0729 資安事件簿

Category	會議紀錄

資訊安全事件處理紀錄 (2025年7月)

編號	SLA 等級	資安事件內容	權責單位
SEC-INC-202507-001	P4	使用者詢問如何設定 M365 多因子驗證 (MFA)。	全球終端服務部 (Field Service)
SEC-INC-202507-002	P4	員工詢問公司可攜帶式裝置的使用規範。	全球終端服務部 (Field Service)
SEC-INC-202507-003	P4	使用者回報收到一封來自「IT 部門」的可疑郵件，請求協助判斷。	全球終端服務部 (Field Service)
SEC-INC-202507-004	P4	新進員工詢問如何申請 VPN 帳號的相關資安問題。	全球終端服務部 (Field Service)
SEC-INC-202507-005	P4	使用者忘記鎖住電腦螢幕，被同事拍照回報。	全球終端服務部 (Field Service)
SEC-INC-202507-006	P4	員工詢問在公共場所使用公司筆電連 Wi-Fi 的安全建議。	全球終端服務部 (Field Service)
SEC-INC-202507-007	P4	使用者請求協助檢查一個從供應商收到的壓縮檔是否安全。	全球終端服務部 (Field Service)
SEC-INC-202507-008	P4	員工回報 Teams 收到不明外部人員的訊息。	協作平台部 (Collaboration)
SEC-INC-202507-009	P4	詢問公司對於使用 USB 隨身碟的政策。	全球終端服務部 (Field Service)

SEC-INC-202507-010	P4	員工請求暫時開放某個被防火牆阻擋的學術研究網站。	網路部 (Network)
SEC-INC-202507-011	P4	使用者回報收到疑似詐騙的快遞通知郵件。	全球終端服務部 (Field Service)
SEC-INC-202507-012	P4	詢問公司密碼原則的具體要求（長度、複雜度）。	全球終端服務部 (Field Service)
SEC-INC-202507-013	P4	員工發現辦公室座位旁的網路孔有多餘的網路線，請求確認。	全球終端服務部 (Field Service)
SEC-INC-202507-014	P4	使用者詢問是否可以安裝某個 Chrome 瀏覽器擴充功能。	全球終端服務部 (Field Service)
SEC-INC-202507-015	P4	回報會議室投影設備上殘留前一位使用者的登入資訊。	全球終端服務部 (Field Service)
SEC-INC-202507-016	P4	員工詢問如何安全地刪除電腦中的敏感檔案。	全球終端服務部 (Field Service)
SEC-INC-202507-017	P4	使用者回報公司網站的某個頁面憑證顯示為不安全。	網路部 (Network)
SEC-INC-202507-018	P4	員工在公司停車場撿到一個來路不明的 USB 隨身碟並上繳。	全球終端服務部 (Field Service)
SEC-INC-202507-019	P4	詢問出差到中國時，使用 VPN 的注意事項。	網路部 (Network)
SEC-INC-202507-020	P4	使用者回報 M365 跳出通知，建議更新密碼。	全球終端服務部 (Field Service)
SEC-INC-202507-021	P4	訪客抱怨訪客用 Wi-Fi 網路速度緩慢。	網路部 (Network)
SEC-INC-202507-022	P4	使用者詢問為何無法存取某個 SharePoint 內的檔案。	協作平台部 (Collaboration)
SEC-INC-202507-023	P4	員工收到冒充 CIO David Chen 的內部郵件，詢問是否正常。	全球終端服務部 (Field Service)
SEC-INC-202507-024	P4	詢問關於電腦螢幕防窺片申請的資安考量。	全球終端服務部 (Field Service)
SEC-INC-202507-025	P4	使用者回報防毒軟體跳出已成功阻擋一個威脅的通知。	全球終端服務部 (Field Service)
SEC-INC-202507-026	P4	員工詢問在社交媒體上分享公司活動照片的規範。	全球終端服務部 (Field Service)

SEC-INC-202507-027	P4	回報辦公室印表機上有多份未取走的文件。	全球終端服務部 (Field Service)
SEC-INC-202507-028	P4	使用者詢問為何無法登入測試環境的 ERP 系統。	伺服器部 (Server)
SEC-INC-202507-029	P4	員工收到 LinkedIn 通知，有不明人士聲稱是同事。	全球終端服務部 (Field Service)
SEC-INC-202507-030	P4	請求協助判斷一封來自合作夥伴的加密郵件如何開啟。	全球終端服務部 (Field Service)
SEC-INC-202507-031	P4	回報某個內部系統的網頁連結已失效。	全球終端服務部 (Field Service)
SEC-INC-202507-032	P4	員工詢問公司是否有提供公開的 PGP 金鑰。	協作平台部 (Collaboration)
SEC-INC-202507-033	P4	使用者回報電腦時間與標準時間有幾分鐘的誤差。	全球終端服務部 (Field Service)
SEC-INC-202507-034	P4	詢問下班後是否需要將電腦關機。	全球終端服務部 (Field Service)
SEC-INC-202507-035	P4	員工回報在網路上看到疑似公司的內部文件。	全球終端服務部 (Field Service)
SEC-INC-202507-036	P4	使用者詢問是否可以在公司電腦上使用個人的雲端硬碟。	全球終端服務部 (Field Service)
SEC-INC-202507-037	P4	員工回報其電腦的攝影機指示燈在沒有開啟應用的情況下亮起。	全球終端服務部 (Field Service)
SEC-INC-202507-038	P4	詢問如何辨識釣魚網站的 URL。	全球終端服務部 (Field Service)
SEC-INC-202507-039	P4	回報一個常用的內部網站突然變成英文介面。	全球終端服務部 (Field Service)
SEC-INC-202507-040	P4	使用者詢問為何一個正常的 email 會被系統歸類到垃圾郵件。	協作平台部 (Collaboration)
SEC-INC-202507-041	P4	員工想要申請一個高權限的本地管理員帳號。	全球終端服務部 (Field Service)
SEC-INC-202507-042	P4	回報公司外部訪客Wi-Fi密碼已過期。	網路部 (Network)

SEC-INC-202507-043	P4	員工詢問如何安全地使用手機上的公司 Teams app。	協作平台部 (Collaboration)
SEC-INC-202507-044	P4	使用者回報其電腦的防毒軟體正在進行全機掃描。	全球終端服務部 (Field Service)
SEC-INC-202507-045	P4	員工詢問是否可以將公司淘汰的舊螢幕帶回家。	全球終단服務部 (Field Service)
SEC-INC-202507-046	P3	採購部員工電腦偵測到惡意廣告軟體 (Adware)，已透過防毒軟體隔離。	全球終端服務部 (Field Service)
SEC-INC-202507-047	P3	某員工的 M365 帳號因在不同地點嘗試登入次數過多而遭鎖定。	協作平台部 (Collaboration)
SEC-INC-202507-048	P3	台灣廠區某台公用電腦被發現安裝了未經授權的加密貨幣挖礦軟體。	全球終端服務部 (Field Service)
SEC-INC-202507-049	P3	防火牆日誌顯示，某員工 IP 在凌晨三點持續嘗試連線至遊戲伺服器。	網路部 (Network)
SEC-INC-202507-050	P3	使用者回報點擊了釣魚郵件連結並輸入了密碼，但立即意識到問題。	全球終端服務部 (Field Service)
SEC-INC-202507-051	P3	產線一台用於資料輸入的 PC 防毒軟體過期未更新，且無法手動更新。	全球終端服務部 (Field Service)
SEC-INC-202507-052	P3	IT 資產盤點時發現一台未登記的無線 AP，正在發送訊號。	網路部 & 全球終端服務部
SEC-INC-202507-053	P3	某研發人員被發現在 SharePoint 網站為整個部門資料夾設定了對外匿名分享。	協作平台部 (Collaboration)
SEC-INC-202507-054	P3	伺服器日誌顯示，某離職員工帳號在禁用後仍有來自外部IP的登入嘗試。	伺服器部 (Server)
SEC-INC-202507-055	P3	使用者將含有客戶個資的檔案用個人的 Email 寄出，被 DLP 系統攔截。	協作平台部 (Collaboration)

SEC-INC-202507-056	P3	防毒系統主控台顯示，某個部門的電腦有五台以上未更新病毒碼。	全球終端服務部 (Field Service)
SEC-INC-202507-057	P3	網路部發現一個廠區的網路攝影機使用原廠預設密碼。	網路部 (Network)
SEC-INC-202507-058	P3	一位員工回報其電腦不斷跳出廣告視窗，疑似中毒。	全球終端服務部 (Field Service)
SEC-INC-202507-059	P3	資料庫稽核發現某應用系統服務帳號有異常的資料查詢行為。	資料庫部 (DB)
SEC-INC-202507-060	P3	發現一台測試用的網頁伺服器對外開放，且含有敏感的測試資料。	伺服器部 (Server)
SEC-INC-202507-061	P3	員工使用公司電腦操作加密貨幣交易，違反使用規定。	全球終端服務部 (Field Service)
SEC-INC-202507-062	P3	某台 Linux 伺服器被發現有異常的排程工作。	伺服器部 (Server)
SEC-INC-202507-063	P3	稽核發現某位員工同時擁有 ERP 系統中“申請”與“核准”的衝突權限。	應用系統組 (假設) & 資料庫部
SEC-INC-202507-064	P3	某業務主管回報其手機上的公司 Teams app 無法登入。	協作平台部 (Collaboration)
SEC-INC-202507-065	P3	產線HMI（人機介面）被發現插入了未經許可的USB隨身碟。	全球終端服務部 (Field Service)
SEC-INC-202507-066	P3	發現某台測試伺服器未及時安裝 Windows 重大安全補丁。	伺服器部 (Server)
SEC-INC-202507-067	P3	員工試圖從公司網路下載一個被資安軟體標記為惡意的檔案。	網路部 (Network)
SEC-INC-202507-068	P3	某個 SharePoint 網站因為流量過大而變得緩慢，疑似被濫用。	協作平台部 (Collaboration)
SEC-INC-202507-069	P3	Power BI 儀表板權限設定錯誤，讓非主管職看到敏感的銷售數據。	協作平台部 (Collaboration)
SEC-INC-202507-070	P3	某台VMware ESXi 主機的管理介面被發現暴露在公網。	伺服器部 (Server)

SEC-INC-202507-071	P3	一位使用者回報，他的電腦檔案被加上了奇怪的副檔名，但檔案仍可開啟。	全球終端服務部 (Field Service)
SEC-INC-202507-072	P3	網路掃描發現有員工私自架設 Wi-Fi 熱點。	網路部 (Network)
SEC-INC-202507-073	P3	伺服器備份日誌顯示某台檔案伺服器的備份已有數次不完整。	伺服器部 (Server)
SEC-INC-202507-074	P3	廠商在遠端維護時，被發現使用了不安全的連線方式 (Telnet)。	網路部 (Network)
SEC-INC-202507-075	P3	某員工的電腦被發現持續向一個已知的 C&C 中繼站發送網路信標。	全球終端服務部 & 網路部
SEC-INC-202507-076	P3	Active Directory 中發現一個名稱可疑、久未登入的管理員帳號。	伺服器部 (Server)
SEC-INC-202507-077	P3	發現一個公用資料夾的權限被設定為 "Everyone" 可修改。	伺服器部 (Server)
SEC-INC-202507-078	P3	員工回報在廠區撿到一張寫有帳號密碼的便條紙。	全球終端服務部 (Field Service)
SEC-INC-202507-079	P3	弱點掃描發現一台網管設備存在中度風險的漏洞。	網路部 (Network)
SEC-INC-202507-080	P3	員工回報一封要求提供個人資料的內部問卷調查，未經公告。	全球終端服務部 (Field Service)
SEC-INC-202507-081	P2	偵測到來自研發部門檔案伺服器的異常大量外連流量至可疑雲端儲存IP。	緊急應變中心 (QRC) (監控) & 網路部 (主導)
SEC-INC-202507-082	P2	財務部經理回報其 M365 帳號被盜用，有來自海外的異常登入，並已發送郵件。	緊急應變中心 (QRC) (監控) & 協作平台部 (主導)
SEC-INC-202507-083	P2	防毒系統回報，德國廠區的物料管理伺服器偵測到潛在的勒索軟體前導木馬。	緊急應變中心 (QRC) (監控) & 伺服器部 (主導)
SEC-INC-202507-084	P2	多位使用者回報收到來自人資部門主管的內部釣魚郵件，要求更新薪資資料。	緊急應變中心 (QRC) (監控) & 協作平台部 (主導)

SEC-INC-202507-085	P2	資料庫稽核日誌顯示，某服務帳號在凌晨三點大量讀取客戶聯絡資料。	緊急應變中心 (QRC) (監控) & 資料庫部 (主導)
SEC-INC-202507-086	P2	網路部偵測到來自墨西哥廠區 OT 網路對 IT 網路的異常連接埠掃描行為。	緊急應變中心 (QRC) (監控) & 網路部 (主導)
SEC-INC-202507-087	P2	一位研發高階主管的筆記型電腦在出差時遺失。	緊急應變中心 (QRC) (監控) & 全球終端服務部 (主導)
SEC-INC-202507-088	P2	VPN 系統存在一個已知的遠端執行漏洞 (RCE)，需要緊急更新。	網路部 (Network) & QRC
SEC-INC-202507-089	P2	SharePoint 網站權限設定錯誤，導致標示為「高機密」的研發文件可被全公司讀取。	協作平台部 (Collaboration) & QRC
SEC-INC-202507-090	P2	核心交換器日誌顯示有大量偽造的 ARP 封包，疑似內部網路有設備中毒發動攻擊。	網路部 (Network) & QRC
SEC-INC-202507-091	P2	外部安全機構通報，公司有一個對外 IP 正在參與殭屍網路的 DDoS 攻擊。	網路部 (Network) & QRC
SEC-INC-202507-092	P2	廠區監控系統拍到有未授權人員嘗試尾隨進入資料機房。	全球終端服務部 (Field Service) & QRC
SEC-INC-202507-093	P2	Active Directory 主網域控制器 (DC) 意外關機，導致部分服務驗證失敗。	伺服器部 (Server) & QRC
SEC-INC-202507-094	P2	開發團隊回報，公司對外網站的某個API存在SQL Injection風險。	應用系統組 (假設) & 資料庫部
SEC-INC-202507-095	P2	伺服器主機板管理晶片(BMC)被發現使用預設密碼且暴露在管理網段。	伺服器部 (Server) & QRC
SEC-INC-202507-096	P1	**MES 系統遭勒索軟體攻擊，導致台灣廠區三條產線全面停工。**	**緊急應變中心 (QRC) 指揮 (全體技術團隊協同處理)**

SEC-INC-202507-097	P1	**偵測到勒索軟體在公司主要檔案伺服器上橫向移動，影響全公司檔案存取。**	**緊急應變中心 (QRC) 指揮 (全體技術團隊協同處理)**
SEC-INC-202507-098	P1	**公司對外網站遭置換內容 (Defacement)，並被發現有 SQL Injection 漏洞，客戶資料庫有外洩風險。**	**緊急應變中心 (QRC) 指揮 (應用/網路/資料庫部協同處理)**
SEC-INC-202507-099	P1	**CIO 的 M365 帳號遭魚叉式網路釣魚攻擊攻陷，攻擊者正在對高階主管發送詐騙郵件。**	**緊急應變中心 (QRC) 指揮 (協作平台/網路部協同處理)**
SEC-INC-202507-100	P1	**核心 ERP 資料庫伺服器出現硬體故障且備援未自動啟動，導致全球訂單與財務系統中斷。**	**緊急應變中心 (QRC) 指揮 (伺服器/資料庫部協同處理)**