AML / CFT POLICY

ООО «ИТ Решения»

Дата вступления в силу: 16 апреля 2026
Версия: 1.0

1. Общие положения

1.1 О компании

Общество с ограниченной ответственностью «ИТ Решения» зарегистрировано в Кыргызской Республике и осуществляет деятельность, связанную с дистанционной продажей цифровых товаров через сайт happy-cat-play.ru.

К цифровым товарам относятся цифровые подарочные карты и/или цифровые коды Steam Gift Card / Steam Wallet Code, передаваемые покупателям в электронном виде.

Юридический адрес:

Кыргызская Республика, г. Бишкек, Октябрьский р-н, уч. СК «Горный ветерок»

ИНН: 01203202610354

Регистрационный номер: 326636-3301-ООО

1.2 Назначение политики

Настоящая AML / CFT Policy устанавливает внутренние принципы и меры, направленные на:

• снижение риска использования сервиса в целях легализации (отмывания) денежных средств;

• предотвращение мошеннических операций;

• ограничение операций, связанных с запрещёнными или высокорискованными направлениями;

• соблюдение требований банков, платёжных партнёров, агента и применимого законодательства.

1.3 Характер деятельности

Компания осуществляет продажу цифровых товаров, включая цифровые подарочные карты и/или цифровые коды Steam Gift Card / Steam Wallet Code.

Покупатель выбирает цифровой товар и его номинал, указывает адрес электронной почты для получения цифрового кода и оплачивает заказ через доступный платёжный способ.

После подтверждения оплаты Компания передаёт Покупателю цифровой код в электронном виде путём отправки на указанный e-mail, отображения в интерфейсе заказа либо иным электронным способом.

Активация цифрового кода осуществляется Покупателем самостоятельно в своём аккаунте Steam.

Компания не является банком, платёжной организацией, оператором электронных денежных средств, оператором денежных переводов или обменным сервисом.

Компания не оказывает услуги по пополнению аккаунтов, не принимает денежные средства для последующего перевода третьим лицам, не осуществляет вход в аккаунты Steam Покупателей и не управляет аккаунтами Покупателей.

2. Бизнес-модель

2.1 Общая схема

Покупатель на сайте выбирает цифровой товар — цифровую подарочную карту и/или цифровой код Steam Gift Card / Steam Wallet Code выбранного номинала.

При оформлении заказа Покупатель указывает адрес электронной почты для получения цифрового кода.

После оформления заказа Покупателю предоставляется платёжная ссылка либо иная платёжная форма.

После успешной оплаты Компания проверяет статус оплаты и риск-параметры заказа.

При отсутствии признаков нарушений Компания передаёт Покупателю цифровой код в электронном виде.

Покупатель самостоятельно активирует полученный цифровой код в своём аккаунте Steam.

2.2. Партнёрская инфраструктура

Для исполнения заказов Компания вправе привлекать:

• агента;

• платёжных партнёров;

• поставщиков цифровых товаров;

• технических подрядчиков;

• antifraud-системы;

• иные сервисы, участвующие в обработке платежа, проверке операции, передаче цифрового товара и рассмотрении спорных ситуаций.

2.3 Момент исполнения заказа

Заказ считается исполненным с момента отправки цифрового кода на e-mail Покупателя, отображения цифрового кода в интерфейсе заказа либо предоставления Покупателю доступа к цифровому коду иным электронным способом.

После передачи цифрового кода Покупателю обязательство Компании по передаче цифрового товара считается исполненным.

2.4. Ограничение назначения сервиса

Сервис предназначен исключительно для покупки цифровых товаров для личного использования Покупателем.

Использование сервиса для денежных переводов, вывода денежных средств, транзита платежей, обналичивания, оплаты запрещённых направлений или покупки цифровых товаров в интересах неизвестных третьих лиц не допускается.

3. Подход к оценке рисков

3.1 Основные риски

Компания учитывает, в частности, следующие риски:

• использование чужих платёжных средств или платёжных реквизитов;

• мошеннические операции и fraud-активность;

• возвраты платежей и спорные транзакции;

• множественные либо атипичные покупки цифровых товаров;

• попытки использования сервиса не по назначению;

• попытки использования сервиса для денежных переводов, транзита платежей, вывода или обналичивания денежных средств;

• покупка цифровых кодов по просьбе неизвестных третьих лиц;

• попытки перепродажи цифровых кодов без согласования с Компанией;

• попытки использования сервиса в интересах запрещённых или высокорискованных направлений;

• санкционные риски;

• указание недостоверных контактных данных;

• технические манипуляции, направленные на обход ограничений сервиса, лимитов и платёжной инфраструктуры.

3.2 Уровень риска

С учётом цифрового характера товаров, дистанционного оформления заказов и использования платёжной инфраструктуры общий риск оценивается как средний, с повышенным вниманием к fraud-операциям, chargeback-рискам, множественным покупкам цифровых кодов и нецелевому использованию сервиса.

3.3. Риск-ориентированный подход

Компания применяет риск-ориентированный подход и вправе усиливать проверку отдельных заказов с учётом:

• суммы операции;

• частоты заказов;

• истории Покупателя;

• совпадения или расхождения технических и платёжных параметров;

• признаков использования чужих платёжных средств;

• признаков покупки цифровых товаров в интересах третьих лиц;

• сигналов от банка, агента, платёжного партнёра, поставщика цифрового товара или технической системы мониторинга.

4. Ограничения и запрещённые направления

4.1 Запрещённое использование

Запрещается использовать сервис для:

• оплаты услуг онлайн-казино, ставок, беттинга и букмекерских сервисов;

• оплаты контента 18+ и иных сервисов для взрослых;

• денежных переводов третьим лицам;

• вывода денежных средств;

• транзита платежей;

• обналичивания денежных средств;

• покупки цифровых товаров по просьбе неизвестных лиц, “работодателей”, “служб поддержки”, “брокеров” или иных третьих лиц;

• массовой покупки цифровых кодов для перепродажи без согласования с Компанией;

• операций, не связанных напрямую с покупкой цифрового товара для личного использования;

• операций, нарушающих требования законодательства, правила банков, платёжных систем, агента, поставщиков цифровых товаров или технических партнёров;

• использования чужих платёжных средств, чужих платёжных реквизитов либо недостоверных контактных данных;

• мошеннических, санкционных, незаконных или репутационно рискованных операций.

4.2 Высокорискованные операции

Компания вправе отказать в исполнении заказа, отменить заказ либо приостановить передачу цифрового товара при выявлении признаков того, что операция:

• связана с запрещённой или высокорискованной деятельностью;

• может нарушать применимое законодательство;

• может быть связана с использованием чужих платёжных средств;

• может использоваться для вывода, транзита или обналичивания денежных средств;

• может причинить ущерб банку, агенту, платёжному партнёру, поставщику цифрового товара, техническому подрядчику или деловой репутации Компании.

5. Идентификация и данные пользователей

5.1 Обрабатываемые сведения

В зависимости от характера заказа и технической реализации сервиса Компания может обрабатывать:

• адрес электронной почты Покупателя;

• номер заказа;

• выбранный цифровой товар и его номинал;

• номер телефона, если он используется при оформлении заказа, коммуникации, возврате или дополнительной проверке;

• сумму и параметры заказа;

• сведения о платёжной операции;

• данные, предоставленные Покупателем при обращении в поддержку;

• технические данные, включая IP-адрес, cookie, данные браузера и устройства, дату и время обращения, адреса посещаемых страниц и служебные логи.

Логин, идентификатор или иные данные аккаунта Steam не являются обязательными данными для оформления заказа и могут обрабатываться только в случае, если Покупатель самостоятельно предоставил такие сведения при обращении в поддержку или при рассмотрении спорной ситуации.

5.2 Минимизация данных

Компания стремится обрабатывать только те данные, которые необходимы для:

• оформления и исполнения заказа;

• обработки платежа;

• передачи цифрового товара Покупателю;

• возврата средств в предусмотренных случаях;

• противодействия мошенничеству;

• рассмотрения обращений и спорных ситуаций;

• соблюдения требований законодательства и правил партнёров.

5.3 Дополнительная проверка

Дополнительные меры проверки могут применяться, в частности, при:

• высокой сумме заказа;

• множественных операциях за короткий период;

• выявлении несоответствий в платёжных или технических данных;

• признаках использования чужих платёжных средств;

• признаках покупки цифровых товаров в интересах третьих лиц;

• подозрительном поведении Покупателя;

• сигналах от банка, агента, платёжного партнёра, поставщика цифрового товара или технической системы мониторинга.

В рамках дополнительной проверки Компания вправе запросить подтверждение e-mail, уточнение данных заказа, подтверждение принадлежности платёжного средства, дополнительные сведения для проверки операции, а также иные данные, необходимые для оценки fraud-, AML-, санкционного или иного комплаенс-риска.

6. Мониторинг операций

6.1. Контроль заказов и транзакций

Компания осуществляет мониторинг заказов и платёжных событий в пределах доступной ей информации и технических возможностей.

6.2. Анализируются, в частности:

• частота заказов;

• повторяющиеся суммы;

• множественные покупки цифровых товаров;

• техническое поведение Покупателя;

• региональные и технические несоответствия;

• история предыдущих операций;

• статусы и результаты платёжных событий;

• признаки обхода ограничений сервиса;

• признаки использования сервиса для нецелевых, запрещённых или высокорискованных операций.

6.3. Источники сигналов риска

При анализе риска могут учитываться:

• собственные внутренние данные Компании;

• сигналы банка;

• сигналы агента;

• сигналы платёжных партнёров;

• сигналы технических подрядчиков и antifraud-систем.

7. Меры реагирования

7.1 При выявлении риска Компания вправе

• приостановить обработку заказа до завершения проверки;

• запросить уточнение данных;

• запросить подтверждение принадлежности платёжного средства;

• отменить заказ до передачи цифрового кода;

• отказать в исполнении заказа при выявлении признаков нарушения;

• приостановить передачу цифрового товара до завершения проверки;

• инициировать возврат денежных средств в случаях и порядке, допустимых применимыми правилами и законодательством;

• передать необходимую информацию банку, агенту, платёжному партнёру, поставщику цифрового товара или иному уполномоченному лицу в объёме, необходимом для проверки и исполнения обязанностей.

7.2 Подозрение на мошенничество

При подозрении на fraud, использовании чужих платёжных средств, покупке цифровых товаров в интересах третьих лиц или иных нарушениях Компания вправе временно приостановить заказ и провести дополнительную проверку.

7.3 Решение по результатам проверки

По результатам проверки заказ может быть:

• исполнен;

• отклонён;

• отменён;

• возвращён;

• передан на дополнительное рассмотрение в рамках взаимодействия с банком, агентом, платёжным партнёром или поставщиком цифрового товара.

8. Возвраты и спорные операции

8.1 Основания для рассмотрения возврата

Покупатель вправе обратиться за рассмотрением вопроса о возврате денежных средств, если:

• заказ не был исполнен;

• цифровой код не был передан Покупателю;

• произошёл технический сбой;

• произошло ошибочное списание;

• переданный цифровой код оказался недействительным, ранее использованным или не соответствующим оплаченному номиналу, и это подтверждено проверкой Компании, поставщика цифрового товара или партнёра;

• выявлены иные обстоятельства, подтверждённые по результатам рассмотрения обращения.

8.2 Ограничения

До передачи цифрового кода Покупателю заказ может быть отменён, если он ещё не был исполнен.

После передачи цифрового кода Покупателю возврат денежных средств, как правило, невозможен, поскольку цифровой товар считается переданным.

Возврат после передачи цифрового кода возможен только в случаях, когда:

• цифровой код оказался недействительным;

• цифровой код был ранее использован до передачи Покупателю;

• цифровой код не соответствует оплаченному номиналу;

• ошибка подтверждена проверкой Компании, поставщика цифрового товара, банка, агента или платёжного партнёра;

• возврат допускается применимым законодательством, правилами банка, агента, платёжных партнёров или технической возможностью соответствующего сервиса.

Если Покупатель указал неверный e-mail, Компания вправе провести проверку и повторно отправить цифровой код при наличии технической возможности и подтверждении принадлежности заказа Покупателю.

8.3 Сроки и порядок

Сроки и порядок возврата определяются с учётом правил платёжной инфраструктуры, характера спорной ситуации, статуса передачи цифрового товара, результатов проверки и требований применимого законодательства.

9. Санкционная и комплаенс-политика

9.1. Общий подход

Компания принимает разумные меры для недопущения использования сервиса в интересах лиц, деятельности или операций, связанных с санкционными ограничениями, мошенничеством либо иными запрещёнными направлениями.

9.2. Право отказа

При выявлении повышенного санкционного, правового, fraud-, AML- или репутационного риска Компания вправе отказать в исполнении заказа, отменить заказ либо приостановить передачу цифрового товара до завершения проверки.

10. Хранение данных и передача данных

10.1 Хранение данных

Компания хранит информацию о:

• заказах;

• Покупателях;

• платёжных событиях;

• статусах операций;

• передаче цифровых товаров;

• обращениях и спорных случаях;

• технических логах и служебных данных,

в объёме и в течение срока, необходимых для обеспечения безопасности, рассмотрения споров, ведения учёта, противодействия мошенничеству и соблюдения требований законодательства.

10.2. Передача данных

Компания вправе передавать данные:

• агенту;

• платёжным партнёрам;

• поставщикам цифровых товаров;

• техническим подрядчикам;

• банкам;

• государственным органам,

если такая передача необходима для исполнения заказа, обработки оплаты, передачи цифрового товара, проверки операции, рассмотрения спорной ситуации, соблюдения требований законодательства или правил партнёров.

11. Ответственное лицо

11.1. Ответственность

Ответственным за соблюдение настоящей AML / CFT Policy является уполномоченное Компанией лицо.

11.2. Обязанности ответственного лица

Ответственное лицо обеспечивает:

• контроль рисков;

• анализ подозрительных операций;

• взаимодействие с банками, агентом, платёжными партнёрами и поставщиками цифровых товаров;

• принятие решений по спорным и рискованным заказам;

• актуализацию внутренних процедур при изменении бизнес-модели или требований партнёров.

12. Обновление политики

12.1. Изменение документа

Компания вправе обновлять настоящую политику в зависимости от:

• изменений бизнес-модели;

• подключения новых платёжных решений;

• изменения требований банков, агента, платёжных партнёров или регуляторных ожиданий;

• выявления новых рисков или изменения риск-профиля сервиса.

12.2. Актуальная редакция

Актуальная редакция политики хранится у Компании и может использоваться для предоставления банкам, платёжным партнёрам и иным уполномоченным лицам по запросу.

Контакты:

ООО «ИТ Решения»

Кыргызская Республика, г. Бишкек, Октябрьский р-н, уч. СК «Горный ветерок»

Email: happycatplayru@gmail.com

Telegram: @happycatplayru

Подпись: 

Расшифровка подписи: Кушбактов Усмонали Реджабалиевич