«**УТВЕРЖДЕНО»**

Приказом Директора

ТОО «Super Payment»

от 13 июля 2023 года

Тохунц Я.А.

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ -

ТОВАРИЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «SUPER PAYMENT»

Алматы, 2023 год

Оглавление
Глава 1 «Общие положения».
Глава 2 «Описание платежных услуг, оказываемых платежной организацией».
Глава 3 «Порядок и сроки оказания платежных услуг клиентам платежной организации».
Глава 4 «Стоимость платежных услуг (тарифы), оказываемых платежной организацией».
Глава 5 «Порядок взаимодействия с третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых платежной организацией».
Глава 6 «Сведения о системе управления рисками, используемой платежной организацией».
Глава 7 «Порядок урегулирования спорных ситуаций и разрешения споров с клиентами».
Глава 8 «Порядок информационной безопасности».
Глава 9 «Порядок принятия неотложных мер».
Глава 10 «Порядок соблюдения мер информационной безопасности».
Глава 11 «Правила и сроки предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах».
Глава 12 «Журнал учета инцидентов информационной безопасности».
Глава 13 «Сроки хранения информации».
Глава 14 «Описание программно-технических средств и оборудования, необходимого для осуществления платежных услуг».
Глава 15 «Заключительные положения».

1.Общие положения

1.1. Настоящие Правила осуществления деятельности Платежной организации - Товарищества с ограниченной ответственностью «Super Payment» разработаны в соответствии с Законом Республики Казахстан «О платежах и платежных системах» от 26 июля 2016 года № 11-VI, Правилами организации деятельности платежных организаций, утвержденными Постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 215 и иными нормативно-правовыми актами Республики Казахстан.

1.2. Правила определяют единые условия (правила) оказания Платежной организацией платежной услуги, при наличии регистрационного номера учетной регистрации, присвоенного Национальным Банком Республики Казахстан, по обработке платежей, инициированных Клиентом в электронной форме, и передаче необходимой информации Банку-партнеру для осуществления платежа и (или) перевода либо принятия денег по данным платежам.

1.3. Платежная организация может расширить виды оказываемых платежных услуг в порядке, предусмотренном законодательством Республики Казахстан и после внесения соответствующих изменений в Правила.

1.4. Правила публикуются на веб-сайте Платежной организации по адресу: www.superpayment.com.kz.

1.5. Платежная организация по мере необходимости имеет право вносить изменения и дополнения в Правила путем утверждения и публикации ее новой редакции на веб-сайте Платежной организации.

Термины и определения

1.6. В Правилах используются следующие понятия:

Платежная организация – Товарищество с ограниченной ответственностью «Super Payment», которая является платежной организацией, прошедшей учетную регистрацию в Национальном Банке Республики Казахстан 30.12.2019 года под № 01-19-067, которая вправе оказывать платежные услуги, предусмотренные подпунктом 8) пункта 1 статьи 12 Закона Республики Казахстан «О платежах и платежных системах» (далее - Закона о платежах) и подпунктом 4) пункта 2 статьи 13 Закона о платежах и пунктом 12-1 Правил организации деятельности платежных организаций, утвержденные постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года №215.

Мерчант – 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.

Клиент – физическое лицо, обладающее надлежащей дееспособностью в соответствии с законодательством Республики Казахстан для осуществления Платежа.

web-сайт Платежной организации - Сайт, размещенный в сети Интернет по электронному адресу: www.superpayment.com.kz.

Система платежей (далее – «**Система**») – совокупность программно-технических средств Платежной организации, обеспечивающих информационно-технологическое взаимодействие между участниками расчетов, включая оказание услуг по сбору, обработке и рассылке информации участникам расчетов по операциям с платежными карточками.

Товар – товары, работы, услуги, права на результаты интеллектуальной собственности, реализуемые Мерчантами конечным потребителям (Клиентам) для личного, семейного или

домашнего использования.

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.).

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.

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

2. Описание Платежной услуги, оказываемой 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.

2.2. Платежная организация размещает информацию о действующем Банке-партнере на веб-сайте Платежной организации.

3. Порядок и сроки оказания Платежных услуг клиентам платежной организации

3.1 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), платежной страницы, виджетов - 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, персонального компьютера заходит в соответствующее приложение или платежную страницу 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, и т.д.;
— Клиент инициирует платеж в пользу Мерчанта;
— 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).

3.2. Описание детализированной схемы движения денег и информационных потоков:

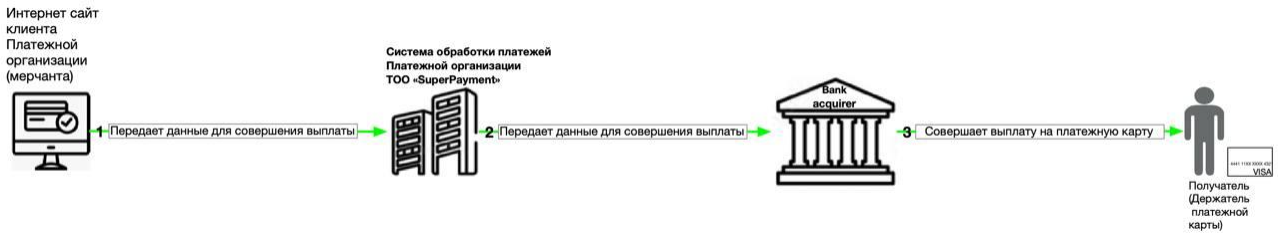
Схема информационных потоков с интернет-магазинами:

1. Плательщик совершает покупку в интернет магазине предпринимателя
2. Для оплаты интернет магазин предпринимателя переадресовывает на платежную страницу Платежной организации
3. Плательщик вводит данные платежной карты на платежной странице Платежной организации
4. Платежные данные принимаются системой обработки платежей Платежной организации
5. Система обработки платежей Платежной организации передает платежные данные Банку эквайеру

6. Банк эквайер передает ответ о успешной оплате системе обработки платежей Платежной организации
7. Система обработки платежей Платежной организации сообщает плательщику на платежной странице о успешной оплате
8. Система обработки платежей Платежной организации сообщает интернет-магазину предпринимателя о успешной оплате

Схема информационных потоков с микрокредитными организациями:

- выплаты кредитов:



1. Мерчант на своем сайте производит скоринг и согласовывает выдачу микрозайма заемщику.
2. Мерчант инициирует перед Платежной организации запрос о необходимости выдачи средств Заемщику с корпоративной карты Мерчанта
3. Платежная организация передает информацию в банк эквайер для осуществления выдачи средств по микрозайму заемщику
4. Банк эквайер исполняет запрос мерчанта по отправке средств с корпоративной карты мерчанта на платежную карту заемщика мерчанта.

- погашение кредитов:

1. Плательщик совершает погашение кредита на сайте мерчанта
2. Для погашения кредита мерчант с своего сайта переадресовывает на платежную страницу Платежной организации
3. Плательщик вводит данные платежной карты на платежной странице Платежной организации
4. Платежные данные принимаются системой обработки платежей Платежной организации
5. Система обработки платежей Платежной организации передает платежные данные Банку эквайеру
6. Банк эквайер передает ответ о успешной оплате системе обработки платежей Платежной организации
7. Система обработки платежей Платежной организации сообщает плательщику на платежной странице о успешной оплате

8. Система обработки платежей Платежной организации сообщает интернет-магазину предпринимателя о успешной оплате

Схема движения денег:

1. Банк эмитент карты плательщика со счета плательщика отправляет сумму платежа в платежную систему
2. Платежная система отправляет сумму платежа Банку эквайеру
3. Банк эквайер отправляет сумму платежа на транзитный счет
4. Банк эквайер с транзитного счета отправляет сумму платежа Предпринимателю (Мерчанту)

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

4. Стоимость платежных услуг (тарифы), оказываемых платежной организацией

Тарифы платежной организации ТОО «Super Payment» по платежным услугам:

4.1 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:

- Стоимость платы, (допустимой дополнительной комиссии), взимаемой с Клиента устанавливается в соответствии с договорными условиями, указанными в договорах, заключенных между ТОО «Super Payment» 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.

5. Порядок взаимодействия с третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых платежной организацией

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

Правилами.

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

5.3 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.

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

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

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

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

5.8 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.
- API и прочая техническая информация, необходимая для построения взаимодействия с Платежной организации для систем третьих сторон является открытой и предоставляется им по запросу.

5.9 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).

6. Сведения о системе управления рисками, используемой платежной организацией

6.1 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.
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.

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.

6.2 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.

7. Порядок урегулирования спорных ситуаций и разрешения споров с клиентами

7.1 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 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 – 050026, ГОРОД АЛМАТЫ, АЛМАЛИНСКИЙ РАЙОН, УЛ. МУКАНОВА, Д. 223Б;
2. путем личного обращения в офис Платежной организации и ее нарочным предоставлением по адресу: 050026, ГОРОД АЛМАТЫ, АЛМАЛИНСКИЙ РАЙОН, УЛ. МУКАНОВА, Д. 223Б.
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 оплате (квитанция).
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.

8. Порядок информационной безопасности

8.1. Порядок разработан с целью определения основных принципов и направлений в области информационной безопасности и охватывает все бизнес-процессы, информационные системы и документы, владельцем и пользователем которых является Платежная организация.

8.2. Целью деятельности по управлению информационной безопасностью в Платежной организации является обеспечение защиты информационных активов Платежной организации и минимизация ущерба от событий, таящих угрозу безопасности информации.

8.3. Задачами деятельности по управлению информационной безопасностью в Платежной организации являются:

– категорирование информационных активов путем разделения их на критичные и некритичные на основании максимального уровня критичности, хранимой и обрабатываемой в них информации;

– своевременное выявление потенциальных угроз информационной безопасности и

уязвимостей в информационных активах Платежной организации;

– исключение либо минимизация выявленных угроз;

– предотвращение инцидентов информационной безопасности или минимизация их последствий.

8.4. Основными мерами защиты конфиденциальности, целостности и доступности информационных активов Платежной организации являются:

– управление сетевой безопасностью;

– управление уязвимостями и политиками безопасности;

– управление безопасностью конечных устройств;

– управление идентификацией и доступом;

– управление инцидентами информационной безопасности;

– управление криптографическими средствами защиты;

– управление антивирусными средствами защиты;

– обеспечение физической безопасности информационных активов;

– обеспечение безопасности при взаимодействии с контрагентами;

– обучение и повышение осведомленности персонала в вопросах ИБ;

– обеспечение безопасности интернет-ресурсов.

8.5. Платежная организация обеспечивают создание и функционирование системы управления информационной безопасностью, являющейся частью общей системы управления Платежной организации, предназначенной для управления процессом обеспечения информационной безопасности. Система управления информационной безопасностью обеспечивает защиту информационных активов Платежной организации, допускающую минимальный уровень потенциального ущерба для бизнес-процессов организации.

8.6. Построение системы управления информационной безопасности в Платежной организации и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

– законность – любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе действующего законодательства РК и ВНД Платежной организации, с применением всех дозволенных законодательством методов обнаружения, предупреждения, локализации и пресечения негативных воздействий на объекты защиты информации Платежной организации;

– ориентированность на бизнес – информационная безопасность рассматривается как процесс поддержки бизнес-процессов в Платежной организации. Любые меры по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий деятельности Платежной организации;

– непрерывность – применение средств управления системами защиты информации, реализация любых мероприятий по обеспечению информационной защиты Платежной организации должны осуществляться без прерывания или остановки текущих бизнес-процессов Платежной организации;

– комплексность – обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их использования и во всех режимах функционирования;

– обоснованность и экономическая целесообразность – используемые возможности и средства защиты должны быть реализованы на соответствующем уровне развития науки и техники, обоснованы с точки зрения заданного уровня безопасности и должны соответствовать предъявляемым требованиям и нормам;

– приоритетность – категорирование (ранжирование) всех информационных ресурсов организации по степени критичности на основании максимального уровня критичности хранимой и обрабатываемой в них информации, а также потенциальных угроз информационной безопасности;

– необходимое знание и наименьший уровень привилегий – пользователь получает минимальный уровень привилегий и доступ только к тем данным, которые являются необходимыми для выполнения им функциональных обязанностей в рамках своих

полномочий;

– специализация – эксплуатация технических средств и реализация мер информационной безопасности должны осуществляться профессионально подготовленными работниками Платежной организации;

– информированность и персональная ответственность – руководители всех уровней и работники Платежной организации должны быть осведомлены обо всех требованиях информационной безопасности и несут персональную ответственность за выполнение этих требований и соблюдение установленных мер информационной безопасности;

– взаимодействие и координация – меры информационной безопасности осуществляются на основе взаимосвязи соответствующих структурных подразделений Платежной организации, координации их усилий для достижения поставленных целей, а также установления необходимых связей с внешними организациями, профессиональными ассоциациями и сообществами, государственными органами, юридическими и физическими лицами;

– подтверждаемость – критичная документация и все записи – документы, подтверждающие исполнение требований по информационной безопасности и эффективность системы ее организации, должны создаваться и храниться с возможностью оперативного доступа и восстановления.

8.7. Платежная организация разрабатывает внутренние процедуры по созданию, сбору, хранению и обработке информации в информационных системах организации. Платежная организация осуществляет мониторинг за процессами создания, хранения и обработки информации и доступа к ней с помощью механизмов информационных систем и технических средств обеспечения безопасности. Доступ к создаваемой, хранимой и обрабатываемой информации в информационных системах Платежной организации предоставляется работникам в соответствии с их функциональными обязанностями в соответствии с принципом наименьшего уровня привилегий.

8.8. Участниками системы управления информационной безопасностью Платежной организации являются:

1) Руководители Платежной организации;
2) Комитет по информационной безопасности (далее – УКО);
3) подразделение информационной безопасности;
4) подразделение по информационным технологиям;
5) подразделение по безопасности;
6) подразделение по работе с персоналом;
7) подразделение правового сопровождения Платежной организации;
8) подразделение комплаенс и внутреннего контроля;
9) подразделение внутреннего аудита;
10) подразделение по управлению рисками ИТ и информационной безопасности.

8.9. Руководители утверждает перечень защищаемой информации, включающий в том числе информацию о сведениях, составляющих служебную, коммерческую или иную охраняемую законом тайну (далее – защищаемая информация), и порядок работы с защищаемой информацией.

8.10. Руководители утверждает внутренние документы, регламентирующие процесс управления информационной безопасностью, порядок и периодичность пересмотра которых определяется Инструкцией по управлению внутренними нормативными документами.

8.11. Платежная организация создаёт УКО, в состав которого входят представители подразделения по информационной безопасности, подразделения по управлению рисками информационной безопасности, подразделения по информационным технологиям, а также при необходимости представители других подразделений Платежной организации.

8.12. УКО осуществляет периодический мониторинг деятельности по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности не реже раза в год. Процесс мониторинга деятельности по обеспечению информационной

безопасности, мероприятий по выявлению и анализу угроз, а также противодействию атакам должен включать отчёт по выявлению, анализу угроз и противодействию атакам на основе данных, предоставленных подразделением информационной безопасности по количеству выявленных угроз, принятых мер и произошедших инцидентов информационной безопасности. Мониторинг мероприятий по расследованию инцидентов информационной безопасности включает в себя оценку последствий инцидентов, указание причин и планов мероприятий по предотвращению, либо уменьшению влияния инцидентов информационной безопасности.

8.13. Подразделение информационной безопасности проводит мониторинг событий информационной безопасности и управления инцидентами информационной безопасности, в рамках которого определяется перечень событий информационной безопасности, подлежащих мониторингу, источники событий, периодичность, правила мониторинга и их методы. Подразделение информационной безопасности, осуществляющее мониторинг, вправе вводить дополнительные контроли, частичную или полную остановку бизнес-процесса в случае выявления инцидента информационной безопасности.

8.14. Перечень событий информационной безопасности, подлежащих мониторингу, источники событий, периодичность, правила мониторинга и их методы пересматриваются подразделением информационной безопасности не реже одного раза в год с учетом имеющейся статистики и эффективности мониторинга.

9. Порядок принятия неотложных мер

9.1. Порядок управления инцидентами информационной безопасности определяется соответствующим пунктом данных Правил Платежной организации и содержит в себе положения по консолидации, систематизации и хранению информации об инцидентах информационной безопасности, порядки отнесения события информационной безопасности к инцидентам информационной безопасности, последующего анализа инцидента информационной безопасности и информирования о произошедшем инциденте информационной безопасности.

9.2. Процесс консолидации, систематизации и хранения информации об инцидентах информационной безопасности должен обеспечивать целостность, доступность и конфиденциальность, а также полноту данных об инциденте, достаточных для осуществления анализа инцидента, проведения служебных проверок и формирования отчетности, предусмотренной Постановлением №48.

9.3. Руководитель Платежной организации осуществляет стратегическое планирование, координацию деятельности всех подразделений Платежной организации для организации и поддержания соответствующего уровня информационной безопасности.

9.4. Руководитель подразделения информационной безопасности обеспечивает разработку, внедрение и совершенствование документированных стандартов и процедур в области информационной безопасности.

9.5. Подразделение информационной безопасности обеспечивает своевременное проведение анализа информации об инцидентах информационной безопасности, который должен включать в себя раскрытие обстоятельств события, при которых стала возможна реализация инцидента информационной безопасности, взаимодействие с подразделением по управлению рисками информационной безопасности, при необходимости, формирование рекомендаций по внедрению защитных мер.

9.6. Подразделение по информационным технологиям обеспечивает исполнение установленных требований по непрерывности функционирования информационной инфраструктуры, конфиденциальности, целостности и доступности данных информационных систем Банка (включая резервирование и (или) архивирование и резервное копирование информации) в соответствии с ВНД Платежной организации, а также обеспечивает соблюдение требований информационной безопасности при выборе, внедрении, разработке и тестировании информационных систем.

9.7. Подразделение по управлению рисками информационной безопасности отвечает за осуществление категорирования информационных активов путем разделения их на критичные и некритичные на основании максимального уровня критичности хранимой и обрабатываемой в них информации.

9.8. Подразделение по безопасности реализует меры физической и технической безопасности, в том числе организует пропускной и внутриобъектовый режим, а также проводит профилактические мероприятия, направленные на минимизацию рисков возникновения угроз информационной безопасности при приеме на работу и увольнении работников Банка.

9.9. Подразделение по работе с персоналом обеспечивает подписание работниками банка, а также лицами, привлеченными к работе по договору об оказании услуг, стажерами, практикантами обязательств о неразглашении конфиденциальной информации, а также участвует в организации процесса повышения осведомленности работников Банка в области информационной безопасности.

9.10. Юридическое подразделение осуществляет правовую экспертизу ВНД и внутренних документов Платежной организации по вопросам обеспечения информационной безопасности, в соответствие с Инструкцией по управлению внутренними нормативными документами.

9.11. Подразделение по комплаенс-контролю совместно с юридическим подразделением Платежной организации, определяет виды информации, подлежащие включению в перечень защищаемой информации.

9.12. Подразделение внутреннего аудита проводит оценку состояния системы управления информационной безопасностью Платежной организации при проведении аудиторских проверок.

9.13. Бизнес-владельцы информационных систем или подсистем отвечают за соблюдение требований к информационной безопасности при создании, внедрении, модификации, предоставлении клиентам продуктов и услуг, а также формируют и поддерживают актуальность матриц доступа к информационным системам.

10. Порядок соблюдения мер информационной безопасности

10.1. Порядок соблюдения мер информационной безопасности в Платежной организации (далее по тексту - Порядок) покрывает следующие области Платежной организации:

- услуги, предоставляемые Платежной организацией в соответствии с договорами, заключенными с контрагентами;
- внутренние процессы, регламентированные в Платежной организации;
- персонал – работники Платежной организации;
- третьи стороны, имеющие доступ к Системе Платежной организации;
- информационные ресурсы Платежной организации, хранящие и обрабатывающие информацию.

10.2. Целью Порядка является построение эффективной системы управления информационной безопасностью Платежной организации.

10.3. Порядок основан на следующих принципах:
1) обеспечение и поддержание соответствующего уровня целостности, доступности и конфиденциальности критичной информации;
2) соответствие требованиям законодательства Республики Казахстан;
3) экономическая целесообразность.

10.4. 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», а также рекомендации Международных платежных систем;

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.

10.5. 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 Порядка.

10.6. 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.

10.7. Должностные инструкции каждого работника Платежной организации, а так же документы описывающие отношения с третьими сторонами, банками, контрагентами, Мерчантами содержат требования по обеспечению и соблюдению информационной безопасности.

11. Правила и сроки предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах

11.1. Настоящие Правила и сроки предоставления информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах (далее – Правила) разработаны в соответствии с пунктом 7 статьи 61-5 Закона Республики Казахстан "О банках и банковской деятельности в Республике Казахстан" и определяют порядок и сроки предоставления организациями, осуществляющими отдельные виды банковских операций (далее – организация), информации об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах.

11.2. В Правилах используются понятия, предусмотренные Законом Республики Казахстан "Об информатизации", а также следующие понятия:

1) информационная безопасность в сфере информатизации (далее – информационная безопасность) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

2) информационно-коммуникационная инфраструктура (далее – информационная инфраструктура) – совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;

3) угроза информационной безопасности – совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;

4) информация об инцидентах информационной безопасности – информация об отдельно или серийно возникающих сбоях в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающих угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов банка, организации;

5) инцидент информационной безопасности – отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов банка, организации;

6) доступ – возможность использования информационных активов;

7) атака типа "отказ в обслуживании" (DoS или DDoS-атака, в зависимости от количества атакующих внешних источников атаки) – атака на информационную систему с целью нарушения штатного режима ее работы или создание условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым ресурсам, либо этот доступ затруднен;

8) уполномоченный орган – уполномоченный орган по регулированию, контролю и надзору финансового рынка и финансовых организаций.

11.3. Платежная организация предоставляют в уполномоченный орган 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) иных инцидентах информационной безопасности, повлекших простои информационных систем более одного часа.

11.4. Информация об инцидентах информационной безопасности, указанных в настоящем пункте, предоставляется организацией незамедлительно посредством автоматизированной системы уполномоченного органа, предназначенной для обработки информации о событиях и инцидентах информационной безопасности и интегрированной с системами информационной безопасности или системами организации, осуществляющими в реальном времени сбор и анализ информации о событиях в информационной инфраструктуре (далее – АСОИ) или в электронном формате с использованием транспортной системы гарантированной доставки информации с криптографическими средствами защиты, обеспечивающей конфиденциальность и некорректируемость представляемых данных.

11.5. Организация обеспечивают передачу сведений об отдельно или серийно возникающих событиях в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, включая системы информационной безопасности, свидетельствующих о нарушении принятых мер обеспечения информационной безопасности либо о ранее неизвестной ситуации, потенциально имеющей отношение к информационной безопасности (далее – сведения о нарушениях, сбоях в информационных системах) посредством АСОИ. Сведения о нарушениях, сбоях в информационных системах предоставляются в автоматизированном режиме путем передачи из систем информационной безопасности или систем организации, осуществляющих в реальном времени сбор и анализ информации о событиях в информационной инфраструктуре банка, организации.

12. Журнал учета инцидентов информационной безопасности

Согласно Постановления Национального Банка Республики Казахстан от 31 августа 2016 года № 215 Об утверждении Правил организации деятельности платежных организаций, главы 6. Требования к программно-техническим средствам платежных организаций и системе управления информационной безопасностью ст. 43. в платежной организации ведется журнал учета инцидентов информационной безопасности с отражением всей информации об инциденте информационной безопасности, принятых мерах и предлагаемых корректирующих мерах.

ЖУРНАЛ УЧЕТА ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Форма Журнала учета инцидентов информационной безопасности

№	Дата инцидента	№, дата справки или акта по результатам расследования или краткое содержание инцидента	ФИО проверяющего	Подпись проверяющего

13. Сроки хранения информации

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

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

14. Описание программно-технических средств и оборудования, необходимого для оказания Платежной организацией Платежной услуги

14.1. Программно-технические средства и оборудование, используемые Платежной организацией при оказании Платежной услуги посредством Системы обеспечивают:

1) 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;

2) многоуровневый доступ к входным данным, функциям, операциям, отчетам, реализованным в программном обеспечении, предусматривающим как

минимум, два уровня доступа: администратор и пользователь;

3) 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);

4) 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;

5) обработку информации и ее хранение по дате и времени;

6) автоматизированное формирование форм отчетов, представляемых платежными организациями в Национальный Банк Республики Казахстан, а также отчетов о проведенных операциях;

7) ведение и автоматизированное формирование журналов системы внутреннего учета. Программное обеспечение формирует журнал полностью, а также частично (на указанный диапазон дат, определенную дату);

8) возможность резервирования и восстановления данных, хранящихся в учетных системах;

9) возможность вывода выходных документов на экран, принтер или в файл;

10) возможность обмена электронными документами;

11) 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.

14.2. Платежная организация с учетом уровня развития технологий определяет и устанавливает минимальные требования к составу аппаратных средств; к оборудованию для веб- приложения; к сети; к поддерживаемым веб-браузерам. Указанные минимальные требования доводятся третьим лицам при установлении деловых отношений.

15. Заключительные положения

15.1. Ответственность за неисполнение/ненадлежащее исполнение требований Правил, а также за обеспечение информационной безопасности при исполнении возложенных на них функциональных обязанностей несут все работники Платежной Организации.
15.2. Контроль за исполнением требований, устанавливаемых Правилами, возлагается на УКО.
15.3. Правила вступают в силу на следующий рабочий день после внесения в БД ВНД и является общеобязательной к применению и руководству всеми работниками Платежной Организации, а также доводится до сведения третьих лиц, имеющих доступ к информационным активам Платежной Организации.
15.4 Вопросы, не урегулированные Правилами, разрешаются в соответствии с законодательством Республики Казахстан и ВНД.