



FINEOS Supplier Code of Conduct

Introduction

FINEOS is committed to conducting business with the highest standards of integrity, ethics, and sustainability. This Supplier Code of Conduct outlines our expectations for all direct suppliers who provide contracted products and services to FINEOS. We expect our direct suppliers to adhere to these principles, but do not require them to ensure compliance throughout their own supply chain.

Please note: While FINEOS favours suppliers who comply with this Code of Conduct, adherence is not a mandatory requirement currently. Suppliers are encouraged to adhere to this Code of Conduct.

This Code aligns with best practice in sustainability reporting such as the Corporate Sustainability Reporting Directive (CSRD) and the EU Omnibus Directive amendments, focusing proportionately on direct suppliers as prescribed by these regulations.

Ethical Business Practices:

- Conduct business with integrity, transparency, and in compliance with all applicable laws and regulations.
- Prohibit all forms of corruption, bribery, extortion, and embezzlement. Suppliers must not offer or accept bribes or other improper advantages.
- Engage in fair business practices, including accurate and truthful advertising, and comply with competition and antitrust laws, where applicable.
- Disclose any potential conflicts of interest to FINEOS and avoid situations that may compromise business decisions.
- Protect confidential information and comply with relevant data protection and privacy laws
- Implement ethical AI practices where artificial intelligence technologies are used in products or services supplied to FINEOS, with particular attention to risk classification system established for AI.

Legal Compliance:

- Comply with all applicable laws, regulations, and standards in the countries where they operate.
- Adhere to international trade regulations, including import/export controls and sanctions.
- Respect intellectual property rights and safeguard FINEOS's proprietary information, where applicable
- Comply with applicable sustainability disclosure regulations relevant to supplier's jurisdiction and size.

Social Responsibility:

- Respect human rights and prohibit any form of harassment, discrimination, or abuse in employment practices.
- Ensure fair labour practices, including appropriate working hours, fair wages, and freedom of association, where applicable.
- Provide a safe and healthy working environment for all employees, where applicable.
- Promote diversity, equity, and inclusion in the workplace, where applicable

- Address social impacts of digital products and services, including digital inclusion and accessibility.

Environmental Stewardship:

- Operate in an environmentally responsible manner and comply with environmental laws and regulations.
- Strive to reduce consumption of energy, water, and other resources, where applicable.
- Minimise waste generation and promote recycling and proper disposal, where applicable.
- Work towards reducing greenhouse gas emissions and supporting climate action
- For software and digital service providers: Consider and optimise the energy consumption of applications and services.
- Implement measurement and reporting of carbon emissions aligned with the Greenhouse Gas Protocol and CDP reporting framework.

Information Security:

- Maintain appropriate information security controls to protect FINEOS and customer confidential data and information.
- Implement reasonable technical and organisational measures to prevent unauthorised access, disclosure, or loss of confidential information.
- Report any security incidents that may impact FINEOS data or systems promptly, with suppliers committing to notification within 24 hours of discovery.
- Comply with relevant information security standards and practices appropriate to the supplier's industry and the nature of services provided.
- Ensure staff are trained on basic information security practices relevant to their role
- For software providers: Follow secure coding practices and maintain secure software development lifecycles.
- Conduct regular security testing and vulnerability assessments for software and other digital products and services.
- Maintain appropriate software supply chain security controls and third-party dependency management processes.
- Provide software bills of materials (SBOMs) upon request to facilitate transparency in software components.
- Implement vulnerability management processes with clear timelines for addressing identified security issues based on severity.

Monitoring and Compliance:

- Self-declare compliance with this Code through a simplified process proportionate to their size and maturity.
- Provide a mechanism for employees to report concerns without fear of retaliation.
- Strive for continuous improvement in sustainability performance
- Engage transparently with FINEOS on sustainability matters.