法規名稱：臺北市政府員工使用資通訊裝置應注意事項

修正日期：民國 111 年 07 月 13 日

當次沿革：中華民國 111 年 7 月 13 日臺北市政府（111）府授資安字第 1113008933 號函修正第 4～8、10、12、15 點條文；並自函頒日生效

四、資通訊裝置存取管理，應依下列規定辦理：

（一）資通訊裝置應以設定鎖定機制，如通行密碼、憑證或生物辨識（如：指紋、人臉、瞳孔等）等方式，管理可存取之人員。

（二）員工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）通行密碼應每九十日至少更新一次。

（五）若將通行密碼記錄在書面上，應妥善保管避免外洩，且不得將通行密碼張貼在資通訊裝置、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或有不明存取紀錄時，應立即更改密碼。

（七）各機關及員工應積極防止資通訊裝置遭竊、損毀，並避免誤用、濫用或違法使用，下班時應將資通訊裝置關機並收妥。

（八）資通訊裝置應設定螢幕保護程式或其他保護機制，於未操作十五分鐘內啟動；再次使用資通訊裝置時，應輸入密碼啟動。

（九）資通訊裝置及資通訊系統服務之帳號不得共用，以利鑑別使用者。但情況特殊經使用者之資訊管理單位及系統管理單位同意，並實施補償性控管機制者，不在此限。

（十）各機關之資通訊裝置應指定專人管理，非經授權不得任意使用、拆卸及更動週邊設備。

五、資通訊裝置軟體及網路服務之管理，應依下列規定辦理：

（一）資通訊裝置之作業系統或應用程式之漏洞應即時更新修補。

（二）資通訊裝置應安裝防毒軟體並定期更新及掃描偵測，防制惡意軟體之侵入。

（三）資通訊裝置應安裝來自可信任來源之軟體，於安裝軟體時，應注意該軟體是否要求不必要之權限，且不得破解資通訊裝置之安全措施。除因公務需要且經權責主管核可外，禁止使用下列軟體或工具：

1.點對點（ Peer-to-Peer, P2P）。

2.非本府之虛擬私人網路（ VPN）。

3.遠端遙控，如 RDP、 VNC、teamviewer 或 anydesk 等。

4.影響或大量耗用資通訊裝置及網路資源之軟體，如：挖礦軟體等。

5.禁止使用密碼破解、網路竊聽工具軟體（ Sniffer）或其他駭客工具。

（四）下列軟體及網路服務禁止使用：

1.洋蔥路由器（ Tor）、非法代理伺服器（ Proxy）、加密網域名稱解析服務（DNS over HTTPS）等規避網路管理之機制。

2.有危害國家資通安全疑慮之軟體及網路服務。

3.非法或影響智慧財產權之軟體及網路服務。

4.股票、遊戲或博弈等違反公務紀律之軟體及網路服務。

5.其他本府公告禁止使用之軟體及網路服務。

六、資通訊裝置之網路及其他連線管理，依下列規定辦理：

（一）應確保所使用之網路系統為可信任之網路，禁止使用公開無線 Wi-Fi 網路。

（二）以下功能應保持關閉狀態，需要使用時始得啟用：

1.Wi-Fi 功能。

2.藍牙（ Bluetooth）功能。

3.全球定位（Global Positioning System, GPS）功能。

4.近場通訊（ Near Field Communication, NFC）功能。

（三）參與具機密性會議時，得關閉資通訊裝置之網路連線。

（四）使用外部取得授權之資通訊裝置或網路設備，與機關內部網路連線作業時，應確實遵守臺北市政府網路管理規範。

七、員工電子郵件之使用，依下列規定辦理：

（一）員工不得使用非公務用電子郵件系統進行電子郵件公務訊息及資料交換應用，且針對具公務機密信件不得逕行轉發至非公務信箱。

（二）機密性資料及文件，不得以電子郵件或其他電子方式傳送；機密性資料及文件以外之敏感性、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。

（三）電子郵件附加之檔案，應事前檢視內容無誤後方可傳送。

（四）電子郵件應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及其附件，以免感染惡意程式。

（五）寄送電子郵件時宜署明寄件者相關身分識別資訊，如姓名、職稱、服務單位、電話等，以使收信者易於識別信件來源。

（六）寄送電子郵件給多人時，得使用「密件副本」進行，並得於電子郵件內告知收件者該郵件不顯示收件者相關資訊之說明，避免暴露過多電子郵件帳號。

（七）電子郵件帳號之使用涉及違法或惡意之網路行為（如：散發垃圾郵件、發佈不實謠言及誹謗郵件等），或違反相關規範，經查證屬實者，本府有權終止該電子郵件帳號之使用。

（八）員工查覺電子郵件帳戶或密碼遭人非法使用、破壞、收到異常信件或有任何異常時，應立即通知機關管理者。

（九）非員工個人電子郵件帳號之公務帳號，限以本府員工身分申請，且經核准方得使用；離（調）職並應進行相關移交或變更程序。

八、員工公務資料之使用，依下列規定辦理：

（一）除業務所需外，資通訊裝置應儘量避免儲存私人資料檔案，並保持電腦桌面淨空。

（二）因公務儲存於資通訊裝置內之敏感性、個人隱私資料及文件，應透過安裝或使用內建之加密機制予以防護，並妥善保管加密之金鑰；行動資通訊裝置得安裝或啟動內建具有「可遠端定位並進行資料清除」之資料保護功能。

（三）使用可攜式儲存媒體前，須經防毒軟體掃描確認無風險，且儲存機密性、敏感性或個人隱私資料時，應先取得授權並予加密保護，且妥善保管加密之金鑰，使用完畢應立即刪除。

（四）公務資料如採用線上傳遞，應予以加密，始得傳送；通行密碼應由不同管道另行提供。

（五）應定期將重要資料備份多份存放，其中一份離線備份於不同儲存設備上。

（六）嚴禁將機密或敏感性、個人隱私資料及文件上傳至府外雲端服務平臺儲存或共享；如經主管同意使用府外雲端服務，應透過壓縮加密、帳號多因子認證、存取控制等預防措施保護資料存取安全，確保資料檔案安全。

（七）不得使用任何即時通訊軟體（如：Line、Juiker、 Teams、Telegram、 Skype 等）傳遞臺北市政府文書處理實施要點規範之機密文書等資料（訊）。但使用公務開發之即時通訊軟體者，依該即時通訊軟體使用規定辦理，不受本款之規定限制。

（八）使用即時通訊軟體時，應避免討論重要資訊或交換檔案及加入來歷不明之聯絡人，並應遵守本府訂定之即時通訊軟體相關規定，以防止機關內部之機密或文件資料遭洩漏。

（九）丟棄或捐贈任何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、其他行為規範：

（一）各機關應善用本府網路與其他資通訊資源，不得作非公務或違反公務紀律之使用或有浪費資源等行為。

（二）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。

（三）使用本府公務資通訊裝置及網路應遵循網路禮節，不得有惡意中傷或人身攻訐、謾罵、散佈不實言論之行為，或發表個人政治立場等違反行政中立之情事。

（四）不得在任何公開之即時通訊公開頻道、網路直播、論壇、社群網站或公佈欄中透露任何公務機密相關之細節。

（五）使用本府提供之服務不得有下列不當行為：

1. 發送廣告信件。
2. 以破解、盜用或冒用他人帳號及密碼等方式，未經授權使用網路資源或無故洩露他人帳號及密碼。
3. 利用網路進行犯罪之行為。
4. 無故洩漏個人使用之密碼。
5. 無故洩漏工作上所持有或接觸應保密之資訊。
6. 未經授權變更網路環境設施。
7. 於網路上散佈詐欺、誹謗、侮辱、猥褻、騷擾、非法軟體交易或其他違法之訊息，或蒐集猥褻文字、圖像、影像、聲音等資料。
8. 散佈電腦病毒或其他干擾或破壞系統機能之程式。
9. 非經授權截取網路傳輸訊息。
10. 未經 IP 登記管理人同意而使用他人網路位址。
11. 其他不法或重大不當之行為。

（六）有前款所定不當行為之使用者，本府有拒絕提供服務之權利。

十二、本府提供之各項網路與系統之員工使用軌跡及存放資料，管理單位得因管理需求進行紀錄、稽核、過濾等工作；為確保電子形式軌跡資料之蒐集、處理及利用符合本府資通安全及資訊隱私之規定，各機關因公務需求而有調閱系統使用、查詢軌跡紀錄檔之必要者，應依下列規定提出申請：

（一）各機關因管理資通訊系統所需（如：故障排除、資安稽核、系統效能監控等），得以申請單敘明申請理由，逕向管理單位提出申請。

（二）因非屬前款情形之公務需求申請調閱者，應敘明調閱事由、法源依據及調閱範圍，採公文書以機關全銜發文至管理單位。前開調閱範圍並應以申請調閱事由之必要範圍為限。

管理單位回復前項第二款之申請，應以機關名義為之；其同意提供者，應將該資料加密後，以密件方式提供予申請單位。

十五、本注意事項於各機關員工以外之人員，如：駐點廠商、臨時人員等

，準用之。