National Chengchi University Information Security Operation Guidelines

Passed at the 3rd meeting of the Information Security Promotion Committee on July 24, 2000
Amended and passed at the 5th meeting of the Information Security Promotion Committee on May 10, 2001
Amended and passed at the 6th meeting of the Information Security Promotion Committee on November 20, 2001
Amended and passed at the 14th meeting of the Information Security Promotion Committee on January 25, 2006
Amended and passed at the 16th meeting of the Information Security Promotion Committee on November 19, 2008
Amended and passed at the 18th meeting of the Information Security Promotion Committee on April 2, 2012
Amended and approved by the Information Security Promotion Committee on November 26, 2012, after approval by the President
Amended and approved by the Information Security and Personal Data Protection Implementation Committee on March 19, 2019, after approval by the President

A. Objective

I. In order to ensure the security of information collection, processing, transmission, storage, and circulation in all units of National Chengchi University (hereinafter referred to as "NCCU"), and to protect the rights and interests of faculty, staff, and students, NCCU has formulated these guidelines (hereinafter referred to as "the Guidelines") in accordance with the "Information Security Management Directions for the Executive Yuan and its Subordinate Agencies".

B. General provisions

II. The Guidelines shall be communicated in writing, electronically or otherwise to all faculty, staff, and students of NCCU, as well as public and private organizations operating online and vendors providing information services for joint compliance.

III. The Guidelines shall be evaluated at least once a year to follow the latest innovations in technology, business practices, and other related areas, in order to ensure the effectiveness of practical operations.

IV. If deemed necessary during the implementation of the Guidelines, each department shall create descriptive documents, such as management regulations, operating procedures, information security control documents, etc.

V. Information security shall be audited regularly or as needed.

C. Division of authority and responsibility

VI. When implementing the Guidelines, the division of authority and responsibilities is detailed as follows:

(I) The "Information Security and Personal Data Protection Implementation Committee" has been established to organize, coordinate, and discuss NCCU's various information security policies, plans, and resource allocation strategies. Regulations governing the establishment of this committee shall be separately established.

(II) Each information or management unit and its staff shall be responsible for the discussion, establishment, and evaluation of security plans and technical specifications for various computer software and hardware equipment, application systems, and network communications.

(III) Each relevant unit or its staff shall be responsible for handling the security requirements, use management, and protection of various data.

(IV) Matters related to information confidentiality and audit/use management shall be handled by the Secretariat in conjunction with relevant units.

D. Staff management

VII. Units of NCCU shall conduct safety assessments for information-related duties and work, and carefully assess the suitability of staff when hiring, assigning tasks, and working together, and conduct necessary assessments.

VIII. Each unit shall strengthen evaluation and assessment of staff who have access to confidential and sensitive information or systems, and staff who need to be assigned special access rights to systems on an ad hoc basis.

IX. Each unit shall conduct education, training, and awareness initiatives related to information security, tailored to the specific requirements of various job roles, including management, administration, and information technology, to establish information security awareness and improve the information security level of units.

X. Units shall strengthen the training of information security manpower and improve their information security management capabilities.

XI. Where a unit has insufficient information security manpower or experience, it may contact scholars, experts or professional institutions (organizations) to provide consulting services.

XII. The authority and responsibility of staff from units responsible for the management, maintenance, design, and operation of important information systems shall be appropriately distributed; in addition, check and balance mechanisms shall be established as necessary, as well as staff rotation measures and a manpower backup system.

XIII. The supervisors of each relevant unit shall be responsible for the information security operations of their staff and prevent illegal and improper behaviors.

E. Computer system security management

XIV. When a unit outsources information-related operations, it shall discuss the information security requirements in advance, clearly define the information security responsibilities and confidentiality regulations of the vendor, and include them in the contract, requiring the vendor to abide by and perform regular assessments.

XV. When a unit develops its own system or outsources the development of a system, it shall take information security needs into consideration at the initial stage of the system life cycle. System maintenance, updates, online execution and version change operations shall be safely managed to avoid unauthorized software, trapdoor, computer viruses, etc., from endangering system security.

XVI. It is the responsibility of each unit to manage and limit the scope of the systems and information accessible to the vendor’s personnel involved in the establishment and maintenance of software and hardware systems. In addition, issuing long-term system identification codes and passwords shall be strictly prohibited.

Based on actual operational needs, units may issue short-term and temporary system identification codes and passwords for vendors to use. However, such permissions shall be canceled immediately after the relevant tasks are completed.

Vendors entrusted by units to establish and maintain important software and hardware systems shall be supervised and accompanied by relevant staff of the unit.

XVII. Units shall establish a control mechanism for system change operations and create records for reference.

XVIII. The usage rights and responsibilities of units utilizing software shall be regulated by the Copyright Act and applicable contractual agreements.

Units shall establish software usage management mechanisms based on the "Guidelines for Computer Software Management of Administrative Agencies at All Levels of Government".

XIX. Units shall take the necessary preventive and protective measures to detect and prevent computer viruses and other malicious software, ensuring normal system operations.

F. Network security management

XX. Units that use public networks to transmit information or process transactions shall comply with the " Taiwan Academic Network Management and Norms "and shall assess potential security risks to determine the security requirements for data transmission, including integrity, confidentiality, identity authentication, and non-repudiation.

XXI. Units shall develop appropriate security control measures for data transmission, dial-up lines, network lines and equipment, external connection interfaces and routers, etc.

XXII. The websites connecting units to external networks must use firewalls or other security measures as necessary to control data transmission and resource access between external parties and the internal network of the unit.

XXIII. When their information systems are open to external connections, units shall, as necessary, adopt technologies or measures of different security levels, such as data encryption, identity authentication, electronic signatures, firewalls, and security vulnerability detection, depending on the importance and value of the data and system, in order to protect relevant data and systems from intrusion, destruction, tampering, deletion, and unauthorized access.

XXIV. When their information systems are open to external connections, units shall, as necessary, provide external access to data through proxy servers, among other methods, to prevent external parties from directly entering the information system or database to access data.

XXV. When using the Internet and global information networks to publish and circulate information, units shall implement data security level assessments. Units are prohibited from sharing online any information or documents that are confidential, sensitive, or related to personal privacy without obtaining consent from the relevant parties.

XXVI. Websites belonging to units that store personal information and files shall enhance their protective security strategies to avert the unlawful or inappropriate theft and utilization of personal privacy information.

XXVII. NCCU shall formulate rules for the use of emails. Confidential information and documents shall not be transmitted via email or other electronic means.

In cases where the electronic transmission of sensitive information and documents, excluding confidential materials, is necessary, NCCU shall use appropriate encryption or electronic signature measures, among other security technologies, to handle them as necessary.

When the type of business conducted by the unit requires it to transmit confidential information and documents via email or other electronic means, such unit shall implement encryption or electronic signature measures, among other security technologies, approved by the competent authority.

XXVIII. When purchasing information software and hardware equipment, units shall formulate information security requirements in accordance with national standards or government information security regulations set by the competent authority, and include them in the

procurement specifications.

Units developing and adopting encryption technology shall use cryptographic module products approved by the relevant competent authority.

When purchasing foreign-made cryptographic module products, units shall ask the vendor to provide an export license or relevant authorization documents to ensure the security of the cryptographic module, and avoid purchasing products with key escrow or key recovery functions.

G. System access control

XXIX. Units shall formulate system access policies and authorization regulations, and inform faculty, staff, students, and users of the relevant permissions and responsibilities via written documents, electronic channels, or by other means.

XXX. Units shall grant the necessary system access rights to staff at all levels in accordance with information security policies; system access rights shall be limited to those necessary to perform relevant tasks as stipulated by law. Units shall carefully evaluate staff who are given the highest access rights for system management and specific personnel in charge of important technical and operational control before being granted authorization.

XXXI. Units shall immediately cancel all permissions to access the various information resources on campus of staff from the various units of NCCU who have resigned (retired), and implement the necessary procedures for resigning (retired) staff.

The access rights of staff undergoing job adjustments and transfers in each unit shall be modified within the set time limit in accordance with system access authorization regulations.

XXXII. Units shall establish a registration management system for faculty, staff, students, and users, strengthen password management, and require regular updates. The frequency at which passwords are updated will be set by units, taking into account their specific operating systems and security management needs, but the maximum time allowed between updates shall not exceed six months.

For staff with special access rights to internal and external systems, units shall establish a staff roster to strengthen security control and minimize the interval for updating passwords.

XXXIII. Units that permit connections from external sources shall sign a contract or agreement in advance clearly stating the relevant information security regulations, standards, procedures, and responsibilities.

XXXIV. Units shall strengthen security control over system service providers who perform system maintenance through remote login methods, establish a staff roster, and assign relevant security and confidentiality responsibilities.

XXXV. When a unit's data is outsourced for filing, it is crucial for the unit to enforce adequate security control measures to prevent the theft, tampering, sale, leak, improper backup, etc., of data, whether the filing is conducted internally or externally.

XXXVI. Units shall set system audit items, establish an information security audit system, and conduct information security audit operations regularly or as necessary; The deletion and alteration of audit record files within systems is strictly forbidden.

H. Business continuity plans

XXXVII. Units shall formulate business continuity plans, assess the impact of various man-made and natural disasters on their normal business operations, formulate emergency response and recovery procedures, set the duties and responsibilities of relevant staff, and regularly conduct drills, adjusting and updating such plans accordingly.

XXXVIII. Units shall establish an emergency response mechanism for information security incidents. When such incidents occur, units shall immediately report to the responsible staff of the unit in accordance with the prescribed handling procedures. After taking the necessary response measures, NCCU shall contact the relevant agency to initiate legal action and conduct an investigation.

I. Other security measures

XXXIX. Units shall formulate and identify data security levels in accordance with relevant laws and regulations, and take appropriate and necessary information security measures according to different security levels.

XL. Units shall formulate appropriate equipment and environmental safety management measures regarding equipment placement, working environment, and staff access control.

J. Supplementary provisions

XLI. The Guidelines shall take effect after being approved by the President. The same shall apply to any amendments.