資通安全責任等級分級辦法草案總說明

「資通安全管理法」（以下簡稱本法）業於一百零七年六月六日制定公布。依本法第七條第一項規定，主管機關應衡酌公務機關及特定非公務機關業務之重要性與機敏性、機關層級、保有或處理之資訊種類、數量、性質、資通系統之規模及性質等條件，訂定資通安全責任等級之分級。為明確規範資通安全責任等級之分級基準、等級變更申請、義務內容、專責人員之設置及其他相關事項，以利各受規範對象得妥適辦理資通安全維護事務，以強化資通安全管理能量，爰擬具「資通安全責任等級分級辦法」（以下簡稱本辦法）草案，其要點如下：

一、本辦法之授權依據。（草案第一條）

二、資通安全責任等級之級別。（草案第二條）

三、資通安全責任等級之提交、核定及變更程序。（草案第三條）

四、資通安全責任等級分級原則及例外考量因素。（草案第四條至第十條）

五、各機關應依附表規定辦理其資通安全責任等級應辦事項。（草案第十一條）

六、本辦法之施行日期。（草案第十二條）

資通安全責任等級分級辦法草案

條文	說明
第一條　本辦法依資通安全管理法（以下簡稱本法）第七條第一項規定訂定之。	明定本辦法訂定之依據。
第二條　公務機關及特定非公務機關（以下簡稱各機關）之資通安全責任等級，由高至低，分為A級、B級、C級、D級及E級。	一、明定公務機關及特定非公務機關（以下簡稱各機關）之資通安全責任等級，由高至低，分為A級至E級。 二、有關資通安全責任等級之核定方式、區分原則及認定等級之其他考量因素，依第三條至第十條為之。
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（構）、省諮議會應每二年提交自身、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、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，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。	一、第一項明定主管機關應每二年核定自身之資通安全責任等級。 二、基於尊重總統府、國家安全會議及行政院以外其他四院之權限，該等公務機關及其所屬、監督或所管之各機關（特定非公務機關部分，例如司法院所管之財團法人法律扶助基金會）之資通安全責任等級，宜由其自行認定，並於核定後送主管機關備查即可；至於行政院直屬機關（構）（包含省政府）、省諮議會與各地方自治團體之行政及立法機關，主管機關應督導或協助其辦理資通安全維護業務，該等機關及其所屬、監督或所管之各機關之資通安全責任等級，宜由主管機關核定，爰分別於第二項至第五項明定各機關資通安全責任等級之認定程序。 三、各機關之資通安全責任等級如因應組織或業務調整，致須配合變更者，應即依第一項至第五項規定辦理其等級變更事宜；有新設機關時，亦應立即辦理該機關資通安全責任等級之認定，爰為第六項規定。 四、考量各機關可能有特定內部單位業務性質特殊，其辦理資通安全維護業務相較其他單位，須為更嚴格要求之情形，此時宜單獨將該單位之資通安全責任等級分級為不同之處理，爰為第七項規定。

第四條　各機關有下列情形之一，或屬下列機關者，其資通安全責任等級為A級： 一、業務涉及國家機密。 二、業務涉及外交、國防或國土安全事項。 三、業務涉及全國性民眾服務或跨公務機關共用性資通系統之維運。 四、業務涉及全國性民眾或公務員個人資料檔案之持有。 五、公務機關，且業務涉及全國性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項。 六、關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將產生災難性或非常嚴重之影響。 七、公立醫學中心。	一、明定各機關資通安全責任等級應列為A級之情形。於該等情形，因其機關業務所涉重要性或機敏性較高，具有較高之資通安全風險，爰應予以較高程度之資通安全維護責任。 二、第三款所稱全國性，指含括全國之地域範圍；所稱跨公務機關共用性資通系統，指單一公務機關主責設置、維護或開發之伺服器、網路通訊服務之機房設施或其他資通系統，其餘公務機關僅為該資通系統之使用者之情形。 三、第四款所稱全國性民眾或公務員個人資料檔案，指含括全國地域範圍內之絕大部分民眾或公務員之個人資料檔案。
第五條　各機關有下列情形之一，或屬下列機關者，其資通安全責任等級為B級： 一、業務涉及公務機關捐助或研發之敏感科學技術資訊之安全維護及管理。 二、業務涉及區域性、地區性民眾服務或跨公務機關共用性資通系統之維運。 三、業務涉及區域性或地區性民眾個人資料檔案之持有。 四、公務機關，且業務涉及區域性或地區性之能源、水資源、通訊傳播、交通、銀行與金融、緊急救援事項。 五、關鍵基礎設施提供者，且業務經中央目的事業主管機關考量其提供或維運關鍵基礎設施服務之用戶數、市場占有率、區域、可替代性，認其資通系統失效或受影響，對社會公共利益、民心士氣或民眾生命、身體、財產安全將	一、資通安全責任等級應列為B級之情形。於該等情形，其機關業務所涉重要性或機敏性雖較第四條所定情形為低，惟亦具有相當之資通安全風險，爰應予以相當之資通安全維護責任。 二、第二款所稱區域性，指跨直轄市、縣（市）之地域範圍；所稱地區性，指單一直轄市或縣（市）之地域範圍。所稱跨公務機關共用性資通系統，如第四條說明二。 三、第三款所稱區域性或地區性民眾個人資料檔案，指含括跨直轄市、縣（市）或單一直轄市、縣（市）地域範圍內之絕大部分民眾之個人資料檔案。

產生嚴重影響。 六、公立區域醫院或地區醫院。	
第六條　各機關維運自行或委外開發之資通系統者，其資通安全責任等級為C級。	鑒於各機關之業務涉及維運自行或委外開發之資通系統，其業務所涉重要性或機敏性較前二條所列情形為低，其資通安全責任等級應列為C級，爰為本條規定。
第七條　各機關未維運自行或委外開發之資通系統，惟仍自行辦理資訊業務者，其資通安全責任等級為D級。	考量各機關如屬自行辦理資訊業務，未維運自行或委外開發之資通系統，其資通安全風險較低，其資通安全責任等級應列為D級，爰為本條規定。
第八條　各機關有下列情形之一，或屬下列機關者，其資通安全責任等級為E級： 一、無資通系統且未提供資通服務。 二、公務機關之全部資訊業務由其上級或監督機兼辦或代管。 三、特定非公務機關之全部資訊業務由其中央目的事業主管機關、中央目的事業主管機關所屬公務機關，或中央目的事業主管機關所管特定非公務機關兼辦或代管。	考量各機關如無資通系統且未提供資通服務，或全部資訊業務由其上級或監督機關、中央目的事業主管機關、中央目的事業主管機關所屬公務機關、中央目的事業主管機關所管特定非公務機兼辦或代管，其資通安全風險較低，其資通安全責任等級原則應列為E級，爰為本條規定。
第九條　各機關依第四條至第八條之規定，符合二個以上之資通安全責任等級者，列為其符合之最高等級。	為避免各機關依第四條至第八條規定認定資通安全責任等級時，可能有符合二個以上之資通安全責任等級之情形，於辦理其等級之提交或核定將發生疑義，爰明定有上開情形者，應列為其符合之最高等級。
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	有關各機關資通安全責任等級之認定，除第四條至第八條規定外，因業務機敏性、個人資料檔案之數量等不同因素，仍可能有其他應考量事項，而有調整分級之必要。為利第三條第一項至第五項之公務機關於提交或核定資通安全責任等級時，得有調整之彈性，爰為本條規定。各機關資通安全責任等級之認定，原則應依第四條至第九條規定辦理，例外則得視實務狀況，依本條規定予以適當調整其等級。

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。 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。 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，如因技術限制、資通系統之設計、結構或性質等因素而顯有困難，得經第三條第二項至第四項所定其等級提交機關或第五項所定其等級核定機關同意並報請主管機關備查後，免執行該事項及控制措施之全部或一部。 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。	一、 考量不同資通安全責任等級之機關，其業務所涉範圍與機敏性等有所不同，資通安全風險程度亦有所差異，爰於第一項規定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，並於第二項明定各機關自行或委外開發之資通系統應依附表九及附表十辦理資通系統分級及控制措施。 二、 考量部分公務機關或特定非公務機關辦理附表一至附表八所定事項及附表十所定控制措施，可能因技術限制或、資通系統之設計、結構或性質上等因素而顯有困難，為利實務運作之彈性，並能符合資通安全維護之要求，爰於第三項明定有該等情形者，經第三條第二項至第四項之等級提交機關或第五項之等級核定機關同意並報請主管機關備查後，得免執行該事項及控制措施之全部或一部。 三、 資通安全責任等級為A級或B級者之公務機關，宜強化對該等機關資通安全維護情形之管考，爰於第四項明定其應依主管機關指定之方式，提報第一項及第二項所定事項之辦理情形。考量特定非公務機關之資通安全維護情形之管考，宜由特定非公務機關之中央目的事業主管機關執行，爰為第五項之規定。
第十二條 本辦法之施行日期，由主管機關定之。	明定本辦法之施行日期，由主管機關定之。

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，及附表十之控制措施；其後並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 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並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。
	業務持續運作演練		全部核心資通系統每年辦理一次。
	資安治理成熟度評估		每年辦理一次。
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理二次。
		系統滲透測試	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。
	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
		網路防火牆	

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

備註：

1. 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。
2. 資通安全專職人員係指其主要業務為資通安全相關之業務者。
3. 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。
4. 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。

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，及附表十之控制措施，或關鍵基礎設施領域中央目的事業主管機關訂定之防護基準；其後並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 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並於三年內完成公正第三方驗；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。
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理二次。
		系統滲透測試	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。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	

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

備註：

1. 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。
2. 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。
3. 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。
4. 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。

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；其後並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 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並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。
	資安治理成熟度評估		每年辦理一次。
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理一次。
		系統滲透測試	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。
	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
		網路防火牆	

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

備註：

1. 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。
2. 資通安全專職人員係指其主要業務為資通安全相關之業務者。
3. 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。
4. 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。

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，或關鍵基礎設施領域中央目的事業主管機關訂定之防護基準；其後並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資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並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。
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理一次。
		系統滲透測試	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	
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	

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

備註：

1. 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。
2. 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。
3. 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。
4. 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。

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；其後並應每年至少檢視一次資通系統分級妥適性；系統等級為「高」者，應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準；並持續維持導入。
	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。
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每二年辦理一次。
		系統滲透測試	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	

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

備註：

1. 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。
2. 資通安全專職人員係指其主要業務為資通安全相關之業務者。
3. 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。
4. 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。

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；其後並應每年至少檢視一次資通系統分級妥適性；系統等級為「高」者，應於初次受核定或等級變更後之二年內完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入CNS 27001資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準；並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每二年辦理一次。
		系統滲透測試	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	
認知與訓練	資通安全教育訓練	資通安全及資訊人員	每年至少一名人員接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。

		一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。
	資通安全專業證照		初次受核定或等級變更後之一年內，資通安全專責人員總計應持有一張以上，並持續維持證照之有效性。

備註：

1. 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。
2. 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。
3. 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。
4. 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。

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	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	
認知與訓練	資通安全教育訓練	一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。

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。

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一般資通安全教育訓練。

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。

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。

附表十 資通系統防護基準

系統防護需求分級 / 控制措施 構面	措施內容	高	中	普
存取控制	帳號管理	一、逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出。 二、應依機關規定之情況及條件，使用資通系統。 三、監控資通系統帳號，如發現帳號違常使用時回報管理者。 四、等級「中」之所有控制措施。	一、已逾期之臨時或緊急帳號應刪除或禁用。 二、資通系統閒置帳號應禁用。 三、定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。 四、等級「普」之所有控制措施。	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。
	最小權限	採最小權限原則，僅允許使用者（或代表使用者行為之程序）依機關任務及業務功能，完成指派任務所需之授權存取。		無要求。
	遠端存取	一、應監控資通系統遠端連線。 二、資通系統應採用加密機制。 三、資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點。 四、等級「普」之所有控制措施。		對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化，並採用伺服端之集中過濾機制檢查使用者之授權。
稽核與可歸責性	稽核事件	一、應定期審查稽核事件。 二、等級「普」之所有控制措施。		一、依規定時間週期及紀錄留存政策，保留稽核紀錄。 二、確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件。 三、應稽核資通系統管理者帳號所執行之各項功能。
	稽核紀錄內容	一、資通系統產生之稽核紀錄，應依需求納入其他相關資訊。 二、等級「普」之所有控制措施。		資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一

系統防護需求分級 / 控制措施		高	中	普
構面	措施內容			
				日誌紀錄機制，確保輸出格式的一致性。
	稽核儲存容量	依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。		
	稽核處理失效之回應	一、機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。 二、等級「中」及「普」之所有控制措施。	資通系統於稽核處理失效時，應採取適當之行動。	
	時戳及校時	一、系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。 二、等級「普」之所有控制措施。		資通系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對映到世界協調時間(UTC)或格林威治標準時間(GMT)。
	稽核資訊之保護	一、定期備份稽核紀錄至與原稽核系統不同之實體系統。 二、等級「中」之所有控制措施。	一、應運用雜湊或其他適當方式之完整性確保機制。 二、等級「普」之所有控制措施。	對稽核紀錄之存取管理，僅限於有權限之使用者。
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處之獨立設施或防火櫃中，儲存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。	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。
	系統備援	一、訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。 二、原服務中斷時，於可容忍時間內，由備援設備取代提供服務。		無要求。

識別與鑑別	內部使用者之識別與鑑別	一、對帳號之網路或本機存取採取多重認證技術。 二、等級「中」及「普」之所有控制措施。	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。
	身分驗證管理	一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。 三、等級「普」之所有控制措施。	一、使用預設密碼登入系統時，應於登入後要求立即變更。 二、身分驗證相關資訊不以明文傳輸。 三、具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 3 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。 四、基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限制。 五、使用者更換密碼時，至少不可以與前三次使用過之密碼相同。 六、上述第四點至第五點對非內部使用者，可依機關自行規範辦理。
	鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。	
	加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	無要求。
	非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。	
系統與服務獲得	系統發展生命週期需求階段	針對系統安全需求（含機密性、可用性、完整性），以檢核表方式進行確認。	
	系統發展生命	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。	無要求。

	週期設計階段	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。		
	系統發展生命週期開發階段	一、執行「源碼掃描」安全檢測。 二、具備系統嚴重錯誤之通知機制。 三、等級「中」及「普」之所有控制措施。	一、應針對安全需求實作必要控制措施。 二、應注意避免軟體常見漏洞及實作必要控制措施。 三、發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息。	
	系統發展生命週期測試階段	一、執行「滲透測試」安全檢測。 二、等級「中」及「普」之所有控制措施。	執行「弱點掃描」安全檢測。	
	系統發展生命週期部署與維運階段	一、於系統發展生命週期之維運階段，須注意版本控制與變更管理。 二、等級「普」之所有控制措施。		一、於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。 二、資通系統相關軟體，不使用預設密碼。
	系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。		
	獲得程序	開發、測試及正式作業環境應為區隔。		無要求。
	系統文件	應儲存與管理系統發展生命週期之相關文件。		
系統與通訊保護	傳輸之機密性與完整性	一、資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。 二、使用公開、國際機構驗證且未遭破解的演算法。 三、使用演算法支援的最大長度金鑰。 四、加密金鑰或憑證週期性更換。	無要求。	無要求。
	資料儲存之安全	靜置資訊及相關具保護需求之機密資訊應加密儲存。	無要求。	無要求。

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、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：

1. 靜置資訊指資訊位於資通系統特定元件，如儲存設備上之狀態，或與系統相關需要保護之資訊，例如設定防火牆、閘道器、入侵偵測、防禦系統、過濾式路由器及鑑別符內容等資訊。
2. 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。