National Taiwan Normal University Guidelines for the Management of Information Security

Approved by the Information Security Management Committee on September 30, 2011

A. Purpose

I. To strengthen the management of information security, National Taiwan Normal University (hereinafter referred to as NTNU) has formulated these guidelines in accordance with the "Personal Data Protection Act" and the "Information Security Management Guidelines of the Executive Yuan and Its Subordinate Agencies" for the establishment of an electronic system that is secure and reliable to ensure the security of data, systems, equipment, and network, thereby protecting the rights of the faculty, staff, and students of NTNU.

B. General Rules

II. These guidelines are for all departments at NTNU and all faculty, staff, and students of NTNU.

III. Each department should take the appropriate information security measures for each respective information system under its management to ensure the security of data collection, processing, transmission, storage, and circulation.

IV. If deemed necessary during the implementation of these guidelines, each department should create descriptive documents such as management regulations, operation guidelines, and special precautions.

C. Organization, Power and Responsibilities

V. The Information Technology Center (ITC) is responsible for the formulation, establishment and assessment of information security policies and technologies.

VI. Each individual unit undertaking tasks and projects shall be responsible for discussing their security needs and the management and maintenance of information systems.

VII. The ITC is responsible for the promotion of information security education and training.

VIII. The ITC is responsible for information security audits.

IX. NTNU may, on a regular basis or as necessary, audit all administrative and academic departments on their information security.

D. Information Asset Management

X. Departments should assign dedicated members of personnel to the management and maintenance of information assets.

XI. Departments should assign dedicated members of personnel for the management and safekeeping of storage media such as disks, tapes, and CDs that hold classified information or programs to prevent information leakage or impairment.

XII. All personal data in computers or relevant equipment should be deleted before they are removed from service or converted for other uses.

E. Personnel Management and Information Security Education and Training

XIII. Personnel who have access to sensitive information should sign an Affidavit of Confidentiality and fulfill their duty of confidentiality.

XIV. Each department should assign contact persons for information security, who shall receive information security education and training on a regular basis.

XV. Backup mechanisms should be established for the management, maintenance, design, and operation of vital systems of each department.

XVI. When the personnel of each department leave their positions, their access to relevant resources must be are terminated and their computer software/hardware and relevant documents must be completely transferred.

XVII. The supervisors of each department are responsible for the supervision of the information operational security of faculty and staff, and shall prevent illegal or improper conduct.

F. Physical and Environmental Security Management

XVIII. Before the installation of new hardware equipment, the power capacity should be assessed to avoid interruptions to important services due to power overload.

XIX. Fire extinguishers should be placed in server rooms and classrooms.

XX. Equipment, software, and media with saved information or sensitive documents must not be carried out of the server rooms or offices without authorization. The approval of the appropriate supervisor should be obtained first if such removals are necessary.

XXI. Information equipment that holds personal data should be kept in a safe place to prevent them from being stolen.

G. Communications and Operations Management

XXII. More than one person should be familiar with the information systems that are capable of affecting the operation and management of the businesses of departments. If job duties cannot be segregated due to limited manpower, measures such as supervision and auditing should be enhanced.

XXIII. A responsible person should be assigned for the main server and network equipment of each department to ensure the normal operation of the server. When the responsible person is unable to perform such management duties, a deputy should take over the job duty.

XXIV. In the event of changes to the network structure, building repairs, and the construction of new buildings, each department should notify the ITC before the scheduled construction date.

XXV. Firewalls should be set up for information systems, which should only allow access to necessary network services and communications.

XXVI. Suitable encryption technology should be used for e-mails or other electronic transmissions of sensitive data or documents.

XXVII. Application and approval procedures should be set up for the viewing of sensitive personal data. Reliable methods of transmission that keep the sensitive personal data confidential should be used.

XXVIII. Sensitive business information or documents must not be stored in information systems that are open to non-NTNU personnel. If doing so is required for special reasons, the information should be encrypted for the purpose of security and control.

XXIX. For information systems that are open to non-NTNU personnel, the transmission of sensitive information should be encrypted and kept safe to prevent the information from being stolen or transferred for other uses, which would lead to violations of privacy.

XXX. The competent authority should review and approve the information posted on websites

or in hard copy, making sure that no sensitive information, violations of intellectual property rights, or illegal information are involved.

XXXI. In principle, maintenance personnel or system suppliers maintaining information systems that involve personal data should not be allowed to connect via remote connection. If a remote connection is required for maintenance, security control technologies such as encrypted portals should be used when needed.

XXXII. The system's responsible person should regularly inspect and fix system vulnerabilities and update virus definitions in anti-virus software to keep the system functioning normally.

XXXIII. The system's responsible persons should periodically set up automatic backup or manual backup for the configuration files, webpage information, and database information in the information systems.

H. System Control Management

XXXIV. Segregation of duties should be taken into consideration when assigning personnel positions. Based on business needs, a deputy should be assigned for each job while conforming to the principle of segregation of duties as much as possible.

XXXV. Each person should primarily only access information assets that are related to their own job responsibilities. No personnel may access information assets outside the scope of their job responsibilities without permission.

XXXVI. Passwords that fulfill the safety control requirements should be set up for information systems.

XXXVII. The maintenance personnel of suppliers should have limited access to the system and data. Passwords should expire immediately after use; the use of a single, permanent password should be prohibited.

XXXVIII. The system manager should monitor, observe, and analyze the storage capacity of the system at all times to avoid suspension of service or data impairment due to insufficient capacity.

I. Development and Maintenance of the System

XXXIX. During the planning phase, critical security needs should be included in the system functions for the development of new information systems or the reinforcement of existing systems.

XL. Self-developed information systems or outsourced information systems for the processing of personal data should avoid using real personal data for testing. If real personal data is required, the identifiable personal information should be modified into unidentifiable and ambiguous information, and the data should be deleted immediately after the test.

XLI. When coding for webpage application programs, avoid writing unsafe source code and complete the relevant security testing and webpage vulnerability scanning before placing it online.

XLII. When designing exception handling mechanisms, avoid displaying the original complete error message in its entirety.

XLIII. A testing record for the testing of important system programs should be made. Furthermore, the testing record should be updated in case of major changes to the content of the programs and re-testing is required.

J. Outsourcing Management

XLIV. The procurer of the processing unit should request the outsourced suppliers to provide the relevant documents of the delivered equipment and tech support services, and also provide educational training courses if necessary.

XLV. If a system was developed by an outsourced supplier, the procurer of the processing unit should ask the supplier to provide documents that comprehensively record the system structure and specifications of the system.

XLVI. The procurer of the processing unit should ask the outsourced supplier and its personnel to comply with the Personal Data Protection Act and the relevant regulations of NTNU and sign the “Outsourced Supplier Affidavit of Confidentiality” and “Outsourced Supplier Personnel Affidavit of Confidentiality”.

XLVII. The procurer of the processing unit should ask the outsourced supplier to perform a technology security audit for the delivered system to ensure the security of the system, and the supplier should also provide the relevant security audit report.

XLVIII. For systems developed or maintained by outsourced suppliers, if security vulnerabilities are found in the system during the contract period, the procurer of the processing unit should ask the outsourced supplier to correct the problem; however, the method of correction and the delivery time should be approved by the processing unit.

XLIX. If the building of personal data files is outsourced, obligations of confidentiality for the personal data, relevant liabilities of information security, and the punishments of violation should be stated in the contract with outsourced suppliers.

K. Information Security Incident and Business Sustainable Operation Management

L. In the event of information security incidents, all departments must cooperate with the ITC for investigations and the restoration of operations.

LI. Clues and relevant records of major information security incidents should be kept for at least 6 months to serve as evidence of an investigation for the investigation agencies.

LII. After the information security incident, relevant departments should review the integrity of the existing control measures and formulate relevant operational regulations or establish and adjust the control measures to reinforce the security protection of the systems.

L. Miscellaneous

LIII. These guidelines have been approved by the Information Security Committee, and implemented with the approval of the President. The same applies to all subsequent amendments.