Vulnerability Disclosure Policy

Vertice is committed to the security of its systems and values the effort of security researchers who help to identify potential vulnerabilities in good faith. If you discover a security vulnerability, please report it to us responsibly using the guidelines below.

Safe Harbor

Researchers who report vulnerabilities in good faith and comply with this policy will not face legal action from Vertice.

Submitting a Report

Please email vulnerability reports to security@vertice.one.

In the report, please include as much as possible to assess the vulnerability root cause, such as:

- Affected service and URL
- Exploitation or reproduction steps
- Severity assessment (if known or possible)

If possible, do not include any sensitive data or exposure.

Remediation and Disclosure Timeline

Vertice aims to remediate validated vulnerabilities within ninety (90) days of the initial report. Researchers agree not to disclose vulnerability details to the public until this remediation period has expired or a fix has been confirmed by Vertice.

Rewards and Recognition

Vertice does not currently offer a bug bounty program or monetary rewards for vulnerability disclosures. We may, at our discretion and agreement with the reporter, provide public recognition for researchers who follow this policy. No obligation to provide recognition is created by this policy or by any prior instance of recognition having been given.

Prohibited Activities

The following activities are strictly prohibited:

- Denial of Service (DoS/DDoS) testing
- Social engineering (phishing) of Vertice employees or customers
- Physical security attacks against Vertice offices or infrastructure
- Intentional destruction, modification, or exfiltration of Vertice data