

*SwiftTech*

*Speed, Flexibility, Success*

**Information Security Policy**

**Updated by: Prashant Kumar**

**Date: 21/07/2020**

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. The customer can choose from our different plans which will be notified by our sales management team.

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 Cybersecurity framework**, which is divided into three main parts which are – Core, Profile and Tiers. Which basically uses a five-step method to identify and handle cybersecurity challenges. First to Detect the problem, then to create a Response to that problem, then to Recover the system, then to Identify similar threats, and finally to Protect the system from any type of threat.

2. **COSO framework**, which is the second option for this project, has five main factors upon which the system runs. Control Environment, Risk Assessment, control Activities, Information and Communication, and Monitoring. These five main factors can be divided into 17 principles by which the whole framework operates.

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 – 256 encryptions. The cloud database will be provided by SwiftTech and an annual subscription fees will be charges to the company. The access to the cloud will be limited as per agreement. A team will be provided by SwiftTech that will look after the security of the cloud system.

1. **End User Management**

SwiftTech provides an advanced password management system to provide the most secure environment for data. The password management software will help the user to choose suitable high strength passwords which are longer than 6 characters and include a uppercase letter, number and a symbol.

SwiftTech helps its user to create a secure network for internal use and cloud-based services. We suggest our customers to avoid doing transactions and important works through the public network. We always make sure that our customer gets a secure connection using VPN control.

SwiftTech advises the companies to use only genuine and licensed software, as our team observed earlier that some users use pirated and cracked software, which can affect our security system as the pirated software contains malware. SwiftTech also suggested keeping important data in the cloud as it is more secure than the system hard drive.

1. **Network Controls**

SwiftTech offers its customers free training because by educating the employees, most of the cyber attacks can be stopped. In the training session, the employees will learn about different types of network systems and different possible and common ways they are hacked. By this education, the employees will be able to differentiate between a malicious internet link and how to save themselves from being a victim.

SwiftTech also recommends the customers to use strong passwords in the network access points. Backup your data in different places. Encryption is a must.

1. **Vulnerability and Patch Management**

SwiftTech found that unpatched flaws continue to be a major security issue for many organizations. Organizations under growing pressure are advised to imply vulnerability and patch management. The key practices of patch management are – Making an inventory, classify your own system, fast patching process, creating a test environment, regular patching, scanning and auditing vulnerabilities regularly, automation, and reporting. Through these processes, successful patch management can be achieved.

1. **Code Scanning**

SwiftTech provides a system that ensures the customer a secure platform for code scanning and further processing.