Content

Title：	Enforcement Rules of the Cyber Security Management Act Ch
Date：	2026.01.05
Legislative：	1.On November 21, 2018, the Executive Yuan issued Order yuan tai hu zi No. 1070213547, promulgating 13 articles in full; the date those provisions come into effect will be set by the competent authority On December 5, 2018, the Order yuan tai hu zi No. 1070217128 promulgated by the Executive Yuan effective on January 1, 2019 2.On August 23, 2021, the Executive Yuan issued Order yuan tai hu zi No. 1100182012, amending Articles 6, 7 and 13; the amendments come into effect on the date of issuance On August 24, 2022, the Executive Yuan announced yuan tai gui zi No. 1110184307 that the duties listed under the “Executive Yuan” in Article 3, Paragraph 1 of Article 11, Article 12, and Paragraph 1 of Article 13 will be transferred to the “Ministry of Digital Affairs”, effective on August 27, 2022 3.On January 5, 2026, the Ministry of Digital Affairs issued Order shu shou zi fa zi No. 1145000413, amending and publishing the full text of 15 articles, the amendments come into effect on the date of issuance
Content：	Article 1 These Enforcement Rules are prescribed pursuant to Article 34 of the Cyber Security Management Act (hereinafter referred to as the “Act”). Article 2 The designated agency for cyber security referred to in Paragraph 2, Article 2 of the Act is the Administration for Cyber Security, Ministry of Digital Affairs. Article 3 As referred to in Subparagraph 5, Article 3 of the Act, “military agencies” refer to the Ministry of National Defense and its subordinate agencies (institutions), units, and schools; “intelligence agencies” refer to the agencies specified in Subparagraph 1, Paragraph 1 and Paragraph 2, Article 3 of the National Intelligence Work Act. Article 4 Before designating enterprises, organizations, or institutions controlled by the government pursuant to Subparagraph 10, Article 3 of the Act, the central competent authority in charge of the relevant sector shall provide them with an opportunity to present their views. The same requirement applies to the designation of critical infrastructure providers under Paragraph 1, Article 20 of the Act. Article 5 A “major cyber security incident” as defined in Subparagraph 5, Paragraph 1, Article 4 of the Act refers to an incident involving a private sector entity that meets one of the following criteria and poses a significant risk to social public interest, people’s daily lives, or economic activity, while also drawing substantial public attention: 1. Serious disclosure of core business information. 2. Serious tampering with core business information or core information and communication systems. 3. The operation of core information and communication systems is affected or interrupted, and cannot be restored to normal operation within the tolerable interruption time. Article 6

When government agencies or specific non-government agencies (hereinafter referred to as “agencies”) submit a corrective action report in accordance with Paragraph 2, Article 8; Paragraph 1, Article 16; Paragraph 5, Article 20; or Paragraph 3, Article 21 of the Act, they shall present the following information based on the audit findings regarding the implementation of their cyber security maintenance plans:
1. Items and content found deficient or requiring improvement.
2. Cause(s) of occurrence.
3. Measures implemented across management, technical, human resources, or other resource dimensions to correct deficiencies or strengthen areas requiring improvement.
4. The scheduled completion timeline for the aforementioned measures in the preceding subparagraph and the methods for tracking implementation progress.
Following submission of the corrective action report as stipulated in the preceding paragraph, agencies shall submit a report on the implementation status of the corrective action report within the timeframe and according to the procedures designated by the auditing agency.

Article 7
When agencies outsource the establishment, maintenance, or operation of information and communication systems, or the provision of information and communication services in accordance with Article 10 of the Act (hereinafter referred to as “outsourced services”), they shall pay attention to the following matters when selecting and supervising contractors:
1. The contractor shall be equipped with sufficient cyber security personnel who have undergone appropriate qualification training, hold cyber security professional certifications, or possess equivalent professional experience in related service areas.
2. Whether the outsourced services may be further subcontracted, the permissible scope of and counterparties for such subcontracting, and the cyber security maintenance measures to be adopted by subcontractors.
3. Personnel executing outsourced services that involve classified national security information shall undergo suitability reviews and be subject to exit restrictions in compliance with the Classified National Security Information Protection Act.
4. For outsourced services containing customized information and communication system development, the contractor must provide security testing certification. When the information and communication system is classified as a core information and communication system of the contracting agency or the contract value exceeds NT$10 million, the agency shall either perform its own security testing or engage a third party to conduct it. Where the use of systems or resources not developed by the contractor is involved, the non-self-developed content and its source shall be marked, and proof of authorization shall be provided.
5. When a contractor executes outsourced services and violates cyber security laws or regulations or becomes aware of any cyber security incidents, the contractor shall immediately notify the contracting agency and implement appropriate remedial measures.
6. Ensuring that upon termination or dissolution of the outsourcing relationship, the contractor returns, transfers, deletes, or destroys all data held in the course of contract performance.
7. Other cyber security and maintenance measures to be implemented by the contractor.
8. The contracting agency shall periodically, or upon learning of any cyber security incidents that may impact the outsourced services, verify the execution of such operations through audits or other suitable methods.
When conducting suitability reviews for Subparagraph 3 of the preceding paragraph, the contracting agency shall consider the classification level and content of classified national security information involved in the outsourced services. Within the necessary scope, it shall verify whether personnel of the contractor responsible for executing such business and other personnel who may have access to the classified national security information have any of the following circumstances:
1. Persons who have been convicted by a final judgment of any offense under

the Chapter of Offenses Against Computer Security of the Criminal Code, or who are currently wanted in unresolved cases related to such offenses.
2. Persons who have been convicted of Offenses of Disclosure of Secrets, or who, after the end of the period of national mobilization for suppression of communist rebellion, committed Offenses Against the Internal Security of the State or Offenses Against the External Security of the State, and have been convicted by a final judgment or are currently wanted in unresolved cases.
3. Persons who were previously employed as civil servants and received a disciplinary sanction or an administrative action of a demerit or heavier for violating relevant security and confidentiality regulations.
4. Persons who have been induced or coerced by a foreign government or authorities from Mainland Area, Hong Kong, or Macau to carry out actions that harm national security or the country's significant interests.
5. Other specific matters related to the protection of classified national security information.
Circumstances as described in Subparagraph 3, Paragraph 1 shall be documented in the tender announcement, tender documents, and contract. Prior to conducting suitability reviews, written consent from the persons concerned is also required.

Article 8
The third-party assistance mechanism as referred to in Paragraph 4, Article 10 of the Act refers to an impartial and professional institution that is independent from the competent authority, and the government agencies and specific non-government agencies participating in the drills.

Article 9
The cyber security maintenance plans specified in Article 13; Paragraph 2, Article 20; and Paragraph 1, Article 21 of the Act shall include the following items:
1. Core businesses and their significance.
2. Cyber security policies and goals.
3. Cyber security promotion organization.
4. Allocation of full-time staff and funding.
5. Appointment of a Chief Information Security Officer.
6. Inventory of information and communication systems and designation of core information and communication systems and related assets.
7. Cyber security risk management.
8. Cyber security protection and control measures.
9. The reporting, response, and drill mechanisms for cyber security incidents.
10. Mechanisms for assessing and responding to cyber security information.
11. Management measures for outsourced information and communication systems or services.
12. Performance evaluation mechanism for personnel whose duties involve cyber security matters.
13. Continuous improvement of cyber security maintenance plans and implementation status and performance management mechanisms.
Agencies shall include the execution results and relevant explanations of each subparagraph mentioned above when submitting reports on the implementation status of their cyber security maintenance plans as required under Article 14; Paragraph 3, Article 20; or Paragraph 2, Article 21 of the Act.
The formulation, revision, and implementation of cyber security maintenance plans referred to in Paragraph 1, as well as the submission of the implementation status referred to in the preceding paragraph, may be carried out by the receiving agency, its subordinate or supervised government agencies, or the following entities under its jurisdiction: township (town, city) offices, district offices of indigenous districts in special municipalities, township (town, city) representative councils, and representative councils of indigenous districts in special municipalities, provided that the government agency obtains the consent of the agency that receives the implementation status of its cyber security maintenance plan pursuant to Article 14 of the Act. For a specific non-government agency, the matters referred to in the preceding paragraph may, subject to the

consent of its central competent authority in charge of the relevant sector, be carried out by such central competent authority, or the subordinate or supervised government agencies or specific non-government agencies under the jurisdiction of such central competent authority.

Article 10
The scope of core businesses referred to in the Subparagraph 1, Paragraph 1 of the preceding article shall be as follows:
1. For government agencies, business that can be reasonably determined as falling within their core responsibilities and authority based on their organizational regulations.
2. Business necessary for each agency to operate, maintain, or provide critical infrastructure.
3. The primary services or functions of public enterprises, specific foundations, and government-controlled enterprises, organizations, or institutions.
4. Business operations of agencies involving the matters specified in Subparagraphs 1 to 5, Article 4, or Subparagraphs 1 to 5, Article 5 of the Regulations on Classification of Cyber Security Responsibility Levels.
The core information and communication system referred to in Subparagraph 6, Paragraph 1 of the preceding article refers to a system necessary to support the continuity of core business operations, or any system determined to have a high required defense level according to the provisions of Appendix 9, Principles for Classifying Protection Requirement Levels for Information and Communication Systems, of the Regulations Governing the Classification of Cyber Security Responsibility Levels.

Article 11
With respect to the superior agency as defined in Article 14 of the Act, the following shall apply at the central agency level:
1. Secondary agencies and independent agencies under the Office of the President and the Executive Yuan and secondary agencies under the Examination Yuan and the Control Yuan are, respectively, under the jurisdiction of the Office of the President, the Executive Yuan, the Examination Yuan, and the Control Yuan.
2. Agencies at the third level and below under the Executive Yuan, Examination Yuan, and Control Yuan are under the jurisdiction of the second-level agencies within their respective jurisdictions.
3. The courts directly under the Judicial Yuan and the Judges Academy are under the jurisdiction of the Judicial Yuan. The various branch courts, district courts, and the Taiwan Kaohsiung Juvenile and Family Court under the Taiwan High Court are under the jurisdiction of the Taiwan High Court. The local courts under the Fuchien High Court Kinmen Branch Court are under the jurisdiction of the Fuchien High Court Kinmen Branch Court.

Article 12
The investigation, handling, and corrective action report regarding cyber security incidents, as specified in Paragraph 3, Article 17 and Paragraph 3, Article 24 of the Act, shall include the following items:
1. The time of incident occurrence or discovery and the completion time of damage control and recovery operations.
2. Assessment of the incident’s impact scope and damage.
3. The progression of damage control and recovery operations.
4. The progression of incident investigation and handling procedures.
5. Root cause analysis of the incident.
6. Measures implemented across management, technical, human resources, or other resource dimensions to prevent the recurrence of similar incidents.
7. The scheduled completion timeline for the aforementioned measures in the preceding subparagraph and the performance tracking mechanism.

Article 13
The term “major cyber security incident” referred to in Paragraph 5, Article 17; Paragraph 2, Article 18; Paragraphs 3 and 5, Article 24; and Paragraphs 1 and 2, Article 25 of the Act refers to level 3 and level 4 cyber security incidents as defined in Paragraphs 4 and 5, Article 2 of the Regulations Governing the Reporting, Response and Drills for Cyber Security

Incidents.

Article 14
When the competent authority, the agency receiving reports on the implementation of cyber security maintenance plans as specified in Article 14 of this Act, or the central competent authority in charge of the relevant sector becomes aware of a major cyber security incident and announces the necessary contents and response measures related to the incident pursuant to Paragraph 5, Article 17 and Paragraph 5, Article 24 of this Act, it shall specify the time of occurrence or discovery of the incident, its cause, the extent of impact, the control status, and subsequent improvement measures.
Where the necessary content and response measures related to the incident in the preceding paragraph fall under any of the following circumstances, they shall not be publicly announced:
1. The information involving trade secrets or relating to business operations of an individual, juristic person, or group, the disclosure of which might infringe upon the rights or other legitimate interests of the government agency, individual, juristic person, or group, unless it is otherwise provided by law, necessary for the public interest or for the protection of the lives, bodies, or health of the people, or with the consent of the parties involved.
2. Other circumstances where the information shall be kept confidential, or its disclosure restricted or prohibited, pursuant to laws and regulations.
Where the necessary content and response measures related to the incidents in Paragraph 1 contain information that falls under the non-disclosure circumstances described in the preceding paragraph, only the remaining parts may be publicly announced.

Article 15
These Enforcement Rules shall come into effect on the date of promulgation.

Files： 資通安全管理法施行細則.pdf