Responsible Vulnerability Disclosure Policy

Riverbed Technology ("**Riverbed**") is committed to maintaining the security of our products, services, and customers. We value the work of security researchers and encourage responsible reporting of potential security vulnerabilities.

If you believe you have discovered a security vulnerability related to a Riverbed product, service, or system, we ask that you report it responsibly by following the guidelines outlined below.

Scope

This vulnerability disclosure process applies to:

- Riverbed-owned products and services;
- Cloud services operated by or on behalf of Riverbed; and
- Public-facing Riverbed systems

This process does not authorize testing of third-party systems or customer environments.

How to Report a Vulnerability

Please submit potential security vulnerabilities via email to infosec@riverbed.com.

To help us evaluate and respond efficiently, please include the following information where possible:

- Product, service, or system affected
- Detailed description of the vulnerability
- Steps to reproduce the issue (proof-of-concept, if available)
- Potential impact or risk
- Your contact information (optional, but helpful)

Safe Harbor for Responsible Research

Riverbed supports responsible vulnerability research conducted in good faith. If you comply with this policy, we will consider your research to be authorized under our safe harbor.

To qualify for safe harbor requirements, you must:

- Take all reasonable steps to avoid data loss and service disruption to Riverbed's customers, channel partners, and other third parties as a result of your actions.
- Ensure that your actions do not result in the violation of any individual's privacy rights, including the unauthorized disclosure of personal data, or the unauthorized disclosure of any confidential information of Riverbed, its customers, or its channel partners.
- Ensure that you do not exploit a suspected vulnerability beyond what is necessary to demonstrate its existence.
- Preserve the confidentiality of the suspected vulnerability. Do not publicly disclose the suspected vulnerability until Riverbed has had a reasonable opportunity to investigate and remediate it and has notified you that you may disclose it.

What You Can Expect from Us

Upon receiving a vulnerability report, Riverbed will:

- Acknowledge receipt of your report where contact information is provided;
- Assess and validate the reported issue;
- Take appropriate remediation actions in accordance with our internal vulnerability management processes; and
- Communicate as appropriate regarding resolution status.

Riverbed does not currently operate a bug bounty program but appreciates responsible disclosures that help improve the security of our products and services.

Thank You

We value the efforts of the security community and believe that responsible disclosure helps protect our customers, our partners, and the broader ecosystem.