苗栗縣銅鑼鄉鎮公所

111 年度安全維護專報

「資訊產品安全使用注意事項」

一、前言

回顧世界經濟論壇(World Economic Forum， WEF)2018~2021 連續四年的「全球風險報告」(The Global Risks Report)，針對全球主要風險發生可能性、衝擊性進行評估，從 2018~2020 以網路攻擊(Cyber attack)、數據詐騙竊盜(Data fraud or theft)為風險評估事件，到 2021 年則改以資訊基礎設施故障(IT infrastructure breakdown)、網路安全防護弱點(Cybersecurity failure)為風險評估事件，除知悉網路安全乃係全球性關注的風險重點，更可一窺全球對網路安全從針對外部駭客的攻擊角度分析，移轉為強調使用者自身的安全防護。不期待資訊網路世界無惡意侵害行為，而是聚焦在網路資訊使用者自身軟、硬體面的安全防護完整度。

日前有報導烏俄戰爭中，有烏國士兵使用中國製無人機後，旋即遭精準砲擊的新聞，顯見各項電子設備均有其安全性隱憂。

二、資訊設備使用安全注意事項

以下整理一般日常資訊安全注意事項，請同仁注意並落實

(一)處理公務應使用機關提供之資訊設備、網路，及規定之軟體，勿任意安裝不明軟體、連結不明網站或開啟不明電子郵件，以免感染電腦病毒、木馬或惡意程式。

(二)作業系統應經常更新，修補程式漏洞，避免被駭客攻擊(例如：勒索病毒)。

(三)個人電腦應安裝掃毒軟體，定期更新病毒碼，防堵可能中毒的網路管道，隨身碟或外接式硬碟等儲存設備，放入電腦讀取前應先進行

掃毒再使用。

(四)公務資料應定期備份，可以在中毒或遭受攻擊時將損失風險降到最低。

(五)不使用公務電子信箱帳號登記做為非公務網站的帳號，如社群網站、電商服務等。

(六)公務資料傳遞及聯繫應使用公務電子郵件帳號，不使用非公務電子郵件傳送或討論公務訊息。

(七)應注意不使用即時通訊軟體傳送帳號、密碼或公務敏感資料。傳送公務資訊或個人資料等，應有適當保護，例如加密傳送。

(八)帳號密碼必須妥善保存，並遵守機關規定，密碼設定應注重複雜度，禁止使用與帳號名稱相同、身分證字號、學校代碼、易猜測之弱密碼，亦不可使用廠商預設密碼或其他公開資訊，如有外洩疑慮，除了儘速更換密碼外，應通報資安窗口。

(九)委外辦理資通系統時,應將資通系統依防護基準要求之安全需求,明定委外契約，並於上線前落實安全檢測。

(十)資通系統存取控制，應採最小權限原則，非業務需要，不得提供授權。

(十一)有資安疑慮或異常時，應即時通報資安窗口。

(十二)公務 3C 資訊設備禁止使用中國產品，個人 3C 資訊設備亦宜排除使用。

二、結語

鑒於兩岸之特殊政治關係，資安議題即屬國安議題，尤其中國製造資通產品「後門技術」晶片隱憂揮之不去。透過滾動調整安全防護計畫，明確緊急應變程序，於軟硬體之安全均同等重視，有效加強資安防護能量。