

*SwiftTech*

*Speed, Flexibility, Success*

**Information Security Policy**

**Updated by: Nawaf AlMazyad**

**Date: 2/1/2024**

I. **Information Security Policy Statement** SwiftTech acknowledges 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 will protect our customer’s information and align with SwifTech’s overall business goals and appetite for risk.

II. **Policy Updates** This policy shall be updated at least annually or as changes to SwiftTech’s architecture, security controls, or risk posture dictate.

III. **Statement on Compliance** To establish security control baselines appropriate for SwiftTech’s size, risk posture, and overall business goals, SwiftTech shall rely on a number of compliance and control frameworks and best practice standards. While SwiftTech will not implement every control or best practice as presented, SwiftTech shall consider frameworks such as:

1. NIST Security Framework
2. Vendor Risk Management (And/or)
3. Operational Risk Management

IV. **Information Security Risk Management** 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 shall be completed at least annually and may be updated as changes to SwiftTech’s architecture demand.

**Controls**

V. **Data Storage** SwiftTech shall, at a minimum, store customer data using AES-256 encryption.

VI. **End User Management** Password length – The password shall be at least 8 characters long.

VII. **Network Controls** TLS 1.2 shall be used instead of TLS 1.1. Application Development tier and Business Application server shall be decoupled.

VIII. **Patching and Vulnerability Management** Servers shall be patched.

IX. **Secure Software Development** Code that will be sent to production shall be scanned.

**Explanation for Risk Management Scenarios:** SwiftTech will utilize the NIST Security Framework, Vendor Risk Management, and Operational Risk Management frameworks to establish security control baselines. While not implementing every control, SwiftTech shall consider these frameworks based on its size, risk posture, and overall business goals.

In the risk management practice, SwiftTech shall conduct annual risk assessments to identify and evaluate risks. These assessments shall be updated as changes to SwiftTech’s architecture demand, ensuring ongoing alignment with the organization's risk appetite and goals.