

*SwiftTech*

*Speed, Flexibility, Success*

**Information Security Policy**

**Updated by: MOHAMAD ALMADANI**

**Date: 11/04/2022**

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 Security Framework

2. HIPPA

And/or

3. Vendor Risk Management

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**
2. **Password Policy: must be complex with at least 8 characters including capital letters, small letter, numbers and special characters with set duration for 60 or 90 days.**
3. **Apply Multifactor Authentication for login.**
4. **Reduce the number of attempts login.**
5. **Network Controls**
6. **Using TLS V1.2 instead of TLS V1.1**
7. **Install next generation firewall NGFW to enhance network security and protection.**
8. **Patching And Updating Management.**

**All servers must be patched and updated to avoid unwanted vulnerabilities.**

1. **Secure Production Environment.**

**All codes must be scanned while they in are in testing environment before applying them to the production environment.**