

*SwiftTech*

*Speed, Flexibility, Success*

**Information Security Policy**

**Updated by: Lama Alhaza**

**Date: 09/01/2023**

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 CSRC
2. CIS Controls to Reduce Risk
3. ISO 27001 & ISO 27002
4. HIPAA Security Rule
5. **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**
   1. The following steps will be Implemented to improve password security: -
      1. Only a mix of letters, numbers, and special characters passwords will be allowed.
      2. Passwords will have a 120-day expiration date.
      3. Passwords shall have more than 12 characters.
2. **Network Controls**
   1. An intrusion prevention system (IPS) will be installed in the network to prevent brute force and denial of service.
   2. To improve security postures, security gateways, proxies, and firewalls will be used within the network.
3. **Data Protection**
   1. Data will be encrypted whenever it’s being transferred or stored.
   2. Data will be accessible only by authorized individuals.
4. **Malware Defense**
   1. To prevent malware from being executed, a real time Anti-Virus on each endpoint will be installed.
   2. Security awareness and training shall be conducted on a regular basis.