

*SwiftTech*

*Speed, Flexibility, Success*

**Information Security Policy**

**Updated by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Date: \_\_\_\_\_\_\_\_\_\_\_\_**

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 800 53r5

2. HIPAA Privacy Rule & HIPAA Security Rule

And/or

3. ISO/IEC 27000 Series

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 Internal Network users require Passwords need to contain a mixture of lowercase, uppercase, numbers and special characters.**
2. **Network Controls TLS v1.2 or higher is used between the cloud production environment and SwiftTech’s physical location**
3. **Etc.** **Patching and Vulnerability Management Development Tier servers must be patched and contain NO vulnerabilities.**
4. **Etc.** **Secure Software Development Application code must be scanned for vulnerabilities before being published into production environment**