

*SwiftTech*

*Speed, Flexibility, Success*

**Information Security Policy**

**Updated by: Hyunbyung, Park**

**Date: 2021-08-30**

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 SwiftTech’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. HIPAA (The US Health Insurance Portability and Accountability Act) security standards

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

And

3. NCSC (National Cyber Security Center) Cloud Security Guidance

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**
2. SwiftTech shall, at a minimum store customer data using AES-256 encryption.
3. SwiftTech shall encrypt the database in production environment
4. **End User Management**
5. SwiftTech must require at least 8-characters password for Internal Network users
6. SwiftTech shall not expire the password unless there is evidence of compromise of the authenticator
7. SwiftTech shall require MFA(Multi-Factor Authentication) for VPN access
8. **Network Controls**
9. SwiftTech shall use TLS version 1.2 or above to connect between the cloud production environment and SwiftTech’s physical location
10. SwiftTech shall logically segment Application development Tiers from Business Application servers
11. **Patching and Vulnerability Management**
12. SwiftTech shall patch and manage vulnerabilities of servers
13. **Secure Software Development**
14. SwiftTech shall use software assurance tools and scan application code before being published into production environment