屏東縣政府

人員資訊安全守則

1　目的：為定義屏東縣政府（以下簡稱本府）一般人員的資訊安全責任，以維護本府資訊作業環境之機密性、完整性及可用性，特訂定此規範。

2　適用範圍：所有本府人員，及使用本府資訊資源的非本府人員。

3　電腦設備使用規範

3.1 電腦應設定登入密碼，以避免未經授權人員使用。

3.2 電腦應設定為等候 15 分鐘以下自動登出或鎖定作業系統（例如螢幕保護程式、電腦睡眠...等），並要求登入密碼才能繼續使用。

3.3 電腦應設定為自動安裝更新，以即時修補 Windows、Office...等軟體的漏洞。

3.4 電腦應安裝本府專用防毒軟體(OfficeScan)、資產管理軟體(SmartIT)及政府組態基準軟體(GCB doctor)，且不可任意移除或關閉。

3.5 電腦所使用的軟體均須具有合法版權，不可私自安裝來路不明、有違法疑慮或與業務無關的軟體。

3.6 電腦中重要資料應定期備份並妥善保管，避免硬體損壞或其他因素導致資料無法存取。

3.7 除經過授權的管理者外，禁止使用密碼破解軟體或網路掃描/監聽工具。

3.8 禁止借用或盜用他人帳號，或以任何方式使用其他人身分或權限登入系統。

3.9 當有跡象顯示發生資訊安全事件時，應儘速通知資訊管理科人員。

3.10 電腦或可攜式儲存設備報廢前，應先確認儲存的機敏資料已無法解讀(例如以低階格式化、消磁或實體破壞等方式處理電腦硬碟或隨身碟)。

3.11 機敏性資料不宜以電子郵件傳送，如必須使用電子郵件傳輸機敏資料時須經加密處理。

3.12 機敏性資料應妥善保存；若為電子檔案，不得放置於無存取控制的儲存空間，並評估針對個別檔案設定密碼保護。

3.13 為避免受社交工程入侵，點擊電子郵件的附件或連結應謹慎，而不明來源的郵件請勿開啟。

3.14 使用密碼應注意下列要點：

3.14.1 應維持密碼的機密性，若將密碼記錄在書面上，應妥善保管避免外洩，並且不得將密碼張貼於電腦主機、螢幕、辦公桌或其它容易洩漏的場所。

3.14.2 6 個月內須更改一次密碼，並禁止使用相同的密碼。若有跡象顯示密碼可能遭破解時，應立即更改密碼。

3.14.3 密碼長度應為 8 碼以上,且包含英、數字與特殊符號等 3 種以上要素。

3.14.4 如使用預設密碼，必須在第 1 次登入後立即變更。

3.14.5 設置密碼應儘量避免採用易猜測的資訊，例如：

3.14.5.1 個人相關資訊，如電話號碼、出生年月日、身分證字號...等。

3.14.5.2 常用代碼，如機關代碼、電話號碼、員工識別代碼...等。

3.14.5.3 單字或以外觀類似的字元替換，如 password、p@ssw0rd...等。

3.14.5.4 鍵盤上相鄰字元，如!QAZ@WSX、qwerty...等。

3.14.5.5 與帳號完全相同或有部分字元相同。

3.14.5.6 常用弱密碼，如空白、123456、abc123、admin、111111...等。

4 網路使用規範

4.1 本府人員需由 OA 系統線上填寫「帳號申請／異動單」，由單位主管審核後，送資訊管理科確認，始得以公務電腦或設備使用本府網路。

4.2 非本府人員之長期駐府人員如需使用本府網路或其他資訊資源，應由機關首長核准後，再由本府承辦人員代為填寫「帳號申請／異動單」，送資訊管理科確認後，始得發給帳號或開放使用權限，惟使用期限最長 6 個月，屆期需重新進行本項所述流程。

4.3 非本府人員需以非本府設備使用本府網路時，應由本府承辦人員代為填寫「設備連線申請單」送資訊管理科審核，且該設備需經過資訊管理科執行標準處理(例如掃毒、安裝本府專用軟體)後，始得使用該設備連接本府網路，申請日期須依實際需求填寫且至多為 6 個月。

4.4 嚴禁介接私人無線基地台(AP)、IP 分享器或集線器（Hub）等網路設備，違反者得由資訊管理科直接拆除該設備。

4.5 禁止任意更動本府電腦的網路相關設定。

4.6 禁止將本府電腦連接非本府網路，例如私接無線網卡或行動上網設備(例如連接手機行動網路)。

4.7 嚴禁上傳或下載任何侵權或違法的資料或檔案。

4.8 嚴禁瀏覽侵權、賭博、暴力、色情、毒品、駭客...等不當或違法網站。

4.9 嚴禁張貼具誹謗性、猥褻性、騷擾性、機密性、恐嚇、侵權等不當或違法的訊息或資料於聊天室、討論區...等公開的網路空間。

4.10 禁止進行與業務無關的網頁瀏覽、串流影音撥放、檔案傳輸，以避免網路資源消耗，影響本府資訊作業及系統運作效率。

4.11 禁止將機敏性資料上傳至網際網路儲存空間(例如 Google Drive、Dropbox、OneDrive...等)，以避免資料外洩風險。

4.12 禁止安裝點對點互連(P2P)軟體(例如 BT、Foxy、PPS、迅雷、暴風影音、影音先鋒...等)。

4.13 嚴禁任何網路上非正常行為，例如監聽、干擾、偽裝或入侵、攻擊其他設備或系統。

4.14 本府網路資源，如 e-mail 帳號密碼、網頁及網路硬碟空間等，僅限申請人個人執行公務使用，嚴禁轉移予第 3 者。

4.15 各單位如有使用外部的社群網路平台或即時通訊軟體，進行公務推展或聯繫的需求，應由機關首長核准後，填寫「公務社群平台使用登記表」送資訊管理科確認，始得開放使用權限。

5　個人行動裝置使用規範

5.1 個人行動裝置設備係指私人之筆記型電腦、智慧型手機、平板電腦及其他可

攜的處理設備。

5.2 禁止將個人行動裝置連接至本府電腦或設備(例如透過 USB 充電/傳檔、透過行動網路上網)，以防止惡意程式進入府內網路。

5.3 除因業務需要且經權責主管同意外，不得使用個人行動裝置存取公務資料，以避免資料外洩。

5.4 如果因業務需要使用個人行動裝置，必須採取適當的安全措施，相關安全措施如下：

5.4.1 以登入密碼保護行動裝置，且應設定為當行動裝置重新啟動、閒置時自動進入畫面上鎖模式。

5.4.2 只安裝來自於合法的官方軟體商店(如 App Store、Google Play)，下載的軟體，且於安裝軟體時需注意該軟體是否要求不必要的權限。

5.4.3 行動裝置上的軟體或作業系統應定期自動或手動安裝更新修補程式。

5.4.4 建議安裝資安防護軟體（如防毒軟體）。

5.4.5 如有使用雲端備份服務，需謹慎設定與選擇備份的資料項目。

5.4.6 因行動裝置體積小容易遺失，故建議不要儲存機敏資料，如需儲存機敏資料則加密儲存。

5.4.7 不使用任何破解方式(如 Root、刷機等)取得行動裝置上的最高權限。

5.4.8 應謹慎使用簡訊及通訊軟體（如 Line、WhatsApp、WeChat...等），避免遭受社交工程詐騙。

5.4.9 相關連線功能(如 Wi-Fi、藍芽(Bluetooth)、全球定位(GPS)、近場通訊

(NFC)...)只在必要時才開啟，平時應關閉。

人員如未遵守上述規範，必須承擔所有引發的風險及責任，且資訊資源使用權利將受限制或撤銷。