臺北市政府秘書處資訊化設備使用管理要點

95年2月頒訂

一、本處資訊化設備指個人電腦、手提式電腦、資訊服務站、掌上型電腦等資訊化設備。

二、硬體管理：

1、資訊化設備由使用者及使用單位負責電腦外觀之清理，並隨時保持整潔。

2、本處各種用途之伺服器由使用單位負責保管與維護，各伺服器應使用不斷電設備，以防止供電異常時伺服器資料之流失。

3、含有儲存媒體之設備項目（例如硬碟），使用者應在汰換、維護前詳加檢查，以確保任何機密性、敏感性資料及有版權之軟體已經被移除或有適當之保護。

4、非因公務所需，不得使用攜帶式媒體（如外接式硬碟、攜帶型硬碟、拇指碟、磁帶、光碟片等媒體）或使用燒錄器燒錄。

5、不得擅自改裝本處資訊週邊設備、零件或加裝任何設備或零件。

6、不得擅自攜出本處資訊化設備。

三、軟體管理：

1、應使用有智慧財產權之軟體，並遵守相關法令及契約規定。

2、不得下載、安裝或執行來路不明之軟體。

3、不得使用即時通訊軟體及點對點軟體。

4、不應保有、複製及使用未取得授權之軟體。

5、須在原授權許可外之機器上使用隨機版本之軟體時，應取得正式授權或另行採購。

四、使用者帳號與密碼管理：

1、人事人員應將員工職務異動或到、離（休）職資料通知系統管理人員，俾利新增、修改、刪除該使用者帳號及權限。

2、員工職務異動或到、離（休）職時，系統管理人員應配合人事異動資料儘速變更其系統存取及使用權限。

3、使用者應遵守下列事項：

(1)個人應負責保管密碼，維持密碼之機密性。

(2)應避免將密碼記錄在書面上，或張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所。

(3)當有跡象足以顯示系統及使用者密碼可能遭破解時，應立即更改密碼。

(4)使用系統宜變更系統（包含作業系統及應用系統）預設之帳號與密

碼。

(5) 系統預設之帳號（如 guest）若不需使用，應停用該帳號。

(6) 個人電腦應至少設定三種密碼

a. 基本輸入輸出系統〈ＢＩＯＳ〉開機密碼。

b. 作業系統或網域登入密碼（若有加入網域或使用 Windows XP / 2000 作業系統）。

c. 螢幕保護程式密碼。

(7) 密碼應定期變更（原則上三個月）；且儘量避免重複或循環使用舊的密碼。

(8) 應設定優質密碼，原則上長度最少應由六位長度組成並包含文、數字、符號。

五、 網路資源管理：

1、 員工利用網路使用任何電腦資源，均需恪遵被授權之權限，並確實做到病毒之防治作業。

2、 任何非本處員工因公務需求必須使用本處網路者（例如記者），須經業務單位授權並通知資訊人員後，在授權範圍內使用並存取網路資源。

3、 IP網路位址應由資訊人員統一控管並設定，網路使用者不得自行設定。

4、 網路使用者非必要不得將自己之登入身份識別與登入網路之密碼交付他人使用。

5、 網路使用者請勿以任何儀器設備或軟體工具監聽、擷取網路上之通訊。且不得以任何手段蓄意干擾或妨害網路系統之正常運作。

6、 網路使用者不得將非公務使用之檔案建置在機關網路，亦不得在網路上散播色情文字、圖片、影像、聲音等不法或不當資訊。

六、 電子郵件管理：

1、 本處員工（以下簡稱員工）得申請建立本處電子郵件帳號，由資訊人員設定其使用之空間大小。員工離職時，由人事室通知資訊人員刪除其使用之電子郵件帳號。

2、 不得盜用他人之電子郵件帳號。

3、 發送電子郵件時，應事前檢視該郵件附加之檔案確無夾帶電腦病毒後方可傳送。

4、 機密性公文及資料，不得以電子郵件傳送；敏感性資訊如有電子傳送之必要，應加密處理後方可始得傳送。

5、 網路使用者發送電子郵件時，不得有下列情事：

(1)利用本處網路資源大量發送電子郵件。
(2)發送電子郵件騷擾他人，導致其他使用者之不安與不便。
(3)發送匿名信或偽冒他人名義發送電子郵件。
(4)發送廣告信或商業行為信函。

七、 電腦病毒防範管理：

1、 本處資訊化設備使用之作業系統軟體、辦公室自動化軟體及應用軟體皆應定期更新，有自動化更新功能者並應啟動，以即時修補使用軟體之安全漏洞，防止駭客惡意破壞或入侵。

2、 防毒軟體管理：

(1)各單位保管之伺服器應安裝伺服器防毒軟體。
(2)本處針對使用者端建置個人電腦網路版之防毒架構,對於病毒碼及掃毒引擎之更新、電腦病毒之定期偵測掃描、電腦防毒機制之即時監控等皆由防毒軟體伺服器集中控管。
(3)使用者應隨時注意防毒軟體用戶端之各種顯示狀況,並確定防毒軟體引擎及病毒碼之版本更新，若有異常狀況應隨時回報各單位資訊種子人員，以發揮電腦防毒最大效果。
(4)應啟動個人電腦防毒軟體用戶端郵件掃描之功能。

3、 有關資通安全最新資訊將隨時公布於本處網頁公布欄或以電子郵件通知，同仁應隨時上網查閱並閱讀相關電子郵件。

4、 網路使用者如偵測到電腦病毒入侵或其他惡意軟體，應立即拔除網路線並通知各單位資訊種子人員或本處資訊人員，直到確認病毒已消除後，才可重新連線。

5、 為防止電腦病毒或惡意軟體之入侵，使用者應遵守下列原則：

(1)不任意開啟來路不明之電子郵件或附加檔案。
(2)取消郵件預覽之功能
(3)郵件信箱須設定密碼且不定期更換。使用用戶端軟體收送郵件，取消記憶密碼之功能。
(4)不瀏覽惡意網站。
(5)使用網際網路時，不任意信任網站之安全性並安裝其簽署之程式。
(6)基於智慧財產權及資通安全之責任,不任意下載及安裝使用非正版或來路不明之軟體，請勿使用未取得授權之軟體及檔案。
(7)非因公務所需，不開啟網路資源分享功能（如檔案共享）；因業務關係需開放網路資源分享功能時，請設定為唯讀功能或設定分享密碼。