PRAGYA CYBER

Responsible Disclosure Policy

Table of contents

1. Introduction 3
1.1 Purpose 3
1.2. Scope 3
1.3. Audience 3
2. Guidelines for Responsible Disclosure 3
2.1. Do's: 3
2.2. Don'ts: 4
3. Reporting Vulnerabilities 4
3.1. What to Report 4
3.2. How to Report 5
4. Response and Communication 5
4.1. Non-Disclosure 5
4.2. Resolution and Recognition 5
5. Legal Safe Harbor 5
6. Policy Review and Revision 5
7. Contact Information 5
8. A Word of Thanks from **Pragya Cyber** 6

Version: 1.0

Effective Date: 01-11-2026

Owner: Venu Narasimhan

Classification: Internal Use

1. Introduction

Thank you for taking the time to improve the security of **Pragya Cyber**'s products, services, and systems. We believe in the importance of maintaining a safe and secure environment for our users and customers. We appreciate the efforts of security researchers and ethical hackers who responsibly disclose any potential security vulnerabilities they find.

1.1 Purpose

The purpose of this policy is to provide clear guidelines for security researchers and ethical hackers to report potential vulnerabilities or security issues discovered in **Pragya Cyber**'s products, services, or systems in a responsible manner.

1.2. Scope

This policy is applicable to all products, services, applications, websites, and systems owned or operated by **Pragya Cyber**. Any potential security vulnerability or issue related to the assets is eligible for submission under this policy.

1.3. Audience

This policy is addressed to all security researchers, both external and internal, and internal personnel for reporting security violations by staff, done with or without intention.

2. Guidelines for Responsible Disclosure

Security researchers and ethical hackers are encouraged to act in good faith and make every effort to avoid privacy violations, data breaches, destruction of data, and interruption or degradation of services. Upon discovering a security vulnerability or incident related to our products, services, websites, or systems, we recommend the following guidelines for reporting the issue

2.1. Do's:

- Do provide us with a detailed description of the vulnerability or incident, including the steps to reproduce it, if applicable.
- Do share your contact information so that we can communicate with you regarding the disclosure process and any updates related to the reported issue.
- Do act in good faith and make a reasonable effort to avoid privacy violations, data destruction, and interruption or degradation of our services during your research.

- Do allow us a reasonable amount of time to investigate and address the reported issue before public disclosure.
- Only test for vulnerabilities on systems or assets you own or have explicit permission to test. Unauthorized access or any activity that violates the law is strictly prohibited and may result in legal action.

2.2. Don't:

- Don't exploit any discovered security vulnerabilities beyond what is necessary to demonstrate the issue.
- Don't disclose the issue to any third parties before we have an opportunity to investigate and address it. (**OR**)

  Don't disclose or share the details of any identified vulnerabilities or issues with third parties before receiving explicit written consent from **Pragya Cyber**. (**OR**)

  Don't disclose the issue to any third parties before a mutually agreed upon time expires
- Don't act in ways that may harm **Pragya Cyber** or its customers intentionally or unintentionally

3. Reporting Vulnerabilities

The following sections describe what can be reported as vulnerabilities and the methods and channels of reporting them.

3.1. What to Report

We appreciate reports related to potential security vulnerabilities, including but not limited to:

- Software Bugs and Flaws
- Weak Authentication and Passwords
- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Security Misconfigurations
- Outdated Software and Patch Management
- Sensitive Data Exposure
- Insecure Direct Object References (IDOR)
- Remote Code Execution (RCE)
- Denial of Service (DoS) and Distributed Denial of Service (DDoS)
- Phishing and Social Engineering
- Unencrypted Communications
- Insecure File Uploads
- Insufficient Logging and Monitoring
- Buffer Overflow
- Clickjacking
- Information Disclosure

3.2. How to Report

Please submit your findings via email to security@pragyacyber.com. Your report should include the following details:

- Use a clear subject line that includes "Security Vulnerability Report" or "Security Incident Report."
- A detailed description of the vulnerability or issue, including its potential impact.
- The steps taken to reproduce the vulnerability, including any necessary proof-of-concept (POC) code or screenshots.
- Your contact information (name and email address) for communication purposes.

4. Response and Communication

Upon receiving your report, we will acknowledge receipt within 5 business days. Our security team will review and validate the findings internally. We will strive to keep you informed of our progress and any actions taken during the resolution process.

4.1. Non-Disclosure

Pragya Cyber commits to maintaining the confidentiality of your personal information and will not share your details with third parties without your explicit consent unless required by law.

4.2. Resolution and Recognition

If your report is valid and leads to a fix, **Pragya Cyber** may, at its discretion, acknowledge your contribution on our website or through other appropriate channels. We believe in recognizing the efforts of security researchers who responsibly disclose vulnerabilities to us.

5. Legal Safe Harbor

Pragya Cyber will not pursue legal action against security researchers or ethical hackers who report potential security vulnerabilities in accordance with this policy.

6. Policy Review and Revision

This Policy will be reviewed annually to ensure its effectiveness and relevance. Any necessary updates will be made to address changes in the organization's structure, operations, or regulatory environment.

7. Contact Information

If you have any questions or need further assistance, please contact us at security@pragyacyber.com.

8. A Word of Thanks from **Pragya Cyber**

By reporting security vulnerabilities responsibly, you contribute to the safety and security of our organization and its users. We value your efforts and thank you for helping us maintain a secure environment.

Approved by: Vasu Adunutula

Title: CEO

Approval Date:10-11-2026