NovaLink

Published notice — status, accuracy and right to amend. This document is published by the Company in good faith for general information and transparency. It is current only as of its stated date and is provided “as is,” without warranty of completeness or accuracy; it may contain errors or omissions and does not constitute legal, financial, tax, or investment advice, an offer or solicitation, or any guarantee. The Company may revise, correct, update, supplement, or withdraw this document at any time without prior notice, and the version published on the NovaLink Transparency Portal is the controlling current version and supersedes any earlier copy. Where this document conflicts with a signed agreement between you and the Company, or with applicable law, that signed agreement or applicable law prevails. If you believe anything here is inaccurate or out of date, please contact support@novalink.tech so we can review it and, where appropriate, correct it. To the maximum extent permitted by law, the Company accepts no liability for any reliance placed on this document.

Technical Security Whitepaper

Architecture, controls, threat model, and certification roadmap

---

Document ID: NL-SEC-01

Version: 1.1 (revised 10 November 2026)

Status: Issued

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

Applies to: the NovaLink product, network and Nx1/Hx1 Home Stations, regardless of which Community Platform a participant joined through

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. Executive summary

This whitepaper describes the security architecture of the Company Network and the Nx1/Hx1 Home Station ("Nx1/Hx1 Home Station"). It is the document a sophisticated technical reviewer, an enterprise customer, or a Node Operator with infrastructure responsibility would expect to receive before installing an Nx1/Hx1 Home Station on a network they care about.

The Company's security posture is structured around four principles: defence in depth, default-deny for high-risk Workload classes, cryptographic attribution of every Workload Session, and progressive third-party assurance.

> *A note on the maturity of these controls. This whitepaper distinguishes throughout between (i) controls that are implemented and operational today, (ii) controls that are in active rollout, and (iii) controls that are committed-roadmap items with target dates. Items in category (ii) and (iii) are marked accordingly. The maturity of the network is tracked publicly in the Compliance and Certification Roadmap (NL-ROAD-01).*

2. The Company threat model

The Company considers the following actors and threats in its design:

Actor	Goal	The Company's primary defence
Malicious Workload Publisher	Use the Company Network to host CSAM, run malware C2, send spam, or stage DDoS	KYB onboarding, sanctions screening, Workload Publisher Agreement, code-signing, runtime sandboxing, abuse-handling SLAs
Compromised Node Operator	Steal Workload data, deny service, exfiltrate user PII	Workload encryption-in-flight and at-rest, attestation of Nx1/Hx1 Home Station firmware, signed Runtime, no Workload Publisher data left on disk after session
External attacker on the public internet	Compromise the Nx1/Hx1 Home Station over the network	Inbound default-deny firewall, no admin ports exposed to WAN, signed update channel, automatic security patching
External attacker on the Node Operator's LAN	Pivot from the Node Operator's LAN to Nx1/Hx1 Home Station or vice versa	Built-in LAN isolation (LAN interface in a separate network namespace; no route from any Workload to the LAN), default-deny host firewall on the LAN interface, no inbound ports
Insider (the Company personnel)	Disclose Workload traffic content, exfiltrate User data	Least-privilege access, dual-control for production data access, audit logging of admin actions, no-content-logging at the Workload layer
Law enforcement / state actor	Compel disclosure or operational assistance	Documented LE Policy with minimum-necessary disclosure, attribution-only metadata model, transparency reporting

3. Hardware

There is one machine: a single hardware model running a single operating system. “Nx1” and “Hx1” are the same machine — the name reflects the participant's community, nothing else. There are no hardware versions, generations or OS variants; the operating system on every machine is kept current through signed over-the-air updates delivered by the Technology Provider through the network's coordination plane (the Control Tower), so no machine is ever left behind on an older version.

- The Nx1/Hx1 Home Station is an Intel N-family x86 mini-computer with 12 GB LPDDR5 RAM, 256 GB M.2 SSD, dual gigabit Ethernet, Wi-Fi 6, Bluetooth 5.2. It has no microphone and no camera.
- Production units ship with a Trusted Platform Module (TPM 2.0) or fTPM, used for boot attestation and to anchor disk-encryption keys.
- Each Nx1/Hx1 Home Station has a unique factory-provisioned device identity ("Nx1/Hx1 Home Station Device Identity") in the form of an X.509 certificate, with the private key generated and held by the TPM and never exported.

Status: hardware spec is current, and it is the same for every machine — one model, one operating system; there are no hardware batches or versions with different capabilities. The TPM 2.0 module is present on every machine; TPM-anchored boot attestation is an operating-system capability being enabled fleet-wide by signed over-the-air update, with fleet-wide completion targeted for Q3 2026. Nx1/Hx1 Home Station Device Identity provisioning is live as of Q1 2026 on all machines.

4. Operating system and base image

- Nx1/Hx1 Home Station ships with a hardened Linux base image (kernel hardening, AppArmor, IPv6 ULA disabled by default, journald audit on).
- The base image is read-only outside designated mutable directories.
- Inbound SSH is disabled by default. Remote administration is via a the Company-managed reverse channel (mTLS, audited).
- OS updates are delivered via a signed update channel; package signatures are verified against a the Company-controlled trust root.

5. The Workload Runtime

5.1 Containment.

Each Workload runs in its own isolation domain. The Company uses a layered approach:

1. For most Workload classes, isolation is a Linux container (cgroups v2 + namespaces + seccomp profile + read-only root + dropped capabilities + dedicated network namespace).
2. For high-risk classes (e.g., third-party connectivity relay), isolation is a lightweight virtual machine (Firecracker-class microVM) with a dedicated kernel.
3. The Node Operator's LAN interface is in a separate network namespace from any Workload network namespace. Workloads cannot reach the Node Operator's LAN.

Status: container isolation is live. MicroVM isolation is in late development and is the gating control for the Consumer Connectivity Relay class — that class will not be enabled in production until microVM isolation is independently reviewed (target Q4 2026).

5.2 Workload code signing.

Every Workload artefact must be signed with a Workload Publisher's key. The Runtime verifies the signature against a the Company-issued certificate before launch. Unsigned, modified, or revoked artefacts are refused.

5.3 Workload egress policy.

- Privacy-preserving compute Workloads have egress only to a whitelisted set of the Company coordination endpoints.
- Storage Workloads have egress only to the Company and partner storage coordinators.
- Bitcoin proof-of-work Workloads have egress only to the mining pool endpoint; enterprise edge compute Workloads have egress only to allow-listed endpoints.
- Connectivity relay Workloads have egress controlled by per-Workload-class destination policy and per-Workload rate limits.

5.4 Attribution.

Every outbound packet from a connectivity-relay Workload Session is correlated with a Workload Session ID. The mapping is retained for the 180-day window described in the Data Minimisation & Retention Policy, sufficient to respond to abuse complaints and law-enforcement requests.

Stated precisely, because it matters: the automated abuse screening is flow analysis, not payload inspection. No TLS session is terminated or intercepted anywhere in the path. The control operates on connection metadata — server name indication, size, timing and pattern — together with DNS resolution checked against policy in memory and then discarded; DNS queries are not collected, and nothing inside an encrypted session is read.

6. Networking

6.1 What the Nx1/Hx1 Home Station listens on.

- WAN interface: no inbound ports open by default. Outbound TLS to the Company coordination plane only.
- LAN interface: only the local management port (used by the Node Operator to view dashboard / status). Bound to RFC1918 / link-local addresses by default. Optional Wi-Fi Direct setup mode disabled after pairing.

6.2 Built-in LAN isolation.

LAN isolation is built into the Nx1/Hx1 Home Station: the LAN interface sits in its own network namespace, no Workload namespace has a route to it, and a default-deny host firewall and AppArmor profiles protect both interfaces. No router configuration is needed.

6.3 Bandwidth and capacity.

See Section 5 of the Node Operator Agreement and the Company WIKI for the bandwidth allocation (up to 200 Mbps per machine, which the Node Operator may cap) and the 5-machines-per-IP rule.

7. Identity, access management, and cryptography

- User authentication: email + password with mandatory MFA/2FA, in line with Section 4 of the Terms and Conditions. Password storage: Argon2id with per-user salt.
- Workload Publisher authentication: API key with HMAC-signed requests, plus mTLS for high-volume publishers.
- Nx1/Hx1 Home Station-to-coordination plane authentication: mutual TLS using the Nx1/Hx1 Home Station Device Identity certificate.
- Cryptographic primitives in use: TLS 1.3, AES-256-GCM, ChaCha20-Poly1305, Ed25519 for signing, X25519 for key agreement.

8. Personnel and operational controls

- The Company personnel with access to production are subject to background checks at hire and to annual policy refreshers.
- Production access is segregated by role; no single individual can both write code and deploy it without secondary review (the four-eyes principle).
- All production admin actions are logged to an append-only audit log retained for 24 months.
- Encryption keys for log stores are stored in a hardware security module under dual control.

9. Vulnerability management

- The Company runs continuous SCA (software composition analysis) on the Runtime and base image, with security-critical patches deployed via the signed update channel within published SLAs.
- A Vulnerability Disclosure Policy (NL-VDP-01) is published and reachable from /.well-known/security.txt on the NovaLink web properties. Security researchers acting in good faith are protected by the safe-harbor language in that policy.
- The Company will commission a first independent penetration test of the Nx1/Hx1 Home Station, Runtime, and coordination plane in 2027, and annually thereafter (see Compliance and Certification Roadmap).

10. Incident response

- The Company maintains an Incident Response procedure with named roles (Incident Commander, Communications Lead, Technical Lead, Legal Lead).
- On confirmation of a security incident affecting User personal data, the Company will notify the affected User and, where required, the relevant supervisory authority within 72 hours (GDPR Art 33), the Office of the Australian Information Commissioner (where applicable), and the California Attorney General (where the CCPA threshold is met).
- A summary post-incident report will be published in the annual transparency report.

11. What this whitepaper does not yet claim

Consistent with a transparent, evidence-based approach, the Company expressly does not claim, as of the date of this whitepaper, the following:

- ISO/IEC 27001:2022 certification — target Q3 2028.
- SOC 2 Type I or Type II report — target Q2 2027 (Type I), Q4 2027 / Q1 2028 (Type II).
- Independent no-content-logging assurance review — target 2027.
- Cure53-equivalent independent application security assessment — target 2027.

Each of these is a tracked commitment in the Compliance and Certification Roadmap. This whitepaper should be assessed alongside that roadmap when evaluating the maturity of the network.

12. Contact

Security questions: support@novalink.tech | Responsible disclosure: see Vulnerability Disclosure Policy (NL-VDP-01).