Responsible Disclosure Policy

Data security is a top priority for Curvo, and Curvo believes that working with skilled security researchers can identify weaknesses in any technology.

If you believe you've found a security vulnerability in Curvo's service, please notify us; we will work with you to resolve the issue promptly.

Disclosure Policy

- If you believe you've discovered a potential vulnerability, please let us know by emailing us at Security@Curvolabs.com . We will acknowledge your email promptly.

- Provide us with a reasonable amount of time to resolve the issue before disclosing it to the public or a third party.

- Make a good faith effort to avoid violating privacy, destroying data, or interrupting or degrading the Curvo service. Please only interact with accounts 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 Curvo employees or contractors
- Any attacks against Curvo's physical property or data centers

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

Changes

We may revise these guidelines from time to time. The most current version of the guidelines will be available at www.curvolabs.com/security

Curvo is always open to feedback, questions, and suggestions. If you would like to talk to us, please feel free to email us at security@curvolabs.com

Disciplinary Action

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Curvo management will determine how serious an employee's offense is and take the appropriate action.

Responsibility

It is the Curvo InfoSec team's responsibility to see if this policy is enforced.