[INSERT FIRM LEGAL NAME]
Responsible Disclosure Policy

[Insert Firm Logo]

Version 1.0
[Insert Date]

[Insert Firm Logo]

Contents

Instructions

Documents are in a template format and are to be customized to fit the appropriate business and operational requirements. Use the sample as a foundation to build a bespoke policy for your business.

If any element of the following Sample/Template is not operationally feasible or appropriate for a particular business, be sure to delete that element from the company specific document. **Otherwise, it would be a liability exposure to establish a policy and not to comply with it.**

The following recommendations are designed to limit, but will not eliminate, the security risks associated with the use of the policy subject. Businesses should deploy a defense-in-depth security model of technical, operational, and physical security controls.

Delete the instructions after finalizing and adopting the policy.

Policy Overview

As a provider of <services> to many customers and users, <company name> takes security very seriously. We investigate all reported vulnerabilities, which we accept from many sources including independent security researchers, customers, partners, and consultants.

We work diligently to identify and correct any security issues found in our <products>. Individuals who believe they have identified a security issue or vulnerability in one of our <products> are advised to contact <email/phone> in order to have an engineer evaluate and document a possible security issue for our engineering teams to confirm and remedy when appropriate. Customers wishing to report a suspected security vulnerability should contact <Customer Support>.

Scope and Purpose

- Maintain security safeguards designed to ensure the confidentiality of the information provided to us.
- To treat everyone who contributes with respect and recognize your contribution to keeping our staff and customers safe and secure.
- To work with many sources including independent security researchers, customers, partners, and consultants to validate and remediate reported vulnerabilities.
- To investigate and remediate issues in a manner consistent with protecting the safety and security of both on-prem and cloud customers. Addressing a valid reported vulnerability will take time. This will vary based on the severity of the vulnerability and the affected systems.

Compliance

- We request that you communicate about potential vulnerabilities in a responsible manner, providing sufficient time and information for our team to validate and address potential issues. We request that researchers make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction of data during security testing.
- We request that researchers provide the technical details and background necessary for our team to identify and validate reported issues, using the form below.
- We request that researchers act for the common good, protecting user privacy and security by refraining from publicly disclosing unverified vulnerabilities until our team has had time to validate and address reported issues. When possible, we would prefer that our respective public disclosures be posted simultaneously.
- You can submit a vulnerability report through our <Help Center> using the <email> below.

Safe Harbor

Any activities conducted in a manner consistent with this policy will be considered authorized conduct and we will not initiate legal action against you. If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

Exceptions

When reporting vulnerabilities, please consider (1) attack scenario / exploitability, and (2) security impact of the bug.

Out of scope vulnerabilities

The following issues are considered out of scope:

- Clickjacking on pages with no sensitive actions
- Cross-Site Request Forgery (CSRF) on unauthenticated forms or forms with no sensitive actions
- Attacks requiring MITM or physical access to a user's device.
- Previously known vulnerable libraries without a working Proof of Concept.
- Missing best practices in SSL/TLS configuration.
- Any activity that could lead to the disruption of our service (DoS).

- Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS
- Rate limiting or bruteforce issues on non-authentication endpoints
- Missing HttpOnly or Secure flags on cookies
- Missing email best practices (Invalid, incomplete or missing SPF/DKIM/DMARC records, etc.)
- Vulnerabilities only affecting users of outdated or unpatched browsers [Less than 2 stable versions behind the latest released stable version]
- Software version disclosure / Banner identification issues / Descriptive error messages or headers (e.g. stack traces, application or server errors).
- Open redirect - unless an additional security impact can be demonstrated
- Issues that require unlikely user interaction

Definitions and Terms

Appendix

<Add Appendix Here>

Revision Table

Revision History				
#	**Version #**	**Date**	**Updates/Changes**	**Owner**
1	1.0	2022	Initial Draft	Riskigy
2				