Southern Taiwan University of Technology
Computer and Information Networking Center
Information Security Policy

Confidential level: general
File Number: STUT-ISMS-A-001
Revision: 1.2
Release Date: 98 May 6

Revision record

Edition	Revision Date	Page Modified	Revised by	Revision Summary
1.0	97.09.19		Cai Quanfeng	First edition
1.1	98.03.20	P1, P2	Cai Quanfeng	To modify the format and merge text 1. Amendment 1 2. Amendment 2 3. Amendment 3.1, 3.2, 3.3, 3.4 4. Amendment 4.1, 4.2, 4.3, 4.4
1.2	98.05.06		Cai Quanfeng	Add Chapter 5, Management Indicators

Information Security Policy					
File number	STUT-ISMS-A-001	Secret level	General	Edition	1.2

Table of contents

1. Purpose 1
2. Scope 1
3. Objectives 1
4. Responsibility 2
5. Management Indicators 2
6. Review 3
7. Implementation 4

Information Security Policy					
File number	STUT-ISMS-A-001	Secret level	General	Edition	1.2

1. Purpose

   To ensure the confidentiality, integrity and availability of Southern Taiwan University of Computer and Information Networking Center's (hereinafter referred to as the Center) information belongs to the assets, in order to comply with the relevant laws, regulations and requirements.

   To save it from internal and external threats by deliberately or accidentally, and keep on the center of the business requirements, as prescribed in these policies.

2. Scope

   2.1 This policy applies to all staffs of the range-based centers, business units, outsourcing vendors and visitors and the users of the services center.

   2.2 Information Security Management areas were covering 11 fields, to avoid human error and possible risks, intentional or natural disasters and other factors that could result in data misuse, leakage, tampering, destruction, violations and harm. The fields are as follows:

   2.2.1 Information security policy setting and evaluation.

   2.2.2 Information security organization.

   2.2.3 Information asset classification and control.

   2.2.4 Safety management and training.

   2.2.5 Physical and environmental security.

   2.2.6 Communications and safety management.

   2.2.7 Access control security.

   2.2.8 Security of system development and maintenance.

   2.2.9 Information security incident and treatment response.

   2.2.10 Operation of business continuity management.

   2.2.11 Implementation of relevant regulations and policy compliance

3. Objectives

   To maintain the confidentiality, integrity and availability of the Center's assets information and protect the privacy of user data safety. All of the Center's colleagues work together to achieve the following objectives:

   3.1 Protect the security of business services center, to ensure that the authorized personnel can access the required information, to ensure its confidentiality.

   3.2 Protect the security of business services center, to prevent unauthorized changes to ensure its accuracy and integrity.

   3.3 Maintain a sustainable operation of the business establishment of the Centre plans, to ensure the continuous operation of the business services center.

   3.4 To ensure that the center of business service executives comply with the requirements of relevant laws or regulations.

4. Responsibility
   - 4.1 The center should be established to co-ordinate the organization information security to promote information security matters.
   - 4.2 Management should actively participate and support the information security management system through the appropriate standards and procedures to implement this policy.
   - 4.3 All the staffs of the center, outsourcing vendors and visitors have to comply with this policy.
   - 4.4 The center staffs and outsourcing services companies have the responsibility through the appropriate notification mechanism, to communicate any information security incidents or vulnerabilities.
   - 4.5 Any act of threatening security, will be held depending on the seriousness of their civil, criminal and administrative responsibility or the relevant regulations under this proposed Center office.

5. Management Indicators

   To evaluate the attainment of information security management objectives, in particular set of information security management indicators are as follows:

   - 5.1 Quantitative Indicators
     - 5.1.1 Ensure the maintenance and operation of the center of information throughout the year of service with more than 96% of work time availability.
     - 5.1.2 Ensure the information security for events, unusual events, accidents caused by other systems or the host abnormal circumstances that interrupt the operation of services not more than 4 times per quarter.
     - 5.1.3 Ensure the information security for events, unusual events, accidents caused by other systems or the host abnormal circumstances that interrupt the operation of services, each no longer than 4 working hours.
     - 5.1.4 The Centre should properly protect its confidentiality and integrity of information assets, at least once in a year being tested its risk assessment and management.
     - 5.1.5 To ensure information security measurement of the center line with existing laws or regulations, regulatory requirements, each audit at least once per visit.
     - 5.1.6 Maintenance and operation of business continuity planning exercise to be conducted at least once per visit, to ensure that the center sustainable operation of the IT business services.
   - 5.2 Qualitative Indicators
     - 5.2.1 Should periodically review the Center staff in charge of information security organizations, to ensure the promotion of information security work.
     - 5.2.2 Staffs should comply with the requirements, duties and responsibilities to provide appropriate information security relevant training.
     - 5.2.3 The Centre should be strengthened by the environmental safety information room facilities, the protection and authority to take appropriate control mechanism.
     - 5.2.4 Should ensure that the information transfer process is not a result of, or act unintentionally, disclosed to unauthorized third parties.
     - 5.2.5 Access control should be strengthened to prevent unauthorized and improper access of information, to ensure that the center has been subject to appropriate protection of assets.
     - 5.2.6 The Centre should consider the security of information systems development needs, and regularly auditing security vulnerabilities.

5.2.7 Should ensure that all information security incidents or suspected of security vulnerabilities, are being followed up to the appropriate response, the notification mechanism and be a proper investigation and treatment.

6. Review
This policy should be reviewed at least once per visit per year to reflect the government regulations, the latest technology and business development status, to ensure sustainable operation of the center operations capabilities.

7. Implementation
This policy is established by the "Information Security Committee " for approval and further revision.