季別	類型	錯誤行為態樣	處理建議
113Q1	物聯網 設備安全性	機關(單位)使用的網路攝影機(監控攝影機)因未定期進行安全性更新導致遭駭客入侵執行挖礦連線。	單位的網路攝影機等物聯網設備應禁止使用出廠預設之帳號密碼，並定期確認設備韌體版本是否有對應安全性修補更新。
113Q4	物聯網 設備安全性	機關(單位)IP分享器因配置不當導致遭駭客入侵。	1. 建議IP分享器應定期檢查其韌體版本更新，並確認其如「DMZ指向外網功能」等相關配置設定是否有關閉。 2.另分享器帳號登入密碼應禁止使用預設密碼。 3.應建立相關防火牆及防毒軟體資源。
113Q2	資通系統 安全性	於Google Hacking上發現單位網站上存在含有機敏個資檔案。	若網站有提供檔案上傳功能應加入檔案內容審查機制，若其檔案資料有包含敏感個人資料應做去識別化處理。
113Q2	資通系統 安全性	機關(單位)網頁主機遭外部攻擊者透過特定網頁開發語言CVE弱點進行探測攻擊。	網站若使用的網頁開發語言有遭揭露高風險弱點(CVE>7)應請網頁維護人員(或廠商)僅速進行修補，並於確認修補完成之前改以靜態網頁或先行下架。
113Q2	網路架構 安全性	機關(單位)系統運行之儀表板網頁暴露於公開網路。	機關(單位)內部系統運行相關監測網頁非有對外服務必要，應於開發階段即考慮限制外部訪問權限。
113Q3	資通系統 安全性	機關(單位)內部網站開發程式碼版本管控軟體介面暴露在公開網路上。	因版本管控軟體可以直接更改網站系統的程式碼，故應限制其存取來源端的IP，並定期檢視軟體的存讀取權限配置。
113Q3	資通系統 安全性	機關(單位)網站內容遭發現存在例如「民眾費用收據」等含個人資料的檔案。	建議含個人資料檔案在執行轉檔前就應先進行去識別化處理，避免直接在原始檔案上透過疊圖層等方式進行，此舉可能導致當圖層被移除後一樣可看到被遮蔽之資料。
113Q3	資通系統 安全性	機關(單位)網站上遭發現系統操作手冊存有個資的內容。	1. 檔案上架前，需詳細檢視檔案內容。 2. 若為其他機關所提供之操作手冊，建議改以URL連結方式提供，以避免資料喪失正確性。
113Q3	資通系統 安全性	單位網址列的參數存在SQL注入的漏洞	建議網站系統應定期執行弱掃滲透等資安檢測，並應導入WAF等資安設備之防護。
113Q1	網路架構 安全性	機關(單位)主機例如「醫療設備主機」遭境外IP嘗試遠端桌面登入。	1. 主機(伺服器)應導入防火牆等資安防護資源。 2. 機關(單位)應限制外部存取IP，以防止非法來源。
113Q1	網路架構 安全性	機關(單位)主機或個人電腦有異常連線挖礦行為。	公務主機及個人電腦應避免訪問或執行非公務相關之網站或程式。
113Q2	網路架構 安全性	機關(單位)網路設備的Admin登入介面暴露在公開網路，讓外部攻擊者可以直接做登入嘗試。	機關(單位)之網路設備若非必要應關閉Admin登入介面或是限制外部存取權限，以避免導致該設備成為駭客攻擊之跳板。
113Q4	資通系統 安全性	機關(單位)網站因存在安裝二張以上網路卡導致遭駭客入侵。	1. 主機如有外部遠端維運連線需求應透過防火牆限制存取來源。 2. 禁止使用安裝雙網卡方式直接從外網存取到單位內部系統。
113Q1	網路 惡意活動	同仁使用手機聯結電腦頻繁觸發防毒系統偵測病毒告警。	因智慧型手機本身兼具檔案存儲及傳輸功能，故禁止將手機接入到公務電腦避免發生資安事件。
113Q2	網路 惡意活動	公務資訊設備有下載疑似殭屍網路等相關駭客工具。	公務資訊設備應由負責同仁或維護廠商定期進行維護同時確認安全性更新，若設備或軟體已達EOS，則應停止使用並予以下架。