



VULNERABILITY DISCLOSURE POLICY

We believe in safe harbors for security researchers. Teisoft LLC is committed to the security of our systems and our customers. We appreciate the work of the security research community and welcome reports of potential vulnerabilities in our public-facing infrastructure.

Scope

- **In Scope:** *.teisoft.com, and our public cloud infrastructure explicitly marked as ours.
- **Out of Scope:** Customer assets (unless you are the authorized customer), Third-party SaaS providers (e.g., our payment processors), and Denial of Service (DoS) attacks.

Safe Harbor If you conduct security research in good faith and in accordance with this policy, Teisoft LLC considers your research authorized. We will not recommend or pursue legal action against you related to your research.

How to Report Please submit detailed reports to: cybersec@teisoft.com

- Include a Proof of Concept (PoC) or steps to reproduce.
- Do not access, modify, or delete data belonging to us or our customers.
- Give us reasonable time (90 days) to remediate the vulnerability before public disclosure.

Rewards At this time, Teisoft LLC does not operate a cash Bug Bounty program. However, researchers who submit valid, critical vulnerabilities may be listed in our "Hall of Fame" (with permission) as a token of professional recognition.