The Millennium Group of Delaware, Inc.'s Responsible Vulnerability Disclosure Policy

We at The Millennium Group of Delaware, Inc. are committed to the security of our customers, products, and services. We value the work of security researchers and the broader community in helping us maintain our security posture. This policy is intended to provide a clear framework for security researchers to report vulnerabilities to us responsibly.

Our Commitment

We are dedicated to working with the security community to find and resolve vulnerabilities in a fair and timely manner. We will:

Respond to your report within a 3 business days.

Work to validate the reported vulnerability in a timely manner.

Keep you informed of our progress.

Credit you for your report if you are the first to report it and the vulnerability is confirmed and addressed.

What to Report

We encourage you to report any potential security vulnerability you discover in our products or services, including but not limited to:

Cross-Site Scripting (XSS)

Cross-Site Request Forgery (CSRF)

SQL Injection

Broken Authentication or Session Management

Insecure Direct Object References (IDOR)

Server-Side Request Forgery (SSRF)

Remote Code Execution (RCE)

How to Submit a Report

To help us quickly validate and resolve the vulnerability, please include the following information in your report:

Vulnerability Title: A clear and concise title.

Description: A detailed description of the vulnerability.

Steps to Reproduce: A clear, step-by-step guide on how to reproduce the vulnerability. This is the most critical part of the report.

Proof of Concept (PoC): A screenshot, video, or script that demonstrates the vulnerability.

Impact: Explain the potential security impact of the vulnerability.

Your Contact Information: Your name/alias and preferred method of contact.

Please submit your report via email to: security@TMGOfficeServices.com].

Safe Harbor

We will not pursue legal action against individuals who adhere to this policy. We grant you "safe harbor" protection, meaning you will not be prosecuted or subject to legal action for:

Acting in good faith without malicious intent.

Complying with the guidelines outlined in this policy.

Avoiding privacy violations, destruction of data, or interruption/degradation of our services.

Exclusions (What to Avoid)

The following activities are considered out of scope and may lead to legal action. Do not engage in:

Testing on live customer data or personal information.

DDoS (Denial of Service) attacks.

Social engineering (phishing, vishing, etc.).

Physical attacks against our facilities or data centers.

Scanning or testing that is not specifically authorized.

Destruction or corruption of data.

Using automated tools that could generate a high volume of traffic.

Recognition

We may recognize individuals who submit valid reports and who adhere to this policy. Recognition may include a public mention on our website (with your consent) or other forms of appreciation at our discretion. We do not currently offer a bug bounty program with financial rewards.

Policy Updates

This policy may be updated periodically. Please check back for the latest version.

Thank you for your cooperation in helping us make our products and services more secure.