**УТВЕРЖДЕНЫ**

**Директором Товарищества**
**с ограниченной ответственностью**
**«Мобильный портал»**

**Альмухамбетова Ш.К.**_____

**Дата 17 марта 2023 год**

# Правила платежной организации ТОО «Мобильный портал»

**г. Алматы, 2023 г.**

**Содержание:**

## Введение

1. Настоящие Правила деятельности платежной организаций (далее – Правила) разработаны в соответствии с законом Республики Казахстан от 26 июля 2016 года «О платежах и платежных системах» (далее – Закон о платежах) и определяют порядок организации деятельности платежной организации и представляют собой документ, устанавливающий порядок осуществления переводов денег в системе, порядок взаимодействия мерчантов Системы QIT с ее Оператором, условия участия в системе и другие условия, определенные настоящими Правилами.

2. Разработанные Правила направлены на обеспечение бесперебойного функционирования системы.

3. Правила системы разрабатывает и вводит в действие оператор системы. Регулирование организационного и технологического взаимодействия между мерчантами системы, установление стандартов безопасности и управление рисками является исключительной прерогативой оператора системы. Требования в названных областях являются одинаковыми для всех субъектов Системы.

4. Оператором Системы QIT является Товарищество с ограниченной ответственностью «Мобильный портал», БИН 141240003309, зарегистрированное по адресу: г.Алматы, улица Тимирязева, дом 42.

*Оператор намерен оказывать:*

- *услуги по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации участникам рынка, для осуществления платежа и (или) перевода либо принятия денег по данным платежам Оператором.*
- *услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег*.

## Термины и определения

5. Для целей настоящих Правил Системы используются следующие термины и определения:

**Баланс** – сумма, находящаяся на виртуальном счете Мерчанта в Системе, обеспечивает проведение платежей от Мерчанта в пользу Поставщика. Сумма Баланса определяется как сумма поступившего обеспечения платежей в виде банковского(–их) перевода(–ов) по оказанным Услугам, за минусом суммы проведенных транзакций.

**Виртуальный счет** – счет Мерчанта в Системе, на котором отражаются все финансовые транзакции в Системе, приходы и расходы.

**Клиент** – физическое или юридическое лицо, филиал или представительство юридического лица, получающие услугу Поставщика.

**Клиринговый центр** – Товарищество с ограниченной ответственностью «Мобильный портал», обеспечивающее в рамках системы сбор, сверку и зачет взаимных денежных требований и обязательств.

**Мерчант** – участник системы – юридическое лицо, заключившее с организацией договор об аутсорсинге по оказанию услуг сбора и передаче платежей посредством Системы QIT.

**Оператор системы** – Товарищество с ограниченной ответственностью «Мобильный портал», осуществляющее деятельность по обеспечению функционирования Системы QIT, а также ответственное за технологическое обеспечение своих услуг.

**Поставщик услуг** – субъект рынка, непосредственно оказывающий услугу ее потребителям (конечным пользователям, то есть клиентам).

**Каналы продаж** – территория, на которой Платежная организация, в том числе через своих Мерчантов, осуществляет прием платежей с использованием, касс, специализированных кассовых устройств, терминалов самообслуживания (специализированных автоматов по приему платежей), а также область пространства сети Интернет, в которой Платежная организация, ее Мерчант осуществляет прием платежей с использованием специализированного программного обеспечения.

**Реестр платежей** – документ или совокупность документов, содержащих информацию, необходимую для осуществления расчетов в рамках Системы QIT за определенный период времени, составляемый и предоставляемый Оператором системы в электронной форме.
**Система** – система QIT.
**Субъекты системы** – мерчанты, клиенты.

## Раздел 1. Описание платежных услуг, оказываемых платежной организацией

6. Оператор намерен оказывать следующие услуги:
   - услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег;
   - 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.

Услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег оказываются Платежной организацией на основании договоров, заключаемых Платёжной организацией с поставщиками различного рода услуг. Условия данных договоров предусматривают возможность привлечения к оказанию услуг мерчантов, на основании договора, заключаемого между платежной организацией и мерчантом. Услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег, оказываются по средством внесения плательщиком наличных денежных средств через терминалы, принадлежащие мерчантам.

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

## Раздел 2. Порядок и сроки оказания платежных услуг клиентам платежной организации

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

7. Условия оказания платежной 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. Мерчанту необходимо иметь:
   - зарегистрированное юридическое лицо;
   - расчетный счет, открытый в любом банке второго уровня РК;
   - работающий интернет-сайт, который должен иметь: API-интерфейс для сопряжения с внешними системами, предотвращение несанкционированного доступа к информации и/или передачи ее лицам, не имеющим права на доступ к информации,

применение механизмов обнаружения попыток вторжения на интернет-сайт и получения несанкционированного доступ, не должен предоставлять услуги «развлечений для взрослых», наличие актуальной справочной информации о Мерчанте. Обязательным условием является наличие наименования страны, адреса места нахождения, адреса для корреспонденции, а также номера контактных телефонов, по которым клиент может связаться со службой поддержки интернет-сайта.

- входные данные от Мерчанта: контактные данные, документы в целях надлежащей проверки клиента в соответствии с внутренними документами и требованиями законодательства Республики Казахстан, а также ссылка на интернет-сайт Мерчанта (URL-адрес). В целях подписания Договора об оказании платежных услуг Мерчанта предоставляет информацию и документы согласно требованиям внутренних документов Платежной организации.

8. Для подключения к Системе, Мерчанту необходимо направить письмо в адрес Платежной организации с содержанием адреса веб-сайта Мерчанта, номера телефона и электронного адреса контактного лица. После проведения проверки пакета документов, представленных Партнером и подписания договора, в административной панели Системы создается доступ для Мерчанта в виде Личного кабинета.

9. Мерчант должен предоставить следующий пакет документов, который подписан уполномоченным представителем Мерчанта и заверен печатью. При необходимости Платежная организация может запросить дополнительные документы. Перечень документов:

- документ, выданный уполномоченным органом, подтверждающим факт прохождения государственной регистрации (перерегистрации) юридического лица;
- документы, удостоверяющие личность либо подтверждающие факт прохождения государственной регистрации (перерегистрации) учредителей (участников) юридического лица (за исключением документов учредителей (участников) акционерных обществ, а также хозяйственных товариществ, ведение реестра участников которых осуществляется единым регистратором), а также документы, удостоверяющие личность бенефициарных собственников юридического лица (за исключением случаев, когда бенефициарный собственник является учредителем (участником) юридического лица и выявлен на основании выписки из реестра акционеров (участников);
- документы, подтверждающие полномочия должностного(-ых) лица (лиц) на совершение действий от имени клиента без доверенности, в том числе на подписание документов юридического лица на совершение операций с деньгами и (или) иным имуществом.

10. Перевод денег в Системе QIT осуществляется в валюте Республики Казахстан. Перевод денег в Системе осуществляется в форме безналичных расчетов – расчетов платежными поручениями. Перевод денег осуществляется с использованием внутрибанковского транзитного счета и банковских счетов Мерчентов системы. Перевод представлен в следующих формах:

– Перевод денег Оператору системы от Мерчанта осуществляется за счет денег, находящихся на банковском счете Мерчента посредством расчета платежными поручениями на внутрибанковский транзитный счет Оператора.

– Перевод денег Поставщику услуг от Оператора системы осуществляется за счет денег, находящихся на внутрибанковском транзитном счете посредством расчета платежными поручениями. Платежные поручения при этом формируется Оператором системы.

– Оператор принимает деньги **только** от Мерчентов, с которыми заключены договора, и **только** посредством безналичного расчета платежными поручениями на внутрибанковский транзитный счет.

11. Порядок приема платежей Клиентов по платежным карточкам Visa, MasterCard и других:

- Клиент Мерчанта со страницы его интернет-сайта переходит на страницу оплаты в Системе.
- Клиент Мерчанта вводит реквизиты платежной карточки (тип платежной карточки, имя держателя платежной карточки, номер, срок действия, CVV).

Оказание Услуги по типу авторизации (при выборе Мерчанта):

- *одностадийная*, Платежная организация передает Банку информацию о списании заявленной суммы с платежной карточки плательщика, после чего Банк-эквайер передает информацию Банку-эмитенту, Банк-эмитент списывает сумму с платежной карточки клиента, далее Банк-эквайер зачисляет сумму на Транзитный счет Банка, предназначенный для проведения расчетов с Мерчантами.
- *двустадийная,* Платежная организация передает Банку информацию о блокировке указанной суммы и Банк-эквайер блокирует сумму на платежной карточке клиента Мерчанта. Далее, если Мерчант подтверждает операцию, в этом случае Платежная организация передает Банку информацию о списании указанной суммы с платежной карточки клиента Мерчанта и Банк-эквайер передает информацию Банку- эмитенту, Банк-эмитент списывает сумму с платежной карточки клиента Мерчанта. Платежная организация получает от Банка подтверждение исполнения Операции, и выдает Клиенту электронный чек, подтверждающий совершение Клиентом операции. При не подтверждении Мерчантом операции, Платежная организация не передает Банку информацию о списании суммы и Банк-эмитент не списывает сумму с платежной карточки клиента Мерчанта.

12. Схема движения денег и информационных потоков в системе следующая:

12.1. Инициирование платежа. Плательщик в целях оплаты за Услуги на интернет-сайте Мерчанта выбирает сервис (платежное решение), представленное Платежной организацией «оплатить карточкой»

12.2. Переход с сайта Мерчанта на платежную страницу. После выбора производится переключение на платежную страницу Платежной организации.

12.3. Заполнение реквизитов**.** На платежной странице Плательщик осуществляет заполнение реквизитов платежной карточки для осуществления платежа. АПК осуществляет обработку информации с дальнейшей ее передачей в сторону банка для проведения платежа. В случае необходимости ввода 3D SecureCode/SMS Code клиент перенаправляется на страницу Банка-эмитента Платежной карточки для ввода 3D SecureCode/SMS Code. В случае отсутствия у Банка-эмитента требования по вводу 3D SecureCode/SMS Code банк осуществляет обработку транзакции.

12.4. Введение 3D SecureCode/SMS Code. По результатам успешного ввода клиентом 3D SecureCode/SMS Code либо в случае отсутствия у Банка-эмитента требований по 3D SecureCode/SMS Code банк осуществляет обработку транзакции. Обработка транзакций (одностадийная или двустадийная авторизация согласно п.11 настоящих Правил).

12.5. Завершение операционного дня. По итогам операционного дня Платежная организация направляет реестр платежей банку для завершения расчетов с Мерчантами (перевод денег на банковский счет Партнера с транзитного счета, открытого в банке). По операциям, проведенным в течение предыдущего операционного дня, Платежная организация направляет отчетный реестр Мерчанту по платежам, проведенным в его пользу посредством автоматизированной системы по формированию отчетов. В случае возврата отказа Клиентом от Услуги, Мерчант инициирует проведение Операции возврата в Личном кабинете либо действует согласно положениям заключенного с Платежной организацией договора. Платежная организация обеспечивает хранение информации в электронном виде по всем совершенным операциям в течение 5-ти лет от даты прекращения деловых отношений с Мерчантом.

Платежная организация на периодической основе - один раз в сутки, и в соответствии с Правилами осуществляет Обработку Операций, совершенных с момента предыдущего цикла Обработки Операций. Обмен информацией осуществляется Платежной организацией с банком, Мерчантом в соответствии с положениями соответствующих договоров. По результатам обработки Операций за Операционный день Платежная организация направляет отчет.

12.6. Подтверждение оказания платежных услуг Клиенту**.** В качестве подтверждения оказания платежной услуги Клиенту, Платежная организация посредством Системы формирует для Клиента электронную квитанцию, которая в обязательном порядке должна содержать информацию, установленную Законом о платежах и платежных системах и Правилами № 215. Допускается проставление Платежной организацией в документе, подтверждающем факт оказания платежной услуги, дополнительных реквизитов по оказанной платежной услуге.

*Порядок оказания услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег.*

13. Прием наличных денег для осуществления платежа без открытия банковского счета отправителя денег в пользу поставщиков услуг происходит путем внесения физическим лицом денежных средств через каналы продаж платежной организации. По окончании платежа выдается документ, подтверждающий платеж, соответствующий требованиям законодательства Республики Казахстан.

14. Клиент передает наличные средства без открытия банковского счета Мерченту системы, который работает в системе QIT посредством платежных терминалов самообслуживания, специализированные жд-отделения. Далее Мерчент осуществляет перевод денег в форме безналичного платежа (расчета платежными поручениями) на внутрибанковский транзитный счет Оператора. Перевод денег осуществляется с использованием внутрибанковского транзитного счета и банковских счетов Мерчентов системы. Перевод представлен в следующих формах:

- Перевод денег Оператору системы от Мерчанта осуществляется за счет денег, находящихся на банковском счете Мерчента посредством расчета платежными поручениями на внутрибанковский транзитный счет Оператора.
- Перевод денег Поставщику услуг от Оператора системы осуществляется за счет денег, находящихся на внутрибанковском транзитном счете посредством расчета платежными поручениями. Платежные поручения при этом формируется Оператором системы.

15. Детализированная схема движения денег и информационных потоков по платежной услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег представлена следующим образом:

15.1. Мерчант заключает с Платежной организацией (либо как с платежным агентом) договор об оказании платежных услуг.

15.2. Мерчант проходит регистрацию в Системе по учету платежей, с присвоением уникального номера (ID), в связи с чем в согласованный сторонами договора срок Мерчант осуществляет подключение к Системе Платежной организации. Сторонами определяется техническая готовность систем к отправке Мерчантом информации о платежах Платежной организации посредством технического тестирования.

15.3. Оказание платежной услуги обеспечивается по соглашению сторон заключенного договора предоставлением Мерчантом авансового платежа на планируемый объем платежей. Для этого Платежной организацией создается доступ с отражением расчетного баланса Мерчанта в Системе для учета сумм принятых платежей. При совершении платежа клиентом через каналы продаж

Мерчанта, сумма принятых платежей автоматически списывается с расчетного баланса Мерчанта в Системе Платежной организации.

15.4. Мерчант обязуется обеспечивать на счете неснижаемый остаток денежных средств, достаточный для исполнения обязательств перед Платежной организацией.

15.5. Мерчант обязан передавать Системе данные о каждом принятом платеже для внесения изменений в лицевой счет Плательщика поставщиком услуг. Сведения должны быть переданы непосредственно в период приема платежа на основании данных, указываемых клиентом, без ошибок и искажений.

15.6. Каждой операции по передаче данных о платеже присваивается уникальный номер в Системе Платежной организации. Сочетание аутентификационных данных мерчанта – логин, пароль и/или ID в Системе и признаются сторонами в качестве однозначного и бесспорного подтверждения совершенного платежа.

15.7. После приема Платежа Мерчант обязан выдать клиенту квитанцию использования канала продаж Мерчанта для передачи данных о платеже.

15.8. Также сторонами в договоре может быть предусмотрено оказание платежных услуг без предварительного возмещения, в порядке перечисления/перевода сумм принятых платежей на периодической основе.

15.9. Мерчант обеспечивает передачу информации о каждом принятом платеже Платежной организации в режиме реального времени в соответствии с протоколом технического взаимодействия сторон, при этом по мере передачи Платежной организации информации о принятых платежей, сумма таких распоряжений автоматически уменьшает сумму остатка гарантийного взноса, которое засчитывается в счет исполнения обязательств агента по перечислению Платежной организации суммы принятых платежей.

15.10. При приеме платежей Мерчантом взимается комиссия с платежа. Размер комиссии устанавливается Мерчантом самостоятельно.

15.11. На ежемесячной основе производится сверка взаиморасчетов, на основании которой Мерчант предоставляет подписанный со своей стороны акт выполненных работ и(или) счет-фактуру на сумму вознаграждения, на основании которого происходит сверка взаиморасчетов (в случае, если сторонами договора достигнута договоренность по предоставлению указанных документов).

16. Перевод денег в Системе QIT осуществляется в валюте Республики Казахстан.

17. При этом непосредственные клиенты (потребители) оказываемых услуг в рамках Системы могут воспользоваться услугой в любое удобное для них время посредством тех мерчантов, которые функционирует по графику 24/7 (то есть непрерывно).

18. График работы платежной системы. В Системе QIT устанавливается операционный день с 00:00:00 по времени города Астана до 23:59:59 по времени города Астана календарного дня. В качестве единой шкалы времени при расчетах в Системе признается время города Астана. Контрольным является время системных часов аппаратных средств Оператора системы. Регламент обработки распоряжений и проведения расчетов представлены в Таблице №1.

Таблица №1.

| Событие | Время города Астана |
|---|---|
| Закрытие Отчетной даты (периода) | 23:59:59 |
| Составления реестров платежей и отчётов за закрытый Отчётный период и их передача в Организацию | С 09:00 по 13:00 |
| Осуществление расчётов Поставщику услуг по счетам участников Оператором Системы за закрытый отчетный период | С 09:00 по 18:00 |

19. Оператор не занимается реализацией электронных услуг в виде оформления посадочных мест и не контактирует напрямую с клиентами (т.е потенциальными пассажирами).

20. Оператор создаёт условия для участников рынка в лице мерчантов и их каналов продаж (касс, веб-касс, платежных терминалов самообслуживания, интернет-сайтов) осуществлять деятельность по оформлению электронных услуг для клиентов.

21. Основная задача Оператора – поддерживать и сопровождать систему реализации электронных услуг в части технической (IT) составляющей, осуществлять разработку нового функционала по заданию Поставщика.

## Раздел 3. Стоимость платежных услуг (тарифы), оказываемых платежной организацией

22. Тарифы (вознаграждение), применяемые к Мерчантам Системы. Услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег – виды, размер, порядок взимания комиссий определяется сторонами Договора при оказании Платежной организацией услуг исходя из действующих рыночных тарифов на услуги подобного вида, с учетом сумм комиссий, подлежащих в последующем перечислению третьим лицам (мерчантам, поставщикам услуг, лицам, обеспечивающим технологическое взаимодействие с Платежной организацией при оказании последними платежных услуг).

23. Тарифы (вознаграждение), применяемые к Мерчантам Системы. 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 – размер, единица измерения представлены в таблице ниже.

| **Проект Системы QIT** | **Единица измерения, или к чему применяется Вознаграждение** | **Вознаграждение** |
|---|---|---|
| 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.<br><br>Автоматизация процессов работы процессинговых и иных систем (АППС) | Одно посадочное место, или один билет | От 10 до 200 тенге с учетом НДС (размер определяется от набора приобретаемых IT-услуг) |

Детали формирования, порядок установления комиссий, взимаемых с Клиента, Поставщика услуг, а также полный список сервисов, устанавливается в соответствии с Тарифной политикой, утвержденной Платежной организацией, договорными условиями, указанными в договорах, заключенных между ТОО «Мобильный портал» и поставщиками услуг, и иными лицами, предоставляющими услуги Клиентам.

## Раздел 4. Порядок взаимодействия с банками, Поставщиками услуг, мерчантами и третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых платежной организацией

24. **Порядок взаимодействия с Банком**. Платежная организация заключает с Банком договор о взаиморасчетах и информационно техническом взаимодействии. Платежная организация проходит регистрацию в Системе Банка, для чего:

- В согласованный сторонами договора срок Платежная организация осуществляет реализацию Интерфейса подключения к Системе Банка.
- Сторонами определяется техническая готовность систем к отправке информации о платежах посредством технического и технологического тестирования систем.
- Платежная организация обязана передавать данные Банку о каждом обработанном платеже.
- Банк обязан передавать Платежной организации данные о каждом обработанном платеже.
- Сведения должны быть переданы непосредственно в период обработки платежа.
- Каждой операции по передаче данных о платеже присваивается уникальный номер в Системе Банка.
- Платежная организация с Банком проводит ежедневную сверку по обработанным платежам.
- На ежемесячной основе производится сверка взаиморасчетов.

Детализированное описание передвижения денежных средств при положительно обработанной операции оплаты:

- Банк-эмитент осуществляет перевод платежа в пользу Банка-эквайера;
- Банк-эквайер перечисляет платеж на расчетный счет Поставщика услуг или на транзитный счет Расчетного банка, с которым у платежной организации заключен соответствующий договор, Расчетный банк осуществляет перевод с транзитного счета на расчетный счет Поставщика услуг.

25. **Порядок взаимодействия при работе с Мерчантами**. Все мерчанты Системы для участия в системе подписывают договор между Оператором и Мерчантом.

26. Если мерчант решает присоединиться к проекту АППС, условия наличия прямого договора с Оператором, следующие:

- Форма собственности ТОО;
- Наличие 3000 проданных билетов ежемесячно в течение последовательных 3 (трех) месяцев (потенциальный Мерчант предоставляет подтверждение в виде официального документа).

27. Взаимодействие между Оператором Системы и Мерчантом осуществляется с момента выражения намерения юридического лица присоединиться к Правилам Системы (выражением намерения является подписание мерчантского договора участия в Системе) в качестве Мерчанта системы, и в дальнейшем в процессе осуществления им функций Мерчанта системы вплоть до момента прекращения указанной деятельности последнего. Основной предмет мерчантского договора – предоставить возможность мерчанту реализовывать электронные услуги в виде продажи посадочных мест Поставщика данных мест.

28. Права и обязанности Мерчанта Системы QIT:

- является юридическим лицом с формой собственности ТОО, должным образом, созданным и осуществляющим свою деятельность в соответствии с законодательством Республики Казахстан
- организовать прием платежей от Клиентов в пользу Поставщиков Системы через ее Оператора через свои Структурные подразделения, согласно требованиям отдельных Поставщиков, согласно условиям договора с мерчантом;
- уведомлять Оператора о поступлении оплаты от Клиента для дальнейшего учета суммы оплаты, посредством пересылки Информационного файла через Систему. Формат файла и метод передачи указаны в Техническом протоколе, являющегося неотъемлемой частью заключенного договора с мерчантом;

- самостоятельно и собственными силами ежедневно отслеживать и обеспечивать положительный Баланс для осуществления приема платежей в пользу Поставщика. При этом баланс считается положительным в момент физического поступления обеспечения платежей на счет Оператора Системы;
- в течение 5 (пяти) рабочих дней со дня получения письменного уведомления от Оператора, представить Оператору отчет о ходе оказания Услуг по Договору в соответствии с формой и сроками, определяемыми Оператором;
- при наличии расхождений между данными программно–технических средств Мерчанта и Системой Оператора, в течение 5 (пяти) рабочих дней предоставить анализ и заключение по такому расхождению. При этом данные Оператора принимаются за основу для такого анализа и заключения;
- при внедрении процесса приема платежей в пользу каждого нового Поставщика, строго следовать логике прохождения платежа, описанной в технических протоколах (API) для каждого отдельного Поставщика в договоре;
- обеспечить сохранность информации Оператора, полученной в ходе выполнения договорных обязательств, а также сохранность персональных данных граждан, Клиентов, вводимых при проведении платежа и не передавать их третьим лицам;
- Мерчант вправе привлекать к исполнению договора третьих лиц, оставаясь при этом ответственным за их действия перед Оператором.

29. Операции по переводу денежных средств в Системе за приобретение электронных услуг в виде посадочных мест совершаются Клиентами через: Платежные терминалы самообслуживания, Информационные киоски, Автоматизированные кассы самообслуживания, специализированные кассы, веб–ресурсы (интернет–сайты и прочие программные продукты мерчантов Системы), мобильные приложения.

30. Права и обязанности Оператора:
- Самостоятельно производить учет суммы платежей, принятых и перечисленных Мерчантом платежей, а также осуществлять контроль за полнотой и своевременностью зачисления Мерчантом принятых платежей путем проверки расчетов и сумм, зачисленных Мерчантом на счет Оператора. Если в ходе проверки будут выявлены какие–либо несоответствия, Оператор обязуется не позднее 5 (пяти) рабочих дней с момента выявления таких несоответствий письменно уведомить о результатах проверки Мерчанта;
- предоставить Мерчанту доступ в Систему на основании утвержденного процесса. Процесс работы предоставляется Мерчанту по электронной почте на указанный им в мерчентском договоре электронный почтовый ящик;
- не разглашать сведения, составляющие банковскую, коммерческую, служебную и иную, охраняемую законом тайну, ставшие известными в результате исполнения условий Договора, за исключением случаев, прямо предусмотренных законодательными актами Республики Казахстан;
- Приостановить прием платежей от Мерчанта, в случае достижения Мерчантом порогового значения по балансу, где порог определяется как минимальная сумма остатка на Балансе, для обеспечения проведения остаточных транзакций;
- Приостановить прием платежей от Мерчанта, в случае нарушения Мерчантом условий данных Правил и заключенного Мерчантского договора с Оператором, до момента устранения Мерчентом подобных нарушений;
- не вправе уступать, передавать и любым способом отчуждать, а также передавать в залог свои права и/или обязательства по договору полностью или частично третьим лицам без письменного согласия на то Субъекта Системы, с которым заключен договор.

31. Обязанности Субъектов Системы перед ее Оператором:
- обеспечить необходимые программно–технические средства и их бесперебойную работу для осуществления защищенного обмена информацией в электронном виде;
- обеспечить безопасность хранения данных и ограничение доступа к конфиденциальной информации в рамках заключенного договора с Оператором, а также обеспечить передачу данных по защищенным каналам связи;

- использовать Электронно–цифровую подпись для обеспечения подлинности передаваемых финансовых и транзакционных данных;
- не вправе уступать, передавать и любым способом отчуждать, а также передавать в залог свои права и/или обязательства по договору полностью или частично третьим лицам без письменного согласия на то Оператора Системы.

32. **Порядок взаимодействия с третьими лицами**. Третьи лица — это юридические лица и индивидуальные предприниматели, которые при этом предоставляют услуги платежной организации или действуют в интересах платежной организации, и при этом не входят в группу компании платежной организации и не являются работниками платежной организации. Подключение информационных систем третьей стороны к системам платежной организации производится на основании заключенного договора на оказание информационных и\или технологических услуг и соглашения о неразглашении конфиденциальной информации.

33. Соглашение о неразглашении конфиденциальной информации устанавливает обязанность третьей стороны соблюдать конфиденциальность информации, а также ответственность за разглашение конфиденциальной информации, к которой она получает доступ. Заключаемый договор или соглашение о неразглашении конфиденциальной информации должны учитывать типовые положения по исполнению третьей стороной требований по обеспечению информационной безопасности. Требования должны включать как минимум ответственность и обязательства за поддержание требуемого уровня информационной безопасности, а также мероприятия по уведомлению об инцидентах информационной безопасности и нарушениях в системе защиты информации.

34. Меры, принимаемые к участнику Системы QIT за нарушения Правил. В случаях, если нарушения Субъектов обязательств, принятых на себя в соответствии с настоящими Правилами, не влияют на бесперебойность функционирования Системы, либо на оказываемые ими услуги, Оператор осуществляет следующие действия:

– доводит до сведения Мерчантов информацию о выявленном нарушении в письменной форме с указанием допущенного нарушения и срока, в течение которого такое нарушение должно быть устранено;

– осуществляет контроль за устранением Субъекта выявленного нарушения в установленный в уведомлении.

35. В случаях, если нарушения Субъектами обязательств, принятых на себя в соответствии с настоящими Правилами, влияют на бесперебойность функционирования Системы, либо на оказываемые ими услуги, Оператор применяет одну из следующих мер принуждения:

– направляет данному Субъекту уведомление об устранении нарушения с указанием срока для его устранения;

– ограничивает (приостанавливает) оказание услуг;

– приостанавливает участие в Системе в соответствии с Правилами.

– применяет штрафные санкции за каждый выявленный случай нарушения.

36. Вышеуказанные меры принуждения применяются Оператором также в следующих случаях:

- при действиях (бездействии) Субъектов, повлекших приостановление (прекращение) осуществления переводов денежных средств в рамках Системы либо их несвоевременное осуществление;
- если уведомление Оператора об устранении выявленного нарушения не было выполнено Субъектов в установленный срок.

37. Меры принуждения вводятся на основании направляемого Оператором системы уведомления. Уведомление идентифицирует нарушение и определяет срок, в течение которого нарушение должно быть устранено. Указанный срок не должен превышать 10 (десяти) рабочих дней.

38. В случае, если по истечении срока действия мер принуждения, допущенные нарушения не устранены, срок действия данной меры принуждения может быть продлен Оператором Системы до устранения нарушения.

39. Уведомление Оператора Системы о применении мер принуждения, направляется участнику Системы, в отношении которого вводится ограничение.

40. В случае неоднократного невыполнения уведомлений с требованием об устранении нарушения, влияющего на бесперебойность функционирования Системы, в течение 6 месяцев со дня направления Оператором Системы первого уведомления об устранении такого нарушения Оператор Системы вправе прекратить участие Субъекта системы в Системе в соответствии с условиями приостановления и прекращения участия в Системе, установленными Правилами.

41. Субъекты Системы несут ответственность за неисполнение или ненадлежащее исполнение своих обязательств в соответствии с законодательством Республики Казахстан и Правилами.

42. В случае неисполнения Мерчантом предусмотренных Правилами и мерчантским договором обязательств, связанных с обеспечением возврата выручки на счет Оператора Системы для осуществления расчетов по операциям, совершенных клиентами Системы, а также в случае неисполнения обязательств по оплате оказанных услуг, Оператор Системы вправе начислить, а Мерчант обязан (в случае начисления) уплатить пеню в размере 0,1% (Ноль целых одна десятая) процентов от недостающей суммы за каждый день просрочки. В случае неоднократного неисполнения данного обязательства, Оператор системы вправе лишить организацию статуса Мерчанта системы, расторгнув мерчантский договор в одностороннем порядке с последующим уведомлением организации о расторжении договора.

43. В случае сбоев в системе или наступления иных обстоятельств, повлекших излишнее перечисление, не перечисление или не полное перечисление денежных средств, связанных с работой в системе, Оператор обязуется в кратчайшие сроки устранить последствия таких сбоев или обстоятельств. Штрафные санкции со стороны, допустившей не перечисление, перечисление в неполном объеме или перечисление излишних денежных средств, вызванное вышеуказанными сбоями или обстоятельствами, не взимаются.

44. Оператор несет ответственность за прямой ущерб, подтвержденный документально, причиненный Субъектам вследствие несоблюдения Оператором настоящих Правил, неисполнения или ненадлежащего исполнения своих обязательств.

45. Оператор не несет ответственности за наступление неблагоприятных последствий для третьих лиц, включая Клиентов, возникших в результате неисполнения Субъектами ненадлежащего/несвоевременного исполнения обязательств, предусмотренных Правилами системы и договорами/соглашениями.

46. Оператор не несет ответственности за нарушения в работе системы, произошедшие в следствие:

– неквалифицированного обслуживания или неисправности оборудования (в том числе каналов связи) Мерчантов, третьих лиц, предназначенного для работы в системе;

– неквалифицированного использования Субъектами, их сотрудниками программного обеспечения, предназначенного для использования в системе;

– неквалифицированных действий со стороны сотрудников Субъектами, взаимодействующих посредством автоматизированных рабочих мест, в том числе несанкционированного доступа неуполномоченных лиц к данным системы.

47. Субъекты Системы освобождаются от ответственности за неисполнение или ненадлежащее исполнение своих обязательств, если оно явилось следствием непреодолимой силы при условии, что эти обстоятельства непосредственно повлияли на исполнение обязательств.

48. Под непреодолимой силой понимаются чрезвычайные и непредотвратимые обстоятельства, которые невозможно было предвидеть и предотвратить имеющимися в распоряжении нарушившего обязательство Субъекта Системы разумными средствами, в том числе: землетрясения, наводнения, пожары, эпидемии, аварии на транспорте, военные действия, массовые беспорядки и др.

49. Субъект Системы, подвергшийся действию обстоятельств непреодолимой силы и оказавшийся вследствие этого не в состоянии выполнить свои обязательства, должен сообщить об этом в течение 2 (двух) рабочих дней с момента возникновения указанных обстоятельств в устной форме и в течение 3 (трех) рабочих дней в письменной форме Оператору системы, в

противном случае Субъект системы, нарушивший обязательство, не вправе ссылаться на обстоятельства непреодолимой силы. Уведомление должно содержать данные о характере обстоятельств, оценку их влияния на возможность исполнения своих обязательств и срок исполнения обязательств с приложением подтверждения официальных органов о действии обстоятельств непреодолимой силы.

50. Меры по обеспечению и внедрению в Системе QIT организационных и процедурных мероприятий, направленных на предотвращение мошенничества, легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма:

Внутренний контроль – деятельность ТОО «Мобильный портал», по выявлению операций, подлежащих обязательному контролю, и иных операций с денежными средствами или иным имуществом, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма;

Меры, направленные на противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма:

— организация и осуществление внутреннего контроля;

— обязательный контроль;

— запрет на информирование клиентов и иных лиц о принимаемых мерах противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, за исключением информирования клиентов о приостановлении операции, об отказе в выполнении распоряжения клиента о совершении операций;

— иные меры, принимаемые в соответствии Законами Республики Казахстан.

Для наиболее полной реализации указанных мер ТОО «Мобильный портал» обеспечивает соблюдение всеми сотрудниками организации настоящих Правил с учетом следующих требований:

— участие в процессе организации и осуществления внутреннего контроля в целях ПОД/ФТ всех работников независимо от занимаемой должности в рамках их компетенции;

— сохранение конфиденциальности информации, получаемой в процессе реализации правил внутреннего контроля в целях ПОД/ФТ;

— исключение участия работников организации в осуществлении легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма;

— недопущение информирования клиентов, иных лиц о мерах, принимаемых организацией в результате осуществления внутреннего контроля в целях ПОД/ФТ, за исключением информирования клиентов о приостановлении операции, об отказе в выполнении распоряжения клиента о совершении операций, о необходимости предоставления документов по основаниям, предусмотренным Законом Республики Казахстан;

— сохранение конфиденциальности сведений о внутренних документах организации, разработанных в целях ПОД/ФТ;

— применение эффективных процедур оценки рисков, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма.

Идентификация клиента, представителя клиента и (или) выгодоприобретателя, а также бенефициарного владельца включает в себя следующие мероприятия:

- установление определенных сведений в отношении клиента, представителя клиента, до их приема на обслуживание;
- принятие обоснованных и доступных в сложившихся обстоятельствах мер по идентификации бенефициарных владельцев, в том числе мер по установлению в отношении указанных владельцев сведений;
- проверка наличия или отсутствия в отношении клиента, представителя клиента, а также бенефициарного владельца сведений об их причастности к экстремистской деятельности или терроризму;
- выявление юридических и физических лиц, имеющих соответственно регистрацию, место жительства или место нахождения в государстве (на территории), которое (которая) не выполняет рекомендации Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ), либо использующих счета в банке, зарегистрированном в указанном государстве (на указанной территории);

- оценка и присвоение клиенту степени (уровня) риска в соответствии с программой оценки риска;
- обновление сведений, полученных в результате идентификации клиентов и бенефициарных владельцев.

ТОО «Мобильный портал» осуществляет идентификацию на основании действительных на дату предъявления документов, содержащих сведения, позволяющие идентифицировать клиента.

## Раздел 5. Сведения о системе управления рисками

51. Система управления рисками в Системе QIT определяет процедуры:

- выявления, измерения рисков, мониторинга и управления рисками;
- обеспечения непрерывности деятельности системы и содержит план восстановления деятельности оператора системы.

Под системой управления рисками в компании ТОО «Мобильный портал» понимается комплекс мероприятий и способов снижения вероятности возникновения неблагоприятных последствий для бесперебойности функционирования Системы с учетом размера причиняемого ущерба.

52. В целях снижения уровня рисков Системы процесс управления рисками направлен на предупреждение нарушений Системы управления рисками и организацию оперативного устранения нарушений Системы.

53. Для реализации указанной цели Оператор организует процесс управления рисками, включающий следующие процедуры:

- выявление факторов риска;
- анализ рисков;
- определение степени и характера влияния указанных факторов на Систему;
- оценка достигнутого уровня рисков;
- принятие мер, направленных на минимизацию риска и поддержание приемлемого уровня рисков;
- мониторинг рисков (выявление текущих изменений достигнутого уровня риска);
- информационное взаимодействие участников Системы в целях управления рисками.

54. Основными рисками, которые могут привести к нарушению Системы, принимаются риски:

1. *Расчетный (кредитный + ликвидности)*. Кредитный риск и риск ликвидности – риски Системы, обусловленные влиянием на Систему финансового состояния участников Системы. Вероятность наступления расчетного риска – минимальная. Оценка вероятности наступления расчетного риска на минимальном уровне обусловлена тем, что участники Системы имеют возможность совершать операции в Системе только в пределах остатка денежных средств на банковских счетах, открытых в Расчетном центре (далее РЦ). Расчетный риск включает:

a) Кредитный риск – риск, при котором участник не способен полностью выполнять свои обязательства в срок или в любое время в будущем;
b) Риск ликвидности – риск, при котором участник будет иметь недостаточно средств для исполнения своих финансовых обязательств в полном объеме в срок несмотря на то, что участник в состоянии исполнить обязательства в какой–либо момент в будущем;

Общие принципы управления расчетным риском состоят в контроле соблюдения Оператором следующих процедур:

- выполнение участниками требований по финансовому обеспечению расчетов в Системе, контроля Оператором лимитов авторизации участников Системы;
- выполнение Оператором мониторинга объемов операций между участниками, оперативный контроль резкого роста объемов операций того или иного участника;
- возможность блокирования в случае угрозы возникновения риска Оператора по операциям между участниками.

Все операции по переводу денежных средств в Системе QIT осуществляются только при обязательном соблюдении следующих условий: сумма авторизованного запроса не превышает сумму расходного лимита, установленного Расчетным центром на участника Системы.

2. *Операционный риск*. Операционный риск обусловлен влиянием на Систему операционных факторов в части неисправностей технологического обеспечения или возникшими операционными ошибками. Вероятность наступления операционного риска для Системы – средняя. Оценка вероятности наступления операционного риска обусловлена многообразием факторов и источников данного вида риска:

- случайные или преднамеренные действия физических и (или) юридических лиц, направленные против интересов Системы;
- несовершенство организационной структуры участников в части распределения полномочий подразделений и сотрудников, порядков и процедур совершения операций в рамках Системы, их документирования и отражения в учете;
- несоблюдение сотрудниками участников установленных порядков и процедур, неэффективность внутреннего контроля;
- сбои в функционировании информационных систем и оборудования;
- неблагоприятные внешние обстоятельства, находящиеся вне контроля участников.

Общие принципы управления операционным риском состоят в применении Оператором Системы, Операторами услуг и участниками Системы следующих мер:

a) обеспечение информационной безопасности, контроль над доступом к информации, применение многоуровневой защиты информации с использованием сертифицированных средств защиты информации, а также с аттестацией объектов информатизации Системы QIT по требованиям информационной безопасности;
b) учет и контроль совершаемых операций, регулярные выверки расчетных документов по операциям;
c) ведение единой системы управления информацией через автоматизированные средства;
d) регламентирование порядка выполнения основных процессов в Правилах и внутренних документах;
e) создание необходимых организационных и технических условий для обеспечения Системы при совершении операций (на случай аварий, пожаров, терактов и других непредвиденных ситуаций);
f) регламентирование порядка совершения операций в рамках внутренних нормативно–методологических документах;
g) применение принципов разделения и ограничения функций в целях определения предела полномочий сотрудников, осуществляющих операции;
h) использование механизмов усиления контроля за совершением операций, установление ограничений на сроки и объемы операций;
i) обеспечение работоспособности аппаратно–программных комплексов (АПК) всех участников Системы, в том числе – разработка технических требований на создание, внедрение и эксплуатацию АПК с учетом требований к показателям бесперебойности, тестирование АПК перед их внедрением, регулярный мониторинг системного, прикладного программного обеспечения и доступа к информационным ресурсам, обеспечение целостности информационных активов, разработка, поддержание в актуальном состоянии планов обеспечения непрерывности деятельности и восстановления деятельности после сбоев;
j) реализация процедур административного и финансового внутреннего контроля (предварительного, текущего и последующего) за организацией бизнес–процессов, деятельностью участников и совершением операций сотрудниками, соблюдением установленных лимитов по проводимым операциям.

3. *Правовой риск*. Правовой риск – несоблюдение участниками Системы требований законодательства, нормативных актов и заключенных договоров, внутренних документов, регламентирующих их деятельность. Вероятность наступления правового риска для Системы – средняя. Оценка вероятности наступления правого риска обусловлена определением количества выявленных фактов в заданный временной интервал претензий правового характера к Субъектам Системы со стороны:

— государственных органов власти;
— клиентов участников Системы;
— других Субъектов Системы.

Система управления правовым риском состоит в применении Оператором, Мерчантами и другими участниками Системы следующих способов минимизации данного вида рисков:

— предварительная проверка Оператором потенциальных Мерчантов услуг платежной инфраструктуры на обладание необходимой правоспособностью;
— периодическая, не реже одного раза в год, выборочная проверка Оператором Системы и Мерчантов услуг на обладание необходимой правоспособностью путем запросов на предоставление необходимой информации об их деятельности и документов, в том числе внутренних документов и договоров.

4. *Системный риск*. Данный риск возникает вследствие неспособности одного из участников Системы исполнить принятые на себя обязательства или нарушений в самой Системе, который вызовет неспособность большинства или всех Субъектов Системы исполнить свои обязательства в срок. Таким образом, возникновение системного риска является следствием возникновения одного из основных рисков (расчетного, правового или операционного).

55. В Системе QIT установлены следующие уровни рисков нарушения Системы с учетом влияния потенциального негативного эффекта (потерь):

| Категория риска | Допустимый уровень значения показателя |
|---|---|
| Операционный риск | <=6 |
| Расчетный риск | <=3 |
| Правовой риск | <=9 |
| Системный риск | <=18 |

56. Приемлемые уровни рисков нарушения Системы могут быть изменены путем внесения изменений в настоящее Положение на основе рекомендаций участников.

57. В процессе функционирования Оператором могут быть дополнительно выявлены иные риски и установлены иные показатели Системы, к которым могут относиться:

– финансовое состояние Операторов услуг;
– технологическое обеспечение Операторов услуг;
– зависимость от Платежных систем, с Операторами которых заключены договора (соглашения) о взаимодействии Систем;
– зависимость от внешних поставщиков (провайдеров) услуг;
– возможность возникновения конфликта интересов Субъектов Системы, связанных с деятельностью в рамках Системы и связанных с иной деятельностью.

Для каждого нового устанавливаемого показателя Системы определяется процедура и методика его формирования (порядок расчета) на основе первичной информации о функционировании Системы, а также приемлемые уровни соответствующих рисков нарушения Системы.

Анализ рисков нарушения Системы включает в себя следующие этапы:

➢ Выявление факторов риска нарушения. В результате выявления фактора риска определяются неблагоприятные события, которые могут произойти в результате воздействия этого фактора, локализация (место проявления), форма проявления.

| Категория риска | *Без риска* | *Низкий* | *Средний* | *Высокий* |
|---|---|---|---|---|
| Уровень риска (u) | 0 | 1 | 2 | 3 |

➢ Определение степени и характера влияния указанных факторов на Систему. Количественная оценка степени и характера влияния факторов риска на Системы производится расчетом показателей Системы (доступности – d), где d = (1 — t / T) с учетом особенностей значений показателей t (средняя длительность нарушений работоспособности в течение

заданного временного интервала) и T (продолжительность заданного временного интервала), характерных для каждого риска.

- Оценка достигнутого уровня рисков нарушения Системы производится в соответствии с принятой классификацией с учетом попадания рассчитанного конкретного значения показателя Системы (d) в заданный интервал, соответствующий уровню риска

| Баллы (Б) | Негативный эффект (Нэ) |
|---|---|
| 1 | *Незначительный* |
| 2 | *Допустимый* |
| 3 | *Значительный* |

58. Для учета последствий размера потенциального негативного эффекта (потерь) для Системы вследствие наступления конкретного риска полученные значения уровней риска корректируются с учетом негативного эффекта.

- Подтверждение соответствия достигнутого уровня рисков нарушения Системы установленному приемлемому уровню осуществляется путем сопоставления значений уровней риска с приемлемыми уровнями.

Принятие мер, необходимых для достижения или поддержания приемлемого уровня рисков нарушения Системы.

59. В соответствии с основными рисками, которые могут привести к нарушению Системы, применяются следующие меры:

*Для поддержания приемлемого уровня операционного риска:*

- регламентирование порядка и времени выполнения основных операций;
- учет и регулярные сверки по операциям;
- контроль за деятельностью участников Системы;
- контроль учета требований к показателям бесперебойности при разработке технических требований на создание, внедрение и эксплуатацию аппаратно– программных комплексов;
- регулярный мониторинг системного, прикладного программного обеспечения и доступа к информационным ресурсам;
- периодическая проверка обеспечения целостности информационных активов, средств идентификации и аутентификации, процедур протоколирования и аудита, криптографической защиты информации, резервного копирования и архивирования информационных ресурсов;
- проверка планов обеспечения непрерывности деятельности и восстановления деятельности после сбоев;
- проведение регулярной оценки качества и надежности функционирования информационных систем, операционных и технологических средств.
- обеспечение информационной безопасности;
- проверка подготовки и обучения персонала Субъектами Системы.

*Для поддержания приемлемого уровня расчетного (кредитного и риска ликвидности) риска:*

- установление предельных размеров (лимитов) обязательств участникам Системы с учетом уровня риска;
- установление ограничений на объемы операций;
- изучение финансового состояния участника;
- контроль выполнения информационных центров и РЦ регламента осуществления платежного клиринга.

*Для поддержания приемлемого уровня правового риска:*

- предварительная проверка потенциальных участников и Операторов услуг платежной инфраструктуры на обладание необходимой правоспособностью;
- периодическая, не реже одного раза в год, выборочная проверка участников Системы и Операторов услуг платежной инфраструктуры на обладание необходимой правоспособностью путем запросов на предоставление необходимой информации об их деятельности и документов, в том числе внутренних документов и договоров.

Выявление текущих изменений достигнутого уровня риска нарушения Системы (далее — мониторинг рисков нарушения Системы):

– ежемесячный расчет показателей Системы и уровней рисков;

– сравнение расчетных значений уровней рисков с приемлемыми значениями и выявление текущих изменений уровней рисков;

– анализ динамики изменений уровней рисков;

– доведение до органов управления Оператора информации о текущих изменениях уровней рисков нарушения Системы;

– выработка рекомендаций по снижению уровней рисков и доведение их до Субъектов Системы.

## Раздел 6. Порядок урегулирования спорных ситуаций и разрешения споров с клиентами

60. Все диспутные ситуации и спорные моменты, которые возникают у конечного пользователя, должны быть переданы в структурное подразделение мерчанта, который оказал платежную услугу посредством Системы, вследствие которой у конечного пользователя возникла данная ситуация.

61. В свою очередь в случае невозможности самостоятельного решения спорных ситуаций мерчанты размещают обращения клиентов посредством Электронной Системы Обработки Заявлений (ЭСОЗ Jira). Работа с данной системой заявок размещена в Приложении №1.

62. Процедуры отзыва указания по платежу и (или) переводу денег. Все денежные транзакции, взаиморасчеты в Системе QIT проводятся в тенге. Отзыв, возврат (аннулирование) Переводов между Оператором и Мерчантом Системы осуществляется по инициативе Оператора в одностороннем порядке в следующих случаях:

- прекращение сотрудничества Оператора с участником – исполнителем;
- наступление иных обстоятельств, делающих невозможной выдачу Перевода Получателю;
- участником–исполнителем или иным участником по причинам, не зависящим от Отправителя и Получателя.

63. В случае ошибочного, в соответствии с положениями действующего законодательства Республики Казахстан, зачисления Мерчантом на счет Оператора не подлежащих перечислению сумм, Субъекты имеют право произвести перерасчет сумм последующих перечислений Оператору. В случае если перерасчет не может быть произведен, Субъект направляет Оператору обоснованное в письменной форме уведомление с подтверждаемыми банковскими либо финансовыми документами, подтверждающими факт осуществления ошибочного зачисления сумм, на основании которого Оператор, в случае своего согласия, в течение 3 (трех) банковских дней осуществляет возврат Мерчанту сумм, ошибочно зачисленных на счет Оператора. В случае если Оператор не согласен с обоснованием Субъекта он предоставляет ему мотивированный отказ в течение 5 (пяти) рабочих дней.

64. В рамках работы АППС у клиента существует возможность отказаться от услуги приобретения билета за купленное посадочное место и получить причитающиеся ему денежные средства назад. Однако данная возможность существует при соблюдении определенных факторов, влияющих на сам Процесс возврата. Более подробная информация будет предоставлена Протоколе взаимодействия, который является неотъемлемой частью договора между Оператором и Мерчантом.

65. Порядок урегулирования неплатежеспособности субъектов Системы:

Данный порядок определяет методы привлечения денег для завершения платежей и (или) переводов денег. Мерчанты Системы QIT в целях обеспечения исполнения обязательств по возврату сумм принятых платежей предоставляют Оператору системы гарантированный денежный взнос в размере суммы ежесуточной выручки (с 00:00 по 23:59). Учет операций осуществляется в рамках календарной даты принятых платежей (с 00:00 часов до 23:59:59

текущей даты по времени города Астана). В случае неисполнения/ненадлежащего исполнения Мерчантом условия по возврату сумм принятых платежей и наличии вины Мерчанта, Оператор системы имеет право удержать сумму принятых Мерчантом платежей из суммы обеспечения исполнения обязательств по возврату сумм принятых платежей, либо активировать банковскую гарантию.

66. Порядок разрешения споров и обстоятельства непреодолимой силы:

В случае возникновения разногласий при выполнении условий мерчантского договора, Оператор системы и Мерчант обязуются предпринять все необходимые меры для их урегулирования во внесудебном порядке. В случае не достижения взаимного согласия сторон, споры разрешаются судом в соответствии с действующим законодательством Республики Казахстан.

67. Участники Системы освобождаются от ответственности за неисполнение либо ненадлежащее исполнение своих обязанностей, если оно явилось следствием наступления обстоятельств непреодолимой силы: наводнений, пожаров, землетрясений, стихийных бедствий, блокад, забастовок, военных действий и иных обстоятельств, которые участники не могли предвидеть и которые непосредственно повлияли на исполнение их обязательств. Сроки исполнения обязательств Участника, подвергшегося влиянию обстоятельств непреодолимой силы, передвигаются на период действия таких обстоятельств. При этом участники принимают необходимые меры для незамедлительного уведомления друг друга об этих обстоятельствах и прекращении их действия.

68. В случае если данные обстоятельства будут длиться более 1 (одного) месяца, то участники имеют право в одностороннем внесудебном порядке отказаться от дальнейшего исполнения обязательств по действующему договору, расторгнув его. При этом ни одна из сторон не будет иметь право требовать от другой стороны возмещения каких–либо убытков. Расторжение договора не освобождает участников от проведения взаиморасчетов.

## Раздел 7. Порядок соблюдения мер информационной безопасности

69. В целях обеспечения защиты информации в Системе при хранении, обработке, обмене защищаемой информации Субъекты Системы обеспечивают осуществление, включая, но, не ограничиваясь, следующих мер:

- соблюдение организационных мер защиты информации;
- поддержка программы управления уязвимостями;
- создание и поддержание безопасной сетевой инфраструктуры;
- мониторинг сетевой инфраструктуры;
- внедрение и поддержание мер по управлению доступом к защищаемой информации;
- иные меры, направленные на повышение защиты информации.

70. В рамках создания и поддержания безопасной сетевой инфраструктуры Субъекты Системы обеспечивают поддержку конфигурации межсетевых экранов для защиты данных, обеспечивающую анализ проходящей через них информации, а также обеспечивающую ограничение прямого доступа извне к компонентам системы, содержащим защищаемую Информацию.

71. В рамках реализации мер по внедрению и поддержание мер по управлению доступом к защищаемой информации Субъекты Системы обеспечивают ограничение доступа и учет лиц, имеющих доступ к защищаемой информации, в том числе:

- обеспечивают доступ к защищаемой информации только тем лицам, которым такой доступ необходим для выполнения возложенных на них функций;
- обеспечивают многокомпонентность и многоразрядность (не менее пяти символов) используемых паролей, а также периодическую смену паролей;
- обеспечивают предоставление доступа каждому сотруднику с использованием уникального имени, учетной записи, пароля и/или ключа проверки Электронной Подписи для доступа к защищаемой информации;
- обеспечивают ограничение доступа к материальным носителям, содержащим защищаемую информацию, строгий контроль за их хранением;

– обеспечивают немедленный отзыв доступа при прекращении полномочий лица на доступ к защищаемой информации.

Субъекты Системы обеспечивают защиту информации при осуществлении:

– приема платежей,

– работы со средствами внутри системы.

72. Мерчанты и Оператор Системы в рамках деятельности по обеспечению защиты информации применяют средства криптографической защиты информации (далее – СКЗИ) в составе системы обеспечения безопасности ИТ, в том числе, прошедшие в установленном порядке процедуру оценки соответствия. Участники Системы проводят работы по обеспечению защиты информации с помощью СКЗИ.

73. Все субъекты и Оператор Системы принимают меры антивирусной защиты своей информационной инфраструктуры, в том числе:

- проведение регулярного (в случае технической возможности – в автоматическом режиме) обновления антивирусных баз и антивирусного ПО;
- обучение сотрудников мерам антивирусной защиты;
- выполнение предварительной проверки антивирусным ПО устанавливаемого ПО;
- а также других мер ежедневно в начале работы при загрузке компьютера (для серверов – при перезапуске) в автоматическом режиме. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD – ROM, флеш картах и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере или, при условии начальной загрузки операционной системы в оперативную память компьютера с заведомо "чистой" (не зараженной вирусами) и защищенной от записи системной дискеты, – на любом другом компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

74. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

75. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка:

- на защищаемых серверах и рабочих стациях (далее РС) – ответственным за обеспечение информационной безопасности подразделения;
- на других серверах и РС автоматизированных систем (далее АС), не требующих защиты, лицом, установившим (изменившим) программное обеспечение, в присутствии и под контролем руководителя данного подразделения или сотрудника, им уполномоченного.

Факт выполнения антивирусной проверки после установки (изменения) программного обеспечения должен регистрироваться в специальном журнале подразделения за подписью лица, установившего (изменившего) программное обеспечение, и лица, его контролировавшего.

76. Субъект Системы при выявлении в Системе инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении приема платежей в пользу Поставщиков услуг, принимает меры по снижению негативных последствий, вызванных нарушением требований, информирует Субъекта Системы, в функциональной зоне ответственности которого находится область возникновения инцидента, в порядке и сроки, определенные в порядке взаимодействия в рамках Системы в чрезвычайных ситуациях.

77. Субъект Системы, допустивший инцидент, реализует комплекс мер, направленных на устранение причин, вызвавших инцидент, и на недопущение его повторного возникновения, и последствий инцидента.

78. Оператор Системы информирует Операторов услуг платежной инфраструктуры, Мерчантов системы о выявленных в Системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, носящих системный характер, а также о рекомендуемых методиках анализа и реагирования на указанные инциденты путем размещения соответствующей информации на странице Протокола взаимодействия, являющейся неотъемлемой частью договора, заключаемого между Оператором и Мерчантом.

79. Операторы услуг платежной инфраструктуры и Мерчанты системы в составе информации о своей деятельности, представляют данные для целей анализа обеспечения в Системе защиты информации при осуществлении приема платежных средств.

## Раздел 8. Описание программно-технических средств и оборудования, необходимого для осуществления платежных услуг

80. Целью компании ТОО «Мобильный портал» является автоматизация процессов работы процессинговых и иных систем с построением мульти–уровневой архитектуры взаимоотношений участников системы (далее – АППС), внедрение платежных технологий электронной коммерции для участников рынка экономики Казахстана.

АППС инициируется в рамках реализации мероприятий, нацеленных на поддержание государственной программы «Цифровой Казахстан», которая предусматривает ускорение темпов развития экономики республики и улучшение качества жизни, а также создание условий для перехода экономики Казахстана на принципиально новую траекторию развития, обеспечивающую создание цифровой экономики будущего в долгосрочной перспективе.

81. Описание операций, осуществляемых в Системе. АППС:

- Оформление различных электронных услуг на территории РК
- Возврат электронных услуг на территории РК, с использованием вспомогательных электронных документов.
- Гашение электронных услуг
- Переоформление электронных услуг
- Взаимодействие с оператором фискальных данных
- Открытие/закрытие электронных счетов
- Ведение финансовых операций на выделенных электронных счетах
- Формирование и ведение бухгалтерских и финансовых документов
- Предоставление нормативной и операционной отчетности
- Предоставление аналитической отчетности
- Предоставление технической и административной отчетности
- Ведение тарифных сеток
- Получение справочной информации из основной системы
- Частичный возврат электронных услуг
- Выдача дубликатов основных документов
- Постановка в Лист ожидания.

82. QIT имеет модуль для управления информационной безопасностью, который выполняет следующий функционал:

1) безопасное хранение данных,
2) защита от несанкционированного доступа,
3) резервирование данных, целостность баз данных и полная сохранность информации на серверах и базах данных, с целью предотвращения форс мажорных обстоятельствах, и с возможностью быстрого восстановления данных;
4) многоуровневый доступ для Мерчантов, использующих Систему QIT, к входным данным, функциям, операциям, отчетам, реализованным в программном обеспечении,

предусматривающим уровни доступа: администратор, технический специалист, пользователь, оператор;

5) многоуровневый доступ для Мерчантов, использующих свое ПО, к входным данным, функциям, операциям, отчетам, реализованным в программном обеспечении, предусматривающим уровни доступа: администратор, технический специалист, пользователь;
6) система QIT контролируют все поступающие и вводимые данные, для обеспечения правильного алгоритма действий при выполнении различных операций, связанных с предоставление электронных услуг. Если данные пришли некорректные, операции не будут обработаны.
7) Все данные хранятся согласно заданным критериям (по дате, времени и др.показателям).
8) Модуль системы QIT автоматически формирует журнал действий и внутреннего учета, 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, все данные хранятся на сервере.

Клиентские приложения системы QIT предоставляет возможность Мерчантам:

1) формировать отчетность по операциям, согласно утвержденным критериям.
2) Выводить на экран приложения электронные документы, с последующей возможностью печати.

В рамках обеспечения информационной безопасности системы QIT используются стойкие алгоритмы шифрования для организации защищенных подключений удаленных точек через VPN туннели, обеспечивая DMZ демилитаризованную зону для любых внешних подключений. Помимо этого, используется понятие hash ключей, которые привязывают пару логин/пароль к конкретному аппаратному обеспечению программной инфраструктуры через считывание аппаратных данных, таких как серийный номер материнской платы, жесткого диска, номер операционной системы и тд. Далее данный ключ шифруется открытым ключом и передается на сервер вместе с парой логин/пароль по защищенному VPN туннелю, где он расшифровывается закрытым ключом, обеспечивая полную гарантию безопасности внешних подключений. В случае попытки использования пар логин/пароль с любого, неавторизированного устройства выйдет ошибка.

Все данные и приложения на сервере находятся в виртуальной среде, обеспечивающей быструю замену аппаратных мощностей и отказоустойчивость системы в целом. Инкрементное резервное копирование средствами veeam и raid дисковые массивы производства ведущих мировых компаний с технологией hot swap обеспечивают безопасность хранения данных.

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

1) разработка модуля 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;
2) Модернизация и доработка модуля управления информационной безопасностью, для внедрения новейших методов, средств и механизмов управления, обеспечения и контроля информационной безопасности
3) обеспечение методологической поддержки процесса обеспечения информационной безопасности;
4) сбор, хранение и обработка информации об инцидентах информационной безопасности;
5) анализ информации об инцидентах информационной безопасности;
6) 6) обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности, а также предоставление доступа к ним;
7) создает роли для регулирования и ограничения по использованию привилегированных учетных записей;

8) организует и проводит мероприятия по обеспечению осведомленности работников платежной организации в вопросах информационной безопасности;
9) проводит мониторинг состояния модуля управления информационной безопасностью платежной организации;
10) ежедневно и еженедельно проводит информирование руководства и ответственных сотрудников платежной организации о состоянии модуля управления информационной безопасностью платежной организации.

83. Техническое описание проекта:

Клиент – серверное приложение. В качестве интерфейса обмена данными используются формат сообщений JSON и XML.

Интегрированная среда разработки: Microsoft Visual Studio 2019.

Серверная часть построена на программной платформе Microsoft .NET Framework 4.5, с использованием языка программирования C# на платформе Windows Server 2022, система управления базой данных - MS SQL Server 2019. Для работы с базой данных используется технология MICRO-ORM Dapper.Net, Entity Framework

Клиентское приложение работает на операционной системе Windows с поддержкой Microsoft .NET Framework 4.5. Авторизация пользователей осуществляется с использованием схемы авторизации basic authentication scheme, а также ЭЦП.

Язык программирования: C#.

Тип реализующей ЭВМ: IBM PC-совместимый ПК.

**Схема движения денежных средств и информационных потоков**