屏東市公所

「資訊安全管理制度」
行動裝置管理作業說明書

機密等級：一般
編　號：ISMS-3-002
版本編號：1.0
發行日期：
使用本文件前,如對版本有疑問,請與資訊安全執行小組確認最新版次。

本文件歷次變更紀錄：

版次	發行日	修訂者	說明	核准者
1.0	109.8.24	資訊安全執行小組	初版文件發行	李英宗

本程序書由資訊安全執行小組負責維護。

目錄：

1 目的

為確保屏東市公所（以下簡稱本所）人員安全使用個人或本所配發之行動裝置，避免機敏資料外洩，特訂定本作業說明。

2 適用範圍

全體人員。

3 權責

3.1 資訊安全執行小組

3.1.1 負責擬定相關資訊安全規範。

3.1.2 負責辦理資訊安全教育訓練相關事宜。

4 名詞定義

4.1 行動裝置：

指具可移動性之處理裝置，如筆記型電腦、智慧型手機、平板電腦及其他可攜之處理設備...等。

5 流程圖

無。

6 作業說明

6.1 除因業務需要，且經權責主管同意外，嚴禁使用行動裝置存取公務資料。

6.2 經核准存取公務資料之行動裝置不得使用未經核准的網路(例如:2G、3G、WiMAX、Hinet WIFI 或 4G 等)進行資料交換，應以經府內申請程序取得帳號之無線網路服務作為資料交換管道。

6.3 無線網路使用

6.3.1 本所員工於使用無線網路服務前需以上網帳號提出申請，經網路管理人員審核確認後，始得使用網路服務。

6.3.2 非本所員工需要使用網路時，需由本所承辦人員代為填寫「設備連線申請單」，經承辦單位主管審核及網路管理人員確認後，該設備使得連接本所網路。

6.4 經核准存取公務資料之行動裝置，應採取適當的安全控制措施，相關控制措施如下：

6.4.1 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。

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

6.4.3 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。

6.4.4 建議安裝資安防護軟體（如防毒軟體）。

6.4.5 如有使用雲端備份服務，需謹慎設定與選擇備份之資料項目。

6.4.6 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。

6.4.7 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。

6.4.8 謹慎使用行動裝置上的通訊軟體（如 Line、WhatsApp、WeChat 等），避免遭受社交工程詐騙。

6.4.9 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。

6.5 私人行動裝置不得連接至本所電腦或設備(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。

7 相關文件

設備連線申請單。