



Last Update Status: Proof Data Technology Inc ("Proof")
Title: Responsible Disclosure Policy
Effective Date: 10/08/2020

Responsible Disclosure Policy

Data security is a top priority for Proof, and we believe that working with skilled security researchers can identify weaknesses in any technology. If you believe you've found a security vulnerability in Proof's service, please notify us; we will work with you to resolve the issue promptly.

Disclosure Policy

- Support is provided 24 hours per day, 7 days per week.
- If you believe you've discovered a potential vulnerability, please let us know by emailing us at incidents@proofgov.com. We will acknowledge your email within 24 hours.
- Provide us with a reasonable amount of time to resolve the issue before disclosing it to the public or a third party. We aim to resolve critical issues within Five business days of disclosure.
- Make a good faith effort to avoid violating privacy, destroying data, or interrupting or degrading the Proof service. Please only interact with domains you own or for which you have explicit permission from the account holder.

Exclusions

While researching, we'd like you to refrain from:

- Distributed Denial of Service (DDoS)
- Spamming
- Social engineering or phishing of Proof employees or contractors
- Any attacks against Proof's physical property or data centers

Thank you for helping to keep Proof and our users safe!

Changes

We may revise these guidelines from time to time. The most current version of the guidelines will be available here at <https://proofgov.com/disclosure>

Contact

Proof is always open to feedback, questions, and suggestions. If you would like to talk to us, please feel free to email us at incidents@proofgov.com

Responsibility

It is the Security team's responsibility to see this policy is enforced.