Swartley Bros. Engineers, Inc.
Electrical & Mechanical Contractors

Effective Date: 05/13/2025
Next Review Date: 05/13/2026
Contact: HR Department
HR@Swartley.com | (215) 368-7400

Responsible Vulnerability Disclosure Policy

Introduction

At Swartley Brothers Engineers Inc., we are committed to maintaining the highest standards of security and integrity across our systems and services. We recognize the important role that security researchers and members of the public play in helping us improve our cybersecurity posture. If you discover a vulnerability, we want to hear from you — and we're committed to working with you to resolve the issue promptly and responsibly.

Scope

This policy applies to any Swartley Brothers-owned web application, digital platform, network system, or technology infrastructure where vulnerabilities could impact our operations or the data we manage, including information related to our partners and clients.

Reporting a Vulnerability

If you believe you've discovered a security vulnerability, please report it to us by emailing: IT@swartley.com

Include the following information in your report:

- A detailed description of the vulnerability
- Steps to reproduce the issue
- Any relevant screenshots or logs
- Your contact information (optional) so we can follow up

What to Expect

- We will acknowledge receipt of your report within 5 business days.
- We will investigate the issue and confirm its validity.
- We will keep you informed on the progress and timeline for remediation.
- We will credit you publicly if you wish, after the issue has been resolved.

Swartley Bros. Engineers, Inc.
Electrical & Mechanical Contractors

Safe Harbor

Individuals who:

- Act in good faith to report a vulnerability
- Do not exploit or misuse the vulnerability
- Avoid accessing or modifying data without permission
- Do not perform actions that could negatively impact our systems

will not be subject to legal action, if their actions are aligned with these guidelines.

Out of Scope

The following activities are not permitted under this policy:

- Social engineering or phishing attempts
- Physical security testing
- Denial of Service (DoS) or disruption-based attacks
- Automated scans that degrade system performance
- Accessing, modifying, or destroying data without authorization

Contact

To report a vulnerability or ask a question about this policy, please email:
IT@swartley.com

Thank you for helping keep Swartley Brothers secure.