

NET GROUP OÜ

Supplier Code of Conduct*

Responsible supply chain. Trusted technology.
Secure delivery.

This Supplier Code of Conduct sets the minimum legal, ethical, quality, information security, privacy, human rights and sustainability standards expected from suppliers, subcontractors and other business partners working with Net Group OÜ.

PREPARED

22 July 2026

APPLIES TO

All suppliers, subcontractors, consultants, vendors, agencies and other business partners providing goods or services to Net Group or its customers.

MANAGEMENT SYSTEM CONTEXT

Supports Net Group's ISO 9001 certified quality management approach and the implementation of an ISO/IEC 27001-aligned information security management system.

COMPANY DETAILS

A.H. Tammsaare tee 92, Tallinn 13423, Estonia | +372 664 4355 | info@netgroup.com | netgroup.com

CORE EXPECTATION

Suppliers must act lawfully, honestly, securely and responsibly. When a requirement is unclear, the supplier must ask its Net Group contact for guidance before acting, especially where the matter involves customer data, public-sector procurement, security, privacy, human rights or subcontracting.

Supplier requirements at a glance

AREA	MINIMUM EXPECTATION
Legal and ethical conduct	Comply with laws, avoid bribery and conflicts of interest, compete fairly, keep accurate records and follow sanctions/export control restrictions.
Human rights and labour	No forced labour, human trafficking, prohibited child labour, discrimination, harassment or retaliation; provide fair working conditions and grievance channels.
Security and privacy	Protect confidential information, personal data, credentials, systems and customer environments; report incidents without undue delay.

Quality and delivery	Meet agreed specifications, competence, documentation, testing, change control, acceptance and corrective-action requirements.
Sustainability	Use resources responsibly, comply with environmental rules and reduce waste, emissions and negative impacts where relevant.
Subcontractors	Do not use subcontractors for Net Group work without required approval; flow down equivalent obligations and remain responsible for their work.

CONTENTS

- | | | | |
|-----------|--|-----------|---|
| 1 | Introduction, scope and supplier commitment | 2 | Governance, management systems and documentation |
| 3 | Legal compliance and business integrity | 4 | Labour, human rights and respectful treatment |
| 5 | Health, safety and working conditions | 6 | Information security, privacy and secure delivery |
| 7 | Quality, service delivery and customer commitments | 8 | Responsible technology, AI and intellectual property |
| 9 | Environmental responsibility and sustainability | 10 | Subcontractors, supply chain transparency and due diligence |
| 11 | Reporting, audits, corrective actions and consequences | A | Appendix A. Supplier acknowledgement and commitment |
| B | Appendix B. Practical compliance checklist | | |

1 Introduction, scope and supplier commitment

Net Group OÜ relies on suppliers and business partners to help deliver reliable, secure and high-quality digital services. Supplier conduct can affect Net Group, its customers, end users, public trust and the integrity of the solutions we build and operate.

This Supplier Code of Conduct defines the minimum standards expected from every supplier that provides goods or services to Net Group or participates in Net Group customer work. It is intended for procurement, contracting, supplier onboarding, supplier risk management and periodic review.

1.1 Scope and applicability

- This Code applies to suppliers, subcontractors, consultants, independent contractors, agencies, resellers, distributors, technology providers, cloud and hosting providers, software vendors, professional service providers, facility providers and any other third party that provides goods or services to Net Group.
- The Code also applies to a supplier's personnel, temporary workers, agents, subcontractors and any other person contributing to goods or services provided to Net Group.
- When this Code is referenced in a contract, purchase order, statement of work or onboarding pack, it forms part of the supplier relationship.
- The supplier must comply with the stricter requirement if this Code, a contract, customer requirement, project instruction or applicable law sets different standards.
- The supplier remains responsible for all work performed by its subcontractors, agents and personnel.

1.2 Supplier commitment

By accepting a purchase order, contract, statement of work or by signing the acknowledgement at the end of this Code, the supplier commits to:

- **Comply:** follow this Code, applicable laws, contractual obligations and project-specific requirements.
- **Communicate:** make relevant requirements understandable to personnel and approved subcontractors who support Net Group work.
- **Control:** maintain reasonable policies, procedures, training, monitoring and records proportionate to the supplier's role and risk.
- **Report:** promptly notify Net Group of concerns, violations, security incidents, privacy incidents, quality failures or human rights risks that may affect Net Group or its customers.
- **Improve:** cooperate with due diligence, audits, corrective actions and continual improvement activities where required by risk or contract.

1.3 Zero-tolerance conduct

Net Group has zero tolerance for misconduct that creates serious legal, ethical, human rights, security or customer risk. The following conduct may lead to immediate suspension, termination of work, termination of contracts, reporting to authorities or other lawful measures:

- Bribery, kickbacks, extortion, embezzlement, facilitation payments, fraud or intentional misrepresentation.
- Forced labour, modern slavery, human trafficking, debt bondage, forced prison labour or prohibited child labour.
- Discrimination, harassment, violence, threats or retaliation against anyone who raises a concern in good faith.
- Intentional misuse of credentials, access rights, confidential information, personal data, source code or customer environments.
- Knowingly introducing, concealing or exploiting malware, backdoors, unauthorised access mechanisms or security vulnerabilities.
- Serious or intentional breach of sanctions, export controls, public-sector procurement integrity, competition law or data protection obligations.

1.4 Standards that inform this Code

REFERENCE AREA	HOW IT INFORMS SUPPLIER EXPECTATIONS

ISO 9001	Suppliers must support disciplined quality planning, documented requirements, competent delivery, change control, corrective action and continual improvement.
ISO/IEC 27001 implementation	Suppliers that handle information, systems or access must support an information security management approach based on risk, controls, evidence and incident response.
Data protection laws	Suppliers processing personal data must follow GDPR and other applicable privacy and data protection requirements.
ILO, UN and OECD principles	This Code reflects widely recognised expectations on human rights, labour rights, anti-corruption, responsible supply chains and business conduct.

2 Governance, management systems and documentation

Supplier compliance must be managed in practice, not only stated in policy. Suppliers are expected to maintain governance, responsibilities and records that are proportionate to their size, service type, risk and access to Net Group or customer information.

2.1 Supplier governance

- Assign a responsible contact for the supplier relationship and for compliance with this Code.
- Ensure personnel working on Net Group matters understand relevant legal, quality, security, privacy, ethical and customer requirements.
- Maintain appropriate policies, procedures and controls for the goods or services provided.
- Keep records that demonstrate compliance with contractual and legal requirements, including training, approvals, testing, access reviews, incident response and corrective actions where relevant.
- Escalate material risks or changes that may affect service quality, timelines, customer commitments, security, privacy, sanctions, business continuity or compliance.

2.2 Management system expectations

Certification is not required unless stated in a contract or procurement requirement. However, suppliers must be able to demonstrate controls and evidence appropriate to the services they provide. Where relevant, Net Group may request copies of policies, certifications, audit reports, self-assessments, risk assessments, business continuity evidence, insurance certificates or other reasonable assurance materials.

- Quality-related suppliers must support requirements management, acceptance criteria, documentation, delivery control, defect management and corrective action.
- Information, technology, software, cloud, hosting, security or data-processing suppliers must support risk-based information security, access control, incident response and data protection obligations.
- Critical suppliers must maintain business continuity and disaster recovery arrangements appropriate to the service and customer impact.
- Suppliers must notify Net Group before material changes to ownership, subcontracting, key personnel, service location, security posture, certifications or ability to perform agreed obligations where such changes may affect Net Group work.

2.3 Documentation and records

- Records must be accurate, complete, legible, traceable and retained according to legal, contractual and project requirements.
- Time records, invoices, expenses, delivery evidence, project records, test results, approvals and incident records must not be falsified or manipulated.
- Records containing Net Group, customer or personal information must be protected against unauthorised access, alteration, disclosure, loss or misuse.
- Records relevant to an audit, investigation, dispute, security incident or regulatory request must be preserved and not destroyed, altered or concealed.

3 Legal compliance and business integrity

Suppliers must conduct business lawfully, honestly and transparently. Net Group expects suppliers to win and perform work on merit, quality, competence, security and trust.

3.1 Compliance with laws and regulations

- Comply with all applicable laws, regulations, permits, licenses, tax obligations, labour rules, environmental obligations, data protection laws, information security requirements and contractual commitments.
- Do not ask Net Group employees, customers or other suppliers to act unlawfully or outside their authority.
- Promptly notify Net Group if a legal, regulatory, sanctions, export control, licensing or permit issue may affect the supplier's ability to deliver.

3.2 Anti-bribery and anti-corruption

- Do not offer, promise, give, request or accept bribes, kickbacks, facilitation payments, secret commissions or any improper advantage.
- Do not offer gifts, hospitality, travel, employment, donations, sponsorships, discounts or other benefits to improperly influence a business, public-sector, procurement, audit or regulatory decision.
- Interactions with public officials, public-sector customers, state-owned entities and procurement officials must follow all applicable public-sector ethics and procurement rules.
- Use third parties only for legitimate purposes and never to do indirectly what the supplier or Net Group may not do directly.

3.3 Gifts, hospitality and conflicts of interest

- Gifts and hospitality must be modest, occasional, transparent, lawful and connected to a legitimate business purpose.
- Cash, cash equivalents, personal loans and benefits intended to influence a decision are prohibited.
- Disclose actual or potential conflicts of interest, including family or close personal relationships with Net Group personnel, ownership interests, outside employment, side projects or relationships that could affect impartiality.
- Do not use Net Group opportunities, information, assets or customer relationships for unauthorised personal gain.

3.4 Fair competition, sanctions and trade compliance

- Comply with competition and antitrust laws. Do not agree with competitors on prices, bids, margins, market allocation, customer allocation, capacity or other anti-competitive conduct.
- Obtain competitive information lawfully and ethically. Do not misuse confidential information from competitors, customers or former employers.
- Comply with applicable sanctions, export controls, anti-money laundering, anti-boycott and trade restrictions.
- Do not provide goods or services to Net Group using sanctioned parties, prohibited destinations, restricted technology or unlawful payment routes.

3.5 Financial integrity

- Invoices, expenses, time reports, delivery evidence and other business records must be accurate and complete.

- Bill only for authorised work, agreed rates, actual expenses and delivered goods or services.
- Do not conceal quality issues, delivery risks, security incidents, conflicts, sanctions exposure or subcontracting arrangements that could affect Net Group.

4 Labour, human rights and respectful treatment

Suppliers must respect the dignity, rights, privacy and safety of all workers and individuals affected by their operations. This applies to office work, remote work, client sites, production sites, recruitment, labour providers, subcontractors and supply chains.

4.1 No forced labour, human trafficking or modern slavery

- All work must be voluntary. Workers must be free to leave employment or terminate work in accordance with applicable law and contract terms.
- Do not use slavery, servitude, bonded labour, debt bondage, coerced labour, forced prison labour, human trafficking or any similar form of exploitation.
- Workers must not be required to surrender identity documents, pay recruitment fees, lodge unreasonable deposits or accept restrictions that prevent free movement.
- Recruitment agencies, labour brokers and subcontractors must follow the same standards and must not charge workers unlawful or exploitative fees.
- Security personnel, workplace controls and housing arrangements must not be used to intimidate, abuse or unlawfully restrict workers.

4.2 No prohibited child labour

- Child labour is prohibited. The minimum age for employment must comply with applicable law and must not be below the age for completing compulsory schooling or below 15, whichever is higher, unless a lawful and internationally recognised exception applies.
- Workers under 18 must not perform hazardous work, night work or work that may harm health, safety,

morals, education or development.

- If child labour is identified, the supplier must act in the best interests of the child, remove the child from harmful work and cooperate on remediation that supports education and wellbeing.
-

4.3 Fair wages, working time and freedom of association

- Pay at least the statutory minimum wage, provide legally required benefits and comply with overtime, leave and rest-period requirements.
 - Provide workers with clear information about employment terms, wages, deductions, benefits, working time and applicable policies.
 - Do not make punitive wage deductions, withhold wages unlawfully or use wage practices that create coercion or debt bondage.
 - Respect lawful freedom of association, collective bargaining and employee representation. Where such rights are legally restricted, allow lawful alternative channels for worker dialogue.
-

4.4 Non-discrimination, harassment and grievance channels

- Do not discriminate on the basis of gender, age, nationality, ethnic or social origin, language, religion or belief, disability, health status, family status, pregnancy, sexual orientation, gender identity, political opinion or any other protected characteristic.
- Do not tolerate harassment, bullying, intimidation, humiliating conduct, unwanted sexual attention, threats, violence or retaliation.
- Maintain appropriate grievance or reporting channels so workers can raise concerns without fear of retaliation.
- Investigate concerns fairly, protect confidentiality where possible and take corrective action when

misconduct is confirmed.

5 Health, safety and working conditions

Suppliers must provide a safe and healthy working environment and comply with applicable occupational health and safety laws, including requirements for offices, remote work, client sites, travel, warehouses, production locations and equipment handling.

5.1 Occupational health and safety

- Identify health and safety risks and implement appropriate preventive controls, instructions, training and supervision.
- Provide safe equipment, adequate workspace, emergency arrangements, drinking water, sanitary facilities and protective equipment where relevant.
- Report and investigate workplace accidents, near-misses, unsafe conditions and health risks related to Net Group work.
- Do not require excessive working hours or conditions that create avoidable physical or mental fatigue.

5.2 Work at Net Group or customer sites

- Follow all site access, security, safety, confidentiality and conduct requirements at Net Group offices, customer premises, data centres, project locations and events.
 - Ensure supplier personnel have the required competence, authorisation, identification, insurance and equipment before starting work on site.
 - Promptly report injuries, unsafe conditions, security issues or conduct concerns to the relevant site contact and to the supplier's Net Group contact.
-

6 Information security, privacy and secure delivery

Suppliers may receive access to Net Group systems, customer systems, confidential information, source code, credentials, personal data or production environments. Suppliers must protect these assets with security controls appropriate to the risk and must support Net Group's ISO/IEC 27001-aligned information security implementation.

6.1 Confidentiality and information classification

- Use Net Group and customer information only for authorised business purposes and only for the agreed work.
- Protect confidential information, personal data, source code, architecture diagrams, security findings, credentials, commercial information and internal records against unauthorised access, disclosure, alteration, loss and misuse.
- Share information only with authorised personnel who have a legitimate need to know and are bound by appropriate confidentiality obligations.
- Do not discuss confidential information in public places or post it in public, personal or unapproved collaboration tools.

6.2 Access control and secure use of systems

- Access must be based on business need, least privilege, approved roles and project-specific authorisation.
- Passwords, tokens, certificates, private keys, API keys and multi-factor authentication devices must be protected and never shared.
- Access must be removed or adjusted promptly when personnel change roles, leave the supplier, leave a

project or no longer need access.

- Use only approved devices, software, networks, storage locations and collaboration tools for Net Group or customer work unless an exception is approved.
- Do not bypass logging, monitoring, security controls, change control, segregation of duties or customer approval requirements.

6.3 Privacy and personal data

- Process personal data only on documented instructions, for specified purposes and in accordance with applicable data protection laws and contractual data processing terms.
- Apply data minimisation, privacy by design, retention limits and security by design where personal data is involved.
- Do not transfer personal data to another country, vendor, tool, subprocessor or testing environment unless permitted by contract, lawful and appropriately protected.
- Support data subject rights, privacy impact assessments, deletion, return of data and breach notification obligations where required.

6.4 Secure development, cloud and technology services

- Apply secure development, testing, deployment, configuration, change management and vulnerability management practices appropriate to the work.
- Store source code in approved repositories with appropriate access controls, review processes and audit trails.
- Do not hard-code secrets or store credentials in plaintext repositories, tickets, logs, screenshots or chat messages.

- Assess and manage open-source components, third-party libraries, dependencies, licenses, vulnerabilities and end-of-life technologies.
- Do not use production data in development or test environments unless explicitly approved, lawful, minimised and protected.

6.5 Security incidents and vulnerability reporting

- Report suspected security incidents, data breaches, unauthorised access, malware, lost devices, exposed credentials, suspicious emails, critical vulnerabilities and control failures without undue delay and through the agreed channel.
- Where no specific contractual timeframe applies, notify the supplier's Net Group contact as soon as possible and, where feasible, within 24 hours of discovery for material incidents.
- Preserve evidence, cooperate with investigation and remediation, and do not conceal, destroy or alter incident information.
- Do not contact customers, regulators, the media or external parties about a Net Group-related incident unless authorised or legally required.

6.6 Business continuity and resilience

- Maintain continuity and recovery arrangements appropriate to the criticality of the goods or services provided.
- Notify Net Group of outages, disruptions, cyber events, supplier failures or force majeure events that may affect delivery, availability, security or customer commitments.
- Test continuity arrangements where required by contract or risk and provide reasonable evidence upon request.

7 Quality, service delivery and customer commitments

Suppliers contribute to Net Group's ability to deliver reliable services and maintain its ISO 9001 certified quality management approach. Supplier work must meet agreed requirements, be traceable and support continual improvement.

7.1 Requirements and acceptance

- Understand agreed specifications, scope, service levels, acceptance criteria, legal requirements, customer requirements, assumptions and dependencies before starting work.
- Clarify incomplete, inconsistent or risky requirements early. Do not proceed on assumptions that may affect quality, security, privacy, cost or delivery.
- Deliver goods and services that conform to agreed requirements, professional standards and documented acceptance criteria.

7.2 Competence, documentation and delivery discipline

- Assign personnel with appropriate competence, experience, language ability, authorisation and availability for the work.
- Use agreed project management, engineering, testing, release, documentation and quality assurance processes.
- Document decisions, designs, assumptions, risks, approvals, test results, configurations and handover materials where relevant.

- Do not substitute key personnel, locations, tools or subcontractors where this could affect delivery or risk without required approval.
-

7.3 Change control, defects and corrective action

- Changes to scope, design, architecture, configuration, schedule, cost, risk, access or security controls must be assessed, approved and recorded according to the applicable process.
-
- Quality issues, defects, nonconformities and complaints must be logged, prioritised, corrected and analysed for root causes where appropriate.
-
- Suppliers must cooperate in corrective and preventive actions, provide evidence of completion and verify effectiveness where required.
-
- Suppliers must promptly disclose delivery risks, quality failures, security weaknesses or dependencies that could affect Net Group commitments.
-

7.4 Customer and user impact

- Treat Net Group customers, users and stakeholders professionally and respectfully.
-
- Do not make commitments, statements, changes or disclosures to customers on behalf of Net Group unless authorised.
-
- Consider accessibility, usability, maintainability, resilience, privacy, security and sustainability where relevant to the goods or services provided.
-

8 Responsible technology, AI and intellectual property

Suppliers providing software, data, digital services, AI-enabled services, consulting, design, infrastructure, hardware or technical components must use technology responsibly and protect intellectual property and customer information.

8.1 Responsible use of AI and automation

- Use AI tools and automated systems lawfully, securely, transparently and with appropriate human oversight.
- Do not input Net Group confidential information, customer confidential information, personal data, source code, credentials or trade secrets into public AI tools unless the use is expressly approved, lawful and contractually permitted.
- AI-generated code, content, decisions or analysis used for Net Group work must be reviewed by competent personnel before use or delivery.
- Suppliers must consider bias, explainability, security, privacy, intellectual property, data provenance and quality risks when using or delivering AI-enabled solutions.

8.2 Intellectual property and third-party rights

- Respect Net Group, customer, supplier and third-party intellectual property rights, including copyrights, trade secrets, trademarks, patents, designs, databases and know-how.
- Do not use unauthorised software, data, images, models, libraries, fonts, code, datasets or materials in Net Group work.

- Ensure that deliverables do not infringe third-party rights and that licenses are compatible with the intended use.
- Disclose open-source, third-party components, license restrictions and known vulnerabilities where required by contract or good practice.

8.3 Technology ethics and misuse prevention

- Do not develop or provide functionality intended for unlawful surveillance, unauthorised access, deception, discrimination, malware, exploitation or other harmful purposes.
- Report concerns if a requested feature, dataset, integration or deployment could create significant legal, security, privacy, human rights or societal risk.
- Do not bypass access controls, licensing restrictions, security testing rules, customer approvals or regulatory requirements for convenience or speed.

9 Environmental responsibility and sustainability

Net Group expects suppliers to comply with environmental laws and to reduce negative environmental impacts in a practical, risk-based manner. This is relevant to office services, hardware, electronics, facilities, data centres, cloud services, travel, logistics and waste management.

9.1 Environmental compliance and resource use

- Comply with applicable environmental laws, permits, licenses and reporting obligations.
- Use energy, water, materials, packaging, office resources and transport responsibly and avoid unnecessary waste.
- Handle, store, transport, label and dispose of chemicals, batteries, electronic equipment and hazardous materials safely and lawfully.
- Dispose of electronic waste, hardware, media and equipment through responsible and lawful channels, including secure data erasure where relevant.

9.2 Climate, emissions and efficient digital delivery

- Monitor and reduce energy use, greenhouse gas emissions, air emissions, wastewater, waste and resource consumption where relevant to operations and service delivery.
 - Support lower-impact travel, remote collaboration and efficient logistics where practical and consistent with business needs.
-

- For cloud, hosting or infrastructure services, consider energy efficiency, resilience, capacity management, data retention and efficient architecture.
 - For hardware and electronics, support responsible sourcing, durability, repairability, secure reuse, recycling and lawful disposal.
-

9.3 Conflict minerals and responsible sourcing

Where suppliers provide hardware, electronics or materials that may contain tin, tungsten, tantalum, gold, cobalt or other higher-risk minerals, the supplier should maintain reasonable due diligence processes consistent with responsible sourcing expectations and provide evidence upon request.

10 Subcontractors, supply chain transparency and due diligence

Net Group must understand who contributes to its work and where material risks arise. Suppliers must manage their own supply chains responsibly and must not create hidden legal, quality, security, privacy, human rights or continuity risks.

10.1 Subcontracting and flow-down obligations

- Do not subcontract Net Group work, customer work, regulated processing or sensitive services unless the contract permits it or Net Group has provided required approval.
- Flow down equivalent obligations on quality, security, privacy, confidentiality, human rights, anti-corruption, environmental responsibility and audit cooperation to approved subcontractors.
- Remain fully responsible for the acts, omissions, quality, security and compliance of subcontractors and agents.
- Maintain a current list of approved subcontractors and subprocessors used for Net Group work where required by contract or data protection terms.

10.2 Due diligence and supply chain risk

- Identify and manage risks in the supplier's own operations and supply chain, including corruption, sanctions, human rights, labour, environmental, data protection, information security and continuity risks.
- Provide reasonable due diligence information when requested, including ownership, certifications, policies, security questionnaires, data locations, subprocessors, audit reports or corrective action evidence.

- Inform Net Group promptly of actual or suspected violations, material risks, adverse media, investigations, sanctions exposure or supply chain disruptions that could affect Net Group.
-

10.3 Higher-risk suppliers and services

Net Group may apply enhanced due diligence for suppliers that handle sensitive data, operate critical services, access production environments, support public-sector customers, process personal data, operate in higher-risk jurisdictions, use labour providers, provide hardware or have significant subcontracting chains.

11 Reporting, audits, corrective actions and consequences

Early reporting helps prevent harm and allows issues to be corrected before they become serious. A concern does not need to be proven before it is reported. Suppliers must not retaliate against anyone who raises a concern in good faith.

11.1 What suppliers must report

- Actual or suspected violations of this Code, law, contract requirements, customer requirements or internal supplier policies that may affect Net Group.
- Bribery, fraud, conflicts of interest, unfair competition, procurement integrity issues, sanctions exposure or financial irregularities.
- Security incidents, privacy incidents, data breaches, exposed credentials, lost devices, malware, unauthorised access or suspicious system activity.
- Quality nonconformities, critical defects, delivery failures, business continuity events or major customer-impacting risks.
- Modern slavery, forced labour, child labour, discrimination, harassment, retaliation, unsafe working conditions or environmental concerns.

11.2 Reporting channels

- Report concerns to the supplier's regular Net Group business contact unless a contract, project instruction or incident response plan specifies another channel.
-

- Security and privacy incidents must be reported through the designated security, privacy or incident-response channel for the relevant project or customer environment. If no channel is specified, notify the supplier's Net Group contact and info@netgroup.com without undue delay.
- General supplier conduct concerns may be reported to the Net Group business contact or through info@netgroup.com unless a specific contractual reporting channel applies.
- If the concern involves the regular business contact, the supplier should escalate to another Net Group management, procurement, quality, security or legal contact known to the supplier.

11.3 Audit, monitoring and evidence

- Net Group may assess supplier compliance through due diligence, questionnaires, policy reviews, certifications, management reviews, audits, customer requirements, incident reviews and performance monitoring.
- Where required by contract, law, customer requirement or risk assessment, suppliers must cooperate with reasonable audits or reviews during normal business hours and subject to appropriate confidentiality safeguards.
- Suppliers may object to an audit measure where it would violate mandatory law, data protection rules or confidentiality obligations, but must cooperate to find a reasonable alternative assurance method.
- Suppliers must provide timely, accurate and complete information and must not mislead Net Group or conceal material risks.

11.4 Corrective actions and consequences

- If a violation or risk is identified, the supplier must cooperate with Net Group to create and implement a corrective action plan with clear responsibilities, deadlines and evidence of completion.
- Corrective actions may include training, process changes, access removal, technical fixes, remediation for

affected people, supplier changes, monitoring, independent assurance or contract amendments.

- Serious, repeated or unremediated violations may lead to suspension of work, removal of personnel, withholding of acceptance, termination of contracts, claims for damages, reporting to authorities or other lawful measures.
-
- Net Group may suspend onboarding, system access, data sharing, payments for disputed work or new purchase orders while material risks are assessed or remediated, subject to applicable contract and law.
-

11.5 Non-retaliation and cooperation

- Suppliers must not retaliate against workers, subcontractors or other persons who raise concerns in good faith or cooperate with investigations.
-
- Retaliation may include dismissal, demotion, threats, bullying, exclusion, loss of opportunities, contract penalties or other negative treatment because a concern was raised.
-
- Suppliers must cooperate honestly with investigations, preserve relevant information and avoid interference with evidence or witnesses.
-

A Supplier acknowledgement and commitment

This acknowledgement may be signed as a standalone confirmation or attached to a contract, purchase order, supplier onboarding pack or statement of work. It does not replace stricter contractual obligations.

SUPPLIER COMMITMENT STATEMENT

The supplier confirms that it has received, read and understood the Net Group OÜ Supplier Code of Conduct. The supplier commits to comply with the Code, applicable laws, contracts and relevant Net Group requirements; to communicate equivalent standards to relevant personnel and approved subcontractors; and to cooperate with reasonable due diligence, audits and corrective actions.

SUPPLIER LEGAL NAME

REGISTRATION NUMBER

REGISTERED ADDRESS

REPRESENTATIVE NAME

REPRESENTATIVE TITLE

EMAIL / TELEPHONE

SIGNATURE

DATE

NET GROUP CONTRACT / PO REFERENCE

Authorised signature confirms acceptance on behalf of the supplier organisation, unless otherwise specified in the applicable contract.

B Practical compliance checklist

Suppliers can use this checklist before starting Net Group work, before onboarding personnel or subcontractors, and before accessing Net Group or customer information.

- | | |
|---|---|
| 1 | Have we received and understood the current contract, statement of work, project instructions and this Code? |
| 2 | Have we assigned a responsible contact for quality, security, privacy, delivery and supplier compliance? |
| 3 | Do all personnel working on Net Group matters have the required competence, confidentiality obligations and training? |
| 4 | Have all subcontractors, subprocessors and tools been approved where approval is required? |
| 5 | Are access rights limited to authorised personnel and protected by appropriate authentication controls? |
| 6 | Do we know what information is confidential or personal data, where it may be stored, and how it must be protected? |
| 7 | Do we have a process for reporting security, privacy, quality, human rights, legal or ethical concerns without undue delay? |
| | |

- 8 Are deliverables, testing, approvals, changes and corrective actions documented and traceable?
- 9 Are invoices, expenses, time records and delivery evidence accurate and supported?
- 10 Have we reviewed whether any planned AI tool, open-source component, data transfer, subcontractor or country/location creates additional risk?

ESCALATION RULE

Do not ignore a concern because it seems small. Small issues in quality, security, privacy, human rights or ethics can become significant if not addressed early.