Jiko Vulnerability Disclosure Policy

We take the security of our systems seriously, and we value the security community. The disclosure of security vulnerabilities helps us ensure the security and privacy of our users and systems.

Guidelines

We require that all researchers:

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing;
- Perform research only within the scope set out below;
- Use the identified communication channels to report vulnerability information to us; and
- Keep information about any vulnerabilities you've discovered confidential between yourself and Jiko until we've had 90 days to resolve the issue.

If you follow these guidelines when reporting an issue to us, we commit to:

- Not pursue or support any legal action related to your research;
- Work with you to understand and resolve the issue quickly (including an initial confirmation of your report within 72 hours of submission);
- Recognize your contribution with a monetary reward, if you are the first to report the issue and we make a code or configuration change based on the issue.

Scope

- Jiko.io

Out of scope

Any services hosted by 3rd party providers and services are excluded from scope.

In the interest of the safety of our users, staff, the Internet at large and you as a security researcher, the following test types are excluded from scope:

- Findings from physical testing such as office access (e.g. open doors, tailgating)
- Findings derived primarily from social engineering (e.g. phishing, vishing)
- Findings from applications or systems not listed in the 'Scope' section

- UI and UX bugs and spelling mistakes
- Network level Denial of Service (DoS/DDoS) vulnerabilities

Things we do not want to receive:

- Personally identifiable information (PII)
- Credit card holder data

How to report a security vulnerability?

If you believe you've found a security vulnerability or a compliance issue in one of our products or platforms please send it to us by emailing security@jiko.io. Please include the following details with your report:

- Description of the location and potential impact of the vulnerability;
- A detailed description of the steps required to reproduce the vulnerability (POC scripts, screenshots, and compressed screen captures are all helpful to us).