111年維護計畫查核表演練說明與資產盤點及風險評鑑

大綱

- 111年維護計畫查核表說明
- 資產盤點及風險評鑑
- 結論

資通安全責任等級分級辦法 (110/08/23修正)

- 第 6 條
  1. 各機關維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 C 級。
  2. 前項所定自行或委外設置之資通系統，**指具權限區分及管理功能之資通系統**。
- 第 7 條
  1. 各機關自行辦理資通業務，未維運自行或委外設置、開發之資通系統者，其資通安全責任等級為 D 級。

資通安全責任等級分級辦法修正草案內容

修正條文	現行條文
第六條 各機關維運自行或委外開發之資通系統、**或維運具權限區分及管理功能之非自行或委外開發系統**者，其資通安全責任等級為C。	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。
說明： 機關基礎資通環境或處理，使用市面既有資通系統，如**電子郵件、目錄服務系統，資料庫、帳務處理**等，仍應就其資安風險進行管控，為明確其資安責任等級要求，爰調修第六條 。→原資安責任等級D級之**「具有郵件伺服器者，應備電子郵件過濾機制」**條款刪除。	

大陸廠牌資通訊產品盤點

受文者：教育部

發文日期：中華民國110年9月23日
發文字號：院臺護長字第1100186822號
速別：普通件
密等及解密條件或保密期限：
附件：

主旨：有關大陸廠牌資通訊產品盤點結果中，屬「在臺陸資廠商」之產品採購，請依說明事項辦理，請查照並轉知所屬公務機關。

說明：

一、為避免公務及機敏資料遭不當竊取，導致機關機敏公務資訊外洩或造成國家資通安全危害風險，請各機關應於本(110)年12月31日前完成汰換大陸廠牌資通訊產品。

二、有關本院評估結果屬「在臺陸資廠商」者，如聯想集團(Lenovo)，雖非屬於本次盤點及汰換範圍，惟機關辦理採購時，如涉及經濟部投資審議委員會公告之「具敏感性或國安(含資安)疑慮之業務範疇」，應確實於招標文件中載明不允許在臺陸資廠商(陸資資訊服務業者)參與。

WHY資產盤點與風險評估！？

❑ 資通安全管理法施行細則第6條規定

本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項：

一、核心業務及其重要性。

二、資通安全政策及目標。

三、資通安全推動組織。

四、專責人力及經費之配置。

五、公務機關資通安全長之配置。

六、資訊及資通系統之盤點，並標示核心資通系統及相關資產。

七、資通安全風險評估。

八、資通安全防護及控制措施。

九、資通安全事件通報、應變及演練相關機制。

十、資通安全情資之評估及因應機制。

十一、資通系統或服務委外辦理之管理措施。

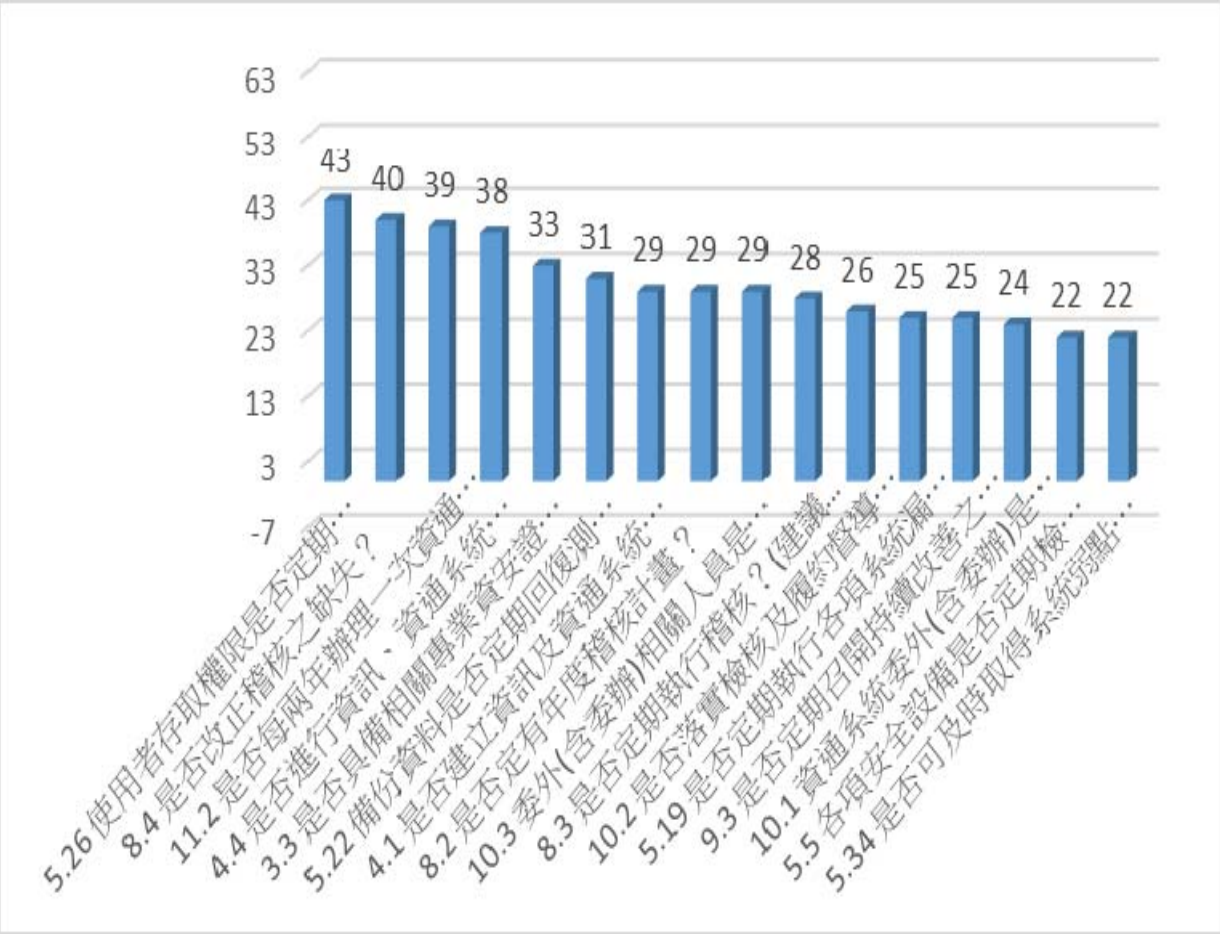
十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制。

十三、資通安全維護計畫與實施情形之持續精進及績效管理機制。

111年維護計畫查核表說明

110年63校維護計畫實地訪視結果

- 前三名不符合問題統計
  1. 5.26使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？
  2. 8.4 是否改正稽核之缺失？
  3. 11.2 是否每兩年辦理一次資通安全健診？ (本項C級機關列入評分，D級機關不列入評分)



資通安全政策之推動及目標訂定

查核內容	準備資料或客觀證據
1.1 是否定義符合組織需要之資通安全政策及目標？	資通安全政策或資通安全維護計畫
1.2 組織是否訂定資通安全政策及目標？	資通安全政策或資通安全維護計畫
1.3 組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	審核紀錄及公告紀錄
1.4 組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	管審會紀錄
1.5 是否隨時公告資通安全相關訊息？	公告紀錄

錯誤的範例

維護本校資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由本校全體同仁共同努力來達成下列定性及定量目標：

4.1 定性目標：

4.1.1 確保相關資通安全措施或規範符合政策與現行法令的要求每年至少進行一次內部稽核。

4.1.2 每年至少進行一次業務持續計畫之測試或檢核。

4.2 定量目標：

4.2.1 確保資訊資產受適當之保護，每年未經授權或因作業疏失對資產所造成的損害降至最低。

4.2.2 確保所有資通安全事件或可疑之安全弱點，每年不依適當通報程序反應，並予以適當的調查及處理事件降至最低。

4.2.3 符合政府資通安全相關政策、規訂及相關法令要求。

4.2.4 定期實施資通安全教育訓練。

設置資通安全推動組織&配置適當之資通安全專業人員及適當之資源

查核內容	準備資料或客觀證據
2.1 是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	資通安全組織成員表
2.2 是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	資通安全組織成員表
2.3 是否訂定組織之資通安全責任分工？	資通安全組織成員表

查核內容	準備資料或客觀證據
3.1 是否訂定人員之安全評估措施？	人員安全守則
3.2 是否符合組織之需求配置專業資安人力(資安專責人員)？	資通安全維護計畫中敘明配置資通安全專責人員 (C級機關應辦事項：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。)
3.3 是否具備相關專業資安證照或認證？(本項C級機關列入評分，D級機關不列入評分)	專業安證照及職能訓練
3.4 是否配置適當之資源？	資安或資訊相關經費情形(全年度與前年度經費之占比)

人員資通安全守則(範例)

1 目的：為落實本校資訊通訊安全作業，維護資訊及處理設備之機密性、完整性及可用性，特訂定此守則。

2 範圍：本守則適用於正職人員與約聘（僱）人員。

3 作業守則

3.1 電腦應設定密碼確實保密。

3.2 電腦應使用螢幕保護程式，設定螢幕保護密碼，並將螢幕保護啟動時間設定為 15 分鐘以內。

3.3 電腦之作業系統漏洞應即時更新修補。

3.4 電腦應安裝防毒軟體並即時更新病毒碼。

3.5 應定期將重要資料備份存放。

3.6 除管理需求及經授權外，禁止使用密碼破解、網路監聽工具軟體，並不得突破他人帳號，中斷系統服務。

3.7 不得在任何公開的新聞群組、論壇、或公佈欄中透露任何有關本校資訊細節。

3.8 在丟棄任何曾經儲存本校資訊之電子媒介前，應將電子媒介中的資訊刪除，並徹底消磁或銷毀至無法解讀之程度。

3.9 敏感等級（含）以上資訊之紙本文件若不再使用時，應以碎紙機銷毀該份紙本文件，並刪除電子檔。

3.10 重要機密文件或合約，應妥善保存；若為電子檔案應考慮設定保護密碼。

3.11 開啟來路不明之電子郵件及其附件時應謹慎小心，以防電腦中毒。

3.12 當有跡象顯示系統可能中毒時，應儘速通知相關人員。

3.13 禁止濫用系統及網路資源，複製與下載非法軟體。

3.14 應遵守「個人資料保護法」規範，保護個人資料使用之合法性及機密性。

4 密碼使用原則

4.1 應保護通行密碼，維持通行密碼的機密性；資通系統之系統管理者應至少每 3 個月更換密碼一次，一般資通系統之使用者應至少 6 個月更換密碼，並禁止重複使用相同的密碼。

4.2 應避免將通行密碼記錄在書面上，或張貼於個人電腦、螢幕或其它容易洩漏秘密之場所。

4.3 當有跡象顯示系統及通行密碼可能遭破解時，應立即更改密碼。

4.4 通行密碼的長度最少應有 8 位長度，且應符合密碼設置原則。

4.5 密碼設置原則，應儘量避免使用易猜測或公開資訊為設定：

4.5.1 個人姓名、出生年月日、身分證字號。

4.5.2 機關或單位名稱識別代碼或是其他相關事項。

4.5.3 使用者識別碼、使用者姓名、群體使用者之識別碼或是其他系統識別碼。

4.5.4 電腦主機名稱、作業系統名稱、或電腦上使用者的名稱。

4.5.5 電話號碼。

4.5.6 英文或是其他外文字典的字彙。

4.5.7 專有名詞。

4.5.8 空白。

5 電腦軟體版權之使用與管理

5.1 禁止使用未經授權之電腦軟體，遵守智慧財產權相關規定。

5.2 本校資訊機房伺服器所使用之電腦軟體均須具有合法版權，人員不得私自安裝非法電腦軟體。

5.3 本校人員若有安裝機房伺服器軟體需求時，需填寫「資通服務申請表」，經權責主管以上核准後，始得執行安裝。

6 保密協定

6.1 本校人員應填具「保密切結書」，承諾任職期間，因職務上所獲悉之任何資訊或持有之資料、檔案、技術、財務或業務上之機密，非經主管授權不得對外透露或加以濫用。

7 公告與實施

7.1 本守則由本校資通安全委員會通過後公告實施，修訂時亦同。

7.2 本校員工若未遵守上述規定或資通安全政策及程序者，得依相關懲戒程序處置違紀人員。

簽署人：_____

中　　華　　民　　國　　年　　月　　日

專職(責)人力及經費配置

- 經費配置
  - 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查

機關名稱	機關年度經費-資本門	機關年度經費-經常門	年度資訊經費-資本門	年度資訊經費-經常門	年度資安經費-資本門	年度資安經費-經常門
○○學校	1,000,000	700,000	40,000	30,000	10,000	8,000

計畫分級 / 年度	中長程計畫總經費		
	1 億以下(含)	1~10 億(含)	10 億以上
2020 年資安經費	至少為計畫之資訊建設經費 7%	至少為計畫之資訊建設經費 6%	至少為計畫之資訊建設經費 5%
2025 年資安經費	至少為計畫之整體經費 7%	至少為計畫之整體經費 6%	至少為計畫之整體經費 5%

資料來源：107~114年資安產業發展行動計畫

資訊及資通系統之盤點及風險評估

查核內容	準備資料或客觀證據
4.1 是否建立資訊及資通系統資產目錄，並隨時維護更新？(本項將列為實地稽核重點項目，並納入機關(校長)考核參考)	資訊資產清單
4.2 各項資產是否有明確之管理者及使用者？	資訊資產清單
4.3 是否定有資訊、資通系統分級與處理之相關規範？	維護計畫核心系統
4.4 是否進行資訊、資通系統之風險評估，並採取相應之控制措施？	資訊資產清單風險評估表

資產盤點範例

A	B	C	D
資產編號	資產類別	資產名稱	資產說明
IS-CM-00	CM	負載平衡器	FortiADC 200F 負載平衡器 1部
IS-CM-00	CM	防火牆	FG-201E對外防火牆 1部
IS-CM-00	CM	流量控制	GSI內部上網行為管理 1部
IS-CM-00	CM	核心交換器	Cisco C4503-E 核心交換器 1部
IS-CM-00	CM	主幹網路中繼交換器(各棟樓)	Cisco C2650-S 交換器 4部 Cisco C2650-X 交換器 1部
IS-CM-00	CM	一般網路邊際交換器(各辦公室)	ZyXEL GS2200-24 交換器 17部 Cisco C2960-L 交換器 1部
IS-CM-00	CM	一般網路交換器(收容電腦與專科教室)	Cisco C3750G 交換器 1部
IS-CM-00	CM	無線網路邊際供電交換器(POE)	Cisco C3650G POE交換器 3部 Aruba 1930 POE交換器 1部
IS-CM-00	CM	無線網路控制器	Aruba 7030 控制器 1部
IS-DA-00	DA	重要系統資料	Core Switch設定檔
IS-DA-00	DA	一般系統資料	學校網站及公告資料
IS-DA-00	DA	一般系統資料	校園網路連線架構圖
IS-DA-00	DA	一般系統資料	無線AP點位圖與列表
IS-DA-00	DA	一般系統資料	各類資訊設備紀錄檔
IS-DC-00	DC	限閱文件(固定資產)	網路機房資訊設備清冊
IS-DC-00	DC	限閱文件(機房維護合約)	機房維護合約
IS-DC-00	DC	限閱文件(ISP合約)	TANET與兩條光纖線路合約
IS-DC-00	DC	限閱文件(設備採購與保固資料)	各項設備採購與授權保固等資料
IS-DC-00	DC	敏感文件(IP清冊)	全校設備、網段與IP清冊
IS-DC-00	DC	一般文件(各式申請表)	資通資產報廢硬碟處理申請表
IS-DC-00	DC	一般文件	機房進出紀錄、巡檢表
IS-EV-00	EV	穩壓器	穩壓器 1部
IS-EV-00	EV	不斷電系統	UPS 3部
IS-EV-00	EV	冷氣設備	機房內2部及辦公區1部，共3部
IS-EV-00	EV	消防設施	滅火器二氧化碳，共2支
IS-EV-00	EV	監視設備	監視主機1部、監視鏡頭4支
IS-EV-00	EV	門禁設備	門禁主機1部
IS-HW-00	HW	主要系統主機	HP DL380 Gen10 伺服器 3部 VMware主機16部
IS-HW-00	HW	磁碟儲存陣列	NetApp E2812 儲存設備 2部 HP MSA2000 儲存設備 1部
IS-HW-00	HW	主要系統網路設備	Cisco MDS9148 HP StorageWorks 8/8 SAN switch
IS-HW-00	HW	網路附加儲存系統	Synology RS4017XS+ NAS 1部
IS-HW-00	HW	一般系統主機	HP DL380 Gen9 伺服器 1部(優質化網站)
IS-HW-00	HW	一般系統主機	HP DL380 Gen8 伺服器 1部(TQC檢定伺服器)
IS-HW-00	HW	無線網路AP主機	Aruba AP92 共16台、AP225共20台、AP325共10台、AP335共8台，共54台
IS-HW-00	HW	個人電腦	辦公區桌上型電腦共3部
IS-HW-008	HW	個人電腦	辦公區桌上型電腦共3部
IS-HW-009	HW	筆記型電腦	網管人員使用筆電(測線用)，共1部
IS-HW-010	HW	一般系統主機	DELL直立式伺服器 2部(TQC檢定伺服器)
IS-HW-011	HW	LOG管理分析系統	N-Reporter 1部
IS-PE-001	PE	設備維護人員	網管1位
IS-PE-002	PE	資訊設備委外維護人員	機房維護廠商工程師1位、業務1位
IS-PE-003	PE	一般使用人員	一般網路使用者
IS-PE-004	PE	資通安全組織	資通安全組織成員
IS-PE-005	SW	智慧網管軟體	Pixis
IS-SW-001	SW	作業系統(個人電腦用)	Windows OS(全校授權)
IS-SW-002	SW	作業系統(伺服器用)	Windows Server 2012R2 Windows Server 2019 標準版 x 2套
IS-SW-003	SW	套裝軟體(授權軟體)	MS Office辦公室應用軟體(全校授權)
IS-SW-004	SW	防毒軟體(個人電腦用)	ESET校園授權500U
IS-SW-004	SW	防毒軟體(伺服器用)	ESET伺服器授權1U(優質化主機用)
IS-SW-005	SW	備份軟體(系統備份)	Veeam
IS-SW-006	SW	備份軟體(行政備份)	Acronis 授權75套

核心業務及重要性

❑ 非核心業務及說明範例

非核心業務系統	業務失效影響說明	最大可容忍中斷時間
防火牆系統	可能使本校資安防護中斷	○小時
防毒系統	可能使本校資安防護中斷	○小時
監視系統等OT系統	可能使本校部分業務中斷	○小時
其他(不含親師生**個人資料**之資通系統)	可能使本校部分業務中斷	○小時

註：

1. 盤點對象為**具權限區分及管理功能之資通系統**
2. 最大可容忍中斷時間參考核心業務訂定原則，但**應大於或等於核心業務資通系統中最大值者**

資通安全管理措施之實施情況

查核內容	準備資料或客觀證據
5.1 人員進入重要實體區域是否訂有安全控制措施？	資訊設備主機機房門禁照片
5.2 重要實體區域的進出權利是否定期審查並更新？	進出人員清單
5.3 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	人員進出紀錄表
5.4 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？	巡查紀錄表
5.5 各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？	消防、CCTV、門禁設施檢查紀錄或保養資料。 設備使用訓練紀錄。
5.6 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	陪同進出之紀錄及照片
5.7 重要資訊處理設施是否有特別保護機制？	實體安全管理制度
5.8 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？	例如：資訊機房偵煙、偵熱與滅火設備、漏水偵測等照片。

資通安全管理措施之實施情況(cont.)

查核內容	準備資料或客觀證據
5.9 電源之供應及備援電源是否作安全上考量？	電力保護設施照片(UPS、穩壓器接地線等)、緊急照明設備照片
5.10 通訊線路及電纜線是否作安全保護措施？	線路保護設施照片(如線槽、高架地板、套管等)
5.11 設備是否定期維護，以確保其可用性及完整性？	系統主機及網路維護紀錄或合約、機房查檢紀錄表
5.12 設備送場外維修，對於儲存資訊是否訂有安全保護措施？	設備進出管理制度。(B-002 5.7.2)設備進出紀錄表
5.13 可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)？	防毒軟體、登入等照片、設備領用紀錄。
5.14 設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	報廢管理制度及報廢紀錄
5.15 公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	管理制度及實體防護照片(例如：資料上鎖)。
5.16 系統開發測試及正式作業是否區隔在不同之作業環境？	測試環境與正式環境照片、不適用則免附。

資通安全管理措施之實施情況(cont.)

查核內容	準備資料或客觀證據
5.17 是否全面使用防毒軟體並即時更新病毒碼？	至少2位一般使用者的個人電腦設定畫面
5.18 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	至少2位一般使用者的個人電腦設定畫面
5.19 是否定期執行各項系統漏洞修補程式？	系統主機及個人電腦各兩臺設定畫面
5.20 是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？	管理制度(B-007 5.3.5)
5.21 重要的資料及軟體是否定期作備份處理？	備份工作相關紀錄
5.22 備份資料是否定期回復測試，以確保備份資料之有效性？	備份回復演練紀錄
5.23 對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	系統登作畫面、https、檔案加密。
5.24 是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？	可攜式媒體管理制度

防毒軟體程序設定

快速掃描

建議的 () 快速掃描查看可能已註冊惡意程式碼的所有位置，例如登錄機碼和已知的 Windows startup 資料夾。結合 always on 即時保護，可在開啟及關閉檔時對其進行審閱; 每當使用者流覽至資料夾時，快速掃描可協助對以系統和內核層級惡意程式碼開頭的惡意程式碼提供強防護。

在大多數情況下，快速掃描足以滿足計畫掃描的建議選項。

完整掃描

完整掃描會從執行快速掃描開始，繼續執行所有已裝載固定磁片及移除/網路磁碟機的連續檔案掃描(如果完整掃描已設定為執行此作業) 。
根據需要掃描的資料量和類型，完整掃描可能需要數小時或數天才能完成。

完成完整掃描之後，就可以使用新的安全性智慧，並必須進行新的掃描，以確保不會以新的安全性情報偵測到其他威脅。

由於完整掃描所涉及的時間和資源，在一般情況下，Microsoft 不建議排程完整掃描。

自訂掃描

自訂掃描是在您指定的檔案和資料夾上執行的快速掃描。 例如，您可以選擇掃描 USB 磁片磁碟機，或裝置的本機磁片磁碟機上的特定資料夾。

Windows 系統管理工具→工作排程器→Microsoft→Widnows→Windows Defender→Windows Defender Schedule→觸發程序→新增→設定

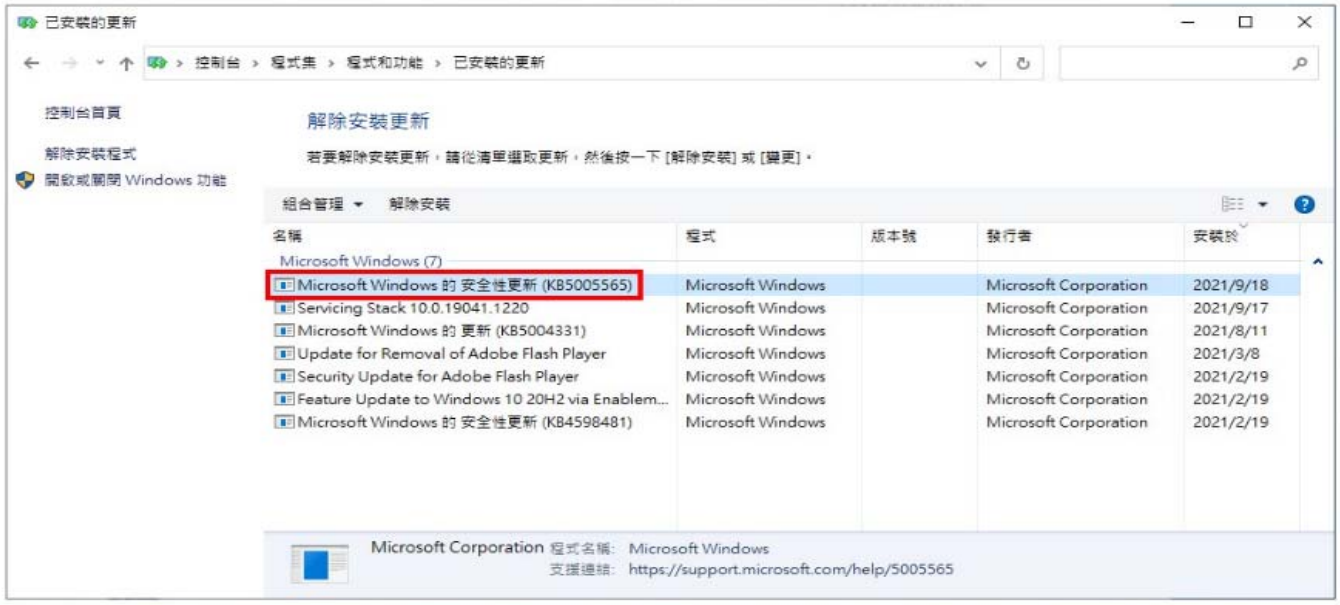
電腦使用之安全管理

- 微軟Windows之MSHTML引擎存在安全漏洞(CVE-2021-40444)

請各位同仁檢視自己的電腦並於中午12:00回填表單

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444

開始→Windows系統→控制台→檢視方式:類別→程式集→程式與功能→檢視已安裝的更新



Win10的各版本中，只要有 KB5005565、66、68、69、73 其中一個，就表示有確實進行更新！

留意的已安裝的過舊軟體

- 7-Zip 18.05版本以上
- 防毒軟體
- Acrobat Reader
- Office軟體

End Of Life – Microsoft Windows and Office

Microsoft has a support lifetime for each of their products. Below is a list of software that has or soon will reach its end of life and support. You should not run software that is not supported, since it may contain security issues that are not fixed and can put your computer and information at risk. Michael Spice can help you with replacement and updating to a supported version of Office, Windows and Windows Server.

Microsoft Office

Microsoft Office 2003 – April 8, 2014
Microsoft Office 2007 – October 10, 2017
Microsoft Office 2010 – October 13, 2020
Microsoft Office 2011 for Mac – October 10, 2017
Microsoft Office 2013 – April 11, 2023
Microsoft Office 2016 – October 14, 2025
Microsoft Office 2016 for Mac – October 13, 2020
Microsoft Office 2019 – October 14, 2025
Microsoft Office 2019 for Mac – October 10, 2023
Microsoft Office 2021 – October 13, 2026
Microsoft Office 2021 for Mac – October 13, 2026

Microsoft Windows

Microsoft Windows XP – April 8, 2014
Microsoft Windows Vista – April 11, 2017
Microsoft Windows 7 – January 14, 2020
Microsoft Windows 8 – January 12, 2016 users must upgrade to Windows 8.1
Microsoft Windows 8.1 – January 10, 2023
Microsoft Windows 10 release 1507 from July 2015 – May 9, 2017

資料壓縮軟體 7-Zip 發現安全漏洞，儘速升級最新版本

7-Zip 是一款自由及開放原始碼軟體（free and open source software，FOSS）的資料壓縮軟體，主要應用在微軟 Windows 作業系統，不須註冊或支付使用費，是由俄羅斯程式設計師伊戈爾帕夫洛夫（Игорь Павлов）自 1999 年開始開發。7-Zip 預設的檔案格式為自行開發的 7z 格式，副檔名則是 .7z，這款軟體也支援常見的檔案格式如 ZIP、RAR 等解壓縮。

網際網路安全中心（Center for Internet Security，CIS）近日指出，7-Zip 有任意代碼執行（Arbitrary Code Execution，ACE）的安全漏洞，這代表不法人士可在您的電腦植入並執行惡意程式，查看、編輯或刪除用戶電腦的數據資料，甚至創立具有完整用戶權限的帳號。

CIS 表示目前雖然沒有災情傳出，不過 7-Zip 18.05 之前的所有版本皆有漏洞，呼籲用戶前往官網下載、儘速升級至 4 月 30 日發表的最新版本。

- A Vulnerability in 7-Zip Could Allow for Arbitrary Code Execution
- A serious security vulnerability has been found in 7-Zip

Release Notes | Acrobat, Reader

Acrobat DC and Acrobat Reader DC Continuous Track release notes

Date	Release Notes	Release Type*	Focus
Oct 12, 2021	DC Oct 2021 (21.007.20099)	Continuous	**Latest Release:** This update provides security mitigations and bug fixes.
Sep 29, 2021	DC Sep 2021 (21.007.2009x)	Optional Update	This patch fixes specific functionality issues.
Sep 14, 2021	DC Sep 2021 (21.007.20091)	Continuous	This update provides new features, security mitigations, feature enhancements, and bug fixes.
Jul 28, 2021	DC Jul 2021 (21.005.20060)	Optional Update	**[Win Only]** This patch fixes specific functionality issues.
Jul 13, 2021	DC Jul 2021 (21.005.20058)	Continuous	This update provides new features, security mitigations, feature enhancements, and bug fixes.
Jun 08, 2021	DC Jun 2021 (21.005.20048)	Continuous	This update provides new features, security mitigations, feature enhancements, and bug fixes.
May 11, 2021	DC May 2021 (21.001.20155)	Continuous	This update provides security mitigations and bug fixes.

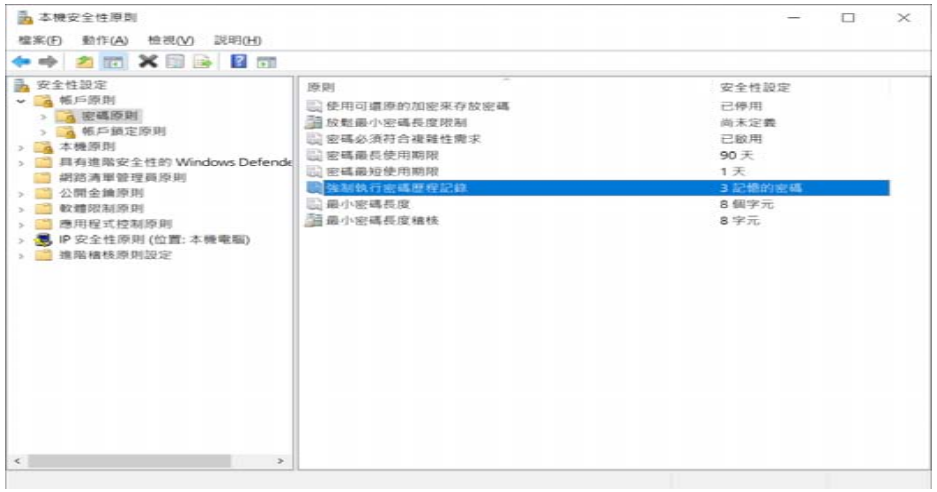
資通安全管理措施之實施情況(cont.)

查核內容	準備資料或客觀證據
5.25 是否訂定使用者存取權限註冊及註銷之作業程序？	帳號申請及註銷管理制度
5.26 使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？	帳號
5.27 通行碼長度是否超過8個字元？	通行
5.28 通行碼是否規定需有大小寫字母、數字及符號組成？	通行
5.29 是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？	網路架構圖及業務與網段對應資料，內網區隔狀況、網路管理規定
5.30 對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？	遠端連線作業
5.31 是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)？	行動式電腦設備管理制度
5.32 重要系統是否使用憑證作為身份認證？	憑證使用認證佐證資料 (不適用者免附)

建議包含重要系統、主機、網路設備帳號清查佐證紀錄，並每年定期清查一次

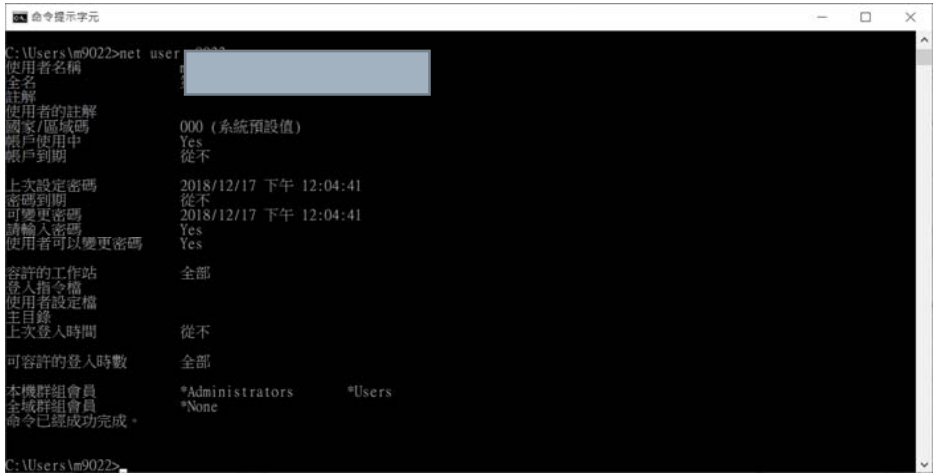
密碼設定與查詢

- Windows 系統管理工具→本機安全性原則→安全性設定→帳戶原則→密碼原則



- CMD模式→net user 帳號

若上次設定密碼時間為當下時間，則表示從未設定密碼



資通安全管理措施之實施情況(cont.)

查核內容	準備資料或客觀證據
5.33 系統變更後其相關控管措施與程序是否檢查仍然有效？	資訊服務變更管理制度及紀錄。
5.34 是否可及時取得系統弱點的資訊並作風險評估及採取必要措施？	弱掃報告及高風險弱點修補處理狀況
5.35 限制使用危害國家資通安全產品-大陸廠牌產品清冊列管及說明。	1.檢視資通系統及設備是否使用危害國家資通安全產品(如大陸廠牌) 2.大陸廠牌產品清冊(包含硬體、軟體、服務，請上傳可編輯檔案如excel,ods等)
5.36 限制使用危害國家資通安全產品-汰換大陸廠牌產品及說明。 1.110年12月31日前完成汰換大陸廠牌產品 2.如無法於期限內完成汰換，須於大陸廠牌產品清冊述明理由	1.大陸廠牌產品汰換紀錄 2.大陸廠牌產品清冊(包含硬體、軟體、服務，請上傳可編輯檔案如excel,ods等)

訂定資通安全事件通報及應變之程序及機制&定期辦理資通安全認知宣導及教育訓練

查核內容	準備資料或客觀證據
6.1 是否建立資通安全事件發生之通報應變程序？	資通安全事件通報及應變管理程序。
6.2 機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理？	宣導及公告相關資料。
6.3 是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？	安全事件報告單或矯正紀錄

查核內容	準備資料或客觀證據
7.1 是否定期辦理資通安全認知宣導？	資通安全公告、宣導及研習資料
7.2 是否對同仁進行資安評量？	資安評量或資安研習評量資料
7.3 是否對同仁依層級定期舉辦資通安全教育訓練？	資安教育訓練資料 資通安全認知訓練時數要求： 1.全體同仁每人每年須接受3小時以上一般資通安全教育訓練。 2.專職(責)人員以外之資訊人員每人每年須接受3小時以上之資通安全專業課程訓練或資通安全職能訓練。 3.專職(責)人員每年須接受12小時以上資通安全專業課程訓練或資通安全職能訓練。
7.4 同仁是否瞭解單位之資通安全政策、目標及應負之責任？	公告、宣導、人員安全守責等資料。

資通安全維護計畫實施情形之精進改善機制&資通安全維護計畫及實施情形之績效管考機制

查核內容	準備資料或客觀證據
8.1 是否設有稽核機制？	內稽制度
8.2 是否定有年度稽核計畫？	內稽計畫書
8.3 是否定期執行稽核？(建議2年1次)	內稽紀錄
8.4 是否改正稽核之缺失？	內稽缺失矯正紀錄

查核內容	準備資料或客觀證據
9.1 是否訂定安全維護計畫持續改善機制？	矯正及預防管理制度
9.2 是否追蹤過去缺失之改善情形？	矯正及預防處理單
9.3 是否定期召開持續改善之管理審查會議？	管審會議紀錄

Why內部稽核(維護計畫範例)

- 資通安全維護計畫及實施情形之持續精進及績效管理機制(第拾節)
  - 本校資通安全維護計畫之實施
    - 為落實本安全維護計畫，使本校之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本局之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。
  - 本校學校資通安全維護計畫實施情形之稽核機制
    - 稽核機制之實施
      - 資通安全推動小組應於12月前(至少每年一次)或於系統重大變更或組織改造後執行 1次內部稽核作業(自我檢查作業)，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。

稽核計畫

- 資訊安全稽核小組成員
  - 組長
  - 組員
- 稽核時程
- 稽核日期

日期	時間	項目	稽核人員	地點
xxx/xx/xx	10:00-10:20	啟始會議		
	10:20-10:30	高階主管訪談		
	10:30-12:00	一、核心業務及其重要性 二、資通安全政策及目標 三、設置資通安全推動組織 四、人力及經費之配置 五、資訊及資通系統之盤點及核心資通系統、相關資產之標示 六、資通安全風險評估 七、資通安全防護及控制措施	xxx Xxx xxx	
	12:00-13:00			
	13:00-15:30	七、資通安全防護及控制措施 八、資通安全事件通報、應變及演練相關機制 九、資通安全情資之評估及因應機制 十、資通系統或服務委外辦理之管理 十一、資通安全教育訓練 十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制 十三、資通安全維護計畫及實施情形之持續精進及績效管理機制	xxx xxx xxx	
	15:30-16:00	稽核結果彙整		
	16:00-16:30	結束會議		

資通系統委外(含委辦)案之履約檢核及督導管理(無則請填寫不適用)

查核內容	準備資料或客觀證據
10.1 資通系統委外(含委辦)是否簽訂協議書或契約？	委外(含委辦)案之協議書、契約書等文件，應符合資安法施行細第4款各項規定。
10.2 是否落實檢核及履約督導管理？	檢核受託單位繳交之資料，應附廠商承諾辦理資安相關事項之證明文件。
10.3 委外(含委辦)相關人員是否簽訂保密合約書？	保密切結書、保密合約書等文件

其他應辦事項

查核內容	準備資料或客觀證據
11.1 是否每年檢視一次資通系統(自有及委外)分級妥適性？	資通系統(自有及委外)分級相關文件(資通安全責任等級分級辦法附表九)
11.2 是否每兩年辦理一次資通安全健診？ (本項C級機關列入評分，D級機關不列入評分)	資通安全健診報告
11.3 是否完成資通安全防護(防毒軟體、網路防火牆、電子郵件過濾機制)？	1. 檢視資通設備是否安裝防毒軟體 2. 檢視網路防火牆建置情形 3. 具有電子郵件伺服器者，檢視電子郵件過濾機制
11.4是否完成資通安全弱點通報機制導入作業 (111年尚在導入階段，暫不列入評分，C級機關應於2年完成導入)	C級機關：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。 資安法於110年8月23日修法，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。

資產盤點與風險評估

資產與資訊

- 資產是甚麼？
  - 組織直接賦予價值並需要組織的保護
  - 相關於資訊安全管理系統的範圍
- 資訊是組織資產的一部份，具有價值且需要持續被適切地保護

資產清冊建立

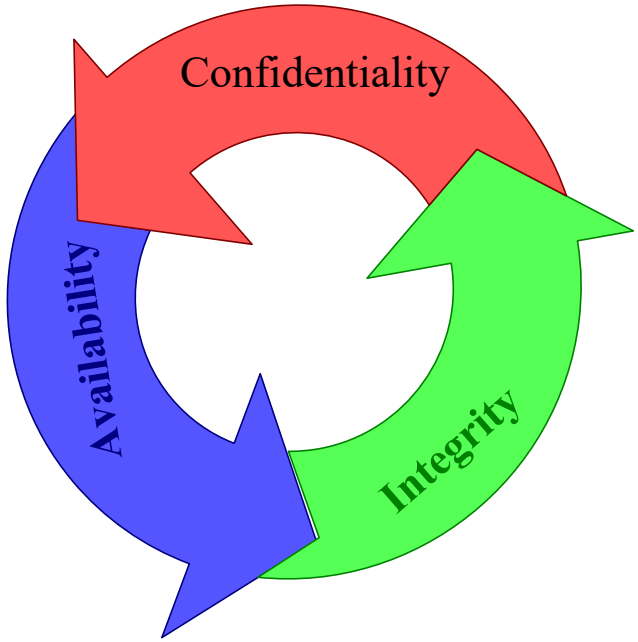
- 權責單位應建立「資訊資產清冊」
  - 清點及鑑別所管轄之資訊資產
  - 定期更新與維護
  - 彙整資訊資產清冊，陳報至資訊安全管理小組予以統一控管，確保資訊資產編號及清冊之完整性

資產鑑別

- 資訊資產分類
  - 人員：同仁、廠商
  - 文件：紙本存在之文書資料，公文、報表等
  - 資料：存放於儲存媒介之數位資訊
  - 軟體：作業軟體、套裝軟體、原始碼、資料庫等
  - 通訊：網路設備、資訊傳輸或服務
  - 硬體：主機設備
  - 環境：基礎設施與服務、環控、電力

資訊資產價值鑑別

- 不被洩露與確保機密（機密性，C）
- 資訊、系統、服務等正確性被扭曲（完整性，I）
- 系統不會因破壞而影響持續運轉（可用性，A）



機密性評估標準

- 範例

評估標準	數值
一般：此資訊資產無特殊之機密性要求	1
限閱：此資訊資產含敏感資訊，但無特殊之機密性要求，且僅供組織內部人員或被授權之外部單位使用	2
敏感：此資訊資產僅供內部相關業務承辦人員存取	3
機密：此資訊資產所包含資訊為組織或法律所規範的機密資訊	4

完整性評估標準

- 範例

評估標準	數值
資產本身完整性要求極低	1
資產本身具有完整性要求，但是完整性被破壞不會對本會造成傷害	2
資產具有完整性要求，且完整性被破壞會對組織造成傷害，但不至於太嚴重	3
資產具有完整性要求，且完整性被破壞會對組織造成傷害，甚至會造成業務終止	4

可用性評估標準

- 範例

評估標準	數值
該資訊資產容許失效 3 天以上，不用被修復或是尋找替代品。	1
該資訊資產容許失效 8 小時以上，3 天以下，不用被修復或是尋找替代品。	2
該資訊資產容許失效 4 小時以上，8 小時以下，不用被修復或是尋找替代品。	3
該資訊資產容許失效 4 小時內不用被修復或是尋找替代品。	4

資產盤點範例

產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	擁有者	機密性	完整性	可用性	資產價值
PE-001	PE	管理階層人員	校長、教務主任、資訊組長	人事室	人事室	人事室	1	1	1	1
PE-002	PE	網路、系統維護人員	代理資訊教師	人事室	人事室	人事室	1	1	1	1
PE-003	PE	一般使用人員	教職員	人事室	人事室	人事室	1	1	1	1
IF-001	IF	作業文件	資料庫與資料檔案、備份資料	教務處	資訊組	資訊組長	1	1	1	1
IF-002	IF	系統文件	網路架構圖	教務處	資訊組	資訊組長	1	1	1	1
IF-003	IF	資訊紀錄（電子/紙本）	啟用與報廢紀錄單、資訊工作日誌、系統特權帳號清單、設備進出紀錄表	教務處	資訊組	資訊組長	1	1	1	1
IF-004	IF	系統紀錄（Log）	防火牆Log紀錄(一個月一次)	教務處	資訊組	資訊組長	1	1	1	1
HW-001	HW	伺服器	學校Web主機	教務處	資訊組	資訊組長	1	1	1	1
HW-002	HW	其他硬體	印表機、影印機	總務處	總務處	總務處	1	1	1	1
HW-003	HW	個人電腦	桌上型電腦	教務處	資訊組	資訊組長	1	1	1	1
HW-004	HW	可攜式電腦	筆記型電腦	教導處	教導處	教導主任	1	1	1	1
HW-005	HW	資安設備	Zyxel防火牆	教務處	資訊組	資訊組長	1	1	1	1
HW-006	HW	網路設備	Zyxel交換器、L3交換器	教務處	資訊組	資訊組長	1	1	1	1
HW-007	HW	可攜式儲存媒體	USB、記憶卡、CD、DVD、投影機。	教務處	資訊組	資訊組長	1	1	1	1
SW-001	SW	作業系統	KMS	教務處	資訊組	資訊組長	1	1	1	1
SW-002	SW	資訊安全系統	防火牆軟體(Zyxel)	教務處	資訊組	資訊組長	1	1	1	1
EV-001	EV	一般辦公區域	辦公室、會議室。	學校	學校	學校	1	1	1	1
EV-002	EV	資訊機房	電腦機房	教務處	資訊組	資訊組長	1	1	1	1
EV-003	EV	建築保護設施	不斷電系統、穩壓器、機櫃、滅火器、發電機	總務處	總務處	總務處	1	1	1	1

類別：人員 (PE)、資訊 (IF)、硬體 (HW)、軟體 (SW)、環境 (EV)

表單之前，請確認表單版本是否已更新

資產盤點重點建議

- 備份設備、資料
- 重要作業系統、資料庫、應用軟體盤點與版本註記
- 人員與環境資產盤點

資產價值標示與使用

- 實體設備(沒有一定要標示)
  - 資產價值1→紅色
  - 資產價值2→綠色
  - 資產價值3→黃色
  - 資產價值4→藍色
- 文件資料
  - 一般、限閱、敏感、機密
- 程序書
  - 實體安全管理、存取控制管理、系統開發與維護...

資產管理循環

資產複核與銷毀

- 權責單位每年至少進行1次資產盤點與資產清冊複核。
- 當範圍內有以下的狀況發生之時，則實施不定期的複核
  - 有新增、變更或移除資訊資產
  - 系統有重大異動
  - 作業環境改變
- 資訊資產之報廢（或銷毀）應視其機密等級，採取適當之方式進行銷毀

汰除儲存設備處理

[原件]大量行政文件洩露了硬盤轉售的稅收記錄等

神奈川硬盤流出

勝木茂　十二月6，2019 5:00

分享　鳴叫　書籤　電子郵件　印刷

清單　970

包括朝日新聞採訪中發現的大量個人信息和機密信息（例如稅務局 神奈川縣 行政文件）已經被積累的 硬盤（HDD），網絡拍賣 被轉售出去。從縣服務器上卸下的HDD被作為二手物品出售，數據擦除不足。據該縣稱，一家公司的員工承擔著從擦除數據到丟棄數據的所有工作，並承認他們參與了轉售。

經縣確認，HDD用作共享服務器，用於累積有關縣辦公室內每個部門的信息。其中包括稅務檢查 後的公司名稱通知，帶有個人名稱和地址的 汽車納稅 記錄，公司提交的文件，縣職員的業務記錄以及目錄。..

據該縣稱，已轉售的HDD 被用於從富士通租賃公司（ 東京千代田區 ）租用的服務器，並在今年春天將要更換的服務器上將其從服務器中取出。根據與縣的合同，富士通租賃 將使 數據不可恢復的工作委託給 Brodrink（東京都中央區）進行處理，該公司負責信息設備的再現業務。富士通租賃已指示其銷毀它並使它無法使用，然後再丟棄它或完全擦除數據。

從縣到 Broadlink 交付時，HDD進行了簡單的數據擦除（初始化）。HDD 存儲在東京的 Broadlink 設施中，但是負責擦除數據的人員帶出了一部分數據，並將其放在拍賣現場。

一家經營IT公司的人成功地使用了9塊HDD進行工作。當該人檢查內容以確認使用前的安全性時，他注意到數據的存在。據說使用該恢復軟件保存了被認為是 神奈川縣的 正式文件的大量文件。

資料來源：招日新聞

資訊及資通系統盤點範例

項次	資產名稱	類別	擁有者/職稱	管理者（部門）	使用者（部門）	存放位置	數量	說明	備註
1.	EVO 派送軟體	軟體資產	資訊教師	總務處	全校師生	電腦教室	1 套		
2.	個人電腦	實體資產	全體教職員	資訊教師	全體教職員	教室/辦公室	42 台		
3.	行動裝置	實體資產	全體教職員	資訊教師	全體教職員	教室/辦公室	33 台	筆電、平板、手機	
4.	可攜式媒體	實體資產	全體教職員	全體教職員	全體教職員	教室/辦公室	1 式	有資料的光碟、外接式硬碟、隨身碟	
5.	學校網站	軟體資產	資訊教師	資訊教師	全體教職員	教育局	1 式	局端雲端機房	
6.	NAS 儲存裝置	實體資產	資訊教師	資訊教師	全體教職員	主機房	1 台		
7.	AD 系統	軟體資產	資訊教師	資訊教師	資訊教師	教育局	1 套	局端雲端機房	
8.	主管人員	人員資產	校長	校長	校長	辦公室	1 式	主任以上	

風險評鑑範例

項次	資產名稱	類別	擁有者/職稱	機密性©	完整性(I)	可用性(A)	資訊資產價值(T)(C,I,A取最大值)	潛在風險事件	風險發生可能性(V)	風險值 資訊資產價值*(T*V)
1.	EVO派送軟體	軟體資產	資訊教師	1	1	3	3	1.3.2	2	6
2.	個人電腦	實體資產	全體教職員	1	1	2	2	2.3.3	2	4
3.	行動裝置	實體資產	全體教職員	1	1	1	1	2.4.3	2	2
4.	可攜式媒體	實體資產	全體教職員	1	1	1	1	2.5.2	2	2
5.	學校網站	軟體資產	資訊教師	1	1	1	1	1.2.2	1	1
6.	NAS儲存裝置	實體資產	資訊教師	2	1	2	2	2.1.3	1	2
7.	AD系統	軟體資產	資訊教師	3	2	2	3	1.1.4	1	3
8.	主管人員	人員資產	校長	1	1	1	1	4.2.1	1	1

風險評鑑範例(cont.)

資產大類	資產小類	潛在風險事件	管控措施範例說明
1. 軟體資產類	1. 1 作業系統	1. 1. 1 未落實作業系統更新/漏洞修補，致使遭受惡意攻擊、資料外洩或其他侵害。	-WSUS 機制失效 -定期檢查漏洞更新狀態 -資訊單位定期彙整提供發佈更新資訊(，供業務單位進行比對
1. 軟體資產類	1. 1 作業系統	1. 1. 2 未購買妥適的作業系統授權/使用授權超過購買數，致使遭受廠商求償或抗議。	-作業系統授權清單
1. 軟體資產類	1. 1 作業系統	1. 1. 3 未汰換原廠公告停止技術支援之作業系統，進而無法修補漏洞，致使遭受惡意攻擊、資料外洩或其他侵害。	
1. 軟體資產類	1. 1 作業系統	1. 1. 4 未加入組織之網域，進而無法套用 GCB 或群組原則政策，致使無法有效管控。	-套用 GCB 設定，或設定適當權組原則
1. 軟體資產類	1. 1 作業系統	1. 1. 5 個人電腦或伺服器等資訊設備，未安裝適當之防毒軟體或安全防護軟體，於網路連線時遭電腦病毒入侵或被植入惡意程式，致使資料外洩或遭受其他侵害。	
1. 軟體資產類	1. 1 作業系統	1. 1. 6 作業系統最高管理權限管制不當，有共用或浮濫設定的情形。	
1. 軟體資產類	1. 2 套裝軟體	1. 2. 1 未購買妥適的套裝軟體授權或使用超過購買授權數量，致使可能違反智慧財產權，遭受廠商求償。	-軟體管制清單 -軟體授權資料 -資產管理工具

風險評鑑範例(cont.)

資產大類	資產小類	潛在風險事件	管控措施範例說明
3. 資料資產類	3. 1 紙本文件	3. 1. 1 資訊系統相關技術說明、設定或規劃文件，未有適當控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-如文件櫃上鎖存放
3. 資料資產類	3. 1 紙本文件	3. 1. 2 業務資料或其它包含機敏資訊之文件，未依安全等級控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-依資訊資產安全等級限閱或敏感等級進行管理
3. 資料資產類	3. 1 紙本文件	3. 1. 3 業務資料或其它包含一般資訊之文件，違反組織作業程序或法令法規之要求，致使資料遭不當使用後，影響法律規章遵循或損害組織信譽。	-依資訊資產安全等級一般或公開等級進行管理
3. 資料資產類	3. 1 紙本文件	3. 1. 4 包含個人資料之文件，未有適當控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-依個人資料檔案機密等級進行管理
3. 資料資產類	3. 1 紙本文件	3. 1. 5 逾保存期限之紙本文件、表單或紀錄，未能適度予以銷毀，造成保存之文件與資料過多，致使發生遺失或外洩情況時，增加組織遭損害求償之風險或損害組織信譽。	-依文件與紀錄管理程序書進行管理

風險評估注意事項

- 相關資訊資產是否皆納入風險評估範圍？
- 風險評估之影響程度、發生可能性之判斷原則。
- 可能面對的潛在風險因子(威脅、弱點)
- 是否識別出可接受風險值？
- 針對高於可接受風險值之項目採取改善措施！

- 戴口罩
- 實名制
- 區域消毒
- 居家隔離
- 人潮分流
- 施打疫苗
- 罰款
- .....

風險處理-計畫

- 風險處理計畫是定義行動以降低無法接受的風險，和實施所需的控制措施以保護資訊的一種「合作文件」
  - 針對高風險(超過可接受風險)項目或認為應該要處理的項目
  - 避免偶發、特殊或超過組織處理能力的風險
  - 預估風險處理後之殘餘風險(若無法低於可接受風險即應重新擬定風險處理計畫)

風險處理-方向

- 接受殘餘(剩餘)的風險
- 避免風險
- 轉移風險
- 降低風險到可接受程度

可接受風險的等級

- 要達到完全的安全是不可能的
- 總是有殘餘的風險
- 甚麼樣程度的剩餘風險能為組織所接受

〔即時新聞／綜合報導〕嚇死人！新竹竹北大風來襲，路上的紅路燈被吹倒，有車輛當場受到波及，所幸車主沒有大礙。

在東北季風、熱帶性低氣壓外圍環流的影響下，北部多處地區下起豪大雨，全台18個縣市也出現強風，「我們新竹竹北的風不是開玩笑的大」，有網友在臉書社團「爆廢公社」分享新竹竹北某處道路的行車紀錄器畫面，可以看到道路中央的紅綠燈突然倒下，硬生生直接倒在車子上，擋風玻璃被砸出裂痕，駕駛嚇到當場飆髒話，所幸無人傷亡，恐怖畫面讓原PO不禁驚呼，「這個風都可以演絕命終結站了」。

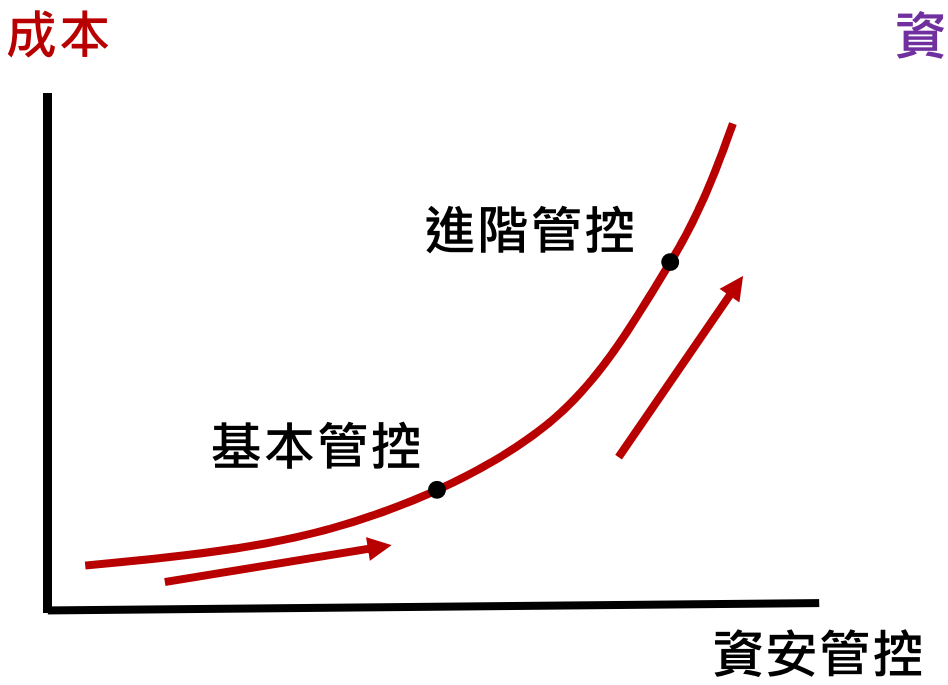
資料來源：自由電子報

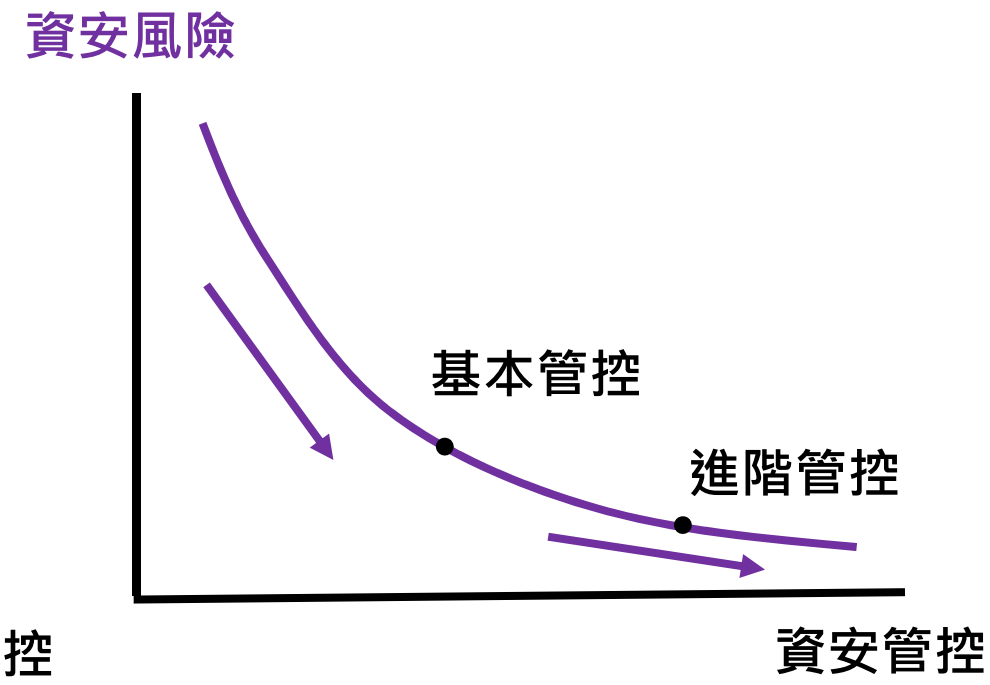
結論

資安法的修訂與發展

- 修訂原則愈趨嚴格。
  - 資通系統認定包括電子郵件、目錄服務系統，資料庫、帳務處理。
  - 保留稽核事件紀錄至少六個月以上。
- 可能仍處於滾動式修正的狀態。
- 各級學校皆應積極應對與推動資安業務。

資安管控與成本考量






QUESTIONS
ANSWERS