臺中市烏日區公所資訊安全計畫

中華民國 104 年 4 月 27 日烏區秘字第 1040009047 號函頒

壹、資訊安全目標及範圍

一、前言

為推動臺中市烏日區公所(以下簡稱本所）資訊安全教育，強化資訊安全管理，確保本所資料、系統、設備及網路安全，特訂定本計畫。

二、目標

(一)維持本所各項資訊系統持續運作。

(二)防止駭客、病毒等入侵及破壞。

(三)防止人為意圖不當及不法使用。

(四)避免人為疏失意外。

(五)維護實體環境安全。

三、範圍

本規範管理之範圍包括本所之人員、應用系統、硬體設備及網路設施等四部分。

(一)人員：

涵蓋本所全體員工(含正式人員、技工、工友、約聘僱人員、行政助理及替代役)，及使用本所資訊資源之委外廠商人員。

(二)應用系統：

1. 本所業務系統（如戶役政資訊系統)。
2. 本所行政資訊系統（如人事、會計、出納、公文暨檔案管理等行政作業系統)。
3. 網際網路應用：電子郵件、本所全球資訊服務網站等。
4. 本所採用之套裝軟體。

(三)硬體設備：

本所辦公室內各式主機、戶役政資訊系統工作站、公文檔案管理系統伺服器及個人行政用電腦。

(四)網路及其設備：

本所辦公室區域網路、網際網路之數據專線及相關網路設施。

貳、人員管理及教育訓練

一、人員安全評估及管理

(一)本所應成立資通安全處理小組，負責督導屬員之資訊作業安全，防範不法及不當行為，成員、職掌如下：

1. 召集人：主任秘書擔任，負責推動及研議資通安全管理相關業務。
2. 各課室主管：負責各課室之資通安全管理及相關業務。
3. 政風人員：負責稽核本所資通安全工作是否落實。

4.資訊人員：負責網站、個人電腦資訊安全。

(二)離職、退休人員，應立即取消其識別碼、通行碼，管制系統使用權限。本所各課室人員變動時(新進人員、職務變動、人員離職)，人事人員應主動通知資訊人員進行臺中市政府 e 化公務入口網及公文管理資訊系統之帳號及權限修正。

二、員工維護資訊安全及公務機密責任

(一)員工應遵守本規範及其他相關資訊安全規定，若違反資訊安全相關規定，得依情節輕重予以處分。

(二)本所員工應遵守維護公務機密之相關法令規定；在職及離(退)職後，均不得洩漏所知悉之業務機密或為不當之使用，否則得視其情節輕重予以處分或追究其民、刑事責任。

三、資訊安全教育訓練

(一)本所應派員參加中央及市政府辦理之資訊安全教育訓練及宣導，或上網參加公務人員終身學習網之資訊安全課程，促使員工瞭解資訊安全的重要性，各種可能的安全風險，以提高員工資訊安全意識，促其遵守資訊安全規定。

(二)各課室應加強資訊安全管理人力之培訓提升資訊安全管理能力。

參、電腦系統作業安全管理

一、電腦系統作業程序及責任

(一)各承辦人應訂定所承辦業務之電腦系統作業程序，以確保正確及安全的操作使用電腦，俾供職務代理人或職務接交人作業之依據。

(二)資訊安全事件之處理程序除正常的應變計畫外(如系統及服務之回復作業)，尚應納入下列事項：

1.導致資訊安全事件原因之分析。

2.防止類似事件再發生之補救措施的規劃及執行。

(三)系統發展測試作業及系統正式作業之軟體，應分別在不同處理器或不同的目錄下作業，以便系統測試與正式作業分開處理，並避免作業軟體或資料遭意外竄改或不當使用。

(四)資訊業務委外時，應於事前審慎評估可能的潛在安全風險(例如資料或使用者通行碼被破解、系統被破壞或資料損壞等風險)，與廠商簽訂適當的資訊安全協定，將相關的安全管理責任納入契約條款。

二、日常作業之安全管理

(一)重要的資料及軟體應定期執行備份作業，俾災害迅速回復。

(二)資訊設施及系統的變更作業，應建立管控機制，並應記錄電腦系統作業中斷及更正等異常事項。

(三)必須使用具有智慧財產權的合法軟體，並禁止使用未經合法授權之軟

體。

(四)電腦病毒之防範應採行必要的事前預防措施，防制電腦病毒入侵，並慎選功能完整的電腦病毒防制軟體，定期維護更新。

肆、網路安全管理

一、網路安全規劃與管理

(一)各系統伺服器與外界網路連接之網點，須設立防火牆以控管外界與內部網路之資料傳輸及資源存取，避免外界直接進入資訊系統或資料庫存取資料。

(二)應建立電腦網路系統的安全控管機制，以確保網路傳輸資料的安全，保護連網作業，防止未經授權的系統存取。

(三)對於跨組織之電腦網路系統，應特別加強網路安全管理，並協定應遵循之網路安全規定。

(四)利用公眾網路傳送敏感性資訊，應採取特別的安全保護措施，以保護資料在公共網路傳輸的完整性及機密性，並保護連線作業系統之安全性。

(五)網路使用者之管理：

被授權的網路使用者，只能在授權範圍內存取網路資源，不得將自己的登入身份識別與登入網路的密碼交付他人使用。禁止使用違反著作權、善良風俗或會妨害網路系統的正常運作之不法或不當的資訊。

(六)主機安全防護：

存放機密性及敏感性資料之主機或伺服器主機，應規劃各種安全控管技術，以提昇網路作業之安全性。

(七)防火牆之安全管理：

本所與外界公眾網路連接的網點網路之節點，依業務性質與安全等級，設置防火牆區隔內、外網路，以控管外界與內部網路之間的資料傳輸與資源存取。

(八)軟體下載之管制：

1. 禁止使用非法軟體。
2. 經由網際網路下載軟體或資料檔案，得視業務特性及需要，經測試及掃瞄確認安全無虞及不違反智慧財產權前提下，方得下載執行。

(九)網路資訊之管理：

1. 機密性及敏感性資料或文件不得存放於對外開放的資訊系統中。
2. 存放民眾申請或註冊的私人資料檔案，應研究以安全方式處理，以防止資料被非法使用。
3. 對外開放的資訊系統應針對蓄意破壞者進行導致系統作業癱瘓之行為，預作有效的防範，以免影響本所的服務品質。

4.對外開放的資訊系統所提供之網路服務(FTP、HTTP 等)，應做適當的存取控管，以維護系統正常運作。

二、電子郵件之安全管理

(一)機密性資料或文件，不得以電子郵件傳送；機密性資料以外之敏感性資料如有電子傳送之必要，應經加密或電子簽章等安全處理後傳送。

(二)對來路不明的電子郵件，切勿隨意打開電子郵件，以免啟動惡意執行檔，使網路系統遭到破壞。

三、全球資訊網之安全管理

(一)全球資訊網：

內部使用的瀏覽器，對下載的每一檔案應做電腦病毒或惡意內容的掃描。

(二)網路入侵之處理：

發現網路被入侵或疑似被入侵時(如：網頁遭竄改、分散式攻擊、資料非法存取、密碼被破解等)，應立即依下列程序處理，並採取必要的行動。

1.立即拒絕入侵者任何存取動作，防止災害繼續擴大。

2.切斷入侵者的網路連接，如無法切斷則必須關閉防火牆；或為達到追查入侵者的目的，可考慮讓入侵者做有條件的連接，一旦入侵者危害到內部網路安全，則必須立即切斷入侵者的網路連接。

3.應全面檢討網路安全措施及修正防火牆的設定，以防範類似的入侵與攻擊。

4.應記錄入侵的情形及評估影響的層面。

5.立即向權責主管人員報告入侵情形。

依行政院國家資通安全會報通報及應變作業流程辦理，並向臺中市政府資訊中心反應，以獲取必要的外部協助。

四、網路安全稽核

(一)網路安全稽核事項：

1.操作紀錄及作業紀錄應至少保存半年以上。

2.視業務需要，對於通過防火牆之特定網路服務，應向市政府網路管理單位申請。

(二)網路入侵之追查：

網路入侵者之行為若觸犯法律規定，構成犯罪事實，應立即通報檢警憲調單位處理。

伍、系統存取控制

一、系統存取之管理

(一)應建立系統使用者註冊管理制度，並加強使用者通行碼之管理，伺服

主機之使用者通行碼應定期更新，最長不得超過六個月為原則。

(二)系統存取權限之配賦，應以執行業務及職務所必需者為限，當使用者調整職務及離（休）職時，應儘速註銷其系統存取權限。

(三)終端使用者之識別碼及通行碼，均應限制使用，並嚴禁轉知他人，若已為他人知悉者，應即報告上級主管適時更新；凡因故被冒用致造成不良後果，應負洩密之責。

(四)個人必須負責保護通行密碼，以維持其機密性。

(五)避免將通行密碼記錄在書面上，或張貼在個人電腦或終端機螢幕或其他容易洩漏秘密之場所。

(六)使用者密碼的長度最少應由六位長度組成（密碼安全強度請參照行政院國家資通安全會報密碼設置原則),避免使用下列事項作為通行密碼：

1. 個人姓名、出生日、身分證字號或汽機車牌照號碼。
2. 機關、單位名稱、識別代碼或是其他相關事項。
3. 電話號碼。
4. 使用者識別碼、使用者姓名、群體使用者之識別碼或是其他系統識別碼。
5. 電腦主機名稱、作業系統名稱。

二、網路存取之安全控制

盡量避免允許系統服務廠商以遠端登入方式進行系統維修,如因業務需要應經申請核准後才可使用;維修完畢後,需將該系統之遠端登入權限關閉。

三、電腦主機之存取控制

(一)使用者進入電腦系統，應經由安全的系統登入程序。

(二)登入程序應具備下列的功能：

1. 限制系統登入不成功時可以再嘗試的次數。
2. 在系統登入被拒絕後，應立即中斷登入程序。

四、應用系統之存取控制

(一)應用程式原始程式碼、資料庫及執行檔應分別存放。

(二)開發中及正式作業之應用程式及資料庫應各自存放。

(三)各系統應保有各版本之更新紀錄。

五、系統存取及應用之監督

例外事件及資訊安全事項發生時應建立記錄，並保存至結案查出原因為止，以作為日後調查及監督之用。

陸、系統發展及維護之安全管理

一、系統安全需求規劃

(一)系統安全需求分析及規格

新發展的資訊系統，或是現有系統功能之強化，應在系統規劃之需求階段，即將安全需求納入系統功能。

(二)除由系統自動執行的安控措施之外，亦可考量由人工執行安控措施；在採購套裝軟體時，亦應進行相同的安全需求分析。

(三)系統的安全需求及控制程度，應與資訊資產價值相稱。

(四)資料加密：

對高敏感性的資料，應在傳輸或儲存過程中以加密方法保護。

三、應用系統軟體之安全

(一)程式版本之控制

應用系統執行時,應嚴格控制程式版本,減少可能危害作業系統的風險:

1.程式執行碼更新作業，應限定只能由授權的管理人員才可執行。

2.應用程式執行碼的更新應建立紀錄。

3.更新應保留舊版的軟體。

(二)系統測試資料之保護

1.應保護及控制測試資料，避免以含有個人資料的真實資料庫進行測試。

2.測試完畢後，真實資料應立即從測試系統中刪除。

3.真實資料的複製情形予以記錄，以備稽核運用。

四、系統維護環境之安全

(一)對廠商之軟體系統建置及維護人員,應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。

(二)核發短期及臨時性之系統辨識及通行密碼供廠商使用,於使用完畢後應立即取消其使用權限。

(三)委外建置或維護軟硬體設施時，應在機關相關人員監督及陪同下為之。

柒、資訊資產的安全管理

一、資訊資產目錄之建立及保護

(一)本所建立的資訊資產目錄，內容應包括資訊資產的項目、保管者及安全等級分類等。

(二)資訊資產包括項目如下：

1.資料：資料庫及資料檔案、系統文件、使用者手冊、訓練教材、作業及支援程序、備援回復作業計畫、資料儲存媒體等。。

2.軟體：應用軟體、系統軟體、發展工具及公用程式等。

3.硬體：電腦及通訊設備。

4.其他相關設備。

二、資訊安全等級分類

(一)應納入安全等級分類的項目，包括系統文件、螢幕顯示、資料儲存媒體、電子訊息及檔案資料等。

(二)資訊安全分類標準，應考量資訊分享及資料的機密性、正確性。

(三)本所資訊安全分類，區分為機密性、敏感性及一般性等三類。

(四)資訊資產之安全等級，由業務單位或指定的系統管理者負責界定。

捌、實體及環境安全管理

一、設備安全管理

(一)設備（應含電腦、電力及通訊纜線等）應安置在適當的地點並予以保護，以減少環境不安全引發的危險及減少未經授權存取系統的機會。

(二)電源供應應考量安置預備電源，對於特別敏感性或是特別重要的系統，應採取額外強化的安全措施。

(三)應依據設備特性訂定維修服務期限及說明，進行設備維護，以確保設備的完整性及可以持續使用。

(四)設置在外部以支援業務運作的資訊設備，應同樣遵守資訊安全管理授權規定，維持與內部資訊設備一樣的安全水準。

(五)含有儲存媒體的設備，報廢前應詳加檢查，以確保任何機密性、敏感性的資料及有版權的軟體已經被移除。

二、周邊安全管理

(一)周圍環境之安全：

實體環境的安全保護程度，應視資訊資產及系統價值的安全風險而決定。

(二)人員進出管制：

1. 非因業務需要或被授權核准者，不得進入電腦機房。
2. 進入電腦機房應登記相關資料(進出時間和目的)。
3. 電腦維修廠商或其他廠商人員，應由業務相關人員陪同，始得進入機房工作。

(三)電腦機房安全管理：

1. 機房內嚴禁吸煙、飲食。
2. 機房內嚴禁存放易燃物及未經核准之電器或其他物品。
3. 資訊人員應隨時注意機房環境監控系統，若發現異常狀況應即刻處理。
4. 資訊人員應熟悉滅火器位置及操作方法。

(四)辦公桌面之安全管理：

1. 公文及各式資料存取之磁碟、光碟長時間不使用及下班後，應妥為存放；機密性、敏感性資訊，應妥為收存。
2. 含機敏資料之紙張不得再回收利用，應以碎紙機銷毀廢棄之影印公

文及已過保存期限之公文，應予以銷毀。

3.個人電腦及終端機不使用時，應予關機、登出、設定螢幕密碼或是以其他控制措施保護。

(五)資訊財產攜出之安全管理：

電腦設備、資料或軟體，未經許可，不得帶離辦公室。

玖、備援及回復作業

一、依業務重要性訂定作業程序，並界定優先順序。

二、評估各種災害對業務可能的衝擊。

三、明確界定應變小組人員責任，及緊急應變措施之安排。

四、定期測試、檢討備援回復作業相關計畫。

五、應配合業務、組織及人員的調整變更定期更新。

拾、資訊安全事件通報處理機制

一、資訊安全事件之通報

(一)業務系統如因資訊安全事件(包括系統有安全漏洞、遭受非法入侵及破壞、遭遇阻斷服務攻擊及功能不正常事件等)，致電腦系統無法運作或影響執行效率時，系統相關人員應視其狀況嚴重程度及影響層面，循序速向各權責主管通報。

(二)本所資通安全處理小組，並應依『行政院資通安全危機通報及應變作業計畫』規定向上通報。

二、資訊安全事件之處理

(一)發現資訊安全事件時,應通知相關人員進行評估,並進行處理及通報。

(二)應立即停止使用受影響之電腦系統或設備，並保留現況，並迅速通知系統管理人員或維護廠商協助處理。

(三)事件之處理情形，應向直屬主管回報處理結果，並作成紀錄。

拾壹、本計畫未規定事項，準用臺中市政府資訊安全管理要點之規定。

拾貳、本計畫奉區長核可後實施，修正時亦同。