



SOSME VULNERABILITY DISCLOSURE POLICY

Framework: SOSME Enterprise Trust Framework

Document ID: TCP-SEC-002

Version: 1.0

Effective Date: [01.01.2025]

Last Updated: [01.01.2025]

Our Commitment

At SOSME, security is a shared responsibility.

We value the efforts of security researchers, customers, partners, and members of the security community who help us identify and responsibly report potential security vulnerabilities.

This Policy explains how to report suspected security issues and how SOSME manages vulnerability reports.

Security Reporting at a Glance

We encourage responsible disclosure.

If you believe you have identified a security vulnerability affecting SOSME, please:

- ✓ Report it to us promptly.
- ✓ Provide sufficient information to reproduce the issue.
- ✓ Allow us reasonable time to investigate and resolve the issue.
- ✓ Avoid publicly disclosing the vulnerability until it has been addressed or we agree on a coordinated disclosure.

1. Scope

This Policy applies to suspected security vulnerabilities affecting:

- ◆ SOSME Platform
- ◆ SOSME Mobile Applications
- ◆ SOSME Website
- ◆ SOSME APIs
- ◆ SOSME Studio



- ◆ Artificial Intelligence capabilities, including Yara AI
- ◆ Customer Portal
- ◆ Demo Environment
- ◆ Other SOSME services operated by SOSME

2. What to Report

Examples of security issues include:

- ◆ authentication or authorization weaknesses;
- ◆ access control issues;
- ◆ privilege escalation;
- ◆ security misconfigurations;
- ◆ vulnerabilities affecting customer information;
- ◆ remote code execution;
- ◆ injection vulnerabilities;
- ◆ cross-site scripting (XSS);
- ◆ cross-site request forgery (CSRF);
- ◆ insecure API behavior;
- ◆ cryptographic implementation concerns;
- ◆ vulnerabilities affecting Artificial Intelligence features;
- ◆ supply chain vulnerabilities;
- ◆ authentication bypass;
- ◆ exposed secrets or credentials;
- ◆ insecure cloud configuration; and
- ◆ other issues that may impact the confidentiality, integrity, or availability of SOSME Services.

3. Responsible Disclosure

When reporting a vulnerability, we ask that you:

- ◆ act in good faith;
- ◆ avoid accessing, modifying, or deleting customer information;

- ♦ avoid disrupting production services;
- ♦ perform only the minimum testing necessary to validate the issue;
- ♦ immediately stop testing if there is any risk of affecting other users; and
- ♦ keep the information confidential until the issue has been resolved or coordinated disclosure has been agreed.

4. What Not to Do

The following activities are not permitted without prior written authorization from SOSME:

- ♦ denial-of-service or stress testing;
- ♦ social engineering of SOSME personnel or customers;
- ♦ phishing campaigns;
- ♦ physical security testing;
- ♦ malware deployment;
- ♦ automated scanning that could significantly impact service availability;
- ♦ accessing customer data beyond what is necessary to demonstrate the issue;
- ♦ attempting to access another customer's information;
- ♦ exploiting vulnerabilities beyond what is necessary to demonstrate the issue; or
- ♦ activities that violate applicable laws or regulations.

5. How to Report a Vulnerability

Please include, where possible:

- ♦ a description of the vulnerability;
- ♦ affected service or feature;
- ♦ steps to reproduce the issue;
- ♦ screenshots or supporting evidence;
- ♦ proof of concept (where appropriate);
- ♦ potential impact; and
- ♦ your contact information for follow-up communication.

Reports should be submitted using the security contact information published on the SOSME website.

6. Vulnerability Severity

SOSME assesses reported vulnerabilities using risk-based criteria that consider factors such as exploitability, potential business impact, affected services, and customer risk. The assessment helps determine remediation priorities and response timelines.

7. Our Response Process

When we receive a vulnerability report, we aim to:

- ♦ acknowledge receipt;
- ♦ review and assess the report;
- ♦ determine the severity and potential impact;
- ♦ investigate and validate the issue;
- ♦ prioritize remediation based on risk; and
- ♦ communicate with the reporter, where appropriate, throughout the process.

Response times may vary depending on the nature and complexity of the reported issue.

SOSME will prioritize remediation based on the assessed business impact, exploitability, and risk to customers.

8. Coordinated Disclosure

We believe responsible disclosure benefits everyone.

Where appropriate, SOSME may work with the reporter to coordinate public disclosure after the vulnerability has been resolved or appropriate mitigations have been implemented.

9. Safe Harbor

SOSME will not pursue legal action against individuals who:

- ♦ act in good faith;
- ♦ comply with this Policy;
- ♦ avoid harming customers or disrupting services;
- ♦ promptly report identified vulnerabilities; and
- ♦ cooperate with SOSME during the investigation.

This Safe Harbor applies only to activities conducted in accordance with this Policy and does not authorize unlawful activities or access beyond what is reasonably necessary to identify and report a vulnerability.

Need Help?

If you have questions about this Policy or wish to report a suspected security issue, please contact the SOSME Security Team using the contact details published on our official website.

Our Commitment

Security is strengthened through collaboration.

We appreciate the efforts of individuals and organizations that help us improve the security of our platform through responsible disclosure.

By working together, we can continue to provide a secure, resilient, and trusted operating environment for our customers.

Thank you for supporting SOSME.

Business. Rebuilt.

Related Documents

- ◆ TCP-SEC-001 – Security Statement
- ◆ TCP-GOV-001 – Governance & Compliance Framework
- ◆ TCP-SVC-001 – Business Continuity Statement
- ◆ TCP-PRI-001 – Privacy Policy
- ◆ TCP-AI-001 – Responsible Artificial Intelligence Policy
- ◆ TCP-AI-002 – AI Transparency Statement
- ◆ LEG-004 – Terms of Use

The latest versions of all SOSME Trust Center documents are available through our official website.