

*SwiftTech*

*Speed, Flexibility, Success*

**Information Security Policy**

**Updated by: Abdullah Alshalan**

**Date: 01/08/2021**

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 quarterly or as changes to SwiftTech’s architecture, security controls, or risk posture dictates.

1. **Statement on Compliance**

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

2. SP 800

And/or

3. 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. **Data Storage**

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

1. **End User Management**

* SwiftTech shall, at a minimum require Internal Network users 8-character password
* SwiftTech shall, at a minimum make the Passwords expires after 48 days
* SwiftTech shall, at a minimum make VPN access require MFA

1. **Network Controls**

* SwiftTech shall, at a minimum use TLS v1.2 it’s used between the cloud production environment and SwiftTech’s physical location
* SwiftTech shall, at a minimum make Application development Tiers are logically segmented from Business Application servers

1. **Patching and Vulnerability Management**

* SwiftTech shall, at a minimum make Development Tier servers are patched and not contain vulnerabilities

1. **Secure Software Development**

* SwiftTech shall, at a minimum make Application code scanned for vulnerabilities before being published into production environment
* SwiftTech shall ensure that all application code is tested and free of security flaws that would create risk greater than a rating of “low”. Any security flaws that are risk rated as “High” (or equivalent) or “Medium” (or equivalent) using a standard, recognized risk rating mechanism must be remediated prior to the code being deployed to production environments.