

Responsible Vulnerability Disclosure Policy

1. Purpose

Foxguard is committed to ensuring the security of its customers and their affiliated entities by protecting their information. We welcome the private and responsible submission of vulnerability disclosures to help us reduce risk to our customers and further improve our security posture.

This policy defines the guidelines and restrictions for conducting vulnerability discovery activities, including what systems and types of research are covered, and the preferred methods to submit discovered vulnerabilities to Foxguard.

We encourage you to contact us to submit potential vulnerabilities in our systems.

2. Reference documents

N/A

3. Authorization

Foxguard embraces good faith security research that is beneficial to its customers. If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized, we will work with you to understand and resolve the issue quickly, and Foxguard will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

Foxguard is not obligated to consider research that violates this policy and will consider a submission noncompliant if the vulnerability is publicly disclosed without express written consent from Foxguard.

4. Guidelines

Under this policy, “research” means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability’s presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- Treat all vulnerability information and discussions with us as confidential. Do not disclose any such information or communications to any third party or to the public in general without the prior written authorization of Foxguard.
- Do not submit a high volume of low-quality reports.
- Do not perform research on Foxguard products licensed, owned, or operated by a customer without their express permission.
- Do not perform attacks against Foxguard employees, customers, partners, or representatives.
- Do not engage in extortion.
- Do not run automated scanning tools against Foxguard products outside of your own network.
- Do not perform network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data.

- Do not perform physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing.
- Perform testing only on in-scope systems, and respect systems and activities which are out-of-scope.

Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information (PII), financial information, or proprietary information or trade secrets of any party), you must stop your test, notify us immediately, and not disclose this data to anyone else.

5. Scope

- Foxguard Portal
- SFTP transfer mechanisms
- Patchintel Reports
- Patchintel Binaries

Any service not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing. **Additionally, vulnerabilities found in systems from our vendors fall outside of this policy's scope and should be reported directly to the vendor according to their disclosure policy (if any).** If you aren't sure whether a system is in scope or not, contact us at Disclosure@foxguardsolutions.com before starting your research.

6. Submission Process

Any submissions from security researchers should be sent to Disclosure@foxguardsolutions.com. No other mechanisms should be used to discuss Foxguard vulnerabilities or exploits.

All submissions should include:

- A detailed description of the vulnerability or exploit and the location it was discovered.
- Detailed description of the steps needed to reproduce the vulnerability or exploit (proof of concept or screenshots are helpful).
- Information about your system's configuration (browser, OS, product version, IP address associated with your activities).

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect other entities, Foxguard may share information regarding your submissions, your name or contact information (if provided) will not be shared without express permission.

7. Questions

Questions regarding this policy may be sent to Disclosure@foxguardsolutions.com. We also invite you to contact us with suggestions for improving this policy.