**SwiftTech**

***Speed, Flexibility, Success***

# Information Security Policy

**Updated by: Simone Canty**

**Date: April 13, 2022**

# I. 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.

# II. Policy Updates

This policy will be updated at least annually or as changes to SwiftTech's architecture, security controls, or risk posture dictates.

# III. 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 Secure Software Development Framework (NIST SP 800-128)

2. Health Insurance Portability and Accountability Act Security Rule (HIPAA) (NIST SP 800-66) and NIST SP 800-63 B

And/or

3. Security Guidelines for Storage Infrastructure (NIST Special Publication 800-29) and Storage Security: Data Protection (SNIA Technical White Paper 2018)

# IV. 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

# V. Data Storage

SwiftTech shall, at a minimum store customer data using AES-256 encryption. AES-256 is the strongest advance encryption system (AES) to use due to the number of rounds. The more rounds, the more complex and difficult to cause a brute force attack.

# VI. End User Management

SwiftTech shall ensure that internal network users will require not only a password but will incorporate a combination of two or more of the following options:

- Token
- Personal Identity Verification (PIV) card
- Fingerprint

SwiftTech shall, ensure that end users will have passwords at least 8 characters in length.

## VII. Network Controls

SwiftTech will have the Application Development tiers segmented from the Business Application servers to eliminate the potential risk of attackers or vulnerabilities affecting the network system.

## VIII. Secure Software Development

SwiftTech will use Code Analysis Tools and Security Analysis tools to assure that software development is secure.

## IX. Vulnerability and Patch Management

SwiftTech will use Patch Management for the centralized management of the detection, download, installation, and reporting of patches. This process will be automated on a weekly basis and will be used to mitigate vulnerabilities. To verify that the patch management is working, reports will be generated weekly to determine if the patches are installed correctly and if there are any failed patch installations.