Утверждены
Директором ТОО «Smartplat»
Приказ №ВНД-1 от 13.10.2023 г.

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ ТОО «Smartplat»

2023 г.

ОГЛАВЛЕНИЕ

Глава 1. Общие положения

1.1. Настоящие Правила организации деятельности Платежной организации «Smartplat» (далее – Правила) разработаны в соответствии с законом Республики Казахстан от 26 июля 2016 года «О платежах и платежных системах» (далее – Закон о платежах) и определяют порядок организации деятельности Платежной организации и единые условия и процедуры, обеспечивающие осуществление операций в Системе.

1.2. Настоящие Правила обязательны для исполнения всеми Участниками расчетов Системы и размещаются на интернет ресурсе Платежной организации.

1.3. Взаимоотношения сторон участников Системы регулируются законодательством Республики Казахстан и договорами, заключаемыми между Платежной организацией и другими участниками Системы.

1.4. Платежная организация при наличии регистрационного номера учетной регистрации Платежной организации, присвоенного Национальным Банком Республики Казахстан, (далее – регистрационный номер) оказывает следующие виды 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.

Глава 2. Термины и определения

2.1. В настоящих Правилах используются понятия, предусмотренные Законом о платежах, а также следующие понятия:

1) **Бесперебойность функционирования Платежной организации** – комплексное свойство Платежной организации «Smartplat», обозначающее ее способность предупреждать нарушения надлежащего функционирования (в том числе не допускать приостановления (прекращения) осуществления операций или ненадлежащего осуществления операций), а также восстанавливать надлежащее функционирование в случае его нарушения.

2) **Значимые (существенные) риски** – риски, негативные последствия реализации которых, оказывают существенное влияние на оценку достаточности капитала Платежной организации, а также ликвидности и оценку финансовых показателей Платежной организации, в т.ч. оказывающие влияние на возможность соблюдения обязательных требований законодательства Республики Казахстан.

3) **Клиент/Плательщик** – физическое лицо, обладающее надлежащей дееспособностью в соответствии с действующим законодательством Республики Казахстан для осуществления Платежа, совершившее конклюдентные действия, направленные на заключение Договора об оказании услуг, и обладающее Аутентификационными данными для доступа к Системе для ее использования в целях управления своей Учетной записью, и последующего оказания Платежной организацией платежных услуг, предусмотренных Правилами.

4) **Лимит** – установленное численное ограничение значений показателей, характеризующих (каждый в отдельности или в совокупности) уровень риска. Лимит может быть установлен в абсолютном и относительном значении.

5) **Оценка риска** – оценка вероятности реализации риска и величины возможных потерь при реализации конкретного вида риска и/или совокупных рисков (группы рисков), принимаемых на себя Платежной организацией.

6) **Платежная организация** – Товарищество с ограниченной ответственностью «Smartplat» (БИН 231040018021), являющееся коммерческой организацией, которое в соответствии с Законом о платежах правомочно осуществлять деятельность по оказанию платежных услуг.

7) **Поставщик услуг** – юридическое лицо или физическое лицо, зарегистрированное в качестве индивидуального предпринимателя, заключившее отдельный договор с Платежной организацией, и в пользу которого Клиент осуществляет платеж в счет оплаты за Товары, либо физическое лицо, принимающее денежные средства от Клиента, не связанные с предпринимательской деятельностью.

8) **Расчетный банк** – банк второго уровня Республики Казахстан, привлекаемый Платежной организацией в целях проведения расчетов между Платежной организацией и Поставщиком услуг по Договору.

9) **Риск** – присущая деятельности Платежной организации возможность (вероятность) возникновения убытков, ухудшения ликвидности или иных негативных последствий вследствие наступления неблагоприятных событий, связанных с внутренними факторами (сложность организационной структуры, уровень квалификации работников, организационные изменения, текучесть кадров и т.д.) и внешними факторами (изменение экономической конъюнктуры, применяемые новые технологий, внедрение новых продуктов и т.д.).

10) **Система** – совокупность программно-технических средств Платежной организации, обеспечивающих информационно-технологическое взаимодействие и регистрацию платежей.

11) **Склонность к риску** – система плановых показателей развития бизнеса, характеризующих максимальный уровень риска, который Платежная организация в целом готово принять в процессе достижения, установленных стратегией развития целей, в том числе целевого уровня доходности, реализации стратегических инициатив и выполнения своих основных бизнес-задач.

12) **Товар** – товары, работы, услуги, права на результаты интеллектуальной деятельности, реализуемые Поставщиком услуг конечным потребителям (Клиентам) для личного, семейного или домашнего использования.

13) **Третьи лица** — это юридические лица и индивидуальные предприниматели, которые:

- предоставляют услуги Платежной организации или действуют в интересах Платежной организации;
- не входят в группу компании Платежной организации и не являются работниками Платежной организации.

14) **Участники расчетов** – Поставщик услуг, Клиент/Плательщик, Банк-эквайер.

Глава 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.

Указанные услуги осуществляется путем согласования с системой банка и с соблюдением требований действующего законодательства Республики Казахстан.

Платежная организация вправе оказывать платежные услуги при условии и не ранее получения регистрационного номера учетной регистрации Платежной организации в соответствии с применимым законодательством.

Глава 4. Порядок и сроки оказания платежных услуг клиентам Платежной организации

4.1. Порядок оказания 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.

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 (далее – «Банк/Банк-эквайер», «платежная услуга») осуществляется следующим образом:

1) Платежная организация, в рамках договора, заключенного с Банком, обеспечивает обработку платежей, инициированных с использованием банковских 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, а Банк в свою очередь исполняет указание Клиента, переданное через Платежную организацию в электронной форме.

2) Инициация Клиентом операций/платежей производится посредствам WEB – приложений, online - приложений, мобильных приложений (приложений для мобильных устройств), программного обеспечения терминалов самообслуживания, виджетов и прочих приложений - обеспечивающих возможность инициации клиентом в электронной форме распоряжений на списание денег с 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) При оказании платежной услуги Платежная организация обеспечивает следующий алгоритм действий:

– Клиент посредством сети интернет/мобильного телефона, терминала самообслуживания заходит в соответствующее приложение Платежной организации;

– Клиент ознакамливается с тарифом/размером комиссии за предоставление Платежной организации соответствующей услуги;

– Клиент ознакамливается с условиями предоставления платежной услуги и соглашается с условиями договора - оферты размещенными в соответствующем приложении;

– Клиент в приложении инициирует платеж в пользу Поставщика услуг;

– Клиент вводит в электронное приложение 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 банковской карты и перевода Платежа в пользу Поставщика услуг, указанного в поручении Клиента, сумму инициируемой клиентом операции с учетом вознаграждения Платежной организации и комиссионного вознаграждения Банка;

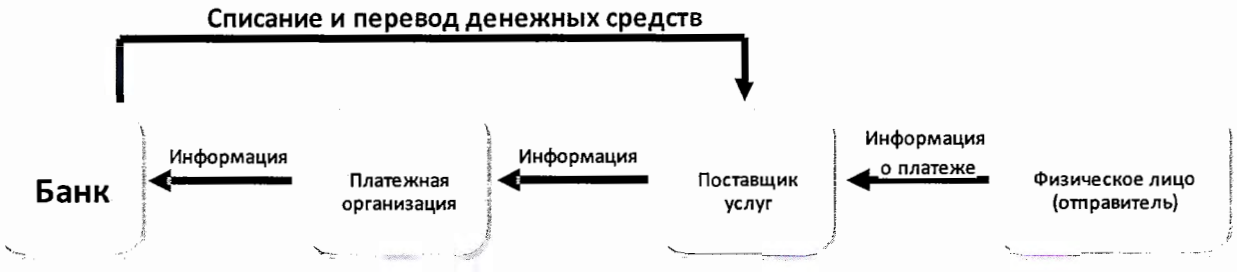
– Платежная организация получает от Банка подтверждение исполнения Операции;

– Платежная организация выдает Клиенту электронное подтверждение о совершении Клиентом операции и списания с Клиента комиссии Платежной организации.

Перевод Банком на текущий счет Поставщика услуг по совершенным транзакциям производится Банком в национальной валюте Республики Казахстан.

Сроки оказания платежной услуги - в течении 1 (одного) рабочего дня, следующего за днем приема платежа.

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



Глава 5. Стоимость платежных услуг (тарифы), оказываемых Платежной организацией

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:

№	Наименование категорий сервисов, предоставляемых Поставщиками услуг при осуществлении деятельности по интернет эквайрингу	Дополнительная плата (допустимая дополнительная комиссия), взимаемая с Клиента.
1.	Игровые сервисы	5% от суммы операции
2.	Букмекеры	5% от суммы операции
3.	Социальные сети	5% от суммы операции
4.	Сотовые операторы	5% от суммы операции
5.	Подарочные карты, купоны	5% от суммы операции
6.	ЖКХ	5% от суммы операции
7.	MLM	5% от суммы операции
8.	Интернет и телефония	5% от суммы операции
9.	Хостинг	5% от суммы операции
10.	Благотворительностьот	Не взимается
11.	Реклама	5% от суммы операции
12.	Страхование	Не взимается
13.	Интернет - магазины	5% от суммы операции
14.	Билеты (авиа, ж/д)	5% от суммы операции
15.	МКО	5% от суммы операции
16.	Места общественного питания, рестораны, магазины, супермаркеты, салоны красоты и прочие виды сервисов, не включенные в отдельные категории	От 0% до 15% от суммы операции

Стоимость дополнительной платы (допустимой дополнительной комиссии), взимаемой с Клиента, устанавливается в соответствии с договорными условиями, указанными в договорах, заключенных между ТОО «Smartplat» и поставщиками услуг, и иными лицами, предоставляющими услуги Клиентам.

Ценовая политика по взимаемой дополнительной комиссии с плательщика устанавливается Платежной организацией самостоятельно в рамках допустимых значений, указываемых в договорах.

Дифференциация процентного соотношения допустимой дополнительной комиссии, взимаемой с плательщика зависит от рыночных условий по каждому сервису.

Приведенный выше список сервисов не является исчерпывающим и может дополняться по мере заключения новых договоров с поставщиками услуг.

Глава 6. Порядок взаимодействия с третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых Платежной организацией

6.1. При условии соблюдения положений применимого законодательства, Платежная организация вправе уполномочивать третьих лиц на оказание информационно-технологической поддержки для целей оказания платежных услуг.

6.2. 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.

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

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.

6.3. Порядок взаимодействия при работе с поставщиками услуг.

Платежная организация при необходимости проводит маркетинговые исследования, включающие в себя анализ рынка, конкурентоспособности, потребительскую способность. Финансовым подразделением проводится экономическое обоснование заведения нового Поставщика услуг в систему Платежной организации, а также выявляется платежная нагрузка на Клиентов. После проведения вышеуказанных действий и принятия положительного решения по работе с Поставщиком услуг, у последнего запрашиваются все необходимые документы в рамках проведения оценки на соответствие законодательству о ПОД/ФТ. При отсутствии комплаенс рисков производится обмен технической документацией для подключения Поставщика услуг к системе Платежной организации по протоколу технического взаимодействия API.

6.4. Заключение договора с Поставщиком услуг.

6.4.1. После проведения всех действий в соответствии с п. 6.3. настоящих Правил между Платежной организацией и Поставщиком услуг заключается Договор. Поставщик услуг проходит регистрацию в Системе, с присвоением идентификатора.

6.4.2. Оказание платежной услуги обеспечивается предоставлением Платежной организацией гарантийного взноса (авансового платежа) на планируемый объем принятия платежей. При совершении платежа клиентом, сумма принятых платежей списывается с расчетного счета (баланса) в системе Поставщика услуг.

6.4.3. Платежная организация обязуется обеспечивать на указанном счете неснижаемый остаток денежных средств, достаточный для исполнения обязательств перед Поставщиком

услуг. При отсутствии в день приема платежей денежных средств в остатке гарантийного взноса Платежной организации, обязательство Платежной организации является необеспеченным, и Поставщик услуг вправе приостановить исполнение договора либо предоставить Платежной организации отсрочку в перечислении платежа (коммерческий кредит, либо овердрафт) на основании отдельного соглашения, заключаемого Платежной организацией с Поставщиком услуг или гарантийного письма.

6.4.4. Платежная организация передает Поставщику услуг данные о каждом принятом платеже для внесения изменений в лицевой счет Клиента. Сведения должны быть переданы непосредственно в период приема платежа на основании данных, указываемых клиентом, без ошибок и искажений.

6.4.5. Каждая операция по передаче данных о платеже сопровождается подписанием Платежной организацией электронного документа, форма которого согласована с соответствующим Поставщиком услуг. Сочетание аутентификационных данных – логин, пароль и/или номер терминала в Системе - определены как аналог собственноручной подписи (далее АСП) Платежной организации и признаются сторонами в качестве однозначного и бесспорного подтверждения совершенного платежа.

6.4.6. При приеме платежей Платежной организации взимается комиссия с платежа. Размер комиссии устанавливается Платежной организацией, и определяется условиями работы с Поставщиками услуг.

6.5. Порядок взаимодействия Платежной организации с банками.

Основанием взаимодействия Платежной организации с банком является договор о взаиморасчетах и информационно-техническом взаимодействии, содержащий, по меньшей мере, но не ограничиваясь, следующую информацию:

- общее описание оказываемых платежных услуг, включая порядок и максимальный срок их оказания;
- размеры взимаемых сборов и комиссий, а также порядок их взимания;
- порядок расчетов с Платежной организацией и поставщиком услуг;
- условия, при которых банк вправе расторгнуть договор в одностороннем порядке;
- порядок предъявления претензий и разрешения споров.

6.5.1. Предварительными условиями взаимодействия с банком являются:

6.5.1.1.соответствие банка следующим критериям:

- общая финансовая устойчивость;
- осуществление мер по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- наличие необходимых лицензий (разрешений) на осуществление деятельности банка в соответствии с требованиями применимого законодательства;
- обеспечение информационной защиты и банковской тайны.

6.5.1.2.регистрация Платежной организации в системе банка. Для целей такой регистрации:

- Платежная организация осуществляет реализацию интерфейса подключения (API) к системе банка;
- Платежная организация совместно с банком проводят тестирование систем на определение их технической готовности к отправке информации о платежах.

6.6. Платежная организация и банк обязуются передавать друг другу информацию о каждом обработанном платеже непосредственно в период обработки платежа, на основе предоставленных клиентом данных. Каждой операции по передаче платежных данных присваивается уникальный номер в системе банка. В установленный договором о взаиморасчетах и информационно-техническом взаимодействии срок Платежная организация совместно с банком проводят сверку по успешно обработанным платежам.

Глава 7. Сведения о системе управления рисками, используемой Платежной организацией

7.1. В основные задачи системы управления рисками, используемой Платежной организацией входит:

- 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;
- 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.

7.2. Под системой управления рисками в Платежной организации понимается комплекс мероприятий, принятых Платежной организацией с целью своевременного выявления, измерения, контроля и мониторинга рисков для обеспечения финансовой устойчивости и стабильного функционирования.

7.3. При разработке процедур выявления, измерения мониторинга и контроля за рисками Платежная организация учитывает, но не ограничивается следующими факторами:

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

7.4. 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.

7.5. 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.

7.6. Цели и задачи стратегии управления рисками в большой степени определяются постоянно изменяющейся внешней экономической средой, в которой приходится работать.

В основу управления рисками положены следующие принципы:

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

7.7. Система управления рисками характеризуется такими элементами как мероприятия и способы управления.

7.7.1. Мероприятия по управлению рисками включают:

1) определение организационной структуры управления рисками, обеспечивающей контроль за выполнением партнерами 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;
8) определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев;
9) 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.
7.7.2. 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. Способы управления рисками включают, но не ограничиваются:
1) управление очередностью исполнения распоряжений должностными лицами;
2) осуществление расчета в Платежной организации до конца рабочего дня;
3) обеспечение возможности предоставления лимита;
4) использование безотзывных банковских гарантий;
5) отказ от взаимодействия с неблагонадежными партнерами;
6) страхование возможных рисков;
7) другие способы управления рисками.

Глава 8. Порядок соблюдения мер информационной безопасности

8.1. Участники расчетов обязуются принимать все необходимые меры для обеспечения безопасности и по защите информации и документов, обмен которыми осуществляется в Платежной организации или которые доступны Участникам расчетов в связи с использованием Платежной организации, а также с целью выявления (предотвращения) мошенничества и противодействия легализации доходов, полученных преступным путем, и финансированию терроризма.
8.2. 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. Участники расчетов обязуются принимать все необходимые меры по сохранению конфиденциальности, предотвращению несанкционированного использования и защите идентификационных данных от несанкционированного доступа со стороны третьих лиц.
8.3. Порядок соблюдения мер информационной безопасности основан на следующих принципах:
1) обеспечение и поддержание соответствующего уровня целостности, доступности и конфиденциальности критичной информации;
2) соответствие требованиям законодательства;
3) экономическая целесообразность.

8.4. Ниже раскрыты принципы и методы их соблюдения:

1) Целостность информации достигается аутентификацией и авторизацией при доступе к ней и при изменении, информация всегда имеет актуальное или заданное значение. Аутентификация и авторизация может быть реализована административными мерами и/или автоматизированными средствами. Доступность означает, что в любой момент времени субъекты, которым легитимно предоставлено право доступа к информации могут реализовать его в соответствии с назначенными правами – чтение, изменение и т.п. Конфиденциальность информации – это сохранение тайны, недопущение разглашения информации лицам, не имеющим право на ознакомление с ней. Конфиденциальность достигается ограничением доступа к информации в необходимом объеме и классификацией информации по решению ее владельца если иное не установлена законами и нормативно правовыми актами;

2) Соблюдение Порядка основано на законодательных актах Республики Казахстан, в том числе на требованиях Национального Банка Республики Казахстан, отраженных в нормативно-правовых актах. При построении системы управления информационной безопасностью, обеспечивающей выполнение Порядка и соблюдение законодательных и нормативно правовых актов, применяются рекомендации международного стандарта ISO/IEC 27001 «Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;

3) средства, направленные на организацию Порядка, не превышают возможный ущерб при реализации угрозы информационной безопасности и адекватно минимизируют риск реализации. Оценку возможного ущерба производят исходя из множества факторов актуальных на текущий момент или на момент предполагаемого инцидента.

8.5. Первый руководитель Платежной организации осуществляет общий контроль и несет персональную ответственность за достижение целей и соблюдение основных принципов, в том числе за предоставление необходимых условий и ресурсов для достижения целей Порядка, а также принимает на себя обязательства по постоянному улучшению и выполнению применимых требований СУИБ.

8.6. Каждый работник несет персональную ответственность за нарушение и/или невыполнение установленных Порядком принципов и последствий, вызванных этими нарушениями, и обязан сообщать обо всех выявленных нарушениях и Первому руководителю Платежной организации.

8.7. Должностные инструкции каждого работника Платежной организации, а также документы описывающие отношения с третьими лицами содержат требования по обеспечению и соблюдению информационной безопасности.

8.8. В соответствии с требованиями бизнесов и рисков, связанных с утечкой и разглашением конфиденциальной информации, к которой осуществляется доступ третьей стороной, работниками отдела информационных технологий по согласованию с третьей стороной осуществляется контроль должного уровня обслуживания и уровня информационной безопасности третьей стороны.

Контроль может включать:

- анализ отчетов о работах (услугах), предоставляемых третьей стороной;
- регулярные совещания по вопросам и проблемам, возникающим в ходе работ;
- анализ отчетов и результатов расследования возникших инцидентов информационной безопасности;
- актуальность сертификатов по информационной безопасности (если применимо).

8.9. Платежная организация предпринимает необходимые меры для обеспечения необходимой консолидации, систематизации и хранению информации об инцидентах информационной безопасности, полученная в ходе мониторинга деятельности по обеспечению информационной безопасности.

8.10. Платежной организацией ведется журнал учета инцидентов информационной безопасности с отражением всей информации об инциденте информационной безопасности, принятых мерах и предлагаемых корректирующих мерах, связанных с недопущением повторного инцидента информационной безопасности.
8.11. Платежная организация представляет в Национальный Банк Республики Казахстан 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 денежных средств вследствие нарушения контролей информационной безопасности;
6) инцидентах информационной безопасности, несущих угрозу стабильности деятельности платежной организации.
8.12. Информация об инцидентах информационной безопасности, указанных в настоящем разделе, предоставляется платежной организацией не позднее 48 (сорока восьми) часов с момента выявления инцидента информационной безопасности по регламентированной форме согласно нормативно-правовым актам Республики Казахстан.
8.13. Информация по обработанным инцидентам информационной безопасности представляется в электронном формате с использованием платформы Национального Банка Республики Казахстан для обмена событиями и инцидентами информационной безопасности. На каждый инцидент информационной безопасности заполняется отдельная карта инцидента информационной безопасности.
8.14. Срок хранения информации об инцидентах информационной безопасности составляет не менее 5-и (пяти) лет.

Глава 9. Описание программно-технических средств и оборудования, необходимого для осуществления платежных услуг

9.1. Программное обеспечение, используемое Платежной организацией обеспечивает соотвествие требованиям к программно-техническим средствам Платежной организации и системе управления информационной безопасностью
9.2. Для целей обеспечения надежного хранения информации применяется дублирование систем хранения данных (производитель HP), а также наличие холодного резерва комплектующих к ним.
9.3. Защиту от несанкционированного доступа обеспечивает:
9.3.1. использование сетевого оборудования отвечающими характеристикам с показателями не ниже:

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	1500

9.3.2. Использвание программного обеспечения на сетевом оборудовании:

- Threat Prevention – включает функциональные возможности IPS, Antivirus, Anti-Bot, Anti-Spyware;
- URL-Filtering – фильтрация URL-запросов пользователей по категориям;
- 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.
- WildFire –возможность использовать публичное облако специализированных компаний, оказывающих услуги в области информационной безопасности, для сканирования подозрительных файлов на вредоносную активность.

9.4. 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:

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

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

- 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;
- управление ресурсами - отдельные узлы в кластере могут предоставлять физические ресурсы, например, подключаемое напрямую хранилище, сетевые интерфейсы и доступ к общему дисковому хранилищу.
- мониторинг работоспособности - определение исправности основного узла и исправности между узлами осуществляется за счет сочетания сетевых соединений по типу тактовых импульсов и мониторинга ресурсов;
- 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.

9.4.3. расположением оборудования, использующегося для обработки и хранения баз данных в центрах обработки данных, отвечающих требованиям:

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

9.5. Доступ к входным данным, функциям, операциям, отчетам, реализованным в программном обеспечении предоставляется пользователям в соответствии с «Матрицей владельцев и администраторов информационных систем» определяющей как минимум следующие уровени доступа:

- Владелец;
- Администратор;
- Разработчик;
- Пользователь.

9.6. Требования к учетным записям пользователей:

9.6.1. 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;

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

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

9.7. 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 соответсвующее записи в журнал и\или ввыдачу соответствующего уведомления;

9.8. 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;

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

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

- локальная вычислительная сеть;
- физические сервера;
- виртуальные сервера;
- прикладное программное обеспечение: сервисы обработки операций, системы управления базами данных;
- облачные сервисы.

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

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

- оповещения ответственного сотрудника при удачном\неудачном резервном копировании
- тестирования восстановления баз данных информационных систем не реже 1 (одного) раза в год.

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

9.13. Программное обеспечение реализует возможность обмена электронными документами.

9.14. Регистрацию и идентификацию происходящих в информационной системе событий с сохранением следующих атрибутов: дата и время начала события, наименование события, пользователь, производивший действие, идентификатор записи, дата и время окончания события, результат выполнения события фиксируется средствами используемых СУБД, в том числе:

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

Глава 10. Порядок урегулирования спорных ситуаций и разрешения споров с клиентами (плательщиками)

10.1. В случае возникновения у клиента каких-либо претензий к Платежной организации по любой спорной ситуации, связанной с оказанием платежных услуг, клиент вправе направить Платежной организации соответствующую претензию в письменной форме.

10.2. Клиент обязан обратиться к Платежной организации с письменным заявлением, составленным в произвольной форме, содержащим указание на возникшую спорную ситуацию (далее – «Претензия»), путем направления его почтовым отправлением по адресу - 050011, Республика Казахстан, город Алматы, Туркисбский район, улица Заветная, здание 31.

10.3. При каждом направлении Платежной организации Претензии клиента, она подлежит регистрации Платежной организацией путем присвоения даты и порядкового номера входящей корреспонденции. Датой приема Претензии клиента Платежной организации считается фактическая дата регистрации входящего обращения клиента.

10.4. Обращения в службу технической поддержки клиентом по телефону, направления сообщений через форму обратной связи в приложении системы не могут быть признаны обращением к Платежной организации с Претензией и (или) расцениваться как досудебное урегулирование споров.

10.5. Ко всем Претензиям, направляемым клиентами 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 клиента;
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 клиенту право использования абонентского номера, указанного клиентом при регистрации учетной записи клиента в системе и др.

10.6. Платежная организация рассматривает полученную Претензию клиента и подготавливает ответ для направления в срок не более 30 (тридцати) календарных дней со дня получения соответствующей Претензии клиента.

10.7. Для надлежащего рассмотрения Претензии клиента и подготовки ответа Платежная организация:

- 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);
- запрашивает и получает от клиента дополнительно документы (или их копии), объяснения и иные сведения. По запросу Платежной организации клиент обязан предоставить запрашиваемые Платежной организацией сведения и документы (их копии) в целях надлежащего досудебного урегулирования возникшего спора;

- проводит тщательный анализ полученных сведений и разъяснений для формирования полного и достоверного ответа на Претензию клиента;
- подготавливает мотивированный письменный ответ клиенту на Претензию.

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.

Глава 11. Порядок внесения изменений в настоящие Правила

11.1. Изменения и/или дополнения в Правила могут вноситься как путем утверждения новой редакции Правил, так и путем подготовки текста изменений и/или дополнений к Правилам. Дата вступления в силу изменений и/или дополнений в Правила определяется Платежной организацией.

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