宜蘭縣蘇澳鎮公所資訊安全系統存取控制管理規範

中華民國111年7月29日蘇鎮秘字第1110012243號函定發布

一、目的

為有效管理宜蘭縣蘇澳鎮公所(以下簡稱本所)資訊系統之存取安全，防止非法授權存取之事件，以維護資料之保密性，特訂定本規範。

二、適用範圍

E化資訊系統帳號、密碼、權限申請及使用管理等相關事宜。

三、帳號新增及異動管理

(一)宜蘭縣政府EIP公務入口網之帳號新增及異動須經本所人事室登錄後再由秘書室資訊人員依程序向宜蘭縣政府計畫處資訊管理科提出公文帳號申請，並保留紀錄。

(二)帳號、密碼之通知過程，應有保護措施，防止被窺視竊取。

(三)每一使用者在同一系統上應以使用1個帳號為原則，避免1個帳號有2人以上共用情形，以區分資訊安全責任。

(四)離職人員及留職停薪人員應辦理帳號異動程序，並由帳號管理人員依申請程序向宜蘭縣政府計畫處資訊管理科提出申請作業。

(五)系統存取權限之配賦，應以執行公務必要者為限。

四、使用存取權限管理

(一)應依宜蘭縣政府EIP公務入口網規則之通行碼管理，並符合通行碼長度至少為8個字元、複雜度包括數字及英文大小寫或特殊字元等三種以上、使用者每90天應更換一次通行碼。

(二)使用者使用資通系統前應經授權，並使用唯一之使用者ID，除有特殊營運或作業必要經核准並紀錄外，不得共用ID。

(三)使用者調動、離職或退休等無繼續使用資通系統時，應立即停用或移除使用者ID。

五、系統登入作業管理

(一)宜蘭縣政府EIP公務入口網登入失敗，依規定可由自然人憑證進行解鎖，或由帳號管理人員(人事室)確認該帳號擁有人身分後協助解除鎖定。

(二)若使用自然人憑證登入失敗達3次者，卡片會被鎖卡，或使用者忘記PIN碼時，連結至內政部憑證管理中心參考說明及操作步驟，辦理PIN碼/鎖卡解碼等相關作業。

(三)資訊業務委外辦理時，應與廠商簽訂適當的資訊安全協定，賦與相關的安全管理責任，並納入契約條款。

(四)機關進行遠端視訊會議所使用之軟體，應具資通安全性，禁止使用資安疑慮的軟體，例如ZOOM。

六、內部稽核作業依下列原則辦理存取控管作業查核：

(一)定期辦理帳號清查。

(二)監控有無違反系統存取規定之安全事件，並定期檢視紀錄，分析其異常狀況。

(三)存取紀錄檔須另行查核。

七、個人電腦使用之安全管理

(一)嚴禁任意拆卸或加裝其他電腦設備，且不可擅自更改系統環境設定。

(二) 個人電腦作業系統應設置密碼長度至少為8個字元，避免使用與個人有關資料如：生日、身份證字號、單位簡稱、電話號碼等作為密碼之設定。

(三)使用者應負責保護帳號及密碼之機密性，不張貼在個人電腦、螢幕或其他容易洩露秘密之處，避免他人知悉。

(四)個人電腦之使用若超過10分鐘不使用時，是否立即登出或啟動螢幕保護功能或取出自然人憑證，以確保資訊安全。

(五)連網電腦應配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等相關作業。

(六)為強化防護相關網頁瀏覽器，如有安全等級應設定，應設為中級(標準防護)或更高(強化服務)。

(七)使用者應確遵禁止私自安裝點對點檔案分享軟體及未經合法授權軟體之規定。

(八)機密資料如需以行動設備存取、處理或傳送，應經許可後為之。

(九)機密文件及可移除式媒體在不使用或不上班時，應存放於櫃子內並上鎖，切勿隨意放置。

(十)電腦內重要資料文件應定期備份，避免資料毀損；使用外來檔案，應先掃毒，勿任意移除或關閉防毒軟體(本所電腦防毒軟體會自動掃瞄外來檔案)。

(十一)禁止於上班時間閱覽不當之網路(如暴力、色情、賭博、駭客、惡意網站、釣魚詐欺、傀儡網站等)及瀏覽非公務用途網站，以避免內部頻寬壅塞，各單位主管應加強監督同仁使用網路情形。

(十二)下班時，應確實先行關機始得離去，電腦關機應依正常程序操作。

八、電子郵件使用安全

(一)電子郵件使用應以純文字模式開啟並關閉郵件自動預覽功能；各單位主管應加強監督同仁使用電子郵件(Webmail)情形，以避免漏洞產生。

(二)電子郵件未經確認寄件者身分前不任意開啟信件、連結郵件內容中的超連結及下載附件檔案。

(三)公務通訊應使用公務電子郵件信箱且不以私人電子郵件信箱代替使用。

(四)涉及機密或敏感資料應加密傳輸或不以電子郵件傳送，以免外洩。

九、軟體使用管理：

(一)本所各單位因業務需要須增置軟體者，應依本所既有之請購流程，會知資訊人員知悉，簽奉核准後購置之。

(二)本所各單位自行採購之軟體(如光碟或磁片…等)由保管人自行保管，應於安裝前將軟體授權資料(如授權書)或影本彙送資訊人員留存。

(三)本所單位同仁應遵守法律使用合法軟體，不得任意自行安裝、散佈、複製及傳輸未經合法授權之軟體；另屬專業特殊之軟體之安裝與移除，以委由專業廠商會同資訊人員或資訊人員執行為原則。

(四)本所同仁不得隨意安裝來路不明之軟體，於安裝後各單位應向資訊人員回報安裝電腦位置。

十、實體環境安全

(一)機關內電腦及網路設備由所內資訊人員專職管理。

(二)各項電腦設備應定期檢查、維護，以確保其可用性及完整性。

(三)電腦設備報廢前應將機敏性資料及授權軟體予以移除或實施安全性覆寫，並於設備報廢後實施實體破壞措施。

(四)電腦機房內應嚴禁存放易燃物及未經核准之電器或其他物品，並應加強檢查電路及冷氣空調(溫度及濕度)設備之使用情形。

(五)電腦機房應設置門禁設施，防止未經授權者進出；機房進出管制應依下列原則辦理：1.除資訊專責人員外，進出機房人員均須登記非機房管理人員未經許可不得進入機房。 2.如有廠商維護人員進入機房，應由機房管理人員全程陪同。3.不得攜帶非工作所需物品進入機房。