Nordic Hyperscale Tech AB

Whistleblowing Policy

Anyone who works with Nordic Hyperscale Tech AB can report serious wrongdoing safely, through our channels or directly to an authority, and will not suffer for doing so.

Document control

Item	Detail
Company	Nordic Hyperscale Tech AB, corporate ID no. 559447-6276
Policy owner	Legal Counsel Yurii Orzikh
Approved by	Board of Directors on 2026-09-25 (updated last version 2, earlier adopted 2025-06-31)
Effective from	2026-09-26
Next review	2028-09-26, at least every two years and whenever the law changes
Audience	Employees and every other person listed in section 2, including consultants, suppliers' staff, board members and active shareholders
Published	Nhtech.se
Legal basis	Swedish Whistleblowing Act (2021:890), Ordinance (2021:949), Directive (EU) 2019/1937 and contractual obligations in relation to external parties as customers, service suppliers etc.
Language	English. A Swedish version is in preparation.

1. Purpose and scope

We want concerns raised early, because a problem we hear about is a problem we can fix. This policy explains what you can report, how to report it, what happens next and how you are protected.

The policy implements the Swedish Act on the protection of persons reporting wrongdoing (lag (2021:890) om skydd för personer som rapporterar om missförhållanden, the "Whistleblowing Act") and the EU Whistleblower Directive (EU) 2019/1937. It does not reduce any protection you have under other laws, collective agreements or the Swedish constitutional freedoms of the press and of expression. If this policy and the law ever differ, the law applies.

Our internal channels are for wrongdoing in Nordic Hyperscale Tech AB's own operations. If you learn of wrongdoing at a supplier, customer or partner through your work, you are also protected when you report it through that organisation's channels or to an authority.

2. Who can report and who is protected

You do not have to be an employee. The Act protects anyone who learns of wrongdoing in a work-related context and belongs to one of these groups (chapter 1, section 8):

- employees, on any type of contract
- job applicants and people asking about work
- volunteers and trainees, and people applying to be one
- agency staff, consultants and others working under our control and direction
- self-employed persons seeking or carrying out assignments for us
- members of our board, management or supervisory bodies, and candidates for those roles
- shareholders who are active in the company, or available to be
- former members of any of these groups, for information obtained while active with us

Protection against retaliation also covers the people around you: anyone at Nordic Hyperscale Tech AB who assists you, such as a union representative or safety representative (skyddsombud); colleagues and relatives who work here; and any legal entity you own, work for or are otherwise connected with.

Our internal channels are open to everyone in the list above, including applicants and former staff. Customers and members of the public with no work-related link to us fall outside the Act and can contact contact@nhtech.se instead.

3. What you can report

You can report wrongdoing (missförhållanden) that there is a public interest in bringing to light, and breaches of EU law in the areas the Directive covers, including arrangements designed to defeat the purpose of EU rules (chapter 1, section 2). You do not need proof. You need reasonable grounds to believe the information is true when you report it.

Examples relevant to our business:

- bribery, corruption, fraud, embezzlement or false accounting
- tax evasion or abusive tax arrangements
- price fixing, market sharing or other breaches of competition law
- irregularities in public procurement, public grants or state aid
- breaches of international sanctions or export controls, including supplying equipment, capacity or services to sanctioned parties
- serious weaknesses in the security of our networks and information systems, or concealment of significant incidents under the Swedish Cybersecurity Act (2025:1506)
- unlawful processing or misuse of personal data, including data our customers host with us
- breaches of the EU AI Act, to which the Directive expressly applies (Regulation (EU) 2024/1689, Article 87)
- environmental breaches, such as unlawful emissions, leaks of refrigerants or fluorinated gases, or false reporting of energy and water use

- serious risks to health and safety, including electrical and fire safety at our sites
- money laundering or terrorist financing
- suspected violations of supplier codes of conduct, including unfair or unsafe working conditions, labor rights abuses, or environmentally harmful practices
- deliberate concealment of any of the above

Security-classified information. The Act does not apply to information that is security-classified under the Protective Security Act (2018:585). Contact Yurii Orzikh (yurii.orzikh@nhtech.se) before reporting anything that may fall into that category.

4. How to report internally

You choose the route: internal channel, competent authority, or in limited cases public disclosure. We encourage internal reporting where you feel safe doing so, because it lets us act fastest. You lose no protection by going straight to an authority.

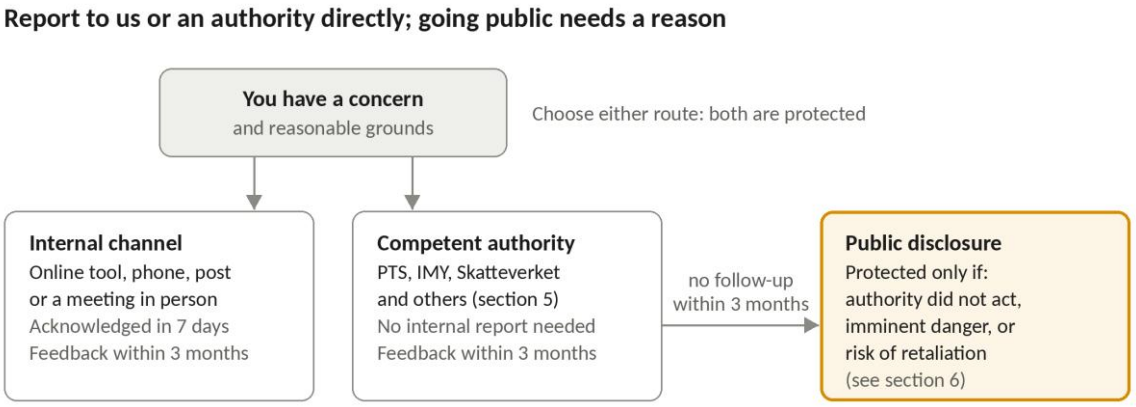


Figure 1. Reporting routes. Public disclosure is protected only in the three cases listed in section 6.

Channel	How to use it	Availability
Online reporting tool	https://visselblasning.trustheart.se/nhtech, operated by Human & Heart AB on our behalf; written report or voice message	24 hours a day; anonymous option
Telephone	+46 (0)8-82 40 00 open 08.00-16.00	00.09-15.00 Mon-Fri
Meeting in person	Ask through any channel; we offer a meeting within 7 days	On request
Post	Nordic Hyperscale Operations AB, Fabriksgatan 8, 702 10 Örebro, envelope marked "Confidential: whistleblowing"	Opened only by case handlers

Reports are received by the case handlers named in section 7, who act independently of line management.

Use these channels to be sure of protection. A report made only to your manager or a colleague is not covered by the Act's protection for internal reporting, unless our channels are missing or do not

meet the legal requirements (chapter 4, section 5). Managers who receive such a report must forward it, unchanged and promptly, to the case handlers and keep it confidential.

What to include. Describe what happened, when and where, who is involved, how you know, and whether anyone else knows. Attach any documents you hold lawfully. Do not investigate on your own: there is no protection for a crime committed to obtain information.

Anonymous reports. You may report anonymously through the online tool and keep in contact with the case handlers there without revealing who you are. We follow up anonymous reports as far as the information allows. If your identity later becomes known, you keep your full protection.

Honest mistakes are protected; deliberate lies are not. If you had reasonable grounds to believe the information was true, you are protected even if it turns out to be wrong. Knowingly false reports are not protected and may lead to disciplinary action.

5. Reporting externally to authorities

You can report directly to a Swedish competent authority through its external reporting channel, without reporting to us first. The authority must acknowledge your report within seven days and give feedback within three months, or six months in special cases.

The Swedish Work Environment Authority (Arbetsmiljöverket) is the special competent authority. It handles reports no other authority covers and publishes the full list of competent authorities with contact details. The authorities most relevant to our business are:

Area	Competent authority
Security of network and information systems; privacy and personal data	Post- och telestyrelsen (PTS); Integritetsskyddsmyndigheten (IMY)
Competition; public procurement	Konkurrensverket
Tax in the areas of EU financial interests and corporate tax	Skatteverket
Fraud against EU financial interests	Ekobrottsmyndigheten
Environmental protection	Naturvårdsverket; the county administrative boards (länsstyrelserna)
Product safety and compliance, including electrical equipment	Elsäkerhetsverket and other sector authorities
International sanctions	Tullverket, Kommerskollegium, Polismyndigheten, Finansinspektionen and others
Anything not covered above	Arbetsmiljöverket

Reports of breaches of EU law can also go to EU institutions, bodies and agencies that run their own reporting channels, such as the European Anti-Fraud Office (OLAF), provided you follow that channel's procedure (chapter 4, section 8).

Reporting to an authority in some other way, for example reporting a crime to the police, is also protected if you first reported internally without adequate follow-up or feedback, if there is an

imminent or manifest danger to life, health, safety or the environment, or if internal reporting would risk retaliation or be ineffective (chapter 4, section 7).

6. Public disclosure and your constitutional freedoms

Making information public, for example through the media or social media, is protected under the Act only if one of these conditions is met (chapter 4, section 9):

1. You reported externally and the authority did not take reasonable follow-up action, or did not give reasonable feedback within three months (six months in special cases, if you were told why).
2. You have reasonable grounds to believe the wrongdoing is an imminent or manifest danger to life, health or safety, or risks extensive damage to the environment, or you otherwise have justified reason to go public.
3. You have reasonable grounds to believe that external reporting would lead to retaliation, or that the wrongdoing would probably not be remedied effectively.

Separately, the Freedom of the Press Act and the Fundamental Law on Freedom of Expression give everyone the right to provide information to the media for publication (meddelarfrihet) and to gather information for that purpose (anskaffarfrihet). The Act does not limit these freedoms. In a private company such as ours, the constitutional bans on tracing sources and on reprisals generally do not apply, which is why the Act's own protection matters.

Nordic Hyperscale Tech AB commits to more than the minimum: we will not try to identify anyone who has used these freedoms or the channels in this policy, and we will not retaliate against them.

7. How we handle your report

You get an acknowledgement within 7 days and feedback within 3 months. Reports are handled by independent case handlers appointed under chapter 5, section 5 of the Act: Human & Heart AB.

1. **Receipt.** Only the case handlers can open the report. An oral report is documented by a recording, with your consent, or by minutes. You may check, correct and sign the transcript or minutes.
2. **Acknowledgement within 7 days**, unless you declined it or it could reveal your identity.
3. **Initial assessment.** The case handlers decide whether the report falls within this policy. If it does not, they tell you and point you to the right route.
4. **Follow-up.** The facts are investigated impartially. A case handler with a conflict of interest steps aside. External experts may assist under a duty of confidentiality. Anyone named in the report is given the chance to respond.
5. **Feedback within 3 months** of the acknowledgement on what has been done and why, as far as confidentiality and the rights of others allow. If no acknowledgement was sent for a reason other than your choice, the 3 months run from 7 days after receipt.
6. **Action and closure.** Findings go to board of directors for decision. Matters may be referred to the police or a supervisory authority.

7. **Deletion.** Reports and documentation are kept only as long as necessary, and never more than two years after the case is closed (chapter 8, section 4).

The case handlers report to the Board at least once a year on the number and types of cases, without information that could identify anyone.

8. Confidentiality and anonymity

Your identity is protected by a statutory duty of confidentiality. Anyone handling a case may not, without authorisation, disclose information that could reveal your identity or that of anyone else named in the case (chapter 9, section 1). A breach may be a criminal offence and will lead to disciplinary action.

We disclose your identity only with your consent or where the law requires it, for example in a police investigation or court proceedings. If that happens, we tell you in advance, unless doing so would undermine the investigation.

People named in a report are also protected. Their identity is kept confidential, they are presumed innocent until the facts are established, and they are given the chance to respond.

9. Protection against hindering and retaliation

Nordic Hyperscale Tech AB will not hinder or try to hinder a report, and will not retaliate because of one (chapter 3, section 1). Retaliation includes, for example, dismissal, demotion, withheld promotion or training, transfer, reduced pay, negative assessments, harassment or exclusion, non-renewal of a contract, and early termination of a consultancy or supplier agreement. The same protection applies if you consult your trade union about reporting.

Freedom from liability. You cannot be held liable for breaching a duty of confidentiality, including a confidentiality clause or non-disclosure agreement, if you had reasonable grounds to believe that reporting the information was necessary to reveal the wrongdoing. This does not give you a right to hand over documents. You are also not liable for breaching rules on obtaining information, if you reasonably believed it was necessary, unless obtaining it was a crime (chapter 2).

Contract terms cannot remove your rights. Any agreement that limits your rights under the Act is void to that extent (chapter 1, section 6). Nothing in our employment contracts, consultancy agreements, supplier terms or NDAs prevents protected reporting.

Remedies. If we breach these prohibitions, we must pay damages for your loss and for the violation of your rights (chapter 3, section 4). Once you show circumstances suggesting retaliation, it is for the company to prove that none occurred. Disputes involving workers and similar groups are heard under the Labour Disputes Act, and the time limits for claims are short, so act promptly and contact your union or a lawyer.

Limits. You are not protected if you lacked reasonable grounds to believe the information was true, or if you committed a crime by reporting or by obtaining the information.

Report retaliation. Use any channel in section 4. Retaliation by any employee is serious misconduct and will lead to disciplinary action.

10. Personal data

Nordic Hyperscale Tech AB is the controller of personal data processed in whistleblowing cases; Human & Hearty HR AB processes data on our behalf under a data processing agreement. We process personal data to comply with our legal obligation under the Act (GDPR Article 6(1)(c)) and only where necessary for a follow-up case (chapter 7, section 3).

- Data that is clearly irrelevant to a report is not collected, and is deleted as soon as possible if collected by mistake.
- Only the case handlers have access, and only to what each of them needs.
- Data may be shared where necessary for action on the findings, for use as evidence in legal proceedings, or where the law requires it.
- Personal data is deleted no later than two years after the case is closed (chapter 7, section 8).

You and anyone named in a report have rights under the GDPR, including access and rectification. These rights may be limited where necessary to protect confidentiality under chapter 9 of the Act. Questions go to our data protection contact at legal.officer@nhtech.se. You may complain to Integritetsskyddsmyndigheten (IMY).

11. Roles, training and review

Role	Responsibility
Board of Directors	Adopts this policy; receives the annual anonymised report; handles reports concerning senior management
CEO	Ensures the case handlers have the resources, independence and access they need
Case handlers	Receive and follow up reports, give feedback, keep records, protect confidentiality
Managers	Forward misdirected reports unchanged and promptly; prevent retaliation; encourage people to speak up
HR	Includes this policy in onboarding and annual training; supports affected employees
Data protection contact	Oversees compliance with section 10
Procurement	Makes this policy known to suppliers and consultants through contract terms and our supplier code of conduct

This policy is the company's written documentation of its internal channels and procedures (chapter 5, section 6). It is published on our intranet and website so that everyone listed in section 2 can find it. The Swedish Work Environment Authority supervises compliance with the rules on internal channels.

The policy owner reviews this policy at least every two years, and after any change in the law or any case that shows a weakness.

Annex A. Contacts

Purpose	Contact
Online reporting tool	https://visselblasning.trustheart.se/nhtech
Whistleblowing telephone line	+46 (0)8-82 40 00 open 08.00-16.00
Postal address for reports	Fabriksgatan 8, 702 10 Örebro, Sweden
Case handlers	Human & Heart AB
Reports concerning senior management	Board of directors
Data protection contact	Legal.officer@nhtech.se
Security protection officer	Yurii.orzikh@nhtech.se
External authorities	The Swedish Work Environment Authority (Arbetsmiljöverket) publishes the list of all competent authorities and their channels on its website