115年春節期間資通安全注意事項

115年春節連假將至，為確保各機關資安作業持續穩定運作，請各機關預為規劃並配合下列事項：

一、年節前：確認聯絡管道、防禦措施及盤點應處資源

(一)確保「找得到人」：通報管道與資源盤點

1. 確立機關緊急聯繫及通報管道：建立聯絡人及代理人清冊，明列市話、手機號碼及其他有效得以快速聯繫方式，並確認春節期間相關人員易於取得清冊。
2. 確認機關資安事件應處相關人員皆可正常登入「國家資通安全通報應變網站」(https://www.ncert.nat.gov.tw)：包含需確認所有通報人員及資安長聯繫資訊，於春節前確認手機與 Email 的有效性。
3. 應變資源規劃：盤點機關資安資源(如廠商支援合約、備品等)，並確立緊急聯繫群組與應處流程，確保發生資安事件時能「找得到人、調得到資源」。

(二)強化「進不來」的防護力：減少受攻擊目標與加強監控

1. 最小化受攻擊面：盤點並關閉春節期間不需要運作之資訊系統及測試環境、電腦、物聯網設備及電子看板等，減少攻擊目標。
2. 遠端與權限管控：清查特權帳號，落實「最小權限原則」；關閉非必要 VPN，採「原則禁止、例外允許」方式管控。
3. 流量與弱點防禦：測試流量監控與 DDoS 攻擊應處機制；完成高風險漏洞修補並更新防毒特徵碼，檢視系統及應用程式更新紀錄。
4. 機敏資料守護：確保機敏資料已有保護機制。

(三)做好「救得回」的最後防線

1. 備份資料有採用離線備份存放。
2. 測試備份資料還原可行性與完整性。

(四)宣導「不點進去」的資安意識

春節期間賀歲聯繫頻繁，為減少駭客入侵管道，提醒同仁留意長假

前後之電子郵件、簡訊及即時通訊軟體使用安全，確認來源正確性，不開啟不明附檔或連結。

二、年節時：落實監控與即時應處

（一）**「變動看得見」：異常監控**

1. 完整性監控：持續偵測網站內容、程式碼是否遭未經授權變更（如惡意貼文、置換網頁）。若遭竄改，應具備切換至靜態網頁（或備援頁面）的機制。
2. 可用性監控：監測系統服務是否異常中斷、流量異常或快速增加（預防 DDoS 攻擊）。
3. 異常行為監控：監控是否有異常時段的登入嘗試、特權帳號變動或不明的大量資料傳輸行為。

（二）**「告警接得到」：預警及應處**

確保告警即時通知（如手機簡訊、通訊軟體群組）功能正常；發生告警時應立即判定風險等級，若確認為資安事件，應即循資通安全管理法及機關事件通報應變程序（SOP）處理而非等到收假才處理。

（三）**「看板關得掉」：公共看板安全**

若發現或得知公共電子看板播放異常或系統入侵跡象，應「先斷網、後檢查」，立即停止播放。

（四）**「通報依法報」：事件通報程序**

如發生資安事件，應依資通安全管理法時限要求，立即至「國家資通安全通報應變網站」辦理通報。

三、年節後：成效分析與評估

檢視分析日誌：分析假期中相關資安監控日誌、發生的告警或資安事件，評估現行應變程序的及時性與有效性，並檢討春節期間內、外部聯繫之順暢度，修訂緊急聯絡名單。