

臺北市政府員工使用電腦應注意事項修正總說明

臺北市政府員工使用電腦應注意事項自民國一〇三年三月二十日公布生效以來將屆二年多，實施成效良好，惟因本注意事項主要規範四種行為型態：員工通行密碼之管理、電腦安全、電子郵件安全、其他週邊產品；為提升本府同仁對電子郵件之防護觀念，使本注意事項更臻周延，爰擬具本修正草案，修正第貳點「二、員工通行密碼之管理」(二)、第貳點「四、電子郵件安全」(一)及(三)，新增第貳點「四、電子郵件安全」(四)及(五)，其修正及新增注意事項如下：

- 一、修正「個人應負責保護通行密碼，維持通行密碼之機密性。」(新增注意事項第貳點第二項第二款)。
- 二、修正「機密性資料及文件，不得以電子郵件或其他電子方式傳送；機密性資料以外之敏感性、個人隱私資料及文件，如有電子傳送之需要，應以適當之加密或電子簽章等安全措施處理，上述資料及文件除有特殊需求，不宜寄送至私人信箱。」(修正注意事項第貳點第四項第一款)。
- 三、修正「電子郵件宜關閉郵件預覽功能及圖片自動下載功能，且不開啟來路不明之電子郵件附件、網站…等之連結，以免感染惡意程式。」(修正注意事項第貳點第四項第三款)。
- 四、新增「寄送郵件時宜署明寄件者相關身份識別資訊(如：姓名、職稱、服務單位、電話…等)，使收信者易於識別信件來源。」(新增注意事項第貳點第四項第四款)。
- 五、新增「寄出信件給多人時，宜使用「密件副本」進行，避免暴露過多電子郵件帳號。」(新增注意事項第貳點第四項第五款)。

「臺北市政府員工使用電腦應注意事項」修正對照表

105 年 06 月 13 日

修正規定	現行規定	說明
貳、注意事項 二、員工通行密碼之管理 (二) 個人應負責保護通行密碼，維持通行密碼之機密性。	貳、注意事項 二、員工通行密碼之管理 (二) 個人應負責保護通行密碼，維持通行密碼之機密性。	P1 調整用詞一致性，增加文字「密」
貳、注意事項 四、電子郵件安全 (一) 機密性資料及文件，不得以電子郵件或其他電子方式傳送；機密性資料以外之敏感性、個人隱私資料及文件，如有電子傳送之需要，應以適當之加密或電子簽章等安全措施處理， <u>上述資料及文件除有特殊需求，不宜寄送至私人信箱。</u>	貳、注意事項 四、電子郵件安全 (一) 機密性資料及文件，不得以電子郵件或其他電子方式傳送；機密性資料以外之敏感性、個人隱私資料及文件，如有電子傳送之需要，應以適當之加密或電子簽章等安全措施處理。	P2 增加文字內容： 為防止機密性、敏感性、個人隱私資料及文件洩漏，故增加「 <u>上述資料及文件除有特殊需求，不宜寄送至私人信箱。</u> 」。
貳、注意事項 四、電子郵件安全 (三) 電子郵件宜關閉郵件預覽功能及圖片自動下載功能，且不開啟來路不明之電子郵件附件、 <u>網站...等之連結</u> ，以免感染惡意程式。	參、注意事項 四、電子郵件安全 (三) 電子郵件宜關閉郵件預覽功能及圖片自動下載功能，且不開啟來路不明之電子郵件 <u>及其</u> 附件，以免感染惡意程式。	P2 調整文字內容： 1. 因電子郵件寄送訊息多元化，不再只是圖片及附件，故增加網站...等之連結；藉此提高本府同仁對電子郵件傳送訊息之敏感度。 2. 刪除「及其」文字部分。 3. 增加「 <u>、網站...等之連結</u> 」文字部分。
貳、注意事項 四、電子郵件安全 (四) <u>寄送郵件時宜署明寄件者相關身份識別資訊(如：姓名、職稱、服務單位、電話...等)，使收信者易於識別信件來源。</u>	無	P2 新增內容： 現今網站犯罪猖獗，其中網路釣魚手法甚難防範，攻擊者透過電子郵件以利誘、欺騙等手法，為提升本府各機關同仁對於網路釣魚、社交工程等攻擊方式之防護能力，增加此注意事項。
貳、注意事項 四、電子郵件安全 (五) <u>寄出信件給多人時，宜使用「密件副本」進行，避免暴露過多電子郵件帳號。</u>	無	P2 新增內容： 為提升本府同仁對資通安全防護之觀念，藉此提高本府同仁對電子郵件安全相關意識。

臺北市政府員工使用電腦應注意事項

中華民國 103 年 3 月 20 日臺北市政府（103）府授資設字第 10330048700 號函頒。

中華民國 104 年 4 月 13 日臺北市政府（104）府授資設字第 10430055100 號函頒。

中華民國 105 年 6 月 13 日臺北市政府資訊局（105）北市資設字第 10530792400 號函頒。

壹、目的

一、臺北市政府（以下簡稱本府）為確保所屬各機關（以下簡稱各機關）員工正確、安全地操作及使用電腦，特訂定本注意事項。

貳、注意事項

二、員工通行密碼之管理

- （一）員工個人作業電腦應設定通行密碼確實保密。
- （二）個人應負責保護通行密碼，維持通行密碼之機密性。
- （三）通行密碼長度應至少八碼，並取英文字母大小寫、數字與特殊符號其中三種要素之組合。
- （四）通行密碼應每六個月至少更新一次。
- （五）若將通行密碼記錄在書面上，應妥善保管避免外洩，並且不得將密碼張貼在個人電腦、終端機螢幕或其他容易洩漏秘密之場所。
- （六）當有跡象顯示系統及通行密碼可能遭破解時，應立即更改密碼。

三、電腦安全

- （一）電腦之作業系統或應用程式之漏洞應即時更新修補。
- （二）電腦應設定螢幕保護程式於人員未操作電腦十分鐘內啟動，再次使用電腦時，應輸入密碼啟動。
- （三）各機關電腦設備須指定專人管理，非經授權不得任意使用、拆卸及更動週邊設備。
- （四）不得使用未經授權及來路不明之軟硬體。除因公務需要且經權責主管核可外，同仁禁止使用點對點（Peer-to-Peer, P2P）軟體（如 Foxy、ezPeer、eDonkey 等），權責單位應不定期派員檢視稽核。
- （五）員工不得使用即時通訊軟體傳輸公務機密、涉及資訊安全及個人隱私之事項。
- （六）員工個人作業電腦應安裝防毒軟體並定期更新及掃描偵測，防治惡意軟體之侵入。
- （七）員工禁止使用密碼破解、網路竊聽工具軟體，且不得突破他人帳號，中斷系統服務、濫用系統資源，複製非法軟體。

- (八) 員工使用外部取得授權之電腦主機或網路設備，與機關內部網路連線作業時，應確實遵守網路安全規定及連線作業程序。
- (九) 應定期將重要資料備份存放。
- (十) 除非業務所必須，個人電腦應儘量避免儲存個人資料檔案；含有大量個人資料檔案應以密碼或加密措施保護。
- (十一) 在丟棄任何曾經儲存資訊之電子媒介前，應將儲存資訊刪除，並徹底消磁或銷毀至無法解讀之程度。
- (十二) 不得在任何公開之新聞群組、論壇、社群網站或公佈欄中透露任何公務機密相關之細節。
- (十三) 下班時應將個人使用之電腦關機並將可攜式電腦（如筆記型電腦、平板電腦）收妥。

四、電子郵件安全

- (一) 機密性資料及文件，不得以電子郵件或其他電子方式傳送；機密性資料以外之敏感性、個人隱私資料及文件，如有電子傳送之需要，應以適當之加密或電子簽章等安全措施處理，**上述資料及文件除有特殊需求，不宜寄送至私人信箱。**
- (二) 電子郵件附加之檔案，應事前檢視內容無誤後方可傳送。
- (三) 電子郵件宜關閉郵件預覽功能及圖片自動下載功能，且不開啟來路不明之電子郵件附件、**網站...等之連結**，以免感染惡意程式。
- (四) **寄送郵件時宜署明寄件者相關身份識別資訊（如：姓名、職稱、服務單位、電話...等），使收信者易於識別信件來源。**
- (五) **寄出信件給多人時，宜使用「密件副本」進行，避免暴露過多電子郵件帳號。**

五、其他週邊產品

- (一) 使用隨身儲存設備（例如 USB 隨身碟）儲存機密性、敏感性或個人隱私資料時，宜先取得授權並予加密保護。
- (二) 非必要勿使用私人移動式裝置（例如智慧型手機）存取公務資料；如需使用私人移動裝置存取公務資料，應遵守本府資訊安全相關規範。

參、附則

- 六、員工違反本注意事項之規定者，得依人事相關規章議處。