CYBERSECURITY & TRUST GOVERNANCE

Vulnerability Disclosure Policy (VDP)

Last Revised: **2026-09-12** v1.5-VDP

0.0 Preamble & Security Stance

At **Sheernox Technology Group** ("Sheernox", "we", "us", or "our"), an unincorporated sole proprietorship registered in the Province of British Columbia, Canada, maintaining the confidentiality, integrity, and availability of our systems, infrastructure, and client data is our foundational priority.

We recognize the vital role that independent, ethical security researchers, penetration testers, and academic cryptographers play in strengthening global cybersecurity. We welcome responsible security research conducted against our public-facing internet infrastructure and believe that collaboration with the cybersecurity community results in safer services for all our clients.

This Vulnerability Disclosure Policy ("Policy") provides clear, legally grounded parameters under which ethical researchers may investigate, identify, and report potential security vulnerabilities to Sheernox in good faith, and outlines our explicit commitments in return.

POLICY OVERVIEW

Sheernox encourages ethical security research. If you discover a vulnerability in good faith following these guidelines, we provide legal safe harbor, pledge responsive triage within 5 business days, and collaborate under coordinated disclosure.

1.0 Legal Safe Harbor & Authorization

Sheernox considers security research conducted strictly in accordance with this Policy to be **authorized conduct** under applicable legal frameworks. If you conduct vulnerability research in good faith and in full compliance with the conditions outlined herein, Sheernox commits to the following legal protections:

- 1.1 **Criminal Immunity Covenant:** Sheernox will not initiate, pursue, or encourage criminal complaints or law enforcement investigations against you for unauthorized access under Section 342.1 (*Unauthorized use of computer*) or Section 430(1.1) (*Mischief in relation to computer data*) of the Canadian *Criminal Code* (R.S.C. 1985, c. C-46), the United States Computer Fraud and Abuse Act (CFAA, 18 U.S.C. § 1030), or equivalent foreign statutory instruments.
- 1.2 **Civil Litigation Waiver:** Sheernox will not initiate or support any civil lawsuit or claim against you for breach of contract, trespass to chattels, Computer Misuse acts, or intellectual property infringement arising directly from your compliant research activity.
- 1.3 **DMCA / Anti-Circumvention Protection:** Sheernox will not bring a claim against you for circumvention of technological security measures under Section 41 of the Canadian *Copyright Act* (R.S.C. 1985, c. C-42) or Section 1201 of the US *Digital Millennium Copyright Act* (17 U.S.C. § 1201) for security evaluations conducted within the scope of this Policy.
- 1.4 **Third-Party Notice:** If a third party or law enforcement agency initiates an inquiry or legal action against you arising from activities conducted within the strict parameters of this Policy, Sheernox will formally affirm that your activities were conducted with our knowledge, authorization, and consent.

Statutory Framework • Safe Harbor Declaration

Good faith security research adhering to this policy is legally authorized by Sheernox under the laws of British Columbia and Canada, preventing prosecution under Criminal Code s. 342.1 or civil claims under common law trespass and breach of service.

2.0 In-Scope Assets

This Policy applies exclusively to internet-facing digital assets and infrastructure owned, operated, and directly maintained by Sheernox Technology Group. The following targets are explicitly within scope:

Target Type	Identifier / FQDN	Status	Permitted Activities
2.1 **Primary Web Portal**	sheernox.com / www.sheernox.com	IN SCOPE	Web application vulnerability testing, CSRF, XSS, SSRF, authentication checks.
2.2 **Client Management Hub**	my.sheernox.com	IN SCOPE	Authentication flow testing, session handling, IDOR analysis, billing API validation.
2.3 **CDN & Legal Portals**	cdn.sheernox.com / legal.sheernox.com	IN SCOPE	CORS verification, cache poisoning analysis, static asset access controls.
DNS Clusters	Authoritative Anycast Nameservers (ns*.sheernox.com)	IN SCOPE	DNS zone delegation, query spoofing, DNSSEC validation (non-disruptive only).
Public APIs & Endpoints	api.sheernox.com/*	IN SCOPE	REST API parameter manipulation, rate-limit boundary testing, token evaluation.

Any asset, domain, or sub-domain not specifically enumerated above, or belonging to third-party providers, should be presumed out of scope unless verified in writing by Sheernox prior to testing.

3.0 Out-of-Scope Assets & Prohibited Methods

To protect the stability of our operations and the sensitive data of our clients, certain research activities and system targets are strictly prohibited. Engaging in any of the prohibited methods below immediately voids all legal safe harbor protections:

Strictly Prohibited • Immediate Forfeiture of Safe Harbor

Denial of Service (DoS/DDoS) attacks, automated volume flooding, physical facility intrusion, social engineering of personnel, and accessing or exfiltrating client data are strictly prohibited under all circumstances.

- 3.1 **Denial of Service (DoS/DDoS):** Any volumetric attack, SYN flood, HTTP slowloris, application-layer amplification, or actions calculated to degrade system responsiveness or exhaust bandwidth.
- 3.2 **Customer Data Exfiltration:** Accessing, viewing, downloading, altering, or storing any personal data, credit card information, customer source code, or internal client communications. If you discover a vulnerability that yields access to customer data, you must *stop immediately* and report the issue without downloading further data.
- 3.3 **Physical Security Attacks:** Any physical attempt to breach, inspect, or tamper with datacenters, colocation suites, server racks, transit cabinets, or office premises.
- 3.4 **Social Engineering & Phishing:** Phishing, spear-phishing, vishing, SMS spoofing, pretexting, or any psychological manipulation directed at Sheernox employees, contractors, or customers.
- 3.5 **Uncoordinated Automated High-Rate Fuzzing:** Running automated vulnerability scanners (e.g., Nessus, Acunetix, sqlmap) at high concurrency rates that trigger server overload or flood logging mechanisms without prior written coordination.
- 3.6 **Upstream & Third-Party Services:** Third-party infrastructure outside Sheernox direct control, including upstream Tier 1 carrier transit networks, hyperscale cloud hypervisors (OVHcloud, Vultr, AWS), cPanel/WHM upstream core vulnerabilities, or payment processors (Stripe).

4.0 Guidelines for Ethical Research

We require all researchers participating in our disclosure program to adhere to the following professional code of ethics:

- 4.1 **Minimum Proof of Concept:** Use the minimal amount of testing necessary to demonstrate the presence of a flaw. Do not execute destructive payloads, drop persistent backdoors, or pivot deeper into internal subnets once vulnerability is confirmed.

- 4.2 **Privacy First:** If you inadvertently encounter any personal information, payment card numbers, or proprietary business records during testing, immediately cease testing, notify us, and do not copy, transmit, or cache the data.
- 4.3 **Data Purging:** Safely destroy all temporary evidence, logs, payloads, and screen captures containing client or infrastructure data within seven (7) calendar days following confirmation of resolution.
- 4.4 **Single Account Scope:** Create and use only your own test accounts within my.sheernox.com for testing privilege escalation, IDOR, or session separation flaws. Never attempt to access another user's live account without express written consent.

5.0 How to Report Vulnerabilities

All vulnerability submissions must be submitted directly to the Sheernox Security & Abuse Operations Department:

> **Designated Reporting Endpoint**
> **Email: abuse@sheernox.com**
> **Subject Format:** [SECURITY VULNERABILITY] <Target FQDN / Component> - <Severity Rating>

To enable our engineering team to reproduce and validate the vulnerability promptly, please include the following technical details:

- 5.1 **Vulnerability Classification:** OWASP Top 10 or CWE classification, along with estimated CVSS v3.1 score and vector string.
- 5.2 **Affected Target:** Exact FQDN, HTTP endpoint, port number, or API parameter.
- 5.3 **Reproduction Steps:** Clear, step-by-step technical instructions written in English, including raw HTTP request/response transcripts or minimal curl commands.
- 5.4 **Proof of Concept (PoC):** Non-destructive demonstration script or sanitized screenshot illustrating the flaw.
- 5.5 **Potential Impact:** Your assessment of how an attacker could exploit the issue in practice.
- 5.6 **PGP Encryption (Optional):** For sensitive reports containing critical zero-day details, researchers may request our PGP public key prior to sending attachments.

6.0 Response SLA & Triaging Timelines

Sheernox is committed to prompt, respectful, and transparent communication throughout the disclosure lifecycle:

Lifecycle Milestone	Target SLA Window	Sheernox Commitment
6.1 **Initial Acknowledgment**	**≤ 48 business hours**	Confirmation of report receipt with an assigned internal tracking ticket ID.
6.2 **Triage & Validation**	**≤ 5 business days**	Technical validation of reproduction steps and determination of severity and exploitability.
6.3 **Remediation Updates**	**Every 14 business days**	Progress reports on patch development, staging verification, and deployment schedules.
6.4 **Resolution Notice**	Upon deployment	Formal confirmation that the vulnerability has been patched in production and is ready for re-testing.

We ask researchers to respond to clarifying requests in a timely manner to maintain active triage momentum.

7.0 Coordinated Disclosure & Confidentiality

Sheernox operates on the principle of **Coordinated Vulnerability Disclosure (CVD)**. We believe public disclosure before an effective security remediation has been deployed unnecessarily endangers our systems and customers.

- 7.1 **Standard 90-Day Embargo:** Researchers agree to keep details of reported vulnerabilities strictly confidential for a period of ninety (90) calendar days from our initial acknowledgment, or until Sheernox has deployed a verified production patch, whichever occurs first.
- 7.2 **Early Public Disclosure Prohibited:** Disclosing vulnerability details, exploit scripts, or indicators of compromise to public forums, social media, or third parties prior to patch release or the expiration of the embargo voids safe harbor protections.
- 7.3 **Mutual Extension:** In cases involving complex architectural remediations or upstream third-party dependencies, Sheernox and the researcher may mutually agree in writing to extend the disclosure embargo.

> **RESPONSIBLE TIMING**
> Our 90-day embargo gives our engineers adequate time to patch, test, and deploy fixes across all environments before vulnerability specifics become publicly accessible to adversaries.

8.0 Security Researcher Hall of Fame & Recognition

8.1 **Security Researcher Hall of Fame:** We deeply appreciate the efforts of security researchers who dedicate their skill and time to improving Sheernox's security posture. To express our gratitude:

- **Hall of Fame:** Eligible researchers will be formally credited on our public Security Acknowledgements Registry with their name, handle, and professional link.
- **Eligibility Criteria:**
  1. You must be the first researcher to report the specific, valid vulnerability.
  2. The vulnerability must be verifiable and classified as Medium, High, or Critical severity under CVSS v3.1.
  3. You must have complied with all requirements of this Policy, including safe harbor guidelines and confidentiality embargoes.
- **Bounty Policy Notice:** Sheernox does not operate a paid monetary bug bounty program at this time. We provide public professional recognition, letters of appreciation, and collaborative reference support upon request.

9.0 Governing Law & Official Contact Information

This Policy is governed by and construed in accordance with the laws of the **Province of British Columbia** and the federal laws of **Canada** applicable therein. Any dispute arising under this Policy shall be resolved exclusively by the courts of British Columbia sitting in the City of Kamloops.

> **Official Contact Coordinates**
> **Entity:** Sheernox Technology Group (Sole Proprietorship)
> **Physical & Mailing Address:** 1-1885 Grasslands Blvd, Kamloops, BC, V2B 0B8, Canada
> **Vulnerability Reports & Abuse Operations: abuse@sheernox.com**
> **General Inquiries & Legal Administration: support@sheernox.com**
> **Client Support Ticket Portal: https://my.sheernox.com**

© 2026 Sheernox Technology Group • 1-1885 Grasslands Blvd, Kamloops, BC, V2B 0B8, Canada • All Rights Reserved