

*SwiftTech*

*Speed, Flexibility, Success*

**Information Security Policy**

**Updated by: Mohamed AbdelGawad**

**Date: 30/11/2022**

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. The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF).

2. Factor Analysis of Information Risk (FAIR).

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. VPC3 File storage must supports at minimum AES-256 encryption.
2. Databases in production environment must be unencrypted.
3. Internal Network users must use a minimum of 8-character password.
4. VPN access must use MFA.
5. Minimum version of TLS v1.2 must be used between the cloud production environment and SwiftTech’s physical location.
6. Application development Tiers must be logically segmented from Business Application servers.
7. Development Tier servers must be continuously patched and free of any known vulnerabilities.
8. Application code must be scanned for vulnerabilities before being published into production environment.
9. **Data Storage**

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

1. **End User Management**
2. **Network Controls**
3. **Etc.**
4. **Etc.**