**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 If you believe anything here is inaccurate or out of date, please contact support@novalink.tech so we can review it and, where appropriate, correct it.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.

# Data Minimisation & Retention Policy

*What we collect, what we don't, and for how long*

---

Document ID: NL-LOGS-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. Purpose

This Data Minimisation & Retention Policy (the "Logs Policy") describes, with technical specificity, what data the Company ("the Company") collects, processes, and retains in connection with operation of the Company network, including in particular: (a) data routed through the Nx1/Hx1 Home Station ("Nx1/Hx1 Home Station") as part of a third-party Workload Session, (b) operational telemetry generated by the Nx1/Hx1 Home Station, and (c) account and transactional data held by the NovaLink Platform.

This policy is intended to provide the level of transparency that a sophisticated technical operator or auditor would reasonably expect of a network operator that handles residential infrastructure. It supplements (and where more specific, prevails over) the Company Privacy and Cookies Policy.

## 2. Headline position

The Company does not retain the content of third-party Workload traffic routed through an Nx1/Hx1 Home Station. The Company retains a minimum set of metadata sufficient to attribute traffic to a Workload Session (for abuse-handling and law-enforcement attribution purposes) and to operate the Nx1/Hx1 Home Station reliably, on the retention windows set out in Section 5.

For clarity: this is a minimum-metadata, content-free retention model — not a zero-retention or “no logs” model. Account and KYC data, device telemetry and workload session metadata are retained for the defined windows set out in Section 3, while the content of third-party Workload traffic is never retained and is discarded in flight. The no-content-logging position has not yet been independently verified; the first independent assurance review is targeted for 2027. Descriptions of the platform as “keeping no logs” should not be used.

# 3. Three layers of data

**3.1 Layer A — Account and platform data.**

Data that the User provides to the Company to create an account, complete KYC, transact, or use Platform features. Governed by the Privacy and Cookies Policy and listed in Section 1 of that policy.

3.2 Layer B — Nx1/Hx1 Home Station operational telemetry.

Data the Nx1/Hx1 Home Station emits to the Company in order to (a) prove that the device is online and contributing to the network and (b) allow the Company to schedule Workloads to it. This data is about the device, not about any individual User's personal browsing.

**3.3 Layer C — Workload traffic.**

Data that traverses the Nx1/Hx1 Home Station as part of a third-party Workload Session. This is by far the largest data category by volume.

# 4. What the Company collects, by layer

**4.1 Layer A — Account and platform data.**

As listed in the Privacy and Cookies Policy. In short: name, email, phone, KYC documents, transaction records, support correspondence, dashboard activity.

4.2 Layer B — Nx1/Hx1 Home Station operational telemetry.

| Field | Example | Why we collect it |
|---|---|---|
| **Device serial number / Nx1/Hx1 Home Station ID** | Nx1/Hx1 Home Station-A1B2C3D4 | Identifies the device and links it to a Node Operator account |
| Heartbeat (uptime ping) | Every 60 seconds | Proves the device is online; required for reward eligibility |
| Bandwidth used (aggregate, in bytes) | 12.4 GB in 24h | Required for reward calculation and capacity planning |
| Public IP (current) | 203.0.113.42 | Required to enforce the 5-machines-per-IP rule and to attribute abuse |

| | | |
|---|---|---|
| | | complaints |
| CPU / RAM / disk utilisation | 14% / 28% / 32% | Operational health monitoring |
| Workload runtime version | NL-Runtime 1.4.2 | Required for orchestration and security patching |

**4.3 Layer C — Workload traffic.**

For each Workload Session scheduled to an Nx1/Hx1 Home Station, the Company records the following metadata only. The payload content is not retained.

| Field | Example | Why we collect it |
|---|---|---|
| Workload Session ID | WS-2026-05-20-7f3a91 | Allows attribution of any abuse complaint or LE request to a specific Workload Session |
| Workload Publisher ID | PUB-acme-001 | Allows the Company to identify which third-party Publisher is responsible |
| Workload class | compute / storage / connectivity / VPN-relay | Allows risk-tiering and class-specific controls |
| Start timestamp / end timestamp | 2026-05-20 14:00:00 UTC … 14:42:11 UTC | For incident timeline reconstruction |
| Bytes in / bytes out | 218 MB / 304 MB | For Workload metering and Publisher billing |
| Destination endpoints (high-level only) | aggregate per-Workload, e.g. number of distinct destinations contacted | For aggregate abuse-pattern detection — NOT a per-URL log |

**4.4 What the Company expressly does not log in Layer C.**

- The content of any Workload payload (i.e., the bytes inside the session).
- The full URLs, DNS queries, or per-request destinations made by a Workload.
- The personal browsing activity of the Node Operator on their home LAN (the Nx1/Hx1 Home Station is a separate device and does not intercept Node Operator traffic).
- The end-user of any consumer-facing VPN-style service offered to Users (if and when this service launches, it will be governed by a separate Consumer VPN Privacy Notice and is intended to operate on a no-traffic-log basis, with an independent audit to be commissioned once the service exits beta — see Compliance Roadmap).

# 5. Retention windows

| Data | Retention | Trigger for deletion |
|---|---|---|
| Account & KYC data (Layer A) | 5 years | Statutory AML record-keeping period; deleted on the earlier of the 5-year anniversary or User exercise of GDPR Art 17 rights subject to applicable carve-outs |
| Transaction ledger (Layer A) | 5 years | AML record-keeping period |
| **Nx1/Hx1 Home Station heartbeat & telemetry (Layer B)** | 90 days rolling | Automatic deletion at the 90-day mark |
| Workload Session metadata (Layer C, excluding content) | 180 days rolling | Automatic deletion at the 180-day mark |

| | | |
|---|---|---|
| Workload payload content (Layer C content) | Not retained | Discarded in-flight; never written to durable storage |
| Abuse-investigation case files | 24 months from case closure | Required for regulator transparency reporting |

# 6. Independent verification

**6.1 What is independently verified today.**

As of the date of this policy, the no-content-logging position described in Section 4.4 has not been certified by an external auditor. The Company considers this a foundational requirement for the network and has committed, in the public-facing Compliance and Certification Roadmap, to commissioning an independent no-content-logging assurance engagement.

**6.2 Roadmap.**

| Item | Target | Assurance type |
|---|---|---|
| **Independent no-content-logging assurance review of Workload runtime** | 2027 (initial) / annual thereafter | Independent reasonable-assurance engagement by a recognised security audit firm |
| SOC 2 Type I (controls design) | Q2 2027 | Independent CPA firm; AICPA SOC 2 |
| SOC 2 Type II (operating effectiveness) | Q4 2027 / Q1 2028 | Independent CPA firm; AICPA SOC 2 |
| ISO/IEC 27001:2022 certification | Q3 2028 | Accredited certification body |

*These targets are commitments by the Company. They are not statements of present certification. The Compliance and Certification Roadmap document tracks these items publicly.*

# 7. Data subject rights

For Layer A data, the rights described in Section 4 of the Company Privacy and Cookies Policy (GDPR Articles 15–22, and equivalent rights under the California CPRA, the Australian Privacy Principles, and the UK GDPR) apply. The Company will respond to a verified data subject request within 30 calendar days, or 45 days where the request is complex (subject to applicable statutory periods).

For Layer B data, the Node Operator may export their device telemetry from the dashboard.

For Layer C data, the data subject is, in general, the end-user of the Workload Publisher's service. Where a request is made directly to the Company, the Company will redirect the data subject to the responsible Workload Publisher.

# 8. Security of logs at rest

- All retained metadata is encrypted at rest using AES-256-GCM.
- Encryption keys are managed in a hardware security module (HSM) under the control of the Company's infrastructure team. Key access is limited to a documented list of named personnel, dual-control for production.

- Access to log stores is logged (audit log of the audit log).
- Workload payload data, by definition, is never written to durable log storage and therefore is not encrypted at rest by the Company.

## 9. Changes to this policy

Material changes to this policy will be (a) published at the Company legal documentation page, (b) notified by e-mail to all Users, and (c) covered in the next transparency report.

## 10. Contact

Privacy & data subject requests: support@novalink.tech | Security and disclosure: support@novalink.tech