**УТВЕРЖДЕН**

Протоколом учредительного

общего собрания участников №2

от 24 апреля 2022.

# ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ ТОО «DREIDEL FINANCE (ДРЕЙДЛ ФИНАНС)»

**АЛМАТЫ – 2022 год**

**ОГЛАВЛЕНИЕ**

## ВВОДНЫЕ ПОЛОЖЕНИЯ

Настоящие Правила осуществления деятельности Платежной организации (далее – «**Правила**») разработаны в соответствии с положениями:

(i) Закона Республики Казахстан от 26 июля 2016 года «О платежах и платежных системах», с учетом изменений (далее – «**Закон о платежах**»);

(ii) Правил организации деятельности платежных организаций, утвержденных постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 215 (далее – «**Правила ОДПО**»); и

(iii) устава Платежной организации.

Настоящие Правила определяют порядок и условия осуществления деятельности Платежной организации и подлежат размещению в открытом доступе на Сайте на русском языке.

Термины, употребляемые в настоящих Правилах с заглавной буквы, имеют значения, определенные в пункте 1 Приложении № 1. Порядок вступления в силу, внесения изменений и применения настоящих Правил установлен в Приложении № 2.

## 1. ОПИСАНИЕ ПЛАТЕЖНЫХ УСЛУГ, ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

1.1. Платежная организация оказывает услуги по Обработке платежей, инициированных Клиентом в электронной форме, и передаче необходимой информации Банкам и иным организациям, осуществляющим отдельные виды банковских операций, для целей проведения платежа и (или) перевода (зачисления) денежных средств в рамках соответствующего платежа (далее – «**Платежные услуги**»).

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

1.3. Оказание Платежных услуг осуществляется в соответствии со следующим порядком:

(i) Клиент инициирует платеж с использованием платежных карт, указывая реквизиты назначения соответствующего платежа и бенефициара;

(ii) Платежная организация обеспечивает прием платежей, инициированных Клиентом, и последующую передачу реквизитов платежа в адрес Банка; и

(iii) Банк исполняет поручение Клиента, переданное через Систему в электронной форме, и зачисляет денежные средства в пользу бенефициара.

1.4. Основанием оказания Платежных услуг является договор, заключаемый между Платежной организацией и Банком.

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

2.1. Платежная услуга по Обработке платежей, инициированных Клиентом в электронной форме, и передаче необходимой информации Банкам и иным организациям, осуществляющим отдельные виды банковских операций, для целей проведения платежа и (или) перевода (зачисления) денежных средств в рамках соответствующего платежа осуществляется в соответствии с положениями настоящего пункта 2.

2.2. В рамках оказания Платежных услуг Платежная организация обеспечивает сбор, обработку и рассылку информации Участникам расчетов на каждом из следующих этапов:

(i) инициация Клиентом платежа с помощью программного обеспечения (WEB – приложений, online-приложений, мобильных приложений (приложений для мобильных устройств), программного обеспечения терминалов самообслуживания, виджетов и прочих приложений), обеспечивающего возможность формирования Клиентом в электронной форме распоряжений на списание денежных средств с платежной карты;

(ii) передача Платежной организацией реквизитов по платежу для его исполнения в пользу Банка-эквайера; и

(iii) исполнение Банк-эквайером указания Клиента, переданного через Систему в электронной форме.

2.3. Оказание Платежных услуг осуществляется согласно алгоритму, приведенному в Приложении 3, в течение 1 (одного) рабочего дня, следующего за днем приема платежа.

2.4. Подтверждением оказания Платежной услуги является квитанция, формируемая и направляемая Платежной организацией на адрес электронной почты Клиента или с помощью SMS-сообщения на номер телефона Клиента. Квитанция должна содержать информацию, установленную Законом о платежах и Правилами ОДПО, а именно:

(i) номер квитанции и дату ее выдачи;

(ii) наименование Платежной организации;

(iii) сумму Операции;

(iv) валюту Операции;

(v) сумму комиссионного вознаграждения;

(vi) назначение платежа;

(vii) наименование Поставщика услуг;

(viii) наименование либо банковский идентификационный код Банка; а также

дополнительную информации в отношении оказанных Платежных услуг.

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

3.1. Стоимость Платежных услуг определяется на основе тарифа Банка и, в зависимости от конкретной категории сервисов, предоставляемых Поставщиками услуг, может составлять до 15% с каждой Операции.

3.2. Порядок и условия взимания комиссий, а также размер комиссий определяются сторонами договора исходя из действующих рыночных тарифов на соответствующие Платежные услуги, учитывая суммы комиссий, подлежащих перечислению Третьим лицам и (или) взимаемые партнерами Платежной организации.

3.3. Ценовая политика по взимаемой дополнительной комиссии с Клиента устанавливается Платежной организацией самостоятельно в рамках допустимых значений, указанных в договоре. Платежная организация вправе в одностороннем порядке:

(i) изменить или отменить отдельные комиссии;

(ii) установить специальные комиссии за дополнительные виды услуг или за нестандартные Операции, исполняемые по поручению Клиента и не предусмотренные установленным перечнем;

(iii) устанавливать минимальную комиссию вне зависимости от применимых тарифов; и

(iv) предоставлять индивидуальные скидки к утвержденным тарифам отдельным Поставщикам услуг, а также изменить условия оплаты Платежных услуг в зависимости от категории Поставщика услуг.

3.4. При любом изменении размера комиссий, а также установлении специальных комиссий в соответствии с пунктом 3.3 Платежная организация обязуется направить последующее уведомление контрагентам в соответствии с настоящими Правилами и положениями публичного договора, размещенного на Сайте.

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

4.1. При условии соблюдения положений Закона о платежах, Платежная организация вправе уполномочивать Третьих лиц на оказание информационно-технологической поддержки для целей оказания Платежных услуг.

4.2. Подключение информационных систем Третьего лица к Системе осуществляется при условии и на основании заключенных:

(i) договора на оказание информационных и (или) технологических услуг, содержащего типовые положения по исполнению Третьим лицом требований по обеспечению информационной безопасности, включающие по меньшей мере:

(A) ответственность Третьего лица и его обязательства по поддержанию требуемого уровня информационной безопасности; и

(B) необходимость оперативного уведомления Платежной организации о случаях нарушения информационной безопасности и об угрозах таких нарушений; и

(ii) соглашения о конфиденциальности (неразглашении информации), устанавливающего режим конфиденциальности информации, ее охраны и неразглашения.

4.3. Платежная организация также вправе заключить лицензионный договор, содержащий детальное описание информационно-технологических функций, осуществляемых Третьими лицами для обеспечения оказания Платежных услуг Платежной организацией.

*Порядок взаимодействия Платежной организации с Поставщиками услуг*

4.4. Основанием взаимодействия Платежной организации с Поставщиком услуг является договор об оказании Платежных услуг, содержащий, по меньшей мере, но не ограничиваясь, следующую информацию:

(i) общее описание оказываемых Платежных услуг, включая порядок и максимальный срок их оказания;

(ii) размеры взимаемых сборов и комиссий, а также порядок их взимания;

(iii) порядок предоставления информации о Платежных услугах;

(iv) условия, при которых Платежная организация вправе отказать в оказании Платежной услуги и при которых Поставщик услуг вправе расторгнуть договор в одностороннем порядке;

(v) ответственность за необоснованный отказ от исполнения Платежной услуги и (или) ненадлежащее исполнение поручения;

(vi) порядок урегулирования вопросов в отношении несанкционированных Платежных услуг; и

(vii) порядок предъявления претензий и разрешения споров.

4.5. Предварительными условиями взаимодействия с Поставщиком услуг являются:

(i) проведение финансовым департаментом Платежной организации экономического обоснования заключения договора с новым Поставщиком услуг;

(ii) анализ комплаенс рисков; и

(iii) регистрация Поставщика услуг в Системе и присвоение Поставщику услуг идентификационного номера. Для целей регистрации в Системе Платежная организация совместно с Поставщиком услуг проводят:

(A) обмен технической документацией для подключения Поставщика услуг к Системе по протоколу технического взаимодействия API; и

(B) тестирование Систем на определение их технической готовности к отправке информации о платежах.

4.6. Платежная организация обязуется передавать Поставщику услуг информацию о каждом Обработанном платеже для внесения Поставщиком услуг изменений в лицевой счет Клиента. Соответствующие сведения подлежат передаче непосредственно в период Обработки платежа на основе предоставленных Клиентом данных. Каждой Операции по передаче платежных данных присваивается уникальный номер в Системе. В установленный договором об оказании Платежных услуг срок Платежная организация совместно с Поставщиком Услуг проводят сверку по успешно Обработанным платежам.

*Порядок взаимодействия Платежной организации с Банками*

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

(i) общее описание оказываемых Платежных услуг, включая порядок и максимальный срок их оказания;

(ii) размеры взимаемых сборов и комиссий, а также порядок их взимания;

(iii) порядок расчетов с Платежной организацией и Поставщиком услуг;

(iv) условия, при которых Банк вправе расторгнуть договор в одностороннем порядке; и

(v) порядок предъявления претензий и разрешения споров.

4.8. Предварительными условиями взаимодействия с Банком являются:

(i) соответствие Банка следующим критериям:

(A) общая финансовая устойчивость;

(B) осуществление мер по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

(C) наличие необходимых лицензий (разрешений) на осуществление деятельности Банка в соответствии с требованиями применимого законодательства; и

(D) обеспечение информационной защиты и банковской тайны; и

(ii) регистрация Платежной организации в Системе Банка. Для целей такой регистрации:

(A) Платежная организация осуществляет реализацию интерфейса подключения (API) к Системе Банка; и

(B) Платежная организация совместно с Банком проводят тестирование Систем на определение их технической готовности к отправке информации о платежах.

4.9. Платежная организация и Банк обязуются передавать друг другу информацию о каждом Обработанном платеже непосредственно в период Обработки платежа на основе предоставленных Клиентом данных. Каждой Операции по передаче платежных данных присваивается уникальный номер в Системе Банка. В установленный договором о взаиморасчетах и информационно-техническом взаимодействии срок Платежная организация совместно с Банком проводят сверку по успешно Обработанным платежам.

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

5.1. В целях эффективной минимизации расходов Платежной организации и поддержания приемлемого соотношения прибыльности с показателями безопасности и ликвидности в процессе управления активами и обязательствами Платежная организация разрабатывает политику управления рисками, предполагающую систематическую деятельность по разработке и имплементации мер, направленных на выявление, мониторинг и предотвращение рисков, возникающих в ходе оказания Платежных услуг.

5.2. При разработке мер управления рисками Платежная организация руководствуется, среди прочего, следующими факторами:

(i) характером и сложностью коммерческой деятельности;

(ii) доступностью рыночных данных для использования в качестве исходной информации;

(iii) состоянием информационных систем; и

(iv) квалификацией сотрудников, вовлеченных в процесс управления рисками.

5.3. Процедуры выявления, мониторинга и предотвращения рисков распространяются на все виды активов и обязательств Платежной организации и охватывают все виды рыночного риска и их источники. Функции по выявлению, мониторингу и предотвращению рисков в Платежной организации возложены на специального сотрудника, в задачи которого входит:

(i) анализ и оценка рисков, включая оценку возможного ущерба в случае материализации рисков; и

(ii) разработка и имплементация практических мер, направленных на управление рисками, учитывая вероятность возникновения рисков и возможных последствий для Платежной организации.

5.4. Эффективное управление уровнем риска в Платежной организации предполагает удержание рисков на приемлемом и управляемом уровне и должно решать целый спектр задач, от отслеживания (мониторинга) риска до его стоимостной оценки.

Платежная организация регулярно обновляет оценку риска тех или иных событий, пересматривает отношения с Клиентами, оценивает качество собственных активов и обязательств и, как следствие, корректирует свою политику в области управления рисками.

5.5. В основе управления рисками Платежной организации лежат следующие принципы:

(i) прогнозирование рисков, т.е. потенциальных источников убытков или ситуаций, способных повлечь убытки;

(ii) финансирование рисков, т.е. экономическое меры по минимизации рисков;

(iii) ответственность компетентных сотрудников, задействованных в системе управления рисками;

(iv) прозрачность политики и механизмов управления рисками; и

(v) контроль рисков по всем подразделениям Платежной организации.

5.6. Система управления рисками включает в себя в качестве составных элементов мероприятия и способы управления, подробно описанные в Приложении 4.

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

6.1. Настоящие Правила регулируются и толкуются правом Республики Казахстан.

6.2. Вопросы, не предусмотренные настоящими Правилами, регулируются применимым законодательством Республики Казахстан и внутренними документами Платежной организации. В случае если в результате внесения изменений в действующее законодательство Республики Казахстан, включая нормативно-правовые акты Национального Банка Республики Казахстан, какие-либо положения настоящих Правил перестанут соответствовать положениям законодательства (с учетом изменений), то до момента внесения изменений в настоящие Правила подлежат применению соответствующие нормы законодательства Республики Казахстан.

6.3. В случае возникновения у Клиента какой-либо претензии к Платежной организации, возникающей на основании настоящих Правил или в связи с ними и связанной с оказанием Платежных услуг, Клиент вправе направить Платежной организации соответствующую претензию, составленную в произвольной форме с описанием возникшей спорной ситуации и указанием предпочтительного способа обратной связи (далее – «**Претензия**»).

6.4. К любой Претензии, направляемой Клиентом Платежной организации, должны быть приложены надлежащим образом оформленные документы, подтверждающие изложенные в ней факты, а также следующие документы, удостоверяющего личность Клиента.

6.5. Претензия может направлена одним из следующих способов:

(i) почтовым отправлением по адресу – Казахстан, город Алматы, Бостандыкский район, Проспект Нурсултан Назарбаев, здание 193, почтовый индекс 050000; или

(ii) путем личного обращения в офис Платежной организации и ее нарочным предоставлением по адресу: Казахстан, город Алматы, Бостандыкский район, Проспект Нурсултан Назарбаев, здание 193, почтовый индекс 050000.

6.6. Претензия, направленная любым из способов, указанных в пункте 6.5, подлежит обязательной регистрации Платежной организацией путем присвоения даты и порядкового номера входящей корреспонденции. Датой приема Претензии Клиента считается фактическая дата регистрации входящего обращения Клиента.

6.7. Во избежание сомнений, обращения в службу технической поддержки Клиентов по телефонной связи, направления сообщений через форму обратной связи на Сайте не могут быть признаны обращением к Платежной организации с Претензией и не расцениваются в качестве досудебного урегулирования споров.

6.8. Платежная организация обязуется рассмотреть и направить ответ Клиенту на полученную Претензию в срок, не превышающий 30 (тридцати) календарных дней со дня получения Претензии.

6.9. Для целей рассмотрения Претензии и подготовки ответа Платежная организация:

(i) проводит предварительную оценку Претензии и, если это представляется необходимым или целесообразным, перенаправляет запрос в соответствующее(ие) структурное(ые) подразделение(я) Платежной организации для получения разъяснений, дополнительных сведений и иных данных в отношении возникшей спорной ситуации;

(ii) при необходимости запрашивает у Клиента дополнительные документы (или их копии), объяснения и иные сведения. По запросу Платежной организации Клиент обязан предоставить запрашиваемые сведения и документы (их копии) в целях надлежащего досудебного урегулирования возникшего спора;

(iii) проводит анализ полученных сведений и разъяснений для формирования полного ответа на Претензию; и

(iv) составляет и направляет мотивированный письменный ответ Клиенту на Претензию в установленные настоящим пунктом сроки по сообщенному Клиентом адресу с учетом предпочтительного способа обратной связи.

6.10. В случае невозможности разрешения спора в досудебном порядке в течение 30 (тридцати) календарных дней со дня получения Платежной организацией Претензии, такой спор подлежит окончательному разрешению в судебном порядке в соответствии с применимым законодательством Республики Казахстан.

## 7. ПОРЯДОК СОБЛЮДЕНИЯ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. В целях эффективного оказания Платежных услуг проводится комплекс мероприятий, направленных на обеспечение информационной безопасности

Платежной организации. При этом, под «**информационной безопасностью**» понимается состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры Платежной организации от внешних и внутренних угроз.

7.2. Деятельность по обеспечению информационной безопасности Платежной организации формируется из следующих направлений:

(i) внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс обеспечения информационной безопасности, а также предоставление доступа к ним;

(ii) использование по назначению технических средств и телекоммуникационных ресурсов Платежной организации ее сотрудниками и уполномоченными Третьими лицами;

(iii) управление доступом к активам и гарантия физической безопасности активов;

(iv) идентификация, устранение и анализ причин возникновения угроз информационной безопасности;

(v) сбор, консолидация, хранение и обработка информации об Инцидентах информационной безопасности;

(vi) гарантия антивирусной защиты и своевременного выявления уязвимостей в информационных системах Платежной организации;

(vii) гарантия резервного копирования данных;

(viii) управление бесперебойностью деятельности Платежной организации;

(ix) прозрачность принципов внесения изменений, установки, модификации и технического обслуживания информационных систем Платежной организации;

(x) обеспечение осведомленности сотрудников Платежной организации в вопросах информационной безопасности и регулярное информирование менеджмента Платежной организации о состоянии системы управления информационной безопасностью; и

(xi) соблюдение условий всех программных лицензий, авторских прав и нормативно-правовых актов, регламентирующих вопросы интеллектуальной собственности.

7.3. Деятельность по обеспечению информационной безопасности Платежной организации предполагает проведение внутреннего и внешнего (независимого) аудита информационной безопасности.

7.4. Система информационной безопасности, применяемая в Платежной организации, представляет собой совокупность мер по информационной защите, которая формируется в соответствии с методологией менеджмента информационной безопасности и состоит из следующих элементов:

(i) меры, направленные на предотвращение несанкционированного доступа к программно-техническим средствам, применяемым в Платежной организации, включая программно-технические средства защиты, которые должны обеспечивать уровень защиты информации и сохранение ее конфиденциальности в соответствии с требованиями, установленными применимым законодательством; и

(ii) меры по соблюдению сотрудниками Платежной организации режима конфиденциальности информации, предотвращению несанкционированного использования и защите идентификационных данных от несанкционированного доступа.

Конкретные меры, внедряемые Платежной организацией в целях обеспечения информационной защиты, приведены в Приложении 5.

7.5. Сотрудники Платежной организации несут ответственность за соблюдение применимого законодательства и требований внутренних нормативных документов Платежной организации, регламентирующих обеспечение информационной безопасности. Сотрудники Платежной организации, которым стало известно о случаях нарушения информационной безопасности, должны оперативно сообщать об этом своему непосредственному руководителю или, если сообщение касается данного непосредственного руководителя, своему вышестоящему руководителю любым удобным для них способом. Платежная организация обеспечивает независимое и всестороннее рассмотрение всех сообщений о нарушениях информационной безопасности в соответствии со своими внутренними политиками и процедурами.

7.6. Руководитель департамента информационных технологий или уполномоченное им лицо несет ответственность за:

(i) разработку требований по информационной безопасности и имплементацию данных требований в Платежной организации; и

(ii) мониторинг общей эффективности обеспечения информационной безопасности, в том числе ее соответствия требованиям деятельности Платежной организации.

7.7. Владельцы процессов и активов несут ответственность за распределение полномочий и ответственности в части реализации мер обеспечения информационной безопасности для соответствующих активов и устранение в установленные сроки несоответствий по результатам проводимых проверок.

7.8. Против любого лица, допустившего нарушение требований информационной безопасности Платежной организации, могут быть предприняты меры дисциплинарного или иного воздействия вплоть до увольнения и (или) расторжения договора в соответствии с положениями соответствующего договора и применимого законодательства.

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

8.1. Программно-технические средства, используемые Платежной организацией при оказании Платежных услуг, включают в себя:

(i) систему электронных денег (ЭД), представляющую собой совокупность программно-технических средств, документации и организационно-технических мероприятий, позволяющих осуществлять Операции с использованием электронных денег;

(ii) систему Интернет-эквайринга (или Payment System), представляющую собой совокупность программно-технических средств, документации и организационно-технических мероприятий, позволяющих осуществлять Операции, связанные с платежами; и

(iii) оборудование – физические серверы и сетевое оборудование, размещаемые в дата-центрах Поставщиков услуг, обслуживание которых осуществляется специалистами Поставщиков услуг и Платежной организации.

*Система ЭД*

8.2. Цель использования системы ЭД заключается в обеспечении взаимодействия между ее участниками, включающими оператора системы ЭД, (суб)агентов, Поставщиков услуг и Клиентов, в соответствии с едиными стандартами.

8.3. Система ЭД осуществляет учет платежей, проведенных с использованием электронных денег, а также все Операции выпуска и погашения электронных денег и предоставляет сведенные отчеты по соответствующим Операциям для участников системы ЭД (по их запросу) и надзорных органов.

8.4. Каждому участнику системы ЭД доступна опция просмотра своих счетов в режиме реального времени.

8.5. Контроль функционирования системы ЭД обеспечивает автоматизированный онлайн бэк-офис, позволяющий оперативно подключать к системе новых Поставщиков услуг, проводить Операции и сверки в режиме реального времени, а также устанавливать и корректировать настройки безопасности в зависимости от типа той или иной Операции или запроса участника системы ЭД.

8.6. Функционал системы ЭД включает в себя следующие уникальные модули:

(i) шлюзы для подключения платежных сервисов;

(ii) автоматическое подключение к системе;

(iii) система выставления и учета электронных счетов;

(iv) система управления платежным шлюзом;

(v) API для подключения (суб)агентов;

(vi) клиентский интерфейс физических лиц;

(vii) формирование юридических и бухгалтерских документов;

(viii) интеграция с биллингом и системой контроля доступа;

(ix) сервис возврата, отмены и корректировки ошибочных платежей;

(x) модуль информирования плательщиков;

(xi) фильтры для противодействия мошенничеству через систему (фильтры антифрод);

(xii) статистическая отчетность; и

(xiii) модуль сверки реестров.

8.7. Использование системы ЭД позволяет оперативно и технически безопасно объединять нескольких Поставщиков услуг и предоставлять к ним доступ для (суб)агентов через единый интерфейс в рамках одной технической интеграции.

*Система Payment System*

8.8. Цель использования Payment System заключается в обеспечении взаимодействия между ее участниками, включающими Интернет-магазины, Клиентов и платежные сервисы, в соответствии с едиными стандартами вне зависимости от того, с использованием какого платежного сервиса осуществляется оплата за соответствующий Товар.

8.9. Payment System функционирует на основании электронных счетов, формируемых Поставщиками услуг по запросу Клиента. Запрос на выставление электронного счета создается либо полностью в автоматическом режиме (через API), либо в ручном режиме через доступный Поставщику услуг web-интерфейс. Поставщики услуг получают информацию о поступлении платежа сразу же после оплаты в режиме реального времени.

8.10. Подключение платежных сервисов реализуется путем их подключения к электронному шлюзу Payment System, предоставляющему возможность взаимодействия с различными типами международных платежных сервисов, включая:

(i) Интернет-эквайринг банковских карт;

(ii) системы ЭД;

(iii) системы приема наличных платежей; и

(iv) системы мобильных платежей.

8.11. Контроль функционирования Payment System обеспечивает автоматизированный онлайн бэк-офис, позволяющий оперативно подключать к системе новых Поставщиков услуг, проводить Операции и сверки в режиме реального времени, а также устанавливать и корректировать настройки безопасности в зависимости от типа той или иной Операции или запроса участника Payment System.

8.12. Функционал Payment System включает в себя следующие уникальные модули:

(i) шлюзы для подключения платежных сервисов;

(ii) автоматическое подключение к системе;

(iii) система выставления и учета электронных счетов;

(iv) система управления платежным шлюзом;

(v) API для подключения магазинов;

(vi) модули для подключения к CMS;

(vii) подключение к системам бронирования;

(viii) клиентский интерфейс магазинов;

(ix) формирование юридических и бухгалтерских документов;

(x) интеграция с биллингом и системой контроля доступа;

(xi) сервис возврата, отмены и корректировки ошибочных платежей;

(xii) сервис произвольных выплат;

(xiii) модуль информирования плательщиков;

(xiv) сервис выставления ручных счетов;

(xv) фильтры для противодействия мошенничеству через систему (фильтры антифрод);

(xvi) статистическая отчетность; и

(xvii) модуль сверки реестров.

8.13. Использование Payment System позволяет оперативно и технически безопасно объединять несколько платежных сервисов и предоставлять к ним доступ для Интернет-магазинов через единый интерфейс в рамках одной технической интеграции. Payment System также объединяет и сами Интернет-магазины, предоставляя Клиентам возможность выбирать различные Товары на одном Интернет-сайте и осуществлять оплату единым платежом, подключая любые платежные сервисы (в том числе, производить доплату по тому или иному заказу с другого платежного сервиса в случае, если на первоначально выбранном платежном сервисе недостаточно средств для оплаты).

## ПРИЛОЖЕНИЕ 1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1. Определения

Термины, используемые в настоящих Правилах с заглавной буквы, имеют указанное ниже значение, если из контекста явно не вытекает иное:

«**АПК**» – специализированный аппаратно-программный комплекс ТОО «Dreidel Finance (Дрейдл Финанс)» и (или) Банка.

«**Банк**/**Банк-эквайер**» – банк второго уровня, с которым Платежная организация заключила договор в целях оказания Платежных услуг.

«**Банк-эмитент**» – банк, осуществляющий выпуск платежных карт.

«**Держатель платежной карты**» – законный держатель карты, использующий ее для совершения Операций.

«**Закон о платежах**» – имеет значение, данное этому термину в разделе *Вводные положения*.

«**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 Платежной организации.

«**Клиент**» – физическое лицо, обладающее надлежащей дееспособностью в соответствии с законодательством Республики Казахстан для осуществления платежа, совершившее конклюдентные действия, направленные на заключение договора об оказании услуг, и обладающее аутентификационными данными для доступа к Системе в целях управления своей учетной записью, и последующего оказания Платежной организацией Платежных услуг, предусмотренных настоящими Правилами.

«**Международные платежные системы (МПС)**» – международные платежные системы: Visa International и MasterCard International и иные МПС.

«**Обработка платежей**» – обработка Платежной организацией и Банком с применением АПК Банка и Системы, а также в соответствии с правилами МПС информации об Операциях, которая включает в себя сбор, обработку и рассылку Участникам расчетов информации по совершенным Операциям.

«**Операция**» – любой из платежей, совершаемый с использованием платежных карт, включая Операцию оплаты, Операцию отмены оплаты, Операцию возврата, Операцию отмены возврата.

«**Платежная организация**» – товарищество с ограниченной ответственностью (ТОО) «Dreidel Finance (Дрейдл Финанс)», созданное и действующее в соответствии с законодательством Республики Казахстан.

«**Платежные услуги**» – имеет значение, данное этому термину в пункте 1.1.

«**Поставщик услуг**» – юридическое лицо или физическое лицо, зарегистрированное в качестве индивидуального предпринимателя, заключившее отдельный договор с Платежной организацией, и в пользу которого Клиент осуществляет платеж в счет оплаты за Товары.

«**Правила**» – настоящие Правила.

«**Правила ОДПО**» – имеет значение, данное этому термину в разделе *Вводные положения*.

«**Претензия**» – имеет значение, данное этому термину в пункте 6.3.

«**Сайт**» – web-сайт Платежной организации, размещенный в сети Интернет по электронному адресу: office@dreidel.kz

«**Система**» **–** совокупность программно-технических средств, документации и организационно-технических мероприятий, обеспечивающих информационно-технологическое взаимодействие, регистрацию и осуществление платежей и иных Операций в соответствии с настоящими Правилами.

«**Товар**» – товары, работы и услуги, а также права на результаты интеллектуальной деятельности, реализуемые Поставщиками услуг конечным потребителям для личного, семейного или домашнего использования.

«**Третьи лица**» – юридические лица и физические лица - индивидуальные предприниматели, которые:

(i) предоставляют технологическое обеспечение Платежных услуг или иным образом действуют в интересах Платежной организации; и

(ii) не являются аффилированными с Платежной организацией.

«**Участники расчетов**» – Поставщик услуг, Держатель платежной карты и Банк-эквайер.

2. Толкование

В настоящих Правилах:

(i) ссылки на пункты и Приложения являются ссылками на пункты и Приложения настоящих Правил;

(ii) термины в единственном числе включают в себя множественное число и наоборот; и

(iii) заголовки пунктов настоящих Правил введены только для удобства и не влияют на толкование содержания и условий настоящих Правил.

## ПРИЛОЖЕНИЕ 2. ВСТУПЛЕНИЕ В СИЛУ, ИЗМЕНЕНИЕ И ПРИМЕНЕНИЕ НАСТОЯЩИХ ПРАВИЛ

1. Настоящие Правила утверждены Решением общим собранием участников ТОО «Dreidel Finance (Дрейдл Финанс)» Платежной организации и вступают в силу с даты внесения Национальным Банком Республики Казахстан Платежной организации в реестр платежных организаций в соответствии с применимым законодательством.

2. Настоящие Правила могут быть изменены Решением общим собранием участников ТОО «Dreidel Finance (Дрейдл Финанс)» Платежной организации при условии обязательного согласования изменений настоящих Правил с уполномоченным органом в порядке и сроки, предусмотренные применимым законодательством.

3. Настоящие Правила являются обязательными для всех сотрудников Платежной организации и привлекаемых ею Третьих лиц.

4. Платежная организация вправе установить исключения по действию отдельных пунктов настоящих Правил в отношении отдельных Участников расчетов, за исключением случаев, когда такие изменения обусловлены императивными требованиями применимого законодательства.

5. Если у кого-либо из сотрудников Платежной организации и привлекаемых ею Третьих лиц возникают вопросы относительно порядка применения настоящих Правил, иных политик Платежной организации или требований применимого законодательства, они могут обратиться за консультацией в правовой департамент Платежной организации, направив электронное письмо по адресу электронной почты office@dreidel.kz, или по телефону +7 727 350 5356.

## ПРИЛОЖЕНИЕ 3. АЛГОРИТМ ОКАЗАНИЯ ПЛАТЕЖНЫХ УСЛУГ

1. Оказание Платежных услуг осуществляется согласно следующему алгоритму:

**Шаг 1**. Клиент заходит на платежную форму Платежной организации посредством сети Интернет.

**Шаг 2**. Клиент знакомится с порядком предоставления Платежных услуг, включая размер комиссии, взимаемой Платежной организацией, и предоставляет согласие на оказание соответствующей Платежной услуги, принимая условия оферты, размещенной на Сайте.

**Шаг 3**. Клиент инициирует платеж в пользу Поставщика услуги.

**Шаг 4**. По согласованию с Платежной организацией Поставщик услуги выбирает наиболее удобный вариант авторизации (одностадийная либо двухстадийная).

**Шаг 5**. Клиент вводит в платежную форму реквизиты банковской карты для исполнения платежа Банком.

**Шаг 6**. Платежная организация посредством запроса в Банк инициирует поручение Клиента.

**Шаг 7**. Банк производит списание денег с банковской карты и осуществляет перевод платежа в пользу Поставщика услуг, указанного в поручении Клиента, с учетом вознаграждения Платежной организации и комиссионного вознаграждения Банка.

**Шаг 8**. После получения от Банка подтверждения исполнения Операции Платежная организация направляет Клиенту электронный чек (квитанцию об оплате), подтверждающий совершение Операции. С этого момента платеж считается принятым, а Платежная услуга – оказанной.

2. Движение денежных средств при положительно обработанной Операции в рамках вышеуказанного алгоритма выглядит следующим образом:

   (i) Банк-эмитент осуществляет списание денежных средств с банковской карты Клиента;

   (ii) Банк-эмитент осуществляет платеж в пользу Банка-эквайера; и

   (iii) Банк-эквайер перечисляет денежные средства (за исключением вознаграждения Платежной организации и комиссии Банка-эквайера) либо:

      (A) напрямую на счет Поставщика услуг; или

      (B) на специальный (транзитный) счет Банка, с которым у Платежной организации заключен соответствующий договор. В этом случае после зачисления платежей на такой специальный (транзитный) счет Банка, Платежная организация передает Банку электронные реестры платежей с указанием суммы и реквизитов Поставщика услуг, которому необходимо зачислить платежи, а Банк осуществляет соответствующий перевод платежей на указанный счет Поставщика услуг.

3. В случае отказа Клиента от Платежной услуги, либо при необходимости отмены ранее осуществленной Операции, Поставщик услуг инициирует проведение таких Операций в личном кабинете Системы.

4. Совершение Операций фиксируется Платежной организацией в электронном виде и хранится в АПК Платежной организации в течение предусмотренного применимым законодательством срока.

## ПРИЛОЖЕНИЕ 4. МЕРОПРИЯТИЯ И СПОСОБЫ УПРАВЛЕНИЯ РИСКАМИ

1. В целях эффективного управления и контроля над рисками Платежная организация разрабатывает и проводит следующие мероприятия:

   (i) формирование организационной структуры управления рисками, обеспечивающей надлежащий контроль за выполнением партнерами Платежной организации требований к управлению рисками, установленных настоящими Правилами;

   (ii) определение методик анализа рисков;

   (iii) определение порядка оценки качества функционирования операционных и технологических средств, процедур и информационных систем, а также определение порядка их изменения;

   (iv) определение порядка обеспечения защиты информации в Платежной организации;

   (v) определение порядка обеспечения и показателей непрерывности функционирования Системы;

   (vi) определение порядка обмена информацией, необходимой для управления рисками, а также порядка взаимодействия в чрезвычайных ситуациях, включая случаи Инцидентов информационной безопасности; и

   (vii) определение функциональных обязанностей лиц и соответствующих структурных подразделений, ответственных за управление рисками.

2. Определение способов управления рисками в Платежной организации зависит от особенностей деятельности Платежной организации (включая сформированную в ней модель управления рисками, процедуры платежного клиринга и расчетов, количество переводов денежных средств и их суммы). При этом, способы управления рисками включают (без ограничения) следующие:

   (i) установление предельных размеров (лимитов) обязательств Поставщиков услуг;

   (ii) управление очередностью исполнения распоряжений должностными лицами;

   (iii) осуществление расчетов в Платежной организации до окончания рабочего дня; и

   (iv) использование безотзывных банковских гарантий.

## ПРИЛОЖЕНИЕ 5. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. *Стандарты качества программного обеспечения*

Платежная организация внедряет и использует в своей деятельности современное программное обеспечение, которое отвечает всем применимым стандартам информационной безопасности и обеспечивает:

(i) 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;

(ii) многоуровневый доступ к входным данным, функциям, операциям, отчетам, реализованным в программном обеспечении, предусматривающим, как минимум, два уровня доступа: администратор и пользователь;

(iii) возможность поиска информации по критериям и параметрам, определенным для данной информационной системы, с сохранением запроса, а также сортировку информации по любым параметрам;

(iv) обработку информации и ее хранение по дате и времени;

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

(vi) возможность обмена электронными документами;

(vii) автоматизированное формирование форм отчетов, представляемых Платежной организацией в уполномоченный орган, а также отчетов о проведенных Операциях; и

(viii) регистрацию и идентификацию происходящих в информационной системе событий с сохранением таких атрибутов, как: дата и время начала события, наименование события, пользователь, производивший действие, идентификатор записи, дата и время окончания события, результат выполнения события.

2. *Безопасность вычислительных сетей*

Защита сетевой инфраструктуры Платежной организации осуществляется в рамках следующих компонентов:

(i) сервер: доступ до терминальной сессии сервера осуществляется путем аутентификации. Допускается использовать одновременно не более двух сессий терминала; и

(ii) рабочие станции: доступ в сеть Интернет рабочих станций осуществляется путем подключения к WIFI роутеру с защитой подключения типа WPA2-PSK. Рабочие станции подключаются только к локальной сети Платежной организации. Пароль от учетной записи выдается каждому сотруднику под

личную ответственность и может быть изменен только системным администратором.

3. *Доступ пользователей к данным*

Процесс управления доступом пользователей регулируется внутренними актами Платежной организации. Предоставление доступа осуществляется в соответствии с принципом минимально необходимых полномочий для выполнения должностных обязанностей.

4. *Учетные записи*

Работа пользователей в операционных системах осуществляется под уникальными учетными записями. Не допускается работа пользователя под чужой учетной записью и учетной записью «Администратор» или «Гость». Аутентификация на сервере осуществляется путем подключения к терминалу и ввода пользователем персональных данных, предоставленных системным администратором. Для предоставления временного доступа к ресурсам Платежной организации предоставляются временные учетные записи с ограниченным сроком действия.

5. *Пароли учетных записей в операционных системах*

Пароли учетных записей в операционных системах:

(i) должны иметь длину не менее 8 символов;

(ii) должны быть достаточно сложными и содержать символы всех четырех категорий: буквы нижнего регистра, буквы верхнего регистра, цифры и специальные символы; и

(iii) не должны включать осмысленные слова и легко вычисляемые сочетания, общепринятые аббревиатуры и идентифицируемую с их владельцами информацию (персональные данные).

Пароли учетных записей в операционных системах должны меняться:

(i) для систем, поддерживающих автоматическую смену паролей – ежемесячно; и

(ii) для иных систем – каждые 90 (девяносто) дней.

6. *Встроенные учетные записи*

Пароли, первоначально установленные производителем информационных систем для встроенных учетных записей, должны быть изменены при первом подключении информационных систем.

7. *Удаление / блокировка учетной записи*

Учетная запись сотрудника удаляется немедленно при его увольнении. При выходе сотрудника в отпуска или на больничный, учетные записи в операционных системах подлежат блокировке до момента возвращения сотрудника на работу.

8. *Конфиденциальный режим использования учетной записи*

Пользователям запрещается:

(i) разглашать информацию о своих учетных записях; и

(ii) предоставлять доступ к своими учетным записям другим сотрудникам Платежной организации и иным лицам, за исключением случаев исполнения своих должностных обязанностей системным администратором при настройке компьютера пользователя.

При неактивном состоянии компьютера более пяти минут компьютер должен быть автоматически переведен в заблокированное состояние. Блокировка выполняется путем настроек операционной системы на рабочем месте сотрудника. Оставляя рабочее место, каждый сотрудник Платежной организации обязуется самостоятельно заблокировать свою учетную запись.

9. *Обеспечение антивирусной защиты*

В качестве антивирусного программного обеспечения может быть использовано только лицензионное программное обеспечение или программное обеспечение, распространяемое бесплатно, при этом антивирусное программное обеспечение в обязательном порядке должно быть установлено на серверах и на каждом персональном компьютере Платежной организации.

10. *Обеспечение физической безопасности*

В Платежной организации должен быть ограничен физический доступ сотрудников и Третьих лиц к компонентам серверной информационной инфраструктуры. Соответствующий доступ может быть предоставляется исключительно в целях выполнения должностных или договорных обязательств в минимально требуемом объеме.

11. *Инциденты информационной безопасности*

Информация об Инцидентах информационной безопасности, полученная в ходе мониторинга деятельности по обеспечению информационной безопасности, подлежит консолидации, систематизации и хранению. Срок хранения информации об Инцидентах информационной безопасности составляет не менее 5 (пяти) лет.

Платежной организацией определяется порядок принятия неотложных мер к устранению Инцидента информационной безопасности, его причин и последствий.

В Платежной организации ведется журнал учета Инцидентов информационной безопасности с отражением всей информации об Инциденте информационной безопасности, принятых мерах и предлагаемых корректирующих мерах.

Платежная организация предоставляет в уполномоченный орган информацию о следующих Инцидентах информационной безопасности:

(1) эксплуатация уязвимостей в 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 контроля информационной безопасности; и

(6) Инцидентах информационной безопасности, подрывающих стабильность деятельности Платежной организации.

Информация об Инцидентах информационной безопасности, указанная в настоящем пункте 11, предоставляется Платежной организацией в уполномоченный орган максимально оперативно и, в любом случае, не позднее 48 часов с момента выявления, в виде карты Инцидента информационной безопасности по форме, приложенной к Правилам ОДПО.

12. *Непрерывное функционирование информационной инфраструктуры*

Для обеспечения отказоустойчивости применяется дублирование критичных компонентов информационной инфраструктуры Платежной организации. Средствами резервного копирования обеспечивается гарантированное восстановление бизнес-процессов после сбоя в работе одного или нескольких компонентов информационной инфраструктуры, а также минимизация времени восстановления сервисов и бизнес-процессов.