



**Information Security Policy**

**Updated by: \_\_LATHIKA D\_\_**

**Date: \_\_\_\_\_6 August 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. NIST
2. HIPAA

And/or

1. SOC 2
2. **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**

Users must maintain a strong password of at least a length of 8 which must include a combination of characters, numbers and symbols. The password should expire after a particular time, it should be constantly changed in order to secure the user and their info.

1. **Network Controls**

NCSC's recommends to use TLS only v 1.2 or higher. As of now, the most secure version of TLS is 1.3

1. **Patching and Vulnerability Management**

The servers need to be checked for vulnerabilities and then they should be patched accordingly.

1. **Secure Software Development**

The application code must be scanned for any vulnerability before it is published to the market for users to use that application. Cross scripting could be reduced if the application code is scanned properly for vulnerabilities.