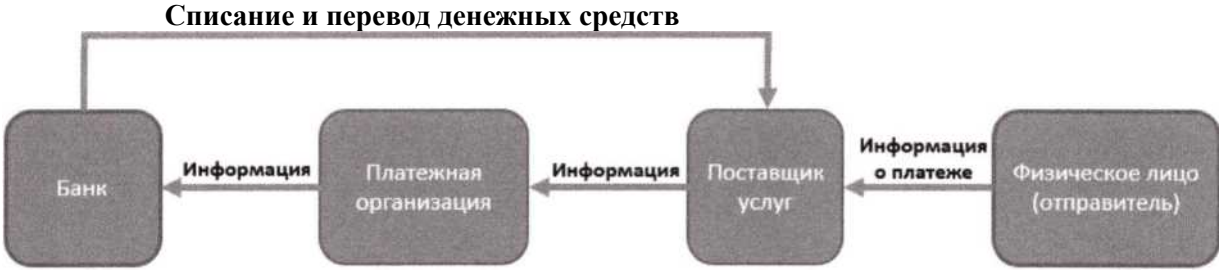
4.1. Услуга по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам оказывается следующим образом:

1. Платежная организация, в рамках договоров, заключенных с Банком обеспечивает прием платежей инициированных с использованием платежных карт с указанием реквизитов назначения соответствующего платежа и бенефициара соответствующего платежа с последующим обеспечением передачи реквизитов по платежу для его исполнения в пользу соответствующего Банка, агентом которого является Платежная организация, а Банк в свою очередь исполняет указание Клиента, переданное через Платежную организацию в электронной форме.
2. Инициирование Клиентом платежных операций/ платежей производится посредствам сети интернет на сайте Мерчанта, мобильного приложения Мерчанта и прочих приложений - обеспечивающих возможность инициирования клиентом в электронной форме распоряжений на списание денег с банковского счета клиента/ банковской карты клиента, с их зачислением в пользу Банка с целью последующего исполнения поручения/ распоряжения Клиента полученного Платежной организацией от Клиента и переданного Платежной организацией в Банк.
3. Платежная организация при оказании услуг совершает следующие действия:

- Клиент посредствам сети интернет/ мобильного телефона, заходит на сайт Мерчанта и при желании приобрести товары либо услуги перемещается на сайт Платежной организации;
- Клиент знакомится с тарифом/ размером комиссии за предоставление Платежной организации соответствующей услуги;
- Клиент знакомится с условиями предоставления платежной услуги и соглашается с условиями договора- оферты размещенными на сайте Платежной организации;
- Клиент по средствам платежной системы инициирует платеж в пользу Поставщика услуг;
- Клиент вводит в платежной системе реквизиты для исполнения платежа Банком;
- Для оплаты платежа Клиент вводит реквизиты банковской карты, банковского счета;
- Платежная организация посредством запроса в Банк инициирует распоряжение Клиента, полученного в электронной форме;
- Банк получив подтверждение от Платежной организации и Клиента производит списание с банковского счета/ банковской карты сумму инициируемой Клиентом операции с учетом комиссионного вознаграждения Платежной организации.
- Платежная организация получает от банка подтверждение исполнения Операции;
- Платежная организация выдает Клиенту электронный чек, подтверждающий совершение Клиентом операции и списание с Клиента комиссии Платежной организации.

4.2. Сроки оказания платежной услуги - в течение 1 (одного) рабочего дня, следующих за днем приема платежа.

Схема потока денежных средств и информационных потоках при оказании платежной услуги:



5. Описание проведения операций в Системе.

5.1. Порядок осуществления платежей по гражданско-правовым сделкам:

5.1.1. Оператор оказывает информационную поддержку Клиенту при передаче осуществлении им платежей в пользу Мерчантов в качестве оплаты за предоставленные товары, работы, услуги.

5.1.2. Оператор определяет список Мерчантов для Клиента и вправе ограничивать его в зависимости от ограничений, приведенных на Сайте Системы.

5.1.3. Клиент направляет Оператору поручение на осуществление платежа в пользу Мерчанта с использованием платежных карт. Операция по осуществлению платежа считается завершенной в момент получения Мерчантом уведомления о зачислении денег, Клиентом — уведомления об успешном завершении платежа. Исполнение распоряжения об осуществлении платежа ведет к уменьшению на карточном счете Клиента суммы денег на сумму платежа и комиссии, в случае ее наличия.

5.1.4. Оплата товаров, работ, услуг и иные операции с использованием платёжных карт при отсутствии требуемой для осуществления операции суммы на карточном счету Клиента - не производятся.

5.1.5. Мерчант предоставляет Клиенту чек в форме электронного документа, подтверждающего осуществленного платежа в случае осуществления платежа через Систему.

5.2. Порядок осуществления возврата по платежным операциям с использованием платежных карт.

5.2.1. В случае необходимости осуществления возврата денег Клиенту-плательщику, возврат осуществляется на условиях и в порядке, предусмотренном настоящими Правилами, соглашением с Клиентом, действующим законодательством Республики Казахстан.

5.2.2. В случае, если необходимость отмены завершенного платежа и/или перевода стала следствием сбоя программного обеспечения и/или ошибки Оператора, произошедшего по вине Оператора, возврат денег осуществляется на счета участников операции путем проведения операции сторнирования — восстановления прав Участников на принадлежащие им деньги, участвующие в данном платеже или переводе, на момент начала операции.

5.2.3. В случае, если возврат денег Клиенту является результатом отказа одной из сторон от исполнения договора, заключенного между Мерчантом и Клиентом, возврат денег по завершенному платежу осуществляется по заявке Мерчанта. Достижение договоренности по осуществлению возврата осуществляется Мерчантом и Клиентом без участия Оператора. Исполнение взаимных обязательств, предшествующее подаче такой заявки, осуществляется в порядке и на условиях, предусмотренных договоренностью между Мерчантом и Клиентом.

5.2.4. Мерчант вправе осуществить возврат на платежную карту Клиента, наличными деньгами или иным способом, согласованным с Клиентом.

5.2.5. В случае, если возврат осуществляется на платежную карту, Мерчант обязан осуществить операцию по возврату суммы платежа в течение 5 (пяти) рабочих дней, с момента формирования заявки на возврат и признания тем самым обязательства по возврату. Клиент и Мерчант вправе согласовать более длительный срок возврата. Клиент не вправе требовать сокращения срока возврата.

5.2.6. В случае, если в течение срока, предусмотренного настоящим разделом для осуществления возврата денег на платежную карту Клиента, осуществить возврат не представляется возможным, Клиент вправе потребовать возврата наличными деньгами или иным способом, согласованным с Мерчантом.

5.2.7. Возврат денег осуществляется в полном объеме полученных Мерчантом средств, за исключением случаев, когда изначальный характер сделки подразумевает комиссии за осуществление возврата.

5.2.8. Комиссия Оператора, обязательному возврату не подлежат, но могут быть возвращены по усмотрению Оператора.

5.2.9. В случае совершения Клиентом-отправителем перевода ошибки при заполнении Операционного поручения и последующего перевода денег в пользу другого Клиента, возврат денег осуществляется по договоренности между Клиентами. В случае отказа Клиента-получателя от возврата денег Клиенту-отправителю, Клиент-отправитель не вправе предъявлять претензии по таким операциям Оператору.

5.2.10. Клиент ознакомлен и согласен с тем, что при осуществлении платежей в адрес Мерчантов, возврат денег по которым не осуществляется в рамках Системы, Клиент самостоятельно обращается к Мерчанту напрямую, по вопросу осуществления такого возврата. При этом Оператор обязуется оказать Клиенту информационную поддержку в ходе разбирательств по таким вопросам.

5.3. Порядок учета и отображения операций, связанных с платежами, осуществленными в платежной Системе.

5.3.1. Учету и фиксации подлежат все произведенные и/или инициированные Участниками операции, произведенных в Системе, включая, уступки права требования, оплата товаров, работ, услуг Мерчантов, погашение, а также иные операции с использованием платежных карт.

5.3.2. В любой момент времени идентифицированный Клиент может получить информацию о проведенных операциях в Системе. История платежей доступна в личном кабинете Клиента/Мерчанта.

5.3.3. Оператор обязуется хранить информацию обо всех операциях, осуществленных Системе, в течение 5 (пяти) лет с даты совершения.

5.4. Порядок осуществления платежей Клиентом:

5.4.1. Клиент вправе с согласия Оператора, в случаях, если операция не ограничена техническими возможностями Системы, способом внесения денег через платежную карту в Системе или иными условиями, предусмотренными Правилами, действующим законодательством Республики Казахстан, иными обстоятельствами, доводимыми до сведения Клиента при попытке проведения операции, осуществить реализацию свое права на покупку/продажу товаров, услуг через интерфейс.

5.4.2. В случае, если у Оператора возникли сомнения в правомерности такой операции, Оператор вправе заблокировать данную операцию до предоставления Оператору доказательства принадлежности карточного счета Клиенту.

5.4.3. В целях осуществления реализации в проведении электронных платежей, Клиенту необходимо направить Операционное Поручение Оператору с предоставлением запрашиваемых Оператором данных. После направления Операционного Поручения, Клиенту посредством отображения в интерфейсе Системы, направляется номер перевода установленного образца, а также код операции, предоставляемый посредством отправки sms-сообщения на мобильный номер, указанный Клиентом в качестве логина. Для осуществления отдельных категорий операций у Клиента могут запрашиваться дополнительные верификационные данные, подтверждающие личность Клиента и/или его права на распоряжение карточным счетом.

5.4.4. Размеры минимальной и максимальной суммы осуществления платежей, а также размеры комиссии, устанавливаются Оператором в рамках действующего законодательства Республики Казахстан и доводятся до сведения Клиента в процессе формирования Операционного Поручения до момента его подтверждения.

5.4.5. С момента передачи данных по осуществленным платежам, Оператор не несет ответственность за несанкционированное использование со стороны третьих лиц данных, которые включают в себя номер операции и код операции.

5.4.6. Клиент принимает на себя обязательства не осуществлять посредством Системы незаконные финансовые операции, незаконную торговлю, операции по легализации (отмыванию) доходов, полученных преступным путем, любые другие операции, нарушающие законодательство Республики Казахстан.

6. Стоимость платежных услуг (тарифы), оказываемых Платежной организацией услуг

Тарифы платежной организации ТОО «SredaPay (СредаПэй)» по платежным услугам*:

1.Услуга по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам:

№	Наименование категорий сервисов	Размер дополнительной комиссии взымаемой с Клиента
1.	Социальные сети	3% от суммы операции
2.	Сотовые операторы	3% от суммы операции
3.	Интернет - магазины	3% от суммы операции
4.	Билеты (авиа, ж/д)	3% от суммы операции
5.	Подарочные карты. купоны	3% от суммы операции
6.	Игровые и развлекательные сервисы	3% от суммы операции
7.	Букмекеры	3% от суммы операции
8.	Услуги ЖКХ	3% от суммы операции
9.	Услуги MLM	3% от суммы операции

10.	Интернет и телофония	3% от суммы операции
11.	Хостинг	3% от суммы операции
12.	Страхование	0%
13.	Реклама	3% от суммы операции
14.	Благотворительность	0%
15.	МКО	3% от суммы операции
16.	Места общественного питания, рестораны, магазины, супермаркеты, салоны красоты и прочие услуги, не включенные в настоящий перечень.	от 0 до 15% от суммы операции

*- без учета комиссии Банков-Эвайеров.

- Окончательная стоимость комиссии, взимаемой с Клиента устанавливается Платежной организацией самостоятельно в рамках допустимых значений, указанными в договорах, заключенных между ТОО «SredaPay (СредаПэй)» и поставщиками услуг (Мерчантами) и иными лицами, предоставляющими услуги Клиентам.
- Приведенный выше список сервисов не является исчерпывающим и может дополняться по мере заключения новых договоров с Мерчантами.

7. Порядок взаимодействия с третьим лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых Платежной организацией

7.1. **Третьи лица** - это юридические лица и индивидуальные предприниматели выполняющие какие-либо работы и оказывающие какие-либо услуги Платежной организации или действуют в ее интересах не входящие в группу компании Платежной организации и не являющиеся работниками Платежной организации.

7.2. Подключение информационных систем третьей стороны к системам Платежной организации производится на основании заключенного договора на оказание информационных и/или технологических услуг и соглашения о неразглашении конфиденциальной информации.

7.3. Соглашение о неразглашении конфиденциальной информации устанавливает обязанность третьей стороны соблюдать конфиденциальность информации, а также ответственность за разглашение конфиденциальной информации, к которой она получает доступ.

7.4. Заключаемый договор или соглашение о неразглашении конфиденциальной информации должны учитывать типовые положения по исполнению третьей стороной требований по обеспечению информационной безопасности. Требования должны включать как минимум следующее:

- ответственность и обязательства за поддержание требуемого уровня информационной безопасности;
- мероприятия по уведомлению об инцидентах информационной безопасности и нарушениях в системе защиты информации.

7.5. Порядок взаимодействия с поставщиками услуг.

7.5.1. Коммерческим отделом Платежной организации выявляется потребность физических лиц/юридических лиц в определенном сервисе по оплате Поставщиков услуг (Мерчантов) и проводятся маркетинговые исследования целесообразности, конкурентоспособности, потребительской способности.

7.5.2. Финансовым отделом проводится экономическое обоснование сотрудничества Поставщика услуг в системе Платежной организации, а также выявляется платежная нагрузка на Клиентов.

7.5.3. В случае принятия положительного решения по вопросу привлечения Мерчантов, у последнего запрашиваются все необходимые документы в рамках требований Закона Республики Казахстан "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма" и проводится полный анализ комплаенс рисков.

7.5.4. При отсутствии комплаенс рисков производится обмен технической документацией для подключения Поставщика услуг к системе Платежной организации по протоколу технического взаимодействия API.

7.6. Заключение договора с Мерчантами.

7.6.1. После проведения всех необходимых действий, указанных в разделе 7.1. настоящих Правил между Платежной организацией и Мерчантами заключается Договор.

7.6.2. Платежной организацией заключается договор с Мерчантом об оказании платежных услуг (или) Договор технического взаимодействия с обязательным наделением правом Платежной организации о принятия платежа в пользу Мерчанта, а также обязательно предусматривается возможность привлечения Платежной организацией Платежных агентов/субагентов.

8. Сведения о системе управления рисками, используемой Платежной организацией.

8.1. Система управления рисками представляет собой систему организации, политик, процедур и методов, принятых Платежной организацией с целью своевременного выявления, измерения, контроля и мониторинга рисков Платежной организации для обеспечения её финансовой устойчивости, и стабильного функционирования.
8.2. Платежная организация в целях эффективного управления рисками разработала политику управления рисками, которая состоит из систематической работы по разработке и практической реализации мер по предотвращению и минимизации рисков, выявлению, измерению, контролю и мониторингу рисков, оценки эффективности их применения, а также контролю за совершением всех денежных операций. В этих целях в Плаежной организации закреплен работник (в случае отсутствия такого работника, данные функции выполняет Директор), выполняющий функции по управлению рисками, в задачи которого входит:

1. анализ и оценка рисков, включающих в себя систематическое определение: объектов анализа рисков; индикаторов риска по объектам- анализа риска, определяющих необходимость принятия мер по предотвращению и минимизации рисков; оценки возможного ущерба в случае возникновения рисков;
2. разработка и реализация практических мер по управлению рисками с учетом: вероятности возникновения рисков и возможных последствий; анализа применения возможных мер по предотвращению и минимизации рисков.

8.3. По договорам с платежными агентами в целях предотвращения финансовых рисков используется обеспечительный взнос, выплачиваемый Платежной организации Платежным агентом, по договору, в объеме необходимом для приема платежей. В случае если сумма обеспечительного взноса исчерпана, то система автоматически блокирует прием платежей.
8.4. При разработке процедур выявления, измерения мониторинга и контроля за рисками Платежная организация учитывает, но не ограничивается следующими факторами:

1) размер, характер и сложность бизнеса;
2) доступность рыночных данных для использования в качестве исходной информации;
3) состояние информационных систем и их возможности;
4) квалификацию и опыт персонала, вовлеченного в процесс управления рыночным риском.

8.5. Процедуры выявления, измерения, мониторинга и контроля за рисками охватывают все виды активов, обязательств; охватывают все виды рыночного риска и их источники; позволяют проводить на регулярной основе оценку и мониторинг изменений факторов, влияющих на уровень рыночного риска, включая ставки, цены и другие рыночные условия; позволяют своевременно идентифицировать рыночный риск и принимать меры в ответ на неблагоприятные изменения рыночных условий.
8.6. Основная задача регулирования рисков в Платежной организации - это поддержание приемлемых соотношений прибыльности с показателями безопасности и ликвидности в процессе управления активами и пассивами Платежной организации, т.е. минимизация потерь.
8.7. Эффективное управление уровнем риска в Платежной организации должно решать целый ряд проблем - от отслеживания (мониторинга) риска до его стоимостной оценки. Уровень риска, связанного с тем, или иным событием, постоянно меняется из-за, динамичного характера внешнего окружения Платежной организации. Это заставляет Платежную организацию регулярно уточнять свое место на рынке, давать оценку риска тех или иных событий, пересматривать отношения с клиентами и оценивать качество собственных активов и пассивов, следовательно, корректировать свою политику в области управления рисками. Процесс управления рисками в Платежной организации включает в себя: предвидение рисков, определение их вероятных размеров и последствий, разработку и реализацию мероприятий по предотвращению или минимизации связанных с ними потерь. Все это предполагает разработку Платежной организацией собственной стратегии управления рисками таким образом, чтобы своевременно и последовательно использовать все возможности развития Платежной организации и одновременно удерживать риски на приемлемом и управляемом уровне.

8.8. Цели и задачи стратегии управления рисками в большой степени определяются постоянно изменяющейся внешней экономической средой, в которой приходится работать.
8.9. В основу управления рисками положены следующие принципы:

1) прогнозирование возможных источников убытков или ситуаций, способных принести убытки, их количественное измерение;
2) финансирование рисков, экономическое стимулирование их уменьшения;
3) ответственность и обязанность руководителей и сотрудников, четкость политики и механизмов управления рисками;
4) координируемый контроль рисков по всем подразделениям Платежной организации, наблюдение за эффективностью процедур управления рисками.

8.10. Система управления рисками характеризуется такими элементами как мероприятия и способы управления.
8.11. Мероприятия по управлению рисками:

1) определение организационной структуры управления рисками, обеспечивающей контроль за выполнением агентами и субагентами Платежной организации требований к управлению рисками, установленных правилами управления рисками Платежной организации;
2) определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений;
3) доведение до органов управления Платежной организации соответствующей информации о рисках;
4) определение показателей бесперебойности функционирования Платежной организации;
5) определение порядка обеспечения бесперебойности функционирования Платежной организации;
6) определение методик анализа рисков;
7) определение порядка обмена информацией, необходимой для управления рисками;
9) определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев; определение порядка изменения операционных и технологических средств и процедур;
10) определение порядка оценки качества функционирования операционных и технологических средств, информационных систем;
11) определение порядка обеспечения защиты информации в Платежной организации.

8.12. Способы управления рисками в Платежной организации определяются с учетом особенностей деятельности Платежной организации, модели управления рисками, процедур платежного клиринга и расчета, количества переводов денежных средств и их сумм, времени окончательного расчета.
8.12.1. Способы управления рисками:

1) установление предельных размеров (лимитов) обязательств агентов и субагентов Платежной организации с учетом уровня риска;
2) установление обеспечительного взноса агентов и субагентов Платежной организации в рамках оказываемых платежных услуг;
3) управление очередностью исполнения распоряжений должностными лицами;
4) осуществление расчета в Платежной организации до конца рабочего дня;
5) обеспечение возможности предоставления лимита;
6) использование безотзывных банковских гарантий;
7) другие способы управления рисками.

9. Порядок урегулирования спорных ситуаций и разрешения споров с клиентами (плательщиками)

9.1. В случае возникновения у плательщика каких-либо претензий к Платежной организации по любой спорной ситуации, связанной с оказанием платежных услуг, Плательщик вправе направить Платежной организации соответствующую претензию в письменной форме.
9.2. Плательщик обязан обратиться к Платежной организации с письменным заявлением, составленным в произвольной форме, содержащим указание на возникшую спорную ситуацию (далее - «Претензия»), одним из следующих способов:

1. путем направления его почтовым отправлением по адресу - Finance@sredapay.kz
2. путем личного обращения в офис Платежной организации и ее нарочным предоставлением по адресу: Республика Казахстан, г.Алматы, пр.Абылай хана, д.56, каб.46, 4 этаж.

9.3. При каждом из перечисленных способов направления Платежной организации Претензии плательщика она подлежит- регистрации платежной организацией путем присвоения даты и порядкового номера входящей корреспонденции. Датой приема Претензии плательщика платежной организации считается фактическая дата регистрации входящего обращения плательщика.
9.4. Обращения в службу технической поддержки плательщиков по телефону, направления сообщений через форму обратной связи на WEB-сайте Системы не могут быть признаны обращением к платежной организации с Претензией и (или) расцениваться как досудебное урегулирование споров.
9.5. Ко всем Претензиям, направляемым плательщиками Платежной организации, должны быть приложены надлежащим образом оформленные копии документов, подтверждающие факты, указанные в Заявлении, а также следующие документы:

1. нотариально заверенная копия документа, удостоверяющего личность плательщика;
2. документ подтверждающий оплату (чек).
3. дополнительно может быть запрошена нотариально заверенная копия договора об оказании услуг сотовой связи, заключенного с оператором сотовой связи и предоставляющего плательщику право использования Абонентского номера, указанного плательщиком при регистрации Учетной записи Пользователя в Системе и др.

9.6. Платежная организация рассматривает полученную Претензию плательщика и подготавливает ответ для направления, в срок не более 30 (тридцати) дней со дня получения соответствующей Претензии плательщика:

1. для надлежащего рассмотрения Претензии плательщика и подготовки ответа Платежная организация;
2. привлекает к всестороннему изучению спора сотрудников компетентных подразделений (технических, правовых, расчетных, и иных структурных подразделений для получения разъяснений, дополнительных сведений и иных данных в отношении оспариваемой ситуации);
3. запрашивает и получает от плательщика дополнительно документы (или их копии), объяснения и иные сведения. По запросу Платежной организации плательщик обязан предоставить запрашиваемые Платежной организацией сведения и документы (их копии) в целях надлежащего досудебного урегулирования возникшего спора;
4. проводит тщательный анализ полученных сведений и разъяснений для формирования полного и достоверного ответа на Претензию плательщика;
5. подготавливает мотивированный письменный ответ плательщику на Претензию.

9.7. Любой спор, если он не был разрешен мирным путем в досудебном порядке, подлежит окончательному разрешению в судебном порядке в соответствии с действующим законодательством Республики Казахстан.

10. Порядок соблюдения мер информационной безопасности, требования к программно-техническим средства и оборудованию, необходимому для оказания для оказания платежных услуг.

10.1. Порядок соблюдения мер безопасности
10.2. В рамках планирования деятельности по обеспечению информационной безопасности осуществляются следующие процессы:

- определения целей и задач по обеспечению информационной безопасности;
- определения направлений для развития системы обеспечения информационной безопасности.

10.3. В рамках реализации деятельности по обеспечению информационной безопасности осуществляются следующие процессы:

- гарантирование использования по назначению компьютеров и телекоммуникационных ресурсов Компании ее сотрудниками, независимыми подрядчиками и другими пользователями.
- выявления, реагирования (противодействие атакам в реальном времени), разрешения и анализ причин возникновения инцидентов информационной безопасности.
- управления доступом к активам.
- антивирусной защиты.
- резервного копирования активов.
- управления непрерывностью бизнеса.
- регистрации, анализа и контроля событий информационной безопасности.

• выявление уязвимостей в информационных системах Платежной организации, с использованием которых могут быть реализованы угрозы информационной безопасности.

• криптографической защиты, определения требований к организации работ, эксплуатации, обеспечению сохранности и безопасному использованию средств криптографической защиты.

• формирования принципов внесения изменений, процедуры установки, модификации и технического обслуживания информационных систем Платежной организации.

• физической безопасности активов.

• защита сетевого периметра.

• соблюдение условий всех программных лицензий, авторских прав и законов, касающихся интеллектуальной собственности.

10.4. В рамках проверки деятельности по обеспечению информационной безопасности осуществляются внутренний и внешний (независимый) контроль/аудит информационной безопасности.

10.5. В рамках совершенствования деятельности по обеспечению информационной безопасности осуществляются анализ результатов функционирования системы обеспечения информационной безопасности Платежной организации.

10.6. Система информационной безопасности Платежной организации

10.6.1. Система информационной безопасности, являющаяся совокупностью применяемых в Платежной организации, мер по защите информации, создаётся в соответствии с методологией менеджмента информационной безопасности. Средства и меры, предотвращения несанкционированного доступа к программно-техническим средствам, применяемые в Платежной организации, включая программно-технические средства, защиты, должны обеспечивать уровень защиты информации и сохранение ее конфиденциальности в соответствии с требованиями, установленными законодательством Республики Казахстан. Все сотрудники обязуются принимать все необходимые меры по сохранению конфиденциальности, предотвращению несанкционированного использования и защите идентификационных данных от несанкционированного доступа со стороны третьих лиц.

10.7. Обеспечение безопасности вычислительных сетей.

10.7.1. Защита сетевой инфраструктуры Платежной организации является одной из основных задач обеспечения информационной безопасности. Вся информационная инфраструктура Платежной организации является средой обработки критичных данных. Принимая во внимание то, что основные бизнес-функции, связанные с обработкой данных, реализуются при помощи связанных вычислительной сетью компонентов информационной инфраструктуры, защита от сетевых угроз является приоритетным направлением обеспечения информационной безопасности.

Сервер

10.7.2. Доступ до терминальной сессии сервера осуществляется путём аутентификации. Одновременно допускается использовать максимум 2 сессии терминала.

Рабочие станции

10.7.3. Доступ в интернет рабочих станций осуществляется путём подключения к Wifi роутеру с защитой подключения типа WPA2-PSK. Все рабочие станции должны быть подключены только к локальной сети Платежной организации. Контроль ограничений входящих и исходящих подключений осуществляется путём настройки межсетевого экрана. Доступ к рабочим станциям осуществляется путём аутентификации пользователя учётной записью домена Active Directory. Пароль от учетной записи выдаётся работнику под личную ответственность для доступа к своей рабочей станции. Пароль может быть изменен Системным Администратором.

10.7.4. Резервированое копирование и восстановления данных, хранящихся в учетных системах, обеспечивается средствами используемых Системой, а также Microsoft Data Protection Manager - систем непрерывного резервного копирования/восстановления. Контроль выполнения процедур резервного копирования осуществляется путем:

1) оповещения ответственного сотрудника при удачном\неудачном резервном копировании;

2) тестирования восстановления баз данных информационных систем не реже 1 (одного) раза в год.

10.7.5. Программное обеспечение реализует возможность вывода выходных документов на экран, принтер или в файл.

10.7.6. Программное обеспечение реализует возможность обмена электронными документами.

10.7.7. Регистрацию и идентификацию происходящих в информационной системе событий с

сохранением следующих атрибутов: дата и время начала события, наи менование события, пользователь, производивший действие, идентификатор записи, дата и время окончания события, результат выполнения события фиксируется средствами используемых СУБД, в том числе:

1) модуль для сбора событий.

2) модуль для анализа и управления событиями и потоками сети из устройств, конечных точек, серверов, антивирусов, брандмауэров и различных систем предотвращения вторжений.

10.8. Управление доступом пользователей к данным

10.8.1. Доступ пользователей к данным является фактором риска информационной безопасности. Процесс управления доступом регламентирован в Платежной организации. Предоставление доступа пользователей к данным осуществляется в соответствии с принципом минимально необходимых привилегий для осуществления должностных обязанностей. Также в Платежной организации реализована и поддерживается система управления парольными политиками.

10.9. Управление учётными записями и парольной защиты

10.9.1. Работа пользователей в ОС и ИС осуществляется под уникальными учетными записями. Не допускается работа пользователя под чужой учетной записью и учетной записью «Администратор», а также включение пользователя в привилегированную группу «Администраторы». Учетная запись «Гость» в операционной системе должна быть отключена. Аутентификация на сервере осуществляется путём подключения к терминалу и ввода пользователем персональных данных, созданных Системным администратором. Для предоставления временного доступа к ресурсам Компании (для лиц. не являющихся работниками Компании, для работников, которым необходимо получить временный доступ к ресурсам Компании, и т.п.) необходимо использовать временные учетные записи (с фиксированным сроком действия) в ОС.

10.9.2. Требования к учетным записям пользователей вкючают, но не ограничиваясь требованиями к учетным записям:

1) учётные записи, включая системные и сервисные, в системном и прикладном программном обеспечении, а также системы и средства защиты информации (включая доступ к управлению межсетевыми экранами и антивирусным программным обеспечением) защищены стойкими методами аутентификации;

2) каждому пользователю информационной системы назначается уникальный идентификатор (имя учётной записи);

3) недопустимость использования разделяемых между несколькими пользователями учётных записей, групповых и общих учётных записей, паролей и других средств аутентификации.

10.9.3. В используемых формах ввода данных используется контроль полноты вводимых данных либо справочники полей обязательных к заполнению, необходимых для проведения и регистрации операций, в случае выполнения функций или операций без полного заполнения всех полей программа может обеспечивать запись соответсвующе записи в журнал и\или ввыдачу соответствующего уведомления;

10.9.4. Программное обеспечение, используемое для проведения и регистрации операций обеспечивает поиск информации по критериям и параметрам, определенным для данной информационной системы, с сохранением запроса, а также сортировку информации по доступным параметрам, а также возможность просмотра информации за предыдущие даты, если такая информация подлежит хранению в информационной системе;

10.9.5. Обработка информации и ее хранение осуществляется по дате и времени;

10.9.6. В информационных системах используется автоматизированное формирование журналов внутреннего учета средствами используемой операционной системы, дополнительно критичные события фиксируются для мониторинга элементов ИТ-инфраструктуры:

1) локальная вычислительная сеть;

2) физические сервера;

3) виртуальные сервера;

4) прикладное программное обеспечение: сервисы обработки операций, системы управления базами данных;

5) облачные сервисы.

При этом обеспечивается сбор и отображение основных метрик состояния, событий, а также формирование журнала\отчета событий за определенный диапазон дат или полностью.

Пароли учетных записей в ОС и ИС Пароли оборудования

10.9.7. Пароль учетных записей ОС и ИС должен иметь длину не менее 8 символов для пользователей и привилегированных пользователя, а также для служебной, системной, встроенной или технологической учетной записи. Пароль пользователей должен быть достаточно сложным и содержать в себе как минимум комбинацию прописных и заглавных букв, цифр. Также возможно, но не обязательно использование специальных символов. Пароль привилегированных пользователей, а также для служебной, системной, встроенной или технологической учетной записи должен содержать в себе символы всех четырех категорий: буквы нижнего регистра, буквы, верхнего регистра, цифры и специальные символы (@, #, $, &, *, % и т.п.). Пароли учетных записей ОС и ИС должны изменяться: для систем, которые поддерживают автоматическую смену паролей, смена пароля осуществляется ежемесячно (каждые 30 дней), а системы, которые не поддерживают автоматическую смену пароля, смена пароля осуществляется каждые 3 месяца (90 дней), исключением является SQL., в которой пароль меняется только в том случае, если работник забыл ранее выданный пароль. Пароли на оборудовании (маршрутизаторы, коммутаторы, беспроводные точки доступа, офисная мини-АТС, видеорегистраторы и др.) должны меняться Системный администратором каждые 180 дней. При смене пароля новый пароль не должен повторять ни один из 12 последних использованных данным пользователем паролей. Данное требование не относится к ИС, в которых не реализована данная функция. Пароль не должен включать в себя осмысленные слова, словосочетания, общепринятые аббревиатуры, а также легко идентифицируемую с его владельцем информацию - имена, фамилии, названия учетных записей, номера телефонов, клички животных, наименования организаций и т.п. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименование автоматизированного рабочего места - АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

Встроенные учетные записи

10.9.8. Пароли, установленные по умолчанию производителем ИС для встроенных учетных записей, должны быть изменены при вводе ИС в эксплуатацию. Это относится и к любому серверному и коммуникационному оборудованию, если это технически возможно. Категорически запрещается использование встроенных учетных записей Administrator (SA для 1С и SQL сервера, root в Unix и т.п.) - для повседневной работы, для запуска служб и сервисов либо для доступа к сетевым ресурсам. Использование встроенных учетных записей допускается только в случаях, требующих реквизитов именно этой учетной записи (восстановление ОС, восстановление поврежденных данных, системы, в некоторых случаях проведение обновлений системы и т.п.). Для встроенных учетных записей Administrator должно быть включено логирование всех действий. Все неиспользуемые учетные записи должны быть отключены или удалены

При увольнении работника

10.9.9. При увольнении работника его учётная запись удаляется/отключается. При выходе работника в любой вид отпуска, а также на больничный, учетные записи в ОС и ИС должны быть заблокированы до момента выхода на работу. Пользователям запрещается разглашать информацию о своих учетных записях. Пользователям запрещается предоставлять доступ к своей учетной записи другим работникам Компании или третьим, лицам. В случае служебной необходимости, разрешается работать на персональном компьютере другого работника под своей учетной записью с устного разрешения его непосредственного руководителя. Исключением является исполнение своих должностных обязанностей Системным администратором при настройке компьютерам, ноутбука пользователя по поданной заявке на бумажном носителе. В этом случае, Системный администратор может производить исполнение заявки и в отсутствие пользователя, но в этом случае, после выполнения всех работ, Системный администратор обязан выключить компьютер пользователя (если пользователь так и не пришел на свое рабочее место). При уходе в отпуск или при переводе работника в другое подразделение, работник должен позаботиться о передаче необходимой информации заменяющему его лицу, а непосредственный руководитель должен проконтролировать данный процесс. При отсутствии пользователя в течение 5 минут на рабочем месте (неактивное состояние компьютера), компьютер должен быть автоматически переведен в заблокированное паролем состояние. Блокировка выполняется путем настроек ОС на рабочей станции работника. Помимо этого, каждый работник Компании, уходя с рабочего места обязан самостоятельно заблокировать свою учетную запись, нажав на клавиатуре комбинацию клавиш «эмблема Windows+L», либо «CTRL+ALT+DELETE» и затем нажать «Блокировать компьютер».

10.10. Обеспечение антивирусной защиты

10.10.1. Информационная инфраструктура, Платежной организации связана с внешней средой (сетью Интернет), поэтому угроза проникновения вредоносного программного обеспечения весьма

актуальна. Для защиты от этой угрозы применяются антивирусные средства. Правила внесения изменений в системы и информационную инфраструктуру в целом регламентированы во избежание проникновения вредоносного кода. В качестве антивирусного программного обеспечения может быть использовано только лицензионное ПО или ПО, распространяемое бесплатно.

Сервер

10.10.2. Сервер должен обязательно иметь установленное антивирусное программное обеспечение для автоматической проверки всех файлов и электронной почты, поступающих на этот сервер. Не реже 1 раза в неделю на терминальном сервере с установленной ОС должно проводиться полное сканирование всех дисков компьютера на предмет заражения вирусами. Антивирусное программное обеспечение на сервере должно обновляться не реже одного раза в день, автоматически путем соответствующих настроек антивирусного ПО.

Рабочие станции

10.10.3. Каждый персональный компьютер компании должен иметь установленное антивирусное программное обеспечение с функцией автоматической проверки всех файлов и электронной почты; поступающих на этот- компьютер. Не реже 1 раза в неделю на каждом персональном компьютере Компании должно проводится полное сканирование всех дисков компьютера на предмет заражения вирусами. Антивирусное программное обеспечение на персональных компьютерах должно обновляется не реже одного раза в день автоматически путем соответствующих настроек антивирусного ПО. При обнаружении заражения оперативной памяти компьютера любым вредоносным ПО. в процессе сканирования, зараженный компьютер должен быть немедленно отключен от локальной сети Платежной организации для дальнейшего тестирования и лечения.

10.11. Обеспечение физической безопасности

10.11.1. Защита от несанкционированного физического доступа к компонентам информационной инфраструктуры является важнейшей задачей обеспечения информационной безопасности. Физический доступ сотрудников Платежной организации и представителей внешних сторон к компонентам серверной информационной инфраструктуры ограничен и предоставляется только для выполнения должностных или договорных обязательств.

10.11.2. Защиту от несанкционированного доступа обеспечивает:

10.11.2.1. использование сетевого оборудования отвечающими характеристикам с показателями указанными в таблице:

Характеристика	**Показатель**
Пропускная способность в режиме Firewall (App-ID enabled)	940 Mbps
Пропускная способность в режиме защиты от угроз	610 Mbps
Пропускная способность IPSec VPN	400 Mbps
Максимальное число одновременно поддерживаемых сессий	128 000
Максимальное количество «новых» сессий	8 300/c
Максимальное количество туннелей VPN/туннельных интерфейсов	1000
Максимальное количество зон безопасности	30
Максимальное число правил безопасности	1 500

10.11.2.2. Использвание программного обеспечения на сетевом оборудовании:

1) Threat Prevention – включает функциональные возможности IPS, Antivirus, Anti-Bot, Anti-Spyware;
2) URL-Filtering – фильтрация URL-запросов пользователей по категориям;
3) GlobalProtect – предоставляет возможность подключения пользователей к ресурсам локальной сети через межсетевой экран Palo Alto Networks. Также позволяет задействовать возможность проверки удаленного хоста на соответствие определенным правилам безопасности такие как наличие на клиентском устройстве антивируса, актуальной версии ОС со всеми актуальными обновлениями.

4) WildFire –возможность использовать публичное облако специализированных компаний, оказывающих услуги в области информационной безопасности, для сканирования подозрительных файлов на вредоносную активность.

10.12. Обеспечение целостности баз данных и полную сохранность информации в электронных архивах и базах данных при полном или частичном отключении электропитания в любое время на любом участке оборудования обеспечивается:

10.12..1. хранением информации с использованием системы управлнения базой данных (далее – СУБД) Microsoft SQL Server версии не ниже Standard Edition выпуска не старше 2016;

10.12..2. использование технологии SQL Server AlwaysOn, решения высокого уровня доступности и аварийного восстановления, включающая в себя в том числе следующие функции:

1) распределение метаданных и уведомлений - метаданные служб и размещенных приложений, конфигурации и состояния хранятся на каждом узле кластера, изменения в метаданных или состоянии узла автоматически распространяются на другие узлы кластера;

2) управление ресурсами - отдельные узлы в кластере могут предоставлять физические ресурсы, например, подключаемое напрямую хранилище, сетевые интерфейсы и доступ к общему дисковому хранилищу;

3) мониторинг работоспособности - определение исправности основного узла и исправности между узлами осуществляется за счет сочетания сетевых соединений по типу тактовых импульсов и мониторинга ресурсов;

4) координация отработки отказа - каждый ресурс настроен для размещения на основном узле, и каждый может быть перенесен автоматически или вручную на один или несколько второстепенных узлов. Политика отработки отказа в зависимости от исправности управляет автоматическим переносом ресурсами между узлами кластера. Узлы и размещенные приложения получают уведомления об отработке отказа, что позволяет им продолжить выполнять возложенные на них функции без прерывания в работе и потери данных.

10.13. Расположением оборудования, использующегося для обработки и хранения баз данных в центрах обработки данных, отвечающих требованиям:

1) гарантированное электропитание;
2) обеспечение необходимого климатического режима;
3) круглосуточный мониторинг и техническое обслуживание;
4) автоматический комплекс газового пожаротушения;
5) круглосуточно охраняемая территория;
6) системы видеонаблюдения;
7) разграничение физического доступа и организационные процедуры контроля доступа во все помещения;
8) порт выхода в сеть Интернет на скорости от 100 Мбит в секунду.

10.14. Обеспечение безопасной поддержки и эксплуатации информационной инфраструктуры

10.14..1. Для обеспечения максимальной прозрачности и безопасности разработки, внедрения и эксплуатации компонентов информационной инфраструктуры, Платежной организации, а также их программного обеспечения изменения, вносимые в информационную инфраструктуру, подлежат тестированию и регистрации. Требования информационной безопасности учитываются при разработке, внедрении и эксплуатации информационных систем, отдельных компонентов и программного обеспечения.

10.15. Мониторинг информационной инфраструктуры

10.15..1. Мониторинг информационной инфраструктуры необходим для своевременного выявления инцидентов и уязвимостей информационной безопасности. Мониторинг осуществляется в отношении производительности систем, доступа к данным, функционирования систем, безопасности. Для оценки общего уровня защищенности информационной инфраструктуры Платежной организации выполняются проверки на уязвимости. Независимый аудит системы безопасности и внутренних контролей проводится на регулярной основе не реже одного раза в год.

10.15..2. Срок хранения информации об инцидентах информационной безопасности составляет не менее 5 (пяти) лет.

10.15..3. Платежная организация определяет порядок принятия неотложных мер к устранению инцидента информационной безопасности, его причин и последствий.

10.15..4. Платежная организация ведет журнал учета инцидентов информационной безопасности с отражением всей информации об инциденте информационной безопасности, принятых мерах и предлагаемых корректирующих мерах.
10.15..5. Информационные системы, задействованные в проведении и хранении операций обеспечивают автоматизированное формирование форм отчетов, представляемых операторами систем электронных денег в Национальный банк, а также отчетов о проведенных операциях;
10.15..6. Платежная организация предоставляет в Национальный Банк информацию о следующих выявленных инцидентах информационной безопасности:

1) эксплуатация уязвимостей в прикладном и системном программном обеспечении;
2) несанкционированный доступ в информационную систему;
3) атака «отказ в обслуживании» на информационную систему или сеть передачи данных;
4) заражение сервера вредоносной программой или кодом;
5) совершение несанкционированного перевода электронных денег вследствие нарушения контролей информационной безопасности;
6) иных инцидентах информационной безопасности, несущих угрозу стабильности деятельности оператора системы электронных денег.

10.15..7. Информация об инцидентах информационной безопасности, указанных в настоящем пункте, предоставляется Платежной организацией в возможно короткий срок, но не позднее 48 часов с момента выявления, в виде карты инцидента информационной безопасности. На каждый инцидент информационной безопасности заполняется отдельная карта инцидента информационной безопасности
10.16. Управление инцидентами и уязвимостями информационной безопасности
10.16..1. Все обнаруженные инциденты информационной безопасности регистрируются и расследуются с целью определения причин их возникновения и предотвращения их повторения. Уязвимости информационной безопасности, обнаруженные при выполнении мероприятий мониторинга, подлежат учету с целью дальнейшего планирования действий по их устранению.
10.16..2. Платежная организация обеспечивает функционирование системы обеспечения информационной безопасности, которая представляет собой совокупность мер организационного и программно-технического характера и системы менеджмента информационной безопасности, направленных на защиту активов организации от угроз информационной безопасности.
10.16..3. Деятельность по обеспечению информационной безопасности осуществляется в виде циклической модели Деминга «планирование → реализация → проверка → совершенствование → планирование» и является частью общей системы управления.
10.16..4. Система управления информационной безопасностью обеспечивает защиту информационных активов Платежной организации, допускающую минимальный уровень потенциального ущерба для бизнес-процессов Платежной организации.
10.16..5. Платежная организация обеспечивает надлежащий уровень системы управления информационной безопасностью, ее развитие и улучшение.
10.17. Обеспечение бесперебойной работы информационной инфраструктуры
10.17.1. Поскольку одной из задач информационной безопасности является обеспечение доступности информации, мерам по защите компонентов информационной инфраструктуры от сбоев отводится значительная роль. Для обеспечения отказоустойчивости применяется дублирование критичных компонентов информационной инфраструктуры. Средствами резервного копирования обеспечивается гарантированное восстановление бизнес-процессов после сбоя в работе одного или нескольких компонентов информационной инфраструктуры, а также обеспечивается минимизация времени восстановления сервисов и бизнес-процессов. Платежная организация обеспечивает бесперебойное функционирование Системы в режиме 24/7/365 (24 часа в день. 7 дней в неделю, 365 дней в году), за исключением времени проведения профилактических работ.
10.17.2. Программное обеспечение, используемое для проведения и регистрации операций обеспечивает поиск информации по критериям и параметрам, определенным для данной информационной системы, с сохранением запроса, а также сортировку информации по доступным параметрам, а также возможность просмотра информации за предыдущие даты, если такая информация подлежит хранению в информационной системе;
10.17.3. Обработка информации и ее хранение осуществляется по дате и времени;

10.17.4. В информационных системах используется автоматизированное формирование журналов внутреннего учета средствами используемой операционной системы, дополнительно критичные события фиксируются для мониторинга элементов ИТ-инфраструктуры:

1) локальная вычислительная сеть;
2) физические сервера;
3) виртуальные сервера;
4) прикладное программное обеспечение: сервисы обработки операций, системы управления базами данных;
5) облачные сервисы.

При этом обеспечивается сбор и отображение основных метрик состояния, событий, а также формирование журнала/отчета событий за определенный диапазон дат или полностью.

11. Меры, принимаемые к участнику платежной системы за нарушение правил платежной системы

11.1. Руководство Платежной организации регулирует вопросы, связанные с:

• определением целей и стратегии достижения целей обеспечения информационной безопасности в Платежной организации;

• выделением ресурсов для осуществления деятельности по обеспечению информационной безопасности в Платежной организации;

• принятием решений в отношении ключевых рисков нарушения информационной безопасности.

• Менеджер Департамента ИТ несёт ответственность за:

определение требований по информационной безопасности и осуществление контроля исполнения данных требований в Платежной организации;

осуществление контроля общей эффективности обеспечения информационной безопасности, её соответствия текущим и будущим требованиям бизнеса.

• Владельцы процессов и активов несут ответственность за:

- распределение полномочий и ответственности по реализации мер обеспечения информационной безопасности (конфиденциальности, целостности, доступности) для своих активов, адекватных существующим рискам;

- устранение в установленные сроки несоответствий по результатам проведенных аудитов/проверок обеспечения ИБ.

11.2. Все работники Платежной организации несут ответственность за соблюдение требований внутренних нормативных документов Платежной организации, регламентирующих обеспечение информационной безопасности, а также своевременное оповещение о нарушениях и недостатках информационной безопасности, которые ими были обнаружены.

11.3. Ответственность работников Платежной организации за нарушение требований информационной безопасности определяется правилами внутреннего трудового распорядка Платежной организации, а также положениями внутренних нормативных документов. В отдельных случаях нарушение работниками требований информационной безопасности влечет уголовную, административную, гражданско-правовую и иную ответственность, предусмотренную законодательством.

12. Порядок изменение условий и внесение изменений в настоящие правила;

12.1. Изменения и/или дополнения в настоящие Правила могут вноситься как путем утверждения новой редакции Правил, так и путем подготовки текста изменений и/или дополнений к Правилам.

12.2. В случае несогласия Участника с изменениями и/или дополнениями в Правила или тарифами, Участник вправе отказаться от дальнейшего использования Платежной организации.

12.3. Дальнейшее использование сервисов Платежной организации после вступления в силу любых изменений и/или дополнений в Правила означает согласие Участников с такими изменениями и/или дополнениями.