Vulnerability Disclosure Policy

Version 1.1 · Last updated 2026-10-20 · Owner: Security Lead and Executive Sponsor

Vulnerability Disclosure Policy

1. Purpose

This policy establishes a formal, public-facing process for external security researchers, federal agency customers, and the general public to report security vulnerabilities discovered in Silkline's systems. A well-defined vulnerability disclosure program demonstrates Silkline's commitment to security transparency and provides a structured channel for receiving, triaging, and remediating externally discovered vulnerabilities. Under FedRAMP 20x, KSI-PIY-RVD requires a documented, accessible vulnerability disclosure policy with defined response timelines and safe harbor protections.

2. Scope

This policy applies to all systems, applications, and services within Silkline's FedRAMP certification boundary, including:

- **Web applications** — customer-facing platform interfaces, APIs, and authentication endpoints
- **Infrastructure** — AWS GovCloud resources accessible from the public internet (load balancers, CloudFront distributions, WAF, public-facing endpoints)
- **Mobile applications** — if applicable, any mobile clients that interact with boundary systems
- **Supporting services** — publicly reachable services that support the platform (DNS, CDN, certificate infrastructure)

2.1 Out of Scope

The following are explicitly out of scope for this disclosure program:

- Third-party services not operated by Silkline (AWS infrastructure, Datadog, GitHub, the FedRAMP IdP) — report these to the respective vendor
- Social engineering attacks against Silkline personnel
- Physical security testing
- Denial-of-service (DoS/DDoS) attacks or testing
- Spam or phishing campaigns
- Findings from automated scanners without validated proof of exploitability

- Issues in third-party libraries where the upstream vendor has already been notified and a fix is pending

3. How to Report a Vulnerability

3.1 Reporting Channels

Vulnerabilities may be reported through any of the following channels:

Channel	Details	Encryption
Email	security@silkline.io	PGP key available at https://silkline.io/.well-known/security.txt
security.txt	https://silkline.io/.well-known/security.txt	Contains PGP key, preferred contact, and canonical policy URL
GitHub Security Advisories	Via the "Report a vulnerability" feature on Silkline's GitHub repositories (if public)	GitHub-managed encryption

3.2 What to Include in a Report

A complete vulnerability report includes:

- **Description** of the vulnerability, including the type (e.g., SQL injection, XSS, authentication bypass, IDOR)
- **Affected system or URL** — the specific endpoint, application, or component affected
- **Steps to reproduce** — a clear, step-by-step description that allows Silkline's security team to reproduce the issue
- **Proof of concept** — screenshots, HTTP request/response pairs, or code snippets demonstrating the vulnerability (do not include customer data or PII)
- **Impact assessment** — the reporter's assessment of what an attacker could achieve by exploiting the vulnerability
- **Reporter contact information** — an email address or other method for Silkline to follow up (anonymous reports are accepted but may limit our ability to coordinate)

3.3 security.txt

Silkline publishes a `security.txt` file at `https://silkline.io/.well-known/security.txt` in accordance with RFC 9116. The file contains:

- Contact email for security reports
- PGP public key for encrypted submissions
- Canonical URL of this vulnerability disclosure policy

- Preferred language (English)
- Expiration date (updated annually)

4. Response Process

4.1 Response Timeline

Silkline commits to the following response timelines:

Milestone	Timeline	Description
Acknowledgment	Within 2 business days	Confirm receipt of the report and assign a tracking identifier
Initial triage	Within 5 business days	Assess severity, validate the vulnerability, and determine scope
Status update	Within 10 business days	Provide the reporter with a triage outcome: confirmed, under investigation, or not applicable
Remediation target	Based on severity (see 4.2)	Develop and deploy a fix according to severity-based SLAs
Resolution notification	Within 5 business days of fix deployment	Notify the reporter that the vulnerability has been remediated

4.2 Severity-Based Remediation Timelines

Validated vulnerabilities are prioritized using CVSS v3.1 scoring aligned with FedRAMP remediation requirements:

Severity	CVSS Score	Remediation Timeline	Escalation
Critical	9.0–10.0	15 calendar days	Immediate escalation to Security Lead and Executive Sponsor
High	7.0–8.9	30 calendar days	Security Lead notified within 24 hours of triage

Medium	4.0–6.9	90 calendar days	Tracked in vulnerability management system
Low	0.1–3.9	180 calendar days	Tracked in vulnerability management system
Informational	0.0	Best effort	Documented for awareness

These timelines align with the Continuous Monitoring Plan remediation SLAs.

4.3 Triage Process

Upon receiving a vulnerability report:

1. **Receive and log**: Security Lead (or designated responder) logs the report in the vulnerability tracking system with a unique identifier
2. **Acknowledge**: Send acknowledgment to the reporter within 2 business days
3. **Validate**: Attempt to reproduce the vulnerability in a non-production environment. If reproduction requires additional information, contact the reporter.
4. **Classify**: Assign severity using CVSS v3.1. Determine whether the vulnerability affects the FedRAMP certification boundary.
5. **Prioritize**: Queue remediation according to severity-based timelines
6. **Remediate**: Engineering develops and tests a fix. For Critical and High severity, the fix follows the emergency change process defined in the Configuration Management Plan.
7. **Verify**: Security Lead verifies the fix resolves the vulnerability without introducing regressions
8. **Notify**: Inform the reporter of the resolution. If applicable, coordinate public disclosure timeline (see Section 6).
9. **Document**: Record the full lifecycle in the vulnerability tracking system. If the vulnerability affected the certification boundary, assess whether it constitutes a security incident per the Incident Response Plan.

5. Safe Harbor

5.1 Commitment to Reporters

Silkline will not pursue legal action against security researchers who:

- Act in good faith and in accordance with this policy
- Avoid accessing, modifying, or deleting data belonging to other users or customers
- Do not disrupt Silkline's services or degrade the experience of other users
- Do not exploit the vulnerability beyond what is necessary to demonstrate its existence

- Report the vulnerability promptly and do not publicly disclose it before Silkline has had a reasonable opportunity to remediate (see Section 6)
- Do not conduct testing that could cause harm to Silkline's customers, users, or infrastructure (no DoS, no social engineering, no physical access attempts)

5.2 Protections Provided

Researchers acting in accordance with this policy can expect:

- **No legal threats**: Silkline considers vulnerability research conducted in compliance with this policy to be authorized and will not initiate legal proceedings
- **No law enforcement referral**: Silkline will not refer researchers to law enforcement for activities conducted in compliance with this policy
- **Good faith interpretation**: If a third party initiates legal action against a researcher for activities covered by this policy, Silkline will take steps to make it known that the researcher's actions were authorized under this program
- **Confidentiality**: Silkline will not publicly identify the reporter without their consent

5.3 Limitations

Safe harbor protections do not extend to:

- Activities that violate applicable law beyond the scope of this policy
- Accessing or exfiltrating customer data, federal data, or personally identifiable information
- Actions that cause material harm to Silkline's systems, customers, or users
- Vulnerability research conducted against out-of-scope systems (Section 2.1)

6. Coordinated Disclosure

6.1 Disclosure Timeline

Silkline follows a coordinated disclosure model:

- **Default disclosure window**: 90 calendar days from the date the vulnerability is confirmed. This gives Silkline time to develop, test, and deploy a fix before public disclosure.
- **Extension**: If remediation requires more than 90 days (e.g., due to complexity or dependency on upstream vendors), Silkline will communicate the expected timeline to the reporter and negotiate a mutually acceptable disclosure date.
- **Early disclosure**: If the vulnerability is actively being exploited in the wild, Silkline may issue a security advisory before the fix is deployed, with appropriate mitigations documented.
- **Reporter credit**: With the reporter's consent, Silkline will credit the researcher in security advisories and, if applicable, in a public acknowledgment page.

6.2 Federal Agency Notification

For vulnerabilities that affect the FedRAMP certification boundary:

- The relevant authorizing officials and agency customers are notified per the timelines defined in the Incident Response Plan and the FedRAMP IEC rules
- FedRAMP PMO is notified if the vulnerability constitutes a significant incident per FRMR.SCN criteria
- Notification timelines follow the FedRAMP security inbox (FSI) requirements

7. Recognition

Silkline values the contributions of security researchers who help improve the security of the platform. Recognition may include:

- **Public acknowledgment**: with the reporter's consent, listing the researcher on a public security acknowledgments page
- **Private thank-you**: a personal acknowledgment from the Security Lead
- **Bug bounty**: Silkline does not currently operate a paid bug bounty program. This decision will be revisited annually as part of the policy review cycle.

Silkline does not currently offer monetary compensation for vulnerability reports but reserves the right to establish a formal bug bounty program in the future.

8. Integration with Internal Processes

8.1 Vulnerability Management

Externally reported vulnerabilities are tracked alongside internally discovered vulnerabilities in the same vulnerability management system:

- Assigned a unique tracking identifier
- Classified with CVSS score
- Subject to the same remediation SLAs as scanner-discovered findings
- Included in vulnerability metrics reported to the Security Lead and Executive Sponsor

8.2 Incident Response

If a reported vulnerability meets any of the following criteria, it is escalated to the incident response process:

- Evidence of active exploitation
- Customer data exposure (confirmed or suspected)
- Compromise of authentication or authorization mechanisms
- Impact to the availability or integrity of the certification boundary

See the Incident Response Plan for escalation procedures.

8.3 Supply Chain Coordination

If a reported vulnerability originates in a third-party component (open-source library, upstream dependency, vendor service):

- Silkline coordinates with the upstream vendor or maintainer per NIST IR-6(3)
- The vulnerability is tracked in the SBOM pipeline per the SBOM Management Procedure
- If the upstream fix is delayed, Silkline implements compensating controls (WAF rules, input validation, feature flags) within the severity-based remediation timeline

9. Roles and Responsibilities

Role	Vulnerability Disclosure Responsibilities
Security Lead	Owns this policy. Monitors the security@silkline.io inbox. Triages incoming reports. Coordinates remediation. Communicates with reporters. Signs off on public disclosures.
Engineering Lead	Develops and deploys fixes for confirmed vulnerabilities. Reviews code changes for regression risk. Provides technical assessment during triage.
DevOps / SRE	Deploys remediation to production. Monitors for exploitation attempts post-disclosure. Updates WAF and security controls as compensating measures.
Executive Sponsor	Approves public security advisories. Authorizes any deviation from standard remediation timelines. Approves future bug bounty program decisions.
Customer Success	Coordinates agency customer notification for boundary-affecting vulnerabilities, in partnership with the Security Lead.

10. Policy Maintenance

- **Review frequency**: Annually, or upon change to the disclosure process, or after any vulnerability disclosure that reveals process gaps

- **security.txt update**: The `security.txt` file is updated at least annually (before its expiration date) and whenever contact information or policy URLs change
- **PGP key rotation**: The PGP key referenced in `security.txt` is rotated annually or upon suspected compromise
- **Approval**: Security Lead and Executive Sponsor
- **Distribution**: This policy is publicly accessible at a URL referenced in `security.txt`. Internal personnel with certification boundary access also receive the policy.
- **Version control**: This document is maintained in the organization's policy repository with pull-request-based review

---