

*SwiftTech*

*Speed, Flexibility, Success*

**Information Security Policy**

**Updated by: Wiam Almokhtar**

**Date: 06-01-2023**

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 Portability and Accountability Act (HIPAA)

2. National Cybersecurity Centre - Cyber Assessment Framework (NCSC – CAF)

And/or

3. Centre of Internet Security (CIS)

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**

* Password length must be at least 12-character long
* Password must contain uppercase, lowercase, digit, and a special character
* MFA must be used for authentication

1. **Network Controls**

TLS v1.1 must be replaced by TLS v1.2 or a higher

1. **Patching and Vulnerability Management**

a plan for regular server patching and updating must be established

1. **Secure Software Development**

Penetration testing must be performed on developed software