SwiftTech

Speed, Flexibility, Success

Information Security Policy

Updated by: LUNA DAHAL

Date: 11/13/2025

I. Information Security Policy Statement

SwiftTech is recognizes that information security is paramount for our customers and the success of our business. As such, SwiftTech is committed to implementing security controls and practices that serve to protect our customer's information and align with SwifTech's overall business goals and appetite for risk.

II. Policy Updates

This policy will be updated at least annually or as changes to SwiftTech's architecture, security controls, or risk posture dictates.

III. Statement on Compliance

In order to establish security control baselines, appropriate for SwiftTech's, its size, risk posture, and overall business goals, SwiftTech relies on a number of compliance and control frameworks and best practice standards. While SwiftTech may choose not to implement every control or best practice as presented, SwiftTech has considered frameworks such as:

1. NIST Cybersecurity Framework (CSF) + CIS Critical Security Controls (CIS Controls)

Focus: Identify → Protect → Detect → Respond → Recover + Technical controls and best practices to defend against common attacks.

2. NIST Risk Management Framework (RMF) + FAIR (Factor Analysis of Information Risk)

Focus: Structured risk management with quantitative analysis of business impact.

And/or

3. COBIT (Control Objectives for Information and Related Technologies)

Focus: Governance and alignment of IT, security, and business objectives.

3. Information Security Risk Management

In order to further establish control appropriateness, SwiftTech has created a cybersecurity risk management practice to identify risks and weigh the appropriateness of best practice controls. Risk assessments are completed at least annually and may be updated as changes to SwiftTech's architecture demands.

Controls

IV. Data Storage

SwiftTech shall, at a minimum store customer data using **AES-256** encryption.

V. End User Management

Access to SwiftTech systems will be carefully controlled. Every user will have only the permissions they truly need no more, no less. Strong passwords and multi-factor authentication will be required, and unusual activity will be monitored to unauthorized or suspicious behavior.

VI. Network Controls

SwiftTech shall implement network segmentation, intrusion detection/prevention systems (IDS/IPS), and firewall protections to prevent and mitigate unauthorized access. Network traffic shall be continuously monitored, and remote connections shall be secured through VPN and multi-factor authentication (MFA).

VII. Incident Response and Recovery

SwiftTech shall maintain an Incident Response Plan to identify, contain, and mitigate security incidents. Post-incident reviews shall be conducted to improve security measures and ensure timely recovery of critical systems.

VIII. Continuous Monitoring and Improvement

SwiftTech shall engage in continuous monitoring of security controls and perform regular risk assessments. Findings shall inform updates to policies, configurations, and controls to ensure ongoing alignment with evolving threats and compliance standards.

IX. Patching and Vulnerability Management

SwiftTech shall maintain a proactive patching and vulnerability management program to keep systems secure and up to date. Security updates, patches, and configuration changes will be applied in a timely manner based on risk and criticality. Vulnerabilities will be regularly scanned, prioritized, and remediated, and the process will be documented to ensure accountability and continuous improvement.