Content

Title：	Regulations Governing the Classification of Cyber Security Responsibility Levels Ch
Date：	2026.01.07
Legislative：	1.On November 21, 2018, the Executive Yuan issued Order yuan tai hu zi No. 1070213547, promulgating 12 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 26, 2019, the Executive Yuan issued Order yuan tai hu zi No. 1080184606, amending Articles 4, 5, 8, 11 and 12; the amendments come into effect on the date of issuance 3.On August 23, 2021, the Executive Yuan issued Order yuan tai hu zi No. 1100182012, amending Articles 5 ~ 7 and Schedules 1 ~8, 10 of Articles 11 On August 24, 2022, the Executive Yuan announced yuan tai gui zi No. 1110184307 that the duties listed under the “Executive Yuan” in Paragraphs 1, 3, 4, 5 of Article 3, Schedules 1 ~ 6 of Paragraph 1, Paragraphs 2, 3, 4 of Article 11, and Paragraph 1 of Article 12 will be transferred to the “Ministry of Digital Affairs”, effective on August 27, 2022. However, Paragraph 1 of Article 3, concerning the Executive Yuan’s approval of its own cyber security responsibility level remains under the jurisdiction of the “Executive Yuan”; the duty listed under the “Executive Yuan” in Paragraph 2 of Article 3 remains under the jurisdiction of the “Executive Yuan”, effective on August 27, 2022 4.On January 7, 2026, the Ministry of Digital Affairs issued Order shu shou zi fa zi No. 1145000416, amending and publishing Articles 1, 3, 10, 11
Content：	Article 1 These Regulations are prescribed pursuant to Paragraph 3, Article 7 of the Cyber Security Management Act (hereinafter referred to as the “Act”). Article 2 The cyber security responsibility levels of government agencies and specific non-government agencies (hereinafter referred to as “agencies”) shall, from highest to lowest, be classified as Level A, Level B, Level C, Level D, and Level E. Article 3 The Executive Yuan shall, every three years, approve its own cyber security responsibility level and submit it to the competent authority for recordation. Agencies directly under the Executive Yuan shall, every three years, submit the cyber security responsibility levels of their own, their subordinate or supervised government agencies, and the specific non-government agencies under their jurisdiction to the competent authority for approval. Special municipality and county(city) governments shall, every three years, submit the cyber security responsibility levels of their own, their subordinate or supervised government agencies, and the following entities under their 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, as well as the subordinate or supervised government agencies of the foregoing offices and councils, and shall report them to the competent authority for approval. Special

municipality and county(city) councils shall, every three years, submit their own cyber security responsibility levels to the competent authority for approval.
The Office of the President, the National Security Council, the Legislative Yuan, the Judicial Yuan, the Examination Yuan, and the Control Yuan shall, every three years, approve the cyber security responsibility levels of their own, their subordinate or supervised government agencies, and the specific non-government agencies under their jurisdiction, and submit them to the competent authority for recordation.
Where an agency is required to change its original cyber security responsibility level due to organizational or operational adjustments, it shall immediately handle the level change in accordance with the procedures set out in the preceding three paragraphs; the same shall apply where a new agency is established.
Where the government agencies under Paragraphs 1 through 3 handle the submission or approval of cyber security responsibility levels and deem it necessary to assign to a unit within a government agency or a specific non-government agency a level different from that of the agency itself, they may determine such level in accordance with Articles 4 through 10, taking into account the nature of the unit's business.

Article 4
Where an agency falls under any of the following circumstances, its cyber security responsibility level shall be Level A:
1. Its business involves national secrets;
2. Its business involves matters of foreign affairs, national defense, or homeland security;
3. Its business involves the maintenance and operation of information and communication systems for nationwide public services, or information and communication systems commonly used across government agencies;
4. Its business involves the possession of personal information files of the public nationwide or of public officials;
5. It is a government agency and its business involves matters of nationwide critical infrastructure;
6. It is a critical infrastructure provider, and the central competent authority in charge of the relevant sector, taking into account the number of users, market share, geographic scope, and substitutability of the critical infrastructure services they provide or maintain and operate, deems that failure of or impact on their information and communication systems would have catastrophic or severe adverse effects on social and public interests, public morale, or the life, body, or property of the people; or
7. It is a public medical center.

Article 5
Where an agency falls under any of the following circumstances, its cyber security responsibility level shall be Level B:
1. Its business involves the security maintenance and management of national core technology information funded, subsidized, or researched and developed by government agencies;
2. Its business involves the maintenance and operation of information and communication systems for regional or local public services, or information and communication systems commonly used across government agencies;
3. Its business involves the possession of personal information files of the public on a regional or local basis;
4. Its business involves the maintenance and operation of information and communication systems shared among central second-level agencies and the agencies (institutions) at all subordinate levels thereunder;
5. It is a government agency and its business involves matters relating to critical infrastructure on a regional or local basis;
6. It is a critical infrastructure provider and the central competent authority in charge of the relevant sector, taking into account the number of users, market share, geographic scope, and substitutability of the critical infrastructure services they provide or maintain and operate, deems that failure of or impact on their information and communication systems would have serious adverse effects on social and public interests,

public morale, or the life, body, or property of the people; or
7. It is a public regional hospital or district hospital.

Article 6
Agencies that maintain and operate information and communication systems established or developed by themselves or through outsourcing shall be classified as Level C.
The information and communication systems established by themselves or through outsourcing referred to in the preceding paragraph mean information and communication systems with differentiated access privileges and management functions.

Article 7
Agencies that handle their information and communication affairs on their own, but do not maintain or operate any information and communication system established or developed by themselves or through outsourcing, shall be classified as Level D.

Article 8
Where an agency falls under any of the following circumstances, its cyber security responsibility level shall be Level E:
1. It neither has an information and communication system, nor provides information and communication services;
2. It is a government agency and all its information and communication affairs are handled concurrently by or managed by its superior agency, supervisory agency, or a government agency designated by the foregoing agencies; or
3. It is a specific non-government agency, and all its information and communication affairs are concurrently handled or managed by its central competent authority in charge of the relevant sector, the subordinate government agencies of such authority, the specific non-government agencies under the jurisdiction of such authority, or the funding government agencies.

Article 9
Where an agency meets the criteria for two or more cyber security responsibility levels under Articles 4 through 8, its cyber security responsibility level shall be the highest of those levels.

Article 10
The cyber security responsibility levels of agencies shall be determined in accordance with the preceding six Articles. However, where a government agency submits or approves cyber security responsibility levels under Paragraphs 1 through 3 of Article 3, it may adjust the levels of agencies after taking into account the degree of impact that the following matters would have on national security, social and public interests, the life, body, or property of the people, or the reputation of the government agency concerned:
1. Where the business involves foreign affairs, national defense, homeland security, or critical infrastructure, the interruption or hindrance thereof;
2. Where the business involves personal information, official secrets, or other information required to be kept confidential by laws and regulations or by contract, the quantity and nature of such data, official secrets, or other information, and any unauthorized access, use, control, disclosure, damage, alteration, destruction, or other infringement thereof;
3. The functions of agencies being affected, failing, or interrupted, depending on their different hierarchical levels; or
4. Other specific matters relating to the provision, maintenance and operation, scale, or nature of information and communication systems.

Article 11
Agencies shall handle the matters set out in Appendices 1 through 8 in accordance with their cyber security responsibility levels.
Information and communication systems developed by agencies themselves or through outsourcing shall be classified in accordance with Principles for

	Classifying Protection Requirement Levels for Information and Communication Systems set out in Appendix 9, and the control measures set out in Appendix 10, Security Baselines for Information and Communication Systems, shall be implemented accordingly. Where the central competent authority in charge of the relevant sector of a specific non-government agency deems it necessary to prescribe separate defense standards for specific types of information and communication systems, it may draft such defense standards and submit them to the competent authority for approval, after which those standards shall apply. With the consent of their superior or supervisory agency, government agencies may apply mutatis mutandis the relevant provisions on defense standards prescribed by the central competent authority in charge of the relevant sector under the preceding paragraph; the same shall apply to other specific non-government agencies with the consent of their respective central competent authority in charge of the relevant sector. Where an agency, in handling the matters set out in Appendices 1 through 8 or implementing the control measures set out in Appendix 10, encounters manifest difficulty in handling or implementing a specific matter or control measure due to technical limitations or factors such as the design, structure, or nature of an individual information and communication system, it may, with the consent of the agency that submits its level under the latter part of Paragraph 1 and Paragraph 2 of Article 3, or of the agency that approves its level under the former part of Paragraph 1 and Paragraph 3 of the same Article, and after reporting to the competent authority for recordation, be exempted from handling or implementing that matter or control measure. Where the agency that submits the level falls under the foregoing circumstances, it may be exempted with the consent of the competent authority; where the agency that approves the level falls under such circumstances, it may be exempted after reporting to the competent authority for recordation. Government agencies shall, in the manner designated by the competent authority, submit the implementation status of the matters set out in Paragraphs 1 and 2. The central competent authority in charge of the relevant sector may require the specific non-government agencies under its jurisdiction to submit the implementation status of the matters set out in Paragraphs 1 and 2 in the manner it designates. Where agencies are required, as a result of amendments to Appendices 1 through 10, to add or modify items within a specified period, that period shall be calculated from the effective date of the amendments. Article 12 The effective date of these Regulations shall be prescribed by the competent authority. The amended provisions of these Regulations shall come into force on the date of promulgation.
Files：	資通安全責任等級分級辦法.pdf
Attachments：	附表一 資通安全責任等級A級之公務機關應辦事項.pdf 附表二 資通安全責任等級A級之特定非公務機關應辦事項.pdf 附表三 資通安全責任等級B級之公務機關應辦事項.pdf 附表四 資通安全責任等級B級之特定非公務機關應辦事項.pdf 附表五 資通安全責任等級C級之公務機關應辦事項.pdf 附表六 資通安全責任等級C級之特定非公務機關應辦事項.pdf 附表七 資通安全責任等級D級之各機關應辦事項.pdf 附表八 資通安全責任等級E級之各機關應辦事項.pdf 附表九 資通系統防護需求分級原則.pdf 附表十 資通系統防護基準.pdf