ENFEC LLC

ENFEC Responsible Vulnerability Disclosure Policy

Contents

Policy

At ENFEC, the security of our systems, products, and services is a top priority. We welcome responsible vulnerability disclosures from the security research community, as they help us identify and address potential weaknesses in our infrastructure, ensuring the safety and privacy of our users.

This policy outlines the guidelines for reporting security vulnerabilities to ENFEC, the steps we take to address them, and the protections we offer for responsible disclosure.

Our Commitment to Security

We are committed to:

- Promptly investigating all reported vulnerabilities.
- Resolving vulnerabilities as quickly as possible, prioritizing high-risk issues.
- Maintaining transparent communication with researchers throughout the process.
- Recognizing and acknowledging the contributions of responsible researchers.

Scope of the Program

We encourage reports of vulnerabilities related to the following ENFEC systems, products, and services:

- Web Applications: enfec.com

Excluded from the program:

- Third-party services and platforms not owned or operated by ENFEC.
- Social engineering attacks, phishing attempts targeting ENFEC employees.
- Physical security vulnerabilities, unauthorized access to ENFEC premises.

Reporting a Vulnerability

If you believe you've discovered a vulnerability in one of ENFEC's systems, please follow these steps to report it:

1. Do not exploit the vulnerability or access user data unless explicitly authorized.
2. Report the issue to us via **email**: **security@enfec.com**.
3. Include the following information in your report:
    - A clear and concise description of the vulnerability.
    - Detailed steps to reproduce the issue.
    - The potential impact of the vulnerability.
    - Any supporting materials - screenshots, proof of concept, or logs.

We will acknowledge receipt of your report within **2 business days**.

What to Expect After Reporting

Once your report has been submitted, here's what you can expect:

- Acknowledgment: We will confirm receipt of your report within 2 business days.

- Investigation: Our security team will investigate the reported vulnerability and may reach out to you for additional information.
- Resolution: If the vulnerability is verified, we will prioritize remediation based on severity and impact.
- Public Disclosure: Once the issue is resolved, we may publish a security advisory detailing the vulnerability and the steps taken to address it, with proper attribution to the researcher.

Safe Harbor

We offer the following protections for individuals who report vulnerabilities responsibly and in accordance with this policy:

- We will not pursue legal action against you for activities related to the vulnerability report, as long as your actions fall within the scope of this policy.
- We will not publicly disclose your identity without your permission, except as required by law.
- You are **protected** from legal liability for research activities if you follow the guidelines, including avoiding disruption or damage to our services or users.

Guidelines for Responsible Disclosure

To ensure that your actions are ethical and responsible, please follow these guidelines:

- Do not exploit the vulnerability in a way that could harm users, services, or systems.
- Do not share the vulnerability with any third parties until we have had the opportunity to address it.
- Limit your testing to activities necessary to confirm the existence of the vulnerability.
- Avoid accessing personal, financial, or sensitive user data unless absolutely required for the investigation and you have explicit authorization.
- If you are unsure whether your actions fall within the responsible disclosure process, please contact us for clarification.

Recognition & Rewards

While ENFEC does not currently offer financial rewards for vulnerability disclosures, we highly value the contributions of ethical hackers and researchers who help us secure our systems. As a thank you, we may:

- **Acknowledge** your contribution in a public security advisory or on our website (with your consent).

Legal Notice

This policy does not authorize illegal or unauthorized actions. Researchers are expected to comply with all applicable laws when identifying and reporting vulnerabilities. Any activity that goes beyond the scope outlined in this policy (e.g., accessing or deleting data, disrupting services) may result in legal consequences.

Contact Information

To report a vulnerability or for any questions related to security, please contact us via:

- **Email**: security@enfec.com

Changes to the Policy

ENFEC reserves the right to modify or update this policy at any time. Any changes will be posted on our website and apply to all future vulnerability reports.

Thank You!

Thank you for helping us maintain the security and integrity of our systems. We appreciate your efforts to report vulnerabilities responsibly and contribute to the safety of ENFEC and its users.