Responsible Vulnerability Disclosure Policy

Inspired Technologies, Inc.

January 2026

Table of Contents

Responsible Vulnerability Disclosure Policy
Company Name: Inspired Technologies, Inc.
Policy Owner: Chief Operating Officer (COO)
Effective Date: January 05, 2026
Version: 1.2
Review Frequency: Annually or following significant regulatory, operational, or incident-driven changes

1. Purpose

This Responsible Vulnerability Disclosure Policy outlines a secure, confidential, and efficient process for receiving, assessing, and remediating potential security vulnerabilities reported by security researchers, ethical hackers, partners, vendors, or other trusted parties.

Reports will be handled privately, with remediation coordinated directly with affected clients where applicable, and without a requirement for public disclosure unless mutually agreed upon with the reporter and relevant clients.

2. Scope

This policy covers vulnerabilities discovered in:

- Systems, networks, applications, APIs, cloud environments (primarily Azure/Microsoft 365), and other assets owned or directly managed by Inspired Technologies
- Client environments or services where Inspired Technologies is contractually responsible for security coordination and remediation.

Out of scope:

- Physical security issues, social engineering, DoS/DDoS, brute-force attempts, or automated scanning without explicit prior permission.
- Vulnerabilities in third-party services or client-managed systems not under our direct control (reporters should use the relevant third-party or client disclosure process).
- Previously known or low-impact issues that do not materially affect confidentiality, integrity, or availability.

3. How to Report a Vulnerability

We welcome good-faith, responsible reports from security researchers and partners. All reports are treated confidentially.

Preferred Method: Email
Email Address: secops.alerts@inspired-tech.net
Subject Line: Confidential Vulnerability Report – [Brief non-specific description, e.g., "Potential authentication issue in client portal"]

Required Information in Report:

- Clear description of the vulnerability (including steps to reproduce).
- Affected asset(s), endpoint(s), or service(s) (avoid including sensitive client data).
- Any proof-of-concept (PoC), screenshots, or logs (do NOT include exploit code that causes harm or accesses real data).
- Your preferred contact method.
- Assessment of potential impact/severity (if known).

We request that reporters:

- Do not publicly disclose the vulnerability at any time without our explicit written consent.
- Do not access, modify, exfiltrate, or delete data belonging to us or our clients.
- Cease testing once the vulnerability is confirmed.
- Comply with all applicable laws.

4. What You Can Expect from Us

We commit to handling all reports professionally and confidentially:

Stage	Timeline (from receipt)	Action
Acknowledgment	Within 3 business days	Confirm receipt and assign a confidential tracking ID.
Initial Triage & Validation	Within 10 business days	Verify the issue and provide preliminary severity assessment.
Remediation Coordination	Within 30–90 days	Develop/test fix; coordinate with internal teams and affected clients as needed.
Resolution	As soon as safely possible	Deploy mitigation or patch; confirm fix with reporter (if requested).
Closure	Upon remediation	Provide final update to reporter; close the case confidentially.

- We will **not** pursue legal action against good-faith reporters who follow this policy and stay within scope.
- We will maintain strict confidentiality and share details only with teams and clients who have a legitimate need to know.
- Public disclosure (e.g., blog post, CVE assignment) is **not required** and will only occur if mutually agreed upon by Inspired Technologies, the reporter, and any affected client(s).
- At our discretion, we may offer private recognition, a thank-you letter, or modest compensation for high/critical impact findings that materially improve security for our clients.

5. Safe Harbor

Good-faith reporters acting in accordance with this policy are authorized for the limited purpose of vulnerability discovery and reporting. We will not initiate or support legal, administrative, or other action against you for activities that:

- Are consistent with this policy.
- Remain within the defined scope.
- Do not cause harm to systems, data, clients, or users.

This safe harbor does **not** apply to malicious, reckless, or harmful conduct.

6. Roles and Responsibilities

- **Security Team / COO**: Receive, triage, validate, coordinate remediation, and communicate with reporters confidentially.
- **Engineering / Operations / Client Services Teams**: Investigate, develop fixes, test, and deploy remediations.
- **Legal / Compliance**: Ensure confidentiality, review scope, and provide guidance on obligations.

7. Disclosure Guidelines

- All disclosure remains **private and client-focused**.
- We aim to remediate within 90 days of validation. If longer timelines are needed, we will communicate with the reporter.
- In cases of active exploitation or imminent client risk, we will accelerate remediation and client notification without waiting for full public disclosure.
- Reporters may **not** publish findings independently unless we provide explicit written permission.

8. Contact Information

Security Reporting Email: secops.alerts@inspired-tech.net

This Responsible Vulnerability Disclosure Policy reflects our commitment to secure, confidential handling of vulnerability information in alignment with our responsibilities to our clients.