Content

Title：	Information Security Management Directions for the Executive Yuan and its Subordinate Agencies Ch
Date：	1999.09.15
Legislative：	Promulgated by Executive Yuan on September 15, 1999
Content：	I. Purpose 1. The Executive Yuan has promulgated these Directions to enhance agencies' information security management; establish a safe and reliable electronic government; ensure the security of information, systems, equipment and the Internet; and protect public rights. II. General Provisions 2. Agencies mentioned in these Directions refer to subordinate ministries, commissions, councils, banks, directorates-general, offices, administrations, museums, Taiwan Provincial Government, and Taiwan Provincial Consultative Council and its subordinate agencies (institutions). 3. Agencies should conduct information security risk assessments to establish the required security standards for various information operations, in accordance with relevant laws and regulations and in consideration of administration goals. Agencies should adopt appropriate and sufficient information security measures to ensure the security of agency information during collection, handling, transmission, storage and distribution. 4. The appropriate and sufficient information security measures mentioned in these Directions should take into consideration the overall importance and value of various information assets; inappropriate utilization; leakage, alteration and damage of agency information assets due to human error, deliberation, natural disasters or other risks; and the degree of impact on or damage to agency functions. The adopted management, operational and technical security measures should match the value and cost efficiency of information assets. 5. Agencies should promulgate the implementation of information security plans in accordance with the following matters, and evaluate implementation performance regularly: (1) Promulgation of information security policy. (2) Management framework for information security. (3) Personnel management, and information security education and training. (4) Computer systems security management. (5) Internet security management. (6) System access control management. (7) System development and maintenance of security management. (8) Security management of information assets. (9) Physical and environmental security management. (10) Management of sustainable operation plans for agency functions.

(11) Other information security management matters.

6. The information security policies mentioned in these Directions should refer to operational directions, measures, standards, and codes of conduct promulgated for achieving information security management goals.

III. Establishment of Information Security Policy

7. Agencies should promulgate information security policies in accordance with actual functions, and request compliance from their personnel, public or private institutions connected via the Internet, and information service providers via written communications, e-mail or other methods.

8. Information security policies promulgated by agencies should be reassessed at least once a year in consideration of the latest developments in government regulations, technologies and functions, and to ensure the effectiveness of information security operations.

IV. Organization and Accountability

9. Agencies should allocate roles and responsibilities to relevant departments and personnel in accordance with the following directions for labor division:

(1) The discussion, establishment and assessment of directions for information security policies, plans and technologies should be conducted by the information technology department.

(2) The department in charge of this function should be responsible for meeting requirements regarding the discussion, usage management and security protection for information and information systems.

(3) The civil service ethics department and related departments should be jointly responsible for maintaining information confidentiality, and auditing the utilization and management of information.

If organization has no delegated information department or civil service ethics departments, the agency head should appoint the appropriate department and personnel to carry out the above duties for agencies .

An agency head may adjust organization division directions prescribed in Paragraph 1 due to special nature of that agency’s functions.

10. Agencies should conduct information security audits on the information operations of subordinate agencies (institutions) on a regular or irregular basis.

Agencies’ information department should conduct external audit operations on subordinate agencies (institutions) jointly with the civil service ethics department or auditing department.

11. Agencies should appoint a deputy head or senior supervisors to be responsible for the coordination and promotion of information security management matters.

Agencies may establish an inter-ministerial promotion task force for information security with regard to the need to coordinate and discuss the overall planning of information security policies, plans, resource allocation and other matters.

The department appointed by the information department or agency head should be responsible for support operations of the information security task force mentioned in the preceding paragraph.

12. Agencies should appoint appropriate personnel to be responsible for matters related to information security with regard to information security management needs.

V. Personnel Management and Information Security Education and Training

13. Agencies should conduct a security assessment for information related duties and tasks, and assess the suitability of personnel during the employment process and when assigning duties and tasks. luations may be conducted necessarily.

14. Agencies should conduct regular information security management education, training and promotion, based on management needs, functions and information, to establish the information security awareness of personnel.

15. Agencies should enhance training for information security management personnel in order to improve their information security management capabilities.

Scholars, experts or professional agencies (institutions) may be invited to provide consulting services to agencies.

16. Agency personnel responsible for the management, maintenance, design and operation of important information systems should organize accountability, and establish a balance mechanism, implement personnel rotations, and develop a manpower support system with regard to agency requirements.

17. Agency heads and function supervisors at all levels should be responsible for supervising the security of information operations conducted by agency personnel to prevent illegal and inappropriate actions.

VI. Computer Systems Security Management

18. Agencies should propose information security needs when outsourcing information functions. Information security responsibilities and confidentiality directions for suppliers should be listed clearly and included in contracts for suppliers to comply with. Suppliers should be evaluated on a regular basis

19. Agencies should establish a control system for system modification operations, and keep records for later reference and evaluation.

20. Agencies should duplicate and utilize software, and establish software utilization management systems in accordance with relevant laws and regulations or contract regulations.

21. Agencies should adopt necessary preventive and protective measures in advance to detect and prevent computer viruses and other malicious software, in order to ensure normal operation of information systems.

VII. Internet Security Management

22. Agencies should assess possible security risks when transmitting information or conducting transactions via public networks, to ensure that security reuqirements, including the completeness of data transmitted, confidentiality, identity authentication and non-repudiation, are met. Agencies should also draft appropriate security control measures for data transmission, dial-up lines, Internet lines and equipment, external connection interfaces, and routers.

23. Agencies should carefully concern while open information systems for external connection operations of the importance and value of data and systems, and adopt data encryption, identity authentication, electronic signatures, firewalls, security vulnerability detection, and other technologies or measures at various security levels to prevent hacking, damage, alteration, deletion and unauthorized access to data and systems.

24. Agency websites connected to an external network should be equipped with a firewall and other necessary security equipment to control data transmission and resource access between external parties and the agency intranet.

25. When opening up information systems to external connection operations, agencies should ask external parties to access data via a proxy server to prevent these parties from entering the information system or database directly when accessing data.

26. Agencies should implement a data security rating assessment system when using the Internet and global information networks to publish and distribute information. Confidential, sensitive and private information and documents which may not be used without proper consent may not be published on the Internet.

Security protection measures should be enhanced for websites with personal data and files, to prevent private information from being stolen and used inappropriately or illegally.

27. Agencies should promulgate e-mail usage regulations. Confidential data and documents may not be transmitted via e-mail or other electronic methods.

Agencies should use encryption, electronic signatures or other security technologies for sensitive, confidential data and documents that need to be transmitted with regard to agency needs.

An agency may use security technologies, such as encryption or electronic signatures approved by the competent agency, for confidential data and documents transmitted via e-mail or other electronic methods due to special nature of that agency’s functions.

28. Agencies should procure information software and hardware in accordance with national standards or government information security directions promulgated by the competent agency, and propose information security requirements to be included in the procurement specifications.

Agencies should utilize encryption applications approved by the competent agency when developing and using encryption technologies.

Agencies should request manufacturers to produce an export permit or relevant authorization documents when purchasing encryption applications manufactured overseas, to ensure the security of these products and avoid the purchase of products with key escrow or key recovery function.

VIII. System Access Control Management

29. Agencies should promulgate system access policies and authorization directions, and inform staff and users about the relevant authority and responsibilities via written communication, e-mail or other methods.

30. Agencies should grant necessary system access authority to staff at different levels in accordance with information security policies with this access authority limited to those necessary for performing statutory duties. Staff granted with the highest level of system administration authority, and designated staff responsible for important technologies and operational control should be assessed carefully.

31. Agencies should terminate information and resource access authority for staff members who have resigned or are on leave, and include this as a mandatory procedure in the resignation and leave application process.

The access authority for agency personnel whose functions have been revised

or transferred should be adjusted before the stipulated deadline and in accordance with the directions for system access authorization.

32. Agencies should establish a user registration administration system to enhance the management of user passwords for access, and request users to update passwords regularly. An agency should determine the password update cycle, which should not exceed a six-month period, with regard to the operating system and security management needs.

Agencies should create a list of personnel with special access authority in order to enhance security control, and shorten their password update cycles.

33. When opening up information systems for external connection operations, external parties should sign contracts or agreements beforehand that prescribe directions, standards and procedures for information security, and responsibilities to be complied with.

34. Agencies should enhance security control and create a list of system service provider personnel who conduct system maintenance by remote log-in, in order to monitor them with relevant security and confidentiality responsibilities.

35. Appropriate and sufficient security control measures should be adopted for the filing of important agency information, inner or outer of the agency, to prevent such information from being stolen, modified, sold, leaked and duplicated improperly.

36. Agencies should establish system audit plan and an information security audit system. Information security audits should be conducted on a regular or irregular basis; deletion and alteration of audit records stored in systems should be prohibited.

IX. System Development and Maintenance of Security Management

37. Agencies should take information security requirements into consideration during the initial phase of the system's life cycle when developing systems independently or outsourcing system development. Security control should be established for the maintenance, update, online implementation, and version control to prevent improper software, trapdoors and computer viruses from damaging the system's security.

38. Agencies should prescribe standards and restrictions on the scope of systems and data that suppliers' software/hardware system development and maintenance personnel come in contact with, and strictly prohibit the issuance of long-term system identification and access passwords.

Agencies may issue short-term and temporary system identification and access passwords for suppliers, based on actual operational needs. However, access authority should be terminated immediately upon completion of duties.

39. Suppliers should only begin the construction and maintenance of important software and hardware for outsourced projects under the supervision and accompaniment of agency personnel.

X. Planning of Sustainable Function Operations

40. Agencies should promulgate a sustainable operation plan for agency functions, assess the impact of man-made and natural disasters on normal agency operations, establish emergency response and recovery procedures, prescribe the responsibilities of relevant personnel, conduct drills, and adjust and update plans regularly.

41. Agencies should establish an emergency management system for information security incidents. Emergency security incidents should be managed in accordance with the prescribed procedures and reported to the competent department or personnel immediately. Response measures should be adopted, and prosecution, police and investigative department should be contacted to assist investigations.

42. Agencies should establish and differentiate data security ratings in accordance with relevant laws and regulations, and adopt appropriate and sufficient information security measures.

XI. Others

43. Agencies should promulgate proper physical and environmental security management measures for equipment installation, the surrounding environment, and personnel access control.

XII. Supplementary Provisions

44. An agency may prescribe relevant directions separately due to special nature of that agency’s functions.

45. Municipal city or county (city) governments which have not promulgated directions for information security management may use these Directions.