臺北市政府資訊安全管理規範

中華民國 103 年 3 月 20 日臺北市政府(103)府授資設字第 10330048700 號函頒。
中華民國 106 年 4 月 25 日臺北市政府(106)府授資設字第 10630682000 號函修訂。
中華民國 108 年 5 月〇日臺北市政府(108)府授資設字第 1083007005 號函修訂。

壹、總則

一、臺北市政府為強化所屬各機關(以下簡稱各機關)資訊安全管理，建立安全及可信賴之電子化政府，確保資料、系統、設備及網路安全，特訂定本規範。

二、 本規範之資訊安全政策、目標與責任如下：

(一) 資訊安全政策：各機關應遵循相關法令法規要求，例如：個人資料保護法及著作權法等，並確保資訊及其處理設備之機密性、完整性與可用性。

(二) 資訊安全目標：

1、發生「資通安全事件通報及應變辦法」所定義之第三級以上資訊安全事件，每年不得高於一次。

2、依「資通安全責任等級分級辦法」之附表九「資通系統防護需求分級原則」所評鑑之防護需求等級「高」之系統可用性每年(三百六十五日乘以二十四小時)達百分之九十九。

3、與民眾相關之服務與系統之可用性每年(三百六十五日乘以二十四小時)達百分之九十七點五。各機關得依據業務特性自行調正上述目標，惟須經機關資通安全長核定。

(三) 資訊安全責任：

1、除上述目標外，各機關應依業務目標考量，盤點資訊資產及注意資訊安全風險管理，以提高資訊系統及資訊蒐集、處理、傳送、儲存及流通之安全。

2、各單位主管對於資訊安全政策、目標及相關作業規範之遵循，應負監督、執行、稽核之職責。

3、所有人員應充分了解資訊安全政策、目標及職責。

貳、資訊安全組織

三、 資訊安全組織：

(一) 各機關應依「資通安全責任等級分級辦法」進行資安責任等級分級，並應依其資通安全責任等級，辦理「資通安全責任等級分級辦法」附表一至八之規定事項。

(二) 由資訊單位主管(或指派專人)負責推動、協調及督導機關資訊安全各項事宜；各業務單位主管負責督導所屬之資訊作業安全事宜。

(三) 資料及資訊系統之安全需求研議、使用管理及保護等事項，由業務單位負責辦理。

(四) 得視需要由資訊單位主管成立跨單位資訊安全推行小組，推動機關資訊安全作業。

(五) 資訊機密維護及稽核使用管理事項，由政風單位會同相關單位負責辦理。未設置資訊及政風單位者，由機關首長指定適當單位及人員負責辦理。

參、人員安全管理及教育訓練

四、 人員安全管理：

(一) 各機關對於可存取機密性與敏感性資訊或系統之人員，及因工作需要配賦系統特別權限之人員，應加強評估及考核。

(二) 人員離(調)職時，應適時取消或調整各項權限。

(三) 人員資訊安全相關作業應遵循「臺北市政府員工使用電腦應注意事項」。

(四) 人員如違反資訊安全相關規定，應依紀律程序處理。

五、 資訊安全訓練：

(一) 各機關同仁應針對不同工作類別之需求，定期參與資訊安全教育訓練(教育訓練時數要求參考「資通安全責任等級分級辦法」附件一至八所定制度面向「認知與訓練」) 。

(二) 各機關應加強資訊安全管理人力之培訓，提升資訊安全管理能力。

肆、實體與環境安全

六、 安全之辦公處所：

(一) 應使用安全周界（諸如圍牆、入口閘門或人員駐守之接待櫃檯等屏障）或藉由適當之入口控制措施加以保護，確保經授權人員始得進出。

(二) 應考慮火災、水災及其他形式自然或人為之災害所造成損失之可能性，設計辦公室、隔間及設施之實體安全措施並施行之。

七、 設備安全：

(一) 設備應安置於適當地點並予以保護，以減少環境不安全所引發之危險及減少未經授權存取系統之機會。原則如下：

1、 重要設備應避免設置於公眾進出之位置。

2、 處理機密性及敏感性資料之工作站，應放置於員工可以注意及照顧之地點。

3、 需要特別保護的設備，應考量與一般設備區隔，安置在獨立之區域。

4、 檢查及評估火災、煙、水、灰塵、地震、電力供應等可能之風險。

(二) 電源供應依據製造商所提供之規格設置。

(三) 應謹慎使用電源延長線，以免電力無法負荷導致火災。

(四) 重要設備得考量使用不斷電系統(UPS)。

(五) 電力及通信用之電纜線，應予適當之保護，以防止被破壞或資料被截取。

(六) 重要設備應妥善維護設備，以確保設備之完整性及可以持續使用。

(七) 設置在外部以支援業務運作之資訊設備，應同樣遵守資訊安全管理規定，維持與內部資訊設備相同之安全水準；其內、外部區分係以單位或機關主要辦公處所為準。

(八) 含有儲存媒體之設備(例如硬碟)應在異動(例如汰除與再利用)前詳加檢查，並確保任何機密性、敏感性資料及版權軟體已被移除。

八、 機房管理：

(一) 電腦機房應有門禁管制措施，並設置防火、空調、緊急照明及監視錄影設備。

(二) 電腦機房應禁止抽煙及飲食。

(三) 電腦機房內應避免置放危險性及大量易燃性物品。

伍、資訊系統作業安全管理

九、 資訊系統作業程序及責任：

(一) 資訊系統應依「資通安全責任等級分級辦法」之附表九「資通系統防護需求分級原則」，進行系統分級作業，機關並應依據評估結果，參考「資通安全責任等級分級辦法」之附表十「資通系統防護基準」進行防護。

(二) 測試與正式作業資訊系統應分開處理，避免作業軟體或資料遭意外竄改或不當使用。

(三) 資訊業務委外時，應於事前審慎評估可能之潛在安全風險，並與廠商簽訂適當之資訊安全協定，將安全管理責任相關事項納入契約條款。

(四) 委外人員資訊系統使用權限應經適當控管；委外期間結束後，應立即收回該項權限。

(五) 系統文件應予適當儲存與保護。

十、 日常作業之安全管理：

(一) 對於資訊系統作業中斷及更正等異常事項，應詳實記錄。

(二) 重要資訊系統應隨時監測作業環境狀況。

十一、 電腦病毒及駭客防範：

(一) 電腦應設定密碼保護、安裝防毒軟體，並即時更新系統與軟體漏洞修補。

(二) 防毒軟體應更新病毒碼，除線上即時防護外，每月至少實施一次完整檔案掃瞄。

(三) 各機關業管之電腦系統(例如戶政機關辦理戶政業務所使用之電腦系統)應每年至少實施二次弱點檢核，防止被駭客入侵而影響業務運作及損害信譽。

十二、 稽核存錄：

(一) 資訊系統應啟動稽核存錄功能，留存帳號登入、登出與特殊權限使用等電腦稽核紀錄(log)。

(二) 電腦稽核紀錄應予妥善保護，防止未經授權之存取、竄改與刪除。

(三) 電腦稽核紀錄應視需求保留，至少應保留六十天以上。

(四) 重要系統電腦稽核紀錄得異機備份保存。

十三、 軟體使用：

(一) 各機關使用軟體應遵守智慧財產權相關法令規定及契約約定。

(二) 使用廠商提供之套裝軟體，各機關應儘可能避免自行變更或修改。

十四、 個人資料保護：

(一) 應依據「個人資料保護法」等相關規定，審慎處理及保護個人資料。

(二) 資訊系統應合理留存個人資料之新增、修改、刪除、資料匯出、列印等活動之操作紀錄。

(三) 處理含個人資料之資訊系統，除了執行業務所必要者外，應避免提供資料整批匯出功能。

(四) 任何系統如具個人資料，應考量個資外洩風險，於必要時執行滲透測試。

十五、 資料備份：

(一) 各機關應準備適當及足夠容量(例如硬碟或儲存設備空間)，定期執行必要之資料及軟體備份。

(二) 備份資料應定期測試以確保其可用性。

十六、 電腦媒體之安全：

(一) 可隨時攜帶及移動的電腦媒體，於儲存含有機密性、敏感性或個人資料檔案時，應加密或以密碼保護。

(二) 保存重要資料檔案之儲存媒體應以安全之方式保存(例如：儲存於上鎖之箱櫃)。

(三) 儲存機密性、敏感性或個人資料檔案之媒體，當不再繼續使用時，應以實體破壞或燒毀等安全方式處理。

十七、 資料及軟體交換之安全：

(一) 各機關間或與往來對象進行例行性資料或軟體交換，得訂定交換協定將機密性及敏感性或個人資料檔案之安全保護事項及有關人員責任列入。

(二) 電腦媒體運送及傳輸過程應有妥善之安全措施，以防止資料遭破壞、誤用或未經授權之取用。

陸、網路安全管理

十八、 網路安全管理：

(一) 各機關開放外界連線作業之資訊系統，應視資料及系統之重要性，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統遭侵入、破壞、竄改、刪除及未經授權之存取。

(二) 各機關與外界網路連接之網路應以防火牆及其他必要安全設施，控管外界與機關內部網路之資料傳輸及資源存取。

(三) 各機關防火牆之管理活動(例如：管理者帳號登入、登出或網路連線進出規則變更)應留存稽核紀錄(log)至少九十天；另外，對於通過防火牆之網路連線應留存目的與來源 IP 位址、通訊埠等連線稽核紀錄(log)至少四十五天。

(四) 使用無線網路得與機關內部辦公作業網段區隔；若需使用於辦公作業網段應使用身分鑑別、加密機制或其他額外之安全控管措施。

(五) 各單位應注意外來人員使用可攜式電腦或其他資訊設備連結防火牆之內之網路連接埠，以防止內部資料外洩或資訊系統毀損。

(六) 網路使用應遵守「臺北市政府所屬機關網路使用規範」。

十九、 全球資訊網之安全管理：

(一) 各機關利用網際網路及全球資訊網公布及流通資訊，應加以保護免於詐欺行為、契約爭議及未經授權之揭露與修改。

(二) 機密性、敏感性及個人隱私資料與文件不得公布於全球資訊網。但因執行業務致有公布之必要，且符合下列情形之一者，不在此限：

1、 為防止他人權益之重大危害。

2、 經當事人書面同意。

3、 為增進公共利益。

(三) 各機關全球資訊網頁資料之正確性與時效性應參考「臺北市政府各機關網站資料檢核計畫」辦理。

(四) 各機關網頁程式碼應經過測試及弱點修正 (含 SQL Injection 與 Cross Site Scripting 等弱點)，始可公布於網際網路。

(五) 禁止開放網頁瀏覽目錄權限，以避免公務機密與市民個人資料外洩。

(六) 各機關網頁應每年至少實施一次弱點檢核，防止網頁被駭客入侵而影響業務運作及損害信譽。

柒、系統存取控制

二十、 存取控制機制：各業務單位應將其存取控制需求，明確告知資訊單位以利其執行及維持有效之存取控制機制。

二十一、系統存取管理：

(一) 資訊單位應建立系統使用者註冊管理制度，並落實使用者通行密碼之管理。

(二) 系統存取權限之配賦，應以執行業務及職務所需者為限。

(三) 使用者第一次使用應用系統(AP)時，應更新初始密碼後方可繼續作業。

(四) 對於使用者忘記密碼之處理，應執行身分確認程序，方可再次使用系統。

(五) 應視應用系統(AP)特性限定其作業時間，以減少未經授權人員存取系統之機會。

(六) 系統通行密碼長度應至少八碼，並包含英文字母、數字與特殊符號之組合。

(七) 系統帳號應定期更換通行密碼，更新期限最長不得超過六個月。

(八) 系統帳號應避免共用，以利鑑別使用者；若在特殊情況下需共用帳號，應取得權責單位主管授權，並實施補償性控管機制。

(九) 系統管理者帳號權限應至少每半年實施一次檢討及評估。

(十) 系統應有安全身分鑑別及防止暴力破解帳號密碼機制。

(十一) 多人共同使用或無人看管之工作站與設備應有適當的安全保護措施，防止未經授權之系統存取。

二十二、網路存取控制：

(一) 各機關應視資訊系統或服務之性質儘可能限制網路存取之設備(例如只開放授權之 IP 位址或網路卡(MAC)、使用強制性通道存取資訊系統或網路資源)。

(二) 各機關對於遠端登入方式作業，應採取特別之安全控管機制。

二十三、金鑰管理：代表組織身分之加密金鑰應有明確之啟動與止動日期，並於可用期間，保護其不被修改、遺失和破壞。

捌、系統發展與維護安全管理

二十四、應用系統(AP)安全規劃：

(一) 新發展或現有應用系統功能之強化，應於規劃之需求階段，即將安全需求

納入應用系統功能。

(二) 應用系統應能依使用者之角色設定不同存取權限。

(三) 應用系統應允許使用者自行選擇及更改通行密碼。

(四) 應用系統應具備資料輸入錯誤之更正功能。

(五) 使用者之密碼應與應用系統資料分開存放並加密處理。

(六) 應用系統設計應使用多層次架構避免外界直接進入資料庫存取資料。

(七) 應用系統應有資料輸入合理性檢驗，以確保資料之真確性。

(八) 應用系統內部作業應建立驗證資料正確性之作業程序，例如：比對本次開始作業與前次結束作業檔案資料是否一致、查證系統產生之資料是否正確等。

(九) 應用系統設計須設置連線作業時間控制及操作逾時自動登出機制。

(十) 對於高敏感性之資料應於傳輸或儲存過程中以加密方法保護。

(十一) 應視應用系統需求使用鑑別技術，偵測資料內容是否遭竄改，保護資料內容之真確性。

(十二) 應用系統開發環境應特別注意防止遭受惡意程式碼攻擊，以避免程式原始碼被感染或植入惡意程式碼。

(十三) 應用系統之安全控制措施應符合「資通安全責任等級分級辦法」之附表九「資通系統防護需求分級原則」及附表十「資通系統防護基準」要求。

(十四) 系統開發應避免將連線密碼直接明寫於程式碼中，且連線帳號應限制權限，避免使用最高權限帳號，例如：sa、root、admin 進行連線。

(十五) 應要求委外廠商保證交付之系統不含惡意程式如：病毒、蠕蟲、特洛伊木馬程式、間諜系統等)及隱密通道(covert channel)。，並提供委外廠商保證事項之證明文件如測試報告等。

二十五、 系統變更：

(一) 系統架構、環境變更或線上系統之原始程式碼需要維護時，應經過正式核准之程序辦理。

(二) 作業系統(OS)及環境變更前，應評估其對應用系統是否造成負面影響，或產生安全問題。

(三) 應用系統軟體更新應建立版本控管機制。

二十六、 應用系統程式之控制：

(一) 應用程式館更新，應限於經授權之管理人員始得執行。

(二) 應保留舊版程式作為緊急應變之用。

(三) 應用程式原始碼之存取應建立安全控管機制。

二十七、　測試資料之保護：各機關應保護及控制測試資料，避免含有個人資料之真實資料庫進行測試，例如優先使用模擬資料；如須應用真實資料，應於事前刪除足以辨識個人之資料並採取適當之安全保護措施。

玖、行動裝置應用程式安全

二十八、　各機關提供行動裝置(包含但不限於智慧型手機、平板電腦等具通信及連網功能之隨身設備)應用程式服務，應遵守下列安全要點：

(一) 應針對應用程式檢視系統所需最小權限，並進行存取控制。

(二)於行動裝置上如有必要儲存敏感資料，應採取加密或亂碼化等相關機制保護，以防範資料外洩。

(三)應針對應用程式進行原始碼掃描、黑箱測試或滲透測試，並針對中、高風險弱點及可影響敏感資料被竊取或竄改之弱點進行改善。

(四)前款所定中、高風險，係依據美國國家標準技術研究所(NIST)所公布或以共同漏洞評分系統（Common Vulnerability Scoring System，CVSS）工具計算出之風險等級。

(五)開發行動應用軟體時，應遵循「臺北市政府行動應用軟體(APP)服務發展作業原則」。

拾、資訊安全事件之管理

二十九、資訊安全事件通報與處理：

(一) 發生資訊安全事件，應依「資通安全事件通報及應變辦法」處理。

(二) 資安事件通報程序，應每年至少演練一次。

拾壹、業務持續運作管理

三十、　系統備援及緊急應變：

(一) 核心資訊系統應建置備援方案並訂定復原程序，如備援演練程序、系統回復演練程序。

(二) 核心資訊系統應定期備份，包括完整系統、系統架構組態設定及資料。

(三) 核心系統復原程序應每年至少演練一次，以確認程序之有效性。

拾貳、獎勵及懲處

三十一、獎勵及懲處：

(一) 各機關所屬人員對於機關之資通安全維護績效優良者，應予獎勵。

(二) 各機關所屬人員未遵守本規範者，應按其情節輕重，依相關規定予以懲戒

或懲處。