SwiftTech

Speed, Flexibility, Success

Information Security Policy

Updated by: Sarah Althowebi

Date: 6 / 8 /2021

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 Security Framework.

2. Vendor Risk Management.

And/or

3. Operational Risk Management.

IV. 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

V. Data Storage

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

Database shall be encrypted in production environment .

VI. End User Management

SwiftTech shall implement Multi Factor Authentication to access VPN

SwiftTech shall implement these password polices :

Password length shall be at least 8 character long by alert the users with message that password should be at least 8 character long.

Password period shall be changed every 90 days by scheduled time that would detect password changes that occur outside of the 90 day period. .

VII. Network Controls

SwiftTech shall keep the network secure by updating TLS 1.1 certificate to TLS 1.2 instead. And Application tiers should be segmented from Business Application Servers.

VIII. Patching and Vulnerability Management.

SwiftTech shall implement patch management its control to keep up to date.

It's shall include Scan for vulnerability.

IX. Code Scanning.

SwiftTech shall do code scanning to fix problems before production.