

資通安全情資分享辦法-英譯對照

資通安全情資分享辦法	Cyber Security Information Sharing Regulations
<p>第一條 本辦法依資通安全管理法（以下簡稱本法）第八條第二項規定訂定之。</p>	<p>Article 1 These Regulations are stipulated in accordance with Paragraph 2 of Article 8 of the Cyber Security Management Act (hereinafter referred to as the Act).</p>
<p>第二條 本辦法所稱資通安全情資（以下簡稱情資），指包括下列任一款內容之資訊：</p> <ol style="list-style-type: none"> 一、資通系統之惡意偵察或情蒐活動。 二、資通系統之安全漏洞。 三、使資通系統安全控制措施無效或利用安全漏洞之方法。 四、與惡意程式相關之資訊。 五、資通安全事件造成之實際損害或可能產生之負面影響。 六、用以偵測、預防或因應前五款情形，或降低其損害之相關措施。 七、其他與資通安全事件相關之技術性資訊。 	<p>Article 2 The term cyber security information (hereinafter referred to as the Information) as used in these Regulations refers to the information containing any of the following contents:</p> <ol style="list-style-type: none"> 1. Malicious detections or collections activity of information and communication system. 2. Security vulnerabilities of information and communication system. 3. The methods that invalidate the information and communication systems security control measure or make use of the security vulnerability. 4. The information relating to malicious programs. 5. The actual damage or possible negative impact caused by cyber security incident. 6. Relevant measures that are taken to detect, prevent from or respond to the circumstances under the preceding five subparagraphs or to mitigate the damage. 7. Other technical information relating to cyber security incidents.
<p>第三條 主管機關應就情資分享事宜進行國際合作。</p> <p style="padding-left: 2em;">主管機關應適時與公務機關進行情資分享。</p> <p style="padding-left: 2em;">公務機關應適時與主管機關進行情資分享。但情資已依前項規定分享或已經公開者，不在此限。</p> <p style="padding-left: 2em;">中央目的事業主管機關應適時與其所管之特定非公務機關進行情資分享。</p> <p style="padding-left: 2em;">特定非公務機關得與中央目的事業主管機關進行情資分享。</p>	<p>Article 3 The competent authority shall conduct international cooperation in the matters of cyber security information sharing.</p> <p style="padding-left: 2em;">The competent authority shall timely conduct cyber security information sharing with the government agencies.</p> <p style="padding-left: 2em;">The government agency shall timely conduct cyber security information sharing with the competent authority, unless such information has been shared under the preceding paragraph or has been disclosed.</p> <p style="padding-left: 2em;">The central authority in charge of relevant industry shall timely conduct cyber security information sharing with the specific non-government agency under their charge.</p> <p style="padding-left: 2em;">The specific non-government agency may conduct</p>

	cyber security information sharing with the central authority in charge of relevant industry.
<p>第四條 情資有下列情形之一者，不得分享：</p> <p>一、涉及個人、法人或團體營業上秘密或經營事業有關之資訊，其公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益。但法規另有規定，或對公益有必要，或為保護人民生命、身體、健康有必要，或經當事人同意者，不在此限。</p> <p>二、其他依法規規定應秘密或應限制、禁止公開之情形。</p> <p>情資含有前項不得分享之內容者，得僅就其他部分分享之。</p>	<p>Article 4 The cyber security information under any of the following circumstances may not be shared:</p> <ol style="list-style-type: none"> 1. The information involving business secret or relating to business operation of individual, juristic person or group, of which the disclosure or provision might infringe upon right or other legitimate interest of the government agency, individual, juristic persons or group; unless it is otherwise provided by law, or necessary for public welfare, or necessary for the protection of the lives, bodies or health of the people, or with consent of the party involved. 2. Other circumstances under which cyber security information should be kept confidential, should be restricted on or prohibited from disclosure thereof. <p>Cyber security information containing contents that may not be shared under the preceding paragraph may be shared to the extent of other portions only.</p>
<p>第五條 公務機關或特定非公務機關(以下簡稱各機關)進行情資分享，應就情資進行分析及整合，並規劃適當之安全維護措施，避免情資內容、個人資料或依法規規定不得分享之資訊外洩，或遭未經授權之存取或竄改。</p>	<p>Article 5 In conducting cyber security information sharing, the government agency or the specific non-government agency(hereinafter referred to as each agency)shall analyze and integrate the information and shall plan the appropriate security maintenance measure to prevent breach of the content of the information, personal information, or information that may not be shared under laws; or the unauthorized access thereto or the tampering thereof.</p>
<p>第六條 各機關應就所接受之情資，辨識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施。</p>	<p>Article 6 For the cyber security information received, each agency shall identify its reliability and timeliness, shall timely conduct an analysis of threat and vulnerability and make the judgment of potential risk, and shall take corresponding prevention or contingency measure.</p>
<p>第七條 各機關進行情資整合時，得依情資之來源、接收日期、可用期間、類別、威脅指標特性及其他適當項目與內部情資進行關聯分析。</p> <p>公務機關應就整合後發</p>	<p>Article 7 In conducting cyber security information integration, each agency may conduct the correlation analysis with their internal information based on the source, date of receipt, available periods, and kinds of the information, the extent of threat index, and other proper</p>

<p>現之新型威脅情資進行分享。</p>	<p>items. The government agency may conduct the cyber security sharing of the new threat that is found after the integration.</p>
<p>第八條 各機關應就所接收之情資，採取適當之安全維護措施，避免情資內容、個人資料或依法規規定不得分享之資訊外洩，或遭未經授權之存取或竄改。</p>	<p>Article 8 For the cyber security information received, each agency shall take appropriate security measures to prevent the breach of the content of cyber security information, personal information or information that may not be shared under laws; or the unauthorized access thereto or the tampering thereof.</p>
<p>第九條 各機關進行情資分享，應分別依主管機關或中央目的事業主管機關指定之方式為之。 各機關因故無法依前項規定方式進行情資分享者，分別經主管機關或中央目的事業主管機關同意後，得以下列方式之一為之： 一、 書面。 二、 傳真。 三、 電子郵件。 四、 資訊系統。 五、 其他適當方式。</p>	<p>Article 9 In conducting cyber security information sharing, each agency shall follow the procedure as designated by the competent authority or the central authority in charge of relevant industry, respectively. If conducting cyber security information sharing in the manner under the preceding paragraph is prevented for any reason, each agency may conduct it in any of the following manners with the consent of the competent authority or the central authority in charge of relevant industry, respectively: 1. Written documents. 2. Fax. 3. Email. 4. Information system. 5. Other appropriate manner.</p>
<p>第十條 未適用本法之個人、法人或團體，經主管機關或中央目的事業主管機關同意後，得與其進行情資分享。 主管機關或中央目的事業主管機關同意前項個人、法人或團體進行情資分享，應以書面與其約定應遵守第四條至前條之規定。</p>	<p>Article 10 Individual, juristic person or organization, to whom the Act is not applicable, may conduct cyber security information sharing, with the consent of the competent authority or the central authority in charge of relevant industry. In giving consent to individual, juristic person or organization for cyber security information sharing under the preceding paragraph, the competent authority or the central authority in charge of relevant industry shall agree with them in writing on the provisions of compliance with the requirements under Article 4 to the preceding article.</p>
<p>第十一條 本辦法施行日期，由主管機關定之。</p>	<p>Article 11 The date for enforcement of these Regulations shall be decided by the competent authority.</p>