QRIS Materials Intelligence

Suppliers Code of Conduct

May 2026

Summary

1. Introduction

ORIS Materials Intelligence is committed to creating value for all its stakeholders through sustainable and responsible business practices. As a technology company providing innovative solutions for sustainable infrastructure, our principles of responsible development - transparency, data integrity, environmental stewardship, and respect for human rights - are integral to our business strategy.

Our approach to responsible business and ethics extends to the way we work with our service providers and technology partners. Our selection of suppliers at ORIS is based on the standards and principles enshrined in the UN Global Compact's Ten Principles, which guide our commitments to human rights, labor standards, environmental responsibility, and anti-corruption.

As a technology company, ORIS is committed to identifying, preventing, and managing risks pertaining to data privacy and security, AI ethics, cybersecurity, environmental impact of digital services, social responsibility, human rights, business ethics, and legal compliance throughout our ecosystem. This is fully part of our procurement process.

2. Our expectations from service providers

ORIS is committed to meeting high standards in data security, privacy, environmental responsibility, human rights, and business ethics. We expect our service providers to do likewise.

2.1 Data Privacy & Information Security

Service providers must ensure that personal data about individuals is collected, stored, used, processed, or shared in accordance with all applicable data privacy laws, including GDPR. Providers must implement appropriate technical and organizational measures to protect data, including encryption, access controls, and secure data transmission protocols.

Service providers must properly use personal data only per ORIS' instructions and safeguard it from accidental or unlawful destruction, loss, alteration, or unauthorized disclosure.

Service providers must maintain strict confidentiality of all ORIS proprietary information, client data, and intellectual property. This includes technical specifications, business processes, infrastructure data, and any sensitive information accessed during service delivery.

2.2 Cybersecurity & Systems Resilience

Service providers, particularly those providing cloud infrastructure, SaaS platforms, or IT services, should demonstrate compliance with the highest security standards including through ISO 27001, SOC 2 Type 2, or equivalent certifications.

Providers must have documented cybersecurity policies and procedures in place, including incident response plans, vulnerability management, and regular security assessments appropriate to the services they provide.

In the event of a security incident or data breach, providers must immediately notify ORIS and cooperate fully in investigation and remediation efforts.

2.3 AI Ethics & Responsible Technology

For service providers developing or deploying AI systems for ORIS, adherence to ethical AI principles is expected. These principles include transparency in AI system functioning, fairness through mitigation of biases in datasets and algorithms, accountability for AI outcomes, protection of individual privacy, and security against adversarial attacks.

Providers should disclose system limitations and potential risks, ensure AI decisions can be explained and validated where appropriate, and maintain human oversight of automated processes.

2.4 Working Conditions & Labor Rights

Service providers must apply fair and decent working conditions, labor standards, and welfare practices, implementing local and national laws in compensating and providing contracts for all employees and contractors. Workers shall be paid at least the minimum wage stipulated by national law and benefit from social security schemes according to national legal standards. Service providers shall respect working time in accordance with applicable standards and ensure employees have appropriate rest periods and work-life balance.

Employment-related decisions must be based on relevant and objective criteria. Service providers shall make no distinctions on grounds including, but not limited to: age, disability, gender, sexual orientation, political or other opinion, ethnic, indigenous or social origin, or religion.
Workers shall not be subject to discrimination, harassment, or termination in retaliation for exercising employee rights or reporting concerns.

Service providers shall not use forced labor, child labor, or any form of modern slavery. Providers shall not use labor provided involuntarily under threat of penalty, including human trafficking, debt bondage, or withholding of identification documents.

2.5 Environmental Responsibility

We expect service providers shall respect and comply with environmental regulatory requirements applicable to their operations and support a precautionary approach to environmental challenges.
For technology service providers, this includes measurement and consideration of the environmental impact of digital services such as energy efficiency of data centers and cloud infrastructure, use of renewable energy sources for hosting and computing where feasible, and responsible e-waste management and equipment lifecycle practices.

Service providers with significant environmental impact are also encouraged to establish objectives and targets to reduce such impacts.

2.6 Business Ethics & Compliance

Service providers shall comply with all applicable anti-corruption laws and regulations and maintain a zero-tolerance policy towards any form of bribery, corruption, extortion, and embezzlement.
Service providers shall not pay bribes or make any other inducement (including kickbacks, facilitation payments, excessive gifts and hospitality) in relation to their business dealings with clients, partners, public officials, or any other stakeholder. All business dealings must be performed transparently and accurately reflected in business books and records.

Service providers shall comply with all applicable competition laws. Providers shall not engage in anti-competitive practices, price fixing, market allocation, bid rigging, or abuse of market position. Providers must take necessary precautions to avoid disclosure of commercially sensitive information about ORIS to third parties.

Service providers must respect intellectual property rights, including software licenses, patents, trademarks, and copyrights. Providers must only use properly licensed software and must not infringe on third-party IP rights in work performed for ORIS.

Service providers must disclose any actual or potential conflicts of interest that may affect their ability to perform services objectively and in ORIS' best interests.

Service providers shall comply with all applicable trade and economic sanctions rules and regulations, including export controls.

3. Terms of engagement

This Code of Conduct applies to all ORIS service providers and technology partners, and is communicated during the procurement process.

3.1 Verification & Assessment

ORIS may verify compliance with the standards described in this document through appropriate means, which may include review of certifications (such as ISO 27001, SOC 2, GDPR compliance

documentation), self-assessment questionnaires on data privacy, cybersecurity, and business ethics, and verification of adherence to applicable laws and regulations.

The extent of verification will be proportionate to the nature of services provided and the associated risks.

3.2 Support & Corrective Action

When a service provider does not meet ORIS' requirements, corrective action plans may be established within a specified timeframe depending on the severity of the issue, and ORIS will monitor progress.
ORIS may support service providers in developing their capabilities and improving their performance in areas critical to our partnership.

3. 3 Enforcement

ORIS may immediately terminate relationships with service providers that breach zero-tolerance requirements (such as data breaches due to negligence, corruption, forced labor, or child labor) and/or providers refuse to remediate such identified issues.

4. Our commitments to service providers and partners

ORIS seeks to engage in long-term relationships with service providers that are committed to sustainable and ethical technology practices. Our goal is to partner with providers to deliver valuable services for our clients while demonstrating responsible digital ecosystem management.

4.1 Business Conduct

When carrying out procurement duties and responsibilities, all ORIS employees who interact with service providers are expected to demonstrate the company's commitments to high legal, ethical, and moral standards.

Our internal Code of Business Conduct sets norms of behavior in the areas of, conflict of interest, anti-corruption, competition law, data protection, and confidential information. ORIS employees are encouraged to continually consider issues linked to ethical behavior.

4.2 Grievance Mechanism

ORIS offers an independent whistleblower channel for employees and external stakeholders, including service providers, to raise questions and concerns about ORIS' business practices. We respect the right of all workers to speak up and raise grievances without fear of retaliation. It is accessible here.

5. Responsibilities and reviews

This Code of Conduct has been approved by the company's management team. It was developed by the company's ESG lead. Changes are proposed on a regular basis and when needed by the CFO, CTO and ESG lead. Employees are also encouraged to report concerns and suggest changes. All changes are communicated to the team and partners through website publication.

This code has entered into force since June 01, 2026

Nicolas Miravalls

P.O Président

Rachel Aoust

CRO