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。