OBEDIENCE GLOBAL LTD

Vulnerability Disclosure Policy

How to report a security issue to us safely, and what we promise in return.

Version 1.1 | Effective 28 July 2026 | Security

Owner Obedience Global Ltd board | Approved by Obedience Global Ltd board on 28 July 2026
Approval state company-approved | Next review 28 October 2026

01 Reporting

If you believe you have found a security vulnerability in any Obedience service, email hello@obedience.global with the subject "Security report". Include enough detail to reproduce the issue. A machine-readable contact is published at /.well-known/security.txt on each of our domains.

02 What we promise

- Acknowledgement within 3 working days
- An assessment and expected timeline within 10 working days
- We will not pursue legal action for good-faith research that respects the rules below
- Credit, if you want it, once the issue is fixed

03 Ground rules for good-faith research

- Do not access, modify or exfiltrate data that is not yours: use test accounts
- Do not degrade the service for others (no denial-of-service, no spam)
- Do not run automated scanners against production without asking first
- Give us reasonable time to fix before public disclosure

04 Scope and rewards

In scope: obedience.global, obedience.cloud, quantify.obedience.global and their APIs. We do not run a paid bug bounty yet; we say that here so nobody is surprised. That may change as we grow.

Canonical online record: https://obedience.global/policies/vulnerability-disclosure