

# Responsible Disclosure Policy

## Purpose

At Safe Security, we prioritize our customers' and users' security and privacy. We are committed to protecting our systems and data while fostering collaboration with the security research community. This Responsible Disclosure Policy outlines our expectations and process for reporting security vulnerabilities in our core platform, mobile application, website, and infrastructure.

## Scope

Safe Security Responsible Disclosure Policy applies to:

- Safe Product
- Safe X Mobile Applications
- Safe Security Website
- Safe Infrastructure

## Vulnerability Reporting and Disclosure

### Reporting a Vulnerability

If you have identified a vulnerability on any of our web or mobile apps, we request you to follow the steps outlined below:

- **Prepare Your Report:** Ensure it meets all the criteria listed under "Requirements for a Valid Report."
- **Submit Your Report:** Send it to **[vulnerability\\_report@safe.security](mailto:vulnerability_report@safe.security)**. Include all required details and any additional context you deem necessary.
- **Acknowledgment:** You will receive an acknowledgment email confirming receipt of your report within seven working days.
- **Assessment and Validation:** Our security team will evaluate the report to verify the vulnerability, assess its severity, and determine its impact.
- **Follow-Up Communication:** We may contact you for additional information or clarification during the investigation.
- **Resolution and Updates:** Once validated, we will prioritize and address the issue

based on its severity. We will notify you when the issue is resolved or if additional time is required.

## **Requirement for a Valid Report**

To facilitate effective vulnerability reporting, your submission must include the following:

- Vulnerability Summary: Description, severity, and potential impact.
- Affected Resources: Specific URLs, APIs, or systems impacted.
- Steps to Reproduce: Clear and detailed instructions for reproducing the vulnerability.
- Proof of Concept (PoC): Code, screenshots, or other evidence to validate the vulnerability.
- Suggested Remediation: Recommendations for fixing the issue.
- Researcher Contact Information: Email address or other contact details for follow-up.
- Responsible Information Disclosure Policy Acknowledgement: Confirmation that the researcher will not disclose vulnerability details publicly until Safe Security provides approval.

## **Exclusions**

Security researchers must not:

- Engage in physical testing of facilities or resources
- Disclose vulnerability information except as outlined in the 'Reporting a Vulnerability' and 'Disclosure' sections below
- Engage in social engineering
- Execute or attempt to execute "Denial of Service" attacks
- Send unsolicited electronic mail to Safe Security users, including "phishing" messages
- Introduce malicious software
- Test in a manner which could degrade the operation of Safe Security systems
- Delete, alter, share, retain, or destroy Safe data

## **Prohibition on Public Disclosure**

You are prohibited from publicly disclosing the details of the reported vulnerability until the issue has been fixed, and you have received prior written approval from Safe Security. If you fail to strictly comply with the confidentiality requirement, we reserve the right to institute appropriate legal proceedings.

## **Grant of License**

By reporting the vulnerability, you grant Safe Security, its subsidiaries, and affiliates an irrevocable, worldwide, royalty-free, transferable, sublicensable right to use, reproduce, modify, distribute, adapt, and otherwise utilize the information related to the vulnerabilities for any purpose deemed appropriate by Safe Security. Further, you waive any claims, including express or implied contracts, arising from any disclosures accepted by Safe Security.

## **Recognition**

We value and appreciate the time and effort spent by researchers in helping us enhance our security. If your report meets the criteria for validity and significance, you will receive:

- An Appreciation Letter acknowledging your contribution.
- A Swag Package as a token of our gratitude.

Thank you for contributing to Safe Security's security. By working together, we can ensure a safer digital environment for everyone.