壹、 說明:

一、公司的電腦設備分為一般辦公室(OA)與程控儀電(OT)使用。OA 電腦：均有安裝防毒軟體之裝置，並定期部署安全性更新；OT 電腦：基於生產設備之軟硬體運作優先為考量，部份電腦不安裝防毒軟體、不接安裝更新套件，以維持系統穩定運作。

二、為防止因電腦中毒後影響公司之業務正常運作，訂定電腦設備發生中毒後處置 SOP。

貳、 常見電腦中毒後異常狀況處置：

當電腦有異狀或觸發病毒警訊時，使用同仁應採取判斷與處置方式，爭取時效以降低、避免病毒擴散情事發生。依以下列三步驟處置：

1. 確認電腦異常狀況，參考如：當機、自行關機、自行重開機、程式執行異常異常訊息…等狀況。
2. 後續處理方式：斷網(拔除網路線)、關機。
3. 通報：確認電腦管控單位(一般辦公室 OA、程控儀電類 OT)聯繫相關資訊人員等處置方式。

附表一、電腦未安裝防毒軟體常見異常情形

裝置異常狀態描述	建議處理方式
裝置無故關機 裝置經重開機後無法進入系統	直接通報直屬主管，直屬主管無法處置時依電腦管轄單位通報相關資訊人。
裝置異常行為(如：開啟某程式、檔案、網頁連結)後當機無回應	(1) 先重新開機。 (2) 重新開機後，狀況若無改善，直接通報直屬主管，直屬主管無法處置時依電腦管轄單位通報相關資訊人。
裝置突然間不受控制 裝置有陌生應用程式無緣無故被執行、陌生網頁異常跳出 裝置執行應用程式、網頁後效能異常緩慢 裝置上網點選陌生網頁後便有異常行為出現	直接通報直屬主管，直屬主管無法處置時依電腦管轄單位通報相關資訊人。
裝置突然網路不通	(1) 先判斷是否為實體線路問題。 (2) 如非網路問題，則直接通報直屬主管，直屬主管無法處置時依電腦管轄單位通報相關資訊人。
接獲其他同仁反映自己郵件帳號異常發送信件	(1) 直接通報直屬主管，直屬主管無法處置時依電腦管轄單位通報相關資訊人。 (2) 疑似、防毒軟體明確判斷為病毒行為時，有擴散、干擾到其他裝置時，請直接斷網處理(拔除網路線)或關機。

未安裝防毒軟體之電腦，一旦有感染病毒跡象時，判斷依據較為模糊，亦較需要專案人員介入協助。所以當異常行為發生時，應立即向上反映，請求資安窗口協助，以免錯失爭取資安事件處理時效。

附表二、常見的防毒軟體警告與處理方式:

病毒警告視窗內容	建議處理方式	
	程控儀電裝置(OT)	辦公室裝置(OA)
隔離 已清除 已封鎖 成功，不需要處理行動 成功發現病毒，無法清除 成功發現病毒，無法清除。 (隔離) 已加密	(1) 僅需檢視確認感染路徑檔案是否已經處理。若無，手動再刪除。 (2) 同 Level 1 或 Level2 之資訊窗口逐級上報，各單位 Level 1 資安窗口再向 Level 2 Y6Px 資安窗口回報。	(1) 僅需檢視確認感染路徑檔案是否已經處理。若無，手動再刪除。 (2) 若無法處理時直接通報小港 TEL：2048、總部大樓TEL：22048。
暫不處理 暫不處理潛在的安全威脅 需要進一步處理行動 成功發現病毒，無法清除。(用戶端成功執行了隔離，但無法將隔離的檔案傳送到指定的隔離資料夾)	同 Level 1 或 Level 2之資訊窗口逐級上報，各單位 Level 1 資安窗口再向 Level 2 Y6Px 資安窗口回報。	直接通報小港 TEL：2048、總部大樓 TEL：22048。
警告 - OfficeScan 在中毒用戶端上偵測到安全威脅。請重新啟動端點以完成安全威脅清除程序	(1) 紀錄感染路徑，建議重新開機。 (2) 若重新開機後，感染檔案仍存在，同Level 1 或 Level 2之資訊窗口逐級上報，各單位 Level 1資安窗口再向 Level2 Y6Px 資安窗口回報。	(1) 紀錄感染路徑，建議重新開機 (2) 若重新開機後，感染擋案仍存在，則直接通報小港 TEL：2048、總部大樓 TEL：22048。

有安裝防毒軟體的電腦，因有病毒警訊的協助，可在第一時間透過訊息加以判斷並初步排除問題。資訊系統處(F3)會定期彙整月報表，來檢討相關違規資安事件。而訊息提示無法第一時間處理者(如：無法刪除、無法隔離、暫不處理、病毒爆發等狀態)，請同仁依上述內容立即作處置並通報資訊窗口。

參、後續處理方式

電腦中毒後首要處置動作是斷網(拔除網路線)、關機、通報直屬主管，直屬主管無法處置時依電腦管轄單位通報相關資訊人。

肆、電腦管轄單位之判別

一、 F3 資訊單位主要管轄一般辦公室(OA)電腦，通報電話為小港廠區 2048、總部大樓 22048。

二、 Y6P 電控處單位則管轄程控儀電類(OT)電腦，通報方式： 同 Level 1 或 Level2 之資訊窗口逐級上報，由各單位 Level 1 資安窗口再向 Level 2 Y6Px 資安窗口回報。

三、 判別電腦管控單位方法：

1. 連接程控儀電設備→Y6P。
2. 可以使用EIP　F3
3. EIP 直達路徑 ^DT0H 查詢該電腦固定資產管控單位。