D-13

Vulnerability Disclosure Policy

Version	Publication date	Effective date
1.0	**01.10.2026**	**01.10.2026**
Operator	Original language	Publication URL
SteppeGate LLP, BIN 260140019690, Republic of Kazakhstan	**Russian**	**https://dalaway.kz/legal/security**

1. Purpose

1.1. This Policy explains how to report a vulnerability found in the Operator's services, what is and is not permitted during research, and what the researcher should expect in response.

1.2. The operator of the Dalaway website and digital platform is SteppeGate LLP, BIN 260140019690.

1.3. The Operator recognises independent researchers' contribution to the security of the service and endeavours to consider good-faith vulnerability reports.

2. Scope

2.1. This Policy applies to publicly accessible resources owned by the Operator: the dalaway.kz domain and its subdomains, and publicly accessible application programming interfaces of the Platform.

2.2. This Policy does not authorise any actions concerning Participants' data. Users' accounts, Lots, Requests, Offers, Transactions, Appendices, Trading Operations, Participants' correspondence, documents uploaded by them and any other Participant information are outside the scope of research.

2.2-1. The researcher's own accounts and artificial test data created by the researcher are excluded from the prohibition in clause 2.2, to the extent provided for in clause 4.3. Actions concerning other Participants' data remain prohibited regardless of the account from which they are performed.

2.3. This Policy does not apply to the information systems of Participants or their counterparties, including where such systems interact with the Platform.

2.4. This Policy does not apply to services of third-party providers engaged by the Operator. Vulnerability reports concerning those services must be sent to their providers; the

Operator assists in forwarding the report where necessary.

3. How to Report a Vulnerability

3.1. Reports must be sent to security@dalaway.kz.

3.2. Where there are indications of critical severity, the subject line must state “SECURITY — CRITICAL”.

3.3. The following information is recommended in the report:

Information	Purpose
Description of the vulnerability	What exactly was discovered
Affected address or interface	Where the issue can be reproduced
Steps to reproduce	How to reproduce the issue
Date and time of discovery	Correlation with the Operator’s logs
Potential consequences	Impact assessment
Evidence	If available, minimal evidence sufficient to demonstrate the issue

3.4. Reports are accepted in Russian, Kazakh and English.

3.5. The Operator requests that reports contain no third-party personal data or Participant information. If such information is necessary to describe the vulnerability, describe its extent in words without attaching the information itself.

4. Permitted Actions

4.1. Actions with minimal impact on the operation of the service and on data.

4.2. Examining publicly accessible information and the behaviour of publicly accessible interfaces.

4.3. Actions concerning the researcher’s own accounts and test data created by the researcher for research purposes.

4.4. Demonstrating the vulnerability to the minimum extent necessary.

4.5. The principle the Operator suggests following. The purpose of good-faith research is to demonstrate that a problem exists, rather than the harm that could be caused by exploiting it. As soon as the existence of the vulnerability is confirmed, research must cease and a report must be sent.

5. Prohibited Actions

5.1. Without the Operator's prior written permission, the following are prohibited:

1. Denial of service, load testing and other actions affecting service availability.
2. Brute-forcing credentials and attempting to log in to other persons' accounts.
3. Accessing, exporting, modifying, deleting or disseminating other persons' data.
4. Deploying malicious software and establishing persistence in the system.
5. Social engineering targeting the Operator's employees, Participants or their employees, including phishing.
6. Physical access to premises and equipment.
7. Using discovered keys, tokens or credentials to access other systems.
8. Actions concerning the systems and data of Participants and their counterparties.

5.2. If access to another person's data is obtained unintentionally, the researcher must immediately stop, refrain from retaining or disseminating the information obtained, delete any copies, and notify the Operator of the incident and the approximate extent of the information affected.

6. Actions Taken by the Operator

6.1. The Operator acknowledges receipt of the report, verifies it, assesses its impact and informs the researcher when the vulnerability has been remedied.

6.2. The Operator endeavours to respond to well-prepared reports within a reasonable time. The Operator does not undertake to respond or remedy a vulnerability within any specific period.

6.3. The Operator may request additional information from the researcher.

6.4. The Operator may cease communication with a researcher who submitted a report in breach of section 5 and may decline to consider reports that do not describe a vulnerability.

7. Payments for Vulnerability Reports

7.1. The Operator does not operate a public vulnerability reward programme. Payment is not guaranteed.

7.2. With the researcher's agreement, the Operator may include the researcher in a list of persons who have contributed to the security of the service.

8. Publication of Vulnerability Information

8.1. The Operator requests a reasonable time to verify and remedy the vulnerability and release a fix before information about it is published.

8.2. The Operator requests prior agreement on the publication date and level of technical detail.

8.3. Participant information must not be published under any circumstances, including in de-identified form if a Participant or Transaction can be identified from it.

9. The Operator’s Legal Position

9.1. The Operator does not regard research conducted in good faith and within the scope of this Policy as a ground for bringing claims against the researcher or as conduct in bad faith.

9.2. This Policy does not override or replace the requirements of the legislation of the Republic of Kazakhstan and does not relieve the researcher of liability for actions outside its scope.

9.3. This Policy does not authorise actions affecting the rights or property of third parties.

9.4. This Policy creates no obligation on the Operator towards the researcher to pay remuneration, recognise contributions, observe time limits for consideration in the researcher’s interests or provide other benefits, and does not constitute an offer. Actions taken by the Operator under section 6 are performed in the Operator’s own interests and do not become obligations towards the researcher.

9.5. The Operator may amend this Policy. The version in effect on the date a report was submitted applies to that report.

10. Matters Not to Be Sent to This Address

10.1. The address specified in clause 3.1 is intended exclusively for vulnerability reports.

Matter	Where to direct it
Requests concerning Transactions, Lots, Offers and settlements	Contact the moderator from the relevant object's card or email hello@dalaway.kz
Personal data processing, withdrawal of consent and data subject rights	privacy@dalaway.kz
Complaints about the content of posted materials	The procedure established by the Marketplace Rules
General and commercial enquiries	hello@dalaway.kz

11. Operator Details

Name	SteppeGate Limited Liability Partnership
BIN	260140019690
Correspondence address	010000, Astana, Saryarka District, 5 Berdibek Sokpakbayev Street, non-residential unit 44, Arlan Business Centre, 3rd floor
Vulnerability reports	security@dalaway.kz
General enquiries	hello@dalaway.kz

Version history. Current version — 1.0 of 01.10.2026, effective from 01.10.2026. No previous versions.