檔　　號：
保存年限：

教育部　函

機關地址：100217 臺北市中正區中山南路5號
承辦人：李政諺
電話：(02)7736-9478
電子信箱：ab3300186@mail.moe.gov.tw

受文者：國立臺北大學

發文日期：中華民國115年1月19日
發文字號：臺教資通字第1150002086號
速別：普通件
密等及解密條件或保密期限：
附件：數位發展部來文、資通安全責任等級分級辦法發布令、資通安全責任等級分級辦法部分修正條文、資通安全責任等級分級辦法部分條文修正附表一到十、資通安全責任等級分級辦法部分條文修正總說明及條文對照表 (附件一 A095G0000Q0000000_A09000000E_1150002086_senddoc2_Attach1.PDF、附件二 A095G0000Q0000000_A09000000E_1150002086_senddoc2_Attach2.pdf、附件三 A095G0000Q0000000_A09000000E_1150002086_senddoc2_Attach3.odt、附件四 A095G0000Q0000000_A09000000E_1150002086_senddoc2_Attach4.pdf、附件五 A095G0000Q0000000_A09000000E_1150002086_senddoc2_Attach5.pdf)

主旨：轉知數位發展部「資通安全責任等級分級辦法」部分條文修正相關事宜，請查照並轉知所屬。

說明：依數位發展部115年1月7日數授資法字第11450004164號函辦理。

正本：本部各單位、教育部國民及學前教育署、教育部青年發展署、國立臺灣科學教育館、國立臺灣藝術教育館、國立自然科學博物館、國家圖書館、國立科學工藝博物館、國立教育廣播電臺、國立海洋生物博物館、國家教育研究院、國立公共資訊圖書館、國立臺灣圖書館、國立海洋科技博物館、各國立大專校院、國立臺灣大學生物資源暨農學院附設山地實驗農場、國立臺灣大學生物資源暨農學院附設動物醫院、國立臺灣大學生物資源暨農學院實驗林管理處、國立臺灣大學生物資源暨農學院附設農業試驗場、國立中興大學農業暨自然資源學院實驗林管理處、國立成功大學醫學院附設醫院、國立成功大學醫學院附設醫院斗六分院、國立陽明交通大學附設醫院、財團法人蔣經國國際學術交流基金會、財團法人吳健雄學術基金會、財團法人高等教育評鑑中心基金會、財團法人大學入學考試中心基金會、財團法人高等教育國際合作基金會、財團法人社教文化基金會、財團法人台灣省中小學校教職員福利文教基金會、財團法人教育部接受捐助獎學基金會、財團法人私立學校興學基金會、財團法人臺灣省童軍文教基金會、財團法人中華幼兒教育發展基金會

副本：115/01/19 10:29:30

國立臺北大學
1150500755　115/01/19

檔　　號:
保存年限:

數位發展部 函

地址：100235臺北市中正區北平東路2號
聯絡人：李宇勝
電話：(02)23808812
電子郵件：james74150@acs.gov.tw

受文者：教育部

發文日期：中華民國115年1月7日
發文字號：數授資法字第11450004164號
速別：普通件
密等及解密條件或保密期限：
附件：如主旨（50004164_資通安全責任等級分級辦法部分修正條文文字檔.odt、50004164_資通安全責任等級分級辦法部分條文修正_附表一到十.pdf、50004164_資通安全責任等級分級辦法部分條文修正總說明及條文對照表.pdf、50004164_資通安全責任等級分級辦法發布令掃描檔.pdf）

主旨：「資通安全責任等級分級辦法」部分條文，業經本部於115年1月7日以數授資法字第1145000416號令修正發布，檢送修正條文及附表各1份，請查照並轉知所屬。

正本：總統府及其他機關、行政院各部會行總處(不含本部)、四院及其所屬、各直轄市政府、各縣（市）政府、各直轄市議會、各縣（市）議會

副本：2026/01/07 10:11:33

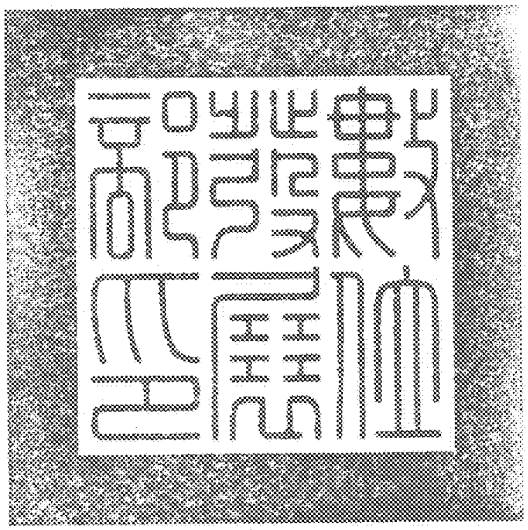
A095G0000Q0000000_A09000000E_1150002086_senddoc2_Attach1.PDF 第 1 頁，共 5 頁

1150002086 收文日期:115/01/07

檔　　號：
保存年限：

數位發展部　令

發文日期：中華民國115年1月7日
發文字號：數授資法字第1145000416號



修正「資通安全責任等級分級辦法」部分條文。

附修正「資通安全責任等級分級辦法」部分條文

部長 林宜敬

資通安全責任等級分級辦法部分條文修正總說明

資通安全責任等級分級辦法（以下簡稱本辦法）前經行政院一百零七年十一月二十一日訂定發布，並自一百零八年一月一日施行。最近一次修正發布日期係一百十年八月二十三日。茲因資通安全管理法於一百十四年九月二十四日修正公布，為配合部分條文內容修正及因應實務運作所需，爰修正本辦法部分條文，其修正要點如下：

一、 修正本辦法訂定之依據。（修正條文第一條）

二、 配合主管機關調適，修正直轄市及縣（市）議會提交自身資通安全責任等級報主管機關核定。（修正條文第三條）

三、 將關鍵基礎設施納為等級調整考量事項，及配合本辦法第三條修正，酌作文字調整。（修正條文第十條）

四、 明定各機關得準用中央目的事業主管機關所定特定類型資通系統防護基準規定、等級提交或等級核定機關經主管機關同意或備查後始得免執行本辦法附表所定事項或控制措施，以及機關於各該次修正施行前已受核定者，其新增應辦事項辦理期限自各該修正施行之日起算；並修正附表一至附表七之資通安全責任等級A至D級機關應辦事項及附表十資通系統防護基準控制措施之規定。（修正條文第十一條）

資通安全責任等級分級辦法部分條文修正條文對照表

修正條文	現行條文	說明
第一條　本辦法依資通安全管理法（以下簡稱本法）第七條第三項規定訂定之。	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。	資通安全管理法（以下簡稱本法）授權訂定本辦法之項次變更，爰配合修正訂定依據。
第三條　行政院應每三年核定自身資通安全責任等級，送主管機關備查；行政院直屬機關應每三年提交自身、所屬、所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。 直轄市、縣（市）政府應每三年提交自身、所屬、所監督之公務機關，與所轄鄉（鎮、市）公所、直轄市山地原住民區公所、鄉（鎮、市）民代表會及直轄市山地原住民區民代表會及其所屬或所監督之公務機關之資通安全責任等級，報主管機關核定；直轄市及縣（市）議會應每三年提交自身資通安全責任等級，報主管機關核定。 總統府、國家安全會議、立法院、司法院、考試院及監察院應每三年核定自身、所屬、所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。 各機關因組織或業務調整，致須變更原資通安全責任等級時，應	第三條　主管機關應每二年核定自身資通安全責任等級。 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。 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。 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。 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。 各機關因組織或業	一、配合現行實務運作及尊重五院立場，仍由行政院核定自身資通安全責任等級，並合併現行條文第一項及第二項，調整各項項次。另因本法第七條第一項規定各機關應報由主管機關核定或備查其資通安全責任等級，爰酌修第一項文字。 二、本辦法自一百零八年施行以來，各機關如因組織或業務變更，應依實際情況適時提報資通安全責任等級異動，考量相關機制已臻成熟，爰將核定週期由二年調整為三年。 三、配合直轄市及縣（市）議會資通安全責任等級報主管機關核定方式變更，將現行條文第三項及第四項合併，並調整各項項次及酌作文字修正。

即依前三項規定程序辦理等級變更；有新設機關時，亦同。 第一項至第三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。	務調整，致須變更原資通安全責任等級時，應即依前五項規定程序辦理等級變更；有新設機關時，亦同。 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。	
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三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： 一、業務涉及外交、國防、國土安全或關鍵基礎設施者，其中斷或受妨礙。 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。 三、各機關依層級之不同，其功能受影響、失效或中斷。	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： 一、業務涉及外交、國防、國土安全、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。 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、	第十條第一款所稱能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院等業務皆涉及關鍵基礎設施，考量除前開事項外，亦有政府機關、科學園區與工業區、糧食等應併予納入，爰該等業務皆以關鍵基礎設施稱之，並配合本辦法第三條修正，酌作文字調整。

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。	破壞、竄改、銷毀或其他侵害。 三、各機關依層級之不同，其功能受影響、失效或中斷。 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。	
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。 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。特定非公務機關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。 公務機關經其上級機關或監督機關同意者，準用中央目的事業主管機關依前項所定防護基準相關規定辦理；其他特定非公務機關經其中央目的事業主管機關同意者，亦同。 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有困難者，得經第三條第一項後段及	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。 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；特定非公務機關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。 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；其為主管機關者，經其同意後，免予執行。	一、考量部分公務機關亦有維運特定類型資通系統，第三項增訂公務機關經其上級機關或監督機關同意者，準用中央目的事業主管機關所定之各該類型防護基準規定辦理，其他特定非公務機關有適用情形者，亦同。 二、現行第三項移列為第四項，並配合實務執行酌作文字修正。 三、現行第四項移列為第五項，並修訂公務機關皆應依主管機關指定方式提報應辦事項辦理情形。 四、現行第五項移列為第六項，並酌作文字修正。 五、第七項增訂機關初次受核定或等級變更後之一定期限內，辦理附表應辦事項或執行控制及防護措施。

第二項所定其等級提交機關或同條第一項前段及第三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。等級提交機關有前段情形者，經主管機關同意後，免予執行；其為等級核定機關者，經報請主管機關備查後，免予執行。 公務機關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。 中央目的事業主管機關得要求其所管特定非公務機關，依其指定之方式提報第一項及第二項事項之辦理情形。 附表一至附表十之規定，各機關因修正而須於所定期限內辦理新增或異動項目，辦理期限自修正施行之日起算。	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。 中央目的事業主管機關得要求所管特定非公務機關，依其指定之方式提報第一項及第二項事項之辦理情形。	

第十一條附表一修正對照表

修正規定

附表一　資通安全責任等級A級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		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及其防護基準之妥適性。
	資訊安全管理系統之導入及通過公正第三方之驗證		全部核心資通系統導入CNS 27001或ISO 27001等資訊安全管理系統標準、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，完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專職人員		配置四人以上。
	內部資通安全稽核		每年辦理二次。
	營運持續計畫演練		全部核心資通系統每年辦理一次。
	資安治理成熟		每年辦理一次。

現行規定

附表一　資通安全責任等級A級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
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。
	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或ISO 27001等資訊安全管理系統標準、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。
	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		全部核心資通系統每年辦理一

說明

一、配合本辦法中華民國一百十年八月二十三日修正施行前已受核定者，以及本辦法第十一條第七項增訂機關初次受核定或等級變更後之一定期限內完成各應辦事項，爰調整相關文字，並於備註九增列期限之要求。

二、機關自行或委外開發之資通系統除應每年檢視分級之妥適性外，亦應確認防護基準執行情形，爰增訂應每年檢視資通系統防護基準之妥適性。

三、配合本法第十八條第一項之修正，定明為資通安全專職人員，並修正備註三資通安全專職人員及資通安全專職人員以外之資訊人員之定義。

四、配合附表十資通系統防護基準規定，「業務持續運作演練」改為「營運持續計畫演練」。

五、為強化資料庫防護安全，機關應定期檢視資料庫連線及登入等防護情形，以防安全性設定不足，使內部資訊遭致不當揭露、竄改或竊取之可能風險，

	演練		次。
	資安治理成熟度評估		每年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每年辦理二次。
		滲透測試	全部核心資通系統每年辦理一次。
	資通安全健診	網路架構檢視	每年辦理一次。
		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。其監控範圍應包括本表所定「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心

爰於資通安全健診項目調修文字並增訂「核心資通系統資料庫安全檢視」。

六、「資通安全威脅偵測管理機制」更名為「資通安全監控管理機制」，其監控範圍酌作文字修正。

七、「資通安全弱點通報機制」更名為「資通安全弱點管理」；另機關針對資安警訊、資通安全弱點管理或安全性檢測作業等所發現弱點，應適時修補或採行緩解措施，爰調修該項及備註五相關文字。

八、「認知與訓練」酌作文字修正，以資明確。

九、調修備註七「資通安全專業證照」之名詞定義，並於備註八新增「資通安全職能訓練證書」之名詞定義；備註九律定各應辦事項辦理期限規定，其中「端點偵測及應變機制」改為初次受核定或等級變更後之一年內，完成導入作業。

	度評估		
技術面	安全性檢測	弱點掃描	全部核心資通系統每年辦理二次。
		滲透測試	全部核心資通系統每年辦理一次。
	資通安全健診	網路架構檢視	每年辦理一次。
		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	
		目錄服務系統設定及防火牆連線設定檢視	
		核心資通系統資料庫安全檢視	
	資通安全監控管理機制		完成監控管理機制建置，並持續維運及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所定「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務

			資通系統之資通設備紀錄及資訊服務或應用程式紀錄。
	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。
	資通安全弱點通報機制		一、初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
	端點偵測及應變機制		一、初次受核定或等級變更後之二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關
		系統與核心資通系統之日誌紀錄及資通設備紀錄。	
	政府組態基準	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。	
	資通安全弱點管理	一、知悉資通安全弱點時，應適時修補或採行緩解措施。 二、依主管機關指定方式導入弱點管理作業，並持續維運。	
	端點偵測及應變機制	完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。	
	資通安全防護	防毒軟體 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	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。

		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	資通安全專職人員	每人每年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。
		資通安全專職人員以外之資訊人員	每人每二年接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書		資通安全專職人員各自持有證照及證書各一張以上，並持續維持證照及證書之有效性。

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；第三方核發之驗證證書應有前開委託機構之認證標誌。

三、資通安全專職人員，指應全職執行資通安全業務者，亦即資通安全為其主要核心業務，且應優先辦理。資通安全專職人員以外之資訊人員，指其他實際從事資通安全業務或資訊業務之人員。

四、公務機關辦理本表「資通安全健診」時，除依本

			指定之方式提交偵測資料。
	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	資通安全專職人員	每人每年至少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。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。

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、資通安全弱點管理，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。

六、端點偵測及應變機制，指具備對端點進行主動式掃描偵測、漏洞防護、可疑程式或異常活動行為分析及相關威脅程度呈現功能之防護作業。

資通安全專業證照，指經主管機關公告之資通安全專業證照。

資通安全職能訓練證書，指通過主管機關資通安全職能評量所核發之證書。

九、應辦事項辦理期限

(一)資通系統分級及防護基準：應於初次受核定或等級變更後之一年內完成；資通系統新增、系統分級變更或其適用防護基準有異動情形時，亦同。

(二)資訊安全管理系統之導入及通過公正第三方之驗證：應於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資訊安全管理系統，並於三年內完成公正第三方驗證。

(三)資通安全監控管理機制、政府組態基準、資通安全弱點管理、端點偵測及應變機制：應於初次受核定或等級變更後之一年內，完成導入作業；主管機關公告新增政府組態基準項目，亦同。

(四)資通安全防護：應於初次受核定或等級變更後之一年內完成啟用，並持續使用。

(五)配置資通安全專職人員、資通安全教育訓練、資通安全專業證照及職能訓練證書：應於初次受核定或等級變更後之一年內完成；

	一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書	一、初次受核定或等級變更後之一年內，至少四名資通安全專職人員，分別各自持有證照及證書各一張以上，並持續維持證照及證書之有效性。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內符合規定。

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；第三方核發之驗證證書應有前開委託機構之認證標誌。

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、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。

六、端點偵測及應變機制，指具備對端點進行主動式掃描偵測、漏洞防護、可疑程式或異常活動行為分析及相關威脅程度呈現功能之防護作業。

七、資通安全專業證照，指由主管機關認可之國內外

人員異動時，亦同。 (六)其餘應辦事項應於初次受核定、等級變更或核心資通系統異動後之次年度起，依附表規定辦理。	發證機關（構）所核發之資通安全證照。	

第十一條附表二修正對照表

修正規定

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

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		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及其防護基準之妥適性。
	資訊安全管理系統之導入及通過公正第三方之驗證		全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、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，完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專職人員		配置四人以上。
	內部資通安全稽核		每年辦理二次。
	營運持續計畫演練		全部核心資通系統每年辦理一次。
	資安治理成熟度評估		關鍵基礎設施提供者每年辦理一次。

現行規定

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

制度面向	辦理項目	辦理項目細項	辦理內容
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。
	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 或 ISO 27001 等資訊安全管理系統標準、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。
	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。
	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。
技	安	弱點掃描	全部核心資通系統每年辦理二

說明

一、配合本辦法中華民國一百十年八月二十三日修正施行前已受核定者，以及本辦法第十一條第七項增訂機關初次受核定或等級變更後之一定期限內完成各應辦事項，爰調整相關文字，並於備註十增列期限之要求。

二、機關自行或委外開發之資通系統除應每年檢視分級之妥適性外，亦應確認防護基準執行情形，爰增訂應每年檢視資通系統防護基準之妥適性。

三、配合本法第二十條第二項及第二十一條第一項之修正，定明為資通安全專職人員，並於備註三新增資通安全專職人員及資通安全專職人員以外之資訊人員之定義，其後點次遞移。

四、配合附表十資通系統防護基準規定，「業務持續運作演練」改為「營運持續計畫演練」。

五、為提升關鍵基礎設施提供者資安治理，爰新增每年辦理一次「資安治理成熟度評估」。

六、為強化資料庫防護安全，機關應定期檢視資料庫連線及登入等防護情形，以防安全性設定

技術面	安全性檢測	弱點掃描	全部核心資通系統每年辦理二次。
		滲透測試	全部核心資通系統每年辦理一次。
	資通安全健診	網路架構檢視	每年辦理一次。
		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	
		目錄服務系統設定及防火牆連線設定檢視	
		核心資通系統資料庫安全檢視	
	資通安全監控管理機制		完成監控管理機制建置，並持續維運及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所定「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄。
技術面	全性檢測		次。
		滲透測試	全部核心資通系統每年辦理一次。
	資通安全健診	網路架構檢視	每年辦理一次。
		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。其監控範圍應包括本表所定「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄。
	資通安全弱點通報機制		一、關鍵基礎設施提供者初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持

不足，使內部資訊遭致不當揭露、竄改或竊取之可能風險，爰於資通安全健診項目調修文字並增訂「核心資通系統資料庫安全檢視」。

七、「資通安全威脅偵測管理機制」更名為「資通安全監控管理機制」；另為即時掌握資通安全監控管理情形，提升國家資安整體應變與防護能力，爰增訂特定非公務機關提交資料之規定。

八、「資通安全弱點通報機制」更名為「資通安全弱點管理」；另機關針對資安警訊、資通安全弱點管理或安全性檢測作業等所發現弱點，應適時修補或採行緩解措施，爰調修該項及備註五相關文字。

九、考量資通安全威脅日趨多樣，為提升特定非公務機關主動偵測及防護能力，爰增訂「端點偵測及應變機制」，並於備註六新增定義。

十、為提供特定非公務機關資安專職人員多元訓練管道，除規定須取得資通安全專業證照外，新增亦可取得資通安全職能訓練證書，爰修正相關規定。

十一、調修備註七「資通安全專業證照」之名詞定義，並於備註

			八新增「資通安全職能訓練證書」之名詞定義；備註十律定各應辦事項辦理期限規定。	
			續維運及依主管機關指定之方式提交資訊資產盤點資料。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。	
	資通安全防護	防毒軟體 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	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。	
			通系統之日誌紀錄及資通設備紀錄。	
		資通安全弱點管理	一、知悉資通安全弱點時，應適時修補或採行緩解措施。 二、關鍵基礎設施提供者依主管機關指定方式導入弱點管理作業，並持續維運。	
		端點偵測及應變機制	完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。	
	資通安全防護	防毒軟體 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	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。	

		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	資通安全專職人員	每人每年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。
		資通安全專職人員以外之資訊人員	每人每二年接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照或職能訓練證書		資通安全專職人員各自持有證照或證書一張以上，並持續維持證照或證書之有效性。

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；第三方核發之驗證證書應有前開委託機構之認證標誌。

三、資通安全專職人員，指應全職執行資通安全業務者，亦即資通安全為其主要核心業務，且應優先辦理。資通安全專職人員以外之資訊人員，指其他實際從事資通安全業務或資訊業務之人員。

四、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

		施	
認知與訓練	資通安全教育訓練	資通安全專責人員	每人每年至少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。
		資通安全專責人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照		一、初次受核定或等級變更後之一年內，至少四名資通安全專責人員，各自持有證照一張以上，並持續維持證照之有效性。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內符合規定。

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；第三方核發之驗證證書應有前開委託機構之認證標誌。

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

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。 五、資通安全弱點管理，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。 六、端點偵測及應變機制，指具備對端點進行主動式掃描偵測、漏洞防護、可疑程式或異常活動行為分析及相關威脅程度呈現功能之防護作業。 七、資通安全專業證照，指經主管機關公告之資通安全專業證照。 八、資通安全職能訓練證書，指通過主管機關資通安全職能評量所核發之證書。 九、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。 前項應辦事項辦理期限 (一)資通系統分級及防護基準：應於初次受核定或等級變更後之一年內完成；資通系統新增、系統分級變更或其適用防護基準有異動情形時，亦同。 (二)資訊安全管理系統之導入及通過公正第三方之驗證：應於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資訊安全管理系統，並於三年內完成公正第三方驗證。 (三)資通安全監控管理機制、資通安全弱點管理、端點偵測及應變機制：應於初次受核定或等級變更後之一年內，完成導入作業。 (四)資通安全防護：應於初次受核定或等級變更後之一年內完成啟用，並持續使用。 (五)配置資通安全專職人員、資通安全教育訓練、資通安全專業證照或職能訓練證書：應	或以上效用之措施。 四、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。 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。 六、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。	

於初次受核定或等級變更後之一年內完成；人員異動時，亦同。 (六)其餘應辦事項應於初次受核定、等級變更或核心資通系統異動後之次年度起，依附表規定辦理。		

第十一條附表三修正對照表

修正規定

附表三　資通安全責任等級B級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面		資通系統分級及防護基準	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及其防護基準之妥適性。
		資訊安全管理系統之導入及通過公正第三方之驗證	全部核心資通系統導入CNS 27001或ISO 27001等資訊安全管理系統標準、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，完成公正第三方驗證，並持續維持其驗證有效性。
		資通安全專職人員	配置二人以上。
		內部資通安全稽核	每年辦理一次。
		營運持續計畫演練	全部核心資通系統每二年辦理一次。
		資安治理成熟度評估	每年辦理一次。

現行規定

附表三　資通安全責任等級B級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
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。
		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或ISO 27001等資訊安全管理系統標準、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。
		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。
		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。

說明

一、配合本辦法中華民國一百十年八月二十三日修正施行前已受核定者，以及本辦法第十一條第七項增訂機關初次受核定或等級變更後之一定期限內完成各應辦事項，爰調整相關文字，並於備註九增列期限之要求。

二、機關自行或委外開發之資通系統除應每年檢視分級之妥適性外，亦應確認防護基準執行情形，爰增訂應每年檢視資通系統防護基準之妥適性。

三、配合本法第十八條第一項之修正，定明為資通安全專職人員，並修正備註三資通安全專職人員及資通安全專職人員以外之資訊人員之定義。

四、配合附表十資通系統防護基準規定，「業務持續運作演練」改為「營運持續計畫演練」。

五、為強化資料庫防護安全，機關應定期檢視資料庫連線及登入等防護情形，以防安全性設定不足，使內部資訊遭致不當揭露、竄改或竊取之可能風險，爰於資通安全健診項目調修文字並增訂「核心資通系統資料

	資安治理成熟度評估		每年辦理一次。	庫安全檢視」。 六、「資通安全威脅偵測管理機制」更名為「資通安全監控管理機制」，其監控範圍酌作文字修正。 七、「資通安全弱點通報機制」更名為「資通安全弱點管理」；另機關針對資安警訊、資通安全弱點管理或安全性檢測作業等所發現弱點，應適時修補或採行緩解措施，爰調修該項及備註五相關文字。 八、「認知與訓練」酌作文字修正，以資明確。 九、調修備註七「資通安全專業證照」之名詞定義，並於備註八新增「資通安全職能訓練證書」之名詞定義；備註九律定各應辦事項辦理期限規定，其中「端點偵測及應變機制」改為初次受核定或等級變更後之一年內，完成導入作業。
技術面	安全性檢測	弱點掃描	全部核心資通系統每年辦理一次。	
		滲透測試	全部核心資通系統每二年辦理一次。	
	資通安全健診	網路架構檢視	每二年辦理一次。	
		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		
		目錄服務系統設定及防火牆連線設定檢視		
		核心資通系統資料庫安全檢視		
	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。其監控範圍應包括本表所定「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統之資通設備紀錄及資	
技術面	安全性檢測	弱點掃描	全部核心資通系統每年辦理一次。	
		滲透測試	全部核心資通系統每二年辦理一次。	
	資通安全健診	網路架構檢視	每二年辦理一次。	
		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		
		目錄服務系統設定及防火牆連線設定檢視		
		核心資通系統資料庫安全檢視		
	資通安全監控管理機制		完成監控管理機制建置，並持續維運及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所定「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與核心資	

		通系統之日誌紀錄及資通設備紀錄。	
	政府組態基準	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。	
	資通安全弱點管理	一、知悉資通安全弱點時，應適時修補或採行緩解措施。 二、依主管機關指定方式導入弱點管理作業，並持續維運。	
	端點偵測及應變機制	完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。	
	資通安全防護	防毒軟體 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	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。

		訊服務或應用程式紀錄。	
	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。	
	資通安全弱點通報機制	一、初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。	
	端點偵測及應變機制	一、初次受核定或等級變更後之二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關	

		備應用程式防火牆	
認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年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。
		資通安全專職人員以外之資訊人員	每人每二年接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
	資通安全專業證照及職能訓練證書		資通安全專職人員各自持有證照及證書各一張以上，並持續維持證照及證書之有效性。

			指定之方式提交偵測資料。
	資通安全防護	防毒軟體 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	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。
認知與訓練	資通安全教育訓練	資通安全專職人員	每人每年至少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。
		資通安全專職人員以外之資訊人員	每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
		一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。

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；第三方核發之驗證證書應有前開委託機構之認證標誌。

三、資通安全專職人員，指應全職執行資通安全業務者，亦即資通安全為其主要核心業務，且應優先辦理。資通安全專職人員以外之資訊人員，指其他實際從事資通安全業務或資訊業務之人員。

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、資通安全弱點管理，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。 六、端點偵測及應變機制，指具備對端點進行主動式掃描偵測、漏洞防護、可疑程式或異常活動行為分析及相關威脅程度呈現功能之防護作業。 七、資通安全專業證照，指經主管機關公告之資通安全專業證照。 八、資通安全職能訓練證書，指通過主管機關資通安全職能評量所核發之證書。 九、應辦事項辦理期限 (一)資通系統分級及防護基準：應於初次受核定或等級變更後之一年內完成；資通系統新增、系統分級變更或其適用防護基準有異動情形時，亦同。 (二)資訊安全管理系統之導入及通過公正第三方之驗證：應於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資訊安全管理系統，並於三年內完成公正第三方驗證。 (三)資通安全監控管理機制、政府組態基準、資通安全弱點管理、端點偵測及應變機制：應於初次受核定或等級變更後之一年內，完成導入作業；主管機關公告新增政府組態基準項目，亦同。 (四)資通安全防護：應於初次受核定或等級變更後之一年內完成啟用，並持續使用。 (五)配置資通安全專職人員、資通安全教育訓練、資通安全專業證照及職能訓練證書：應於初次受核定或等級變更後之一年內完成；人員異動時，亦同。		
	資通安全專業證照及職能訓練證書	一、初次受核定或等級變更後之一年內，至少二名資通安全專職人員，分別各自持有證照及證書各一張以上，並持續維持證照及證書之有效性。 二、本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內符合規定。	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；第三方核發之驗證證書應有前開委託機構之認證標誌。 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、資通安全弱點通報機制，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。 六、端點偵測及應變機制，指具備對端點進行主動式掃描偵測、漏洞防護、可疑程式或異常活動行為分析及相關威脅程度呈現功能之防護作業。 七、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。	