

資通安全管理法-英譯對照

資通安全管理法	Cyber Security Management Act
第一章 總則	Chapter I. General Provision
第一條 為積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益，特制定本法。	Article 1. This Cyber Security Management Act (hereinafter referred to as the Act) is duly stipulated in an effort to positively carry out the national cyber security policy, accelerate the construction of environment for national cyber security to safeguard national security, and protect public interests of the entire society.
第二條 本法之主管機關為行政院。	Article 2. The competent authority over the Act is the Executive Yuan.
<p>第三條 本法用詞，定義如下：</p> <p>一、資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。</p> <p>二、資通服務：指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。</p> <p>三、資通安全：指防止資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。</p> <p>四、資通安全事件：指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。</p> <p>五、公務機關：指依法行使公權力之中央、地方機</p>	<p>Article 3. The terms under the Act are defined as follows:</p> <ol style="list-style-type: none"> 1. Information and communication system: That refers to the system to be used to collect, control, transmit, store, circulate, delete information or to make other processing, using and sharing of such information. 2. Information and communication service: That refers to the service to be used to collect, control, transmit, store, circulate, delete information or to make other processing, use and sharing of such information. 3. Cyber security: That refers to such effort to prevent information and communication system or information from being unauthorized access, use, control, disclosure, damage, alteration, destruction or other infringement to assure the confidentiality, integrity and availability of information and system. 4. Cyber security incident: That refers to an event where the state of the system, service or network ,through identification, likely shows violation of the cyber security policy, or failure of the security protective measures, thus adversely affect performance of information and communication system function, and constitute a threat against the cyber security policy. 5. Government agency: That refers to central, local government agency (institution) or public juristic person that exercises public power according to law,

<p>關（構）或公法人。但不包括軍事機關及情報機關。</p> <p>六、特定非公務機關：指關鍵基礎設施提供者、公營事業及政府捐助之財團法人。</p> <p>七、關鍵基礎設施：指實體或虛擬資產、系統或網路，其功能一旦停止運作或效能降低，對國家安全、社會公共利益、國民生活或經濟活動有重大影響之虞，經主管機關定期檢視並公告之領域。</p> <p>八、關鍵基礎設施提供者：指維運或提供關鍵基礎設施之全部或一部，經中央目的事業主管機關指定，並報主管機關核定者。</p> <p>九、政府捐助之財團法人：指其營運及資金運用計畫應依預算法第四十一條第三項規定送立法院，及其年度預算書應依同條第四項規定送立法院審議之財團法人。</p>	<p>excluding military and intelligence agency.</p> <p>6. Specific non-government agency: That refers to critical infrastructure provider, government-owned enterprises and government-endowed foundation.</p> <p>7. Critical infrastructure: That refers to asset, system or network, either physical or virtual, once discontinued from operation or becoming less effective, would lead to significant negative impact upon the national security, public interests, living standard of citizen and economic activities. Which shall be re-examined and promulgated by the competent authority regularly.</p> <p>8. Critical infrastructure provider: That refers to the ones who maintain or provide critical infrastructure either in whole or in part, as designated by the central authority in charge of relevant industry, which shall be submitted to the competent authority for ratification.</p> <p>9. Government-endowed foundation: That refers to a foundation of which the operation and capital employment plan of its funds shall be submitted to the Legislative Yuan in accordance with Paragraph 3 of Article 41 of the Budget Act and its annual budget statement shall be submitted to the Legislative Yuan for deliberation in accordance with Paragraph 4 of the same Article.</p>
<p>第四條 為提升資通安全，政府應提供資源，整合民間及產業力量，提升全民資通安全意識，並推動下列事項：</p> <p>一、資通安全專業人才之培育。</p> <p>二、資通安全科技之研發、整合、應用、產學合作及國際交流合作。</p> <p>三、資通安全產業之發展。</p> <p>四、資通安全軟硬體技</p>	<p>Article 4. In an effort to promote cyber security, the government shall provide resources, and integrate the momentum of both civilian groups and private sectors, and boost cyber security awareness of all people, and implement the following issues:</p> <p>1. Cultivation of cyber security professionals.</p> <p>2. Cyber security technology research and development, integration, application, and industry-academia cooperation, as well as interchange and cooperation with international community.</p> <p>3. Development of cyber security industry.</p> <p>4. Development of cyber security related software and</p>

<p>術規範、相關服務與審驗機制之發展。</p> <p>前項相關事項之推動，由主管機關以國家資通安全發展方案定之。</p>	<p>hardware specifications, relevant services and verification mechanism.</p> <p>Issues Promotion in the preceding Paragraph shall be stipulated by the competent authority under the national cyber security program.</p>
<p>第五條 主管機關應規劃並推動國家資通安全政策、資通安全科技發展、國際交流合作及資通安全整體防護等相關事宜，並應定期公布國家資通安全情勢報告、對公務機關資通安全維護計畫實施情形稽核概況報告及資通安全發展方案。</p> <p>前項情勢報告、實施情形稽核概況報告及資通安全發展方案，應送立法院備查。</p>	<p>Article 5. The competent authority shall plan and promote the cyber security policy, and the cyber security technology development, and interchange and cooperation with international community, and the comprehensive cyber security protection relevant undertakings, as well as announce the report of national cyber security status, the summary auditing report on the implementation of the cyber security maintenance plan for the government agency, and the national cyber security program.</p> <p>The status report, summary auditing report and the national cyber security programs of the preceding Paragraph shall be submitted to the Legislative Yuan for review.</p>
<p>第六條 主管機關得委任或委託其他公務機關、法人或團體，辦理資通安全整體防護、國際交流合作及其他資通安全相關事務。</p> <p>前項被委託之公務機關、法人或團體或被複委託者，不得洩露在執行或辦理相關事務過程中所獲悉關鍵基礎設施提供者之秘密。</p>	<p>Article 6. The competent authority may commission or entrust other government agency, juristic person or organization to implement integrated protection of cyber security, interchange and cooperation with international community, and other cyber security related issues.</p> <p>The government agency, juristic person or organization, or second-tier subcontractor of the preceding Paragraph shall not divulge the secret of critical infrastructure provider which becomes known in the process of enforcement or implement of relevant issues.</p>
<p>第七條 主管機關應衡酌公務機關及特定非公務機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，訂定資通安全責任等級之分級；其分級基準、等級變更申請、義務內容、專責人員之設置及其他相關事項之辦法，由主</p>	<p>Article 7. The competent authority shall stipulate the cyber security responsibility levels by considering the criteria on the importance, confidentiality and sensitivity of the business, the hierarchy of the agency, and the category, quantity and attribute of the information reserved or processed, as well as the scale and attribute of the information and communication system of the government agency and specific non-government agency. The relevant regulations regard the baseline for responsibility levels, application for a change in the level, content of obligation,</p>

<p>管機關定之。</p> <p>主管機關得稽核特定非公務機關之資通安全維護計畫實施情形；其稽核之頻率、內容與方法及其他相關事項之辦法，由主管機關定之。</p> <p>特定非公務機關受前項之稽核，經發現其資通安全維護計畫實施有缺失或待改善者，應向主管機關提出改善報告，並送中央目的事業主管機關。</p>	<p>staffing of dedicated personnel and other regulations and issues concerned shall be stipulated by the competent authority.</p> <p>The competent authority may audit a specific non-government agency in its implementation of cyber security maintenance plan, of which the frequency, content, method and other issues concerned shall be stipulated by the competent authority.</p> <p>A specific non-government agency is audited as per preceding Paragraph, and found defective or needing improvement in the cyber security maintenance program, it shall submit the improvement report to the competent authority and to the central authority in charge of relevant industry.</p>
<p>第八條 主管機關應建立資通安全情資分享機制。</p> <p>前項資通安全情資之分析、整合與分享之內容、程序、方法及其他相關事項之辦法，由主管機關定之。</p>	<p>Article 8. The competent authority shall set up the cyber security information sharing mechanism.</p> <p>Regulation regarding analysis, integration, and the sharing of content, procedure and method, and other matters of the cyber security information in the preceding Paragraph shall be stipulated by the competent authority.</p>
<p>第九條 公務機關或特定非公務機關，於本法適用範圍內，委外辦理資通系統之建置、維運或資通服務之提供，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。</p>	<p>Article 9. A government agency or specific non-government agency outsources for setup, maintenance of the cyber security system, or for provision of cyber security services, such government agency or specific non-government agency shall, within the realm of this Act, take into account outsourced party's professional capability and hands-on experience, as well as attribute of the outsourced item and requirement of cyber security, select the appropriate party for outsourcing and oversee its cyber security maintenance service.</p>
<p>第二章 公務機關資通安全管理</p>	<p>Chapter II. Government Agency Cyber Security Management</p>
<p>第十條 公務機關應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實</p>	<p>Article 10. A government agency shall satisfy the requirements of the cyber security responsibility level, and take into account the category, quantity and attribute of the information reserved or processed, along with the scale and attribute of the information and communication system, to stipulate,</p>

施資通安全維護計畫。	amend and implement the cyber security maintenance plan.
第十一條 公務機關應置資通安全長，由機關首長指派副首長或適當人員兼任，負責推動及監督機關內資通安全相關事務。	Article 11. A government agency shall staff the position of Cyber Security Officer, which to be concurrently served by the deputy head or other appropriate personnel as designated by the agency head. The Cyber Security Officer shall assume the responsibility to carry out and oversee the cyber security business of the agency.
第十二條 公務機關應每年向上級或監督機關提出資通安全維護計畫實施情形；無上級機關者，其資通安全維護計畫實施情形應送交主管機關。	Article 12. A government agency shall submit to the superior or supervisory authority about the implementation of the cyber security maintenance plan annually. Without such superior authority, the implementation report of the cyber security maintenance program shall be submitted to the competent authority.
第十三條 公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。 受稽核機關之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交稽核機關及上級或監督機關。	Article 13. A government agency shall audit the subordinate authority under its supervision about the implementation of the cyber security maintenance plan. When an agency is audited and found defective or needing improvement in the cyber security maintenance plan, it shall submit the improvement report to the auditing agency and the superior or the supervisory authority.
第十四條 公務機關為因應資通安全事件，應訂定通報及應變機制。 公務機關知悉資通安全事件時，除應通報上級或監督機關外，並應通報主管機關；無上級機關者，應通報主管機關。 公務機關應向上級或監督機關提出資通安全事件調查、處理及改善報告，並送交主管機關；無上級機關者，應送交主管機關。 前三項通報及應變機制之必要事項、通報內容、報告之提出及其他相關事項之辦法，由主管機關定之。	Article 14. To cope with cyber security incident, a government agency shall stipulate the reporting and responding mechanism. When privy to a cyber security incident, the government agency shall report to the superior or supervisory authority as well as to the competent authority. Without such superior authority, the government agency shall report to the competent authority. A government agency shall file a report on the investigation, handling and improvement on the cyber security incident, and shall submit the report to the superior or supervisory authority as well as the competent authority. Without a superior authority, the government agency shall submit to the competent authority. Regulations regarding the essentials of the reporting and responding mechanism, content of notification, submittal of report and other matters in the three preceding Paragraphs shall be stipulated by the competent authority.

<p>第十五條 公務機關所屬人員對於機關之資通安全維護績效優良者，應予獎勵。</p> <p>前項獎勵事項之辦法，由主管機關定之。</p>	<p>Article 15. Personnel with proven performance in cyber security maintenance, a government agency shall present incentive award.</p> <p>Regulations for such incentive award in the preceding Paragraph shall be stipulated by the competent authority.</p>
<p>第三章 特定非公務機關資通安全管理</p>	<p>Chapter III. Specific Non-Government Agency Cyber Security Management</p>
<p>第十六條 中央目的事業主管機關應於徵詢相關公務機關、民間團體、專家學者之意見後，指定關鍵基礎設施提供者，報請主管機關核定，並以書面通知受核定者。</p> <p>關鍵基礎設施提供者應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。</p> <p>關鍵基礎設施提供者應向中央目的事業主管機關提出資通安全維護計畫實施情形。</p> <p>中央目的事業主管機關應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。</p> <p>關鍵基礎設施提供者之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交中央目的事業主管機關。</p> <p>第二項至第五項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主</p>	<p>Article 16. The central authority in charge of relevant industry shall, after consulting with the relevant government agency, civil associations, scholars and experts for their opinions, designate the critical infrastructure provider and submit to the competent authority for approval, while notifying the approved provider in writing.</p> <p>A critical infrastructure provider shall satisfy the requirements of the cyber security responsibility level , and take into account the category, quantity and attribute of the information reserved or processed, along with the scale and attribute of the information and communication system, to stipulate, amend and implement the cyber security maintenance plan.</p> <p>A critical infrastructure provider shall submit to the central authority in charge of relevant industry about the implementation of the cyber security maintenance plan.</p> <p>The central authority in charge of relevant industry shall audit the critical infrastructure provider about the implementation of the cyber security maintenance plan.</p> <p>When a critical infrastructure provider is audited and found defective or needing improvement in the cyber security maintenance plan, it shall submit the improvement report to the central authority in charge of relevant industry.</p> <p>Regulations regarding the essentials of the cyber security maintenance plan, and submittal of the implementation, audit frequency, contents and methods, submittal of the improvement reports and other matters in Paragraph 2 to Paragraph 5 shall be drafted by the central authority in charge of relevant industry, and submit to the competent authority for approval.</p>

<p>管機關擬訂，報請主管機關核定之。</p>	
<p>第十七條 關鍵基礎設施提供者以外之特定非公務機關，應符合其所屬資通安全責任等級之要求，並考量其所保有或處理之資訊種類、數量、性質、資通系統之規模與性質等條件，訂定、修正及實施資通安全維護計畫。</p> <p>中央目的事業主管機關得要求所管前項特定非公務機關，提出資通安全維護計畫實施情形。</p> <p>中央目的事業主管機關得稽核所管第一項特定非公務機關之資通安全維護計畫實施情形，發現有缺失或待改善者，應限期要求受稽核之特定非公務機關提出改善報告。</p> <p>前三項之資通安全維護計畫必要事項、實施情形之提出、稽核之頻率、內容與方法、改善報告之提出及其他應遵行事項之辦法，由中央目的事業主管機關擬訂，報請主管機關核定之。</p>	<p>Article 17. A specific non-government agency other than critical infrastructure provider, shall satisfy the requirements of the cyber security responsibility level, and take into account the category, quantity and attribute of the information reserved or processed, along with the scale and attribute of the information and communication system, to stipulate, amend and implement the cyber security maintenance plan.</p> <p>The central authority in charge of relevant industry may request the specific non-government agency under their charge mentioned in the preceding Paragraph, to submit a report about implementation of the cyber security maintenance plan.</p> <p>The central authority in charge of relevant industry may audit the specific non-government agency under their charge mentioned in the Paragraph 1 regarding their implementation of the cyber security maintenance plan. When found defective or needing improvement in the cyber security maintenance plan, the audited specific non-government agency shall be required to submit an improvement report before a specified date.</p> <p>Regulations regarding the essentials of the cyber security maintenance plan, and submittal of the implementation, audit frequency, contents and methods, submittal of the improvement reports and other matters in preceding three Paragraphs shall be drafted by the central authority in charge of relevant industry, and submit to the competent authority for approval.</p>

<p>第十八條 特定非公務機關為因應資通安全事件，應訂定通報及應變機制。</p> <p>特定非公務機關於知悉資通安全事件時，應向中央目的事業主管機關通報。</p> <p>特定非公務機關應向中央目的事業主管機關提出資通安全事件調查、處理及改善報告；如為重大資通安全事件者，並應送交主管機關。</p> <p>前三項通報及應變機制之必要事項、通報內容、報告之提出及其他應遵行事項之辦法，由主管機關定之。</p> <p>知悉重大資通安全事件時，主管機關或中央目的事業主管機關於適當時機得公告與事件相關之必要內容及因應措施，並得提供相關協助。</p>	<p>Article 18. To cope with cyber security incident, a specific non-government agency shall stipulate the reporting and responding mechanism.</p> <p>When privy to a cyber security incident, a specific non-government agency shall report to the central authority in charge of relevant industry.</p> <p>A specific non-government agency shall file a report on the investigation, handling and improvement on the cyber security incident and shall submit the report to the central authority in charge of relevant industry. In case of a severe cyber security incident, it shall further notify the competent authority.</p> <p>Regulations regarding the essentials of the reporting and responding mechanism, content of notification, submittal of report and other matters in the three preceding Paragraphs shall be stipulated by the competent authority.</p> <p>When privy to a severe cyber security incident, the competent authority or the central authority in charge of relevant industry may, in a timely manner, promulgate the essential contents of the incident and coping measures and render relevant support.</p>
<p>第四章 罰則</p>	<p>Chapter IV. Penalties</p>
<p>第十九條 公務機關所屬人員未遵守本法規定者，應按其情節輕重，依相關規定予以懲戒或懲處。</p> <p>前項懲處事項之辦法，由主管機關定之。</p>	<p>Article 19. Personnel of a government agency shall be subject to discipline or penalty in accordance with the relevant regulations if failing to comply with the regulation of the Act.</p> <p>Regulations for such penalty in the preceding Paragraph shall be stipulated by the competent authority.</p>

<p>第二十條 特定非公務機關有下列情形之一者，由中央目的事業主管機關令限期改正；屆期未改正者，按次處新臺幣十萬元以上一百萬元以下罰鍰：</p> <p>一、未依第十六條第二項或第十七條第一項規定，訂定、修正或實施資通安全維護計畫，或違反第十六條第六項或第十七條第四項所定辦法中有關資通安全維護計畫必要事項之規定。</p> <p>二、未依第十六條第三項或第十七條第二項規定，向中央目的事業主管機關提出資通安全維護計畫之實施情形，或違反第十六條第六項或第十七條第四項所定辦法中有關資通安全維護計畫實施情形提出之規定。</p> <p>三、未依第七條第三項、第十六條第五項或第十七條第三項規定，提出改善報告送交主管機關、中央目的事業主管機關，或違反第十六條第六項或第十七條第四項所定辦法中有關改善報告提出之規定。</p> <p>四、未依第十八條第一項規定，訂定資通安全事件之通報及應變機制，或違反第十八條第四項所定辦法中有關通報及應變機制必要事</p>	<p>Article 20. If a specific non-government agency has one among those enumerated below transpired, the central authority in charge of relevant industry shall order it to complete corrective actions within the specified time limit. If it fails to complete corrective actions within the specified time limit, it shall be subject to a fine ranging from NT\$100,000 as the minimum to NT\$1,000,000 as the maximum for each offense:</p> <ol style="list-style-type: none"> 1. If it fails to stipulate, amend or implement the cyber security maintenance plan in accordance with Paragraph 2 of Article 16 or Paragraph 1 of Article 17, or violates the essential items in the cyber security maintenance plan under Paragraph 6 of Article 16 or Paragraph 4 of Article 17. 2. If it fails to submit the report on implementation of the cyber security maintenance plan to the central authority in charge of relevant industry in accordance with Paragraph 3 of Article 16 or Paragraph 2 of Article 17, or fails the requirements with the submittal of the implementation of the cyber security maintenance plan stipulated under Paragraph 6 of Article 16 or Paragraph 4 of Article 17. 3. If it fails the requirements under Paragraph 3 of Article 7, Paragraph 5 of Article 16 or Paragraph 3 of Article 17, unable to submit the improvement reports to the competent authority, the central authority in charge of relevant industry, or violates the regulation with the submitting of the improvement report under Paragraph 6 of Article 16 or Paragraph 4 of Article 17. 4. If it fails to stipulate the reporting and responding mechanism of cyber security incident in accordance with Paragraph 1 of Article 18, or violates the essential items in the reporting and responding mechanism under Paragraph 4 of Article 18. 5. If it fails the requirements under Paragraph 3 of Article 18, unable to submit the cyber security investigation, handling and improvement reports regarding cyber security incidents to the central
--	--

<p>項之規定。</p> <p>五、未依第十八條第三項規定，向中央目的事業主管機關或主管機關提出資通安全事件之調查、處理及改善報告，或違反第十八條第四項所定辦法中有關報告提出之規定。</p> <p>六、違反第十八條第四項所定辦法中有關通報內容之規定。</p>	<p>authority in charge of relevant industry or the competent authority, or violate the regulation with the submitting of the report under Paragraph 4 of Article 18.</p> <p>6. If it violates the regulation regarding the contents of notification under Paragraph 4 of Article 18.</p>
<p>第二十一條 特定非公務機關未依第十八條第二項規定，通報資通安全事件，由中央目的事業主管機關處新臺幣三十萬元以上五百萬元以下罰鍰，並令限期改正；屆期未改正者，按次處罰之。</p>	<p>Article 21. A specific non-government agency violates the provisions Paragraph 2 of Article 18, by failing to report a cyber security incident, the central authority in charge of relevant industry shall impose a fine ranging from NT\$300,000 as the minimum to NT\$5,000,000 as the maximum, and shall order it to complete improvement within a specified time limit. If it fails to complete such requirement within the specified time limit, a penalty for each additional offense shall be re-imposed.</p>
<p>第五章 附則</p>	<p>Chapter V. Supplementary provisions</p>
<p>第二十二條 本法施行細則，由主管機關定之。</p>	<p>Article 22. The enforcement rules of the Act shall be stipulated by the competent authority.</p>
<p>第二十三條 本法施行日期，由主管機關定之。</p>	<p>Article 23. The implementation date of the Act shall be stipulated by the competent authority.</p>