全面協助
企業符規

資通安全管理法

9

大項次達成

UPAS NOC

新世代資安防護解決方案

安全穩定便捷

包含附表十、資通系統防護基準

輕鬆完成軟硬體盤點！

管理面

辦理項目	辦理細項	A級公務與非公務機關	B級公務與非公務機關	C級公務與非公務機關	UPAS NOC
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，於三年內完成公正第三方驗證，並持續維持其驗證有效性。	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。	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。	UPAS符合多項ISO 27001標準降低建置所需成本，請見ISO 27001法規對照表格

技術面

辦理項目	辦理細項	A級公務與非公務機關	B級公務與非公務機關	C級公務與非公務機關	UPAS NOC
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。**非公務機關無要求。**	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。**非公務機關無要求。**	無要求。	UPAS的GPO管理設定可用來幫助管理者瞭解在網域中的設備GPO、GCB套用狀況，查找未合規定套用GCB、GPO之端點設備
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。	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。	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。	UPAS提供防毒軟體、病毒碼更新與安裝檢查，並可介接多項資產軟體與WSUS資料庫，強迫不合規電腦進行更新
資通安全防護	進階持續性威脅攻擊防禦措施	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。	無要求。	無要求。	UPAS提供防毒軟體、病毒碼更新與安裝檢查，並可介接多項資產軟體與WSUS資料庫，強迫不合規電腦進行更新

資通法附表十、資通系統防護基準

構面	措施內容	系統防護需求分級：高	系統防護需求分級：中	系統防護需求分級：普通	UPAS NOC
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。	提供自帶設備驗證機制、訪客帳號申請機制，並可設定使用期限，在到期時自動卸離
稽核與可歸責性	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。	一、資通系統產生之稽核紀錄，應依需求納入其他相關資訊。 二、等級「普」之所有控制措施。	資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌紀錄機制，確保輸出格式之一致性。	自動產生ARP、SNMP、AD軌跡資料並加密保護5年以上。
識別與鑑別	內部使用者之識別與鑑別	–	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。	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。	禁止使用本機登入，強迫使用AD帳號登入電腦設備，以此確定使用者資訊，並限制所能使用人員身分
識別與鑑別	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)。	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)。	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)。	提供准入控制、私接設備管理 提供身分驗證機制、AD管理
系統與資訊完整性	資通系統監控	–	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。	設備違規立即告警管理員
系統與資訊完整性	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。	可檢查應裝軟體是否正確安裝，或是是否有安裝盜版、禁用軟體