(Unofficial Translation)*

Notification of National Statistical Office
Re: Information Security Policy of National Statistical Office
B.E. 2558 (2015)

National Statistical Office, the central state agency in charge of the technical statistics work, has the authority and duties under Statistics Act B.E. 2550 to manage statistics and information systematically for country development and increase competitiveness, conduct censuses or surveys, manage the socio-economic database, information technology database and others including collaborate with international statistical agencies.

Currently at National Statistical Office, a computer network system and electronic methods have been used in statistical management process, statistical production process, dissemination of statistics and information process to maximize performance. By virtue of section 5 and section 7 of the Royal Decree on Regulation of Service Businesses Relating to Electronic Payment B.E. 2006 and Declaration of Regulating Rules and Procedures for Electronic Transactions of the Public Sector in 2006, the Electronic Transaction Committee's Policy Guidelines and Guidelines for Information Security of Government Agencies in 2010 and (No. 2) 2013, this declaration was adopted by National Statistical Office to be the guideline for all sectors of the organization to implement information security and build trust for data and information users, as follows.

1. In this notification

1) "National Statistical Office" means all divisions in the National Statistical Office including Provincial Statistical Offices.

2) "Statistical process" means value creation processes and support processes.

3) "Value creation process" means processes of statistical production, statistical dissemination and statistics system management.

4) "Support process" means processes of technology and information, human development, public relations, statistical knowledge management, general management, statistical collaboration with national and international agencies.

5) "User(s)" means staffs of National Statistical Office, government visitors and external users.

*Translated by Translation Working Group of National Statistical Office of Thailand

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

6) "National Statistical Office Staff(s)" means government officials, government employees, employees, temporary employees, daily contract employees.

7) "Government visitor(s)" means the recipients of the information, trainee attendees and external supporters

8) "External user(s)" means the users or members who have access to the Internet.

9) "General user(s)" means outsiders who use an information system without registration.

10) "Member(s)" means outsiders who have been registered to use an information system that is provided.

11) "External Sponsor(s)" means an official(s) from an outside agency who supports the operation of the National Statistical Office.

12) "User Rights" means the general rights, privileges and other rights related to information assets.

13) "Assets" mean the information assets of the National Statistical Office, including.

(1) Computer system, computer network system, security system, and technical computer system.

(2) Computer bodies, computer components, recorders and any other devices.

(3) Software, application software, and information systems.

(4) Data and statistical information in electronic form and computer information.

14) "Information System" means a computer system supported by the National Statistical Office including:

(1) Management Information System.

(2) Information System for Data production.

(3) Information System for Information Services and Statistics Information.

(4) Information System for Statistical System Management.

15) "Information for organization management" means an application program that supports the management of an organization, for National Statistical Office staff only.

16) "Information for data production" means an application program that supports the operation of the data collection, processing and analyses.

17) "Information for information services and statistics information" means an application program that supports the service operation to general users and members.

18) "Information for statistical system management" means that the application software that supports the statistical system management of the country.

19) "Statistical information" means information obtained through processing or analyses by the means of statistical methodology.

20) "Statistical data" means data obtained from the statistical implementation according to academic principle consisting of raw data, microdata, and individual data.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

21) "Raw data" means the data from the census/survey questionnaire conducted by the National Statistical Office, which are validated but not yet processed.

22) "Microdata" means all individual data which are verified, corrected and consistency checked for readiness to be processed in the next steps.

23) “Individual data" means data of individual person, juristic person, partnership, limited partnership. This data is given by the data owner to the National Statistical Office.

24) "Personal data” means data relating to an ordinary person such as education, financial status, health record, criminal record, resume, and other document which contains his names, his identification number, code, or other information that can be used to identified him such as finger print, voice recordings or photos including information about the identity of the deceased.

25) "Computer system" means a main server and computer equipment, including software in use.

26) "Network system" refers to the remote network, internal network, NGX, wireless network system.

27) "NGX" refers to internal computer systems, wired and wireless networks at the Government Complex Commemorating His Majesty the King's 80th Birthday Anniversary, 5th December, B.E. 2550 (2007) (Building B), which is operated by TOT Public Company Limited.

28) "GIN Network" refers to Government Information Network that connects all government offices together.

29) "Security device" means a firewall device, an IPS / IDS device, a proxy device, a Web Gateway device, an E-Mail Gateway device, or other device that supports security system.

30) "Access or control over the use of information" means the authorization, assignment or grant of access to the user or government visitor, the use the network or the information system, both by electronic or physical access. It may also impose inaccurate access to practices.

31) "Information security" means the maintenance of confidentiality, integrity, and availability of information, including other features: authenticity, accountability, non-repudiation and reliability.

32) "Confidentiality" means the maintenance or preservation of a computer network system, computer system, technical computer system, information system, information, electronic information, or computer data from unauthorized access, use, or disclose by unauthorized persons.

33) "Integrity" means the operation for the information, electronic data, or computer data to be in perfect condition when in use, process, transfer, or store in order to avoid any change, modification, loss, damage or destruction without permission or any illegal acts.

34) "Availability" means the management of the provision of information assets to be ale to gain access or use in a timely manner.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

35) "Security incident" means the occurrence of an event, or a service condition that demonstrates the possibility of violating a security policy or preventive action, or an unknown event that may involve security.

36) "Undesirable or Unforeseen Security Situation" means unintended or unpredictable security situation, which may cause the organization's system to be compromised or attacked, and security threatened.

37) "Administrator" means a computer administrator, network administrator, security administrator, application program administrator, database administrator, information system administrator, and backup system administrator.

38) "Computer administrator" means the officer assigned to manage the main server system.

39) "Network administrator" means the officer assigned to manage a computer network system.

40) "Security administrator" means the officer assigned to manage information security system.

41) "Application Program Administrator" means the officer authorized to administer the application program.

42) "Database Administrator" means the authorized officer to administer the database.

43) "Backup Administrator" means the authorized officer to manage the backup and recovery system.

44) "Information system administrator" means the officer assigned to manage information systems.

45) "Safe method" means a secure method of electronic transactions.

46) "Electronic Transactions" means transactions made by electronic means, in whole or in part.

47) "Transaction" means any action involved in civil and commercial matters, or in the operation of the state as prescribed.

48) "Electronic data" means the message generated, transmitted, stored or processed electronically, such as electronic data interchange, e-mail, telegram, teletype, or fax.

49) "Electronic data interchange" means sending or receiving electronic messages between computers using predefined standards.

50) "Data conversion" means the conversion of data from documents into electronic system by means of key logging or scanning as an image file.

51) "Chief executive" means the person authorized to act in accordance with the administration structure of the National Statistical Office. He/She has roles and responsibilities in policy making, decision making, and guidelines for implementation of the National Statistical Office.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

2. In the case of computer systems or information got damaged or in any danger to any organization or person, due to defects, negligence or breach of compliance with security policy and information security guidelines, the head director of National Statistical Office is responsible for information security.

3. Information Security consists of 11 sections and shall be updated in accordance with the mission every two years as follows.

Section 1 Security Management

> Policies, measures, rules or procedures to assure that information security supported mission and operations of the National Statistical Office retaining credibility, confidentiality, integrity, and availability.

Section 2 Security structure for organizations

> Policies, measures, rules or operations exist to define responsibilities and operational agreements in information security activities of National Statistical Office staff and external supporters.

Section 3 Information Asset Management

> Policies, measures, rules or operations exist to protect information assets to be in ready to use condition with no hindrance for operations,

Section 4 Human Resources Security

> Policies, measures, rules or operations exist to prevent damage from internal or external personnel.

Section 5 Enhancing physical and environmental security

> Policies, measures, rules or operations exist to protect information assets, buildings, or other assets from personnel, natural disasters, accidents or other physical hazards.

Section 6 Computer system communication and operation management

> Policies, measures, rules or operations exist to manage communication and computer systems to be safe and ready to use.

Section 7 Information Access Control

> Policies, measures, rules or operations exist to control user access to computer systems, network systems, security systems, applications, files, and databases.

Section 8 The security situation management for threat

> Policies, measures, rules or operations exist to handle natural disaster, network security threat, or others that may damage information assets.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

Section 9 Management for services to ensure continuity

Policies, measures, rules or operations exist to prepare computer recovery, backup, data recovery, or provide alternate backup site to recover information systems in the least amount of time.

Section 10 System acquisition, development and maintenance

Policies, measures, rules or operations exist to control the supply, installation, application program development, and maintenance of the system to be ready to use at all times.

Section 11 Monitoring and action evaluation from policy and regulation

Policies, measures, rules or operations exist to monitor and evaluate information security systems from the internal audit unit or external audit unit.

4. Each section should have guidelines and regulations in written documents on information security work and appropriate penalties in case they are infringed or violated. These documents should be notified to all the National Statistical Office staff.
5. Promote and support the pragmatic implementation of information security guidelines and use of information asset regulation in the organization. There should be the Security and Information Security Commission or the Information Technology Committee appointed to control and monitor information security implementation in organization.
6. Promote and support IT Governance, IT Risk and Compliance, and internal audit.
7. Promote and encourage all divisions of the National Statistical Office to use safe methods in the statistical process in the value creation process and support process.
8. Promote and support the application of the necessary security technology to strengthen the network prevention to withstand disasters on network systems in both the National Statistical Office and the Provincial Statistical Offices.
9. Promote and support the contingency plan for incidents of fire, floods and threats from the internet in case of an emergency and not be able to handle these situations in electronic way.
10. Promote and encourage the internal auditor to monitor the information security system at preliminary level in accordance with the organization regulations and have external auditors verify the integrity of the security system.
11. Promote the dissemination of knowledge and training staff to be aware of the hazards and cooperation to protect the various types of potential disasters.
12. Encourage personnel who maintain and manage information security systems to get trained and be knowledgeable in acceptable standards.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

This will take effect from now on.

Noticefied on the 10th September B.E. 2558 (2015)

(Mrs. Nuannapa Thanasak)
Deputy Director-General of the National Statistical Office
Acting Director General

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

Information Security Guideline B.E.2558 (2015)

Since data and statistical information of the National Statistical Office are stored electronically. They are the organization's core information assets which must be managed in a secure manner, accurate and reliable. With the threats to information security to the information system of the organization is likely to be increased; there are many external and internal factors that can damage information assets and the image of the National Statistical Office which may lead to a lack of credibility for users of information and statistical information. In addition, Section 15 of the Statistics Act B.E. 2550 states that all personal or individual data acquired must be strictly confidential. Therefore, the National Statistical Office has set up guidelines in line with the policy as a guideline in order to secure information of the agencies effectively.

Section 1

Security Management

Objective

To ensure the management of information security system maintains the confidentiality, integrity, and availability. The operation requires a quality management cycle (PDCA) which consists of plan, do, check and act.

Guidelines

1. Analyze and define security requirements in the statistical process including specify safe methods in the statistical process for the value creation processes and support processes to use as a framework for information security.

2. Information security management must not affect the users.

3. Define the Information Security Management System to be used as process of information security management system as follows.

1) Planning activities are as follows:

(1) To review and update 11 sections of policy guidelines and the security architecture on a regular basis every two years to meet the needs of the statistical process, the changing environment of information technology and regulations.

(2) Plan the improvement of information security technology and specify in the information technology master plan of the National Statistical Office.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

(3) Make regular self-assessment plans to check the completeness of operations in the information security management process.

2) Doing activities:

(1) Announce to all the National Statistical Office staff about the Information Security Policies and Guidelines, including the Regulations for the Use of Information Assets.

(2) Implement the requirements of the 11 sections of information security guideline by daily monitoring information security incidents and response to information security incidents.

(3) Report to the directors when the information security incident occurs in the National Statistical Office.

(4) Disseminate information and educate staff to be aware of the danger to the information and to be sure of the security of information on a regular basis.

(5) Collaborate with international and national organizations to identify possible threats to the network system.

3) Checking activities are as follows:

(1) Regularly assess the risk and handle potential risks to information assets, with risk identification procedures, risk identification, risk analysis, and risk management.

(2) Vulnerability scan of important information assets on a regular basis, perform the hardening on main server, network device, security device, application program that are detected, then notify staff to fix and monitor.

(3) Test the contingency plan regularly.

(4) Regularly check user behavior and alert them, control the usage that damages the users and the services.

4) Acting can be specified as:

(1) Regularly check and evaluate information security systems and use the audit and evaluation results for planning activities to improve information security.

(2) Review and perform gap analysis.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

Section 2

Security structure for organizations

Objective

To determine who is responsible for managing information security systems and operations in related activities which consists of persons with primary responsibility: staff of the National Statistical Office and external supporters?

Guidelines

1. The Head Director of the National Statistical Office is responsible for information security in the case of computer systems or information gets damaged or harms to the organization or any person due to defects, negligence or breach of compliance with security policy and guidelines in the field of information security.

2. The Information Security Committee or the Information Technology Committee regularly review and update the security policies and practices.

3. The Information and Communication Technology Center is responsible for the management of information security systems and defines information security architecture to comply with the mission of the National Statistical Office.

4. The Provincial Statistical Offices are responsible for managing the information security system of the Provincial Statistical Office in accordance with the mission of the Provincial Statistical Office in 6 sections:

Section 3 Information asset management

Section 4 Human resources security

Section 5 Enhancing physical and environmental security

Section 6 Communication administration and computer system operation

Section 7 Information asset access control

Section 9 Service management to ensure continuity

5. The Legal Group shall coordinate the litigation operation if the offense under the Computer Related Offense Act B.E. 2550 or other Act is violated.

6. The Personnel Group shall be responsible for the notification of staff names who resign from the National Statistical Office to the Information and Communication Technology Center on a monthly basis to remove user right from the system.

7. The Internal Audit Group shall be responsible for administering and monitoring the information security system of the National Statistical Office.

8. Set a confidentiality agreement for external sponsors for installation, maintenance and the work related to security information systems.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

9. The person responsible for the information exchange system shall set a confidentiality agreement, maintainence of computer system and computer devices for external agencies that the National Statistical Office has installed in other ministries.

10. System administrators, consisting of information system administrator, application program administrator, computer system administrator, network administrator and backup administrator are responsible for their assigned functions and complied with the related requirements of the Security Information Security Guideline.

11. Information Security Coordination Committee is responsible for management and coordination when disaster occurs.

12. Information Disaster Response Team is responsible to create continuity plan and support recovery of the information system back to normal.

13. For missions that do not appear to have responsible person but there are incidents related to these missions, the committee shall be appointed to response to the work.

14. The bureau/ office /group under the administration of the director/ provincial statistical office shall take information security guideline into practice regularly.

Section 3

Information Asset Management

Objective

To manage information assets of the National Statistical Office consisting of computer network system, computer system, security system, technical computer system, documents, information, and other assets to be ready to use in the operation and service.

Guidelines

1. Set regulations on the use of information assets in writing and inform users of the correct way to use the information, prohibitions and penalties in case of violation of the use.

2. Register an asset list and keep the information up to date every year. The following information is required:

1) Number of equipment

2) Type of equipment

3) Occupier or caretaker

4) Location

5) Priority level

6) Sourcing value

7) Storage method

8) Application control

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

3. Manage assets, computer network, computer system, computer hardware, computer device, recorder, security system, computer technical system, as the following:

1) Set an agreement on the use of information assets prior the use in according to the regulation of the use of information assets.
2) Estalish a loan/ return system, important information assets in external work to detect and prevent damage.
3) Control the movement of assets that need to be used outside organization and use external assets in the organization.

4. Manage the assets, software, application program, information systems as follows.

1) Classify information system into information for enterprise management, information for the infomation production, information for information service and statistical information, and information for statistical management.

2) Identify application program registration by categories of information systems and include the following information;
(1) User
(2) System owner
(3) System administrator
(4) Priority or hierarchy of data confidentiality.
(5) Accessibility level
(6) Accessibility time
(7) Accessibility channels

3) Classify the software license and include the following information:
(1) User
(2) Location
(3) Usage
(4) Copyright usage

5. Manage assets, information, and statistical information in electronic form as following requirements;

1) Establish the data registration, important information, and documents that require levels of confidentiality to specify management methods and to comply with the Regulation on Government Confidentiality B.E. 2544.

2) Classify important documents as follows:

(1) Available to pulic; members or specified groups only;

(2) Priority or hierarchy of data confidentiality

(3) Accessibility level

(4) Accessibility time

(5) Accessibility channel

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/ OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

3) Classify the information records as follows:
(1) The type of data is classified as raw data, microdata, and individual data
(2) Priority or hierarchy of data confidentiality
(3) Accessibility level
(4) Accessibility time
(5) Accessibility channels

6. Record damage from use of information assets in a log file with the following information:

1) Date/ time
2) Number of equipment
3) Damage
4) Cause
5) Effect

7. Estalish accessibility according to the following confidentiality levels:

1) User registration is required to control the rights, to set a limitation of important information and the system functions such as permission to edit data, delete data, read all data, data export, and rights to read only specific columns.

2) Set user ID and password and grant right to use systems according to hierarchy of data, with menu controls to control access to data and functions of working system in accordance with the policy of access control.

3) Define a medium-sensitive data access channel within the intranet system within 24 hours for internal users.

4) Assign a medium-sensitive data accessibility in information network system for the Provincial Statistical Office with 24 hours availability.

5) Assign unencrypted accessibility channels through the internet 24 hours a day for users and members.

6) Use sensitive or confidential data encryption systems or confidential work systems.

Section 4

Human Resources Security

Objective

To prevent damage results from personnel with notification of the regulation of information assets prior to doing the work, gaining knowledge, being aware of a threat so that they do not become the culprit, causing damage to the organization and others by lack of caution including the termination of the authorization and the retrieval of organizational property when out of duty.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/ OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

Guidelines

1. Clarify responsibilities and train newcoming officers of the National Statistical Office in order to be able to use information assets safely and acknowledge both the regulation for the use of information assets and the guideline of information security.

2. Clarify the confidentiality protection of personal data under the Statistics Act B.E. 2550 to the newcoming officers.

3. Assign the officers responsible for personal data to perform duty delegated by a director in order to comply with the authority of the National Statistical Office specified in the Statistics Act B.E. 2550 and a mission or policies of National Statistical Office. These officers shall be responsible for personal data by the delegated authority. The information system officers have authority only to define the system access rights and must not access personal data in the system according to the laws or regulations that related to personal data.

4. Prevent illegal disclosure of personal data. Personal data of National Statistical Office that obtained under the Statistical Act B.E. 2550 shall be protected in accordance with the provisions of Articles 14 to 16. Any person violates the Articles shall be liable for a criminal offense under Articles 20 of the Statistics Act B.E. 2550. When performing his/her duty, the officer shall perform under other regulations such as the Regulation on Government Confidentiality B.E. 2544, the Regulation of National Statistical Office on Complain Handling B.E. 2555, and the Regulation of National Statistical Office on Using Information Asset B.E. 2557.

5. Train officers on the knowledge and the awareness of information security on a regular basis not to be a law offender or violate the regulations notified by the National Statistics Office.

6. Review the rights of users of information systems on an annual basis as follows:

1) Remove the users from information systems or all basic services when they retire, resign from the National Statistical Office. Review the rights of using information systems according to the authority list informed by the human resources division when they are in a change of duty or responsibility.

2) Retrieve all information assets for those who have no rights to use, such as a computer, ID card, etc.

Section 5

Enhancing physical and environmental security

Objective

To control physical and environmental security which may damage important information assets in areas where information assets are installed such as computer centers, training rooms, and working desks in order to prevent the threat of personnel, natural disasters, accidents or other physical hazards.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

Guidelines

1. Check and monitor the computer centers or computer rooms as follows:

   1) Post a security declaration on board in a control area which has control over accessibility and the surveillance of the computer center.

   2) Store a main server and network devices in a computer center or in an area with adequate protection or control and shall define the right of entry in the computer center specifically for computer technical officer, system administrator, and those in related works including the electrical system, back- up electrical system, air-conditioning system, ventilation system, network system, and fire extinguisher system.

   3) Keep entry log for a main server room or a restricted area for authorized personnel only. The record must contain details about the person and entry-departure time.

   4) Ensure the electrical system in perfect condition and equipments ready to be in use and are well protected from fire.

   5) Install fire alarms such as a smoke detector, a heat detector, etc., to prevent or stop a fire from starting.

   6) Provide a fire extinguisher for using in an initial stage and perform a regularly check.

2. Monitor and supervise the use of external attendees who bring computers connected to the organization network system both wired and wireless according to the following requirements:
   1) The computer shall have antivirus software and keep up-to-date.
   2) No password detection software installation or malicious software.

3. Inspect and monitor the computer in the training room according to the following requirements:
   1) The computer shall have antivirus software and keep up-to-date.
   2) Record damage caused by the use of attendee.
   3) Make announcements of the use of computers or software for external person who attends a training course.

4. Inspect and monitor the computer in the data service room according to the following requirements:
   1) The computer shall have antivirus software and keep up-to-date.
   2) Record damage caused by the use of the user.
   3) Control an external data storage that connects to a computer.
   4) Make the announcement of the use of computers or software for external person who uses data and information service.

5. Inspect and monitor a forbidden area according to the following requirements:
   1) Provide an access control with control system and install CCTV at an important point.
   2) Monitor the CCTV equipments so that they can work normally and can record all the time.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

Section 6

Computer administration and computer system operation

Objective

Plan and manage communication systems, a main server and servers to be able to use at all times and to reduce a risk of system failure.

Guidelines

1. Analyze and plan to support a high-volume transaction according to the following requirements:
   1) Plan and manage communication systems and computer system and equipments in order to be able to support the high-volume transactions, data collection and user services.
   2) Analyze the connection architecture that corresponds to the application program and end-user in order to create an effective and secure data transmission path.

2. Set operational procedures for managing the network and computer systems according to the following requirements:

   1) The person who is responsible for managing the network system and computer system shall proceed as follows.
      (1) Network administrator and computer system administrator should prepare a manual for managing network system.
      (2) Network administrator and computer system administrator should monitor the network system regularly.
      (3) Network administrator and computer system administrator should comply with Information Technology Infrastructure Library (ITIL) standards when administering of computer system on daily basis.

   2) The person responsible for providing the communication channel should set service quality levels according to the following requirements:
      (1) Create a Service-Level Agreement (SLA) from a service provider.
      (2) Set an agreement among the service providers of data communication system to provide secure channel management and provide a monthly report about channel transaction volume.

3. Manage network security according to the following requirements:
   1) Control a device connection to both wired and wireless network.
   2) Restore data and details of the connection and backup requirements and recover plan when the network is unavailable.
   3) Inspect the vulnerabilities of network system, computer, security device, application program, and database system yearly and keep up the security level to standards.
   4) Install network protection devices, including IPS / IDS, firewall, security gateway, and anti-virus system by taking into account the need and ability to manage the system.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

5) Manage intrusion prevention devices and detect network intruders according to the following requirements:

(1) Inspect the detection database regularly.

(2) Monitor security situations that are unwanted or unpredictable from daily detection.

6) Manage network service controller according to the following requirements:

(1) Monitor firewall policy according to good system management.

(2) Control specific services to prevent unauthorized use of the services that are harmful to the network system.

(3) Regulatory modification shall not reduce the organization's security or increase risk the loss of service.

7) Manage the security gateway according to the following requirements:

(1) Set up an e-mail gateway to eliminate spam mail and monitor an attack of e-mail system.

(2) Set up a monitoring system of the internet use according to the following requirements:

(2.1) Install a web gateway to monitor the virus threat on the internet.

(2.2) Install URL filtering to control access to inappropriate information and prevent the use of network- damaging protocols and an inappropriate content harmful to the organization.

(2.3) Inspect and monitor usage behavior that violates Information Asset Use Regulations of National Statistical Office.

8) Set up data storage for network monitoring according to the following requirements:

(1) Set all main servers and security devices based on the global standard time.

(2) Store traffic data of network system and application program for service to analyze and monitor security event according to laws.

4. Provide computer system management according to the following requirements:

1) Main server system management requirements as follows:

(1) Check condition of hardwares and equipments on a daily basis.

(2) Check condition of support system in computer center on a daily basis.

(3) Monitor service on a daily basis.

(4) Regularly check the vulnerabilities in the operating system to be able to detect a malicious network attack.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

(5) Manage the program applications installed in main computer servers according to the following requirements:

(5.1) Web-based program applications provided on the internet shall be inspected and in compliance with OWASP or other international standards.

(5.2) Web-based program applications must use HTTP (80) and HTTPS (443) standard ports only.

(5.3) Set session control and session access time control to prevent threat from program.

2) Computer server system management requirements as follows:

(1) Define the program installation and connection requirements that negatively affect the network system of organization.

(2) Control the installation program of a specific computer server that uses in an operation but not for a user computer on service.

3) Anti-virus system management in computer server and computer main server according to the following requirements:

(1) Keep the up-to-date of computer virus database regularly.

(2) Keep track of computers that lack updated on computer virus databases.

(3) Monitor the work of computer antivirus program to perform proper functioning.

(4) Report the virus infection of the computer server, including detailed information of viruses spreading in the organization.

Section 7

Information Asset Access Control

Objective

To control the access to information assets of the organization to the person who has authority in order to prevent damage caused by compulsive use that might cause damage to organization information systems or affects daily operations.

Guidelines

1. Control user access to information assets according to the following requirements:

1) Guidelines for controlling access to computer systems, operating systems, network systems, computer servers, information systems, application programs, databases, data files, and documents and media storage.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

2) An asset control registry of important information for organization and inspection of the condition and the existence of those information assets on a yearly basis.

3) Registration of both internal and external users prior to using the information systems.

2. A user rights management according to the following requirements:

1) A user registration according to the following requirements:

(1) The registration that requires user to register in the form that system administrator needed, and signs for acknowledgment of the conditions and authenticated by director's signature.

(2) The user registration form shall comprise at least as the following information:
(2.1) Name / Surname
(2.2) Identification numer or Government Identification Card
(2.3) Affiliation
(2.4) Contact number
(2.5) User groups (government officers, members, or ordinary people)
(2.6) Requested service
(2.7) Expiration Date
(2.8) Terms of Use
(2.9) Certifiers

2) Manage the user registration according to the following requirements:

(1) The user registration for later use verification shall comprise at least the following information:
(1.1) Name / Surname
(1.2) Identification numer or Government Identification Card
(1.3) Affiliation
(1.4) Contact number
(1.5) User ID
(1.6) Password
(1.7) Licenses
(1.8) Expiration Date

(2) Keep the user registration safe by encrypting the file and being a confidential document, not disclosed to third parties or unrelated persons.

(3) Use the access rights management approach according to the following requirements:

(3.1) Use group-based and role-based controls for information access control.

(3.2) Use identity-based controls for access to network system, operating system, and application program.

(3.3) Grant the user access permission to each user confidentially and to prevent user denial of responsibility.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

3) Review user access permission yearly according to the following requirements:

(1) The human resource division or director inform system administrator if user resigns or ceases to be an officer of the National Statistical Office.

(2) Annually Review user access rights to information assets in the 9 categories above.

(3) Revoke access permission from the registry and in the system if the following conditions are met:

(3.1) Inactive more than 6 months

(3.2) Unable to contact user directly within 3 months.

3. User authentication according to the following requirements:

1) Create user account in both individual and group accounts and authorization to access the data or the system according to the approved permission.

2) Record accountability in details of the use of the system to inspect transaction user performs in the system.

3) User shall always verify his/her access to the information and communication technology system of National Statistical Office at least with a username and password, and it shall be secured by encrypting data.

4) Use secure protocols in the user authentication procedure.

5) Use Lightweight Directory Access Protocal (LDAP) that stores user information and passwords securely encrypted.

6) Create an agreement with the user to prevent a denial of accountability if any damage is caused by the use.

4. Password Management

1) Limit session that user password is active. User shall change the password immediately upon initial login and shall change the password in a specified period.

2) Allow user to set his/her password by creating a confirmation that receives the password to re-enter the login. The system shall verify that it matches the previously entered value; therefore, it is possible to change the password in the system.

3) Have an automatic user password management system that the user shall set a password more than or equal to 8 characters, with the combination of regular letters, numbers and symbols together; therefore, users are able to assign a quality password.

4) The system administrator has to send a temporary password in a secure way and must not pass on third parties by sending in a sealed envelope that cannot be seen.

5) Require password entry. Shall mask or hide password on screen while entering password.

7) Require user to enter ID and password to prevent denial of responsibility.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/ OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

5. Password Usage

1) User shall keep password securely and shall not disclose passwords to others.

2) User shall change temporary password immediately after obtaining it and changing to be the hard-to-guess password for others.

3) User shall not type password while others can see your typing.

4) The user shall not store password on the computer or keep password where others can see or access them.

5) The user shall not use the same password with other systems.

6) The user shall not reuse the old password again.

7) The user shall notify the administrator immediately if he finds that his password is locked or have problems without knowing the cause.

8) User shall change his password immediately if he knows his password is revealed to others.

9) The user shall logout each time the user ends or suspends operation.

6. Password assignment

1) Do not use name or surname of user, family members, close person, phone number, or date of birth to set as a password.

2) A password must consist of letters, symbols, and numbers which are easy to recall but difficult to guess.

3) Do not set password to be a word in a dictionary or name of a place.

7. Protection control of information assets when inactive according to the following requirements:

1) Set requirement of the screen shutdown and lock the screen with the computer password if the system does not respond to the user within 15 minutes.

2) Set shutdown requirements for the computer server, network device, and security equipment if the user does not interact with the system within 15 minutes.

3) Set to terminate the application program if the user ignores the use within 15 minutes.

8. Set access control to computer systems in the computer center according to the following requirements:

1) Set access control to the computer center and announce the security of the computer center.

2) Access control to computer main servers and server devices, network devices, and security equipments through the request form for modification and shall be approved by the authorized person.

9. Set access control to the operating system of computer main server according to the following requirements:

1) Make a register list of programs that are allowed to install on computer server and monitor for program abuse beyond the required limits.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

2) Allow only a specific authorized computer server to access the operating system and use encrypted protocols to access.

3) Make a registration to control the operating system user and classify user permission according to user’s duty.

4) Monitor and evaluate computer main server user accounts on a yearly basis.

5) Vulnerability continued improvement of the operating system.

6) The computer system administrators shall keep the password securely and change the password every two months and become a strong password.

7) Control the installation of the utility software on the computer main server to prevent copyright infringement and prevent the avoidance of security regulation that might make the system vulnerable allowed easy access in accordance with the change management process, and have a system to protect files downloaded from the Internet that might damage from an external security system by using web filtering.

8) Control time of operating system usage to prevent the use from malicious person.

9) Define the operating system environment of computer main server according to the following requirements:

(1) Set time of the machine according to international standards for inspecting security event.

(2) Install computer antivirus programs and keep computer virus database up-to-date.

10. Network access control to prevent unauthorized access to network services according to the following requirements:

1) Network device control according to the following requirements:

(1) Network device shall be installed in the cabinet that stores Mac Address and IP Address to identify the device on the network.

(2) Must shutdown unnecessary ports and services on the network to prevent the connection from external network devices to spread their signals.

(3) Separate network IP (VLAN) numbers to control access rights.

(4) Not allow remote access to the network for important equipment.

2) Access control to the local area network according to the following requirements:

(1) Register computer server and portable devices to use the network and to monitor and store the Mac Address of computer server and portable devices connected to the network in accordance with the security requirements.

(2) The network administrator shall establish a port registry, details of the network device, and network connection structure.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

(3) Monitor computer servers and set the requirements in accordance with security regulation once a year.

(4) Usage control at least port security.

(5) Manage the network as a zone or segment as follows;

(5.1) Separate the internal network and external network with the firewall device.

(5.2) Divide the network into 5 zones as follows:

(5.2.1) The Internet Zone is an access network for internet information services users.

(5.2.2) Core Stat Zone is a network for information processing systems and allowed access only specific authorized persons

(5.2.3) GIN Zone is a network for information systems supporting the Provincial Statistical Office and allowed access to specific authorized persons.

(5.2.4) MIS Zone is a network for information systems of organization management and allowed access to specific authorized persons.

(5.2.5) Infra Zone is a network for IT management and allowed access to specific authorized persons.

3) Wireless access to the network as follows:

(1) Register computer server and portable devices for using wireless network. Monitors and stores the Mac Addresses of computer server and portable devices that connected to the network according to the security requirements.

(2) Authenticate username and password in a user-friendly way to prevent denial of responsibility.

(3) Divide wireless network users into a limited period of use for the third parties (Tickets) and personnel (Employee) for the National Statistical Office.

4) For remote network access, administrators shall provide a person identity verification before allowing users outside the National Statistical Office access to the National Statistical Office network and information system as follows;

(1) Require a remote access connection via Secure Sockets Layer (SSL VPN) in order to access to internal information asset when a user is outside of National Statistical Office.

(2) Before assigning the user the permission to log in remotely, user shall provide evidence identifying reasons or necessities with the National Statistical Office and shall be approved by the director or system owner in written document.

(3) Access to system of National Statistical Office, user shall authenticate with username and password with encryption methods for security.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

(4) The device used to connect to the system must be installed the necessary basic software, such as anti-virus software, firewall, etc.

(5) Set the rights to access information systems according to necessity and officer's duty and responsibility.

5) Internet network access according to the following requirements:

(1) Have the registration of internet network services and electronic mail before use, and attach the operating in a safe way instruction to all users to acknowledge at the same time.

(2) Authenticate with username and password by user's secure method to prevent denial of responsibility.

(3) Have regularly report to a director on usage behavior to the management of the organization.

6) Provide a secure way to exchange data between networks according to the following requirements:

(1) Data transfer among machines requires a protocol that can encrypt prior to data transfer.

(2) Service data exchange by web service, the protocols are used to send information among systems automatically required encryption before data is sent through XML Encryption.

7) Network connection control in both wired and wireless are subject to the following requirements:

(1) System administrator shall monitor and restrict user for network connectivity based on access policy.

(2) Identify equipment and tools used to connect the network without signal-spreading equipment, such as a hub, switch, router, and wireless LAN device to connect to network system before obtaining permission from the network administrator.

(3) Do not rename the computer. Do not change the connection cable in the connection specified in the connection requirements. Do not change the network IP address specified by the network administrator.

(4) Only authorized network services are allowed to connect to the network.

8) Control routing on the network to allow the computer connection and the transmission or data circulation or information on the network in accordance with access control policies as follows:

(1) Set regulatory for network routing and restrict access to the service that can only connect to the destination network through the specified channel.

(2) Provide redundant system on main network device for continuous use. In case one of the main devices cannot operate, the system will automatically redirects to other network.

11. Control access to computer server according to the following requirements.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

1) Set username and password before accessing computer server.

2) Set up the screensaver with username and password before access when computer is inactive for 5 minutes.

3) Control the data file sharing on the network system securely.

4) Control the setting and changing the specifications of computer server.

5) Control the program installation on computer server.

6) Fix the weakness (or vulnerability) of the computer's operating system upon detect.

12. Control access to information system according to the following requirements.

1) Set and update the registration of information system every year.

2) Control the use of information system as a main mission and its direct effect within the organization, including data recording system and data processing system. Set user rights to access the information system for authorized services only.

3) Control the physical of system and no permission for remote network.

4) Allow the information system administrator to determine user rights in application programs according to user's role and duty.

5) Allow the information system administrator to monitor the rights of users on a regular basis.

13. Control access to the application programs according to the following requirements.

1) Register the application program and monitor the completeness in the application program register form.

2) Control the important or high risk application program in secure components separated with firewalls and restrict only to authorized users.

3) Administrators must limit the time for connecting the information systems or the high-risk application program, as follows;
(1) Access for each connection time must be less than two hours per authentication.
(2) Disconnect if accessing time is more than a specified period.
(3) Monitor authentication every time in specified period.

4) Identify the application programs that serve external and internal users in the organization.

5) Keep the log file of users for annual monitoring.

14. Control database system according to the following requirements.

1) Database administrators grant access rights and establish database user registration and keep it up-to-date.

2) Check the vulnerability of the database and update it regularly.

3) Monitor the access of database system for reference later which includes the details of usernames, access date, and time.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

4) Do not use Database Administrato (DBA) of database system to connect the application programs.

5) Control data file connects to the database system of the application programs.

15. Control the data file according to the following requirements.

1) Control the access of processed data files; raw data, micro data, and individual data for authorized user only and to encrypt data files if necessary including fixing the data file specified in announcement.

2) Control the content of data file and the confidentiality class specified in announcement.

3) Control and fix individual data if necessary, by authorized user must provide these details;

(1) Approved by the authority

(2) Processing

(3) Modification

(4) Notify the affected

16. Control access to documents and storage, according to the following requirements

1) Control official documents as follows;

(1) National Statistical Office regulatory document, complied with the confidential official regulations B.E. 2544.

(2) The ICT system document composes with the password document, the systematic documents with IP numbers. Do not disclose the system required document to third party or put it on the desk without safe storage, and if it is a file, make the encryption.

(3) A handbook or documents for processing contains important contents. To be disclosed may damage the information system, so make the clear direction.

2) Control the external storage connected to a computer with individual privacy data file.

3) Control over the destruction of individual data by authorized officer.

(1) Individual data in document forms has to restore according to the document regulations of the Office of the Prime Minister, B.E. 2526.

(2) Individual data in electronic form has to be permanantly deleted or destroyed if lost contact for at least 10 years by crush or beaing for non-reuse. If the electronic data is needed reuse, it has to be formatted at least 5 times so it cannot be retrieved.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

4) Control over individual data modification by the officer, who take responsibility for data modification into electronic systems only.

17. Control over individual data exchange among agencies, to save and store according to the following requirements:

1) Access system data.
2) Entry and departure data of authorized users who exchange data among agencies.
3) Details of the working process when exchanging data.
4) Details of data used for storing.

18. Control over the privilege access to privacy data to directors or head director of the organization especially. The duration of access is limited to no more than 1 week each time. If there is still needed, extend to 1 week each time. When the time is up and no longer in use, do cancel the right of the user.

19. Control the high confidentiality of individual data or the sensitive data that may affect feelings, beliefs, peace, and moral of people who are customer of government agencies or its damage or impact significantly to the rights of data owner such as debit or credit card numbers, ID number, personal identification number, race, religion, belief, political opinion, health, sexual behavior and private data of persons under 18 years old with particular and proper methods.

20. Control over the system sensitive to being disturbed according to the following requirements

1) The system which is sensitive to being disturbed needs to be controlled;

(1) Web recorder system

(2) Micro-data service system

(3) Data exchange system

2) Define the areas where security is required.

(1) Identify and classify information access areas based on access rights by separating them into entry control rooms such as computer rooms.

(2) It is required to have a person responsible for controlling areas.

3) Control entrance and exit to computer room and surrounding area

(1) Provide a closed circuit system to check if there is a problem.

(2) Provide a fingerprint authentication system to access the computer room.

(3) Make announcements to control the area and operation in the room.

(4) People in the control are Direct Computer Center Administrator, System manager, External Sponsor and outsiders who operate the room.

(5) Make regular check-in and check-out every month.

4) Determine control level to computer main server.

(1) Control at the highest level consisting of computer main server to provide service for database and Lightweight Directory Access Protocal (LDAP).

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

(2) High level control consists of computer main server serviced for application software, and Middle Ware.

(3) Moderate level control consists of computer main server for web services.

5) Determine the level of computer network system control.

(1) Control at the highest level with wireless network.

(2) High level control consists of internal network, which must not connect to any location out of the organization area.

6) Control the access system from outside.

(1) Control the access port, only the active one.

(2) Control the remote access, only the access rights to computer server.

7) External authentication

(1) Set the user ID and password to access the work system and ensure the identity data users in each system and each level of confidentiality.

(2) Define a secure access method with Virtual Private Network.

Section 8

The security situation management for threat

Objective

Establish a management plan for undesired and unexpectedly situation to the information system such as the threat of the internet network or conflagration, natural disasters, or other disasters and provide quick aid to minimize impact on the National Statistical Office's information system.

Guidelines

1. To analyze, define, and review the significant threats to information assets which damage to the information system and impact on the mission and operation of the organization by providing a disaster management plan based on priority and probability.

2. Provide a plan for security management to protect undesired incidents from happening according to the following requirements;

1) Provide security plan
(1) Analyze of the occurrence of the situation.
(2) Determine the officer to response to for the situation.
(3) Evaluate the information asset damage
(4) Define tools for operation
(5) Provide knowledge and practice.
(6) Prepare to response to unexpected incident
(7) Operation location

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

2) Detection and surveillance plan

(1) Provide the process of detection and surveillance

(2) Define the form to store data

(3) Store incident information into the form

(4) Provide the protection plan

3) Establish response plan

(1) Operation tools

(2) Communication

(3) Operation steps according to the serverity of the incident.

4) Set plans to investigate and collect evidence.

(1) Litigation

(2) Collect evidence for interrogation.

5) Set recovery plan to get back to the original state.

(1) Tools for system recovery

(2) The officer to be responsible for recovery

3. Provide a detection and abnormal using system through the network and report on urgent weaknesses and vulnerability that were detected, at least the following investigation must be made regularly.

1) Attempt to invade the network.

2) Operate in an irregular manner.

3) Try to modify the network by unauthorized person.

4. Provide for rehearsal and training for fire protection plans annually or in the appropriate frequency and continue improving the operations.

Section 9

Service Management to ensure continuity

Objective

Prepare for situation which organization's assets get damaged by an undesired situation to the worst case scenario that the information system and data get damange or out of service. So be ready to fix the system to back to normal working state.

Guidelines

1. Set a Business Continuity Plan according to the following requirements;

1) Provide Business Impact Analysis

2) Identify the events the urgent plans should be implemented

3) Determine the situation or the severity of the problem

4) Analyze a choice whether to use backup center or other plce to use as backup center

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

5) Determine the responsibility and the officer to make a decision and define the contact channel for the events that occurs

6) Provide the procedures in details for the events that occurs

7) Set the practice to change activities to a temporary area

8) Define the procedures after the migration to resume normal operation.

9) Provide knowledge and awareness to personnel involved in emergency plans.

10) Provide the test and updating the plan once a year continuously and keep an urgent plan in the outside area.

2. Provide backup system to meet the requirement;

1) Determine the procedure or practice for backup data clearly. Specify the back-up data, the frequency for data back-up, media, location for storage, method for storage, and implementation

2) Provide a policy, procedure, or method for backing up data, with the following components required:

(1) Data which must be backup

(2) Frequency of data backup

(3) Media type

(4) Number of copy

(5) Procedures and backup data methods in details

(6) Location and methods of restore backup information in secure way

(7) Follow and monitor backup data results.

3) Record a log book for backup data of the officer, checking, and verification the log book with regular reports.

(1) Provide the detail on data label in the recording media on the backup accurately to be able to find data quickly and prevent using the media in the wrong way.

(2) Store the backup media including copies of procedures or practices outside for safety in case the working area is damaged. That specified place must have the access control system and the protection system for data damage as well.

(3) In case of long-term storage, consider how to take back data in the future such as storage devices and software to read recorded media.

3. Provide a recovery system for data according to the following requirements;

1) Provide main computer server in order to test critical data recovery.

2) Test backup recovery at least once a year to ensure that back up data as well as various system programs are accurate, complete and functional including steps and procedures for testing and implementing backup data from the media.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

Section 10

System acquisition, development and maintenance

Objective

Provide or develop information systems including existing security for practical use by considering the security issues on priority, preventing errors, loss, changing to the software and application program without permission. Protection of secrets has to ensure that the projects or the policies always protect security for information and maintain the security information.

Guidelines

1. Control the measurement of outsource software development. In case of the outsourcing process development, maintenance information system, and network, the following requirements should be met;

1) Risk assessment and security requirements of system to supply or develop in written agreement at least according to the following requirements;

(1) Develop the source code according to the OWASP standard or CWE TOP 25 standard, at least with the input data control, the display, the processing control

(2) Scan testing for vulnerabilities of the application program, if the vulnerabilities have been found, take action to fix them all.

(3) Implement a software engineering method to develop applications and follow standard of ISO/IEC 29110.

(4) Require the work plan and implementation procedures for developing information systems, installation of computer systems and equipment, testing system after installation, and risk management plan. The plan, testing, recording, and result report will be presented to the officer who is in charge of the project.

(5) Provide the acceptance criteria for new system, procurement system, or other information resources as well as checking and testing system thoroughly before accepttance and installation.

2) Regulatory for information system modification according to the following requirements;

(1) Control the modification of the information technology system software, edit or change the database structure according to an amending form upon the approval of qualified person and the authority including detailed record of fixing from external supporter.

(2) Access only the develop environment part, but if it is necessary to access a production environment part, exercise control or monitor strictly to ensure that this access follows the regulatory.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

(3) Provide to control the vulnerable information of organization. If it is necessary to use the fact data for testing system, to use partial data or unimportant data must get approval from the responsible officer only.

2. Measures to control the external supporter according to the following requirements;

1) Define the selection criteria with well and trusted operation to select qualified external supporter.

2) Define the monitoring criteria for maintenance and system development employees.

3) Provide the external supporters who work at the operation network and computer room. Getting permit from the authority or the administrator before working and operation every time must be under the responsibility of the authority or the administrator.

4) External supporters will be allowed to use the computer server which connects to computer main server in order to fix the software only.

5) Set the sign contract of system development to be unrevealed confidential information and work which link the information security system of organization.

6) Provide steps to operate for controlling the software installation on the information system for service.

7) External supporters must submit the operation report, various problems, and guidelines to solve these problems.

8) External supporters must comply with the requirements and regulation of the National Statistics Office strictly. At the end of the project, external supporters' rights will be cancelled immediately.

3. Provide the system maintenance and monitoring the quality of the use according to the following requirements;

1) Provide annually maintenance to the support system in computer center; the power backup systems, the fire extinguishing systems, the smoke detection systems, the air condition systems, the water leak detection systems, the computer system and connection device, the network equipment, and security system.
2) An administrator writes the system management handbook, the operation handbook, and related documents accurately and up-to-date as always.
3) Monitor the resource in the system and tracking the quality service of each system. If found, make improvement specified criteria.

4. Provide the encryption measurement for data transmission according to the following requirements;

1) Check the rights of users in web page.
2) Application programs and services on the internet need security.
3) Transferring data files among computers with confidential data.

5. Measurement to control of the modified data files according to the following requirements;

1) Manage and control the rights to access and edit the data files.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/ COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.

2) Analyze the modified data file whether or not the services have been affected.

3) Back-up the data files which changed every time before restore data.

6. Monitor the vulnerability of information systems regularly according to the following requirements;

1) Check the vulnerability of the networks, the computer main servers, and the application programs.

2) Fix system quickly for the vulnerability detected and dangerous to the system.

Section 11

Monitoring and Evaluation action from policy and regulatory Compliance

Objective

Monitor of the implementation of information security policy and guidelines including the use of information assets of the user in line with the regulations by manual checking process for the operator and internal audit for the user. Monitor from external audits for security check of information system in the orgranization.

Guidelines

1. Administrators of information security perform self-assessment to bring perfect operation process yearly according to the following requirements;

1) Self-assessment with the self-assessment form to analyze Gap

2) Self-assessment with the system penetration testing

2. Administrators of information security perform self-assessment.

3. The internal audit units of the National Statistical Office evaluate users who comply with the rules of information assets and the implementation of information security guidelines regularly as of every 2 years.

4. The external audit units evaluate the complex security systems that are required expertise regularly as of every 2 years.

5. Get monitored by the internal and external audit units and use the assessment results of the units to plan for the improvement of the information security system next year.

DISCLAIMER: THIS TEXT HAS BEEN PROVIDED FOR EDUCATIONAL/COMPREHENSION PURPOSES AND CONTAINS NO LEGAL AUTHORITY. THE NATIONAL STATISTICAL OFFICE SHALL ASSUME NO RESPONSIBILITY FOR ANY LIABILITIES ARISING FROM THE USE AND/OR REFERENCE OF THIS TEXT. THE ORIGINAL THAI TEXT AS FORMALLY ADOPTED AND PUBLISHED SHALL IN ALL EVENTS REMAIN THE SOLE AUTHORITY HAVING LEGAL FORCE.