Advice RegTech

Supplier Code of Conduct

Version 26.01
Last updated 26/01/2026

Table of Contents

Advice RegTech Supplier Code of Conduct

1. Purpose

This Supplier Code of Conduct (Code) sets out the standards that key suppliers, vendors, contractors, and third parties (Suppliers), are expected to meet when providing goods or services to Advice RegTech (the Company). This Code supports the Company's information security obligations under ISO/IEC 27001, contractual client requirements under CPS 234 and CPS 230, applicable Australian laws, and includes ESG, Modern Slavery, and human rights obligations.

Compliance with this Code is a condition of engagement and forms part of the Company's supplier due diligence, onboarding, and ongoing monitoring processes.

2. Scope

This Code applies to Suppliers of the Company, Advice RegTech, that:

- Access the Company's information, systems, or facilities;
- Process or store Company or client data; or
- Provide goods or services that may impact the Company's operational, legal, security, or reputational risk profile.

Suppliers are responsible for ensuring their employees, contractors, and sub-suppliers comply with this Code.

3. Governance and Accountability

- Maintain appropriate governance structures, policies, and controls relevant to the services provided;
- Assign clear responsibility for information security, privacy, ESG, and ethical compliance;
- Cooperate with the Company's reasonable assurance, audit, and information requests.

4. Organisational Security Policies and Procedures

Maintain documented, implemented, and regularly reviewed policies and procedures covering:

- Information security management;
- Acceptable use of systems and data;
- Access control and identity management;
- Information classification and handling;
- Records management and retention;
- Secure development and change management (where applicable).

Policies must be aligned with recognised standards such as ISO/IEC 27001 or equivalent frameworks.

5. Data Protection and Privacy

- Comply with all applicable privacy and data protection laws, including the Australian Privacy Act 1988 (Cth) and any contractual data protection obligations;

- Process personal information only for authorised purposes;
- Implement appropriate technical and organisational measures to protect data against unauthorised access, loss, or disclosure;
- Notify the Company promptly of any actual or suspected data breach affecting Company or client data.

6. Network and Infrastructure Security

Implement security controls proportionate to risk, including:

- Secure network architecture and segmentation;
- Protection against malware, unauthorised access, and denial-of-service attacks; secure configuration and hardening of systems;
- Monitoring and logging of security-relevant events;
- Physical security controls to prevent unauthorised access to facilities, systems, and assets.

7. Vulnerability and Patch Management

- Maintain a vulnerability management program to identify, assess, and remediate security vulnerabilities;
- Apply security patches within reasonable timeframes based on risk;
- Conduct regular testing (e.g. vulnerability scanning, penetration testing) where appropriate;
- Manage technology assets to ensure supported, maintained, and secure configurations.
- Maintain a vulnerability management program to identify, assess, and remediate security vulnerabilities.

8. Incident Management

- Maintain documented incident response procedures;
- Detect, respond to, and contain security and operational incidents promptly;
- Notify the Company without undue delay of incidents that may impact the Company or its clients;
- Support investigation, remediation, and post-incident review activities.

9. Business Continuity and Disaster Recovery

- Maintain business continuity and disaster recovery plans appropriate to the criticality of the services provided;
- Identify and test recovery objectives (RTOs and RPOs) where relevant;
- Ensure continuity arrangements include cyber incidents, system failures, and key personnel risks.

10. Compliance and Legal Obligations

- Comply with all applicable laws, regulations, and industry standards;
- Not engage in bribery, corruption, fraud, or anti-competitive conduct;
- Maintain accurate records relevant to services provided to the Company.

11. Third-Party and Subcontractor Management

- Conduct due diligence on subcontractors that may impact the Company;
- Flow down relevant obligations from this Code to sub-suppliers;

- Remain responsible for the acts and omissions of subcontractors.

12. Competence, Training, and Awareness

- Ensure personnel have appropriate qualifications, skills, and experience;
- Provide regular training relevant to information security, privacy, and ethical conduct;
- Restrict access to Company information to authorised and trained personnel only.

13. Environmental, Social and Governance (ESG) Expectations

13.1 Environmental Responsibility

- Identify and manage environmental risks associated with their operations;
- Comply with applicable environmental laws and regulations;
- Take reasonable steps to reduce environmental impact, including energy use, emissions, waste, and water consumption;
- Support sustainable sourcing and responsible resource use.

13.2 Social Responsibility

Operate in a socially responsible manner, including:

- Providing safe and healthy working conditions;
- Respecting diversity, inclusion, and equal opportunity;
- Prohibiting harassment, bullying, and discrimination.

13.3 Governance and Ethics

- Act with integrity and transparency;
- Maintain policies addressing conflicts of interest, whistleblowing, and ethical conduct;
- Maintain appropriate insurance coverage and financial resilience commensurate with the services provided;
- Cooperate with audits or assessments relating to ESG and ethical risks.

13.4 Responsible Use of Emerging Technologies

Where suppliers use artificial intelligence or other emerging technologies in providing services, it is expected that they:

- Use such technologies responsibly, lawfully, and transparently;
- Manage risks relating to bias, security, and misuse;
- Not deploy emerging technologies in a manner that would expose the Company or its clients to undue legal, regulatory, or ethical risk.

14. Labour Practices

- Comply with all applicable labour and employment laws;
- Pay wages and benefits that meet or exceed legal minimums;
- Respect lawful working hours and leave entitlements;
- Have worker grievance mechanisms;
- Prohibit child labour and ensure age verification processes are in place;

- Respect freedom of association and lawful collective bargaining.

15. Modern Slavery

- Comply with applicable modern slavery and anti-human trafficking laws, including the Modern Slavery Act;
- Take reasonable steps to identify, assess, and address modern slavery risks within their operations and supply chains, noting countries of operation and sourcing risks;
- Not use forced, bonded, or involuntary labour child labour;
- Maintain processes to enable reporting and remediation of modern slavery risks.

16. Human Rights

- Respect internationally recognised human rights, including those set out in the UN Guiding Principles on Business and Human Rights;
- Avoid causing, contributing to, or being directly linked to human rights abuses;
- Implement processes to identify, prevent, and mitigate human rights impacts;
- Provide accessible grievance mechanisms for workers.

17. Monitoring, Assurance, and Audit

The Company may:

- Request information, certifications, or evidence of compliance;
- Conduct risk-based supplier assessments or audits;
- Require remediation of identified issues within agreed timeframes.

18. Reporting and Escalation

Suppliers must promptly report:

- Security incidents, data breaches, or material control failures;
- Actual or suspected breaches of this Code;
- Significant ESG, modern slavery, or human rights issues.

19. Non-Compliance

Failure to comply with this Code may result in:

- Remediation requirements;
- Suspension of access or services;
- Termination of the supplier relationship;
- Reporting to regulators or clients where required.

20. Acknowledgement

Suppliers may be required to formally acknowledge compliance with this Code and confirm ongoing adherence. Otherwise the Company must perform due diligence assessments on Suppliers to ensure they meet this Code.

Acknowledgement - Supplier Code of Conduct

This Supplier Code of Conduct (Code) sets out the standards of ethical behaviour, legal compliance, information security, privacy, and responsible business practices expected of key suppliers, contractors, consultants, and service providers (Suppliers) that provide goods or services to Advice RegTech Pty Ltd.

As a technology provider to regulated financial services organisations, Advice RegTech relies on its Suppliers to operate responsibly, protect confidential information, and support the delivery of secure and reliable services to its clients.

By signing this acknowledgement, the Supplier confirms that it has read, understood, and agrees to comply with the Code, and will take reasonable steps to ensure that its employees, contractors, and sub-suppliers involved in providing services to Advice RegTech comply with the Code's requirements. This attestation forms part of the commercial arrangements between the Supplier and Advice RegTech Pty Ltd. The Supplier acknowledges that Advice RegTech Pty Ltd may rely on this attestation when assessing Supplier compliance, risk, and ongoing suitability.

Supplier details

Supplier Legal Name	
ABN	
Registered Address	
Primary Contact Name & Title	
Email / Phone	
Services Provided	

Authorised signatory

The individual signing below warrants that they are authorised to provide this acknowledgement on behalf of the Supplier.

Name	
Title	
Signature	
Date	