Content

Title：	Regulations Governing the Handling of Cyber Security Matters by Personnel of Government Agencies Ch
Date：	2026.01.13
Legislative：	1. On November 21, 2018, the Executive Yuan issued Order yuan tai hu zi No. 1070213547, promulgating 7 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 4 and 7; 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 Subparagraph 3 of Article 3, Subparagraph 2 of Article 4, and Paragraph 1 of Article 7 will be transferred to the “Ministry of Digital Affairs”, effective on August 27, 2022 3. On January 13, 2026, the Ministry of Digital Affairs issued Order shu shou zi fa zi No. 1155000006, amending and publishing the title and full text of 24 articles, the amendments come into effect on the date of issuance (Former title: Regulations Governing the Commendation and Disciplinary Action of Cyber Security Affairs for Personnel From Government Agencies; New title: Regulations Governing the Operations of Cyber Security Affairs Handled by Personnel From Government Agencies)
Content：	Chapter I. General Provisions Article 1 These Regulations are prescribed pursuant to Paragraph 3, Article 18; Paragraph 6, Article 19; and Paragraph 2, Article 28 of the Cyber Security Management Act (hereinafter referred to as the “Act”). Article 2 In these regulations, cyber security personnel means dedicated cyber security personnel and any other personnel who actually engage in cyber security affairs. Dedicated cyber security personnel in the preceding paragraph means personnel who shall perform cyber security affairs on a full-time basis. Chapter II. Suitability Review Article 3 The phrase “when necessary” in Paragraph 1, Article 19 of the Act refers to cases where dedicated cyber security personnel fall under any of the following circumstances: 1. The affairs handled involve national secrets referred to in the Classified National Security Information Protection Act, or military secrets or national defense secrets referred to in the Guideline for Categories, Scopes and Levels of Military Secrets and Defense Secrets. 2. Other matters determined by a government agency, upon comprehensive assessment of the nature of its operations and the actual circumstances of its personnel. The term “successful candidates” in Paragraph 2, Article 19 of the Act means persons who have passed the cyber security personnel recruitment examination and meet the condition set out in Subparagraph 1 of the preceding paragraph.

Article 4
The following are the items for suitability reviews carried out under Paragraph 1 or 2, Article 19 of the Act:
1. Any of the circumstances specified in Paragraph 1, Article 28 of the Public Functionaries Appointment Act.
2. Persons who meet any of the conditions listed in Subparagraphs 1, 3, 8, or 10, Paragraph 1, Article 3 of the Regulations on Special Checks of Civil Servants Involved in National Security or Significant Interests.
3. Individuals who have been convicted by a final judgment of offenses against computer security as defined in the relevant chapter of the Criminal Code, or who are currently wanted in unresolved cases related to such offenses.
Where the circumstance set out in Subparagraph 1 of the preceding paragraph exists, the person shall be deemed to have failed the review.
When the circumstances described in Subparagraph 2 or 3, Paragraph 1 arise, the government agency must send the case to its Personnel Selection and Evaluation Committee to assess the seriousness and the nature of the intended position, then submit the committee's recommendation to the agency head for approval. Appointment decisions made by the head must include a written explanation of the reasons. When a review finds a potential threat to national security or significant interests, the review will be considered as failed.
In the event that the government agency referred to in the preceding Paragraph has not set up a Personnel Selection and Evaluation Committee, the matter shall be handled through another appropriate meeting.
Current civil servants who believe that the decisions mentioned in Paragraphs 2 and 3 are unlawful or clearly inappropriate and have harmed their rights or interests may seek remedies under the Civil Service Protection Act. Persons who are not incumbent civil servants may seek remedies under the Administrative Appeal Act.

Article 5
When a government agency or the competent authority conducts a suitability review, it shall, with the appended form attached, send an official request to the Ministry of Justice Investigation Bureau to conduct the review, and shall notify the individual concerned.
After the Ministry of Justice Investigation Bureau responds with the review results, the government agency or competent authority shall notify the individual concerned in writing within three days, counted from the day following receipt.

Article 6
Where the individual concerned considers the review results referred to in the preceding Article to be inconsistent with the facts, he or she may, within 15 days from receipt of the written notice, submit a statement and defense to the government agency or the competent authority, limited to one submission.
After receiving the statement and defense referred to in the preceding paragraph, the government agency or competent authority shall send an official request to the Ministry of Justice Investigation Bureau to conduct a renewed review.
After the Ministry of Justice Investigation Bureau responds with the renewed review results, the government agency or competent authority shall notify the individual concerned in writing within three days, counted from the day following receipt.

Article 7
Where the duties of dedicated cyber security personnel referred to in Paragraph 1, Article 19 of the Act are performed on an acting basis by the same incumbent personnel for more than three months, the provisions of this Chapter shall apply mutatis mutandis to the conduct of a suitability review.

Chapter III. Cyber Security Competency Training
Article 8
The competent authority shall plan and promote cyber security competency

training for dedicated cyber security personnel (hereinafter referred to as “cyber security competency training”) and handle the following matters:
1. Establishment and implementation of a cyber security competency training system.
2. Development of training materials for cyber security competency training.
3. Selection of training institutions and review of their instruction.
4. Formulation and implementation of a cyber security competency assessment and certification system.
5. Other matters concerning cyber security competency training.
The implementation methods for the matters set forth in Subparagraphs 1, 3, and 4 of the preceding paragraph shall be separately announced by the competent authority.

Article 9
Examinees who pass the cyber security competency assessment will be issued a cyber security competency training certificate by the competent authority.
When an examinee is confirmed upon verification to have cheated or committed other violations, the competent authority shall revoke their certificate.

Chapter IV. Mobilization
Article 10
Government agencies shall establish and maintain a roster of cyber security personnel, indicating the expertise and experience available for mobilization, and shall submit it for recordation in the manner specified by the competent authority; where any change occurs in the roster, the government agency shall notify the competent authority for updating.

Article 11
Mobilization shall be activated under the following circumstances:
1. When an agency experiencing a major cyber security incident (hereinafter referred to as the "affected agency") submits a support request in the manner specified by the competent authority because of urgent response needs.
2. When the competent authority determines that mobilization is necessary for a major cyber security incident.

Article 12
Mobilization includes damage control during incidents and other aspects of response to cyber security incidents.

Article 13
The competent authority may consider the following factors when deciding whether to mobilize:
1. The scale, nature, and geographic scope of the cyber security incident, as well as the degree of urgency for the required emergency response.
2. The allocation of cyber security personnel and their availability for mobilization across the affected agency itself, its affiliated agencies, supervised agencies, agencies under its jurisdiction, superior government agency, and the supervising agency or central competent authority in charge of the relevant sector.
3. The allocation of cyber security personnel and their availability for mobilization of the agency where mobilized cyber security personnel belongs (hereinafter referred to as the “supporting agency”).
4. Other relevant factors.
Where necessary for making the aforementioned decision, the competent authority may require the affected agency to provide explanations, cooperate, or submit relevant documents and supporting information.

Article 14
When the competent authority activates mobilization, it shall first consult the affected agency and the supporting agency.
Supporting agencies shall follow and carry out orders from the competent authority.

Article 15
When the competent authority activates mobilization, it must provide written notice to both the supporting agency and the affected agency. When notice cannot be given using the method described in the preceding paragraph for any reason, it may be sent by other appropriate means, and the required notification shall be provided afterwards in the prescribed manner.
The notice referred to in Paragraph 1 must include the following items:
1. The affected agency and the supporting agency.
2. Mobilization period and location.
3. Support needs and precautions.
4. Contact details for the competent authority, the affected agency, and the supporting agency.
5. Roster of support personnel.
6. Other precautions.
Each mobilization period shall not exceed seven days. Where the competent authority finds it necessary, it may grant one extension, but the extension may not exceed seven days.

Article 16
Personnel involved in mobilization must cooperate with the competent authority to document emergency response actions, improvement recommendations, and other related matters.

Article 17
Personnel involved in mobilization who, during the mobilization period, learn confidential and sensitive information of government or specific non-government agencies are required to keep that information confidential.

Chapter V. Commendation and Disciplinary Action
Article 18
Government agencies may, in accordance with these Regulations, set their own criteria for commendation and disciplinary action for cyber security matters handled by their personnel.

Article 19
The following situations qualify for commendation:
1. In accordance with the Act, regulations made under its authority or the agency’s internal rules, formulation, revision, and implementation of cyber security maintenance plans and achievement of outstanding performance.
2. Achievement of outstanding performance when conducting audits of the implementation of cyber security maintenance plans under Article 15 of the Act or cyber security drill operations.
3. Cooperation with the competent authority and the agencies designated under Article 15 of the Act in auditing the implementation of cyber security maintenance plans, conducting cyber security drills, or in the performance evaluations and commendation procedures for government agency cyber security tasks, and achievement of outstanding performance upon assessment.
4. Appropriate implementation of cyber security tasks to prevent cyber security incidents and thereby protect this agency, other agencies, or the public from damage.
5. Active identification of new types of cyber security vulnerabilities or intrusion threats and sharing of cyber security information to prevent incidents or minimize their damage.
6. Active monitoring of anomalies in cyber security maintenance, prompt detection of major cyber security incidents, and implementation of reporting and response measures to prevent further spread of damage.
7. Proposal and implementation of concrete suggestions or innovative solutions for cyber security tasks.
8. Management of training and cultivation of cyber security personnel, with tangible contributions.
9. Handling affairs concerning the research and development, integration, application, industry-academia collaboration, or industrial development of

cyber security technology, with tangible contributions.
10. Development of technical specifications for cyber security hardware and software, related services, and verification mechanisms, with tangible contributions.
11. Development of cyber security policies, legal analysis, or international cooperation efforts, with tangible contributions.
12. Cooperation with the competent authority in mobilization operations, with excellent performance or tangible contributions.
13. Development of other cyber security tasks, with tangible contributions.

Article 20
The following situations qualify for disciplinary action:
1. Failure to handle the following matters in accordance with the Act, regulations prescribed under the Act, or the agency's internal rules, where the circumstances are significant:
(1) Cyber security information sharing operations.
(2) Formulation, revision, and implementation of cyber security maintenance plans.
(3) Submission of reports on the implementation of cyber security maintenance plans.
(4) Audit of implementation of cyber security maintenance plans.
(5) Submission of a corrective action report in response to the audit results of the implementation of cyber security maintenance plans conducted by the competent authority and the agencies referred to in Article 15 of the Act.
(6) Establishment of reporting and response mechanisms for cyber security incidents.
(7) Reporting or response operations for cyber security incidents.
(8) Submission of investigation, handling, and corrective action reports regarding cyber security incidents.
2. Poor performance in handling cyber security affairs, as rated by the competent authority, a superior authority, or a supervisory authority, where guidance has proved ineffective and the circumstances are significant.
3. Other violations of the Act, regulations made under its authority, or an agency's internal rules in a serious circumstance.
4. Poor supervision of task operations resulting in their subordinates or personnel of affiliated units or supervised agencies falling in any circumstance of the preceding three subparagraphs.

Article 21
When a government agency carries out regular performance reviews of its personnel, it shall consider the commendation and disciplinary actions described in the preceding two articles. Reviews should be based on the actual causes and course of events, the individual's motives, purpose, methods, and conduct, and the effects of their actions. For personnel who are hired, on contract, or otherwise employed by the agency, any commendation or disciplinary action shall also be taken into account when deciding on renewal of appointment or employment.

Article 22
Before disciplining personnel for any situation under each subparagraph of Article 20, a government agency must give the person an opportunity for defense; where necessary, it may seek advice from relevant experts and scholars on the technical matters of cyber security.

Chapter VI. Supplementary Provisions
Article 23
The competent authority may delegate the suitability review, cyber security competency training, mobilization, commendation and disciplinary action procedures, and other related tasks set out in these regulations to the Administration for Cyber Security, Ministry of Digital Affairs.

Article 24
These Regulations shall come into effect on the date of promulgation.

Files：	公務機關所屬人員辦理資通安全事項作業辦法.pdf
Attachments：	公務機關所屬人員辦理資通安全事項作業辦法第五條附表.pdf

Data Source：Ministry of Digital Affairs Laws and Regulations Retrieving System