Vulnerability Disclosure Policy

Version: 1.0

Document Owner: Product Security Incident Response Team (PSIRT)

---

1. Purpose

Our organization is committed to maintaining the security of its products and services. We value the responsible efforts of security researchers, customers, partners, and other individuals who help identify cybersecurity vulnerabilities.

We currently do not operate a vulnerability reward or bug bounty program.

This Vulnerability Disclosure Policy describes how to report security vulnerabilities and how we handle reported issues in accordance with the principles of responsible and coordinated vulnerability disclosure and applicable regulatory requirements, including applicable cybersecurity legislation and industry best practices.

---

2. Scope

This policy applies to products and services developed, operated, or supported by our organization. Where a reported vulnerability relates to a third-party component used within our products, we will coordinate the assessment and remediation as appropriate. Vulnerabilities relating exclusively to products or services that are not owned, developed, or supported by our organization should be reported to the respective vendor.

---

3. Reporting a Vulnerability

If you believe you have discovered a security vulnerability in one of our products or services, please report it as soon as possible by email.

Email: psirt@company.com

We kindly request that you do not publicly disclose the vulnerability until we have had a reasonable opportunity to investigate and, where appropriate, provide a remediation.

---

4. Information to Include

To help us investigate your report efficiently, please include as much of the following information as possible:

- Vulnerability title
- Product name and model
- Affected URL or service (where applicable) (optional)
- Software or firmware version
- Description of the vulnerability
- Potential security impact
- Weakness classification (e.g., CWE), if known (optional)
- Severity assessment (e.g., CVSS), if known (optional)
- Steps to reproduce the issue
- Supporting evidence (such as screenshots, logs, or proof of concept)
- Possible mitigation or recommendation (optional)
- Your contact information for follow-up questions (optional)

---

5. Our Commitment

Upon receiving a vulnerability report, we will:

- Acknowledge receipt of your report within **5 business days**.
- Review and assess the reported vulnerability.
- Aim to complete the initial technical assessment within **10 business days**, where reasonably practicable.
- Contact you if additional information is required.

- Keep you informed of significant progress where appropriate.
- Notify you when our investigation has been completed and, where appropriate, when a remediation or mitigation is available.

Where a reported vulnerability affects third-party components or suppliers, additional coordination may be required and resolution timelines may be extended.

Vulnerabilities are prioritized based on their potential impact, severity, exploitability, and the affected products or services. Investigation and remediation timelines may vary depending on the complexity of the issue. We kindly ask reporters to avoid requesting status updates more frequently than once every **14 days**, allowing our teams to focus on remediation.

---

6. Responsible Disclosure

We ask security researchers to:

- Act in good faith.
- Avoid actions that could disrupt our products or services.
- Avoid accessing, modifying, or deleting data that is not necessary to demonstrate the vulnerability.
- Report vulnerabilities responsibly and allow reasonable time for investigation and remediation before any public disclosure.
- Comply with all applicable laws and regulations during their research.
- When validating a vulnerability, please use only the minimum testing necessary to demonstrate the issue and avoid actions that could damage, disrupt, or negatively affect our products, services, or customer data.

---

7. Safe Harbor

We will not pursue legal action against individuals who:

- Act in good faith.
- Comply with this Vulnerability Disclosure Policy.
- Avoid causing harm to our customers, products, services, or data.

- Do not exploit the vulnerability beyond what is necessary to demonstrate its existence.
- Coordinate disclosure with us before making information public.

This Safe Harbor applies only to activities conducted in accordance with this policy.

Nothing in this policy limits applicable legal or regulatory obligations.

---

8. Security Advisories

Where appropriate, security advisories, vulnerability information, and available security updates will be published on our Product Security webpage.

Security Advisories:

https://company.com/security-advisories (this link is currently in development)

---

9. Contact Information

For all security vulnerability reports and questions related to this policy, please contact:

Product Security Incident Response Team (PSIRT)

Email: psirt@company.com

Thank you for helping us improve the security of our products and protect our customers through responsible vulnerability disclosure.