Responsible Vulnerability Disclosure Policy

Verveba Telecom LLC

At Verveba, we are committed to maintaining the security and integrity of the systems, applications, software, and services we provide to our customers. We recognize the important role that security researchers and our extended technical community play in helping us identify and remediate potential security vulnerabilities.

If you believe you have discovered a security vulnerability that may affect a Verveba system, application, software module, cloud environment, or customer-connected workflow, we encourage you to report it to us responsibly.

How to Report a Vulnerability

Please send all vulnerability reports to:
info@verveba.com
Include as much detail as possible:
Description of the issue
Steps to reproduce (if available)
Impact assessment (if known)
Any supporting screenshots or logs
Verveba does not authorize testing against customer-owned infrastructure. Please report only issues related to Verveba-owned assets or software delivered by Verveba.

What to Expect

Upon receiving a report:
Verveba will acknowledge receipt of your submission.
Our Information Security Lead will review the issue and assign a severity level. If validated, Verveba will work to remediate the issue in accordance with our Vulnerability Management Program.
We may contact you if additional information is needed.
We will notify you once the issue is resolved or mitigation steps are implemented.
Safe Harbor

If you follow the guidelines below, Verveba will consider your actions to fall within authorized security research:

Do not access customer data or customer-owned systems at any time.
Do not disrupt services, modify data, or use automated tools that could cause system instability.
Do not publicly disclose issues without coordinated communication with Verveba.
Make a good-faith effort to avoid privacy violations or unauthorized data exposure.
Verveba will not pursue legal action for good-faith, responsible research conducted within these boundaries.

Scope

This policy applies to:

Verveba-developed software and tools
Verveba-hosted services and internal applications
Cloud environments managed by Verveba
Websites and portals owned by Verveba
This policy does not apply to customer-owned systems or networks, which are governed by their respective owners.

Out of Scope

Denial-of-service attacks
Social engineering attempts
Physical security testing
Attacks against customer systems
Thank You

We appreciate the contributions of the security community and the shared mission of protecting our customers and partners.