«УТВЕРЖДЕНО» Приказом Директора ТОО «QAPITALA PAY»
№ 09-1 ОД от 22.07.26

# ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ ТОО «QAPITALA PAY» ПРИ ОКАЗАНИИ ПЛАТЕЖНЫХ УСЛУГ

**Алматы 2026 г.**

**Оглавление**

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

**1.** Настоящие Правила осуществления деятельности платежной организации ТОО «QAPITALA PAY» при оказании платежных услуг (далее – Правила) разработаны в соответствии с законом Республики Казахстан от 26 июля 2016 года «О платежах и платежных системах» (далее – Закон), Правилами организации деятельности платежных организаций, утвержденными постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 215, Уставом ТОО «QAPITALA PAY», и определяют порядок организации деятельности Платежной организации 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;

2. В настоящих Правилах используются понятия и определения, предусмотренные Законом.

## 2. ОПИСАНИЕ ПЛАТЕЖНЫХ УСЛУГ, ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

**2.1. 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 отдельных договоров, заключенных с банком/банками второго уровня и Платежной организацией с третьими лицами и 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, партнером которого является Платежная организация, а банк в свою очередь исполняет указание Клиента, переданное через Платежную организацию в электронной форме.

## 3. ПОРЯДОК И СРОКИ ОКАЗАНИЯ ПЛАТЕЖНЫХ УСЛУГ КЛИЕНТАМ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ

**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.**

**3.1.1.** 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 (далее – «Банк», «платежная услуга») осуществляется 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, партнером которого является Платежная организация, а Банк в свою очередь исполняет указание Клиента, переданное через Платежную организацию в электронной форме.

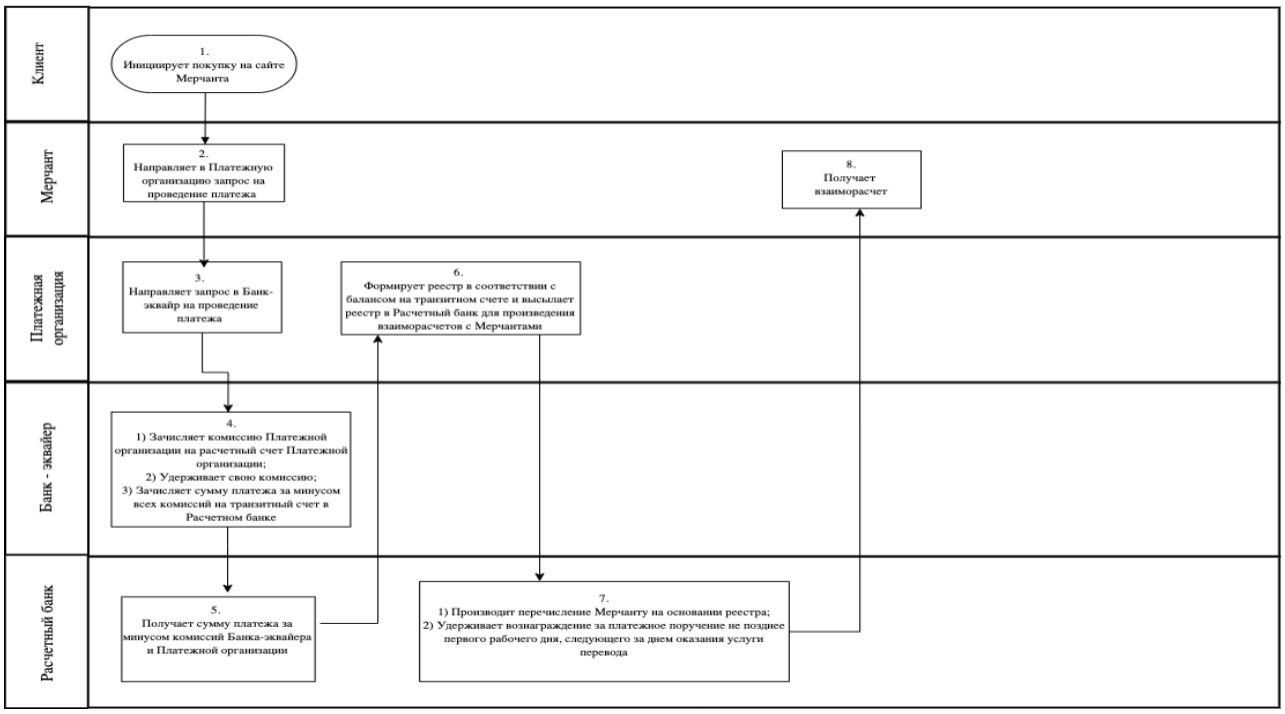
2) Инициация Клиентом платежей производится посредствам WEB – приложений, online- приложений, мобильных приложений (приложений для мобильных устройств), программного обеспечения терминалов самообслуживания, виджетов и прочих приложений- обеспечивающих возможность инициации Клиентом в электронной форме 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 посредствам сети интернет, мобильного телефона, терминала самообслуживания заходит в соответствующее приложение 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 Мерчанта, размещенными в сети интернет/приложении, терминале самообслуживания и т.д.;
- Клиент в приложении инициирует платеж в пользу Мерчанта;
- Клиент вводит в электронное приложение реквизиты для исполнения платежа Банком;

 Для оплаты платежа Клиент вводит реквизиты банковской карты;
 Платежная организация посредством запроса в Банк инициирует распоряжение Клиента, полученного в электронной форме;
 Банк получив подтверждение от Платежной организации и Клиента производит списание денежных средств с платежной карточки Клиента и осуществляет перевод суммы Платежа указанной в поручении Клиента в пользу Мерчанта с учетом комиссионного вознаграждения Платежной организации;
 Платежная организация получает от Банка подтверждение исполнения операции;
 Платежная организация выдает Клиенту электронную квитанцию, подтверждающую совершение Клиентом операции и списание с Клиента комиссии Платежной организации (в случае, если комиссия удерживается с Клиента).

**3.1.2.** Схема денежных, информационных потоков при обслуживании Платежной организацией платежных операций Клиентов, порядок взаимодействия между Расчетным банком, Банком (Банк-эквайер) и Платежной организацией и Мерчантом.




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

## 4. УЧАСТНИКИ СИСТЕМЫ И УСЛОВИЯ ИХ УЧАСТИЯ

**4.1.** **Оператор** - участник системы, юридическое лицо, осуществляющее деятельность по обеспечению функционирования системы и выполняющее установленные Законом «О платежах и Платежных системах» обязанности, относящиеся к такой деятельности.

Оператор определяет порядок/ правила функционирования системы, порядок участия в системе других лиц, заключает договора с поставщиками услуг (получателями денег/ бенефициарами), осуществляет сбор и обработку платежей от участников системы с последующим перечислением данных платежей в пользу соответствующих получателей/ бенефициаров соответствующих платежей. Оператор самостоятельно и от своего имени заключает договора с участниками системы, определяет порядок их работы в системе.

**Оператор системы:**

1) устанавливает правила системы и осуществляет контроль за их соблюдением участниками системы;
2) осуществляет обработку и выдачу платежных и информационных сообщений участников (участникам) системы, индивидуальное исполнение указаний или клиринг;
3) заключает договора с участниками системы об участии в системе;
4) определяет систему управления рисками;
5) обеспечивает функционирование инфраструктуры системы;
6) обеспечивает соблюдение мер информационной безопасности и непрерывности деятельности;
7) обеспечивает равный и открытый доступ участников системы к оказываемым им услугам;
8) утверждает внутренние документы по управлению деятельностью оператора системы;
9) выполняет иные обязанности на основании договоров, заключенных с участниками системы.

**4.2.** **Поставщик/ Мерчант (бенефициар платежа)** – юридические лица, индивидуальные предприниматели, лица, в пользу которых осуществляются платеж и (или) перевод денег.

**4.3.** **Клиент** - физическое лицо/ юридическое лицо (представитель), оплачивающее платежи через систему Оператора;

## 5. СТОИМОСТЬ ПЛАТЕЖНЫХ УСЛУГ (ТАРИФЫ), ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

5.1. Тарифы платежной организации ТОО «QAPITALA PAY» по платежным услугам:

5.2. 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 | Дополнительная плата, взимаемая с Клиента. |
|---|---|---|
| 1. | Игровые сервисы | от 0 % до 10% от суммы операции |
| 2. | Букмекеры | от 0 % до 15% от суммы операции |
| 3. | Социальные сети | от 0 % до 10% от суммы операции |
| 4. | Сотовые операторы | от 0 % до 10% от суммы операции |
| 5. | Подарочные карты, купоны | от 0 % до 10% от суммы операции |
| 6. | ЖКХ | от 0 % до 10% от суммы операции |
| 7. | MLM | от 0 % до 10% от суммы операции |
| 8. | Интернет и телефония | от 0 % до 10% от суммы операции |
| 9. | Хостинг | от 0 % до 10% от суммы операции |
| 10. | Благотворительность | Не взимается |
| 11. | Реклама | от 0 % до 10% от суммы операции |
| 12. | Страхование | Не взимается |
| 13. | Интернет - магазины | от 0 % до 10% от суммы операции |
| 14. | Билеты (авиа, ж/д) | от 0 % до 10% от суммы операции |
| 15. | МКО | от 0 % до 10% от суммы операции |
| 16. | Прочие виды сервисов, не включенные в отдельные категории | от 0 % до 10% от суммы операции |

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

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

 Ценовая политика по взимаемой комиссии с Мерчанта устанавливается Платежной организацией индивидуально в рамках заключенных договоров с Мерчантами.

В случае изменения размера комиссионного вознаграждения, информация о новых тарифах, а также информация о сроках введения их в действие доводится до сведения Мерчантов в порядке, предусмотренном в заключенных договорах.

 Приведенный выше список сервисов не является исчерпывающим и может дополняться по мере заключения новых договоров с Мерчантами в соответствии с законодательством Республики Казахстан.

## 6. ВЗАИМОДЕЙСТВИЯ С ТРЕТЬИМИ ЛИЦАМИ, ОБЕСПЕЧИВАЮЩИМИ ТЕХНОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПЛАТЕЖНЫХ УСЛУГ, ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

**6.1.** Порядок взаимодействия с третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых Платежной организацией, регулируется соответствующими договорами, заключенными с третьими лицами, а также настоящими Правилами.

**6.2.** Взаимодействие Платежной организации с третьими лицами при оказании платежных услуг подлежит осуществлению в строгом соответствии с требованиями законодательства Республики Казахстан.

**6.3.** При взаимодействии с третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых Платежной организацией, принимаются надлежащие меры безопасности, в том числе позволяющие обеспечить зависящую от соответствующей стороны взаимодействия информационную безопасность, защищенность персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Республики Казахстан.

**6.4.** Цель: поддерживать защиту конфиденциальной информации, к которой имеют доступ третьи стороны, которая обрабатывается третьими сторонами, передаётся третьим сторонам или управляется третьими сторонами.

**6.5.** Под «третьей стороной» понимаются юридические лица и индивидуальные предприниматели, которые предоставляют услуги Платежной организации или действуют в интересах Платежной организации;

**6.6.** Подключение информационных систем третьей стороны к системам Платежной организации производятся на основании заключённого договора и соглашения о неразглашении конфиденциальной информации.

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

**6.8.** 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.

**6.9.** API и прочая техническая информация, необходимая для построения взаимодействия с Платежной организации для систем третьих сторон является открытой и предоставляется им по запросу.

**6.10.** В целях минимизации рисков Платежной организации, связанных с утечкой и разглашением конфиденциальной информации, к которой осуществляется доступ третьей стороной, работниками отдела IT по согласованию с третьей стороной осуществляется контроль должного уровня обслуживания и уровня информационной безопасности третьей стороны. Контроль может включать:

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

## 7. СВЕДЕНИЯ О СИСТЕМЕ УПРАВЛЕНИЯ РИСКАМИ, ИСПОЛЬЗУЕМОЙ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

**7.1.** Система управления рисками направлена на обеспечение финансовой устойчивости и стабильного функционирования Платежной организации, и представляет собой систему организации, политик, процедур и методов, принятых Платежной организацией, и позволяющих Платежной организации своевременно осуществлять выявление, измерение, контроль, мониторинг за возникающими рисками и разработка мероприятий по минимизации рисков при оказании платежных услуг.

Процесс управления рисками имеет решающее значение для поддержания стабильной рентабельности Платежной организации, и каждый отдельный сотрудник Платежной организации несёт ответственность за риски, связанные с его или её обязанностями.

**7.2.** Политика управления рисками в Платежной организации и капиталом Платежной организацией определяет базовые принципы, в соответствии с которыми Платежная организация формирует систему управления рисками и достаточностью собственных средств (капитала).

В рамках системы управления рисками Платежная организация определяет финансовые и

нефинансовые риски.

**К финансовым рискам относятся:**

**Рыночный риск** – это риск возникновения у Платежной организации убытков вследствие неблагоприятного изменения рыночной стоимости финансовых инструментов в инвестиционном портфеле Платежной организации, а также курсов иностранных валют.

**Риск ликвидности** – риск возникновения проблем, связанных с недостаточностью средств для обеспечения выполнения собственных обязательств Платежной организации, связанный с недополученными доходами при вынужденной продаже активов по текущей стоимости на покрытие разрыва ликвидности, либо с избыточными расходами на вынужденное привлечение пассивов для компенсации недостатка ликвидных ресурсов

**Операционный риск** – это риск возникновения прямых или косвенных убытков, связанных с несовершенством системы внутреннего контроля, ошибками информационных систем, ошибками и/или злоупотреблениями (мошенничеством) персонала, неадекватными процедурами деятельности.

К нефинансовым рискам относятся:

**Риск потери деловой репутации** – это риск возникновения у Платежной организации убытков в результате уменьшения числа Мерчантов (контрагентов) вследствие формирования в обществе негативного представления о финансовой устойчивости Платежной организации, качестве оказываемых услуг или характере деятельности в целом.

**Правовой риск** – это риск возникновения у Платежной организации убытков вследствие:

- несоблюдения требований законодательства и заключенных договоров;
- допускаемых правовых ошибок при осуществлении деятельности (некорректные юридические консультации или неверное составление документов, в том числе при рассмотрении спорных вопросов в судебных органах);
- несовершенства правовой системы (противоречивость законодательства, отсутствие правовых норм по регулированию отдельных вопросов, возникающих в процессе деятельности);
- нарушения контрагентами нормативных правовых актов, а также условий заключенных договоров.

**Комплаенс-риск** – риск возникновения расходов (убытков) вследствие несоблюдения платежной организацией требований законодательства Республики Казахстан, в том числе нормативных правовых актов уполномоченного органа, а также внутренних правил и процедур компании.

**Стратегический риск** – это риск возникновения у Платежной организации убытков в результате ошибок (недостатков), допущенных при принятии решений, определяющих стратегию деятельности и развития Платежной организации (стратегическое управление) и выражающихся в недостаточном учете возможных опасностей, которые могут угрожать деятельности Платежной организации, неправильном или недостаточно обоснованном определении перспективных направлений деятельности, в которых Платежная организация может достичь преимущества перед конкурентами, отсутствии или обеспечении в неполном объеме необходимых ресурсов (финансовых, материально-технических, людских) и организационных мер (управленческих решений), которые должны обеспечить достижение стратегических целей деятельности Платежной организации.

**7.3. Управление рисками**

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 указанных целях в Платежной организации закреплен работник (в случае отсутствия такого работника, данные функции выполняет первый руководитель), 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.

По договорам с Клиентами, при необходимости, в целях предотвращения финансовых рисков используется обеспечительный взнос, выплачиваемый Клиентами Платежной организации по договору.

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.

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.

Основная задача регулирования рисков в Платежной организации - поддержание приемлемых соотношений прибыльности с показателями безопасности и ликвидности в процессе управления активами и пассивами Платежной организации, т.е. минимизация потерь.

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 с Мерчантами 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.

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

Мероприятия по управлению рисками:

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

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:

1) установление предельных размеров (лимитов) обязательств контрагентов Платежной организации с учетом уровня риска;
2) установление обеспечительного взноса контрагентов Платежной организации в рамках оказываемых платежных услуг;
3) осуществление расчета в платежной организации до конца рабочего дня;
4) обеспечение возможности предоставления лимита;

5) использование безотзывных банковских гарантий;
6) проведение внутреннего или внешнего аудита бухгалтерской отчетности, показателей ликвидности, прогнозных показателей и других показателей риска.
7) другие способы управления рисками.

**Способы управления комплаенс риском:**

**1. Идентификация**

• Анализ всех бизнес-процессов;
• Выявление зоны, где может произойти нарушение: клиенты (особенно высокорисковые: PEP, офшоры, санкционные лица), продукты (новые финансовые инструменты, кросс-бордер услуги), операции (крупные транзакции, транзитные потоки),
• IT-системы (обработка персональных данных, киберриски).

**2. Оценка рисков**

• Использование Методики расчета рисков;
• Риски классифицируются на: низкие/средние/высокие;
• Определяется приоритет — какие зоны надо контролировать в первую очередь.

**3. Контроль**

• Внедряются внутренние документы: Правила внутреннего контроля в целях ПОД ФТ ФРОМУ, Методика расчета рисков, Методика выявления пороговых и подозрительных операций;
• Используются технические меры: автоматические системы скрининга по санкционным спискам, лимиты на транзакции, стоп-листы клиентов и контрагентов.

**4. Мониторинг**

• Проводятся регулярные внутренние проверки, аудиты;
• Отслеживаются изменения законодательства в части ПОД ФТ ФРОМУ;
• Ведётся реестр нарушений и инцидентов (при наличии);
• Разработка и внедрения автоматизированных систем для выявления пороговых, подозрительных операций, а также операций, соответствующих типологиям и схемам).

**5. Обучение сотрудников**

• Регулярные тренинги (онлайн-курсы, тесты, живые тренинги);
• Кейсы из реальной практики (например, штрафы банкам или платежным организациям);
• Формирование культуры: каждый сотрудник понимает, что комплаенс — это его зона ответственности тоже.

**6. Реагирование**

• При выявлении нарушения проводится внутреннее расследование;
• Разрабатываются корректирующие меры (например, ужесточение KYC);
• При необходимости направляются соответствующие сообщения в Агентство Республики Казахстан по финансовому мониторингу;
• Инциденты фиксируются, чтобы предотвратить повторение.

В целях идентификации клиента, его операций в Платежной организации разработаны Внутренние нормативные документы, которые регламентируют такие процессы как идентификация клиентов (их представителей) и бенефициарных собственников, мониторинг и изучение операций клиента, оценка риска и меры по минимизации рисков.

## 8. ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРНЫХ СИТУАЦИЙ И РАЗРЕШЕНИЯ СПОРОВ С КЛИЕНТАМИ

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 соответствующее обращение в письменной форме.

Клиент обязан обратиться к Платежной организации с письменным заявлением, составленным в произвольной форме, содержащим указание на возникшую спорную ситуацию (далее – «Заявление»), одним из следующих способов:

1. путем направления его почтовым отправлением по адресу – 050012, Республика Казахстан, г.Алматы, проспект Достык, д.192, офис 302;
2. путем личного обращения в офис Платежной организации и ее нарочным предоставлением по адресу: Республика Казахстан, город Алматы, проспект Достык, д.192/2, офис 300.

При каждом из перечисленных способов направления Платежной организации Заявления, она подлежит регистрации Платежной организацией путем присвоения даты и порядкового номера входящей корреспонденции. Датой приема Заявления Платежной организацией считается фактическая дата регистрации входящего обращения Клиента.

Обращения в службу технической поддержки по телефону, направления сообщений через форму обратной связи на Сайте Системы не могут быть признаны обращением к Платежной организации и (или) расцениваться как досудебное урегулирование споров.

Ко всем Заявлениям, направляемым в Платежную 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 (квитанция).
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.

Платежная организация рассматривает полученное Заявление и подготавливает ответ для направления в срок не более 30 (тридцати) календарных дней со дня получения соответствующего Заявления.

Для надлежащего рассмотрения Заявления и подготовки ответа Платежная организация:

1) привлекает к всестороннему изучению спора работников компетентных подразделений (технических, правовых, расчетных, и иных структурных подразделений для получения разъяснений, дополнительных сведений и иных данных в отношении оспариваемой ситуации);
2) 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;
3) проводит тщательный анализ полученных сведений и разъяснений для формирования полного и достоверного ответа на Заявление;
4) подготавливает мотивированный письменный ответ Клиенту на Заявление.

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

## 9. ПОРЯДОК СОБЛЮДЕНИЯ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

9.1. **Платежная организация** обеспечивает создание и функционирование системы управления информационной безопасностью, являющейся частью общей системы управления платежной организации, предназначенной для управления процессом обеспечения информационной безопасности.

**9.2.** Основы обеспечения информационной безопасности

**Система управления информационной безопасностью (СУИБ)** - часть системы управления Платежной организации, основанная на подходе бизнес-рисков по созданию, внедрению, функционированию, мониторингу, поддержке и улучшению информационной безопасности.

**Информационная безопасность** - сохранение конфиденциальности, целостности и доступности информации.

**Конфиденциальность** - свойство информации, предполагающее обеспечение секретности и не доступности
информации для не авторизованных на ее получение субъектов, включая процессы Платежной организации.

**Доступность** - свойство информации, быть доступной и готовой к использованию для авторизованных на это субъектов.

**Целостность** - свойство сохранения достоверности, неизменности и полноты информации.

Основной целью СУИБ минимизация ущерба в следствии нарушения целостности, конфиденциальности и доступности информации.

**9.3. Система управления информационной безопасностью** обеспечивает защиту информационных активов платежной организации, допускающую минимальный уровень потенциального ущерба для бизнес-процессов платежной организации. Платежная организация обеспечивает надлежащий уровень системы управления информационной безопасностью, ее развитие и улучшение.

В рамках деятельности по построению системы управлению информационной безопасности, Платежной организацией обеспечивается функционирование следующих процессов:

- Определения целей и задач системы управления информационной безопасностью;
- Определение направлений развития системы управления информационной безопасностью;
- Оценка рисков и угроз информационной безопасности Платежной организации;
- Разработки и применения компенсирующих мер по результатам оценки рисков и угроз информационной безопасности.

В рамках реализации системы управлению информационной безопасностью, Платежная организация проводит следующие мероприятия, но не ограничиваясь ими:

- выявление и реагирование на атаки в реальном времени;
- разрешение и анализ причин возникновения инцидентов информационной безопасности;
- управление доступом к активам;
- резервирование информационных систем и данных платежной организации;
- управление непрерывностью деятельности;
- регистрация, анализ и контроль событий информационной безопасности;
- выявление уязвимостей в информационных системах платежной организации, с использованием которых могут быть реализованы угрозы информационной безопасности;
- использование средств криптографической защиты информации;
- обеспечение физической безопасности активов;
- защита сетевого периметра;
- соблюдение условий всех программных лицензий, авторских прав и законов, касающихся интеллектуальной собственности.

В целях совершенствования системы управления информационной безопасностью периодически осуществляется анализ результатов функционирования системы.

**9.4.** Платежная организация в целях обеспечения конфиденциальности, целостности и доступности информации платежной организации осуществляет следующие функции:

- организует систему управления информационной безопасностью, осуществляет координацию и контроль деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;
- обеспечивает методологическую поддержку процесса обеспечения информационной безопасности;
- осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля информационной безопасности в рамках своих полномочий;
- осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах информационной безопасности;
- осуществляет анализ информации об инцидентах информационной безопасности;
- обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности, а также предоставление доступа к ним;
- определяет ограничения по использованию привилегированных учетных записей;
- организует и проводит мероприятия по обеспечению осведомленности работников платежной организации в вопросах информационной безопасности;
- осуществляет мониторинг состояния системы управления информационной безопасностью платежной организации;
- периодически (но не реже одного раза в год) осуществляет информирование руководства платежной организации о состоянии системы управления информационной безопасностью платежной организации.

**9.5. Программное обеспечение обеспечивает:**

- надежное хранение информации, защиту от несанкционированного доступа, целостность 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;
- многоуровневый доступ к входным данным, функциям, операциям, отчетам, реализованным в программном обеспечении, предусматривающим как минимум, два уровня доступа: администратор и пользователь;
- контроль полноты вводимых данных полей обязательных к заполнению, необходимых для проведения и регистрации операций (при выполнении функций или операций без полного заполнения всех полей программа обеспечивает выдачу соответствующего уведомления);
- поиск информации по критериям и параметрам, определенным для данной информационной системы, с сохранением запроса, а также сортировку информации по любым параметрам (определенным для данной информационной системы) и возможность просмотра информации за предыдущие даты, если такая информация подлежит хранению в информационной системе;
- обработку информации и ее хранение по дате и времени;
- автоматизированное формирование форм отчетов, представляемых платежными организациями в Национальный Банк, а также отчетов о проведенных операциях;

- ведение и автоматизированное формирование журналов системы внутреннего учета. Программное обеспечение формирует журнал полностью, а также частично (на указанный диапазон дат, определенную дату);
- возможность резервирования и восстановления данных, хранящихся в учетных системах;
- возможность вывода выходных документов на экран;
- 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.

**9.6. Процедуры безопасности**

**9.6.1.** В целях обеспечения безопасности предоставления Услуг, проведения Операций возможны только на карты, эмитированные банками на территории Республики Казахстан.

**9.6.2.** Предоставление Услуг производится в соответствии с процедурами безопасности, установленными настоящими Правилами и Договором.

**9.6.3.** ТОО «QAPITALA PAY» при оказании Услуг осуществляет сбор и обработку персональных данных с согласия субъекта персональных данных, за исключением случаев, предусмотренных Законом Республики Казахстан “О персональных данных и их защите”.

**9.6.4.** Процедуры безопасности обеспечивают:

- Достоверную идентификацию клиента и его право на получение соответствующих Услуг;
- Защиту от несанкционированного доступа к информации, составляющей банковскую тайну, и целостность данной информации.

**9.6.5.** Платеж является санкционированным, если он произведен лицом, которое имело полномочие совершить данный платеж, и не противоречит законодательству Республики Казахстан, а также при условии, если указание принято банком отправителя денег с соблюдением установленного порядка защиты действий от несанкционированных платежей.

**9.6.6.** Предоставление Услуг является санкционированным в случае выполнения клиентом процедур безопасности, установленных настоящими Правилами и Договором.

**9.6.7.** Несанкционированным является платеж, осуществленный без соблюдения требований, установленных законодательством, а также с использованием поддельных платежных инструментов.

**9.6.8.** В качестве элементов защиты действий используются идентификационные коды, шифрование и иные способы защиты, не противоречащие законодательству Республики Казахстан.

**9.6.9.** ТОО «QAPITALA PAY» осуществляет мониторинг за соблюдением клиентами требований к защите информации, определенных Договором и настоящими Правилами.

**9.7**. Платежная организация управляет рисками информационной безопасности с указанием критериев приемлемого уровня по отношению к информационным активам. При реализации рисков информационной безопасности разрабатывается план мероприятий, направленный на минимизацию возникновения подобных рисков.

**9.8.** Информация об инцидентах информационной безопасности, полученная в ходе мониторинга деятельности по обеспечению информационной безопасности, подлежит консолидации, систематизации и хранению.

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

Платежной организацией определяется порядок принятия неотложных мер к устранению инцидента информационной безопасности, его причин и последствий. В платежной организации ведется журнал учета инцидентов информационной безопасности с отражением всей информации об инциденте информационной безопасности, принятых мерах и предлагаемых корректирующих мерах.

**9.9.** Платежная организация предоставляет в Национальный Банк информацию о следующих выявленных инцидентах информационной безопасности:

- эксплуатация уязвимостей в прикладном и системном программном обеспечении;
- несанкционированный доступ в информационную систему;
- атака «отказ в обслуживании» на информационную систему или сеть передачи данных;
- заражение сервера вредоносной программой или кодом;
- совершение несанкционированного перевода денежных средств вследствие нарушения контролей информационной безопасности;
- инцидентах информационной безопасности, несущих угрозу стабильности деятельности платежной организации.

**9.10.** Информация об инцидентах информационной безопасности, указанных в пункте 15.9. настоящей главы, предоставляется платежной организацией в возможно короткий срок, **но не позднее 48 часов** с момента выявления, в виде карты инцидента информационной безопасности по форме согласно приложению 7 к Правилам №215.

Информация по обработанным инцидентам информационной безопасности представляется в электронном формате с использованием платформы Национального Банка для обмена событиями и инцидентами информационной безопасности.

На каждый инцидент информационной безопасности заполняется отдельная карта инцидента информационной безопасности.

**9.11.** Обязательства по обеспечению общей безопасности платежных услуг, защиты передаваемых данных и информации несет ТОО «QAPITALA PAY».

**9.12.** ТОО «QAPITALA PAY» обязуется соблюдать конфиденциальность в отношении всех переданных ему Мерчантами данных, а также данных, ставших ему известными в ходе использования ТОО «QAPITALA PAY» Покупателями/Клиентами, за исключением случаев предусмотренных Правилами и/или законодательством Республики Казахстан, а также случаев, когда такая информация является общеизвестной или раскрыта по требованию или с разрешения Мерчанта/Покупателя.

**9.13.** Мерчант обязуется незамедлительно уведомлять ТОО «QAPITALA PAY» о любых операциях, произведенных без его согласия. В случае непредоставления соответствующего уведомления в течении календарных суток с момента осуществления операции и направления ТОО «QAPITALA PAY» соответствующего уведомления, операция считается осуществленной Мерчантом.

**9.14.** Стороны признают сочетание аутентификационных данных (уникального идентификатора пользователя и пароля) аналогом собственноручной подписи, являющимся необходимым и достаточным условием подтверждения права Мерчанта на проведение Транзакций.

## 10. ОПИСАНИЕ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ И ОБОРУДОВАНИЯ, НЕОБХОДИМОГО ДЛЯ ОСУЩЕСТВЛЕНИЯ УСЛУГ

### 10.1 Техническое описание сервиса и используемые технологии:

- Платежный агрегатор функционирует на облачной платформе Servercore Kazakhstan;
- Инфраструктура размещена в одной зоне, расположенной на территории Казахстана;
- Бизнес-приложения развернуты в Kubernetes, обеспечивающем отказоустойчивость и масштабируемость;
- В качестве основной СУБД используется PostgreSQL; для обмена сообщениями применяется RabbitMQ;
- Управление инфраструктурой осуществляется по принципам Infrastructure as Code: для управления ресурсами используется HashiCorp Terraform, для конфигурации и оркестрации сервисов применяются Ansible и манифесты Kubernetes;
- Инфраструктура соответствует требованиям стандарта PCI DSS, что подтверждается ежегодной сертификацией аудитором;

### 10.2. Составляющие сервиса

Система представляет собой платформу для проведения платежей, обеспечения их безопасности, а также сбора и предоставления информации. Основные логические блоки:

- Администратор;
- Личный кабинет;
- Интерфейс пользователя (UI);
- Авторизация;
- API;
- Платежная форма;
- Логи.

### 10.3. Администратор

Функционал администратора и службы технической поддержки реализован через графический интерфейс. Возможности:

- Подключение / отключение пользователя;
- Просмотр данных клиента;
- Просмотр и изменение тарифов клиента;
- Просмотр и изменение настроек шлюза клиента;
- Управление настройками API-интеграций с партнерскими информационными системами (ИС);
- Настройка параметров маршрутизации.

### 10.4. Личный кабинет

Личный кабинет обеспечивает управление подключением и персональными настройками клиента:

- Регистрация на платформе;
- Авторизация;

- Идентификация пользователя;
- Пополнение кошелька банковской картой;
- Оплата сервисов;
- Вывод средств на банковскую карту;

### 10.5. Авторизация

Сервис реализует полный цикл авторизации владельца карты или кошелька с эмитентом:

- Запрос авторизационной сессии;
- Обмен авторизационными данными;
- Подтверждение авторизации;

### 10.6. API

Сервис предоставляет набор интерфейсов взаимодействия с партнерскими ИС. Поддерживаемый функционал:

- Запуск и подтверждение платежной сессии;
- Прохождение идентификации;
- Получение статуса сессии;
- Пополнение кошелька: наличными у агента, банковской картой, со счета лотереи;
- Оплата услуг с баланса кошелька;
- Предварительная проверка реквизитов и расчет комиссии;
- Вывод средств: через агента, наличными через агента с холдированием, на банковскую карту;
- Получение комиссий по банковской карте;
- Получение статуса операции;
- Получение баланса агента;
- Прямое пополнение мобильных операторов агентом;
- Получение персональных данных по кошельку;
- Токенизация банковской карты;

### 10.7. Платежная форма

Платежная форма позволяет плательщику оплатить счет, выставленный мерчантом, с помощью банковской карты.

### 10.8. Логи

Сервис ведет журналирование всех действий системы. Это позволяет:

- Оперативно выявлять и устранять сбои;
- Анализировать причины отказов;
- Повышать отказоустойчивость системы;
- Прогнозировать возможные сбои;
- Моделировать состояние системы при масштабировании и развитии;

### 10.9. Используемые технологии:

СУБД и хранилища:

- PostgreSQL;
- HashiCorp Vault;
- Elastic;

ПО для обработки сетевых запросов:

- Nginx;
- Suricata;
- Wazuh;

Языки и технологии разработки клиентских приложений:

- .NET;
- NodeJS;
- JavaScript;

## 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.

**11.2.** В случае несогласия Участника с изменениями и/или дополнениями в Правила или тарифами,

Участник вправе отказаться от дальнейшего использования услуг Платежной организации.

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