

*SwiftTech*

*Speed, Flexibility, Success*

**Information Security Policy**

**Updated by: Kareem El sabbagh**

**Date: 29 November 2021**

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. Health Insurance Probability and Accountability Act (HIPAA)

2. NIST Cybersecurity Framework (National Institute of Standards and Technology)

And/or

3. 14 Cloud Security Principles / UK Govcloud

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

Databases in production environment must be encrypted

1. **End User Management**

minimum requirements for password acceptance to be at least 12 characters containing capitalized and special characters.

Multi Factor Authentication (MFA) for login must be established to increase a security layer and prevent unwanted visitors.

The number of failed logins must be low to prevent brute force attack.

The password needs to be updated every 2 months.

1. **Network Controls**

we must upgrade the TLS from version (1.1) to (1.2) and it is also so important to decouple the app development tier and the server 0f the business app

Application development Tiers and Business Application servers need to be decoupled

1. **Vulnerability and patch management**

Repair the vulnerabilities of the server to fix the bugs and enhance it with new features after the releasing of the new patches

1. **Code scanning**

Identify potential security issues within the code before sending it to the production cycle