

Gem Software, Inc. Responsible Disclosure Policy

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

If you believe you've found a security vulnerability in Gem Software, Inc.'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@gem.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 24 hours of disclosure.
- Make a good faith effort to avoid violating privacy, destroying data, or interrupting or degrading the Gem Software, Inc. 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 Gem Software, Inc. employees or contractors
- Any attacks against Gem Software, Inc.'s physical property or data centers

Thank you for helping to keep Gem Software, Inc. 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 <https://www.gem.com/bugbounty>.

Contact

Gem Software, Inc. is always open to feedback, questions, and suggestions. If you would like to talk to us, please feel free to email us at support@gem.com.

Responsibility

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

Last updated: 5/14/2019