

資通安全責任等級分級辦法-英譯對照

資通安全責任等級分級辦法	Regulations on Classification of Cyber Security Responsibility Levels
第一條 本辦法依資通安全管理法（以下簡稱本法）第七條第一項規定訂定之。	Article 1 These Regulations are stipulated according to Paragraph 1 of Article 7 of the Cyber Security Management Act (hereinafter referred to as “the Act”).
第二條 公務機關及特定非公務機關（以下簡稱各機關）之資通安全責任等級，由高至低，分為 A 級、B 級、C 級、D 級及 E 級。	Article 2 The cyber security responsibility levels of the government agency or specific non-government agency(hereinafter referred to as “each agency”) are classified from high to low into Level-A, Level-B, Level-C, Level-D and Level-E.
<p>第三條 主管機關應每二年核定自身資通安全責任等級。</p> <p>行政院直屬機關應每二年提交自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，報主管機關核定。</p> <p>直轄市、縣（市）政府應每二年提交自身、所屬或監督之公務機關，與所轄鄉（鎮、市）、直轄市山地原住民區公所及其所屬或監督之公務機關之資通安全責任等級，報主管機關核定。</p> <p>直轄市及縣（市）議會、鄉（鎮、市）民代表會及直轄市山地原住民區民代表會應每二年提交自身資通安全責任等級，由其所在區域之直轄市、縣（市）政府彙送主管機關核定。</p> <p>總統府、國家安全會議、立法院、司法院、考試院及監察院應每二年核定自身、所屬或監督之公務機關及所管之特定非公務機關之資通安全責任等級，送主管機關備查。</p> <p>各機關因組織或業務調整，致須變更原資通安全責</p>	<p>Article 3 The competent authority shall approve its own cyber security responsibility levels every two years.</p> <p>The agencies directly subordinate to the Executive Yuan shall, every two years, propose the cyber security responsibility levels of their own, their subordinate or supervisory government agencies, and the specific non-government agencies under their charge, and shall report the same to the competent authority for approval.</p> <p>Special municipality, county(city) government shall, every two years, propose the cyber security responsibility levels of their own, their subordinate or supervisory government agencies, and their governed villages(townships/cities), mountain indigenous district offices of municipality, and the subordinate or supervisory government agencies of such governed villages(townships/cities) and mountain indigenous district offices of special municipalities, and shall report the same to the competent authority for approval.</p> <p>Special municipality and county (city) council, village (township/city) council, and mountain indigenous districts of special municipality council shall, every two years, submit their own cyber security responsibility level, which shall be compiled and submitted by the municipality and county (city) government where it is located to the competent authority for approval.</p> <p>The Presidential Office, the National Security</p>

<p>任等級時，應即依前五項規定程序辦理等級變更；有新設機關時，亦同。</p> <p>第一項至第五項公務機關辦理資通安全責任等級之提交或核定，就公務機關或特定非公務機關內之單位，認有另列與該機關不同等級之必要者，得考量其業務性質，依第四條至第十條規定認定之。</p>	<p>Council, the Legislative Yuan, the Judicial Yuan, the Examination Yuan, and the Control Yuan shall, every two years, approve the cyber security responsibility level of their own, their subordinate or supervisory government agencies, and the specific non-government agencies under their charge, and shall submit the same to the competent authority for recordation.</p> <p>If each agency is required to change its cyber security responsibility level due to adjustment to the organization or business, it shall immediately conduct the change to level according to the procedures under the preceding five paragraphs; the same shall apply to the case when a new agency is established.</p> <p>In conducting the submission or approval of cyber security responsibility level under Paragraph 1 to Paragraph 5, if the government agency thinks it is necessary to otherwise give the entity within the government agency or the specific non-government agency the level that is different from those of such agency, it may determine such level in accordance with the requirements of Article 4 to Article 10, by taking into consideration the nature of business of such entity.</p>
<p>第四條 各機關有下列情形之一者，其資通安全責任等級為A級：</p> <ol style="list-style-type: none"> 一、業務涉及國家機密。 二、業務涉及外交、國防或國土安全事項。 三、業務涉及全國性民眾服務或跨公務機關共用性資通系統之維運。 四、業務涉及全國性民眾或公務員個人資料檔案之持有。 五、屬公務機關，且業務涉及全國性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項。 六、屬關鍵基礎設施提供者，且業務經中央目的事業 	<p>Article 4 The cyber security responsibility level of each agency under any of the following circumstances is Level-A:</p> <ol style="list-style-type: none"> 1. Its business involves national security information. 2. Its business involves matters of foreign issue, national defense, or homeland security. 3. Its business involves the maintenance operation of information and communication system commonly used for nationwide people service or cross agencies. 4. Its business involves the possession of personal information of nationwide people or civil servants. 5. It is a government agency, and its business involves matters of nationwide energy, water resource, telecommunication, transportation, banking & finance, or emergent rescue.

<p>主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生災難性或非常嚴重之影響。</p> <p>七、屬公立醫學中心。</p>	<p>6. It is a critical infrastructure provider, and the central authority in charge of relevant industry, based on the consideration of the number of users, market share, the area and the substitutability of its business or maintenance operation of critical infrastructures and services, considers that the failures of or impact on its cyber security system might cause disasters or extremely serious impact on social public interests, people's morale, or the security of people's lives, body or property.</p> <p>7. It is a government medical center.</p>
<p>第五條 各機關有下列情形之一者，其資通安全責任等級為B級：</p> <p>一、業務涉及公務機關捐助或研發之敏感科學技術資訊之安全維護及管理。</p> <p>二、業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運。</p> <p>三、業務涉及區域性或地區性民眾個人資料檔案之持有。</p> <p>四、屬公務機關，且業務涉及區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項。</p> <p>五、屬關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生嚴重影響。</p> <p>六、屬公立區域醫院或地區醫院。</p>	<p>Article 5 The cyber security responsibility levels of each agency under any of the following circumstances are Level-B.</p> <p>1. Its business involves the security maintenance and management of sensitively scientific technology information that is donated, researched, or developed by the government agency.</p> <p>2. Its business involves the maintenance operation of information and communication systems that are commonly used for regional or local people services or cross agencies.</p> <p>3. Its business involves the possession of the archives of personal information of regional or local people.</p> <p>4. It is a government agency, and its business involves matters of regional or local energy, water resources, telecommunications, transportation, banking & finance, or emergent rescues.</p> <p>5. It is a critical infrastructure provider, and the central authority in charge of relevant industry, based on consideration of the number of users, market share, the area and the substitutability of its business, or the maintenance operation of critical infrastructure and services, considers that the failure of or impacts on its information and communication system might cause serious impact on social public interest, people's morale, or the security of people's lives, body or properties.</p> <p>6. It is a public regional hospital or local hospital.</p>

<p>第六條 各機關維運自行或委外開發之資通系統者，其資通安全責任等級為 C 級。</p>	<p>Article 6 The cyber security responsibility level of each agency who maintains and operates by itself or outsources the development of information and communication system is Level-C.</p>
<p>第七條 各機關自行辦理資通業務，未維運自行或委外開發之資通系統者，其資通安全責任等級為 D 級。</p>	<p>Article 7 The cyber security responsibility levels of each agency who conducts information and communication business by itself but does not maintain and operate the information and communication system that is developed by itself or outsourced for the development is Level-D.</p>
<p>第八條 各機關有下列情形之一者，其資通安全責任等級為 E 級：</p> <ul style="list-style-type: none"> 一、無資通系統且未提供資通服務。 二、屬公務機關，且其全部資通業務由其上級或監督機關兼辦或代管。 三、屬特定非公務機關，且其全部資通業務由其中中央目的事業主管機關、中央目的事業主管機關所屬公務機關，或中央目的事業主管機關所管特定非公務機關兼辦或代管。 	<p>Article 8 The cyber security responsibility level of each agency under any of the following circumstances is Level-E:</p> <ol style="list-style-type: none"> 1. It neither has the information and communication system, nor provides the information and communication service. 2. It is a government agency, and all its information and communication business is conducted concurrently or managed by its superior or supervisory agency. 3. It is a specific non-government agency, and all of its information and communication business is conducted concurrently or managed by its central authority in charge of relevant industry, the subordinate government agency of the central authority in charge of relevant industry, or the specific non-government agency under their charge by the central authority in charge of relevant industry.
<p>第九條 各機關依第四條至前條規定，符合二個以上之資通安全責任等級者，其資通安全責任等級列為其符合之最高等級。</p>	<p>Article 9 If the cyber security responsibility level of each agency conforms to two or above requirements under Article 4 to Article 8, the level of each agency are classified as the highest level conforming to such requirements.</p>
<p>第十條 各機關之資通安全責任等級依前六條規定認定之。但第三條第一項至第五項之公務機關提交或核定資通安全責任等級時，得考量下列事項對國家安全、社會公共利益、人民生命、身體、財產安全或公務機關聲譽之影響程度，調整各機關之等級：</p> <ul style="list-style-type: none"> 一、業務涉及外交、國防、國 	<p>Article 10 The cyber security responsibility level of each agency shall be determined in accordance with the preceding six articles; however, when the government agency submits or approves the cyber security responsibility level under Paragraphs 1 to 5 of Article 3, the levels of each agency may be adjusted, by taking into consideration the degree of impact of the following matters on national security, social public interests, the security of</p>

<p>土安全、全國性、區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院業務者，其中斷或受妨礙。</p> <p>二、業務涉及個人資料、公務機密或其他依法規或契約應秘密之資訊者，其資料、公務機密或其他資訊之數量與性質，及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。</p> <p>三、各機關依層級之不同，其功能受影響、失效或中斷。</p> <p>四、其他與資通系統之提供、維運、規模或性質相關之具體事項。</p>	<p>people's lives, body, properties, or the reputation of the government agency:</p> <ol style="list-style-type: none"> 1. The business involving foreign issue, national defense, homeland security, or its business involves nationwide, regional or local energy, water resource, telecommunication, transportation, banking and finance, emergent rescues; and hospital are interrupted or impeded. 2. The business involves personal information, official confidentiality, or other information which should be kept confidential by law or contract, the quantity and nature of such information, and the unauthorized access, use, control, breach, damage, tampering, destruction or other infringement. 3. The function of each agency is affected, disabled or interrupted depending on the hierachy of the agency. 4. Other concrete matters relating to the provision, maintenance operation, size, or nature of information and communication system.
<p>第十一條 各機關應依其資通安全責任等級，辦理附表一至附表八之事項。</p> <p>各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施；關鍵基礎設施提供者之中央目的事業主管機關就特定類型資通系統之防護基準認有另為規定之必要者，得自行擬訂防護基準，報請主管機關核定後，依其規定辦理。</p> <p>各機關辦理附表一至附表八所定事項或執行附表十所定控制措施，因技術限制、個別資通系統之設計、結構或性質等因素，就特定事項或控制措施之辦理或執行顯</p>	<p>Article 11 Each agency shall conduct the matters specified in Schedule 1 to Schedule 8, depending on its cyber security responsibility level.</p> <p>For the information and communication system that is developed by each agency itself or outsourced for the development, each agency shall complete the classification of information and communication system according to the principles of classification of defense requirements of information and communication system specified in Schedule 9, and shall implement control measures according to the defense standards of information and communication system specified in Schedule 10; if the central authority in charge of relevant industry of a critical infrastructure provider considers it is necessary to otherwise provide for defense standards of specific types of the information and communication systems, it may propose by itself the defense standards and report such standards to the competent authority for approval, and shall</p>

<p>有困難者，得經第三條第二項至第四項所定其等級提交機關或同條第五項所定其等級核定機關同意，並報請主管機關備查後，免執行該事項或控制措施。</p> <p>公務機關之資通安全責任等級為 A 級或 B 級者，應依主管機關指定之方式，提報第一項及第二項事項之辦理情形。</p>	<p>follow the requirements of such standards, if approved.</p> <p>In conducting the matters specified in Schedule 1 to Schedule 8 or implementing control measures specified in Schedule 10, if each agency has apparent difficulties in conducting or implementing specific matters or control measures due to such factors as technical limitation, design, structure or nature of individual information and communication system, it may, with consent of each agency submitting its level under Paragraph 2 to Paragraph 4 of Article 3 or each agency approving its level under Paragraph 5 of the same article, and upon reporting to the competent authority for recordation, be exempted from the implementation of such matters or control measures.</p> <p>The government agency whose cyber security responsibility level is Level-A or Level-B shall report the implementation status of matters under Paragraph 1 and Paragraph 2 in the manner designated by the competent authority.</p>
<p>第十二條 本辦法之施行日期，由主管機關定之。</p>	<p>Article 13 The implementation date of the Regulations shall be stipulated by the competent authority.</p>

附表一

附表一 資通安全責任等級 A 級之公務機關應辦事項				Schedule 1:Matters to be conducted by the government agency of cyber security responsibility Level-A			
制度面向	辦理項目	辦理項目細項	辦理內容	System aspect	Items conducted	Sub-items conducted	Contents conducted
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。	Management aspect	Classification and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the government agency shall complete the classifications of the information and communication systems developed by itself or outsourced according to Schedule 9, and shall complete the control measures specified in Schedule 10; subsequently, the government agency shall inspect the appropriateness of the classification of levels of the information and communication systems at least once a year.
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。		The importation of the information security management system and verification by a impartial third party		Within two years after receipt of initial approval or change of level, the government agency shall import to all of its core information and communication systems the national standards - CNS 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the government agency itself and approved by the competent authority; within three years of the completion of impartial third-party certification, the government agency shall continually maintain the validity of its certification.
	資通安全專責人員		初次受核定或等級變更後之一年內，配置四人；須以專職人員配置之。				
	內部資通安全稽核		每年辦理二次。				
	業務持續運作演練		全部核心資通系統每年辦理一次。				
	資安治理成熟度評估		每年辦理一次。				
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理二次。	Technical aspect	Dedicated cyber security personnel		Within one year after receipt of initial approval or change of level, the government agency shall deploy four persons on full-time basis.
		系統滲透測試	全部核心資通系統每年辦理一次。		Internal cyber security audit		Conduct twice a year.
	資通安全健診	網路架構檢視	每年辦理一次。		Business sustainable operation rehearsal		Conduct once a year for all core information and communication systems.
		網路惡意活動檢視			Cyber security governance maturity assessment		Conduct once a year.
		使用者端電腦惡意活動檢視			Security detection	Detection of website security vulnerability	Conduct twice a year for all core information and communication systems.
		伺服器主機惡意活動檢視				Testing of system penetration	Conduct once a year for all core information and communication systems.
		目錄伺服器設定及防火牆連線設定檢視					
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料。		Cyber security health diagnosis	Inspection of network framework	Conduct once a year.
						Inspection of cyber malicious activity	
	政府組態基準		初次受核定或等級變更後之一年內，依主管機關公告之項目，完成政府組態基準導入作業，並持續維運。			Inspection of malicious activity of user	

	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
		入侵偵測及防禦機制	
		具有對外服務之核心資通系統者，應備應用程式防火牆	
		進階持續性威脅攻擊防禦措施	
認知與訓練	資通安全教育訓練	資通安全及資訊人員	<u>每年至少四名人員各接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。</u>
		一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。
	資通安全專業證照及職能訓練證書	資通安全專業證照	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有四張以上，並持續維持證照之有效性。
		資通安全職能評量證書	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有四張以上，並持續維持證書之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構。

三、資通安全專職人員，指應全職執行資通安全業務者。

四、公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經主管機關認可之其他具有同等或以上效用之措施。

五、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

		terminal computer	
		Inspection of malicious activity of server	
		Inspection of setting of directory server and setting of firewall connection	
	Cyber security threat detection management mechanism		Within one year after receipt of initial approval or change of level, the government agency shall complete the development of threat detection mechanism, and shall continue the maintenance and operation thereof and submit the monitoring management documentation in the manner designated by the competent authority.
	Government configuration baseline		Within one year of receipt of initial approval or change of levels, the government agency shall complete the import operation of government configuration baseline for the items publicized by the competent authority, and shall continue the maintenance and operation thereof.
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the government agency shall complete activation of various cyber security defense measures, and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
Network firewall			
If the government agency has email server, it should have email filtering mechanism			
Hacking detection and defense mechanism			
If the government agency has the core information and communication system for external service, it should have the application firewall			
	Defense measure for advanced persistent threat attacks		

Awareness and training	Cyber security education and training	Cyber security and information personnel	Each year, at least four persons shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each.
		General user and officer	Each year, each person shall receive general cyber security education training for not less than three hours.
	Cyber security professional license and competence training certificate	Cyber security professional license	Within one year after receipt of initial approval or change of level, the full-time cyber security personnel shall held a total of not less than four licenses, and shall continually maintain the validity of licenses.
		Cyber security competence assessment certificate	Within one year after receipt of initial approval or change of level, the full-time cyber security personnel shall hold a total of not less than four certificates, and shall continually maintain the validity of certificates.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the installation, maintenance or development of such information and communication system.
2. The third party as used in “impartial third-party certification” refers to an agency commissioned by the competent authority for the certification in accordance with the Standards Act of our country.
3. The full-time cyber security personnel refer to the personnel who should implement cyber security businesses in full-time.
4. In conducting “cyber security health diagnosis” of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the government agency may take other measures which have equal or better effects as approved by the competent authority.
5. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority(entity) recognized by the competent authority.

附表二

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				Schedule 2: Matters to be conducted by the specific non-government agency of cyber security responsibility Level-A				
制度面向	辦理項目	辦理項目細項	辦理內容	System aspect	Items conducted	Sub-items conducted	Contents conducted	
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。	Management aspect	Classification and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the specific non-government agency shall complete the classifications of the information and communication systems developed by itself or outsourced according to Schedule 9, and shall complete the control measures specified in Schedule 10; subsequently, the specific non-government agency shall inspect the appropriateness of the classification of levels of the information and communication system at least once a year.	
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。		The importation of the information security management system and verification by a impartial third party		Within two years after receipt of initial approval or change of level, the specific non-government agency shall import to all of its core information and communication systems the national standards - CNS 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the specific non-government agency itself and approved by the competent authority; within three years of the completion of impartial third-party certification, the specific non-government agency shall continually maintain the validity of its certification.	
	資通安全專責人員		初次受核定或等級變更後之一年內，配置四人。		Dedicated cyber security personnel		Within one year after receipt of initial approval or change of level, the specific non-government agency shall deploy four persons.	
	內部資通安全稽核		每年辦理二次。		Internal cyber security audit		Conduct twice a year	
	業務持續運作演練		全部核心資通系統每年辦理一次。		Business sustainable operation rehearsal		Conduct once a year for all core information and communication systems	
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理二次。	Technical aspect	Security detection	Detection of website security vulnerability	Conduct twice a year for all core information and communication systems	
		系統滲透測試	全部核心資通系統每年辦理一次。			Testing of system penetration	Conduct once a year for all core information and communication systems	
	資通安全健診	網路架構檢視	每年辦理一次。		Cyber security health diagnosis	Inspection of network framework	Inspection of cyber malicious activity	Conduct once a year
		網路惡意活動檢視						
		使用者端電腦惡意活動檢視						
		伺服器主機惡意活動檢視						
		目錄伺服器設定及防火牆連線設定檢視						
		資通安全威脅偵測管理機制			初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運。			
		資通安全防護	防毒軟體		初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。			
	網路防火牆							
	具有郵件伺服器者，應備電子郵件過濾機制							
入侵偵測及防禦機制								

		具有對外服務之核心資通系統者，應備應用程式防火牆	
		進階持續性威脅攻擊防禦措施	
認知與訓練	資通安全教育訓練	資通安全及資訊人員	<u>每年至少四名人員各接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。</u>
		一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。
	資通安全專業證照		初次受核定或等級變更後之一年內，資通安全專責人員總計應持有四張以上，並持續維持證照之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構。

三、特定非公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。

四、特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。

資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

		terminal computer	
		Inspection of malicious activity of server	
		Inspection of setting of directory server and setting of firewall connection	
Cyber security threat detection management mechanism			Within one year after receipt of initial approval or change of level, the specific non-government agency shall complete the development of threat detection mechanism, and shall continue the maintenance and operation thereof.
Cyber security defense	Anti-virus software		Within one year after receipt of approval or change of levels, the specific non-government agency shall complete activation of various cyber security defense measures, and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
	Network firewall		
	If the specific non-government agency has email server, it should have email filtering mechanism		
	Hacking detection and defense mechanism		
	If the specific non-government agency has the core information and communication system for external service, it should have the application firewall		
	Defense measure for advanced persistent threat attacks		
Awareness and training	Cyber security	Cyber security and information personnel	Each year, at least four persons shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each.

	education and training	General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours
	Cyber security professional license		Within one year after receipt of initial approval or change of level, the dedicated cyber security personnel shall held a total of not less than four licenses, and shall continually maintain the validity of licenses.
<p>Notes:</p> <ol style="list-style-type: none">1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the installation, maintenance or development of such information and communication system.2. The third party as used in “impartial third-party certification” refers to an agency commissioned by the competent authority for the certification in accordance with the Standards Act of our country.3. In conducting “cyber security health diagnosis” of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the specific non-government agency may take other measures which have equal or better effects as approved by the central authority in charge of relevant industry.4. The central authority in charge of relevant industry of the specific non-government agency may, depending on the actual requirements and to the extent of compliance with these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.5. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority(entity) recognized by the competent authority.			

附表三

附表三 資通安全責任等級B級之公務機關應辦事項				Schedule 3: Matters to be conducted by the government agency of cyber security responsibility Level-B					
制度面向		辦理項目	辦理項目細項	辦理內容		System aspect	Items conducted	Sub-items conducted	Contents conducted
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。		Management aspect	Classification and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the government agency shall complete the classifications of the information and communication systems developed by itself or outsourced according to Schedule 9, and shall complete the control measures specified in Schedule 10; subsequently, the government agency shall inspect the appropriateness of the classification of levels of information and communication system at least once a year.	
			初次受核定或等級變更後之二年內，全部核心資通系統導入CNS 27001資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。					Within two years after receipt of initial approval or change of level, the government agency shall import to all of its core information and communication systems the national standards - CNS 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the government agency itself and approved by the competent authority; within three years of the completion of impartial third-party certification, the government agency shall continually maintain the validity of its certification.	
	資通安全專責人員		初次受核定或等級變更後之一年內，配置二人；須以專職人員配置之。			The importation of the information security management system and verification by a impartial third party		Within three years of the completion of impartial third-party certification, the government agency shall continually maintain the validity of its certification.	
	內部資通安全稽核		每年辦理一次。						
	業務持續運作演練		全部核心資通系統每二年辦理一次。			Dedicated cyber security personnel		Within one year after receipt of initial approval or change of level, the government agency shall deploy two persons on full-time basis.	
	資安治理成熟度評估		每年辦理一次。			Internal cyber security audit		Conduct once a year.	
						Business sustainable operation rehearsal		Conduct once every two years for all core information and communication systems.	
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理一次。		Technical aspect	Security detection	Detection of website security vulnerability	Conduct once a year for all core information and communication systems.	
		系統滲透測試	全部核心資通系統每二年辦理一次。				Testing of system penetration	Conduct once every two years for all core information and communication systems.	
	資通安全健診	網路架構檢視	每二年辦理一次。			Cyber security health diagnosis	Inspection of network framework	Conduct once every two years.	
		網路惡意活動檢視							
		使用者端電腦惡意活動檢視							
		伺服器主機惡意活動檢視							
		目錄伺服器設定及防火牆連線設定檢視							
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料。			Inspection of cyber malicious activity			
	政府組態基準		初次受核定或等級變更後之一年內，依主管機關公告之項目，完成政府組態基準導入作業，並持續維運。				Inspection of malicious activity of user		
		防毒軟體							

	資通安全防護	網路防火牆	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		具有郵件伺服器者，應備電子郵件過濾機制	
		入侵偵測及防禦機制	
		具有對外服務之核心資通系統者，應備應用程式防火牆	
認知與訓練	資通安全教育訓練	資通安全及資訊人員	<u>每年至少二名人員各接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。</u>
		一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。
	資通安全專業證照及職能訓練證書	資通安全專業證照	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有二張以上，並持續維持證照之有效性。
		資通安全職能評量證書	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有二張以上，並持續維持證書之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構。

三、資通安全專職人員，指應全職執行資通安全業務者。

四、公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經主管機關認可之其他具有同等或以上效用之措施。

資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

		terminal computer	
		Inspection of malicious activity of servers	
		Inspection of setting of directory server and setting of firewall connection	
	Cyber security threat detection management mechanism		Within one year after receipt of initial approval or change of level, the government agency shall complete the development of threat detection mechanism, and shall continue the maintenance and operation thereof and submit the monitoring management documentation in the manner designated by the competent authority.
	Government configuration baseline		Within one year of receipt of initial approval or change of levels, the government agency shall complete the import operation of government configuration baseline for the items publicized by the competent authority, and shall continue the maintenance and operation thereof.
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the government agency shall complete activation of various cyber security defense measures, and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		Network firewall	
		If government agency has email server, it should have email filtering mechanism	
		Hacking detection and defense mechanism	
		If the government agency has the core information and communication system for external service, it should have the application firewall	
Awareness and training	Cyber security	Cyber security and information personnel	Each year, at least two persons shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each.

	education and training	General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours
	Cyber security professional license and competence training certificate	Cyber security professional license	Within one year after receipt of initial approval or change of level, the full-time cyber security personnel shall held a total of not less than two licenses, and shall continually maintain the validity of licenses.
		Cyber security competence assessment certificate	Within one year after receipt of initial approval or change of level, the full-time cyber security personnel shall held a total of not less than two licenses, and shall continually maintain the validity of certificates.

Notes:

1.

If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the installation, maintenance or development of such information and communication system.

2.

The third party as used in “impartial third-party certification” refers to an agency commissioned by the competent authority for the certification in accordance with the Standards Act of our country.

3.

The full-time cyber security personnel refer to the personnel who should implement cyber security businesses in full-time.

4.

In conducting “cyber security health diagnosis” of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the government agency may take other measures which have equal or better effects as approved by the competent authority.

5.

Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority(entity) recognized by the competent authority.

附表四

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				Schedule 4: Matters to be conducted by the specific non-government agency of cyber security responsibility Level-B				
制度面向	辦理項目	辦理項目細項	辦理內容	System aspect	Items conducted	Sub-items conducted	Contents conducted	
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。	Management aspect	Classification and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the specific non-government agency shall complete the classifications of the information and communication systems developed by itself or outsourced according to Schedule 9, and shall complete the control measures specified in Schedule 10; subsequently, the specific non-government agency shall inspect the appropriateness of the classification of levels of information and communication systems at least once a year.	
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，於三年內完成公正第三方驗證，並持續維持其驗證有效性。		The importation of the information security management system and verification by a impartial third party		Within two years after receipt of initial approval or change of level, the specific non-government agency shall import to all of its core information and communication systems the national standards - CNS 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the specific non-government agency itself and approved by the competent authority; within three years of the completion of impartial third-party certification, the specific non-government agency shall continually maintain the validity of its certification.	
	資通安全專責人員		初次受核定或等級變更後之一年內，配置二人。		Dedicated cyber security personnel		Within one year after receipt of initial approval or change of level, the specific non-government agency shall deploy two persons.	
	內部資通安全稽核		每年辦理一次。		Internal cyber security audit		Conduct once a year.	
	業務持續運作演練		全部核心資通系統每二年辦理一次。		Business sustainable operation rehearsal		Conduct once every two years for all core information and communication systems.	
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理一次。	Technical aspect	Security detection	Detection of website security vulnerability	Conduct once a year for all core information and communication systems.	
		系統滲透測試	全部核心資通系統每二年辦理一次。			Testing of system penetration	Conduct once every two years for all core information and communication systems.	
	資通安全健診	網路架構檢視	每二年辦理一次。		Cyber security health diagnosis		Inspection of network framework	Conduct once every two years.
		網路惡意活動檢視						
		使用者端電腦惡意活動檢視						
		伺服器主機惡意活動檢視						
		目錄伺服器設定及防火牆連線設定檢視	初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運。				Inspection of malicious activity of user terminal computer	
		資通安全威脅偵測管理機制					Inspection of malicious activity of server	
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。					
		網路防火牆						
		具有郵件伺服器者，應備電子郵件過濾機制						
入侵偵測及防禦機制								

		具有對外服務之核心資通系統者，應備應用程式防火牆	
認知與訓練	資通安全教育訓練	資通安全及資訊人員	<u>每年至少二名人員各接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。</u>
		一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。
	資通安全專業證照		初次受核定或等級變更後之一年內，資通安全專責人員總計應持有二張以上，並持續維持證照之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構。

三、特定非公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。

四、特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。

五、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

		Inspection of setting of directory server and setting of firewall connection	
	Cyber security threat detection management mechanism		Within one year after receipt of initial approval or change of levels, the specific non-government agency shall complete the development of threat detection mechanisms, and shall continue the maintenance and operation thereof.
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the specific non-government agency shall complete activation of various cyber security defense measures, and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		Network firewall	
		If the specific non-government agency has email server, it should have email filtering mechanism	
		Hacking detection and defense mechanism	
		If the specific non-government agency has the core information and communication system for external service, it should have the application firewall	
Awareness and training	Cyber security education and training	Cyber security and information personnel	Each year, at least two persons shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each.
		General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours.
	Cyber security professional license		Within one year after receipt of initial approval or change of level, the dedicated cyber security personnel shall held a total of not less than two licenses, and shall continually maintain the validity of the licenses.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the installation, maintenance or development of such information and communication system.

	<p>2. The third party as used in “impartial third-party certification” refers to an agency commissioned by the competent authority for the certification in accordance with the Standards Act of our country.</p> <p>3. In conducting “cyber security health diagnosis” of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the specific non-government agency may take other measures which have equal or better effects as approved by the central authority in charge of relevant industry.</p> <p>4. The central authority in charge of relevant industry of the specific non-government agency may, depending on actual requirements and to the extent of compliance with requirements of these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.</p> <p>5. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority(entity) recognized by the competent authority.</p>
--	--

附表五

附表五 資通安全責任等級 C 級之公務機關應辦事項				Schedule 5: Matters to be conducted by the government agency of cyber security responsibility Level-C			
制度面向	辦理項目	辦理項目細項	辦理內容	System aspect	Items conducted	Sub-items conducted	Contents conducted
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，其後應每年至少檢視一次資通系統分級妥適性；系統等級為「高」者，應於初次受核定或等級變更後之二年內，完成附表十之控制措施。	Management aspect	Classification and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the government agency shall complete the classifications of the information and communication systems developed by itself or outsourced according to Schedule 9; subsequently, the government agency shall inspect the appropriateness of the classification of levels of information and communication systems at least once a year. If the system levels are “high”, the government agency shall, within two years of receipt of initial approval or change of levels, complete the control measures specified in Schedule 10.
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。		The importation of the information security management system		Within two years after receipt of initial approval or change of level, the government agency shall import to all of its core information and communication systems the national standards - CNS 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the government agency itself and approved by the competent authority, and shall continually maintain the importation thereof.
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。		Dedicated cyber security personnel		Within one year after receipt of initial approval or change of level, the government agency shall deploy one person on full-time basis.
	內部資通安全稽核		每二年辦理一次。		Internal cyber security audit		Conduct once every two years.
	業務持續運作演練		全部核心資通系統每二年辦理一次。		Business sustainable operation rehearsal		Conduct once every two years for all core information and communication systems.
	安全性檢測		全部核心資通系統每二年辦理一次。		Security detection		Conduct once every two years for all core information and communication systems.
技術面	資通安全健診	網站安全弱點檢測	全部核心資通系統每二年辦理一次。		Detection of website security vulnerability	Conduct once every two years for all core information and communication systems.	
		系統滲透測試	全部核心資通系統每二年辦理一次。				Testing of system penetration
		網路架構檢視	每二年辦理一次。	Inspection of network framework	Conduct once every two years.		
		網路惡意活動檢視					
		使用者端電腦惡意活動檢視					
		伺服器主機惡意活動檢視					
	目錄伺服器設定及防火牆連線設定檢視	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。	Inspection of cyber malicious activity		
	網路防火牆					Inspection of malicious activity of user	
	具有郵件伺服器者，應備電子郵件過濾機制						

認知 與訓練	資通安全 教育訓練	資通安全及資 訊人員	每年至少一名人員接受十二小時以上 之資通安全專業課程訓練或資通安全 職能訓練。
		一般使用者及 主管	每人每年接受三小時以上之一般資通 安全教育訓練。
	資通安全專 業證照及職 能訓練證書	資通安全專業 證照	資通安全專職人員總計應持有一張以 上。
		資通安全職能 評量證書	初次受核定或等級變更後之一年內，資 通安全專職人員總計應持有一張以上， 並持續維持證書之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、資通安全專職人員，指應全職執行資通安全業務者。

三、公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經主管機關認可之其他具有同等或以上效用之措施。

四、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

		terminal computer	
		Inspection of malicious activity of server	
		Inspection of setting of directory server and setting of firewall connection	
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the government agency shall complete activation of various cyber security defense measures, and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		Network firewall	
		If government agency has email server, it should have email filtering mechanism	
Awareness and training	Cyber security education and training	Cyber security and information personnel	Each year, at least one person shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each.
		General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours.
	Cyber security professional license and competence training certificate	Cyber security professional license	The full-time cyber security personnel shall hold a total of not less than one license.
		Cyber security competence assessment certificate	Within one year after receipt of initial approval or change of level, the full-time cyber security personnel shall held a total of not less than one certificate, and shall continually maintain the validity of certificate.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the installation, maintenance or development of such information and communication system.

2. The full-time cyber security personnel refer to the personnel who should implement cyber security businesses in full-time.

3. In conducting “cyber security health diagnosis” of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the government agency may take other measures which have equal or better effects as approved by the competent authority.

	4. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority(entity) recognized by the competent authority.
--	---

附表六

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				Schedule6: Matters to be conducted by the specific non-government agency of cyber security responsibility Level-C			
制度面向	辦理項目	辦理項目細項	辦理內容	System aspect	Items conducted	Sub-items conducted	Contents conducted
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，其後應每年至少檢視一次資通系統分級妥適性；系統等級為「高」者，應於初次受核定或等級變更後之二年內，完成附表十之控制措施。	Management aspect	Classification and defense standards of the information and communication system		Within one year after receipt of initial approval or change of level, the specific non-government agency shall complete the classifications of levels of the information and communication systems developed by itself or outsourced according to Schedule 9; subsequently, the specific non-government agency shall inspect the appropriateness of the classification of levels of information and communication systems at least once a year. If the system levels are “high”, the specific non-government agency shall, within two years of receipt of initial approval or change of levels, complete the control measures specified in Schedule 10.
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。		The importation of the information security management system		Within two years after receipt of initial approval or change of level, the specific non-government agency shall import to all of its core information and communication systems the national standards - CNS 27001 information security management system, or other systems or standards with equal or better effects, or other standards developed by the specific non-government agency itself and approved by the competent authority, and shall continually maintain the importation thereof.
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人。				
	內部資通安全稽核		每二年辦理一次。				
	業務持續運作演練		全部核心資通系統每二年辦理一次。				
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每二年辦理一次。		Dedicated cyber security personnel		Within one year after receipt of initial approval or change of level, the specific non-government agency shall deploy one person.
		系統滲透測試	全部核心資通系統每二年辦理一次。		Internal cyber security audit		Conduct once every two years.
	資通安全健診	網路架構檢視	每二年辦理一次。		Business sustainable operation rehearsal		Conduct once every two years for all core information and communication systems.
		網路惡意活動檢視					
		使用者端電腦惡意活動檢視					
		伺服器主機惡意活動檢視					
		目錄伺服器設定及防火牆連線設定檢視					
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。	Technical aspect	Security detection	Detection of website security vulnerability	Conduct once every two years for all core information and communication systems.
		網路防火牆				Testing of system penetration	Conduct once every two years for all core information and communication systems.
						具有郵件伺服器者，應備電子郵件過濾機制	
				Cyber security health diagnosis	Inspection of network framework	Conduct once every two years.	
					Inspection of cyber malicious activity		
					Inspection of malicious activities of user terminal computer		

認知與訓練	資通安全教育訓練	資通安全及資訊人員	每年至少一名人員接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。
	資通安全專業證照		初次受核定或等級變更後之一年內，資通安全專責人員總計應持有一張以上，並持續維持證照之有效性。

備註：

一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。

二、特定非公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。

三、特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。

四、資通安全專業證照，指由主管機關認可之國內外發證機關（構）所核發之資通安全證照。

		Inspection of malicious activities of server	
		Inspection of setting of directory server and setting of firewall connection	
	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, the specific non-government agency shall complete activation of various cyber security defense measures, and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		Network firewall	
		If the specific non-government agency has email server, it should have email filtering mechanism	
Awareness and training	Cyber security education and training	Cyber security and information personnel	Each year, at least one person shall receive the cyber security professional program training or the cyber security competence training for not less than twelve hours each.
		General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours.
	Cyber security professional license		Within one year after receipt of initial approval or change of level, the dedicated cyber security personnel shall held a total of not less than one license, and shall continually maintain the validity of license.

Notes:

1. If the nature of the information and communication system is a shared one, whether it belonged to the core one, it shall be judged by the agency in charge of the installation, maintenance or development of such information and communication system.
2. In conducting “cyber security health diagnosis” of this Schedule, in addition to implementation of the items, contents and timeframes specified in this Schedule, the specific non-government agency may take other measures which have equal or better effects as approved by central authority in charge of relevant industry.
3. The central authority in charge of relevant industry of the specific non-government agency may, depending on actual requirements and to the extent of compliance with requirements of these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.
4. Cyber security professional license refer to the cyber security professional license issued by domestic and foreign issuing authority(entity) recognized by the competent authority.

附表七

附表七 資通安全責任等級 D 級之各機關應辦事項				Schedule 7: Matters to be conducted by each agency of cyber security responsibility Level-D			
制度面向	辦理項目	辦理項目細項	辦理內容	System aspect	Items conducted	Sub-items conducted	Contents conducted
技術面	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。	Technical aspect	Cyber security defense	Anti-virus software	Within one year after receipt of approval or change of levels, each agency shall complete activation of various cyber security defense measures, and continue to use such measures and timely conduct the necessary update or upgrading of software and hardware.
		網路防火牆				Network firewall	
		具有郵件伺服器者，應備電子郵件過濾機制				If each agency has email server, it should have email filtering mechanism	
認知與訓練	資通安全教育訓練	一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。	Awareness and training	Cyber security education and training	General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours.
備註：特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。				Note: The central authority in charge of relevant industry of the specific non-government agency may, depending on actual requirements and to the extent of compliance with requirements of these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.			

附表八

附表八 資通安全責任等級 E 級之各機關應辦事項				Schedule 8: Matters to be conducted by each agency of cyber security responsibility Level-E			
制度面向	辦理項目	辦理項目細項	辦理內容	System aspect	Items conducted	Sub-items conducted	Contents conducted
認知與訓練	資通安全教育訓練	一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。	Awareness and training	Cyber security and education training	General user and officer	Each year, each person shall receive the general cyber security education training for not less than three hours.
備註：特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之資通安全應辦事項。				Note: The central authority in charge of relevant industry of the specific non-government agency may, depending on actual requirements and to the extent of compliance with requirements of these Regulations, otherwise provide for the cyber security matters to be conducted by its regulated specific non-government agency.			

附表九

附表九 資通系統防護需求分級原則				Schedule 9: Principles of classification of levels of defense requirements of information and communication system			
防護需求 等級 構面	高	中	普	Defense requirements Levels Dimension	High	Medium	Common
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。	Confidentiality	The occurrence of cyber security incident resulting in impact on information and communication system might cause unauthorized disclosure of information, leading to very serious or disastrous impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause unauthorized disclosure of information, leading to serious impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause unauthorized disclosure of information, leading to limited impact on the operation, asset or reputation of the agency.
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。	Integrity	The occurrence of cyber security incident resulting in impact on information and communication system might cause the error or tampering of the information, leading to very serious or disastrous impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause the error or tampering of the information, leading to serious impact on the operation, asset or reputation of the agency.	The occurrence of cyber security incident resulting in impact on information and communication system might cause the error or tampering of the information, leading to limit impact on the operation, asset or reputation of the agency.
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。	Availability	The occurrence of cyber security incident resulting in impact on the information and communication system might cause the interruption of access to or use of the information and information and communication system, leading to very serious or disastrous impact on	The occurrence of cyber security incident resulting in impact on the information and communication system might cause the interruption of access to or use of the information and information and communication system, leading to serious impact on the operation, asset or	The occurrence of cyber security incident resulting in impact on the information and communication system might cause the interruption of access to or use of the information and information and communication system, leading to limit impact on the operation, asset or
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。				
備註：資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性、法律遵循性構面中，任一構面之防護需求等級之最高者定之。							

		the operation, asset or reputation of the agency.	reputation of the agency.	reputation of the agency.
	Regulatory compliance	The failure to strictly comply with regulatory requirements relating to the installation or operation of information and communication system involving cyber security might cause impact on the information and communication system, leading to cyber security incidents, or impact on the legitimate rights and interests of others or the impartiality and justifiability of the agencies in the performance of businesses, and cause the personnel of the agencies to be subject to criminal liabilities.	The failure to strictly comply with regulatory requirements relating to the installation or operation of information and communication system involving cyber security might cause impact on the information and communication system, leading to cyber security incidents, or impact on the legitimate rights and interests of others or the impartiality and justifiability of the agencies in the performance of businesses, and cause the agencies or their personnel to be subject to administrative punishments, disciplines or penalties.	Other status of installation or operation of information and communication system under relevant regulatory requirements.
	Note: The defense requirement levels of the information and communication system shall be the highest ones as determined in any of the dimensions of confidentiality, integrity, availability and regulatory compliance relating to such systems.			

附表十

附表十 資通系統防護基準					Schedule 10: Defense standards of information and communication system				
系統防護需求 分級 控制措施		高	中	普	Defense requirements of systems		High	Medium	Common
					Level Control measure				
構面	措施內容				Dimension	Contents of the measures			
存取控制	帳號管理	一、逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出。 二、應依機關規定之情況及條件，使用資通系統。 三、監控資通系統帳號，如發現帳號違常使用時回報管理者。 四、等級「中」之所有控制措施。	一、已逾期之臨時或緊急帳號應刪除或禁用。 二、資通系統閒置帳號應禁用。 三、定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。 四、等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。	Access control	Account management	1. When the expected idle time prescribed by the agency or usable time is exceeded, the system should automatically logout the users.	1. The temporary or emergent accounts which have expired should be deleted or prohibited.	Establish the account management mechanism, including the procedure for application, activation, suspension and deletion.
	最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求。			2. Use the information and communication system according to the circumstances and conditions prescribed by the agency.	2. The idle accounts of information and communication system should be prohibited.	
	遠端存取	一、應監控資通系統遠端連線。 二、資通系統應採用加密機制。 三、資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點。 四、等級「普」之所有控制措施。		對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之權限檢查作業應於伺服器端完成。			3. Monitor the information and communication system accounts; report to the administrator if any abnormal use by an account is found	3. Periodically review the establishment, revision, activation, prohibition and deletion of accounts of information and communication systems.	
稽核與可歸責性	稽核事件	一、應定期審查稽核事件。 二、等級「普」之所有控制措施。		一、依規定時間週期及紀錄留存政策，保留稽核紀錄。 二、確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件。	Least privilege	The principle of least privilege is adopted. The users(or the procures for acts on behalf		No requirement	

			三、應稽核資通系統管理者帳號所執行之各項功能。				of users)are granted the authorized access required for the completion of duties only, depending on the duties and business functions of the agency .	
	稽 核 紀 錄 內 容	一、資通系統產生之稽核紀錄，應依需求納入其他相關資訊。 二、等級「普」之所有控制措施。		資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式之一致性。		Remote access	1. The remote connection with the information and communication system should be monitored. 2. The information and communication system should adopt encryption mechanism. 3. The source of the remote access to the information and communication system should be the access control point ad pre-defined and managed by the agency. 4. All control measures for the level of “common”.	For each kind of permitted remote access, the authorization should be obtained in advance; the use restriction, configuration requirement, connection requirement and documentation should be established; and the inspection operation of users’ privilege should be completed at the server terminal.
	稽 核 儲 存 容 量	依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。						
	稽 核 處 理 失 效 之 回 應	一、機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。 二、等級「中」及「普」之所有控制措施。	資通系統於稽核處理失效時，應採取適當之行動。					
	時 戳 及 校 時	一、系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。 二、等級「普」之所有控制措施。		資通系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。				
營運持續計畫	稽 核 資 訊 之 保 護	一、定期備份稽核紀錄至與原稽核系統不同之實體系統。 二、等級「中」之所有控制措施。	一、應運用雜湊或其他適當方式之完整性確保機制。 二、等級「普」之所有控制措施。	對稽核紀錄之存取管理，僅限於有權限之使用者。	Audit and accountability	Audit event	1. Audit events should be reviewed periodically. 2. All control measures for the level of “common”.	1. Retain the audit records according to the prescribed time cycle and the policies of record retention. 2. Assure that the information and communication system has the function of audit of specific events, and determine the specific information and communication system incidents to be audited. 3. Should audit various functions executed by the administrator account of the
	系 統 備 份	一、應將備份還原，作為營運持續計畫測試之一部分。 二、應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟	一、應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。 二、等級「普」之所有控制措施。	一、訂定系統可容忍資料損失之時間要求。 二、執行系統源碼與資料備份。				

識 別 與 鑑 別		體與其他安全相關資訊之備份。 三、等級「中」之所有控制措施。					information and communication system.
	系 統 備 援	一、訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 二、原服務中斷時，於可容忍時間內，由備援設備取代提供服務。	無要求。				Audit records generated by the information and communication system shall include other relevant information as required. 2. All control measures for the level of “common”.
	內 部 使 用 者 之 識 別 與 鑑 別	一、對帳號之網路或本機存取採取多重認證技術。 二、等級「中」及「普」之所有控制措施。	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。				Audit records generated by the information and communication system shall include the type of incidents, dates of occurrence, places of occurrence, and the information about the identification of the users relating to the incidents; single journal recording mechanism should be adopted to assure the consistency of the formats of output.
	身 分 驗 證 管 理	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。 三、等級「普」之所有控制措施。	一、使用預設密碼登入系統時，應於登入後要求立即變更。 二、身分驗證相關資訊不以明文傳輸。 三、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。 四、基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限制。 五、使用者更換密碼時，至少不可以與前三次使用過之密碼相同。 六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。				
	鑑 別 資 訊 回 饋	資通系統應遮蔽鑑別過程中之資訊。					

	Content of audit record	1. Audit records generated by the information and communication system shall include other relevant information as required. 2. All control measures for the level of “common”.					
	Storage capacity for the audit	Storage capacity required for the audit records shall be equipped depending on the requirement of the storage of audit records.					
	Response to failure in audit process	1. Upon occurrence of the audit failure events which should be reported immediately as required by the agency, the information and communication system should give warnings to the specific personnel within the timeframes prescribed by the agency. 2. All control measures for the levels of “medium” and “common”.					In case of failure in audit process, the information and communication system should take appropriate actions.
	Time stamp and time calibration	1. The internal clock of the system should synchronize with the time cycle specified by the agency and the source of standard times. 2. All control measures for the level of “common”.					The information and communication system should use the internal clock of the system to generate time stamps required for audit records, and such time stamps should be able to correspond to Universal Time Coordinated(UTC) or Greenwich Mean Time(GMT).

	加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。		無要求。
	非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。		
系 統 與 服 務 獲 得	系統發展生命週期需求階段	針對系統安全需求（含機密性、可用性、完整性），以檢核表方式進行確認。		
	系統發展生命週期設計階段	一、根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。 二、將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。		無要求。
	系統發展生命週期開發階段	一、執行「源碼掃描」安全檢測。 二、具備系統嚴重錯誤之通知機制。 三、等級「中」及「普」之所有控制措施。	一、應針對安全需求實作必要控制措施。 二、應注意避免軟體常見漏洞及實作必要控制措施。 三、發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	
	系統發展生命週期測試階段	一、執行「滲透測試」安全檢測。 二、等級「中」及「普」之所有控制措施。	執行「弱點掃描」安全檢測。	
	系統發展生命週期部署與維運階段	一、於系統發展生命週期之維運階段，須注意版本控制與變更管理。 二、等級「普」之所有控制措施。		一、於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。 二、資通系統相關軟體，不使用預設密碼。
	系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。		
	獲得程序	開發、測試及正式作業環境應為區隔。		無要求。
	系統文件	應儲存與管理系統發展生命週期之相關文件。		
系 統 與 通 訊 保 護	傳輸之機密性與完整性	一、資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。 二、使用公開、國際機構驗證且未遭破解之演算法。	無要求。	無要求。

	Protection of audit information	1. Periodically back up the audit records to the physical system different from the original audit system. 2. All control measures for the level of “medium”	1. Should use the integrity of the hashing or other proper methods to assure the mechanism. 2. All control measures for the level of “common”.	The access management of audit records is limited to the users with privileges.
Business continuity plan	Backup of system	1. Should take the backup and restore as a part of the testing of the business continuity plan. 2. Should store the important software of the information and communication system and backup of other security related information in the independent facilities or fire cabinets at the place different from the operating systems. 3. All control measures for the level of “medium”.	1. Should periodically test the backup information to verify the reliability of the backup media and the integrity of the information. 2. All control measures for the level of “common”.	1. Set the requirement for tolerable time of information loss of the system. 2. Execute the system source codes and the data backup.

系 統 與 資 訊 完 整 性		三、支援演算法最大長度金鑰。 四、加密金鑰或憑證週期性更換。 五、伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。		
	資料儲存之安全	靜置資訊及相關具保護需求之機密資訊應加密儲存。	無要求。	無要求。
	漏洞修復	一、定期確認資通系統相關漏洞修復之狀態。 二、等級「普」之所有控制措施。	系統之漏洞修復應測試有效性及潛在影響，並定期更新。	
	資通系統監控	一、資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。 二、等級「中」之所有控制措施。	一、監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。 二、等級「普」之所有控制措施。	發現資通系統有被入侵跡象時，應通報機關特定人員。
	軟體及資訊完整性	一、應定期執行軟體與資訊完整性檢查。 二、等級「中」之所有控制措施。	一、使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 二、使用者輸入資料合法性檢查應置放於應用系統伺服器端。 三、發現違反完整性時，資通系統應實施機關指定之安全保護措施。	無要求。
備註： 一、靜置資訊，指資訊位於資通系統特定元件，例如儲存設備上之狀態，或與系統相關需要保護之資訊，例如設定防火牆、閘道器、入侵偵測、防禦系統、過濾式路由器及鑑別符內容等資訊。 二、特定非公務機關之中央目的事業主管機關得視實際需求，於符合本辦法規定之範圍內，另行訂定其所管特定非公務機關之系統防護基準。				

	System rescue	1. Set the requirements for the tolerable time from the interruption of information and communication system to the recovery of service. 2. When the original service interrupts, the service is provided by the rescue equipment in lieu thereof within the tolerable time.	No requirement	
Identification and authentication	Identification and authentication of internal users	1. Adopt multiple authentication technologies for the network of accounts or the access to the host. 2. All control measures for the level of “medium” and “common”.	The information and communication system should have the function of identification and authentication of sole agency users(or the program of act on behalf of agency users); common accounts are prohibited.	
	identity verification management	1. Identity verification mechanism should prevent from the logon by automatic program or the trials of change of password. 2. The password resetting mechanism have verified identities of users again, and then send one-time and time-based tokens. 3. All control measures for the level of “common”.	1. When using the preset password to login the system, should immediately change the password after logon. 2. Information relating to identity verification may not be transmitted by plain text. 3. Have the account lockout mechanism; if the identity verification for account logon fails for three times, disallow such account to continue the trial of logon at least within fifteen minutes, or use the failure verification	

				<p>mechanisms built by the agencies themselves.</p> <p>4. The information and communication system with password-based authentication should impose the least complexity of password; impose the restriction on the shortest and longest validity of passwords</p> <p>5. When the users change password, at least the password may not be same as those used for previous three times.</p> <p>6. The measures specified in points 4 and 5 may be conducted for non-internal users according to the regulations formulated by the agencies themselves.</p>
		Authentication information feedback	The information and communication system should shield the information in the course of authentication.	
		Encryption module authentication	When the information and communication systems use the passwords for authentication, such passwords should be encrypted, or stored after hashing process.	No requirement
		Identification or authentication of non-internal users	The information and communication systems should identity and authenticate non-internal users(or the program of act on behalf of agency users).	
	Access to systems and services	Requirement phase of system	Use the method of checklist to confirm the system security requirements(including confidentiality, availability and integrity).	

	development life circle		
	Design phase of system development life circle	<ol style="list-style-type: none"> Depending on the system functions and requirements, identify the threats that might impact on the system, to conduct risk analysis and assessment. Feedback the risk assessment results to the screening items of the requirement phase, and submit the revision of security requirements. 	No requirement
	Development phase of system development life circle	<ol style="list-style-type: none"> Execute “source code scanning” security testing. Have the notification mechanisms of serious error of the system. All control measures for the level of “medium” and “common”. 	<ol style="list-style-type: none"> Should practice necessary control measures for the security requirements. Should pay attention to the avoidance of common software vulnerabilities, and practice necessary measures. When errors occur, the user’s pages display short error message and code only, without detailed error message.
	Testing phase of system development life circle	<ol style="list-style-type: none"> Execute “penetration testing” security testing. All control measures for the level of “medium” and “common”. 	Execute “vulnerability scanning” security testing.
	Deployment and maintenance operation phase of system development life circle	<ol style="list-style-type: none"> In the maintenance operation phase of system development life circle, attention should be paid to the version control and change management. All control measures for the level of “common”. 	<ol style="list-style-type: none"> Under the deployment environment, should conduct update and fixing of relevant cyber security threats, and close unnecessary services and ports. Not to use preset passwords for relevant software of information

			and communication system.	
	Outsourcing phase of system development life circle	If the development of the information and communication system is outsourced, the security requirements by level(including confidentiality, availability, integrity) for each phase of system development life circle shall be included in the outsourcing contract.		
	Obtaining programs	Development, testing, and formal operation environments should be separated.	No requirement	
	System documents	Should store the documents relating to the management system development life circle.		
	Protection of systems and communications	confidentiality and integrity of transmission	1. The information and communication system should adopt encryption mechanism, to prevent from unauthorized disclosure of information or to detect the change of information; unless there are substitutive physical protection measures in the course of transmission. 2. Use public, international institution verified and not cracked algorithms. 3. Support the maximum length key of algorithms. 4. Periodically change the encryption key or certification. 5. Should formulate the management regulations on the custody of key at server terminal, and implement	No requirement

			security protection measures that should exist.			
		Securities of data storage	The static information and the relevant confidential information required for protection should be encrypted for the storage.		No requirement.	No requirement.
	Integrity of systems and information	Vulnerability fixing	1. Periodically confirm the status of fixing of relevant vulnerabilities of the information and communication system. 2. All control measures for the level of “common”.		The vulnerability fixing of the system should be tested for the effectiveness and potential impact, and should be updated periodically.	
		Monitoring of information and communication system	1. The information and communication system should adopt automatic tools to monitor the access communication flows; if unusual or unauthorized activities are found, conduct the analysis of such activity. 2. All control measures for the level of “medium”.	1. Monitor the information and communication system to detect the attack and unauthorized connection and to identify the unauthorized users of the information and communication system. 2. All control measures for the level of “common”.	If a sign of hacking to the information and communication system is found, should notify the specific personnel of the agencies thereof.	
		The integrity of software and information	1. Should conduct the inspection of the integrity of software and information. 2. All control measures for	1. Use the integrity verification tools to detect the unauthorized change of specific software and information. 2. The examination of the legitimacy of input data of	No requirement	

			the level of “medium”.	users should be placed on the server terminal of the application system. 3. If any violation to the integrity is found, the information and communication system should implement the security protection measures designated by the agency.	
<p>Notes:</p> <p>1. Static information refers to the information located at the specific elements in information and communication systems, such as the status of being stored in the equipment, or the information relating to the system that is required for protection, such as the information of contents of setting firewalls, gateways, hacking detection, defense system, filtering routers, and authentication token etc.</p> <p>2. The government authority in charge of subject industry at the central government level of the specific non-government agency may, depending on the actual requirements and to the extent of compliance with these Regulations, otherwise provide for the information and communication system defense standards of its regulated specific non-government agency.</p>					