安全管理措施實施辦法

目錄

安全管理措施實施辦法

一、 人員管理措施

(一) 依據作業之必要，設定本校所屬人員關於個人資料蒐集、處理或利用，以及保有個人資料媒體之相關權限，且定期確認權限內容設定之適當與必要性。

(二) 本校所屬人員應落實本程序書中各項安全管理措施之執行。

(三) 本校所屬人員調離職務時，應將所保管之個人資料，返還本校或刪除、銷毀。並移除或停止其所擁有之個資相關權限。

(四) 應與本校所屬人員約定保密義務，至少應包括下列內容：

1. 個資蒐集、處理及利用之注意義務。
2. 蒐集、處理及利用之個資之範圍。
3. 保密義務期間，應及於人員調離職務之後。
4. 人員調離職務時，其所保管之個人資料，應返還本校或加以刪除、銷毀。

二、 個人資料之傳輸

(一) 個人資料之傳輸應有妥善的安全措施。

(二) 在本校內之傳輸，屬於高風險個資（本校依第肆章個資風險評估作業後，所評定屬於較高風險之個資，本校可依自身業務特質自行決定高風險個資之範圍）者，由承辦人員親送。

(三) 在本校外之傳輸，屬於高風險個資者，應由承辦人員親送。屬於非高風險個資者，得由承辦人員所指定人員傳輸，或以掛號函件傳輸。

(四) 個人資料非由承辦人員親送者，應密封交遞。以電子通信工具傳輸高風險個資者，應以適當加密機制傳輸。

三、 個人資料之複製

個人資料如於作業過程中有複製之必要，其複製品應視同原件妥善保管，無繼續使用之必要時，應即銷燬。

四、 個人資料之保管

(一) 依據作業內容之不同，實施適宜之進出管制方式。

(二) 妥善保管個人資料之儲存媒介物。

(三) 針對不同媒介物存在之環境，審酌建置適度之保護設備或技術。

(四) 針對所保有之個人資料內容，如有加密之需要，於蒐集、處理或利用時，宜採取適當之加密機制。

(五) 高風險個資檔案應保管於辦公處所；其有攜離必要者，須經單位主管或其授權之具管理職責之人員核准。

(六) 高風險個資檔案之存放場所，對於人員及物品之進出，應予以管制，並造冊列管，載明進出人員、時間及目的。

五、 電腦系統安全管理

(一) 系統規劃

1. 蒐集、處理或利用個人資料之新系統上線作業前，應執行適當的測試作業，以確認系統功能符合合理可期待之安全水準。
2. 系統的變更，應建立控制及管理機制，以免造成系統安全上的漏洞。

(二) 電腦病毒及惡意軟體之防範

1. 應採行必要的事前預防及保護措施,防制及偵測電腦病毒、特洛依木馬及邏輯炸彈等惡意軟體的侵入。促使員工正確認知電腦病毒的威脅，提升員工的資訊安全警覺，健全系統存取控制機制。
2. 惡意軟體防範應考量的重要原則如下：
   (1) 應建立軟體管理政策，規定各單位及使用者應遵守軟體授權規定，禁止使用未取得授權的軟體。
   (2) 應選用信譽良好、功能健全的惡意軟體防制軟體，並依下列原則使用：

A. 惡意軟體防制軟體應定期更新，並在廠商的指導下使用。

B. 使用防毒軟體事前掃瞄電腦系統及資料儲存媒體，偵測有無感染電腦病毒。

C. 視需要安裝可偵測軟體是否遭更改的工具軟體，並偵測執行碼是否遭變更。

D. 應謹慎使用可掃除電腦病毒及回復系統功能的解毒軟體；使用前應充分瞭解電腦病毒的特性，以及確定解毒軟體的功能。

E. 應定期檢查軟體及檢查重要的系統資料內容，如發現有偽造的檔案或是未經授權的修正事項，應立即調查，找出原因。

F. 對來路不明及內容不確定的磁片，應在使用前詳加檢查是否感染電腦病毒。

G. 應建立防制電腦病毒攻擊及回復作業的管理程序，並訂定相關人員的責任。

H. 為使電腦病毒影響正常運作之程度降至最低，應建立妥適的業務永續運作計畫，將必要的資料及軟體加以備份，並於事前訂定回復作業計畫。

(三) 日常作業之安全管理

1. 資料備份

(1) 應準備適當及足夠的備援設施，定期執行必要的資料及軟體備份及備援作業，以便發生災害或是儲存媒體失效時，可迅速回復正常作業。

(2) 資料備份作業原則如下：

A. 正確及完整的備份資料，除存放在主要的作業場所外，應另外存放在離主要的作業場所有一段距離的場所，以防止主要作業場所發生災害時可能帶來的傷害。

B. 備份資料應有適當的實體及環境保護，其安全標準應儘可能與主要作業場所的安全標準相同；主要作業場所對電腦媒體的安控措施，應儘可能適用到備援作業場所。

C. 應定期測試備份資料，以確保備份資料之可用性。

2. 電腦作業環境之監測

電腦作業環境如溫度、溼度及電源供應之品質等，應依據供應廠商的建議，建立監測系統，隨時監測電腦作業環境，並採取必要的補救措施。

(四) 電腦媒體之安全管理

可隨時攜帶及移動的電腦媒體，應建立使用管理程序，規範磁帶、磁碟及電腦輸出報告等媒體之使用。可重複使用的資料儲存媒體，不再繼續使用時，應將儲存的內容消除，或以適當方式銷毀之。

六、 網路安全規劃與管理

(一) 主機安全防護

1. 存放大量個人資料或高風險個資之大型主機或伺服器主機（如：Domain Name Server 等），除作業系統既有的安全設定外，應規劃安全等級較高之密碼辨識系統，以強化身份辨識之安全機制，防止遠端撥接或遠端登入資料經由電話線路或網際網路傳送時，被偷窺或截取（如：一般網路服務 HTTP、Telnet、FTP 等的登入密碼），及防制非法使用者假冒合法使用者身分登入主機進行偷竊、破壞等情事。

2. 為提升大型主機或伺服器主機連線作業之安全性，應視需要使用電子簽章及電子信封等安全控管技術，以建立安全及可信賴的通信管道。

(二) 防火牆之安全管理

1. 與外界網路連接的網點，應加裝防火牆，以控管與本校網路之間的資料傳輸與資源存取。

2. 防火牆應具備網路服務的轉送伺服器（即：代理伺服器，Proxy Server）以提供 Telnet、FTP、WWW、Gopher 等網路服務的轉送與控管。
3. 網路防火牆的安裝與網路架構之規劃及設置，應依資料安全規定及資料安全等級分類，以最經濟有效的方式配置。
4. 防火牆應由網路系統管理人員執行控管設定，並依制定的資訊安全規定、資料安全等級及資源存取的控管策略，建立包含身份辨識機制、來訊服務、去訊服務與系統稽核的安全機制，有效地規範資源被讀取、更改、刪除、下載或上傳等行為以及系統存取權限等資訊。
5. 網路系統管理人員應由系統終端機登入防火牆主機，禁止採取遠端登入方式，以避免登入資料遭竊取，危害網路安全。
6. 防火牆設置完成時，應測試防火牆是否依設定的功能正常及安全地運作。如有缺失，應立即調整系統設定直到符合既定的安全目標。
7. 網路系統管理人員應配合資訊安全政策及規定的更新，以及網路設備的變動，隨時檢討及調整防火牆系統的設定，調整系統存取權限，以反應最新的狀況。
8. 防火牆系統軟體，應定期更新版本，以因應各種網路攻擊。

七、 系統存取控制

(一) 個人資料資訊系統存取控制規定

1. 訂定本校個人資料資訊系統存取控制規定，並以書面或其他電子方式記錄之。
2. 業務應用系統擁有者，應訂定系統存取控制政策，並明定使用單位及使用人員的系統存取權利。並配賦應用系統的使用者（包括應用系統支援人員）與業務需求相稱的資料存取及應用系統使用權限。

(二) 使用者之存取管理

1. 使用者註冊管理

(1) 對於多人使用的資訊系統，應建立正式的使用者註冊管理程序。

(2) 使用者註冊管理程序，應考量的事項如下：

A. 查核使用者是否已經取得使用該資訊系統之正式授權。

B. 查核使用者被授權的程度是否與業務目的相稱，是否符合本校資訊安全政策及規定 （例如：有無違反權責分散原則）。

C. 應以書面或其他方式告知使用者之系統存取權利。

D. 在系統使用者尚未完成正式授權程序前，資訊服務提供者不得對其提供系統存取服務。

E. 應建立及維持系統使用者之註冊資料紀錄，以備日後查考。

F. 使用者調整職務及離（休）職時，應儘速註銷其系統存取權利。

G. 應定期檢查及取消閒置不用的識別碼及帳號。

H. 閒置不用的識別碼不應重新配賦給其他的使用者。

2. 使用者通行碼之管理

(1) 應建立使用者通行碼之管理制度。

(2) 建立通行碼管理制度，應考量下列事項：

A. 為維持通行碼的機密性，宜以配賦臨時性通行碼並強迫使用者立即更改通行碼的方式處理；使用者忘記通行碼時，可提供臨時性的通行碼，以利系統辨認使用者。

B. 應以安全的方法將臨時的通行碼交付使用者，避免經由第三者，或是以未受保護的電子郵遞等電子方

式交付給使用者，並應建立確認使用者是否收到臨時的通行碼的機制。

C. 使用者之通行碼應具備一定之安全強度。

D. 系統應要求定期更換通行碼，且儘量避免重複或循環使用舊的通行碼。

E. 系統如經評估須建立更高等級的安全機制，可利用電子簽章等安全等級更高的存取控制技術。

3. 系統存取權限之檢討評估

為有效控管資料及系統存取，應定期檢討及評估使用者之存取權限。

(三) 電腦系統之存取控制

1. 建立自動化的端末機身分鑑別系統

針對存取個資系統之端末機，應建立自動化的端末機身分鑑別系統，以鑑別從特定位址連上網路的使用者身分。

2. 端末機登入程序

(1) 使用者存取電腦系統應經由安全的系統登入程序。

(2) 登入程序應具備下列的功能：

A. 不應顯示系統及應用系統識別碼，直到成功登入系統。

B. 在系統登入程序中，應顯示“只有被授權的使用者才可存取系統”等警告性的資訊。

C. 系統不應在登入程序中，提供未經授權的使用者登入系統的說明或協助使用者的訊息。

D. 只有在完成所有的登入資料輸入後，系統才開始查驗登入資訊的正確性；如果登入發生錯誤，系統不應顯示那一部分資料是正確的，那一部分資料是錯誤的。

E. 應限制系統登入不成功時可以再嘗試的次數，原則上以三次為原則，系統並應：

a. 記錄系統登入不成功的事件。

b. 在使用者嘗試登入系統失敗後，應強迫必須間隔一段時間之後才能再次登入。

c. 應中斷資料連結作業。

F. 在系統登入被拒絕後，應立即中斷登入程序，並不得給予任何的協助。

G. 應限制系統登入程序的最長及最短時間，如果超出時間限制，系統應自動中斷登入。

3. 使用者身分辨識

(1) 應對使用者核發使用者識別碼，以明責任歸屬；使用者識別碼不應顯示任何足以辨識使用者特別權限的訊息，例如顯示其為管理者或監督者。

(2) 只有在例外的情況下，可為本校的整體效益，經權責主管人員之同意，核發群組內人員共享同一使用者識別碼，但應採取額外的安全控制措施，明確規範使用者的責任。

4. 連線作業時間之控制

(1) 有高風險的應用系統，應限制使用者的連線作業時間。

(2) 對處理高風險個資的端末機，應限定連線作業及網址連線時間，以減少未經授權存取系統的機會。

(3) 限定連線作業時間的措施如下：

A. 只允許在設定的時間內與系統連線。

B. 如無特別延長作業時間的需求，應限制只能在正常的上班時間內進行連線作業。

C. 應限制連線的網址。

(四) 系統存取及應用之監督

1. 存取記錄

(1) 應建立及製作系統存取異常的稽核軌跡，並保存一段的時間，以作為日後調查及監督之用。

(2) 系統稽核軌跡應包括下列事項：

A. 使用者識別碼。

B. 登入及登出系統之日期及時間。

C. 儘可能記錄端末機的識別資料或其位址。

2. 系統使用之監督

(1) 應建立系統使用情形之監督程序，確保使用者只能執行授權範圍內的事項；個別系統接受監督的程度，應依風險評估結果決定。

(2) 系統使用之監督作業，應經權責主管人員之正式授權始得為之。

八、 實體環境管理措施

(一) 界定安全區域

明確定義本校安全區域，其應包含辦公區域及機房區域。

(二) 辦公區域管理

1. 辦公區域之出入權限應適當控管，並適當安裝門禁系統或門禁系統，未經授權人員，應由授權人員陪同，禁止留在辦公室單獨作業。

2. 於辦公室內需隨時注意身分不明或可疑人員，若發現不明身分之人員時，需主動詢問並儘速通知相關單人員進行處理。

(三) 機房安全管理

1. 機房之安全設計需採用架高地板、隱藏佈線、地板承重度及排水、防火功能等，且電力、網路、通信設備應予以保護，以防止遭有心人士截取或破壞。

2. 機房應擁有獨立發電設備，並配有 UPS 不斷電系統。

3. 機房內應裝置適當之防災設備，並定期檢修測試。

(四) 機房門禁管制

1. 機房應具備門禁管制設備，並安裝架設監視設備。

2. 為確保相關設施之安全，非權責單位指定之人員不得擅自進入機房安全區域或使用相關資訊設備。

(五) 文件設備報廢

1. 硬體、通訊資產或儲存媒體報廢

(1) 硬體、通訊資產或儲存媒體需報廢時，使用單位應填寫「個資資產報廢申請單」，經資訊單位審核並確認個人資料清除後，方可進行個資資產報廢程序。

(2) 個資資產保管單位依據「個資資產異動申請單」經資訊單位審核後，可重複使用之資料儲存媒體。

(3) 儲存媒體如要報廢或移作他用時，儲存媒體上之個人資料必須清除。

(4) 當儲存媒體須報廢或再利用時，應採用以下任一種合宜之措施進行銷毀：

A. 硬碟、USB：利用消磁機或專業資料清除軟體工具，清除硬碟資料。

B. 光碟：光碟一律將反光層抹除或折斷銷毀。

C. 磁帶或磁片：磁帶或磁片應以工具破壞實體，使其無法使用。

D. 儲存個人資料的儲存媒體，嚴格禁止僅使用一般格式化方式進行個資資訊資產報廢程序，應採用上述方式進行銷毀。

2. 文件報廢

文件類個資資產報廢時，文件管理者應填寫「個資資產報廢申請單」，經權責單位審核後，以碎紙機或水銷進行銷毀，並刪除電子檔及其複本，該單位之主管人員應善盡督導之責。

3. 文件設備報廢應留存適當紀錄。