Control ID / Name

Control ID: TISP-600 – 3.2.13

Control Name: Responsible Disclosure Program

Company: Tiami Networks, Inc.

Document Owner: Compliance & Security

Version: 1.0

Date: March 18, 2026

Purpose

Tiami Networks is committed to maintaining the security of its systems, products, and services. This policy provides a process for security researchers and third parties to responsibly report potential vulnerabilities so they can be investigated and remediated in a timely manner.

Scope

This policy applies to all Tiami Networks technology environments, including Tiami Networks platforms, internal and external systems, products and services developed or maintained by Tiami Networks, and any public-facing infrastructure operated by or on behalf of Tiami Networks. It covers vulnerabilities discovered within these environments that could impact the confidentiality, integrity, or availability of Tiami Networks systems, data, or services.

Reporting a Vulnerability

Security researchers who identify a potential vulnerability should report it to security@tiaminetworks.com. Reports should include a description of the issue, steps to reproduce, potential impact, and any supporting evidence.

Response Process

Tiami Networks will acknowledge receipt of vulnerability reports within five business days. Reported vulnerabilities will be investigated and validated by the Compliance and Security

teams, and remediation efforts will be prioritized based on the risk and potential impact to systems, services, or data. During the investigation process, Tiami Networks may contact the reporting researcher to request additional details or clarification if necessary.

Good Faith Research

Tiami Networks will not pursue legal action against researchers who act in good faith, avoid exploiting vulnerabilities for personal gain, and do not access or modify customer data.

Bug Bounty Participation

Tiami Networks may participate in customer-operated bug bounty programs, including those operated by partners or customers, when required as part of contractual security requirements.