

*SwiftTech*

*Speed, Flexibility, Success*

**Information Security Policy**

**Updated by: SIMRANJIT SINGH**

**Date: 04/07/2023**

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. SOC II

2. NIST RMF + FAIR

And

3. HIPAA

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-128 encryption. Company backups must be taken twice a week.

1. **End User Management**

User must use password of atleast 14 characters or more and password shall expire after every 120 days. User must use Laptops provided by IT department and should use bio-metric/OTP for MFA purpose along with VPN to establish connection.

1. **Network Controls**

TLS used for Data in Transit should be either TLS v1.2 or higher for cloud production environment. Logical segmentation must be followed using 3-tier architecture

1. **Patching and Vulnerability Management**

All network devices must have a device management program that handles patching and upgradation of Software’s to initiate a patch installation every 2nd Thursday of each month.

1. **Secure Software Development**

Every Code shall be scanned automatically using antivirus to stop malicious activity before uploading to Production Environment