大 仁 科 技 大 學
Tajen University

管 制 文 件 訂 修 廢 履 歷 表

文件編號	資訊-程序-24	文件名稱	電腦病毒防範管理程序書
使用部門	圖書資訊館	機密等級	普通

版次	頁數	文件修訂摘要	實施日期
A.0	5	初版	99/05/24

訂修廢者	單位主管	資訊安全長

※管制文件不得擅自塗改及做記號並禁止影印。

1.目的

為促使本校電腦病毒之防治管理、處理流程及注意事項有一明確之規範，以有效杜絕電腦病毒造成之危害，維護整體資訊系統之正常運作，特制定本程序書。

2.適用範圍

凡所有資訊相關設施，如：伺服器主機、軟體、電子郵件及個人電腦檔案等，可能遭受電腦病毒威脅之相關設備，均適用本程序書。

3.參考文件

3.1 資訊-程序-21 可攜式設備與儲存媒體管理程序書。

3.2 資訊-程序-23 資訊安全事件通報及危機處理管理程序書

4.名詞定義

4.1 系統管理者

負責維運與管理所管轄之伺服器主機系統(如：校務行政系統、校網頁系統，DNS 系統....等)，並確保伺服主機系統提供正常之服務。

4.2 防毒系統

安裝於前端使用者(Client)電腦中，具有病毒過濾及防護功能之系統。

4.3 企業防毒管控系統

安裝於後端伺服器主機(Server)中，具有管控、更新病毒碼、派送病毒碼及監控全校防毒系統防護況狀之系統。

4.4 企業防毒管控系統管理者

負責維運與管理企業防毒管控系統，並確保此系統提供正常之運作與防毒服務。

4.5 惡意程式

4.5.1 病毒

病毒是一段電腦程式碼，它會將自身附加到程式或檔案，在

電腦之間傳佈，並在散佈途中感染電腦。病毒可能會損壞使用者的作業系統、軟體、硬體和檔案。

4.5.2 特洛伊木馬程式

特洛伊木馬程式不像電腦病毒一樣會感染其他檔案，特洛伊木馬程式通常都會以一些特殊管道進入使用者的電腦系統中，然後伺機執行其惡意行為（如竊取或刪除檔案、竊取密碼等）。

4.5.3 電腦蠕蟲

蠕蟲（Worm）就像病毒，會透過掌控電腦上可傳輸檔案或資訊的功能自動進行複製。例如，蠕蟲可將它本身的複本傳給電子郵件通訊錄所列出的每個人，該人員的電腦接著會執行相同的動作，從而發生大量網路流量之連鎖效應，進而降低整個企業網路和網際網路的速度。當新的蠕蟲散播時，它們會以極快的速度散佈開來，塞滿網路並可能讓使用者等待兩倍的時間才能檢視網際網路上的網頁。

4.5.4 間諜程式

間諜程式掃瞄並非病毒或惡意的程式碼，而是危及隱私的應用程式，允許駭客在使用者毫無知覺的情況下取得電腦的控制權。它們經常隨著使用者下載想要的應用程式的同時，不知不覺地下載到使用者的電腦上。這些安全威脅包括間諜程式、廣告軟體、惡意撥號程式、惡作劇程式、駭客工具、遠端存取工具、密碼破解應用程式，以及其他未分類的軟體。

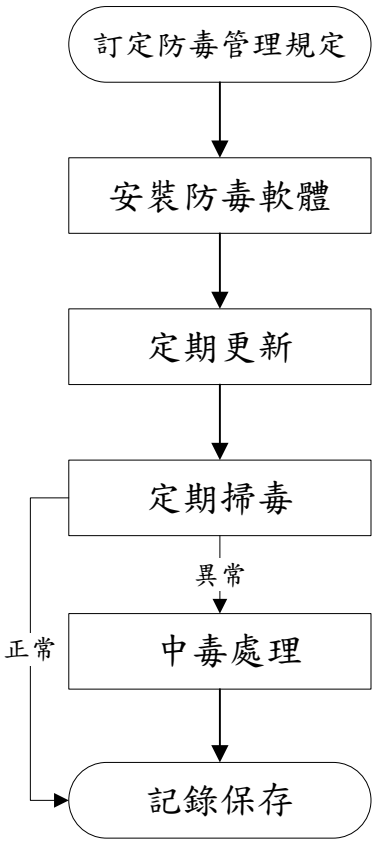
4.6 重大惡意程式感染事件

4.4.1 大範圍個人電腦或伺服主機系統遭受病毒感染。

4.4.2 因中毒造成大規模網路癱瘓。

5.作業內容

5.1 電腦病毒防範管理流程圖

流程	權責	相關文件
	圖書資訊館 系統主機管理者 個人電腦管理者 系統主機管理者 個人電腦使用者 系統主機管理者 個人電腦使用者 系統主機管理者 防毒系統負責人 圖書資訊館	資訊安全事件報告單

5.2 訂定防毒管理規定

5.2.1 使用者如需使用外來的可攜式設備或儲存媒體,必須先進行掃毒的動作，以避免電腦、系統與網路受到惡意程式威脅，可攜式設備與儲存媒體之管理，請依據「資訊-程序-21 可攜式設備與儲存媒體管理程序書」之規定辦理。

5.2.2 系統管理者或個人電腦使用者應使用圖書資訊館所提供之個人電腦防毒系統，自動或定期檢查硬碟及媒體之檔案，確保無電腦病毒潛伏於個人電腦與儲存媒體中。

5.2.3 收取郵件時，若收到來路不明之電子郵件，應立即刪除。

5.2.4 禁止開啟來路不明之檔案或電子郵件及其附加檔案。

5.2.5 系統管理者或個人電腦使用者應將重要資料定期備份。

5.3 安裝防毒軟體

5.3.1 伺服主機與個人電腦須由系統管理者安裝即時防毒軟體。

5.3.2 由圖書資訊館數位學習中心人員負責協助個人電腦使用者安裝最新版本之防毒系統。

5.4 定期更新病毒碼

5.4.1 企業防毒管控系統需由該系統管理者自動與定期更新病毒碼及掃毒程式。

5.4.2 各系統伺服主機與個人電腦需由各系統主機管理者及個人電腦使用者自動或定期執行病毒碼更新作業。

5.5 定期掃毒

5.5.1 各伺服主機與個人電腦應隨時或設定排程執行掃毒作業。

5.6 中毒處理

5.6.1 如遇疑似惡意程式感染情況,防毒系統無法處理或作業仍不正常時，應依據「資訊-程序-23 資訊安全事件通報及危機處理管理程序書」通報圖書資訊館數位學習中心進行報修，並通知相關廠商協助處理。

5.6.2 確認為惡意程式感染事件後，應判斷感染途徑及其惡意程式名稱，並應協助使用者將惡意程式移除或隔離。

5.6.3 當惡意程式無法移除或隔離時，應將電腦關機，並中斷網路連線，如無法短時間內處理，則重新安裝作業系統並利用備份還原資料。

5.6.4 企業防毒管控系統管理者協助使用者處理重大惡意程式感染事件後，應將事件處理情況記錄於「資訊-程序-23-01 資訊安全事件報告單」中，送交圖書資訊館館長審查。

6.附件

6.1 資訊-程序-23-01 資訊安全事件報告單