Effective Date/Issuing Authority
Effective Date: July 28, 2013
Date Last Reviewed: Dec 10, 2021
Date Scheduled for Review: Dec 2023

Issuing Authority: FITECH CIO

Purpose

Information that is collected, analysed, stored, communicated and reported upon may be subject to theft, misuse, loss and corruption. Information may be put at risk by poor education and training, and the breach of security controls.

Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation as well as possible judgements being made against Fitech.

Objectives

The Fitech's security objectives are that:

- Our information risks are identified, managed and treated according to an agreed risk tolerance
- Our authorised users can securely access and share information in order to perform their roles
- Our physical, procedural and technical controls balance user experience and security
- Our contractual and legal obligations relating to information security are met
- Individuals accessing our information are aware of their information security responsibilities
- Incidents affecting our information assets are resolved, and learnt from to improve our controls.

Scope

The Information Security Policy and its supporting controls, processes and procedures apply to all information used, in all formats. The Information Security Policy and its supporting controls, processes and procedures apply to all individuals who have access to Fitech information and technologies.

A detailed scope, including a breakdown of users, information assets and information processing systems, is included in the Information Security Management System (ISMS) Framework document.

Compliance

Compliance with the controls in this policy will be monitored by the Information Security director.

A review of this policy will be undertaken by the Information Security team annually or more frequently as required, and will be approved by the Information Governance Board.

Policy Statement

It is Fitech's policy to ensure that information is protected from a loss of:

- Confidentiality – information will be accessible only to authorised individuals
- Integrity – the accuracy and completeness of information will be maintained
- Availability – information will be accessible to authorised users and processes when required

Fitech will implement an Information Security Management System based on the ISO 27001 International Standard for Information Security. Fitech will also reference other standards as required, mindful of the approaches adopted by its stakeholders, including partners.

1. Information Security Policies

A set of lower level controls, processes and procedures for information security will be defined, in support of the high level Information Security Policy and its stated objectives. This suite of supporting documentation will be approved by the Information Security Board, published, and communicated to users and relevant external parties.

2. Organisation of Information Security

The Fitech will define and implement suitable governance arrangements for the management of information security. This will include identification and allocation of security responsibilities, to initiate and control the implementation and operation of information security.

The Fitech will appoint at least:

- An Executive to chair the Information Governance Board and take accountability for information risk
- An Information Governance Board to influence, oversee and promote the effective management of information
- Information Asset Owners (IAOs) to assume local accountability for information management; and Information Asset Managers (IAMs) responsible for day-to-day information management

3. Human Resources Security

The security policies and expectations for acceptable use will be communicated to all users to ensure that they understand their responsibilities. Information security education and

training will be made available to all staff, and poor and inappropriate behaviour will be addressed. Where practical, security responsibilities will be included in role descriptions, person specifications and personal development plans.

4. Asset Management

All assets (information, software, electronic information processing equipment, service utilities and people) will be documented and accounted for. Owners will be identified for all assets and they will be responsible for the maintenance and protection of their assets.
All information assets will be classified according to their legal requirements, business value, criticality and sensitivity, and classification will indicate appropriate handling requirements.
All information assets will have a defined retention and disposal schedule.

5. Access Control

Access to all information will be controlled and will be driven by business requirements. Access will be granted or arrangements made for users according to their role and the classification of information, only to a level that will allow them to carry out their duties.

A formal user registration and de-registration procedure will be maintained for access to all information systems and services. This will include mandatory authentication methods based on the sensitivity of the information being accessed, and will include consideration of multiple factors as appropriate.

Specific controls will be implemented for users with elevated privileges, to reduce the risk of negligent or deliberate system misuse. Segregation of duties will be implemented, where practical.

6. Cryptography

The Fitech will provide guidance and tools to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information and systems.

7. Physical and Environmental Security

Information processing facilities are housed in secure areas, physically protected from unauthorised access, damage and interference by defined security perimeters. Layered internal and external security controls will be in place to deter or prevent unauthorised access and protect assets, especially those that are critical or sensitive, against forcible or surreptitious attack.

8. Operations Security

The Fitech will ensure the correct and secure operations of information processing systems.

This will include:

- Documented operating procedures
- The use of formal change and capacity management
- Controls against malware
- Defined use of logging
- Vulnerability management

9. Communications Security

The Fitech will maintain network security controls to ensure the protection of information within its networks, and provide the tools and guidance to ensure the secure transfer of information both within its networks and with external entities, in line with the classification and handling requirements associated with that information.

10. System Acquisition, Development and Maintenance

Information security requirements will be defined during the development of business requirements for new information systems or changes to existing information systems. Controls to mitigate any risks identified will be implemented where appropriate.
Systems development will be subject to change control and separation of test, development and operational environments.

11. Supplier Relationships

Information security requirements will be considered when establishing relationships with suppliers, to ensure that assets accessible to suppliers are protected. Supplier activity will be monitored and audited according to the value of the assets and the associated risks.

12. Information Security Incident Management

Guidance will be available on what constitutes an Information Security incident and how this should be reported. Actual or suspected breaches of information security must be reported and will be investigated. Appropriate corrective action will be taken and any learning built in to controls.

13. Information Security Aspects of Business Continuity Management

Fitech will have in place arrangements to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely recovery in line with documented business needs. This will include appropriate backup routines and built-in resilience. Business continuity plans must be maintained and tested in support of this policy. Business impact analysis will be undertaken of the consequences of disasters, security failures, loss of service, and lack of service availability.

14. Compliance

The design, operation, use and management of information systems must comply with all statutory, regulatory and contractual security requirements. This will include IT Health Checks, gap analyses against documented standards, internal checks on staff compliance, and returns from Information Asset Owners.