高雄市政府環境保護局資訊安全管理要點

103 年 11 月 19 日高市環局秘字第 10343941300 號函訂定
106 年 3 月 20 日高市環局秘字第 10632344900 號函修正第 16 點

壹、目的

一、為強化本局資訊安全管理，建立安全及可信賴之電子化系統，確保資料、系統、設備及網路之安全，並參酌「行政院及所屬各機關資訊安全管理要點」，特訂定本要點。

貳、組織及權責

二、本局有關資訊安全管理事務依下列分工原則：

(一)資訊安全政策、計畫及技術規範之研議、建置與評估等事項，由秘書室負責辦理。

(二)資料及資訊系統之安全需求研議、使用管理及維護等事項，由使用單位或業務承辦單位負責辦理。

(三)資訊安全教育訓練及宣導事宜由秘書室負責辦理。

(四)資訊機密維護及稽核使用管理事項，由政風室負責辦理。

三、政風室應會同秘書室於每年進行不定期之資訊安全稽核。

四、秘書室應負責資訊安全管理事項之協調及推動工作。

參、人員管理

五、各機關單位對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要之考核；各單位對可存取機密性或敏感性資訊或系統之人員及因工作需要須配賦系統存取特別權限之人員，應加強評估及考核。

六、各機關單位負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，實施人員輪調，建立人力備援制度。

七、資訊作業相關人員離職時，應取消其系統權限，並確實做好電腦軟硬體及相關文件之移交工作。

八、各機關單位業務主管應負責督導所屬員工之資訊作業安全，防範不法及不當

行為。

肆、電腦系統安全管理

九、各機關單位辦理資訊業務委外作業時，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約中，要求廠商遵守及定期考核，並派員監督。

十、各機關單位應依相關法規或契約規定，複製及使用軟體；嚴禁使用非法軟體。

十一、隨身碟使用前應事先做掃毒檢查，或於電腦系統中裝置防毒軟體，以防止感染電腦病毒。

十二、重要系統與資料應備份，並定期掃毒、防堵入侵、避免洩漏與竊取。

伍、網路安全管理

十三、被授權網路使用者(以下簡稱網路使用者)只在授權範圍內存取網路資源。

十四、各機關單位利用網路公佈及流通資訊時，應評估資料安全等級，機密、敏感性或未經當事人同意之個人隱私資料及文件，不得上網公佈。

十五、網路使用者應遵守網路安全規定，並確實瞭解其應負責任；如有違反市府資安預警事件及本局網路安全情事，應依資訊安全規定，限制或撤銷其網路資源存取權利。

十六、為保持公務網路頻寬品質，禁止下載來路不明軟體檔案(如免費試用軟體、娛樂性軟體等)，以免隱藏電腦病毒滲透，並不得瀏覽與業務無關之網站。本局本部以外各機關單位如有違反市府網路流量異常事件(當日流量超過450MB)或本局本部各單位網路每日流量限制(不得逾450MB)，逾越流量限制使用者，單一使用者每月達二次，**得簽奉核准後，於次月封鎖該員網路三個工作天，情節重大者，得提報各該考績委員會懲處。前項受封鎖網路者如有使用網路之必要，得以書面向秘書室釋明並經查證屬實後，得解除一部或全部封鎖之期間。**)。

十七、網路使用者不得將自己的登入身分識別與登入網路密碼交付他人使用。

十八、禁止網路使用者以任何方法竊取他人的登入身分與登入網路密碼。

十九、禁止網路使用者以任何儀器設備或軟體工具竊聽網路上通訊。

二十、禁止網路使用者在網路上取用未經授權檔案、資訊轉售或轉載。

二十一、網路使用者不得將色情檔案建置在本局所屬設施，亦不得在網路上散播電腦病毒、色情文字、色情圖片、色情影像、色情聲音等不法或不當的資訊。

二十二、網路使用者不得以任何手段蓄意干擾或妨害網路系統的正常運作。

二十三、網路使用者除因公務需要且經簽請局長或其授權人員核可會同政風室外，不得使用點對點(Peer-to-Peer，P2P)分享軟體及 LINE 等即時通訊軟體，本局秘書室得不定期派員檢視稽核。

陸、電子郵件使用安全管理

二十四、對來路不明之郵件、附件或免費軟體等，應直接刪除，不得隨便開啟，以免中毒或使網路系統遭破壞。

二十五、機密性之資料及文件，禁止使用電子郵件傳送，以防止洩密。

二十六、禁止發送電子郵件騷擾他人。

二十七、禁止發送匿名郵件或偽造電子郵件。機密性資料以外之敏感性資料及文件，如有電子傳送之需要，各機關單位應視需要以適當加密或電子簽章等安全技術處理。單位業務性質特殊，須利用電子郵件或其他電子方式傳送機密性資料及文件者，得採用權責主管單位認可之加密或電子簽章等安全技術處理。

柒、系統存取控制

二十八、各機關單位對電腦資料庫及檔案應建立分級（機密及安全等級）管理制度。

二十九、各項正式作業之電腦系統作及資料處理，由各權責單位指定專人負責建檔、核對、更新、審查及維護電腦資料之正確性。非經核准不得操作使用或更改已正式作業之系統檔案。

三十、電腦資料庫及檔案，應按不同業務範圍及使用權限，分別設定目錄、識別保護碼；重要或具機密性資料在建檔或提供使用時，應加設通行密碼、使用權限碼，以確保資料安全，且通行密碼應經常更新。

三十一、各機關單位離職、休職、調職人員，應立即取消使用單位內各項資源之所有權限，並列入人員離職、休職、調職之必要手續；人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

三十二、各電腦系統應建立系統使用者註冊管理制度。

三十三、各機關單位之重要資料及系統委外廠商處理者，不論在機關內外執行，均應採取適當及足夠之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

捌、系統發展及維護安全管理

三十四、各機關單位自行開發或委外發展之系統，應在系統初始階段即納入適當之資訊安全機制，加強隱密性、確認性、完整性、不可否認性。系統之維護、更新、上線執行等作業，應予以安全暨版本控制，且應考慮適當之防毒、防駭、防竊、防災(水、火、磁、震、蟲)措施。

三十五、對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼；基於實際作業需要，得核發短期性及臨時性之系統辨識與通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

三十六、委託廠商建置及維護重要軟硬體設施時，應在系統之初始階段即將資訊安全需求納入考量，並在本局相關人員監督及陪同下始得為之。

玖、資訊資產安全管理

三十七、各機關單位對於儲存各項機密資料或程式軟體之磁片、磁碟、磁帶、光碟片及報表等媒體，應設專人管理並定期備份，防止資料洩漏或損毀。

三十八、對於需要長期保留或重要檔案之備份資料，應存放在防火、防潮、防磁的設備中。

三十九、管理或使用人員應詳細記載電腦設備故障、異常及維護等情形，以作為設備更新及作業安全之依據。

壹拾、實體及環境安全管理

四十、　各機關單位對於電腦設備之裝置地點，應考量使用及管理上之安全，並應指定專人負責管理，非經奉准之人員，不得隨意操作設備。管理或使用人員應詳細記載電腦設備故障、異常及維護等情形，以作為設備更新及作業安全之依據。

四十一、電腦設備機房應設置適當之滅火設備。值班人員下班後，應關閉門窗及不必要之電源，以確保安全。

壹拾壹、業務永續運作之規劃

四十二、各機關單位應建立資訊安全事件緊急處理機制，發生資訊安全事件時，除應依下列規定之處理程序先行處理外,並應立即向單位主管或有關人員通報，並視需要通知秘書室，採取反應措施，必要時，得聯繫政風室或檢警調單位協助偵查。

(一)立即停止使用電腦,並保留當時之電腦現況(主機、螢幕、 印表機等)，不要關機。

(二)記錄日期、時間、地點、單位、螢幕出現之訊息等資料。

壹拾貳、附則

四十三、本要點未規定事項,準用行政院及所屬各機關資訊安全管理要點之規定。