國立高雄大學圖書資訊館

Library and Information Center

資通安全電子報

2026.01.02發行

本期目錄

114年度本校資安工作報告

項次	工作任務	重點工作事項	執行日期	執行情形
1	資通安全暨個人資料保護推動委員會召開	1. 審核、發布本校資訊安全政策。 2. 管審會議報告。 3. 確認人員編組。 4. 推動流程確認。	114 年 1 月 10 日	審查資訊安全相關執行情形及 113 年度工作事項。
2	組織編組	1. 確認各單位窗口人員異動情形。 2. 資安暨個資執行小組成員編組。	**資安窗口及資訊人員名單盤點：** 114 年 2 月 10 日至 114 年 2 月 27 日 **資安暨個資執行小組成員調查：** 114 年 2 月 25 日至 114 年 3 月 7 日	由各單位填寫「各單位資安窗口及資訊人員調查表」回報統計。
3	資安推動教育訓練	資訊安全管理制度程序教育訓練，包含各項日常維運之各式文件產出。	114 年 3 月 18 日	由圖書資訊館董建弘校聘工程師、胡世澤專員擔任講師，進行教育訓練。
4	資訊資產清查	清查並盤點各單位資訊資產。	114 年 3 月 18 日至 114 年 4 月 18 日	由各單位人員盤點所管理之資訊資產，並初步評估各資產價值，交由各單位資安窗口進行分類、彙整、確認資產價值，產出「資訊資產清單暨風險評鑑表」。
5	執行風險評鑑	各單位執行： 1. 進行資訊資產風險評鑑。 2. 資通系統分級妥適性檢視。 3. 委外廠商查核。 4. 執行核心資通系統調查。	114 年 3 月 18 日至 114 年 4 月 18 日	各單位產出： 1. 機關資通系統與服務資產清冊 2. 資訊資產清冊暨風險評鑑表 3. 資通系統妥適性檢視及防護基準實施情形評估表 4. 委外廠商查核項目表

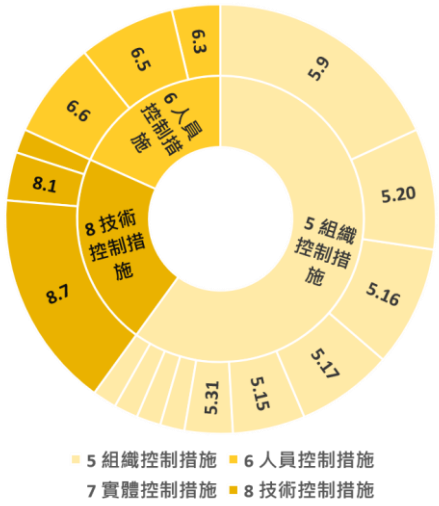
6	帳號清查、弱點掃描	1. 各單位進行資訊設備帳號清查。 2. 本館協助各單位進行弱點掃描，並交由各單位人員進行處理。	**帳號清查：** 114 年 6 月 16 日至 114 年 6 月 27 日 **弱點掃描：** 114 年 9 月 8 日	1. 帳號清查後，各單位產出「帳號清查紀錄表」、「帳號清查結果報告」。 2. 弱點掃描執行完畢後，提供掃描結果予各單位資安窗口，各單位針對所發現的弱點進行修補，並填寫「弱點處理報告單」。
7	資安窗口及資訊人員資安專業教育訓練	資安專業教育訓練。	114 年 4 月 18 日 114 年 6 月 17 日 114 年 11 月 7 日	漢昕科技顧問擔任講師。
8	核心系統及單位網頁營運持續演練	各單位進行核心系統營運持續演練，產出： 1. 業務永續運作計畫。 2. 業務永續運作計畫演練活動紀錄。	**核心系統業務永續演練：** 114 年 8 月 18 日 (教務系統服務) **單位網頁業務永續演練：** 114 年 7 月 1 日至 114 年 7 月 31 日	1. 核心資通系統每兩年辦理一次業務永續運作演練。 2. 於單位網頁業務永續演練後，各單位分別產出「業務永續運作計畫演練活動紀錄」、「資訊安全事件報告單」。
9	內部稽核	召集稽核分組人員產出： 1. 資訊安全管理制度內部稽核計畫。 2. 資訊安全管理制度內部稽核表。 3. 資訊安全管理制度內部稽核報告，並由受稽單位產出矯正與改善處理單。	**全校內稽：** 114 年 8 月 12 日 114 年 8 月 20 日 114 年 9 月 3 日 **圖資館內稽：** 114 年 9 月 5 日	1. 全校內部稽核由本校「資安與個資執行小組稽核分組」及「資訊安全小組」成員協助辦理；圖資館內部稽核委由具資訊安全稽核專業之外部人員協助進行，以確保稽核之客觀性。 2. 於稽核前訂定「資訊安全管理制度內部稽核計畫」、「內部稽核查檢表」。 3. 於稽核後產出「資訊安全管理制度內部稽核報告」、「矯正與改善處理單」。

10	主管教育訓練	主管教育訓練	114 年 11 月 28 日	由中興大學資管系教授兼教育機構資安中心主任陳育毅擔任講師。
11	帳號清查	各單位進行資訊設備帳號清查	114 年 12 月 5 日至 114 年 12 月 19 日	帳號清查後，各單位產出「帳號清查紀錄表」、「帳號清查結果報告」。

114年度本校各單位內稽發現

114 年全校內部稽核於 8 月 20 日至 9 月 3 日辦理，本年度各單位內稽結果統計如下：

項目	敘述	件數
5.9	資訊及其他相關聯資產之清冊	10
8.7	防範惡意軟體	9
5.20	於供應者協議中闡明資訊安全	5
5.16	身分管理	4
5.17	鑑別資訊	4
6.5	聘用終止或變更後之責任	4
6.6	機密性或保密協議	4
5.15	存取控制	3
5.12	資訊之分類分級	2
5.31	法律、法令、法規及契約要求事項	2
6.3	資訊安全認知及教育訓練	2
8.1	使用者端點裝置	2
5.10	可接受使用資訊及其他相關聯資產	1
5.22	供應者服務之監視、審查及變更管理	1
5.32	智慧財產權	1
8.29	開發及驗收中之安全測試	1



114年度本校資安事件統計

項次	事件	通報日期	解決日期	處理作為	備註
1	本校 DNS 伺服器遭 DDoS 攻擊，導致對外網路無法正常運作。	114.02.05	114.02.06	暫時中斷對外線路並請區網中心進行流量清洗。正常運作後，持續監控相關服務。	自行發現
2	OpenSSH 存在高風險安全漏洞。	114.03.06	114.03.10	將 OpenSSH 更新至最新版。	N-ASOC
3	系統使用已知含漏洞之元件。	114.05.21	114.06.05	更新所使用之 Apache、PHP 版本。	HITCON Zeroday
4	測試用虛擬主機設定錯誤，誤掃他校主機。	114.11.28	114.11.28	暫時封鎖該主機的對外網路，確認為設定錯誤，非主機遭非法入侵後即恢復網路。	N-ASOC

資安補給站

㋮當前政府重大資安政策

- 為防範公務及機敏資料遭不當存取，降低國家資通安全風險，行政院已完成各機關「**大陸廠牌資通訊產品（含軟體、硬體及服務）**」以及「**委外營運之公眾活動或使用場地契約**」之全面盤點與風險評估。請各單位確實辦理後續改善與管控措施。
- 針對盤點結果中可能危害國家資通安全之產品，各機關於汰換前應採取適當配套作為，例如停用或封存設備、不與公務網路介接，或訂定其他必要之管制措施，並將實際使用與控管情形納入年度稽核重點。如設備尚未達使用年限但因資安疑慮須報廢者，得於相關文件中註明原因，採**專案報廢方式**處理。
- 此外，各機關未來辦理採購案時，得依實際需要於採購文件或契約中明訂相

關資安限制，包括禁止使用大陸廠牌資通訊產品、要求執行團隊不得包含陸籍人士等；若涉及雲端服務，亦須特別留意資料存取、備份與備援之實體所在地，避免資料位於或傳輸至大陸（含香港、澳門）地區，以確保資料安全與法規遵循。

- 另各機關自行或**委外營運之公眾活動或使用場地**，亦不得使用危害國家資通安全之產品，並應將相關限制明確納入委外契約或場地使用規定中，以避免後續履約爭議。請各單位共同配合相關規定，持續強化資通安全管理，確保政府資訊與系統之安全與穩定。

㋮電子郵件社交工程簡介

- 社交工程為駭客常用入侵管道，透過電子郵件夾帶惡意程式或連結網址等方式，輔以吸引人之信件主旨及內容，誘使缺乏警戒心的使用者開啟後造成進一步破壞且多有實際入侵成功案例，嚴重損害組織或個人之權益。
- 為何駭客會選用電子郵件社交工程的攻擊手法？早期的網路架構是將組織的伺服器或使用者直接連接到網際網路，駭客直接利用作業系統或伺服器的弱點進行入侵、竊取資料或植入後門程式進行遠端遙控。而現在的組織網路架構上為了避免外部入侵行為，會在組織連外的線路中架設防火牆、入侵偵測系統等設備、或進行網路區隔，以阻絕外部未經授權的存取，使駭客要直接從組織外部進行入侵的困難度提高。因此產生另一種駭客手法，藉由電子郵件所夾帶的惡意程式從組織內部主動連外，將不受防火牆、入侵偵測系統、網路區隔等防護手法的限制。
- 社交工程詐騙電子郵件使用的常見陷阱有三種，包括：
  1. 郵件中的惡意網頁連結，當點擊連結後，將連結到惡意網站、釣魚網站，以竊取使用者端之資料或執行惡意程式。
  2. 直接夾帶惡意程式執行檔，如副檔名為.exe、.com、.scr，或捷徑（副檔名.lnk），此外微軟的文書軟體或 PDF 檔案亦發現被利用來做為惡意檔案。
  3. 利用 HTML 郵件格式在郵件內文中夾帶惡意 ActiveX 程式碼、或遠端圖片下載之程式碼。
- 惡意電子郵件的特徵：惡意電子郵件可能具有下述其中一種特徵或其組合：
  1. 假冒寄件者：駭客會假冒使用者信任的人，讓使用者相信電子郵件的內容，進而去開啟這些附件或超連結，並暗中啟動木馬程式。
  2. 使用讓人感興趣的主題及內容：駭客會使用收信者有興趣的主旨，甚至

會配合目前最熱門的新聞事件，來吸引收信者開啟郵件。

3. 含有惡意程式的附件：駭客在電子郵件附帶一個含有惡意程式的檔案，這個檔案不一定是執行檔，可能是各種類型的應用程式，甚至是壓縮檔。駭客會夾帶任何在應用程式上有弱點的文件檔案類型，並想辦法誘騙使用者開啟附件，藉以啟動安裝木馬程式。
4. 利用零時差攻擊：所謂零時差攻擊係指軟體弱點在沒有任何修補方式之前，所出現的相對應針對該弱點的攻擊行為。弱點可能是各種類型的應用程式（如 Office、Arcobat Reader 等）、收信軟體、網頁瀏覽器軟體。只要使用者開啟了這些含有弱點的程式，就會啟動木馬程式。

- 電子郵件社交工程的防護措施：如上所述，啟用預覽視窗等同於「開啟郵件」，所以除了不要點擊可疑郵件內文中的連結與開啟郵件附檔外，建議在收信軟體中設定下述規則：
  1. 關閉自動下載圖片。
  2. 關閉預覽視窗。
  3. 建議不要設定自動回覆讀信回條。
  4. 可設定以純文字格式讀取郵件。
- 使用電子郵件時，應養成良好習慣：
  1. 檢查是否為假冒之寄件者。
  2. 確認信件內容的真實度。
  3. 不輕易開啟郵件中的超連結以及附件。
  4. 開啟電子郵件的檔案、網頁連結前，確認對應軟體（如 Chrome、Office、壓縮軟體等）都保持在最新的修補狀態。

§ 圖書資訊館網路通訊組溫馨小提醒：

教育部為強化人員資安認知，每年進行教職員工電子郵件社交工程演練。114 年度上半年演練結果：開啟測試信比率 3%，點擊測試信內之連結或附件比率 0%；下半年度演練結果：開啟測試信比率 1%，點擊測試信內之連結或附件比率 0%。均符合教育部開啟率低於 10%（含）、點閱率低於 6%之標準。115 年度演練時程待教育部公告後本館再以電子郵件通知相關人員。

㋮ 2025 年最常見密碼調查報告

科技資訊網站 Comparitech 最新研究揭示，「123456」依然是 2025 年最常用密碼，反映全球網路安全意識仍然薄弱。研究團隊從 2025 年數據洩漏論壇收集超

過 20 億組真實帳戶密碼，分析結果顯示大量用戶仍使用極易被破解的密碼組合。

- 最常用密碼排行榜出爐

  研究顯示，十大最常用密碼包括「123456」、「12345678」、「123456789」、「admin」、「1234」、「Aa123456」、「12345」、「password」、「123」及「1234567890」。其中「123456」出現高達 760 萬次，遠超其他密碼。值得注意的是，遊戲「minecraft」成為第 100 位最常用密碼，出現近 7 萬次，另有 2 萬次使用「Minecraft」大寫形式。排名第 53 位的「India@123」也成為較常見但不太通用的密碼選擇。

- 數字與字母組合成主流弱點

  分析顯示，前 1,000 個最常用密碼中，四分之一完全由數字組成。高達 38.6%密碼包含「123」數字串，另有 2%包含倒序數字「321」。同樣地，3.1%密碼包含字母串「abc」。許多常用密碼由單一字元組成，例如「111111」排名第 18 位，「****」排名第 35 位。

  常見單字與片語同樣構成重大安全漏洞。前 1,000 個最常用密碼中，3.9%包含「pass」或「password」變體，2.7%包含「admin」變體，1.6%包含「qwerty」字串，1% 包含「welcome」一詞。這些易於猜測的組合讓駭客能輕易突破帳戶防護。

- 密碼長度普遍不足

  專家普遍建議密碼長度至少 12 個字元，增加長度能大幅降低被破解機會。然而研究發現，65.8%密碼少於 12 個字元，6.9%更少於 8 個字元，僅 3.2%使用 16 個或以上字元。排名第 9 最常用密碼「123」僅含 3 個數字，第 5 位的「1234」也只有 4 個字元。

- 弱密碼帶來重大安全風險

  現代密碼破解程式能輕易破解弱密碼，常見密碼容易被猜中，短密碼則容易遭暴力破解。相對地，強密碼幾乎不可能被破解。強密碼至少 12 個字元長，結合大小寫字母、數字和符號，並具備足夠隨機性避免可識別模式。網路安全專家現時建議密碼長度至少 14-16 個字元，以應對日益進步的破解技術。

【本文摘自：TechNews 科技新報】

§圖書資訊館應用系統組溫馨小提醒：

為維護個人的資訊安全，強烈建議使用者在第一次登錄時務必立即更改預設密碼，並定期進行更換，且避免重複使用相同的密碼與記錄密碼功能。密碼長度至少 8 碼以上，並參雜數字、大小寫英文字母，儘量不要使用易猜測或公開資訊。