Information Security Policy Statement

American Express Saudi Arabia (AESA), a leader in financial services and payment solutions, prioritizes the protection of all its information assets, ensuring the security and trust of its customers and stakeholders. Recognizing the ever-evolving nature of information security, AESA's Board and Management demonstrably commit to safeguarding the confidentiality, integrity, and availability of all physical and electronic information.

AESA strategically aligns its information security requirements with its evolving goals and objectives, ensuring security plays a vital role in achieving its business aspirations. Additionally, AESA demonstrates its dedication to legal and ethical operations by adhering to all applicable laws and regulations.

To build a robust and compliant information security framework, AESA has adopted ISO/IEC 27001:2022, SAMA Cybersecurity Framework, National Cybersecurity Authority and PCI DSS 3.2.1 frameworks. These frameworks serves as a foundation for identifying, assessing, and mitigating information security risks, guaranteeing comprehensive protection for all information assets.

Recognizing that information security is a continuous process, AESA actively strives for improvement by regularly reviewing its risk assessments, implementing new security controls, conducting internal audits, and providing employee training. This commitment to continuous improvement ensures that AESA's information security posture remains agile and responsive, effectively addressing the evolving threat landscape.

Through this comprehensive and evolving information security program, AESA fosters a secure environment that safeguards its customers, partners, and employees, paving the way for continued success and prosperity in the Kingdom.

Glossary

- Information system - Includes all servers and clients, network infrastructure, system, and applications.
- Confidentiality – characteristic of the information by which it is available only to authorized persons or systems.
- Integrity – characteristic of the information by which it changed only by authorized persons or system in an allowed way
- Availability – characteristic of the information by which it is available to authorized persons or systems whenever it is needed.
- Information security - preservation of confidentiality, integrity, and availability of information