

*SwiftTech*

*Speed, Flexibility, Success*

**Information Security Policy**

**Updated by: \_\_\_NALAN DOGANCI\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date: \_\_\_\_27/03/2024\_\_\_\_\_\_\_\_**

1. **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.

1. **Policy Updates**

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

1. **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 Risk Management Framework**

**2. NIST Cybersecurity Framework**

And/or

**3. Health Insurance Portability and Accountability Act (HIPAA)**

1. **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**

1. **Data Storage**

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

**SwiftTech must implement encryption at rest for sensitive data.**

1. **End User Management**

SwiftTech internal network users must create strong passwords with at least 12 characters, including a mix of uppercase, lowercase, digits, and special characters. Passwords cannot be reused, and users must change them every 90 days. Additionally, Multi-Factor Authentication (MFA) is required for VPN access.

1. **Network Controls**

SwiftTech must upgrade to TLS 1.2 or higher for enhanced security. To improve security, SwiftTech must logically segregate its Application Development Tiers from Business Application Servers using network segmentation such as VLANs or subnets.

1. **Patching and Vulnerability Management**

SwiftTech must be ensure that Development Tier servers are up-to-date with patches and free from vulnerabilities.

1. **Secure Software Development**

Prior to deployment in the production environment, SwiftTech must conduct vulnerability scans on the application.