SwiftTech

Speed, Flexibility, Success

Information Security Policy

Updated by: Filippo Calabrese

Date: Aug 18, 2024

I. 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.

II. Policy Updates

This policy will be updated at least annually or as changes to SwiftTech's architecture, security controls, or risk posture dictates.

III. 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 (CSF):** To guide the implementation and continuous improvement of our cybersecurity practices.
2. **HIPAA:** To comply with healthcare-related security regulations, especially since we may engage with healthcare clients.

And / or:

3. **ISO/IEC 27001:** To ensure that our information security management system (ISMS) is robust and compliant with international standards.

IV. 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

V. Data Storage

SwiftTech shall at a minimum store customer data using **AES-256** encryption to ensure data confidentiality and integrity, exceeding the basic AES-128 standard.

All databases in production environments must be encrypted to prevent unauthorized access to sensitive data.

VI. End User Management

- Internal network users are required to have a password with a minimum length of 12 characters to enhance password strength and reduce the risk of unauthorized access.
- Passwords must expire every 90 days to enforce regular updates and minimize the risk of credential theft.
- VPN access must require Multi-Factor Authentication (MFA) to add an additional layer of security for remote access to SwiftTech's systems.

VII. Network Controls

- TLS **v1.2 or higher** must be used for all communications between the cloud production environment and SwiftTech's physical location to ensure secure data transmission and prevent potential interception by unauthorized entities.
- Application development tiers must be **logically segmented** from business application servers to minimize the impact of potential security breaches and prevent lateral movement by attackers within the network.

VIII Patching and Vulnerability Management

Development Tier servers must be **regularly patched** and vulnerabilities addressed promptly to reduce the attack surface and prevent exploitation by threat actors.

Application code must be **scanned for vulnerabilities** before being published into the production environment to ensure the integrity and security of the software.

IX Governance and End-User Management

Password Length Compliance: A governance mechanism will be established to enforce and audit password policies across all users. Regular audits and automated compliance checks will be implemented to ensure adherence to password length and expiration requirements.

MFA Enforcement: MFA will be mandatory for all remote access to SwiftTech's systems. This will be enforced through configuration policies and regular audits to ensure continuous compliance.