SecureTech Inc.

Information Security Policy

Version 1.0

March 2025

Table of Content

Introduction: 3

Purpose: 3

Scope: 4

Version History: 4

Roles and Responsibilities: 4

Compliance Requirements 5

Principles: 6

1.Bring Your Own Device (BYOD) Policy 6

2. Data Protection Policy 6

3. Data Retention Policy 6

4. Mobile Device Policy 6

5. Password Policy 7

7. Asset Management Policy 7

8. Access Control Policy 7

9. Remote Working Policy 8

10. Cloud Service Policy 8

11. Incident Response Policy 8

12. Social Media 8

I. Usage of Social Media within SecureTech Inc.network is restricted, unless approved specifically 8

13. Database Security Procedure 8

14. Patch Management Procedure 9

Exceptions & Compliance 9

Definitions 10

Revision History: 12

Introduction:

The Information Security Policy provides an integrated set of protection measures that must be uniformly applied across SecureTech to ensure a secured operating environment for its business operations

Secure Tech Inc is a UK based company specialized in cloud based solutions for financial institutions. With rapid global expansion, the company faces increasing cybersecurity threats and stringest regulatory requirements. This policy establishes a structured approach to information security to protect data, ensure compliance and manage risk effectively.

This Information Security Policy addresses the information security requirements of:

I. **Confidentiality:** Protecting sensitive unauthorised individuals or systems;
II. **Integrity:** Safeguarding the accuracy, completeness, and timeliness of information;
III. **Availability:** Ensuring that information and vital services are accessible to authorised users when required

Purpose:

To articulate information security policy to safeguard SecureTech Inc. information assets and to ensure SecureTech Inc. comply with ISO 27001 ,GDPR ,PCI DSS and SOC 2.

Scope:

This policy applies to

I. All organisational and customer information regardless of format.
II. All individuals associated with Secure Tech Inc, including temporary workers and external contractors.

Version History:

Version	Version Date	Version description	Name
1.0	6-April-2025		

Roles and Responsibilities:

Executive Leadership:

- Provide strategic oversight and ensure security policies align with business objectives.
- Allocate resources to implement and maintain security measures.
- Review and approve security policies.

Chief Information Security Officer (CISO):

- Develop, implement, and maintain the security program.
- Conduct risk assessments and ensure compliance with regulatory standards.
- Oversee incident response and coordinate mitigation efforts.

IT & Security Department:

- Implement security controls, monitor network security, and manage access controls.
- Ensure secure application development practices.
- Perform regular security assessments and vulnerability testing.

Risk & Compliance Department:

- Monitor adherence to compliance frameworks (ISO 27001, SOC 2, GDPR, PCI-DSS).
- Conduct internal audits and risk assessments.
- Manage third-party security compliance.

Employees and Contractors:

- Follow SecureTech Inc.'s security policies and best practices.
- Report security incidents and potential threats.
- Complete mandatory security awareness training.

Compliance Requirements

SecureTech Inc. must comply with the following regulations and standards:

- **ISO 27001** – Information security management system (ISMS) requirements.

- **SOC 2** – Security, availability, processing integrity, confidentiality, and privacy principles.
- **GDPR** – General Data Protection Regulation for data privacy and protection.
- **PCI-DSS** – Payment Card Industry Data Security Standard for handling payment data.

Principles:

1.Bring Your Own Device (BYOD) Policy

I. Only approved devices can connect to company systems.
II. Devices must have security software, encryption, and remote wipe enabled.
III. Lost or stolen devices must be reported immediately.

2. Data Protection Policy

I. Classify data as Public, Internal, Confidential, or Restricted.
II. Encrypt sensitive data..
III. Limit access based on roles and need-to-know principles.

3. Data Retention Policy

I. Retain financial data for at least 5 years.
II. Store customer data in compliance with GDPR and PCI-DSS.
III. Securely delete outdated data..

4. Mobile Device Policy

I. Only company-approved security software is allowed.
II. Remote wipe must be enabled for lost or stolen devices.

5. Password Policy

I. Use strong passwords (12+ characters, mix of uppercase, lowercase, numbers, and symbols).
II. Enable Multi-Factor Authentication (MFA).
III. Change passwords every 90 days and prohibit reuse of old passwords.

6. Third-Party Risk Management Policy

I. Conduct security assessments before working with vendors.
II. Require vendors to comply with ISO 27001, SOC 2, and GDPR standards.
III. Regular review and monitor vendor security compliance.

7. Asset Management Policy

I. Maintain an up-to-date inventory of all IT assets.
II. Conduct regular audits to ensure assets are accounted for.
III. Implement strict access controls for critical assets.

8. Access Control Policy

I. Enforce Role-Based Access Control (RBAC).
II. Review user access rights every 6 months.
III. Immediately revoke access for terminated employees.

9. Remote Working Policy

I. Remote employees must use company-approved VPNs.
II. Devices must have endpoint security software installed.
III. Avoid accessing sensitive data over public networks..

10. Cloud Service Policy

I. Use only approved cloud providers.
II. Data stored in the cloud must be encrypted.

11. Incident Response Policy

I. Implement real-time monitoring for threat detection.
II. Conduct regular incident response drills.
III. Preserve logs and forensic data for analysis

12. Social Media

I. Usage of Social Media within SecureTech Inc.network is restricted, unless approved specifically.
II. Employees are not authorised to publish or discuss the following on Social Media

- SecureTech Inc. confidential information •
- To cite or reference Customers, partners or suppliers without their approval
- To use SecureTech Inc. logos or trademarks unless approved to do so.

13. Database Security Procedure

I. Encrypt all databases.
II. Restrict access using Role-Based Access Control (RBAC).
III. Conduct regular security audits and monitor database activity.
IV. Apply security patches promptly to mitigate risks.
V. Ensure backup and recovery plans are in place.

14. Patch Management Procedure

I. Implement a structured patch management process.
II. Apply patches quickly to address security vulnerabilities.
III. Test patches in a controlled environment before deployment.
IV. Prioritize and deploy critical security updates immediately.
V. Monitor patch compliance and address non-compliance issues.

Exceptions & Compliance

I. Any exceptions must be formally approved by the Chief Information Security Officer (CISO).
II. Non-compliance may result in disciplinary action, including loss of access or termination.
III. Regular audits will ensure adherence to security policies.

Definitions

Terms	Definition
Access Control	A security measure ensuring only authorized users can access specific systems or data.
Asset Management	The process of tracking and maintaining company-owned IT resources.
Authentication	Verifying a user's identity before granting access.
Backup	A copy of data stored securely to prevent loss or corruption
Bring Your Own Device (BYOD)	A policy allowing employees to use personal devices for work while ensuring security measures are in place.
Cloud Security	Policies and procedures to protect data stored in cloud environments.
Data Classification	Categorizing data based on sensitivity and

	confidentiality levels.
Encryption	The process of converting data into a coded format to protect it from unauthorized access.
Incident Response	A structured approach to identifying, containing, and mitigating security incidents.
Least Privilege	A principle ensuring users have only the minimum access necessary to perform their job functions
Multi-Factor Authentication (MFA)	An additional layer of security requiring multiple verification methods to access a system
Patch Management	The process of updating software to fix security vulnerabilities and improve performance
Remote Wipe	A security feature that allows company data to be erased from lost or stolen devices.
Role-Based Access Control (RBAC)	A security model that restricts access based on user roles and responsibilities.
Security Audit	A systematic evaluation of security policies and practices to ensure compliance.

Third-Party Risk Management	Assessing and monitoring security risks posed by vendors and external partners.
VPN (Virtual Private Network)	A secure connection that encrypts data transmitted between remote devices and company systems.

Revision History:

Date	Description of Change	Reviewer