

*SwiftTech*

*Speed, Flexibility, Success*

**Information Security Policy**

**Updated by: Ziyad Almutairi**

**Date: 8/12/2022**

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. CIS Critical Security Controls

3. HIPAA

4. NCSC CAF

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.

1. **End User Management**

Enforce password policy for Length to be at least 12 characters and Age to be 90 days. Also Requiring MFA in order to access VPN.

1. **Network Controls**

Using TLS 1.2 or higher instead of TLS 1.1 which has security issues

1. **Patching and Vulnerability Management**

Apply logical separation between Application development Tiers and Business Application servers to reduce the risk of impacting current services.

1. **Secure Software Development**

Before pushing any Application code to the production environment, it must be scanned and tested.