Responsible Vulnerability Disclosure Policy, version 1.2.0

Status: ☐ Working Draft ☒ Approved ☐ Adopted
Document Owner: Information Security Committee
Last Updated Date: April 2025

Responsible Vulnerability Disclosure Policy

Introduction

At Locate Software Inc, we take the security of our systems and the data we manage on behalf of our clients very seriously. We believe in coordinated vulnerability disclosure and appreciate the efforts of security researchers who help identify potential vulnerabilities. This policy outlines how to report vulnerabilities to us and what you can expect during the disclosure process.

Scope

This policy applies to:

- Web applications, services, APIs, and systems directly operated or maintained by Locate Software Inc.
- Client systems or applications only when explicitly authorized in a scope of engagement or contract.
- Vulnerabilities could affect the confidentiality, integrity, or availability of our data, systems, or users.

Out of scope:

- Denial-of-service (DoS) or brute-force attacks.
- Social engineering, Phishing, or physical security testing.
- Vulnerabilities in third-party platforms or vendors are not managed by us.
- Use of automated tools or scanning services without prior written approval.

How to Report a Vulnerability

We encourage you to report on potential vulnerabilities responsibly by following these guidelines:

1. Submit your report via email to securityincident@locatesw.com . Please use a descriptive subject line, such as "Vulnerability Report - [Affected System/Service]".
2. Provide clear and concise details of the suspected vulnerability, including:
   - The affected system or service.
   - A detailed description of the vulnerability, including steps to reproduce it.
   - Any relevant configuration information (e.g., operating system, browser version).
   - Potential impact of vulnerability (if known).

   - Any proof-of-concept (PoC) or scripts that demonstrate vulnerability (please use these responsibly and avoid causing harm).

3. Do not publicly disclose the vulnerability until we have had a reasonable time to investigate, validate, and remediate the issue. We request that you allow us 45 days from the date of your report before making any public disclosure. We will communicate our progress during this period.
4. Act in good faith and avoid causing any harm or disruption to our services or data. Do not exploit vulnerability beyond the extent necessary to demonstrate its existence.
5. Comply with all applicable laws and regulations in connection with your research and reporting.

What to Expect

After submitting a report, you can expect:

1. **Acknowledgment**: We will acknowledge receipt of your report within 3 business days
2. **Assessment**: Our security team will evaluate the reported vulnerability
3. **Verification**: We will work to verify the issue and may request additional information
4. **Remediation**: We will develop and test a fix for valid vulnerabilities
5. **Disclosure**: We will coordinate with you on an appropriate disclosure timeline

Responsible Disclosure Guidelines

To qualify under this policy, you must:

- Act in good faith to avoid privacy violations, destruction of data, or interruption of services.
- Do not access or modify data that does not belong to you.
- Avoid degradation of our services or user experience.
- Provide us with a reasonable opportunity to fix the issue before disclosing it publicly (we ask for at least 90 days from the time of reporting).

Safe Harbor

When conducting vulnerability research according to this policy, we consider your actions authorized and will not:

- Initiate legal action against you
- Report on law enforcement
- Pursuing legal claims under applicable computer crime laws

Provided that you:

- Make a good faith effort to avoid violations of privacy, data destruction, service disruption, or degradation
- Only interact with accounts you own or have explicit permission to access
- Do not exploit vulnerability for purposes other than verification
- Refrain from sharing sensitive information with third parties
- Provide us with reasonable time to address issues before public disclosure

Recognition

We appreciate the efforts of security researchers and, where applicable, we may:

- Acknowledge your contribution on our public "Security Hall of Fame."
- Provide a letter of appreciation or other non-monetary recognition.
- Consider a good-faith vulnerability report favorably in future collaborations.

Questions and Contact

If you have any questions about this policy, please contact us at securityincident@locatesw.com.

We reserve the right to modify this policy at any time without prior notice. Please check this page periodically for updates.

Thank you for helping us keep our systems and services secure.

Locate Software Inc

1. REVISION

Document History

Author	Version	Date	Notes
PM	V1.0	Jan 2022	Original version
PM	V1.2	April 2025	• Added recognition