Fin Points

Connect Trading Future

Vulnerability Disclosure Policy

April 2025

Introduction

Fin Points Technology Pte. Ltd. (also as “Fin Points Tech”, “We”, “Our”, “us”) is committed to ensuring the security of our systems and protecting the information of our users. We welcome reports of potential vulnerabilities in our systems. However, to maintain the integrity and security of our services, **all security testing activities must receive prior written authorization**.

This policy outlines the scope of authorized research, how to report vulnerabilities, and what you can expect from us.

Authorization Requirement

Do not conduct any security testing without prior written approval from Fin Points Tech. Unauthorized testing is strictly prohibited and may result in legal action.

To request authorization, please send email request to security.cloud@doo.com.

Please include below information:

- Systems or components you intend to test
- Testing methodologies
- Proposed timeline
- Contact information

We will review your request and respond accordingly.

Scope

This policy applies to:

- Public-facing systems and services owned or operated by Fin Points Tech
- Web applications, APIs, and mobile applications developed by Fin Points Tech
- Infrastructure and cloud assets under our control

Out of Scope:

- Denial of Service (DoS) vulnerabilities

- Social engineering or phishing attacks
- Physical security vulnerabilities
- Spam or content-related issues

Reporting vulnerability

Once authorized, if you discover a vulnerability, please report via email to security.cloud@doo.com.

In order to help us triage and prioritize submissions, we recommend that your reports:

- Describe the location the vulnerability was discovered and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Be in English, if possible.

Report Response

Upon receiving your report:

- We will acknowledge receipt within **5 business days**.
- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues.

Safe Harbor

If you comply with this policy and conduct testing within the authorized scope:

- Your activities will be considered authorized.
- We will not initiate legal action against you.
- We will work with you to understand and resolve the issue promptly.

Report Feedback

Should you have any questions please reach out to security.cloud@doo.com. We appreciate your advice suggestion on this policy.