D-13

Политика раскрытия уязвимостей

Редакция	Дата публикации	Вступает в силу
1.0	**01.10.2026**	**01.10.2026**
Оператор	Язык оригинала	Адрес публикации
ТОО «SteppeGate», БИН 260140019690, Республика Казахстан	**русский**	**https://dalaway.kz/legal/security**

---

1. Назначение

1.1. Настоящая Политика описывает, как сообщить Оператору о найденной уязвимости в его сервисах, что при исследовании допускается, а что нет, и чего исследователю следует ожидать в ответ.

1.2. Оператором сайта и цифровой платформы Dalaway является ТОО «SteppeGate», БИН 260140019690.

1.3. Оператор признаёт вклад независимых исследователей в безопасность сервиса и стремится рассматривать добросовестные сообщения об уязвимостях.

---

2. Область действия

2.1. Настоящая Политика распространяется на принадлежащие Оператору общедоступные ресурсы: домен dalaway.kz и его поддомены, а также общедоступные программные интерфейсы Платформы.

2.2. **Настоящая Политика не даёт разрешения на какие-либо действия в отношении данных Участников.** Учётные записи Пользователей, Лоты, Запросы, Предложения, Сделки, Приложения, Торговые операции, переписка Участников, размещённые ими документы и любые иные сведения Участников в область исследования не входят.

2.2-1. Из запрета, установленного пунктом 2.2, исключены собственные учётные записи исследователя и созданные им искусственные тестовые данные — в объёме, предусмотренном пунктом 4.3. Действия в отношении данных иных Участников остаются недопустимыми независимо от того, с какой учётной записи они совершены.

2.3. Настоящая Политика не распространяется на информационные системы Участников и их контрагентов, в том числе когда такие системы взаимодействуют с Платформой.

2.4. Настоящая Политика не распространяется на сервисы сторонних поставщиков, привлечённых Оператором. Сообщения об уязвимостях таких сервисов направляются их поставщикам; Оператор при необходимости содействует передаче сообщения.

---

3. Как сообщить об уязвимости

3.1. Сообщение направляется на адрес **security@dalaway.kz**.

3.2. При признаках критичности в теме письма указывается «SECURITY — CRITICAL».

3.3. В сообщении рекомендуется указать:

Сведение	Назначение
Описание уязвимости	Что именно обнаружено
Затронутый адрес или интерфейс	Где воспроизводится
Шаги воспроизведения	Как повторить
Дата и время обнаружения	Соотнесение с журналами Оператора
Возможные последствия	Оценка влияния
Подтверждение	При наличии — минимальное, в объёме, достаточном для демонстрации

3.4. Сообщение принимается на русском, казахском и английском языках.

3.5. Оператор просит не направлять в сообщении персональные данные третьих лиц и сведения Участников. Если такие сведения необходимы для описания уязвимости, объём указывается словами, а сами сведения не прикладываются.

---

4. Что допускается

4.1. Действия с минимальным воздействием на работу сервиса и на данные.

4.2. Исследование общедоступных сведений и поведения общедоступных интерфейсов.

4.3. Действия в отношении собственных учётных записей исследователя и созданных им для целей исследования тестовых данных.

4.4. Подтверждение уязвимости в минимальном объёме.

4.5. **Принцип, которым Оператор предлагает руководствоваться.** Цель добросовестного исследования — показать, что проблема существует, а не показать, какой ущерб при её помощи можно причинить. Как только существование уязвимости подтверждено, исследование прекращается и направляется сообщение.

---

5. Что не допускается

5.1. Без предварительного письменного разрешения Оператора не допускаются:

1. Отказ в обслуживании, нагрузочное тестирование и иные действия, влияющие на доступность сервиса.
2. Перебор учётных данных и попытки входа в чужие учётные записи.
3. Доступ к данным других лиц, их выгрузка, изменение, удаление или распространение.
4. Размещение вредоносного программного обеспечения и закрепление в системе.
5. Социальная инженерия в отношении работников Оператора, Участников и их работников, в том числе фишинг.
6. Физический доступ к помещениям и оборудованию.
7. Использование обнаруженных ключей, токенов и учётных данных для доступа к другим системам.
8. Действия в отношении систем и данных Участников и их контрагентов.

5.2. **Если доступ к чужим данным получен непреднамеренно**, исследователь немедленно прекращает действия, не сохраняет и не распространяет полученные сведения, удаляет их копии и сообщает Оператору о факте и о примерном объёме затронутых сведений.

---

6. Что делает Оператор

6.1. Оператор подтверждает получение сообщения, проводит проверку, оценивает влияние и сообщает исследователю об устранении уязвимости.

6.2. Оператор стремится отвечать на качественные сообщения в разумный срок. **Оператор не принимает на себя обязательства ответить или устранить уязвимость**

в определённый срок.

6.3. Оператор вправе запросить у исследователя дополнительные сведения.

6.4. Оператор вправе прекратить взаимодействие с исследователем, направившим сообщение с нарушением раздела 5, а также не рассматривать сообщения, не содержащие описания уязвимости.

---

7. Выплаты за сообщения об уязвимостях

7.1. **Публичной программы выплат за сообщения об уязвимостях Оператор не ведёт. Выплата не гарантируется.**

7.2. По согласованию с исследователем Оператор вправе указать его в перечне лиц, содействовавших безопасности сервиса.

---

8. Публикация сведений об уязвимости

8.1. Оператор просит предоставить разумное время для проверки, устранения уязвимости и выпуска исправления до публикации сведений о ней.

8.2. Дату публикации и степень технической детализации Оператор просит согласовать заранее.

8.3. **Сведения Участников не подлежат публикации ни при каких условиях**, в том числе в обезличенном виде, если из них возможно установить Участника или Сделку.

---

9. Правовая позиция Оператора

9.1. Исследование, проведённое добросовестно и в пределах настоящей Политики, Оператор не рассматривает как основание для предъявления исследователю требований и не расценивает как недобросовестные действия.

9.2. Настоящая Политика не отменяет и не заменяет требований законодательства Республики Казахстан и не освобождает исследователя от ответственности за действия, выходящие за её пределы.

9.3. Настоящая Политика не является разрешением на действия в отношении прав и имущества третьих лиц.

9.4. Настоящая Политика не создаёт обязательств Оператора перед исследователем по выплате вознаграждения, признанию заслуг, соблюдению сроков рассмотрения в интересах исследователя либо предоставлению иных выгод и не является офертой. Действия, которые Оператор выполняет по разделу 6, совершаются в собственном интересе Оператора и обязательством перед исследователем не становятся.

9.5. Оператор вправе изменять настоящую Политику. К уже направленному сообщению применяется редакция, действовавшая на дату его направления.

---

10. Что не направляется по этому адресу

10.1. Адрес, указанный в пункте 3.1, предназначен исключительно для сообщений об уязвимостях.

Вопрос	**Куда**
Обращения по Сделкам, Лотам, Предложениям и расчётам	Вызов модератора из карточки соответствующего объекта либо hello@dalaway.kz
Вопросы обработки персональных данных, отзыв согласия, права субъекта	privacy@dalaway.kz
Жалобы на содержание размещённых материалов	Порядок, предусмотренный Правилами площадки
Общие и коммерческие вопросы	hello@dalaway.kz

---

11. Реквизиты Оператора

Наименование	Товарищество с ограниченной ответственностью «SteppeGate»
БИН	260140019690
Адрес для корреспонденции	010000, г. Астана, район Сарыарка, ул. Бердибек Сокпакбаев, д. 5, н.п. 44, БЦ «Арлан», 3 этаж
Сообщения об уязвимостях	security@dalaway.kz
Общие вопросы	hello@dalaway.kz

Архив редакций. Действующая редакция — 1.0 от 01.10.2026, вступает в силу 01.10.2026. Предыдущих редакций нет.