11108 警戒專案資安處理參考指引

一、 事前

(一) **破口盤點及建立應處機制**：盤點機關本身及所屬之資安破口樣態，預規劃有效防堵破口之因應及應變作為。

(二) **專人 24 小時監測**：

1. 指派專人 24 小時排班及盤點資通系統應處聯繫對口，建立即時溝通管道，強化巡檢及緊急應處。
2. 資安長應親自操兵指揮，並負起全部責任。

(三) **重要活動加強警戒**：如涉及總統府、行政院長官或相關重要人士出席之場域，加強巡檢相關資通訊設備、電子看板、網站及系統服務等，提高警覺，避免有心人士介入干擾。

(四) **社交工程郵件**：

1. 加強宣導同仁提高對郵件點閱之警覺性，先研判郵件真偽。
2. 不開啟來路不明或可疑的電子郵件及附加檔案、不連結及登入未經確認之網站。

二、 事中

(一) 即時通報：

1. 一旦遭遇資安攻擊，務必在最短時間循機制通報，10 分鐘內另以即時溝通管道通報，並回報處理情形。
2. 資安事件如非屬駭侵事件(如為設備故障)，應於 2 小時內向媒體澄清，避免社會大眾誤解。

(二) 以 1 小時內復原為目標，處理建議如下：

1. **DDoS(分散式阻斷攻擊)**：

(1) 評估先阻擋境外 IP，並備妥流量清洗機制，加強監控即時導流。

(2) GSN(政府網際服務網路)如偵測發現，亦會協助先行導流。

(3) 如提升流量清洗量能，遭遇問題時，請洽資安處協請中華電信即時支援排除。

2. **網頁遭置換**：

(1) 於 10 分鐘內切換為備用之靜態服務畫面，並檢測修補弱點及備妥因應作法。

(2) 確認系統及資料備份正確性，備份資料應異地存放。

3. 同仁如誤點擊可疑郵件，請立即通報資安人員協助檢視研判處理。

4. **跡證保存**：與事件相關之設備檔案內容、系統及連線等日誌紀錄，應先予保存，供後續鑑識使用。

三、 事後

(一) **破口補強作業**：因應攻擊發現之缺口，檢討內部作業程序及範圍，儘速予以補強改善。

1. 如大陸廠牌資通訊產品盤點，易遺漏操作硬體所使用的軟體系統。

2. 場地租借者(如廣告推播)之資安管理要求等。

(二) **溯源強化**：將事件跡證資料送鑑識分析，找出可能的駭侵途徑及其他潛在問題，進行清除及補強，並檢討整體作業流程及管制，避免類似肇因再發生。