國立中興大學

個人資料安全控管作業說明書

機密等級：內部使用

文件編號：**NCHU-PIMS-C-001**

版　　次：**1.1**

發行日期：**106.10.02**

本文件歷次變更紀錄：

版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	101.10.22	N/A	資安暨個資保護執行小組	初版發行
1.1	106.10.02	P.1,P.9,P.10	資安暨個資保護推動委員會	修訂目的、參考文件及相關表單內容

目　　錄

壹、目的.....1

貳、適用範圍 1

參、權責.....1

肆、定義.....1

伍、作業內容 1

陸、參考文件 9

柒、相關表單 9

壹、目的

依據「個人資料保護法」、「個人資料保護法施行細則」及國立中興大學(以下簡稱本校)「個人資料保護管理政策」等相關規定，制訂本校個人資料安全控管程序，以確保個人資料受適當的控管與監視，防止不當管控而造成資料外洩之風險。

貳、適用範圍

本校個人資料（含書面、電子個人資料）均適用之。

參、權責

一、 本校全體同仁（含正式員工、約聘僱人員、工讀生與委外廠商人員）

均應遵守本程序書之相關規定，以確保本校相關個人資料（含書面、電子個人資料）之安全。

肆、定義

無。

伍、作業內容

一、實體環境安全控制政策

(一) 個資外洩事故發生時，其發現者可依據本校【個人資料保護緊急應變處理作業說明書】進行相關通報作業事宜，並由該事故權責單位進行後續處理改善。

(二) 各單位公務文書及紙本郵件應有專人負責收發。

(三) 使用影印機、印表機、傳真機、掃描機或多功能事務機後，應立即將資料取走。

(四) 未經授權不得將機敏文件攜出辦公環境區域。若有需要，須經主管人員核准，始得進行。

(五) 處理完之個人資料檔案(紙本、電子)，若無需保留應立即絞碎

或刪除(電子檔案應確實清除「資源回收筒」)，含有個人資料之報廢紙張不得回收及再利用。

(六) 針對存有個人資料之紙本文件及可攜式儲存媒體，不使用或下班時，應遵守桌面淨空政策，放置於抽屜或儲櫃並上鎖，以避免外洩。

(七) 為確保本校相關資訊設施及資料保護之安全，非業管權責單位指定或授權之人員不得擅自進入處理與存放機敏資訊之場所。

(八) 本校同仁應保持警覺，留意陌生人員進出辦公環境，若發現身份不明或可疑的人員，應主動詢問其身份，並視需要通知駐警隊處理。

(九) 委外廠商及訪客應於本校各單位指定之區域內活動。

(十) 存放機敏資訊之儲存空間應建立門禁管理，如透過鑰匙或門禁卡等方式進行管理。

二、一般安全控制

(一) 資料備份

1. 各單位應對存有個人資料之系統伺服器應進行備份，並至少保留 2 代。備份作業應儘量於離峰時段進行。
2. 備份資料至少每年執行資料回復測試，以確認備份資料之可用性。
3. 存放重要機敏資料之備份媒體應另異地存放一份於安全場所。備份媒體運送過程中應存放於上鎖之媒體保護箱由專人親送。

(二) 人員安全與教育訓練

1. 本校同仁、接觸個人資料之外部人員、委外服務廠商人員於在職及離、退職後，均不得洩漏所知悉之機敏資訊，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。
2. 本校同仁於到職時應簽署保密切結，並恪盡保密之責。
3. 每年應對組織內部人員規劃訓練課程，或派員參加外單位辦理之專業課程，以提升人員個人資料保護之安全認知及警覺意識。

4. 為確保教育訓練執行之成效，可採行隨堂抽問、案例討論、習題演練或隨堂測驗等方式進行成效評估。

5. 本校個人資料保護安全教育訓練一般人員至少 3 小時，其簽到表及執行成效等紀錄應由資安暨個資保護執行小組留存備查。

(三) 委外管理

1. 委外廠商人員於專案服務期間所知悉之業務資訊，應遵守「個人資料保護法」及本校相關規定，且不得對外透露。廠商及專案人員並應分別簽署廠商保密切結書或人員保密切結書。

2. 委外廠商履行契約所使用之軟體不得違反著作權法之規定，若因使用非法軟體造成本校單位個人資料外洩，委外廠商須承擔所有法律責任。

3. 委外廠商於專案服務期間所使用之工具軟體及作業執行紀錄，本校有權進行稽核，廠商不得異議。

4. 於專案期間，本校應透過稽核等方式監督委外廠商之個人資料管理作法，如個資蒐集、處理、利用、傳輸與銷毀之管理情形。

5. 委外廠商如因其員工業務過失，造成本校損害時，委外廠商需負賠償或復原責任。

6. 委外廠商進行系統開發、測試與維護時，未經權責主管許可，不得複製或攜出本校保有之教、職、員、工、生等相關個人資料。

7. 提供委外廠商測試之資料，應將個人資料欄位內容轉換為虛擬資料或移除。

三、存取控制政策

(一) 個人資料之存取應與本身業務範圍相關，任何人未經授權不得存取與個人業務無關之個人資料。

(二) 若因特殊需要提供帳號予外部或非業務負責之人員，應填列「主機/系統帳號暨權限申請表」，並考量作業需求及個人資料之機敏性，授與適當之存取權限及有效期限。

(三) 權責主管應審慎評估重要系統特殊權限之授權管理。

(四) 因處理系統當機與異常狀況需視狀況授與適當之存取權限，並

避免共用帳號，如特殊情況，需共用帳號時，應建立可歸責性之機制，以利識別身份。

(五) 可攜式設備及儲存媒體，如筆記型電腦、隨身碟、光碟、磁帶等，應採取適當控管措施，避免個人資料未經授權存取。

(六) 個人資料之存取必須符合「個人資料保護法」、「個人資料保護法施行細則」等相關法令之要求與規定，或契約對資料保護及資料存取使用控管之權責規定。

(七) 公用程式路徑或公(共)用目錄之存取權限應適當控管，防止非授權使用者存取。含個人資料之檔案不得存放於公(共)用目錄。

(八) 針對無人看管的資訊設備，應有適當控管程序，以防未經授權之存取或濫用。公共使用之影印機、印表機、傳真機或多功能事務機應每日應檢視有無個人資料遺留。

(九) 為確保個人資料之安全，對敏感性系統或處理大量個人資料之資訊設備，應採取適當控管程序或隔離措施。

(十) 伺服器、個人電腦及筆記型電腦應設定螢幕保護程式，並設定密碼或採取登出鎖定方式保護；自行啟動螢幕保護程式的時間設定應不超過 15 分鐘。

四、使用者帳號管理

(一) 使用者帳號申請

1. 新進同仁報到後，由人事室建立人事資料，依工作職掌所需開立帳號並授予適當之權限。

2. 本校具機敏性資料之應用系統帳號須經申請並核可後，方可建立帳號使用。非業務權責單位人員如需使用其資訊系統時，須經業務權責單位主管核可後方得使用。

(二) 使用者帳號異動

1. 除特殊規定外，員工離、退職時，系統管理人員於收到相關單位通知後，應進行帳號註銷或停用。

2. 員工內部調職時，應提出異動申請，系統管理人員應確實刪除其原單位之存取權限。

3. 員工留職停薪時，系統管理人員於收到人事室通知後，應停用其帳號。

(三) 特殊權限帳號管理

1. 系統管理人員應避免共用管理者帳號，重要系統管理者帳號與密碼之文件，應密封並存放於上鎖之安全處所。

2. 具機敏性資料之伺服器及資料庫，其特殊權限帳號應每年清查，查核結果填列於「帳號清查紀錄表」，並陳權責主管審核。

3. 新購置之資訊設備或系統，應於安裝完成後刪除或關閉不必要之帳號及更改預設密碼。

五、密碼管理

(一) 首次登入系統時，應立即變更密碼設定，並妥善保管帳號與維持密碼之機密性。

(二) 應用系統或個人建立之帳號密碼檔案，宜加密方式處理。

(三) 應避免將帳號密碼張貼或放置於伺服器、網路設備、個人電腦、螢幕或其他場所。

(四) 除特殊需求外，應避免使用者共用帳號密碼。

(五) 密碼疑遭盜用或破解時，應立即變更密碼。

(六) 登入系統時應避免使用記錄密碼之功能，以免開機時自動登入系統。

(七) 使用者密碼須為英數字混合，且不得與帳號名稱相同、密碼長度至少為 8 碼，且不得與前次設定相同，原則上密碼至少半年變更 1 次；使用者密碼遺忘時，應提出申請並由主管核可或經本人身份確認無誤後，始得進行密碼變更，並保留相關紀錄以備查核。

(八) 密碼複雜度組成應符合以下類別之三種：

1. 英文大寫字元 (A - Z)。

2. 英文小寫字元 (a - z) 。

3. 10 個基本數字 (0 - 9) 。

4. 特殊字元(例如：!、$、#、%)。

(九) 密碼設定應儘量避免使用易猜測或公開資訊，如姓名、出生年月日、身分證字號、機關或單位名稱、電腦主機名稱、作業系統名稱、電話號碼等。

六、使用者存取權限

(一) 對於職務異動如調、離職、留職停薪人員等，依本程序書之使用者帳號異動辦理，據以異動、註銷或停用存取權限。

(二) 使用者存取業務相關之個人資料須經授權，其帳號應為唯一之識別碼，禁止借用他人之帳號或共用帳號。

(三) 久未登入系統之帳號應妥善管理，經確認無須使用後，應予以刪除。

七、作業系統存取控制

(一) 除因老舊系統或特殊情形外，應啟動系統紀錄功能。

(二) 系統紀錄存取，應限定僅由系統管理人員或被授權者存取。

(三) 帳號名稱應避免顯示任何足以辨識為特殊權限的訊息，如管理者或監督者。

八、應用系統之存取控制

(一) 應用系統資訊之使用，僅限業務相關之授權使用者，並應適當控制。

(二) 應用系統之敏感等級以上資訊，應與一般資訊作適當區隔，並加強權限控管措施。

(三) 會談期逾時之控制

應視系統情形，進行會談期逾時(Session timeout)控制，以防止未經授權使用者的存取及阻絕服務之攻擊。

九、網路存取控制

(一) 網路系統應依安全需求區隔不同區域，並設置網路安全設備如防火牆及網路閘門等加以保護。

(二) 網路之存取活動，應定期檢視，並留存日誌備查。

(三) 對於開放提供外部客戶或廠商存取之服務，必須限制使用者之網路功能以確保網路安全。

(四) 網路路由之規劃必須確保任何網路連線或資訊傳輸符合網路存取之安全需求。

十、遠端存取之限制

(一) 非經授權禁止執行遠端存取作業。

(二) 連線存取個人資料時，應限定標的範圍，並填列「遠端連線申請表」，並陳權責主管審核。

十一、資料庫存取控制

(一) 資料庫帳號管理

1. 資料庫存取應啟動作業系統或資料庫之身份識別機制。
2. 具機敏性資料之資料庫系統存取帳號，應依功能區分為應用系統及資料庫管理之帳號，並給予適當之權限。
3. 具機敏性資料之資料庫系統存取授權，應以執行業務及職務所需者為限，當使用者職務異動時，須依照本程序書六、之使用者存取管理原則辦理。
4. 具個人資料之資料庫系統帳號之密碼須為英數字混合，且不得與帳號名稱相同，密碼長度至少為 8 碼，並嚴禁管理人員轉知他人。
5. 具機敏性資料之資料庫最高權限帳號存取授權，應僅限於資料庫管理人員或職務代理人。
6. 應變更資料庫預設帳號之密碼或關閉使用。

(二) 資料庫異動與測試

1. 應用系統測試及正式作業所需資料庫管理系統，宜分別在不同伺服器下執行，並避免資料遭意外竄改或不當使用。
2. 具機敏性之測試資料，應僅由系統管理人員進行存取，且應將個人資料內容轉換為虛擬資料、模糊化或遮蔽。
3. 正式資料庫系統變更作業前，如資料庫系統版本更新、安裝修補程式等，應先評估對現行系統之影響後始得變更，重大變更

作業須經權責主管核准後始可實施。

4. 資料庫變更作業應經由權責主管同意後授權進行。

5. 資料庫公用程式存取權限應適當控管，禁止一般使用者存取。

6. 應用系統應考量有專屬資料庫，並應有防止使用者直接存取資料庫之設計。

7. 對外提供服務之重要應用系統，其後端資料庫應考量連接可限制存取之網路設備統一控管，避免資料庫遭受入侵。

十二、系統開發安全管理

(一) 資訊系統應保護敏感等級以上之資料，防止洩漏或被竄改，必要時應使用資料加密等相關機制保護。

(二) 系統測試環境所使用之設備環境應予獨立，不應與提供服務之設備環境共用。

(三) 具機敏性資訊之應用系統，應設計加密傳輸機制(如 SSL 或 https 等)，必要時應針對資料內容加以保護如資料庫加密，並記錄傳輸的相關資訊，包含傳輸來源、接收目的位址、傳送時間與傳輸成功或失敗等資訊。

(四) 應用系統安裝及佈署時，應評估執行下列安全檢測

1. 資料庫伺服器檢測

檢測內容含：Patch 更新考量、不必要之通訊協定、服務及通訊埠關閉、預設資料庫移除、使用者與系統管理員帳號密碼安全強度、安全稽核功能設定及日誌檔備份等。

2. 網站及應用伺服器檢測

檢測內容含：跨網站指令碼(Cross Site Scripting，XSS)、注入缺失(Injection Flaw)、Patch 更新考量、不必要之通訊協定、服務及通訊埠關閉、使用者與系統管理員帳號密碼安全強度及日誌檔備份、每個網頁之安全控管等。

(五) 應對具個人資料之重要資訊系統定期實施弱點掃描或滲透測試，以鑑別各單位應用系統與作業環境之風險，並針對弱點部分實施修補與改善，並保留相關紀錄以備查核。

(六) 系統開發委外安全控管

為確保應用系統之安全性與可靠性，應於契約或建議書徵求文件中明訂下列安全管理事項：

1. 系統需求分析時，應考量現況及未來應用系統之運作環境配置、資料之重要性及遭受攻擊之可能性，據以發展應用系統之安全需求及系統功能。
2. 程式測試時，應進行相關安全性檢測，並提供相關測試報告與記錄。
3. 應用系統須進行源碼檢測，並提供相關檢測報告，以驗證程式碼之安全性。
4. 委外廠商每次交付之應用程式版本，應進行應用程式安全弱點掃描及程式碼安全檢測，若有弱點存在，委外廠商須負責修改。
5. 契約期間如發生程式錯誤或資料漏失，經確認屬委外廠商責任者，應由委外廠商負責更正；另損及他人權益時，亦由委外廠商負責。
6. 委外廠商對業務上所接觸之資料，應採必要之保密措施。委外廠商及專案相關人員均應依本校規定填具保密切結。
7. 委外廠商應配合本校安全控管要求，辦理應用系統弱點修補、異常排除、事件通報及進行相關演練作業事宜。

陸、參考文件

一、個人資料保護法。

二、個人資料保護法施行細則。

三、個人資料保護管理政策。

四、個人資料保護緊急應變處理作業說明書。

柒、相關表單

一、主機/系統帳號暨權限申請表。

二、帳號清查紀錄表。

三、遠端連線申請表。