Content

Title：	Regulations Governing Cyber Security Information Sharing Ch
Date：	2026.01.05
Legislative：	1.On November 21, 2018, the Executive Yuan issued Order yuan tai hu zi No. 1070213547, promulgating 11 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 3 and 11; 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 Paragraphs 1, 2, 3 of Article 3, Article 9, Article 10 and Paragraph 1 of Article 11 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. 1145000409, amending and publishing the full text of 13 articles, the amendments come into effect on the date of issuance
Content：	Article 1 These Regulations are prescribed pursuant to Paragraph 2, Article 9 of the Cyber Security Management Act (hereinafter referred to as the “Act”). Article 2 The term "cyber security information" (hereinafter referred to as the "Information") as used in these Regulations refers to any of the following information: 1. Malicious reconnaissance or information gathering activities targeting information and communication systems. 2. Security vulnerabilities of information and communication systems. 3. Methods that render the security control measures of information and communication systems ineffective or exploit security vulnerabilities. 4. Information related to malware. 5. The actual damage or possible negative impact caused by cyber security incidents. 6. Relevant measures for detecting, preventing, or responding to the circumstances set out in the preceding five subparagraphs, or for mitigating the damage thereof. 7. Other information relating to cyber security incidents. Article 3 The competent authority shall conduct international cooperation regarding the sharing of the Information. The competent authority and government agencies shall mutually share the Information. The central competent authority in charge of the relevant sector and the specific non-government agencies under its jurisdiction shall mutually share the Information. Except for the competent authority or the central competent authority in charge of the relevant sector, other government agencies or specific non-government agencies are not required to re-share the Information that has already been shared or publicly disclosed. Where the competent authority or the central competent authority in charge of the relevant sector determines that the Information shared under Paragraph 2 or 3 is sufficient to prevent the occurrence of cyber security

incidents in other agencies or to mitigate the resulting damage, the competent authority or the central competent authority in charge of the relevant sector may grant commendations.

Article 4
The Information under any of the following circumstances shall not be shared:
1. Information involving trade secrets or relating to the business operations of an individual, juristic person, or group, the disclosure or provision of which would infringe upon the rights or other legitimate interests of a government agency, individual, juristic person, or group; provided, however, that this restriction shall not apply where it is otherwise provided by laws and regulations, is necessary for the public interest or for the protection of the lives, bodies, or health of the people, or is made with the consent of the parties concerned.
2. Other circumstances where information is required by laws or regulations to be kept confidential or its disclosure is restricted or prohibited.
Where the Information contains content that shall not be shared pursuant to the preceding paragraph, only the remaining parts may be shared.

Article 5
In sharing the Information, government agencies or specific non-government agencies (hereinafter referred to as “agencies”) shall first analyze and integrate the Information and shall plan appropriate security maintenance measures to prevent the content of the Information, or any information that shall not be shared under laws or regulations, from being leaked, accessed without authorization, or tampered with.

Article 6
For the Information received, agencies shall identify the reliability and timeliness of their sources, conduct timely threat and vulnerability analysis, assess potential risks, and take corresponding prevention or response measures.
The competent authority or the central competent authority in charge of the relevant sector may notify the agencies receiving the designated Information to report back on the measures referred to in the preceding paragraph.

Article 7
Agencies may conduct correlation analysis and integration with their internal Information based on the source, date of receipt, period of availability, and types of the information, the characteristics of threat indicators, and other appropriate matters.
Agencies shall share the Information regarding new types of threats identified through the analysis and integration referred to in the preceding paragraph.

Article 8
For the Information received, agencies shall take appropriate security maintenance measures to prevent the content of the Information, or any information that shall not be shared under laws or regulations, from being leaked, accessed without authorization, or tampered with.

Article 9
In sharing the Information, agencies shall proceed in the respective manner designated by the competent authority or the central competent authority in charge of the relevant sector.
Where agencies are unable for any reason to share the Information in the manner prescribed in the preceding paragraph, they may, with the consent of the competent authority or the central competent authority in charge of the relevant sector, respectively, use one of the following methods:
1. In writing.
2. By fax.
3. By email.
4. Through an information and communication system.
5. By other appropriate methods.

Article 10
Individuals, juristic persons, or groups not subject to the Act may mutually share the Information with the consent of the competent authority or the central competent authority in charge of the relevant sector.
In giving consent to individuals, juristic persons, or groups for sharing the Information under the preceding paragraph, the competent authority or the central competent authority in charge of the relevant sector shall enter into a written agreement with them stipulating that they shall comply with the provisions of Articles 4 through 9.

Article 11
Where information and communication systems, services, or products are deemed to raise concerns of harm to national cyber security, the matter shall be handled in accordance with the Regulations for the Review of Products Harmful to National Cyber Security.

Article 12
The competent authority may delegate matters relating to sharing the Information, commendations, and other related matters set out in these Regulations to the Administration for Cyber Security, Ministry of Digital Affairs.

Article 13
These Regulations shall come into effect on the date of promulgation.

Files： 資通安全情資分享辦法.pdf