



Supplier Code of Conduct

This Code reflects SBS Bank's expectations for managing supplier relationships in a prudent, customer-focused and risk-aware manner. Suppliers are expected to support SBS's operational resilience, customer outcomes, information protection and regulatory obligations throughout the lifecycle of the relationship.

Purpose

SBS Bank expects suppliers to support safe, fair, and resilient outcomes by operating with integrity, meeting their obligations, protecting information, and managing the risks they introduce through their services. This Code sets out the minimum standards expected of suppliers, contractors, consultants, service providers, and subcontractors who provide goods or services to SBS Bank. Suppliers are expected to communicate these requirements to relevant employees, contractors, and subcontractors.

1. Application and core expectations

- This Code applies to all suppliers engaged by SBS Bank or providing services on SBS Bank's behalf. Compliance with this Code may be assessed through onboarding, due diligence, contract management, supplier reviews, assurance activity, and incident reporting.

2. Ethical business conduct

- Conduct all SBS-related activities honestly, transparently and fairly, in line with SBS's conduct and risk expectations when dealing with SBS, customers, employees, regulators and other stakeholders.
- Prohibit bribery, corruption, fraud, facilitation payments, money laundering, tax evasion facilitation, and any other improper business practice.

- Maintain accurate records and provide complete, accurate and timely information when requested by SBS.
- Disclose actual, potential, or perceived conflicts of interest promptly and manage them in accordance with SBS requirements.
- Ensure gifts, hospitality or entertainment offered to SBS personnel are reasonable, transparent, infrequent, and never intended to improperly influence a decision.
- Maintain avenues for employees and contractors to raise concerns and protect individuals who report concerns in good faith.

3. People, health, safety, and human rights

- Maintain employment and supply-chain practices that protect worker wellbeing and legal rights, prevent exploitative, coercive or unsafe working conditions, and provide a workplace free from unlawful discrimination, harassment, bullying and victimisation.
- Comply with employment, immigration, wage, leave and workplace health and safety obligations.
- Prohibit child labour, forced labour, human trafficking, modern slavery, and any form of coercive or exploitative labour practice.
- Respect lawful rights to freedom of association and collective bargaining.
- Take reasonable steps to identify and address human rights risks in the supplier's own operations and supply chain.
- Maintain safe systems of work and promptly notify SBS of health and safety issues that may affect SBS sites, people, customers, or services.

4. Customer conduct and service standards

- Support SBS's commitment to fair customer outcomes and act with appropriate care, diligence and skill when providing services connected to SBS customers.
- Ensure customer communications and service activities undertaken on behalf of SBS are clear, accurate, timely and not misleading.
- Escalate complaints, adverse customer impacts, misconduct, service failures, operational incidents, or potential regulatory issues promptly through agreed SBS channels.
- Ensure employees and contractors performing SBS-related services have appropriate capability, training, and supervision.
- Avoid sales, incentive or performance practices that could encourage poor customer outcomes or inappropriate conduct.

5. Information security, privacy, and confidentiality

- Protect SBS information, customer information, systems, assets, credentials and confidential material from unauthorised access, use, disclosure, alteration, loss, or destruction.
- Apply security controls appropriate to the service and risk, including least privilege access, secure authentication, encryption for sensitive data, logging, monitoring, and vulnerability management.
- Use multi-factor authentication for privileged, remote, or high-risk access where relevant to the service.
- Ensure access to SBS data or systems is limited to authorised personnel with a genuine business need and removed promptly when no longer required.
- Notify SBS promptly of any actual or suspected information security, cyber, privacy or data incident, and cooperate with containment, investigation, notification, and remediation activity.
- Comply with data handling, retention, disposal, return, and destruction requirements notified by SBS or set out in the relevant contract.
- Do not transfer SBS data offshore, engage subcontractors or materially change hosting, processing, or support arrangements without required contractual approval.

6. Artificial intelligence and emerging technology

- Use artificial intelligence, generative AI, automated decisioning or emerging technology responsibly, ethically, lawfully, and only within the scope authorised by SBS.
- Do not input SBS confidential information, customer information, personal information, credentials, source code, or commercially sensitive material into public or unauthorised AI tools.
- Maintain governance over AI models, tools, datasets, prompts, outputs, and third-party dependencies used in connection with SBS services.
- Assess and manage AI risks before deployment, including privacy, security, accuracy, bias, explainability, intellectual property, resilience, and customer outcome risks.
- Clearly identify AI-generated content or AI-supported processes where this is relevant to SBS, customers, assurance, decision-making or record keeping.
- Ensure AI outputs used for SBS services are reviewed by appropriately skilled people and are not relied on without reasonable validation.
- Notify SBS of any significant AI-related incident, model failure, data leakage, unauthorised use, regulatory concern, or material change in AI functionality affecting SBS services.

7. Resilience, subcontracting, and continuity

- Maintain appropriate operational resilience, business continuity, disaster recovery, and incident response arrangements for services provided to SBS.
- Notify SBS of material service disruptions, control failures, security issues, financial concerns, or changes that may affect service delivery.
- Obtain required approval before using subcontractors for SBS-related services and remain accountable for subcontractor performance, conduct, security, and compliance.
- Manage critical dependencies, including fourth parties, in a way that protects SBS data, customers, services and regulatory obligations.
- Cooperate with SBS exit planning, transition assistance, data return or deletion and service continuity requirements.

8. Environmental and community responsibility

- Manage environmental impacts in proportion to the goods or services provided, comply with applicable laws and standards, and take practical steps to reduce waste, resource use and emissions where feasible.
- Take reasonable steps to reduce waste, emissions, resource use, and other environmental impacts where practicable.
- Consider climate, sustainability, and community impacts in the delivery of goods and services to SBS.
- Support responsible procurement outcomes, including fair treatment of subcontractors and positive contribution to local communities where appropriate.

9. Monitoring, assurance, and consequences

- Suppliers must maintain evidence of compliance with this Code and provide it to SBS on request.
- SBS may assess supplier compliance through onboarding checks, questionnaires, audits, certifications, access reviews, control attestations, incident reviews, and supplier performance meetings.
- Suppliers must promptly remediate issues identified by SBS and keep SBS informed of progress until closure.
- Failure to comply with this Code may result in corrective action, enhanced monitoring, suspension of activity, removal from approved supplier arrangements, termination of contract or other rights available to SBS.

10. Raising Concerns and Whistleblowing

- SBS expects suppliers to promote a "speak up" culture and maintain effective whistleblowing arrangements. Suppliers must not tolerate retaliation against any person who raises a concern or participates in an investigation in good faith.
- Suppliers must take reasonable steps to protect the confidentiality and anonymity of whistleblowers and ensure that concerns relating to misconduct, fraud, corruption, adverse customer impacts, regulatory breaches, information security, privacy, or other serious wrongdoing are appropriately investigated and remediated.
- Any material concern affecting SBS must be escalated immediately by emailing protecteddisclosure@sbsbank.co.nz