



Acceptable Use Policy

Rules for the use of Nord Node services and managed systems

Version 1.0 · Effective: 24 September 2026

This document forms part of the Agreement between Nord Node AB and the Customer. It applies where an Order Form has been signed and does not apply to use of Nord Node's website.

1. Purpose

- 1.1** This Acceptable Use Policy ("**AUP**") sets out rules for the use of the Services, Nord Node's systems and the Third-Party Services that Nord Node provides or administers. It forms part of the Agreement. The Customer is responsible for ensuring that its Users comply with it.

2. Prohibited use

- 2.1** The Customer and its Users must not use the Services to:
- (a) break the law, or infringe the rights of others, including intellectual property, privacy and data protection rights;
 - (b) distribute malware, carry out unauthorised access to or scanning of systems, denial-of-service attacks or other attacks, except security testing that Nord Node has agreed to in writing;
 - (c) send unsolicited bulk messages (spam) or engage in phishing or fraud;
 - (d) store or distribute material that is illegal, such as child sexual abuse material or content inciting violence;
 - (e) mine cryptocurrency, or run other activities that place an unreasonable load on shared resources, without Nord Node's agreement;
 - (f) circumvent licence restrictions or security controls, or use licences in breach of the Vendor Terms; or
 - (g) attempt to access other customers' data or Nord Node's systems beyond the access granted.

3. Security obligations

- 3.1** The Customer and its Users must:
- keep passwords and authentication devices confidential, and not share accounts;
 - use multi-factor authentication where Nord Node or the Vendor has enabled it;
 - not disable, block or remove the management and security agents installed by Nord Node without Nord Node's agreement;
 - keep customer portal accounts personal and not share them, and tell Nord Node when a portal user should be removed; and
 - report suspected security incidents, lost or stolen devices, and phishing attempts to Nord Node without undue delay.

4. Consequences of breach

- 4.1 If Nord Node becomes aware of a breach of this AUP, it will notify the Customer and ask the Customer to remedy it. Where necessary to limit harm, Nord Node may take immediate measures, such as blocking an account or isolating a device, in accordance with section 16 of the General Terms. A material or repeated breach is a material breach of the Agreement.
- 4.2 Nord Node may report illegal content or activity to the competent authorities where required or permitted by law.

5. Changes

- 5.1 Nord Node may update this AUP in accordance with section 23.3 of the General Terms.