



國立陽明大學

惡意軟體防護管理指引

出版者：國立陽明大學-資訊與通訊中心

文件編號：I-2-009-06

版本編號：6.0

機密等級：一般

文件維護員：楊麗娟

使用本文件前，如對版本有疑問，請與文件維護員確認最新版次。



目錄

壹、	目的.....	4
貳、	適用範圍.....	4
參、	權責.....	4
肆、	相關資料.....	5
伍、	名詞定義.....	6
陸、	作業程序.....	6
柒、	參考文件.....	6



壹、目的

為防範本校之應用軟體及系統不受病毒、木馬或任何形式惡意軟體影響，造成資訊資產的損害或影響業務運作，特制訂本指引。

貳、適用範圍

於國立陽明大學校園內之所有電腦設備使用者。

參、權責

一、系統發展組

(一) 應定期向本校員工進行相關知識及訊息之宣導教育訓練。

(二) 不定期向全體同仁宣導病毒、惡意程式及惡意網站之防範與因應措施。

二、本校全體同仁

(一) 應確認所使用之個人電腦已安裝防毒軟體且定期更新電腦病毒碼，並應定期進行相關系統修補程式，且定期掃描。



- (二) 不任意下載程式、不任意開啟來路不明之電子郵件。
- (三) 不得於所使用之個人電腦中安裝來路不明或非法軟體。
- (四) 勿點選太多與職務無關之網頁，亦不得瀏覽不適當之網站(如賭博或色情網站)。
- (五) 應設定防止自動執行未經授權的行動碼(如：ActiveX等)，且應設定螢幕鎖定。
- (六) 行政資料及備份資訊勿隨意攜出。
- (七) 登入系統使用完應登出。
- (八) 密碼及相關重要資訊勿以便利貼隨意張貼於電腦或桌面上，並遵守本校密碼設定原則(請參考帳號與通行密碼管理程序)。
- (九) 涉個人隱私之資訊(例：公文、委員會委員聯絡資訊等)應妥適放置，勿置於桌上明顯之處，以避免有心人士窺探。
- (十) 使用本校採購之正版軟體，勿使用盜版或來路不明軟體，本校之正版軟體請參閱文件「軟體使用及版權清單」。

肆、相關資料

一、資通安全事件通報/處理紀錄單



伍、名詞定義

無

陸、作業程序

一、本校所有個人電腦、伺服器主機皆應受到防毒機制之保護

如：安裝適當之防毒軟體或以網路安全防毒閘道器等方式進行防護，並定期更新病毒碼，病毒碼必須為最新 7 天內 pattern，防止電腦病毒在網路上擴散。

二、本校採購之正版軟體清單，請參閱本校資訊與通訊中心網站 (<http://icc.web.ym.edu.tw/>) 公佈之最新一覽表。

三、系統發展組應不定期公告目前相關之資訊安全資訊於資安與個資資訊網中 (<http://isms.web.ym.edu.tw>)，以供使用者學習，並採行防範措施。

四、電腦病毒及延伸為資安事件的處理

依「資訊安全事件管理程序」辦理。

柒、參考文件

一、帳號與通行密碼管理程序

二、電子郵件管理指引



三、軟體使用及版權清單

四、資訊安全事件管理程序