



NORD
SECURITY

Modern Slavery Statement for financial year 2025

CYBERSPACE B.V.

Introduction

During the reporting period, Nord Security continued to strengthen its efforts to prevent modern slavery and human trafficking across its global operations and supply chain. While the cybersecurity industry is generally considered to present a lower exposure to such risks, we remain committed to conducting business ethically, respecting human rights, and maintaining effective oversight and due diligence processes. This statement outlines the measures implemented to identify, assess, prevent, and mitigate potential modern slavery risks within Nord Security's operations, supply chain, and business relationships.

Reporting entities

This Modern Slavery Statement is made pursuant to section 54(1) of the UK Modern Slavery Act 2015 and section 13 of the Australian Modern Slavery Act 2018. It is published on behalf of CYBERSPACE B.V. and its subsidiaries, including CyberCare, UAB, Nord Security Inc., nordvpn s.a., and Saily Inc. The statement covers the financial year ending December 31, 2025.

CYBERSPACE B.V., as the group holding company, establishes and oversees the group-wide policies, practices, and risk management framework for addressing modern slavery and human trafficking. The principles and actions described in this report apply to all group entities.

Our business

Nord Security provides advanced cybersecurity and privacy solutions to individuals and businesses worldwide. Its portfolio includes NordVPN, a virtual private network service designed to enhance online privacy and security; NordPass, a password management solution; NordLayer, a network access security platform for businesses; NordLayer Browser, a secure enterprise browser; and NordLocker, an encrypted cloud storage solution.

The Nord Security product ecosystem has expanded further to include Saily, a global eSIM service with integrated cybersecurity features; NordStellar, a cyber threat exposure management and threat intelligence platform designed to help organizations identify and respond to external cyber threats; and NordProtect (now Coveron), an identity theft and cyber protection solution. These products reflect our continued focus on innovation and commitment to improving digital security, privacy, and resilience for users globally.

Our operations remain predominantly digital, with almost no manufacturing or physical product distribution. This business model contributes to a relatively low risk of direct involvement in modern slavery or human trafficking within our core operations.

Our supply chain

Nord Security operates a digital-first business model supported by a global network of suppliers, service providers, and business partners. Upstream, we rely on internet infrastructure providers as well as various infrastructure-as-a-service partners, including data centers, server hosting companies, and cloud computing platforms. Downstream, our distribution and promotional efforts involve channel partners, including distributors, resellers, affiliates, and influencers.

Given the international scope of our partnerships, we recognize the importance of maintaining oversight of potential human rights and modern slavery risks across the supply chain and business operations. We continue to assess the supply chain structure and counterparties through ongoing due diligence, screening, and risk management processes designed to support ethical business practices and responsible partner engagement.

Policies and reporting channels

Nord Security maintains a framework of policies, procedures, and internal controls designed to support ethical business conduct, regulatory compliance, and respect for human rights across its operations and business relationships. These measures enable the identification, assessment, prevention, and mitigation of modern slavery and other ethical or compliance-related risks.

Key governance documents include:

Document	How it supports modern slavery prevention
Anti-Bribery and Anti-Corruption Policy	Establishes standards for ethical business conduct and prohibits corrupt or unethical practices that may contribute to human rights abuses
Anti-Money Laundering and Trade Compliance Policy	Supports risk-based screening and monitoring processes designed to identify legal, regulatory, sanctions-related, and adverse media risks, including potential links to modern slavery or human rights violations
Code of Conduct	Defines the ethical principles applicable to employees and contractors, including commitments relating to integrity, compliance, and respect for human rights
Vendor Risk Management Procedure	Establishes due diligence standards for assessing vendors and identifying potential risks related to unethical labor practices, sanctions exposure, adverse media, and other compliance concerns prior to engagement and throughout the business relationship
Third-party Trade Compliance Policy	Defines rules and obligations for partners involved in selling, distributing, or promoting Nord Security products, requiring them to conduct business ethically and responsibly by complying with economic sanctions, export controls, and trade regulations
Intermediary Sales Partners' Risk Management Procedure	Applies risk-based assessment and monitoring measures to intermediary partners and promotes equivalent compliance expectations across downstream business relationships
Business Customers Management Procedure	Establishes customer screening and monitoring processes, including sanctions and adverse media checks, which may help identify potential involvement in modern slavery or human rights violations
Rules on Internal Compliance Procedures	Defines internal responsibilities and escalation processes for identifying, managing, and reporting compliance and ethical risks across the organization

These procedures define onboarding, due diligence, ongoing monitoring, and offboarding workflows for third parties, and contribute to our ability to detect and mitigate potential compliance or human rights risks.

Nord Security also maintains compliance screening and monitoring measures designed to assess relevant counterparties for sanctions-related, regulatory, reputational, and adverse media risks. These processes may assist in identifying indicators associated with labor exploitation, unethical business conduct, or modern slavery-related concerns.

Employees and external partners may report concerns or suspected misconduct through dedicated reporting channels, including mechanisms that allow anonymous reporting where permitted by applicable law. Reports are reviewed and escalated to the appropriate internal functions, including Legal, Risk, Compliance, or People team, depending on the nature of the matter.

Risk assessment, prevention, and mitigation

Nord Security applies a risk-based approach to identifying, assessing, and managing potential exposure to modern slavery and related human rights risks across its operations, supply chain, and business relationships. This includes screening, monitoring, and evaluation of vendors, sales partners, business customers, affiliates, marketing partners, and other counterparties, taking into account factors such as geographic location, nature of services, business model, and overall risk profile.

We maintain due diligence and compliance processes designed to support both ongoing and periodic risk assessments across relevant third-party relationships. These processes are intended to promote consistent application of compliance standards, facilitate risk identification, and support timely escalation where potential concerns are identified.

Our sanctions screening procedures apply to all relevant counterparties and are conducted through automated, rule-based systems. These screenings cover all major international sanctions regimes, and alerts are reviewed by trained compliance professionals.

To support our group-wide AML and trade compliance policies, we maintain internal procedures that govern vendor, customer, and partner onboarding and offboarding. A structured jurisdictional risk list, updated regularly, helps guide decisions in higher-risk scenarios.

While Nord Security has not identified any confirmed instances of modern slavery or human trafficking within its operations or supply chain through its existing compliance and monitoring processes, it recognizes that such risks may evolve over time. Accordingly, we continue to review our controls, due diligence measures, and risk management practices in response to changes in the operational, legal, and geopolitical environment.

Training and working conditions

Nord Security is committed to providing a safe, fair, and respectful work environment for all employees. As of the end of 2025, the company employed people from 73 nationalities, with 566 new team members joining during the year. Anti-discrimination and anti-harassment policies are actively upheld, and employment practices are designed to ensure equal treatment and dignity for all.

Employee education remains a priority. In 2025, 229 internal learning events were organized, with 1,518 unique learners participating in learning and development programs. These included compliance training on topics such as ethics, privacy, and organizational policies. Additional resources, including online courses, mentorship programs, and internal workshops, further support continuous learning.

To support employee well-being, Nord Security offers private health insurance, paid sick leave, access to wellness programs, and a hybrid-work module with the possibility for work from anywhere for a certain period of time. In 2025, 2,863 employees participated in group physical training, and mental health initiatives included coverage for up to 25 psychotherapy sessions per year (in Lithuania only), mindfulness activities, and well-being workshops.

Statement approval

This statement has been approved by the Board of Directors of Nord Security on behalf of CYBERSPACE B.V. for the financial year ending December 31, 2025. It applies to all Nord Security entities and is reviewed periodically.