NovaLink

Vulnerability Disclosure Policy

Responsible disclosure and safe-harbor for security researchers

---

Document ID: NL-VDP-01

Version: 1.0

Status: Issued

Issuing entity: Auralink Nova Technology L.L.C (Dubai, UAE, Reg. No. 1607764) — Technology Provider

Applies to: security research on the NovaLink network, the Nx1/Hx1 Home Station and the NovaLink web properties

The NovaLink entities: Ntech Link Technologies Ltd, Co. No. 2195904 (Store Operator) · Auralink Nova Technology L.L.C, Dubai, Reg. No. 1607764 (Technology Provider) · NodeLink USA, Inc., Delaware, File No. 10606222 (US Distribution)

Effective date: 22 May 2026

Contact: support@novalink.tech

---

1. Introduction

The Company ("the Company") welcomes security research that helps make the Company Network safer for Node Operators, Users, and Workload Publishers. This Vulnerability Disclosure Policy (the "VDP") sets out how security researchers can report vulnerabilities, what they can expect from the Company, and the safe-harbor protections that apply to good-faith research.

This VDP is aligned with the principles of ISO/IEC 29147:2018 (Vulnerability disclosure) and ISO/IEC 30111:2019 (Vulnerability handling processes).

2. Scope

2.1 In scope.

- The Nx1/Hx1 Home Station hardware and firmware.
- The Company Workload Runtime and Coordination Plane.

- The NovaLink web properties and the community platform web applications, including their APIs.
- The Company AI Chatbot.
- The Company-published mobile applications (when released).

2.2 Out of scope.

- Third-party services not operated by the Company (HMall, Living By Design, partner DePIN systems). Reports about these systems should be sent to the operator concerned.
- Reports based purely on automated scanner output without a demonstrable proof-of-concept.
- Denial-of-service testing against production systems (test environments are available; contact support@novalink.tech to arrange).
- Social-engineering of the Company personnel.
- Physical attacks against the Company offices.

3. How to report

3.1 Channel.

Send reports to support@novalink.tech. PGP key fingerprint and full public key are published at /.well-known/security.txt on the NovaLink web properties. Where the disclosure would expose personal data, please encrypt the report with the public key.

3.2 What to include.

- A clear description of the vulnerability, including affected system, version, and impact.
- Step-by-step reproduction instructions or a proof-of-concept.
- Your assessment of severity (CVSS v3.1 score and vector).
- Whether you intend to publish a write-up, and if so, on what timeline.

4. What you can expect from the Company

Stage	The Company response time
Acknowledgement of receipt	Within 2 business days
Initial triage and severity assessment	Within 5 business days
Validation or rebuttal	Within 10 business days
Remediation plan and target fix date	Within 15 business days
Critical / actively exploited fix	As quickly as practicable; we aim for 72 hours where the fix is within our exclusive control
High severity fix	Within 30 days
Medium severity fix	Within 60 days
Low severity fix	Within 90 days

5. Safe harbor

The Company will not pursue civil or criminal action under the BVI Computer Misuse and Cybercrime Act, the U.S. Computer Fraud and Abuse Act, the UK Computer Misuse Act 1990, the Australian Cybercrime Act 2001 (Cth), or equivalent statutes, against a researcher who in good faith:

1. Reports the vulnerability promptly to support@novalink.tech;
2. Limits testing to the minimum needed to confirm the issue;
3. Does not access, modify, or download data belonging to other Users beyond what is necessary to demonstrate the vulnerability;
4. Does not destroy, exfiltrate, or publicly disclose data obtained through the testing;
5. Provides the Company a reasonable opportunity to remediate before public disclosure (default 90 days from acknowledgement, longer if the issue is complex and we ask).

6. Recognition

The Company does not currently operate a paid bug-bounty program but maintains a public Security Hall of Fame at a public Security Hall of Fame on the NovaLink web properties and is happy to provide letters of recommendation or LinkedIn references for substantive contributions. A funded bug-bounty program is on the Compliance and Certification Roadmap for Q1 2027.

7. Coordinated disclosure

The Company supports coordinated disclosure. We will work with the reporter, CERT/CC, national CERTs, and (where appropriate) MITRE for CVE issuance. We will not name the researcher publicly without permission.

8. Contact

support@novalink.tech | /.well-known/security.txt on the NovaLink web properties