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 If you believe anything here is inaccurate or out of date, please contact support@novalink.tech so we can review it and, where appropriate, correct it.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

Acceptable Use & Network Abuse Policy

Rules of conduct for the Company network, Nx1/Hx1 Home Station devices and Workload Publishers

---

Document ID: NL-AUP-01

Version: 1.1 (revised 10 November 2026)

Status: Issued

Issuing entity: Group-wide policy — adopted by each NovaLink entity listed in the Corporate Structure & Entity Register (NL-ORG-01); administered by Auralink Nova Technology L.L.C (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 and scope

This Acceptable Use Policy and Network Abuse Policy (the "AUP") sets out the conduct rules that govern all use of the Company network, the Nx1/Hx1 Home Station device (the "Nx1/Hx1 Home Station"), the NovaLink Platform, and any third-party workload that is scheduled to run on the Nx1/Hx1 Home Station through the Company infrastructure (each, a "Workload"). The AUP forms part of, and is incorporated by reference into, the Company Terms and Conditions, the Node Operator Agreement, and the agreements the Company concludes with each Workload Publisher.

Capitalised terms used and not defined in this AUP have the meanings given to them in the Company Terms and Conditions.

2. Who this AUP applies to

- Users and Participants of the NovaLink Platform.
- Node Operators (individuals or entities hosting one or more Nx1/Hx1 Home Station devices).
- Workload Publishers (third parties that purchase, license, or otherwise consume compute, storage, or connectivity capacity on the Company network).
- Country Distributors, Country Master Distributors, sponsors, and other commercial counterparties of the Company.

3. Prohibited conduct

3.1 Universally prohibited activities.

The following activities are prohibited under all circumstances on the Company network. The Company reserves the right to take any action set out in Section 7 of this AUP without further notice in respect of any of them.

- Any conduct that is unlawful under (i) the laws of the British Virgin Islands, (ii) the laws of the jurisdiction in which the Nx1/Hx1 Home Station hosting the relevant Workload is located, or (iii) the laws of the jurisdiction in which the User or Workload Publisher is established.
- Child sexual abuse material (CSAM) and any content that sexually exploits a minor, in all forms and at any stage of generation, storage, transmission, or distribution.
- Trafficking in persons, sexual exploitation, forced labour, or modern slavery.
- Terrorism, terrorist financing, the provision of material support to a designated terrorist organisation, or any conduct prohibited by United Nations Security Council resolutions, the BVI Counter-Terrorism Act, the European Union Restrictive Measures regime, the United Kingdom OFSI consolidated list, or the United States Office of Foreign Assets Control (OFAC) regulations.
- Money laundering, structuring, or any conduct prohibited under the BVI Anti-Money Laundering Regulations 2008, the BVI Proceeds of Criminal Conduct Act, the Australian Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), or equivalent legislation in any applicable jurisdiction.
- Distribution, hosting, command-and-control, or staging of malware, ransomware, cryptojacking software, or any code intended to compromise the confidentiality, integrity, or availability of any system.
- Conduct of, or participation in, a Distributed Denial of Service (DDoS) attack, credential-stuffing campaign, brute-force attack, port-scanning of third-party systems without consent, or any other unauthorised intrusion attempt.
- Unsolicited bulk electronic communications ("spam") in violation of CAN-SPAM (United States), the GDPR / ePrivacy Directive (European Union), the UK Privacy and Electronic Communications Regulations 2003, the Australian Spam Act 2003 (Cth), or equivalent legislation.
- Infringement of intellectual property rights, including operating as a streaming-piracy relay, distributing counterfeit media, or facilitating unauthorised peer-to-peer distribution of copyrighted works.

- Operation of unauthorised gambling, unauthorised securities offerings, unauthorised consumer-finance products, or any other regulated activity for which the Workload Publisher does not hold an effective licence in the destination jurisdiction.
- Any activity that violates an applicable sanctions regime, including transactions involving Specially Designated Nationals (SDNs), persons or entities subject to the EU Consolidated List of Sanctions, the UK OFSI Consolidated List, or any UN Security Council Sanctions List.

3.2 Workload-specific restrictions.

The Company classifies Workloads by risk category (see Section 4 of the Node Operator Agreement). Higher-risk classes run in stronger isolation and are enabled by the Company only once their additional controls are in place. The following categories are default-deny on every Nx1/Hx1 Home Station:

- Open residential proxy or exit-node services that route arbitrary third-party traffic through the Nx1/Hx1 Home Station public IP address.
- Anonymising relay services (Tor exit, I2P outproxy).
- Bulk e-mail transmission Workloads.
- Outbound voice or SMS Workloads.

4. Standards expected of Node Operators

Each Node Operator agrees to:

1. Provide accurate registration, KYC, and tax-residency information, and update that information promptly if it changes.
2. Operate the Nx1/Hx1 Home Station in conformity with the Company Hardware Quick-Start guide, including the bandwidth allocation of up to 200 Mbps per device and the 5-machines-per-public-IP rule.
3. Not modify, reverse-engineer, jailbreak, or otherwise tamper with the Nx1/Hx1 Home Station operating system or the Company Workload Runtime.
4. Not deliberately host content or run Workloads in breach of this AUP, and not assist any other person to do so.
5. Promptly report to the Company any Nx1/Hx1 Home Station in respect of which the Node Operator has reason to believe a violation of this AUP is occurring, and cooperate with the Company's investigation.

5. Standards expected of Workload Publishers

Each Workload Publisher contracting with the Company agrees that:

6. It has completed the Company's onboarding due diligence, including the corporate KYB process under Section 5 of the Company Terms and Conditions and the sanctions screening described in the Company Sanctions & OFAC Compliance Policy.
7. It will only submit Workloads classified into the category for which it is approved.
8. It will cryptographically sign each Workload artefact and accept the Company's rejection of any artefact that fails signature verification.

9. It accepts the audit logging set out in the Data Minimisation & Retention Policy, including the assignment of a unique Workload Session ID for traffic attribution.
10. It will respond to the Company abuse notifications within the response timeframes set out in Section 6 of this AUP.
11. It will indemnify the Company and the affected Node Operator(s) in accordance with the Workload Publisher Agreement for any losses, claims, fines, or third-party demands arising from the Workload Publisher's breach of this AUP.

6. Abuse reporting and response

6.1 How to report abuse.

Anyone — including ISPs, hosting providers, copyright holders, regulators, law-enforcement agencies, the Company Users, and members of the public — may submit an abuse report to the Company:

- E-mail: support@novalink.tech (monitored 24/7).
- Postal: Ntech Link Technologies Ltd (Company No. 2195904), British Virgin Islands.

6.2 Information required in an abuse report.

To enable the Company to attribute a report to a specific Workload Session, reporters are asked to include: the source IP address observed, the date and time (with timezone) of the incident, the destination resource, the abusive payload or fingerprint (URL, file hash, message headers, etc.), and the reporter's contact details.

6.3 Response times.

Severity	Examples	Initial response	Mitigation / takedown
Critical	Active DDoS, active CSAM hosting, active terrorist content, malware C2	1 hour	4 hours (and immediate Workload suspension at first reasonable belief)
High	Phishing, fraud relay, account takeover, scanning, repeated copyright complaints	8 hours	24 hours
Medium	Single copyright notice, individual spam complaint, suspected policy violation	1 business day	5 business days
Low	General enquiry, false-positive review, hardening request	3 business days	10 business days

6.4 Provisional measures.

The Company may, prior to the conclusion of any investigation, suspend a Workload Session, quarantine a Workload artefact, throttle traffic from an Nx1/Hx1 Home Station, or temporarily disable an account, where such action is reasonable and proportionate to the suspected breach and to the protection of any affected Node Operator, end-user, or third party.

6.5 Investigation and right of explanation.

Where the action involves a Node Operator account, the Company will, except where prohibited by law (e.g., where doing so would tip off a criminal investigation), notify the Node Operator of the suspected breach, the action taken, and the route to provide an explanation or supporting evidence. The Company will conclude its investigation and either reinstate the account or take final action within a target of fifteen (15) business days.

7. The Company's enforcement remedies

For any breach of this AUP, the Company may, at its sole discretion and without limitation to any other right or remedy available to it:

- Issue a warning.
- Suspend or terminate the relevant Workload Session.
- Suspend or terminate the relevant Node Operator account, in accordance with Section 5 of the Terms and Conditions.
- Disqualify the Node Operator from all reward-generating activity, in accordance with the Risk Disclosure Policy.
- Withhold, claw back, or forfeit accrued but unpaid USDN amounts that are reasonably attributable to the breach.
- Refer the matter to law-enforcement authorities, regulatory authorities, the Node Operator's ISP, or the relevant abuse-response community (e.g., M3AAWG, Spamhaus).
- Pursue any civil claim available to it under the Company Terms and Conditions, the Workload Publisher Agreement, the Node Operator Agreement, or applicable law.

8. Treatment of Node Operators in good standing

Where third-party traffic exiting an Nx1/Hx1 Home Station IP address gives rise to a complaint, the Company will not penalise a Node Operator who is in compliance with this AUP. Specifically, the Company will:

12. Confirm to the complainant (and, where lawful, to the Node Operator) that the traffic originated from a third-party Workload Session attributed to a specific Workload Publisher and not from the Node Operator's personal activity.
13. Where applicable, provide the Workload Session ID, the timestamped attribution, and the contact route to the Workload Publisher.
14. Indemnify the Node Operator on the basis set out in the Node Operator Indemnity Schedule.

9. Changes to this AUP

The Company may amend this AUP from time to time. Any material amendment will be (a) posted on the Company legal documentation page, (b) notified to Users by e-mail or in-platform notice, and (c) where

required by applicable law, made subject to an objection period before taking effect. Continued use of the NovaLink Platform after the effective date of an amendment constitutes acceptance.

10. Governing law and dispute resolution

This AUP is governed by the laws of the British Virgin Islands. Disputes arising out of or in connection with this AUP shall be resolved in accordance with the dispute-resolution clause in the Company Terms and Conditions.

11. Contact

Abuse reports: support@novalink.tech | Legal & policy: support@novalink.tech | General: support@novalink.tech