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。

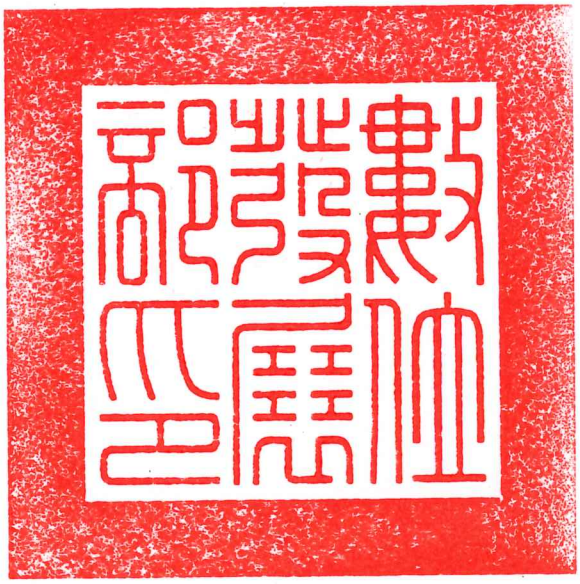
正本：總統府及其他機關、行政院各部會行總處(不含本部)、四院及其所屬、各直轄市政府、各縣（市）政府、各直轄市議會、各縣（市）議會
副本：電子公文交換章 2026/01/07 10:14:33

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



裝

訂　修正「資通安全責任等級分級辦法」部分條文。

線　附修正「資通安全責任等級分級辦法」部分條文

部長 林宜敬

第十一條附表一修正規定

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	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。

(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。

第十一條附表二修正規定

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。
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	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。

十、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。
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	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。
（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。

第十一條附表四修正規定

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

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		關鍵基礎設施提供者每年辦理一次。
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。
	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。

<table>
<tr><td rowspan="6"></td><td colspan="2"></td><td>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。</td></tr>
<tr><td colspan="2">端點偵測及應變機制</td><td>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。</td></tr>
<tr><td rowspan="4">資通安全防護</td><td>防毒軟體</td><td rowspan="4">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。</td></tr>
<tr><td>網路防火牆</td></tr>
<tr><td>具有郵件伺服器者，應備電子郵件過濾機制</td></tr>
<tr><td>入侵偵測及防禦機制</td></tr>
<tr><td rowspan="4">認知
與訓練</td><td rowspan="3">資通安全
教育訓練</td><td>資通安全專職人員</td><td>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。</td></tr>
<tr><td>資通安全專職人員以外之資訊人員</td><td>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。</td></tr>
<tr><td>一般使用者及主管</td><td>每人每年接受三小時以上之資通安全通識教育訓練。</td></tr>
<tr><td colspan="2">資通安全專業證照或職能訓練證書</td><td>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。</td></tr>
</table>

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。
十、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。

第十一條附表五修正規定

附表五 資通安全責任等級C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		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，並持續維持導入。
	資通安全專職人員		配置一人以上。
	內部資通安全稽核		每二年辦理一次。
	營運持續計畫演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		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	
	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。
	資通安全防護	防毒軟體	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	

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		資通安全專職人員分別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、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。

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。

五、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。

六、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。

七、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依附表九完成分級，並於二年內完成附表十控制措施；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：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。

(三)資通安全弱點管理：應於初次受核定或等級變更後之二年內，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。

(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。

第十一條附表六修正規定

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

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		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，並持續維持導入。
	資通安全專職人員		配置一人以上。
	內部資通安全稽核		每二年辦理一次。
	營運持續計畫演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		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	
	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。

	資通安全 防護	防毒軟體	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	
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、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。

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、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。

五、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。

六、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。

七、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。

八、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依附表九完成分級，並於二年內完成附表十控制措施；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：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。

(三)資通安全弱點管理：應於初次受核定或等級變更後之二年內，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。

第十一條附表七修正規定

附表七 資通安全責任等級D級之各機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	資通安全防護	防毒軟體	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	
認知與訓練	資通安全教育訓練	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。

備註：

一、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。

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資通安全應辦事項。

三、應辦事項辦理期限

(一)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。

(二)資通安全教育訓練：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。

第十一條附表八修正規定

附表八 資通安全責任等級E級之各機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
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資通安全通識教育訓練。

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。

第十一條附表九修正規定

附表九 資通系統防護需求分級原則

防護需求等級 / 構面	高	中	普
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。
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。
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。
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、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。

第十一條附表十修正規定

附表十 資通系統防護基準

系統防護需求分級 控制措施		高	中	普
構面	控制措施			
存取控制	帳號管理	一、應依機關規定之情況及條件，使用資通系統。 二、監控資通系統帳號，如發現帳號違常使用時，回報管理者。 三、等級「中」之所有控制措施。	一、機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。 二、逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。 三、等級「普」之所有控制措施。	一、建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。 二、已逾期之臨時或緊急帳號應刪除或禁用。 三、資通系統閒置帳號應禁用。 四、定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。
	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。		
	遠端存取	一、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。 二、使用者之權限檢查作業應於伺服器端完成。 三、應監控遠端存取機關內部網段或資通系統後臺之連線。 四、應採用加密機制。 五、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。		
事件日誌與可歸責性	記錄事件	一、應定期審查機關所保留資通系統產生之日誌。 二、等級「普」之所有控制措施。		一、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。 二、確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。 三、應記錄資通系統管理者帳號所執行之各項功能。

	日誌紀錄內容	資通系統產生之日誌應包含事件類型、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，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。		
	日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。		
	日誌處理失效之回應	一、機關規定需要即時通報之日誌處理失效事件發生時，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。	資通系統於日誌處理失效時，應採取適當之行動。	
	時戳及校時	一、資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間（UTC）或格林威治標準時間（GMT）。 二、系統內部時鐘應定期與基準時間源進行同步。		
	日誌資訊之保護	一、定期備份日誌至原系統外之其他實體系統。 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。	對日誌之存取管理，僅限於有權限之使用者。
營運持續計畫	資料備份	一、應將備份還原，作為營運持續計畫演練之一部分。 二、應建立資料異地備份機制。 三、等級「中」之所有控制措施。	一、應定期測試備份資料，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、訂定資料可容忍損失之時間要求。 二、執行資料備份。
	系統備援	一、應將備援啟動作為營運持續計畫演練之一部分。 二、等級「中」之所有控制措施。	一、應定期測試原服務中斷時，於最大可容忍中斷時間內，由備援設備或其他方式取代並提供服務。 二、等級「普」之所有控制措施。	訂定資通系統從中斷後至重新恢復服務之最大可容忍中斷時間要求。
識別與鑑別	使用者之識別與鑑別	一、對資通系統之存取採取多因子鑑別技術。 二、等級「中」及「普」之所有控制措施。	資通系統應識別及鑑別使用者，並禁止使用者使用共用帳號。	
	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。		一、使用預設密碼初次登入系統時，應於登入後立即變更。

		三、等級「普」之所有控制措施。		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五次後，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、使用密碼進行驗證時，應強制最低密碼複雜度；依機關密碼效期規定變更密碼。 五、密碼變更時，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，對外部使用者，機關得自行規範辦理。
	鑑別資訊保護	一、資通系統如以密碼進行鑑別時，該密碼應經雜湊或其他適當方式處理後儲存。 二、等級「普」之所有控制措施。		資通系統應遮蔽鑑別過程中之資訊。
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）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、系統應具備發生嚴重錯誤時之通知機制。	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、等級「中」及「普」之所有控制措施。	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，應執行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。 二、識別並關閉不必要服務及埠口。 三、資通系統不使用預設密碼。 四、執行系統源碼備份。
	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	一、開發、測試及正式作業環境應為區隔。 二、等級「普」之所有控制措施。		識別資通系統使用之第三方軟體、服務、函式庫或其他元件。
	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。 三、加密金鑰或憑證應定期更換。 四、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。	無要求。	無要求。
	資料儲存之安全	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。	無要求。	無要求。

系統與資訊完整性	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、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。 三、等級「普」之所有控制措施。	使用者輸入資料合法性檢查應置放於應用系統伺服器端。

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系統防護基準。

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

<table>
<tr><th>修正規定</th><th>現行規定</th><th>說明</th></tr>
<tr>
<td>附表一　資通安全責任等級A級之公務機關應辦事項
<table>
<tr><th>制度面向</th><th>辦理項目</th><th>辦理項目細項</th><th>辦理內容</th></tr>
<tr><td rowspan="7">管理面</td><td colspan="2">資通系統分級及防護基準</td><td>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<u>及其防護基準之</u>妥適性。</td></tr>
<tr><td colspan="2">資訊安全管理系統之導入及通過公正第三方之驗證</td><td>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。</td></tr>
<tr><td colspan="2">資通安全專<u>職</u>人員</td><td>配置四人<u>以上</u>。</td></tr>
<tr><td colspan="2">內部資通安全稽核</td><td>每年辦理二次。</td></tr>
<tr><td colspan="2"><u>營運</u>持續<u>計畫</u>演練</td><td>全部核心資通系統每年辦理一次。</td></tr>
<tr><td colspan="2">資安治理成熟</td><td>每年辦理一次。</td></tr>
</table>
</td>
<td>附表一　資通安全責任等級A級之公務機關應辦事項
<table>
<tr><th>制度面向</th><th>辦理項目</th><th>辦理項目細項</th><th>辦理內容</th></tr>
<tr><td rowspan="5">管理面</td><td colspan="2">資通系統分級及防護基準</td><td><u>初次受核定或等級變更後之一年內，</u>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。</td></tr>
<tr><td colspan="2">資訊安全管理系統之導入及通過公正第三方之驗證</td><td><u>初次受核定或等級變更後之二年內，</u>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，<u>於三年內</u>完成公正第三方驗證，並持續維持其驗證有效性。</td></tr>
<tr><td colspan="2">資通安全專責人員</td><td><u>初次受核定或等級變更後之一年內，</u>配置四人；須以專職人員配置之。</td></tr>
<tr><td colspan="2">內部資通安全稽核</td><td>每年辦理二次。</td></tr>
<tr><td colspan="2">業務持續運作</td><td>全部核心資通系統每年辦理一</td></tr>
</table>
</td>
<td>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，</td>
</tr>
</table>

	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

	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。

			系統與核心資通系統之日誌紀錄及資通設備紀錄。			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		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。		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。		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		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。		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	
	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。

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；

		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。	技術面	全性檢測		次。	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」。
		滲透測試	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年辦理一次。	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。
	資通安全健診	網路架構檢視	每年辦理一次。		資通安全健診	網路架構檢視	每年辦理一次。	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。
		網路惡意活動檢視				網路惡意活動檢視		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。
		使用者端電腦惡意活動檢視				使用者端電腦惡意活動檢視		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。
		伺服器主機惡意活動檢視				伺服器主機惡意活動檢視		十一、調修備註七「資通安全專業證照」之名詞定義，並於備註
		目錄服務系統設定及防火牆連線設定檢視				目錄伺服器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。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		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	

			通系統之日誌紀錄及資通設備紀錄。			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。	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。
	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	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。	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			網路防火牆		
		具有郵件伺服器者，應備電子郵件過濾機制			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			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			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		

		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。 十、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

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。		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。
		滲透測試	全部核心資通系統每二年辦理一次。	技術面	安全性檢測	弱點掃描	全部核心資通系統每年辦理一次。	
	資通安全健診	網路架構檢視	每二年辦理一次。			滲透測試	全部核心資通系統每二年辦理一次。	
		網路惡意活動檢視			資通安全健診	網路架構檢視	每二年辦理一次。	
		使用者端電腦惡意活動檢視				網路惡意活動檢視		
		伺服器主機惡意活動檢視				使用者端電腦惡意活動檢視		
		目錄服務系統設定及防火牆連線設定檢視				伺服器主機惡意活動檢視		
		核心資通系統資料庫安全檢視				目錄伺服器設定及防火牆連線設定檢視		
	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		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	

		通系統之日誌紀錄及資通設備紀錄。		訊服務或應用程式紀錄。	
	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。	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。	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	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。	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	
	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。			

		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。

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，除依本表所定項目、內容及時限執行外，亦得採取經主

			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	
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。

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。

(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。		

第十一條附表四修正對照表

修正規定

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

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		關鍵基礎設施提供者每年辦理一次。

現行規定

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

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。
	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。
技	安	弱點掃描	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一次。	技術面	全性檢測		次。	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
		滲透測試	全部核心資通系統每二年辦理一次。			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。		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				網路惡意活動檢視		
		使用者端電腦惡意活動檢視				使用者端電腦惡意活動檢視		
		伺服器主機惡意活動檢視				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				目錄伺服器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		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	

			通系統之日誌紀錄及資通設備紀錄。			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。	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。
	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	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。		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				網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制				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				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	資通安	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。

		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

訓練	全教育訓練	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，至少二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

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。 十、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。	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。	

(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。		

第十一條附表五修正對照表

修正規定

附表五 資通安全責任等級C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		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，並持續維持導入。
	資通安全專職人員		配置一人以上。
	內部資通安全稽核		每二年辦理一次。
	營運持續計畫演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		滲透測試	全部核心資通系統每二年辦理一次。
	資	網路架構	每二年辦理一次。

現行規定

附表五 資通安全責任等級C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；其後應每年至少檢視一次資通系統分級妥適性；並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。
	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，並持續維持導入。
	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。
	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。

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，並於備註七增列期限之要求。

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，並修正備註二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、「資通安全健診」酌作文字修正，統一用語。

六、「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

	通安全健診	檢視		技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。	採行緩解措施，爰調修該項及備註四相關文字。 七、「認知與訓練」酌作文字修正，以資明確。 八、調修備註五「資通安全專業證照」之名詞定義，並於備註六新增「資通安全職能訓練證書」之名詞定義；備註七律定各應辦事項辦理期限規定。
		網路惡意活動檢視				滲透測試	全部核心資通系統每二年辦理一次。	
		使用者端電腦惡意活動檢視			資通安全健診	網路架構檢視	每二年辦理一次。	
		伺服器主機惡意活動檢視				網路惡意活動檢視		
		目錄服務系統設定及防火牆連線設定檢視				使用者端電腦惡意活動檢視		
	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。			伺服器主機惡意活動檢視		
	資通安全防護	防毒軟體	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。			目錄伺服器設定及防火牆連線設定檢視		
		網路防火牆			資通安全弱點通報機制		一、初次受核定或等級變更後之二年內，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，應於修正施行後二年內，完成資通安全弱點通報機制導入作	
		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	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	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					

	育訓練	以外之資訊人員	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		資通安全專職人員分別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、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。

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。

五、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。

六、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。

七、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依附表九完成分級，並於二年內完成附表十控制措施；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

			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	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。
	資通安全專業證照及職能訓練證書		初次受核定或等級變更後之一年內，至少一名資通安全專職人員，分別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、資通安全專職人員，指應全職執行資通安全業務

時，亦同。 (二)資訊安全管理系統之導入：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。 (三)資通安全弱點管理：應於初次受核定或等級變更後之二年內，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。 (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。	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。	

第十一條附表六修正對照表

修正規定

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

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		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，並持續維持導入。
	資通安全專職人員		配置一人以上。
	內部資通安全稽核		每二年辦理一次。
	營運持續計畫演練		全部核心資通系統每二年辦理一次。
技	安	弱點掃描	全部核心資通系統每二年辦

現行規定

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

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；其後應每年至少檢視一次資通系統分級妥適性；並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。
	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 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，並持續維持導入。
	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。

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，並於備註八增列期限之要求。

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，並於備註二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、「資通安全健診」酌作文字修正，統一用語。

六、「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

術面	全性檢測		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	
	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。
	資通	防毒軟體	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
	安	網路防火牆	
技術面	安全性檢測	弱點掃描	全部核心資通系統每二年辦理一次。
		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	
		目錄伺服器設定及防火牆連線設定檢視	
	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二年內，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，應於修正施行後二年內，完成資通安

等所發現弱點，應適時修補或採行緩解措施，爰調修該項及備註四相關文字。

七、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。

八、調修備註五「資通安全專業證照」之名詞定義，並於備註六新增「資通安全職能訓練證書」之名詞定義；備註八律定各應辦事項辦理期限規定。

	全防護	具有郵件伺服器者，應備電子郵件過濾機制	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、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。

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、資通安全弱點管理，指結合資訊資產管理與弱點

			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	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		初次受核定或等級變更後之一年內，至少一名資通安全專責人員持有證照一張以上，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，

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，指經主管機關公告之資通安全專業證照。 六、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。 七、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。 八、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依附表九完成分級，並於二年內完成附表十控制措施；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：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。 (三)資通安全弱點管理：應於初次受核定或等級變更後之二年內，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。	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、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。 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。 五、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。	

第十一條附表七修正對照表

修正規定

附表七 資通安全責任等級D級之各機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	資通安全防護	防毒軟體 網路防火牆	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。
認知與訓練	資通安全教育訓練	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。

備註：

一、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。

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資通安全應辦事項。

現行規定

附表七 資通安全責任等級D級之各機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
技術面	資通安全防護	防毒軟體 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。
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資通安全通識教育訓練。

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。

說明

一、資通安全教育訓練新增資通安全專職人員以外之資訊人員，並於備註一新增資通安全專職人員以外之資訊人員之定義，其後點次遞移。

二、配合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，並於備註三增列期限之要求。

三、應辦事項辦理期限 (一)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。 (二)資通安全教育訓練：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。		

第十一條附表八修正對照表

<table>
<tr><th>修正規定</th><th>現行規定</th><th>說明</th></tr>
<tr>
<td>附表八資通安全責任等級E級之各機關應辦事項
<table>
<tr><th>制度面向</th><th>辦理項目</th><th>辦理項目細項</th><th>辦理內容</th></tr>
<tr><td>認知與訓練</td><td>資通安全教育訓練</td><td>一般使用者及主管</td><td>每人每年接受三小時以上之資通安全通識教育訓練。</td></tr>
</table>
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。</td>
<td>附表八資通安全責任等級E級之各機關應辦事項
<table>
<tr><th>制度面向</th><th>辦理項目</th><th>辦理項目細項</th><th>辦理內容</th></tr>
<tr><td>認知與訓練</td><td>資通安全教育訓練</td><td>一般使用者及主管</td><td>每人每年接受三小時以上之資通安全通識教育訓練。</td></tr>
</table>
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。</td>
<td>本附表未修正。</td>
</tr>
</table>

第十一條附表九修正對照表

修正規定	現行規定	說明
附表九 防護需求等級 構面 高 中 普 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。 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 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 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	附表九 防護需求等級 構面 高 中 普 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。 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 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 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	本附表未修正。

	嚴重或災難性之影響。	之影響。	之影響。		嚴重或災難性之影響。	之影響。	之影響。	
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。	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。	
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	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	其他資通系統設置或運作於法令有相關規範之情形。	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	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	其他資通系統設置或運作於法令有相關規範之情形。	

	性，並使機關所屬人員負刑事責任。	性，並使機關或其所屬人員受行政罰、懲戒或懲處。	

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、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。

	性，並使機關所屬人員負刑事責任。	性，並使機關或其所屬人員受行政罰、懲戒或懲處。	

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、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。

第十一條附表十修正對照表

修正規定

附表十 資通系統防護基準

控制措施 \ 系統防護需求分級		高	中	普
構面	控制措施			
存取控制	帳號管理	一、應依機關規定之情況及條件，使用資通系統。 二、監控資通系統帳號，如發現帳號違常使用時，回報管理者。 三、等級「中」之所有控制措施。	一、機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。 二、逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。 三、等級「普」之	一、建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。 二、已逾期之臨時或緊急帳號應刪除或禁用。 三、資通系統閒置帳號應禁用。 四、定期審核

現行規定

附表十 資通系統防護基準

控制措施 \ 系統防護需求分級		高	中	普
構面	控制措施			
存取控制	帳號管理	一、機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。 二、逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。 三、應依機關規定之情	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申請、建立、修改、啟用、停用及刪除。 四、等級「普」之	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。

說明

一、資通系統皆應建立帳號管控措施，爰將臨時帳號、閒置帳號，以及定期審核帳號等移列普級規範，另將系統閒置時間或可使用期限等移列中級規範。

二、應依使用者所需權限限制系統存取範圍，並建立相關管控措施，爰將最小權限移列普級規範。

三、遠端存取來源應由機關預先定義，以降低資安風險，爰移列普級規

			所有控制措施。	資通系統帳號之申請、建立、修改、啟用、停用及刪除。				範。 四、考量系統內部時鐘產生日誌所需時戳，應定期同步以確保其正確性，時戳及校時爰移列普級規範。 五、營運持續計畫「系統備份」修正為「資料備份」，另將源碼備份移至系統發展生命週期部署與維運階段執行，並酌作文字修正；為強化各機關系統可用性，備援機制納入營運持續計畫演練之一部分，並將最大可容忍中斷時間納入普級規
	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。				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。	
	遠端存取	一、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。 二、使用者之權限檢查作業應於伺服器端完成。 三、應監控遠端存取機關內部網段或資通系統後臺之連線。 四、應採用加密機制。 五、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。				一、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。 二、等級「普」之所有控制措施。	一、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。	
事件日誌與可歸責性	記錄事件	一、應定期審查機關所保留資通系統產生之日誌。 二、等級「普」之所有控制措施。		一、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。 二、確保資通系統有記錄特定事		一、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。 二、確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。 三、應記錄資通系統管理者帳號所執行之各項功能。 四、監控資通系統帳號，如發現帳號違常使用時回報管理者。 五、等級「中」之所有控制措施。	所有控制措施。	

			件之功能，並決定應記錄之特定資通系統事件。 三、應記錄資通系統管理者帳號所執行之各項功能。			二、使用者之權限檢查作業應於伺服器端完成。 三、應監控遠端存取機關內部網段或資通系統後臺之連線。 四、應採用加密機制。	範。 六、「內部使用者之識別與鑑別」及「非內部使用者之識別與鑑別」合併為「使用者之識別與鑑別」，並將「多重認證」技術更名為「多因子鑑別」技術，及酌作文字修正。
	日誌紀錄內容	資通系統產生之日誌應包含事件類型、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，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。		事件日誌與可歸責性	記錄事件	一、應定期審查機關所保留資通系統產生之日誌。 二、等級「普」之所有控制措施。	一、訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。 二、確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事件。	七、內部使用者應依機關定義密碼效期規定更改密碼或展延密碼，而外部使用者可依機關規範自行辦理，並酌作文字修正。
	日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。						八、「鑑別資訊回饋」及「加密模組鑑別」合併
	日誌處理失效之回應	一、機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特	資通系統於日誌處理失效時，應採取適當之行動。					

		定人員提出警告。 二、等級「中」及「普」之所有控制措施。		
	時戳及校時	一、資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間（UTC）或格林威治標準時間（GMT）。 二、系統內部時鐘應定期與基準時間源進行同步。		
	日誌資訊之保護	一、定期備份日誌至原系統外之其他實體系統。 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。	對日誌之存取管理，僅限於有權限之使用者。
營運持續計畫	資料備份	一、應將備份還原，作為營運持續計畫演練之一部分。 二、應建立資料異地備份機制。	一、應定期測試備份資料，以驗證備份媒體之可靠性及資訊之完整性。	一、訂定資料可容忍損失之時間要求。 二、執行資料備份。

			三、應記錄資通系統管理者帳號所執行之各項功能。	
	日誌紀錄內容	資通系統產生之日誌應包含事件類型、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，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。		
	日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。		
	日誌處理失效之回應	一、機關規定需要即時通報之日誌處理失效事件發生時，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。	資通系統於日誌處理失效時，應採取適當之行動。	

為「鑑別資訊保護」，並酌作文字修正。

九、系統發展生命週期部署與維運階段納入源碼備份，並酌作文字修正。

十、考量多數資通系統普遍使用函式庫與程式等第三方元件，並配合本法施行細則第七條規定，涉及利用非受託者自行開發之外部元件應予以標示，爰納入普級規範。

十一、傳輸之機密性與完整性已規範須使用公開、國際機構驗證且未遭破

		三、等級「中」之所有控制措施。	二、等級「普」之所有控制措施。			時戳及校時	一、系統內部時鐘應定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日誌所需時戳，並可以對應到世界協調時間（UTC）或格林威治標準時間（GMT）。	解之演算法，且配合各機關實務執行採行不同加密機制，爰刪除演算法最大長度金鑰規定。 十二、考量使用者輸入資料合法性之檢查，現為系統應具備之功能，爰移列至普級規範。
	系統備援	一、應將備援啟動作為營運持續計畫演練之一部分。 二、等級「中」之所有控制措施。	一、應定期測試原服務中斷時，於最大可容忍中斷時間內，由備援設備或其他方式取代並提供服務。 二、等級「普」之所有控制措施。	訂定資通系統從中斷後至重新恢復服務之最大可容忍中斷時間要求。		日誌資訊之保護	一、定期備份日誌至原系統外之其他實體系統。 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。	對日誌之存取管理，僅限於有權限之使用者。	
識別與鑑別	使用者之識別與鑑別	一、對資通系統之存取採取多因子鑑別技術。 二、等級「中」及「普」之所有控制措施。	資通系統應識別及鑑別使用者，並禁止使用者使用共用帳號。			營運持續計畫	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地點之獨立設施或防火櫃中，儲存	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。	

	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、使用預設密碼初次登入系統時，應於登入後立即變更。 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五次後，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、使用密碼進行驗證時，應強制最低密碼複雜			重要資通系統軟體與其他安全相關資訊之備份。 三、等級「中」之所有控制措施。		
					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，由備援設備或其他方式取代並提供服務。		無要求。
				識別與鑑別	內部使用者之識別與鑑別	一、對資通系統之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。	
					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。		一、使用預設密碼登入系統時，應於登入

			度；依機關密碼效期規定變更密碼。 五、密碼變更時，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，對外部使用者，機關得自行規範辦理。		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。	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五次後，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、使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之	
	鑑別資訊保護	一、資通系統如以密碼進行鑑別時，該密碼應經雜湊或其他適當方式處理後儲存。 二、等級「普」之所有控制措施。	資通系統應遮蔽鑑別過程中之資訊。				
系統與服務	系統發展生命週期需求	針對系統安全需求（含機密性、可用性、完整性）進行確認。					

獲得	階段							
	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、系統應具備發生嚴重錯誤時之通知機制。 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。				效期限制。 五、密碼變更時，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。	
	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。					
					鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。		
					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	系統	針對系統安全需求（含機密性、可用性、完整		

	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，應執行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。 二、識別並關閉不必要服務及埠口。 三、資通系統不使用預設密碼。 四、執行系統源碼備份。	統與服務獲得	發展生命週期需求階段	性）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、系統應具備發生嚴重錯誤時之通知機制。 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	一、執行「滲透測試」安全檢測。	執行「弱點掃描」安全檢測。		
	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	一、開發、測試及正式作業環境應為區隔。 二、等級「普」之所有控制措施。	識別資通系統使用之第三方軟體、服務、函式庫或其他元件。						
	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。 三、加密金鑰或憑證應定期更換。 四、伺服器端之金鑰保管應訂定管理規範及實施應有之安全	無要求。	無要求。

	階段	二、等級「中」及「普」之所有控制措施。		
	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，應執行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	傳輸之機	一、資通系統應採用加	無要求。	無要求。

		防護措施。		
	資料儲存安全	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。	無要求。	無要求。
系統與資訊完整性	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。

與通訊保護	密性與完整性	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。 三、支援演算法最大長度金鑰。 四、加密金鑰或憑證應定期更換。 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	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。	無要求。	無要求。	
	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、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。 三、等級「普」之所有控制措施。	使用者輸入資料合法性檢查應置放於應用系統伺服器端。	系統與資訊完整性	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。

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系統防護基準。

		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：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。					