

WEBSITE SECURITY POLICY

RESPONSIBLE DISCLOSURE

Keeping our systems and the people who rely on them safe is a priority for us. As we work toward a better product, that responsibility is fundamental to our mission. We value the security research community and the role it plays in keeping the wider ecosystem safe, and we welcome reports made in good faith.

01

WHAT WE'RE LOOKING FOR

● IN SCOPE

Original, reproducible issues that relate to our public-facing website and publicly exposed assets and endpoints — for example, vulnerabilities affecting data confidentiality, integrity, or access controls — that can be discovered from public resources.

● OUT OF SCOPE

Denial of service, volumetric attacks, social engineering (phishing of staff), physical security attacks, issues in third-party services outside our control, and missing best practices with no working proof of concept (such as security headers or TLS configuration).

02

REPORTING & RESPONSE

Please send reports to explore@basecamp-research.com with a description of the issue and steps to reproduce. We will acknowledge your report within three ③ to five ⑤ business days and keep you informed of our progress until it is resolved. We aim to triage within thirty (30) days.

3–5

business days to acknowledge your report

30

days' target to triage the issue, with progress shared until it is resolved

03

SAFE HARBOUR

While we are grateful for every report, we are not able to offer financial compensation at this time. Provided you comply with the conditions set out in this policy we will treat your research as authorised, we will not pursue legal action against you and will not refer your research to law enforcement.

In return, please access no more data than is needed to demonstrate a finding, and do not change other users' data, disrupt the service, or disclose the issue publicly before we confirm it is fixed.