



Responsible AI Practices

Risk-Based Governance	AI systems are assessed before operational use and governed according to their intended purpose, the data involved, their level of autonomy, potential impact, and applicable legal or regulatory considerations. Governance measures are designed to be proportionate to the level of risk.
Human Oversight	Appropriate human oversight is incorporated throughout the AI lifecycle. AI is designed to support people and decision-making, with review and escalation mechanisms available where appropriate.
Privacy and Responsible Data Use	Where AI involves personal data, privacy considerations are integrated into its design and use. Data is managed with regard to lawfulness, relevance, quality, accuracy, purpose limitation, data minimization, and appropriate safeguards based on its nature and sensitivity.
Security and Resilience	AI capabilities are supported by security and resilience measures appropriate to their purpose and risk profile. These may include access controls, encryption, monitoring, testing, logging, and mechanisms designed to support reliable and secure operation.
Fairness and Responsible Outcomes	AI systems are evaluated from the perspective of fairness and potential bias. Appropriate testing, review, and monitoring help identify and reduce the risk of unintended or discriminatory outcomes while supporting responsible and ethical use.
Transparency, Accountability, and Traceability	AI initiatives have defined ownership and appropriate governance documentation. Information relating to intended use, limitations, governance, and accountability is maintained to support oversight, transparency, and traceability. Information for users is provided where appropriate.
Lifecycle Monitoring and	AI systems are reviewed throughout their lifecycle and may be reassessed when functionality, data use, intended purpose, performance, or the legal and regulatory environment changes. Processes are in place to identify, assess, investigate, and manage AI-



Incident Management	related incidents, coordinated where appropriate with existing security, privacy, compliance, and risk management processes.
 AI Literacy and Responsible Partnerships	Employees receive guidance and training on the responsible use of AI, while AI suppliers and technology partners are subject to governance and due diligence processes appropriate to the nature of their services. Responsible AI expectations relating to security, privacy, transparency, and governance form part of these relationships.
 Validation and Quality Assurance	AI-generated outputs are subject to appropriate human review before they are relied upon for significant business purposes. Reviews may consider factors such as accuracy, reliability, fairness, intellectual property, and relevant legal or regulatory considerations.
 Trust and Responsible Innovation	AI is developed, integrated and used to support secure, transparent, and trusted payment and commerce experiences. Innovation is pursued within appropriate ethical, legal, privacy, security, and governance boundaries, with consideration given to the potential impact on customers, merchants, partners, shoppers, employees, and other stakeholders.