

財團法人演譯基金會

美兆人體生物資料庫之資訊安全管理規定

索 引

壹、資訊安全管理規定之制定及評估.....	3
一、資訊安全管理規定之制定.....	3
二、資訊安全管理規定之評估.....	4
貳、資訊管理單位之組織、權責及分工.....	6
一、資訊組之任務.....	6
二、資訊組權責.....	6
參、人員管理及資訊安全訓練.....	9
一、人員進用之評估.....	9
二、使用者資訊安全教育及訓練.....	9
肆、電腦系統安全管理.....	10
一、安全作業程序及責任.....	10
二、系統規劃.....	12
三、電腦病毒及惡意軟體之防範.....	13
四、軟體複製的控制.....	13
五、個人資料之保護.....	14
六、日常作業之安全管理.....	14
七、電腦媒體之安全管理.....	15
八、資料及軟體交換之安全管理.....	16
伍、網路安全管理.....	18
一、網路安全規劃與管理.....	18
二、電子郵件之安全管理.....	21
三、全球資訊網之安全管理.....	21
四、網路安全稽核.....	22
五、憑證機構之安全管理.....	23
陸、資訊系統存取控制管理.....	24
一、資訊系統存取控制.....	24

二、使用者之存取管理.....	24
三、系統存取之責任.....	25
四、網路存取之安全控制.....	26
五、電腦系統之存取控制.....	27
六、應用系統之存取控制.....	29
七、系統存取及應用之監督.....	30
八、外部人員存取資訊之安全管理.....	31
九、系統稽核規劃.....	31
柒、資訊系統購置、發展及維護安全管理.....	33
一、系統安全需求.....	33
二、應用系統之安全.....	33
三、應用系統檔案之安全.....	34
四、系統變更及支援環境之安全.....	35
五、系統委外開發管理之安全.....	36
捌、資訊資產之管理.....	38
一、人體生物資料庫資訊資產之保護.....	38
玖、實體及環境安全管理.....	39
一、設備安全管理.....	39
二、周邊安全管理.....	40
拾、資訊安全事件發生之通報及保全處理程序.....	43
一、資訊安全事件之通報.....	43
二、資訊安全弱點之反映.....	43
三、軟體功能不正常之反映.....	43
四、資訊安全事件分級.....	43
五、資訊安全事件之通報程序.....	44
六、資訊安全事件之處理程序.....	44
拾壹、業務持續及回覆管理.....	45
一、業務永續運作之規劃.....	45
二、業務永續運作計畫之測試.....	46
三、業務永續運作計畫之變更.....	46
拾貳、其他有關資訊安全事項.....	48

壹、資訊安全管理規定之制定及評估

一、資訊安全管理規定之制定

（一）依據

衛生署99年7月2日衛署科字第 0990860555 號函頒「人體生物資料庫資訊安全規範」辦理。

（二）資訊安全目的

為建立安全及可信賴的電子交換環境，以確保人體生物資料、系統、設備的安全，資訊的適當安置及資訊安全實務作業的可行性與有效性，此安全規定須配合相關單位資訊安全規範的調整或資訊安全政策補強之所需而定期檢視並更新，所有更新需經倫理委員會同意始生效。

（三）資訊安全組織

由美兆人體生物資料庫資訊安全推動小組，制定人體生物資料庫資訊安全政策。

資訊安全推動小組由基金會設置。使用人員名冊如下：

基金會代表人
資訊組組長
生物醫學組組長
倫理委員會委員
稽核組組長

（四）資訊安全定義

綜合考量各項資訊資產之重要性及價值，以及因人為疏失、蓄意或自然災害等風險，致資訊資產遭不當使用、洩漏、竄改、破壞等情事，影響及危害人體生物資料庫業務之程度，採與資訊資產價值相稱及具成本效益之管理、作業及技術等安全措施。

（五）資訊安全管理措施

- 1、制定人員管理及資訊安全教育訓練。
- 2、制定電腦系統安全管理。
- 3、制定系統存取控制管理。
- 4、制定系統發展及維護安全管理。
- 5、制定資訊資產安全管理。

- 6、 制定實體及環境安全管理。
- 7、 制定資訊安全事件發生之通報及保全處理程序
- 8、 制定業務永續運作計畫管理。

二、資訊安全管理規定之評估

（一） 評估方式

由人體生物資料庫資訊安全推動小組或委請外部公正超然的專業組織進行獨立及客觀的評估，以確保資訊安全之實務作業確實遵守人體生物資料庫資訊安全政策，並檢討人體生物資料庫資訊安全實務作業的可行性及有效性。

（二） 安全評估的項目

1、 人員

包含：資訊設施及系統提供者、資訊及資料擁有者、系統使用者、系統管理者、系統維護者、其他有關人員等人員。

2、 資訊系統作業環境

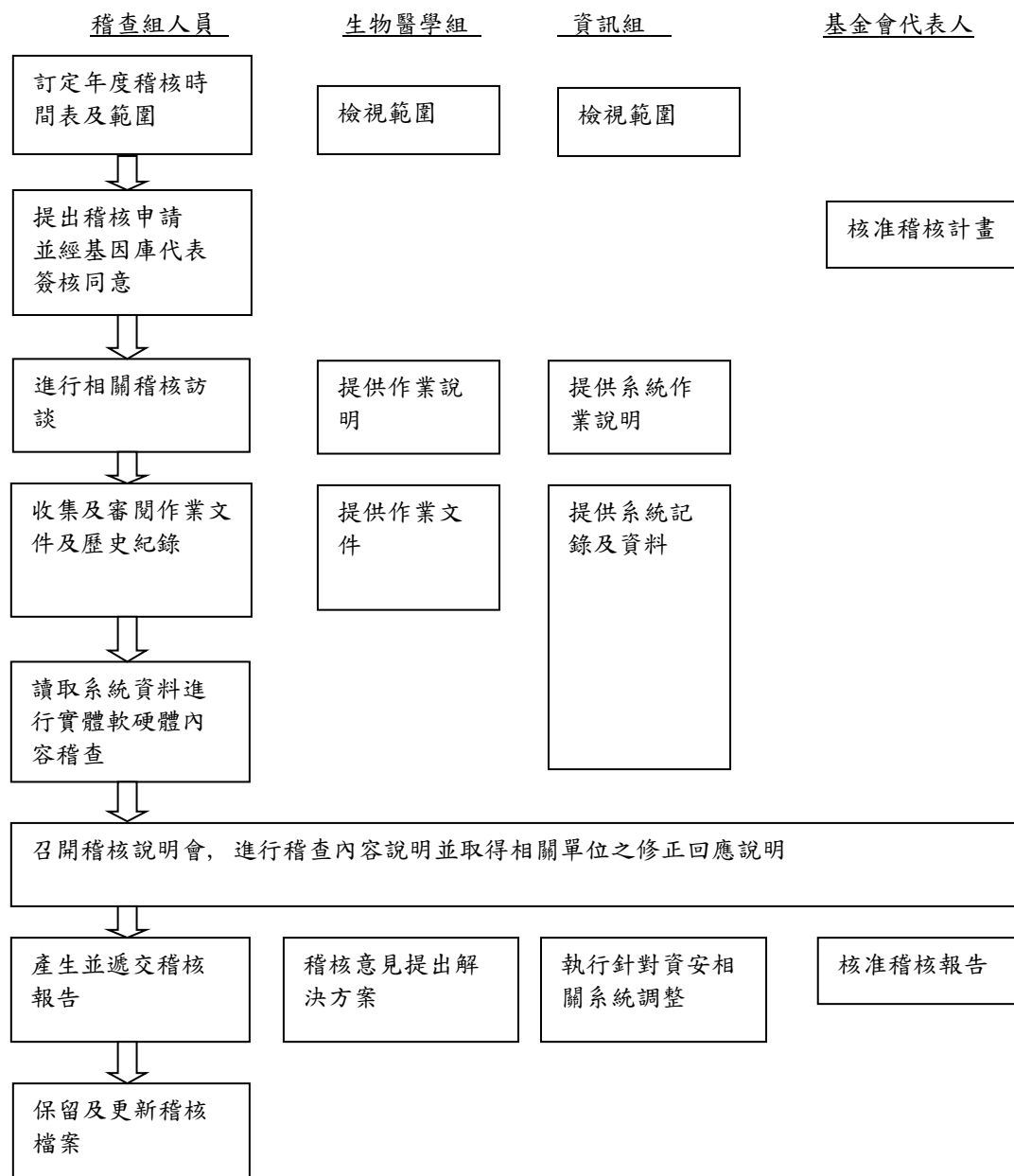
包含：硬體、作業系統、資料庫管理系統、資訊應用系統等。

3、 資料交換及提供的程序及契約

包含：設置者因業務所需而簽訂之各項契約以提供生物檢體、資料或資訊等，需檢視其契約中明定的資安規定並依「一、資訊安全管理規定之制定」內列之「（五）資訊安全管理措施」中各項管理規範對其契約對象進行資訊安全的規定進行檢視。

（三） 定期對相關部門及人員進行資訊系統及技術應用之安全評估

- 1、 資訊系統擁有者必須配合定期的資訊安全評估作業，檢討相關人員是否遵守人體生物資料庫的資訊安全政策、規範及其他安全規定。
- 2、 定期檢討評估各項軟、硬設備的安全性，以確保其符合人體生物資料庫的安全標準。
- 3、 系統安全評估需由具有專業知識及豐富經驗的系統工程人員，在權責主管人員的監督下，以人工的方式執行，或是以自動化的軟體工具執行安全檢查，產生技術評估報告，以利日後解讀分析。
- 4、 實施此資訊安全管理規定時，如有必要，各單位應訂定說明文件，如管理規範、作業程序、資通安全控管文件等。
- 5、 資訊安全評估的稽查進行步驟及相關單位權責如下：

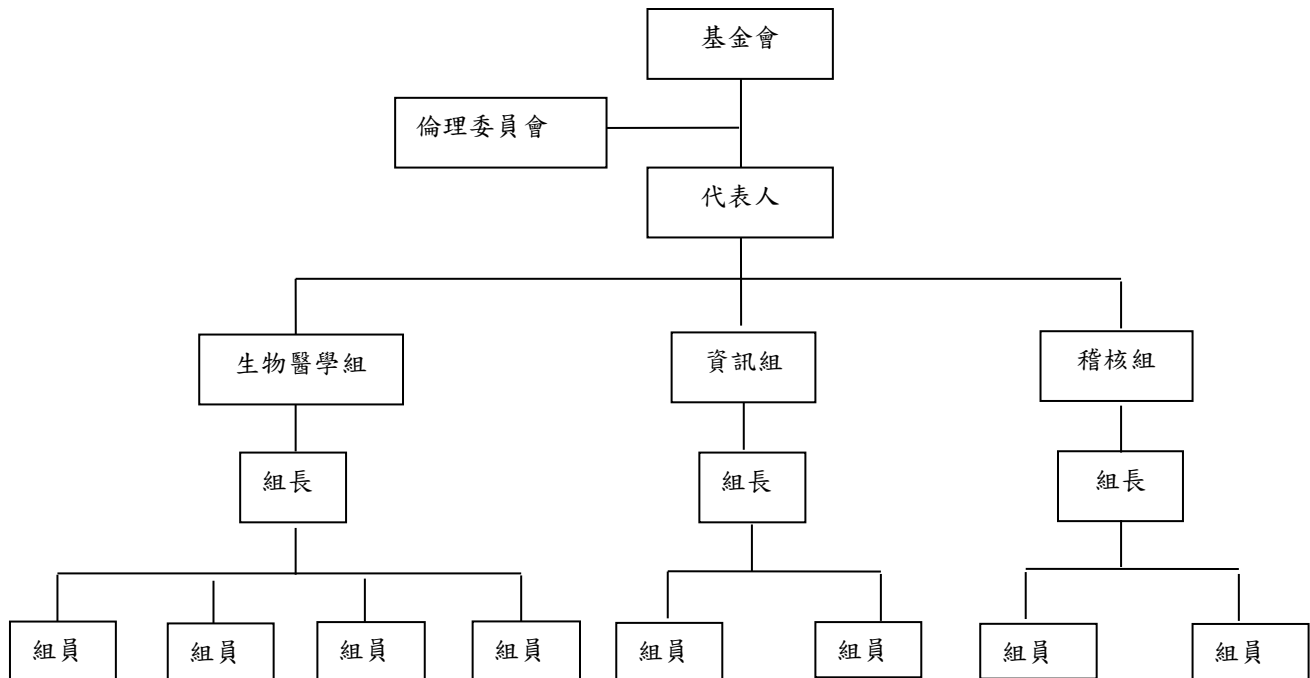


(四) 資訊安全政策及規定之宣達

- 1、人員的資訊安全角色及責任的相關規定，必須在人員的工作說明書或相關作業手冊中詳細敘明。包括執行及維護人體生物資料庫資訊安全政策的一般性責任規定、保護特定資訊資產的特別責任規定，以及執行特別安全程序及作為的特別責任規定。
- 2、人體生物資料庫員工如違反資訊安全相關規定，則依紀律程序處理。

貳、資訊管理單位之組織、權責及分工

資訊管理單位之組織及層級說明如下：



一、資訊組之任務

- (一) 人體生物資料庫資訊安全管理規定之核定及督導
- (二) 人體生物資料庫資訊安全責任之分配及協調
- (三) 人體生物資料庫資訊資產保護事項之監督
- (四) 人體生物資料庫資訊安全事件之檢討及監督
- (五) 其他重要資訊安全事項之核定

二、資訊組權責

(一) 資訊安全責任分配

- 1、訂定保護個人資訊資產及執行特定資訊安全作業相關人員應負之責任。
- 2、訂定資訊安全角色及責任分配之一般性指導原則作為各單位之權責分工依據。
- 3、指定每一系統之系統擁有者，並賦予必要的安全責任。
- 4、明定每一管理者應負的資訊安全責任。
- 5、訂定每一系統的資訊資產項目，並訂定必要的資訊安全程序及措施。
- 6、指定每一項資訊資產及資訊安全程序的管理人員，並以書面或其他方式課其責任。
- 7、訂定資訊安全之授權規定、授權等級及授權程序等，並以書面或其他方式記錄之。

（二） 資訊安全分工原則

1、資訊組組員

資訊安全相關政策、計畫、措施及技術規範之研議，以及安全技術之研究、建置及評估相關事項，由資訊組負責辦理。

2、資訊組組長

建議及支援起草資訊安全政策建議 支援資訊安全的建置及執行資訊安全政策並承擔人體生物資料庫資訊安全的最終責任。

3、倫理委員會

基金會設置「美兆人體生物資料庫倫理委員會」核准資訊安全政策與資訊安全措施的建置並核定、監督，稽查資訊安全政策之執行。

4、稽核組

實施資安內部稽核，依據資安檢核表評估整體資安風險，提出改善建議事項，並協助資安事件之偵防作業。

5、生物醫學組

運用人體生物資料庫資訊及系統，進行生物研究之單位及使用者。負有對系統服務及功能異常反應，及配合協助資安事件通報應變作業之責任。

（三） 資訊設施之使用授權

引進及啟用新資訊科技（如軟體、硬體、通信及管理措施），需於事前進行安全評估，瞭解新資訊科技的安全保護措施及水準。

（四） 跨機關之合作及協調

- 1、資訊安全管理人員需與外部的資訊安全專家或顧問加強協調聯繫，相互合作，分享經驗，以評估可能面臨的資訊安全威脅，研擬及推動資訊安全實務措施。
- 2、應與業務相關的機關、執法機關、資訊服務提供者及通信機構等，建立及維持適當的互動管道，以便在發生資訊安全事件時，能獲得外部的資源協助，即時解決相關問題。
- 3、記載資訊安全之相關資訊，在對外提供及交流時，予與適當的限制，以防止載有人體生物資料庫資訊安全細節的敏感性資訊，遭未經授權的人員取用。

（五） 資訊安全顧問及諮詢

- 1、資訊安全人力、能力及經驗如有不足之處，得委請外界的學者專家提供資訊安全顧問諮詢服務。

- 2、對聘請的外界資訊安全顧問，或人體生物資料庫負責資訊安全之人員，各單位人員需予必要的協助及支援。

(六) 權責分配原則

- 1、資訊組、生物醫學組及稽核組人員不得跨組互為兼任。
- 2、資訊組組員中，資訊管理人員與資訊硬體管理及操作人員不得互為兼任。

參、人員管理及資訊安全訓練

一、人員進用之評估

（一）人員進用之評估作業

- 1、人體生物資料庫甄選及進用之人員，如其工作職責須使用處理敏感性資訊的資訊科技設施或涉及機密性及敏感性資訊者，必須經適當的安全評估程序。
- 2、資訊人員之甄選及進用之安全評估參考項目如下：
 - （1）個人性格之評估。
 - （2）申請者經歷之評估。
 - （3）學術及專業能力及資格之評估。
 - （4）人員身分之確認。
 - （5）負責處理金錢及財物等敏感性工作的人員，得另評估其財物及信用狀況。

（二）機密維護之責任約定

- 1、員工使用資訊科技設施，需依相關規定課予機密維護責任，並簽署書面的約定，以明人員責任。
- 2、當人員任用及約聘僱條件或契約有所變更時，尤其是人員離職或是約聘僱用契約終止時，需立即取消其所有資訊資源使用權限。

二、使用者資訊安全教育及訓練

（一）資訊安全教育及訓練

- 1、定期對員工進行資訊安全教育及訓練，促使員工瞭解資訊安全的重要性，各種可能的安全風險，提高員工資訊安全的意識，並遵守資訊安全規定。
- 2、需以人員角色及職能為基礎，針對不同層級人員進行適當的資訊安全教育及訓練；資訊安全教育及訓練的內容包括人體生物資料庫的資訊安全政策、法令及規定、資訊安全作業程序及如何正確使用資訊科技設施之訓練等。
- 3、同意及授權使用者存取系統前，需教導使用者登入系統的程序，以及如何正確地操作及使用軟體。
- 4、對員工進行資訊安全教育及訓練的政策，除適用人體生物資料庫所屬員工外，對外部的使用者，亦規範一體適用。

肆、電腦系統安全管理

一、安全作業程序及責任

(一) 作業程序之訂定

資訊系統作業程序為正式文件，需以書面或其他方式載明之，其更改必須經權責單位核准，以確保人體生物資料庫員工正確及安全地操作及使用電腦，並以此作為系統發展、維護及測試作業的依據。

(二) 載明電腦作業程序的詳細規定

- 1、 如何正確地處理資料檔案。
- 2、 電腦作業時程的需求，包括與其他系統的相互關係、作業啟動的最早時間及作業結束的最晚時間。
- 3、 處理電腦當機及發生作業錯誤之規定，及其他電腦作業之限制事項。
- 4、 遭遇非預期的電腦作業技術問題時，如何與支援人員聯繫之規定。
- 5、 資料輸出處理的特別規定，例如：使用特別的文具，或是對機密資料輸出之管理、電腦當機或作業錯誤時所輸出資訊之安全處理規定等。
- 6、 電腦當機重新啟動及回復正常作業之程序。
- 7、 電腦及網路之日常管理作業，例如開關機程序、資料備援、設備維護、電腦機房之安全管理；作業程序必須視為正式文件，作業程序的更改必須經權責單位核准。

(三) 資訊安全事件之管理

- 1、 建立處理資訊安全事件之作業程序與紀錄，並課予相關人員必要的責任，以便迅速有效處理人體生物資料庫資訊安全事件。
- 2、 資訊安全事件包含：電腦當機、電腦中斷服務、資料遭侵犯、業務資料不完整，或是資料不正確導致的作業錯誤。
- 3、 除正常的應變計畫外（如系統及服務回復作業），資訊安全事件之處理程序尚需將下列事項納入：
 - ☒ 導致資訊安全事件原因之分析。
 - ☒ 防止類似事件再發生之補救措施的規劃及執行。
 - ☒ 電腦稽核軌跡及相關證據之蒐集。
 - ☒ 與使用者及其他受影響的人員，或是負責系統回復的人員進行溝通及瞭解。

- 4、電腦稽核軌跡及相關的證據，必須以適當的方法保護，以利下列作業：（1）作為人體生物資料庫內部分析問題之依據。（2）作為研析是否違反契約或是違反人體生物資料庫資訊安全規定的證據。（3）作為與軟體及硬體供應商，協商補償之依據。
- 5、以審慎及正式的行政程序，處理資訊安全及電腦當機事件。作業程序必須包括下列事項：
 - （1）在最短的時間內，確認已回復正常作業的系統及安全控制系統，是否完整及真確。
 - （2）向人體生物資料庫管理階層報告緊急處理情形，並對資訊安全事件詳加檢討評估，以找出原因及檢討改正。嚴格限定只有被授權的人員，才可使用已回復正常作業的系統及資料。所有緊急處理的行動，詳細記載以備日後查考。

（四）資訊安全責任之分散

為降低因人為疏忽或故意，導致資料或系統遭不法或不當之使用，或遭未經授權的竄改，對關鍵性的資訊業務需將資訊安全管理及執行作業的責任分散，建立相互制衡機制，分別配賦相關人員必要的安全責任。如資訊人力資源許可，下列業務及功能，需分由不同的人員執行：

- 1、設置者
- 2、業務系統之使用(包含生物資料庫研究人員及生物檢體管理人員)
- 3、資料建檔
- 4、電腦作業
- 5、網路管理
- 6、系統行政管理
- 7、系統發展及維護
- 8、變更管理
- 9、安全管理
- 10、安全稽核

（五）系統發展及實務作業之分散

系統發展及測試作業可能會有變更軟體及共享電腦資源之情形，為降低可能的安全風險，規定將系統發展及系統實際作業的設施分散，以減少作業軟體或資料遭意外竄改，或是遭未經授權的存取。系統發展及系統實際作業之分散，需考量下列安控措施：

- 1、系統發展及實際作業的軟體，必須在不同的處理器上作業，或是在不同的目錄或領域(Domain)下作業。
- 2、系統發展及測試作業必須分開。

- 3、編輯器及其他公用程式不再使用時，不可與作業系統共同存放在一起。
- 4、實際作業及測試用的系統，必須使用不同的登入程序，以減少風險。

二、系統規劃

（一）系統作業容量之規劃

- 1、隨時注意及觀察分析系統的作業容量，以避免容量不足而導致電腦當機。
- 2、進行電腦系統作業容量之需求預測，以確保擁有足夠的電腦處理及儲存容量。
- 3、特別注意系統之作業容量，預留預算及採購行政作業的前置時間，俾利進行前瞻性規劃，及時獲得必要的作業容量。
- 4、系統管理人員，需隨時注意及觀察分析系統資源使用狀況，包括處理器、主儲存裝置、檔案儲存、印表機等系統之使用狀況；管理人員應隨時注意上述設備的使用趨勢，尤應注意系統在業務處理及資訊管理上的應用情形。
- 5、隨時掌握電腦容量使用狀況的資訊，分析及找出可能危及系統安全的瓶頸，預作補救措施之規劃。

（二）新系統上線作業之安全評估

1. 訂定新系統被認可及納入正式作業的標準，並在新系統上線作業前，執行適當的測試。
2. 新系統被認可及納入正式作業的標準，執行事項如下：（1）評估系統作業效能及電腦容量是否滿足需求。（2）檢查發生錯誤後之回復作業及系統重新啟動程序的準備作業，以及資訊安全事件之緊急應變作業是否已經完備。（3）進行新系統正式納入例行作業程序之準備及測試。（4）評估新系統的建置不致影響現有的系統作業，尤其是對系統尖峰作業時段之影響。（5）辦理新系統作業及使用者教育訓練。
3. 在發展重要的系統時，確定系統的功能及確保系統的作業效能能夠滿足需求；例如：在系統發展的每一階段，充分諮詢相關人員的意見。
4. 新系統上線作業前，必須執行適當的測試作業，以驗證系統功能符合既定的標準。

（三）預備作業之規劃

- 1、需規劃資訊系統設備損害或電腦當機時，可維持業務永續作業替代性的預備作業方法。
- 2、每一系統的預備作業需求，需在業務永續運作的基礎上，由系統的擁有者加以界定；資訊服務提供者亦應為每一項系統研訂適當的預備作業計畫。
- 3、必須定期測試預備作業的設備及程序。

（四）作業變更之管理

- 1、資訊設施及系統的變更，要建立控制及管理機制，以免造成系統安全上的漏洞。
- 2、作業變更之管理，執行事項如下：
 - （1）界定及記錄重大變更的事項。
 - （2）評估作業變更之可能衝擊。
 - （3）建立作業變更之程序。
 - （4）與相關使用者事前溝通作業變更之細節。
 - （5）作業變更不能順利執行時之回復作業程序及責任，或放棄執行之作業程序及責任。

三、電腦病毒及惡意軟體之防範

- （一）採行必要的事前預防及保護措施，防制及偵測電腦病毒、特洛伊木馬及邏輯炸彈等惡意軟體的侵入。
- （二）依事前預防重於事後補救的原則，採行適當及必要的電腦病毒偵測及防範措施，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。
- （三）電腦病毒防範應考量的重要原則如下：
 1. 建立軟體管理政策，規定各部門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. 選用信譽良好、功能健全的電腦病毒防制軟體，並依下列原則使用：
 - （1）電腦病毒防制軟體應定期更新，並在廠商的指導下使用。
 - （2）使用防毒軟體事前掃描電腦系統及資料儲存媒體，偵測有無感染電腦病毒。
 - （3）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。
 - （4）謹慎使用可掃除電腦病毒及回復系統功能的解毒軟體；使用前充分瞭解電腦病毒的特性，以及確定解毒軟體的功能。
 - （5）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，則立即調查，找出原因。
 - （6）對來路不明及內容不確定的磁片，不准予使用。
 - （7）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。
 - （8）為使電腦病毒影響正常運作之程度降至最低，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。

四、軟體複製的控制

- （一）使用有智慧財產權的軟體，必須嚴格遵守相關法令及契約規定。
- （二）軟體複製考量之事項如下：
 - 1、不應保有及使用未取得授權的軟體。
 - 2、將智慧財產權保護政策，明確告知員工，禁止員工在未取得智慧財產權擁有者的書面同

意前，即將軟體複製到機器。

- 3、除非取得授權，不可將專屬的軟體複製到人體生物資料庫以外的機器設備。
- 4、需要在額外的機器上使用軟體時，確保取得正式的授權或是另行採購。
- 5、建立軟體使用的註冊機制，並定期稽核軟體使用情形。

五、個人資料之保護

- (一) 依據電腦處理個人資料保護法等相關規定，審慎處理個人資訊。
- (二) 建立個人資料控制及管理機制，並視需要指定負責個人資料保護之人員，以便協調管理人員、使用者及系統服務提供者，促使相關人員瞭解各部門應負的個人資料保護責任，以及應遵守之作業程序。

六、日常作業之安全管理

(一) 資料備份

- 1、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、系統資料備份及備援作業，需符合業務永續運作之需求。

(二) 系統作業紀錄

- 1、應設定電腦系統忠實記錄系統啟動及結束作業時間。
- 2、電腦作業人員應忠實紀錄系統錯誤及更正作業等事項，並定期交予資訊主管檢查，以確認其是否符合訂定的作業程序。

(三) 系統錯誤事項之紀錄

- 1、系統發生作業錯誤時，迅速報告權責主管人員，並採取必要的更正行動。
- 2、使用者對電腦及通信系統作業錯誤的報告，必須正式記錄下來，以供日後查考。
- 3、建立明確的系統作業錯誤報告程序及作業規定，要項如下：（1）檢查錯誤情形的紀錄，確保系統作業錯誤已經改正。（2）檢查更正作業是否妥適，確保更正作業未破壞系統原有的安控措施，及確保更正作業係依正當的授權程序辦理。

(四) 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，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。

七、電腦媒體之安全管理

(一) 電腦媒體之安全管理

- 1、可隨時攜帶及移動的電腦媒體，需建立使用管理程序，規範磁帶、磁碟及電腦輸出報告等媒體之使用。
- 2、電腦作業環境需建置下列安全控管措施：
（1）盡量避免使用有明顯用途標示的資料儲存系統；電腦媒體儲存的資料內容，不應在外部以明顯方式標示，以免被輕易地辨識出來。
（2）可重複使用的資料儲存媒體，不再繼續使用時，需將儲存的內容消除。
（3）對於要帶離人體生物資料庫辦公場所的儲存媒體，務必建立書面的授權規定，並建立使用紀錄，以備日後稽核之用。
（4）儲存媒體應依製造廠商提供的保存規格，存放在安全的環境。

(二) 機密性及敏感性資料之處理程序

- 1、建立機密性及敏感性資料的處理程序，防止機密性及敏感性資料遭洩漏或遭不法及不當的使用。
- 2、研訂處理機密性及敏感性資料的輸入及輸出媒體之安全作業程序，例如文件、磁帶、磁片及書面報告等項目。
- 3、機密性及敏感性資料之安全處理作業，包括下列事項：
 - (1) 輸出及輸入資料之處理程序及標示。
 - (2) 依授權規定，建立收受機密性及敏感性資料的正式收文紀錄。
 - (3) 確保輸入資料之真確性。
 - (4) 要求收受者提出傳送之媒體已送達的收訖證明。
 - (5) 機密性及敏感性資料的分發對象，以最低必要的人員為限。
 - (6) 為提醒使用者注意安全保密，在資料上明確標示資料機密等級。
 - (7) 定期評估機密性及敏感性資料的發文清單，及檢討評估機密性及敏感性資料的內容。
 - (8) 確保資訊系統內部資料與外部資料之一致性。

(三) 系統文件之安全

- 1、系統流程、作業流程、資料結構及授權程序等系統文件，予適當保護，以防止系統文件遭不當利用。
- 2、系統文件的安全保護措施如下：
 - (1) 系統文件應鎖在安全的儲櫃或其他安全場所。
 - (2) 系統文件的發送對象，以最低必要的人員為限，且經系統擁有者的授權。
 - (3) 電腦產製的文件，與其他應用檔案分開存放，且建立適當的存取保護措施。

(四) 媒體處理之安全

- 1、儲存機密性及敏感性資料的電腦媒體，當不再使用時，以安全的方式處理。
- 2、訂定電腦媒體的處理作業程序，以降低可能的安全風險。
- 3、電腦媒體之安全處理原則如下：（1）內含機密性或敏感性資料的媒體，以安全的方式處理，例如燒毀或是以碎紙機處理，或將資料從媒體中完全清除。（2）建立須以安全方式處理的媒體項目清單，包括：
 - 輸入文件
 - 輸出報告。
 - 磁帶。
 - 可攜帶的磁片或是磁帶。
 - 作業程序目錄。
 - 測試資料。
 - 系統文件。
- 4、委外處理的電腦文具、設備、媒體蒐集及委外處理資料，慎選有足夠安全管理能力及經驗的機構作為委辦對象。
- 5、機密性及敏感應性資料的處理過程，以書面記錄之，以利事後查考及稽核之用。
- 6、資訊累積一段時間再作彙總處理時，特別注意及防止大量非機密性資料彙總成為敏感應性或機密性資料。

(五) 資料檔案之保護

- 1、重要的資料檔案依相關規定，以安全的方式保存，以防止遺失、毀壞、被偽造或竄改。
- 2、超過法定保存時限的檔案，可依相關規定刪除或銷毀，惟需於事前考量是否對人體生物資料庫造成不利的影響。
- 3、資料檔案的管理，遵循以下的步驟：（1）訂定檔案保存、儲存、處理等指導原則作為執行的依據。（2）檔案保存期限應依檔案型態及法定保存期限之規定擬訂。（3）建立及維護重要資訊資源之目錄。（4）採行適當的措施，保護人體生物資料庫的重要檔案及資訊，防止資料遺失、毀壞及被偽造或竄改。

八、資料及軟體交換之安全管理

(一) 資料及軟體交換之安全協定

- 1、進行資料或軟體交換，訂定正式的協定，將機密性及敏感性資料的安全保護事項及責任列入協定。

- 2、資料及軟體交換的安全協定內容，考量下列事項：（1）控制資料及軟體傳送、送達及收受的管理責任。（2）控制資料及軟體傳送、送達及收受的作業程序。（3）資料、軟體包裝及傳送的最低技術標準。（4）識別資料及確定軟體傳送者身分的標準。（5）資料遺失的責任及義務。（6）資料及軟體的所有權、資料保護的責任、軟體的智慧財產權規定等。（7）記錄及讀取資料及軟體的技術標準。（8）保護機密或敏感性資料的安全措施（例如：使用加密技術）。

（二）電腦媒體運送及傳輸之安全

- 1、電腦媒體運送及傳輸過程，有妥善的安全措施，以防止資料遭破壞、誤用或未經授權的取用。
- 2、電腦媒體運送及傳輸，考量的安全措施參考要項如下：（1）審慎選用安全及可信賴的運送或傳送機構或人員，報請人體生物資料庫權責主管人員同意，並於事前執行傳遞人員或機構的安全評估程序。（2）運送的物品應有妥適的包裝，以防止傳送過程中受到損害。（3）對於機密及敏感性的資料，採取特別的安全保護措施。

（三）電子資料交換之安全

- 1、人體生物資料庫與來往對象進行電子資料交換，採行特別的安全保護措施，並經倫理委員會同意，以防止未經授權的資料存取及竄改；資料電子交換如有安全及責任上的需要，建立發文及收文證明的機制。
- 2、人體生物資料庫訂定的電子資料交換安全措施，需與電子資料交換的對象及資料加值服務業者共同協商，並徵詢電子資料交換相關協會及組織之意見，以確保符合相關的標準。

（四）電子辦公系統之安全

- 1、訂定電子辦公系統的使用政策及指導原則，確保實施辦公電子化在業務及系統上之安全。
- 2、系統考量的安全事項如下：（1）電子辦公系統如未能提供適當及足夠的安全保護措施，不可將敏感性資訊列入系統目錄。（2）訂定人體生物資料庫資料流通及分享的政策及管理措施。（3）對於特定個人（如負責處理機密性或敏感性資訊的人員）的行程資訊等，不宜開放公開存取，並予適當的限制。（4）評估以電子辦公系統處理重要業務的適當性。（5）建立被授權使用資訊系統的使用者名錄，並建立使用者存取系統權限等資訊。（6）特定的電子辦公設施，限制只有特定人員才能使用。（7）訂定系統儲存資訊的保管作業及備援作業規定。（8）電腦當機的備援作業規定。

伍、網路安全管理

一、網路安全規劃與管理

（一）網路安全規劃

- 1、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。
- 2、對於跨組織之電腦網路系統，特別加強網路安全管理。
- 3、利用公眾網路傳送敏感性資訊，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。
- 4、網路安全管理考量之事項如下：（1）將電腦作業及網路作業的責任分開。（2）建立管理遠端設備的責任及程序。（3）密切協調電腦及網路管理作業，以便發揮網路系統最大的服務功能，確保網路安全措施可以在跨部門的基礎架構上運作。

（二）網路服務之管理

- 1、系統的最高使用權限，必須經權責主管人員審慎評估後，交付可信賴的人員管理。
- 2、網路系統管理人員負責網路安全規範的擬訂，執行網路管理工具之設定與操作，確保系統與資料的安全性與完整性。
- 3、網路系統管理人員負責製發帳號，供授權的人員使用；除非有特殊情況，不得製發匿名或多人共享的帳號。
- 4、提供給內部人員使用的網路服務，執行嚴謹的身分辨識作業，不開放遠端登入內部網路系統的網路服務。
- 5、如果系統使用者已非正式授權的使用者時，網路系統管理人員應立即撤銷其使用者帳號；離（休）職人員確實依人體生物資料庫資訊安全規定及程序，取消其存取網路之權利。
- 6、網路系統管理人員未經權責主管人員許可，不得閱覽私人檔案；但如發現有可疑的網路安全情事，網路系統管理人員得依授權規定，使用自動搜尋工具檢查檔案。
- 7、網路系統管理人員未經使用者同意，不得增加、刪除及修改私人檔案。如有特殊緊急狀況，須刪除私人檔案，必須以電子郵件或其他方式事先知會檔案擁有者。
- 8、對任何網路安全事件，網路系統管理人員立即向人體生物資料庫設置之電腦安全事件緊急處理小組反應。
- 9、網路系統管理人員只能由系統終端機登入主機，並須保留所有登入、登出紀錄。
- 10、網路系統管理人員不得新增、刪除、修改稽核資料檔案，以避免違反安全事件發生時，造成追蹤查詢的困擾。

（三） 網路使用者之管理

- 1、被授權的網路使用者（以下簡稱網路使用者），只能在授權範圍內存取網路資源。
- 2、網路使用者應遵守網路安全規定，並確實瞭解自己應負的責任；如有違反網路安全情事，需依資訊安全規定，限制或撤消其網路資源存取權利，並依紀律規定及相關法規處理。
- 3、網路使用者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。
- 4、禁止網路使用者以任何方法竊取他人的登入身份與登入網路通行碼。
- 5、禁止及防範網路使用者以任何儀器設備或軟體工具竊聽網路上的通訊。
- 6、禁止網路使用者在網路上取用未經授權的檔案。
- 7、網路使用者不得將色情檔案建置在網路，亦不得在網路上散播色情文字、圖片、影像、聲音等資訊。
- 8、禁止網路使用者發送電子郵件騷擾他人，導致其他使用者之不安與不便。
- 9、禁止網路使用者發送匿名信，或偽造他人名義發送電子郵件。
- 10、網路使用者不得以任何手段蓄意干擾或妨害網路系統的正常運作。
- 11、與人體生物資料庫網路連線之電腦主機或網路設備，在連線作業時，確實遵守人體生物資料庫之網路安全規定及連線作業程序。

（四） 主機安全防護

- 1、存放生物資料庫之機密性及敏感性資料之大型主機，除作業系統既有的安全設定外，需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，以防止被偷窺或截取，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。

（五） 防火牆之安全管理

- 1、與外界網路連接的網點，必須加裝防火牆，以控管與人體生物資料庫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(如Telnet、FTP、WWW)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，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。
- 3、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(incoming service)、去訊服務 (outgoing service)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。
- 4、網路系統管理人員須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。

- 5、防火牆設置完成時，須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，立即調整系統設定直到符合既定的安全目標。
- 6、網路系統管理人員須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。
- 7、防火牆系統軟體，須定期更新版本，以因應各種網路攻擊。

(六) 軟體輸入控制

- 1、禁止網路使用者使用非法軟體。
- 2、經由網際網路下載軟體，宜由網路系統管理人員事前測試及掃瞄，確認安全無虞後方可安裝及執行。
- 3、網路上各檔案伺服器須安裝防毒軟體，防止病毒在網路上擴散。
- 4、網路使用者定期以電腦病毒掃瞄工具執行病毒掃瞄，並瞭解病毒與惡意執行檔可能入侵的管道，採行防範措施。
- 5、網路使用者如偵測到電腦病毒入侵或其他惡意軟體，必須立即通知網路管理者；網路管理者亦應將已遭病毒感染的資料及程式等資訊隨時提供使用者，以避免電腦病毒擴散。
- 6、電腦設備如遭病毒感染，必須立即與網路離線，直到網管人員確認病毒已消除後，才可重新連線。

(七) 網路資訊之管理

- 1、對外開放的資訊系統，須以防火牆與內部網路區隔，提高內部網路的安全性。
- 2、對外開放的資訊系統，針對蓄意破壞者可能以發送作業系統指令或傳送大量資料(如：電子郵件、註冊或申請資料等)導致系統作業癱瘓等情事，必須預作有效的防範，以免影響基因庫的服務品質。
- 3、機密性及敏感性的資料或文件，不得存放在對外開放的資訊系統中。
- 4、網路系統管理人員負責監督網路資料使用情形，檢查有無違反資訊安全規定之事件發生
- 5、針對對外開放的資訊系統所提供之網路服務，做適當的存取控管，以維護系統正常運作。
- 6、對外開放的資訊系統，如存放民眾申請或註冊的私人資料檔案，須以加密方式處理，並妥善保管，以防止有心人士竊取或移作他途之用，侵犯民眾隱私。
- 7、資料發佈於對外開放的資訊系統需經過內部規定之授權程序，依資料的機密性及安全性規定等級呈報至資訊安全單位或設置者，經許可發佈後，始可執行。該請求及授權程序必須如實記錄並存檔以供日後稽查之所需。

二、電子郵件之安全管理

- 1、依人體生物資料庫資訊安全政策及規定，明訂電子郵件的使用規定。
- 2、建立電子郵件的安全管理機制，以降低電子郵件可能帶來的業務上及安全上的風險。
- 3、電子郵件的安全管理規定，應評估下列事項：（1）訊息遭未經授權的截取及竄改的安全弱點。（2）發生資料錯誤、錯投及誤投的安全弱點。（3）電子郵件服務的可靠性及可用性。（4）對內及對外溝通方式改變，對行政流程的衝擊（例如：加快發送的速度，以及從人體生物資料庫的通信模式，改為個人對個人的模式等）。（5）電子郵件法律效力的考量，例如來源證明、送達、發送及收受等。（6）評估出版電子郵件目錄的安全性。（7）使用者從遠端存取電子郵件帳號之安全控管。
- 4、密等以上的公文及資料，不得以電子郵件傳送；敏感性資訊如有電子傳送之必要，得經加密處理後傳送。
- 5、為防範假冒人體生物資料庫員工名義發送電子郵件，並達到身分辨識及不可否認的目地，必要時以電子簽章方式簽發電子郵件。
- 6、電子郵件附加之檔案，須事前檢視內容有無錯誤後方可傳送。
- 7、對來路不明的電子郵件，交由網路系統管理者處理，不宜隨意打開電子郵件，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

1. 與外界網路連接之網點，設立防火牆控管外界與內部網路之資料傳輸及資源存取，並執行嚴謹的身分辨識作業。
2. 裝設掃毒軟體，定期掃毒，以提供使用者更安全的網頁瀏覽環境。
3. 建立系統備援設施，定期執行必要的資料、軟體備份及備援作業，以備發生災害或儲存媒體失效時，可迅速回復正常作業。
4. 不定期摹擬駭客攻擊，演練發生安全事件時的系統回復程序，並提供適當的安全防禦等級。
5. 機密性及敏感性的資料或文件，不存放在對外開放的資訊系統中，機密性文件不以電子郵件傳送。
6. 保護網站及個人資料安全，若涉及帳號或資料的傳輸，網站應使用通行標準的SSL保全系統，保障資料傳送的安全性。。

（二） 網路設備備援與系統備援

- 1、網路硬體設備應加裝不斷電系統，以防止不正常的斷電狀況。
- 2、網路系統中之防火牆與各主機應定期做系統備份，包括完整系統備份，系統架構設定備份以及稽核資料備份。

（三） 網路入侵之處理

- 1、網路如有被入侵或有疑似被侵入情形，應依事前訂定的處理程序，採取必要的行動。
- 2、網路入侵的處理步驟如下：
 - ☒ 立即拒絕入侵者任何存取動作，防止災害繼續擴大;當防護網被突破時，系統設定拒絕任何存取;或入侵者已被嚴密監控，在不危害內部網路安全的前題下，得適度允許入侵者存取動作，以利追查入侵者。
 - ☒ 切斷入侵者的連接，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連接。
 - ☒ 全面檢討網路安全措施及修正防火牆的設定，以防禦類似的入侵與攻擊。
 - ☒ 正式記錄入侵的情形及評估影響的層面。
 - ☒ 立即向權責主管人員報告入侵情形。

四、網路安全稽核

（一） 網路安全稽核事項

- 1、對網路系統管理人員或資訊安全主管人員的操作，均建立詳細的紀錄。
- 2、對於通過防火牆之來源端主機IP位址、目的端主機IP位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均予確實記錄。

（二） 網路入侵之追查

- 1、對入侵者的追查，除利用稽核檔案提供的資料外，得使用系統指令執行反向查詢，並連合相關單位(如：網路服務公司)，追蹤入侵者。
- 2、入侵者之行為若觸犯法律規定，構成犯罪事實，須立即告知檢警憲調單位，請其處理入侵者之犯罪事實調查。

五、憑證機構之安全管理

（一）憑證機構之安全評估

- 1、基於業務須要，須自行或委託專業機構建置憑證機構（certificate authority），或選用具公信力的憑證機構時，應綜合考量憑證機構之技術、管理、人員及財務的安全風險；考量事項如下：（1）獨立性。（2）承擔風險之財務資源及財物管理能力。（3）系統安全管理能力。（4）永續經營能力。（5）硬體、軟體及通信設施之可信賴性。（6）系統稽核管理能力。（7）緊應應變計畫。（8）人員管理及內部控制。

（二）憑證機構之技術安全

- 1、針對憑證機構金鑰之產生、儲存、使用、備份、銷毀、更新及復原作業等，建立嚴格的安全管理機制。
- 2、憑證機構資訊系統（含應用系統、密碼模組等）之安全驗證，須遵照權責主管訂定之規範作業，以確保其安全性。
- 3、憑證機構使用之數位簽章或加密金鑰長度，依權責主管建議之參考值及視系統的安全需求設定。
- 4、人體生物資料庫對外採購加密技術時，請廠商提供輸出國核發之輸出許可文件，並避免採購國外金鑰代管或金鑰回復之產品。

陸、資訊系統存取控制管理

一、資訊系統存取控制

- 1、訂定人體生物資料庫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、將業務系統之存取控制需求，明確告知系統服務提供者，以利其執行及維持有效的存取控制機制。
- 3、針對業務應用系統擁有者，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限，每一系統應有兩名最高權限使用者。
- 4、資訊系統存取控制規定之研擬，應考量事項如下：(1)個別業務應用系統之安全需求。(2)資訊傳佈及資料應用之名義及授權規定。(3)相關法規或契約對資料保護及資料存取之規定。

二、使用者之存取管理

(一) 使用者註冊管理

- 1、對於多人使用的資訊系統，建立正式的使用者註冊管理程序。
- 2、使用者註冊管理程序，考量的事項如下：
 - (1)查核使用者是否已經取得使用該資訊系統之正式授權。
 - (2)查核使用者被授權的程度是否與業務目的相稱，是否符合人體生物資料庫資訊安全政策及規定（例如：有無違反權責分散原則）。
 - (3)必須以書面方式告知使用者之系統存取權利。
 - (4)要求使用者簽訂約定，使其確實瞭解系統存取的各項條件及要求。
 - (5)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。
 - (6)建立及維持系統使用者之註冊資料紀錄，以備日後查考。
 - (7)使用者調整職務及離（休）職時，應盡速註銷其系統存取權利。
 - (8)應定期檢查及取消閒置不用的識別碼及帳號。
 - (9)閒置不用的識別碼不應重新配賦給其他的使用者。

(二) 系統存取特別權限之管理

- 1、嚴格管制系統存取特別權限。
- 2、特別保護的系統，如有必要賦予使用者系統存取特別權限，應依下列的授權程序管理：
 - (1)確認系統存取特別權限之事項，例如作業系統、資料庫管理系統、以及須賦予系統存取特別權限的人員名單。
 - (2)依執行業務之需求，視個案逐項考量賦予使用者系統存取特別權限；系統存取特別權限之

配賦，以執行業務及職務所必要者為限。

- (3)建立申請系統存取特別權限之授權程序，並只能在完成正式授權程序後，才能配賦給使用者；另外，將系統存取特別權限之授權資料建檔，以明責任及備日後查考。

(三) 使用者通行碼之管理

- 1、建立使用者通行碼之管理制度，規定至少每一季強制更新使用者通行碼的規範。
- 2、建立通行碼管理制度，須考量下列事項：
 - (1)盡量以簽訂書面約定或其他方式，要求使用者善盡保護個人通行碼之責任；如屬於群組軟體之使用者，確保工作群組的通行碼，僅限群組成員使用。
 - (2)為維持通行碼的機密性，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。
 - (3)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件遞等電子方式交付給使用者，並建立確認使用者是否收到臨時的通行碼的機制。
 - (4)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。

(四) 系統存取權限之檢討評估

- 1、為有效控管資料及系統存取，必須定期檢討及評估使用者之存取權限。
- 2、系統存取權限之評估，考量事項如下：
 - (1)系統存取權限評估，以每六個月評估一次為原則。
 - (2)系統存取特別權限之評估，以每三個月評估一次為原則。
 - (3)定期檢討系統存取特別權限之核發情形，防止有人未經正式的授權程序取得特別權限。

三、系統存取之責任

(一) 使用者通行碼之管理

- 1、使用者選擇及使用通行碼時，必須遵守人體生物資料庫資訊安全規定。
- 2、依下列原則配賦、管理及使用通行碼：
 - (1)以嚴謹的程序核發通行碼，明確規定使用者應負的責任。
 - (2)個人負責保護通行碼，維持通行碼的機密性。
 - (3)避免將通行碼記錄在書面上，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。
 - (4)當有跡象足以顯示系統及使用者密碼可能遭破解時，須立即更改密碼。
 - (5)使用者密碼的長度最少由六位字元組成。
 - (6)避免以下列事項作為通行碼：
 - 年、月、日等時間資訊。
 - 個人姓名、出生年月日、身分證字號或汽機車牌照號碼。
 - 人體生物資料庫單位名稱、識別代碼或是其他相關事項。
 - 電話號碼。
 - 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。 • 重複出現兩個字以上的識別字碼。 • 以全部數字或是全部字母組成密碼。(7)使用者第一次登入系統時，系統須要求更改臨時性通行碼。(8)自動化登入系統之通行碼，不宜存放在巨集或是功能鍵中。(9)定期更換通行碼，每三個月更新一次為原則，最長不得超過六個月；應避免重複或循環使用舊的通行碼。(10)對有存取系統公用程式等特別權限的帳號，使用者密碼的更改頻率須較一般通行碼的更改周期為高。

3、須存取多人使用之系統，或是須進入不同的系統平台，必須使用較高品質及較高安全等級的通行碼。

(二) 暫時不使用或無人看管設備之安全管理

- 1、暫時不使用或無人看管的設備，當研擬適當的安全保護措施；安置在辦公區域內的設備（例如：工作站或檔案伺服器），如一段時間內無人使用或看管，須採行特別的安全保護措施，以防止未經授權的系統存取。
- 2、將暫時不使用及無人看管的設備管理規定，明確告知所有的使用者或服務廠商，並賦予安全保護的責任。
- 3、暫時不使用或無人看管設備之安全管理，考量事項如下：(1)當作業結束時，即關閉有效的通信管道。(2)當通信結束或不使用時，須完全登出 (logout) 電腦系統。

四、網路存取之安全控制

(一) 網路服務之限制

- 1、個別使用者或是從特定端末機存取電腦及網路服務之安全規定，須依人體生物資料庫之業務存取控制規定辦理。
- 2、使用者只能在授權範圍內存取網路系統服務事項。

(二) 遠端診斷連線作業埠之控制

不提供維修廠商以遠端登入方式進入人體生物資料庫電腦網路系統進行維修的通信作業埠，若有維修需求，應要求廠商現場處理。

(三) 網路之分隔

- 1、依據人體生物資料庫訂定的系統存取控制政策及需求決定，並考量成本因素及使用網路路由器和閘門技術對作業效率之影響，將不同使用者及電腦系統分開成不同的領域，以降低可能的安全風險。
- 2、不同領域的網路系統，每一領域應以特定的安全設施加以保護；例如：可設置防火牆及網路閘門隔開不同的網路系統，以安全的閘道控制不同領域的網路系統。

（四） 網路連線作業之控制

- 1、為確保系統安全，須限制使用者之網路系統連線作業能力。例如：以網路閘門技術依事前訂定之系統存取規定，過濾網路之傳輸作業。
- 2、限制網路連線作業能力之安全控制措施如下：
 - （1）只允許使用電子郵遞系統。
 - （2）只允許單向的檔案傳輸。
 - （3）允許雙向的檔案傳輸。
 - （4）使用互動式的系統存取。
 - （5）限制只能在特定的時間或日期進行系統存取。

（五） 網路路由控制

- 1、分享式的網路系統，須建立網路路由的控制，以確保電腦連線作業及資訊流動不會影響應用系統的存取政策。
- 2、於網路路由的控制，建立實際來源及終點位址之檢查機制；網路路由的控制可以硬體或軟體方式執行，並於事先評估瞭解不同方式的安全控制能力。

（六） 網路服務之安全控制

- 1、評估使用該項網路服務之可能風險。
- 2、評估網路服務提供者之安全措施是否足夠、是否提供明確的安全措施說明，並應考量使用該項網路對維持資料傳輸機密性、資料完整性及可用性等各種安全影響。

五、電腦系統之存取控制

（一） 端末機登入程序

- 1、使用者存取電腦系統須經由安全的系統登入程序。
- 2、登入程序應具備下列的功能：
 - （1）不顯示系統及應用系統識別碼，直到成功登入系統。
 - （2）系統不可在登入程序中，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。
 - （3）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，系統不可顯示那一部分資料是正確的，那一部分資料是錯誤的。
 - （4）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：
 - 記錄系統登入不成功的事件。

- 在使用者嘗試登入系統失敗後，強迫必須間隔一段時間之後才能再次登入。
- 中斷資料連結作業。

(5) 在系統登入被拒絕後，立即中斷登入程序，並不得給予任何的協助。

(6) 限制系統登入程序的最長及最短時間，如果超出時間限制，系統自動中斷登入。

(7) 在成功登入系統後，顯示下列的資訊：

- 上一次成功登入系統的日期及時間。
- 上一次成功登入系統之後，有無被系統拒絕登入的詳細資料。

(二) 使用者身分辨識

- 1、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，可為人體生物資料庫的整體效益，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，但須採取額外的安全控制措施，明確規範使用者的責任。

(三) 使用者通行碼之管理

- 1、以安全有效的使用者通行碼管理系統，鑑別使用者身分。
- 2、安全有效的使用者通行碼管理系統，考量的事項如下：
 - (1) 要求必須使用通行碼，以明定系統的使用責任。
 - (2) 允許使用者自行選擇及更改通行碼；系統具備資料輸入錯誤之更正功能。
 - (3) 要求使用者必須使用最低長度的密碼（最少六位長度的通行碼）
 - (4) 要求使用者定期更改通行碼（以三個月一次為原則，最長不宜超過六個月）。
 - (5) 以更頻繁的次數定期更新系統存取特別權限的通行碼。
 - (6) 使用者自行選擇密碼時，在第一次登入系統時，必須強迫使用者更改臨時性的密碼。
 - (7) 建立機制，避免使用者重複使用相同的密碼。
 - (8) 在登入系統程序中，系統不可顯示使用者的密碼資料。
 - (9) 使用者密碼必須與應用系統資料分開存放。
 - (10) 必須使用單向加密演算法儲存使用者密碼。
 - (11) 在軟體完成安裝作業後，立即更改廠商預設的使用者密碼。
 - (12) 利用工具檢查，或由使用者自行考量通行碼是否安全可靠，參考基準如下：
 - 是否使用與日期有關的年、月、日。
 - 是否使用公司名稱、識別碼或是其他參考性資訊作為通行碼。
 - 是否以使用者識別碼，團體識別碼或其他系統識別碼作為使用者通行碼。
 - 是否使用重複出現兩個字以上的識別字碼作為通行碼。
 - 是否使用全數字或是全字母作為通行碼。

(四) 端末機作業時間限制

- 1、安置在高風險地區且不經常使用的端末機（例如：設置在公共場所或人體生物資料庫辦公場所以外的地區），或是對高風險的系統提供服務，必須限定其作業時間，以防止未經授權的人員存取系統。
- 2、必須設定系統的作業時間限制，包括間隔一定時間後自動清除螢幕上的資訊，以及依據事前訂定的時間限制，結束應用系統及網路通信。

(五) 連線作業時間之控制

- 1、針對有高風險的應用系統，限制使用者的連線作業時間。
- 2、對處理機密及敏感性系統的端末機，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：
 - (1) 只允許在設定的時間內與系統連線。
 - (2) 如無特別延長作業時間的需求，限制只能在正常的上班時間內進行連線作業。
 - (3) 限制連線的網址。

六、應用系統之存取控制

(一) 資訊存取之限制

- 1、依資訊存取規定，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。
- 2、資訊存取的控制措施如下：
 - (1) 以選單方式控制使用者僅能使用系統的部分功能。
 - (2) 適當的編輯作業手冊，限制使用者僅能獲知或取得授權範圍內的資料及系統存取知識。
 - (3) 控制使用者存取系統的能力（例如：限定使用者僅能執行唯讀、寫入、刪除或執行等功能。
 - (4) 處理敏感性資訊的應用系統，系統輸出的資料，僅限於與使用目的有關者，且只能輸出到指定的端末機及位址。

(二) 系統公用程式之安全管理

- 1、嚴格限制及控制電腦公用程式之使用。
- 2、電腦公用程式之安控措施如下：
 - (1) 設定使用者密碼以保護系統公用程式。
 - (2) 將系統公用程式與應用系統分離。

- (3)將有權使用系統公用程式的人數限制到最小的數目。
- (4)建立臨時使用公用程式的授權制度。
- (5)限制系統公用程式之可用性，例如變更公用程式的使用時間授權規定。
- (6)記錄系統公用程式的使用情形，以備日後查考。
- (7)訂定系統公用程式的授權規定，並以書面或其他電子方式為之。
- (8)移除非必要的公用程式及系統軟體。

(三) 原始程式資源之存取控制

- 1、對應用系統原始程式資料之存取，建立嚴格的安全控制機制。
- 2、原始程式資源之存取控制，考量下列事項：
 - (1)應用程式原始碼資料庫不要存放在作業系統的檔案中。
 - (2)每一項應用程式原始碼應指定一位管理人員。
 - (3)不應核發人員無限制存取應用程式原始碼之權限。
 - (4)發展中或是維護中的應用程式，與實務作業之程式原始碼資料庫區隔，不可放置在一起。
 - (5)應用程式原始碼資料庫之更新，以及核發應用程式原始碼供程式設計人員使用，須由原始碼資料庫管理人員執行。
 - (6)程式目錄清單應放置在安全的環境中。
 - (7)建立所有存取程式原始碼資料庫的稽核軌跡。
 - (8)舊版的原始程式予妥慎典藏保管，詳細記錄使用的明確時間，並保存所有的支援應用程式軟體、作業控制、資料定義及操作程序等資訊。
 - (9)應用程式原始碼資料庫之維護及複製，須依嚴格的變更控制程序進行。

(四) 機密及敏感性系統之獨立作業

- 1、對機密及敏感性的系統如生物資料庫系統，建置獨立的或是專屬的電腦作業環境。
- 2、建置獨立的或是專屬的電腦作業環境，考量的事項如下：
 - (1)由系統擁有者決定應用系統是否屬於機密或敏感，並以書面記錄。
 - (2)機密及敏感性的應用系統須在分享式的電腦環境中執行時，應界定其他須共享資源的系統項目，並經系統擁有者的同意。

七、系統存取及應用之監督

(一) 事件記錄

- 1、建立及製作例外事件及資訊安全事項的稽核軌跡，並至少保存一年的時間，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：
 - (1)使用者識別碼。
 - (2)登入及登出系統之日期及時間。

(二) 系統使用之監督

- 1、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，依風險評估結果決定。
- 2、系統使用監督考量事項如下：(1)系統存取失敗情形。(2)檢查系統登入的模式，確定使用者識別碼是否有不正常使用或是被重新使用的情形。(3)查核系統存取特別權限的帳號使用情形及配置情形。(4)追蹤特定的系統交易處理事項。(5)敏感性資源的使用情形。
- 3、系統使用之監督作業，須經權責主管人員之正式授權始得為之。

(三) 電腦作業時間校正

定期校正電腦系統作業時間，以維持系統稽核紀錄的正確性及可信度，俾作為事後法律上或是紀律處理上的重要依據。

八、外部人員存取資訊之安全管理

人體生物資料庫資訊系統為獨立內部系統，不提供外部連線之存取。

九、系統稽核規劃

(一) 系統稽核控制

- 1、對作業系統進行查核之稽核需求及實際稽核作業，應審慎規劃，並經權責主管人員同意始得為之，以免影響業務正常運作。
- 2、系統稽核應考量事項如下：
 - (1)稽核需求及查核範圍，須經權責主管人員同意。
 - (2)限定以唯讀方式存取軟體及資料。
 - (3)不能以唯讀方式進行系統存取時，則獨立複製另外一份系統檔案供稽核作業之用，且於稽核作業完成後，立即消除檔案。
 - (4)執行查核所需的技術資源，應於事前明確界定，並準備妥當。
 - (5)執行特別的及額外的查核，應於事前明確界定需求及範圍，並與服務提供者協議。
 - (6)執行稽核作業的所有系統存取作業，須予監督及留下記錄，並永久保存，以備日後查考。
 - (7)稽核作業程序、需求及責任規定，須以書面或其他電子方式為之。
 - (8)每年至少一次或依實際安全風險考量得隨時執行資訊安全稽核。

(二) 系統稽核工具之保護

- 1、須保護系統稽核工具（例如：軟體及資料檔案）以防止誤用或被破解。
- 2、系統稽核工具應與發展中或是實作的系統分隔，且應存放在安全的地點。

柒、資訊系統購置、發展及維護安全管理

一、系統安全需求

(一) 安全需求分析及規格訂定

- 1、在資訊系統規劃之需求分析階段，即將安全需求納入；新發展的資訊系統，或是現有系統功能之強化，皆明定資訊安全需求，並將安全需求納入系統功能。
- 2、除由系統自動執行的安控措施之外，亦可考量由人工執行的安控措施；在採購套裝軟體時，亦進行相同的安全需求分析。
- 3、系統的安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足對人體生物資料庫可能帶來的傷害程度。
- 4、資訊系統安全需求分析應考量事項如下：
 - (1)評估保護資訊機密性、整合性及可用性的需求。
 - (2)找出及決定各種不同的安全控制措施，以防範、偵測電腦當機或發生安全事件時，能立即執行回復作業。
 - (3)資訊安全需求分析，特別考量下列事項：
 - 對資訊及系統之存取控制。
 - 對人體生物資料庫重要業務建立例行性的稽核制度，並為特定查核之事項建立稽核軌跡。
 - 重要的資料，在資料處理過程的每一階段，或是特別選定的某一階段，檢查及保護資料的真確性。
 - 保護機密性或敏感性資料，防止洩漏或被竄改，必要時使用資料加密等技術保護。
 - 遵守法規或契約上對資訊安全控制的要求。
 - 重要的業務資料，須複製備份資料。
 - 訂定電腦當機之立即回復作業程序，尤其是對高使用率的系統有妥適的回復措施。
 - 保護系統避免未經授權的竄改或是修改。
 - 使系統以安全的方式為一般人員操作及使用。
 - (4)於相關文件規定資訊安全控制措施，以利使用者及電腦支援人員明瞭電腦系統內建之安控系統功能。

二、應用系統之安全

(一) 資料輸入之驗證

- 1、輸進應用系統的資料，應在事前查驗，以確保資料的真確性。
- 2、資料輸入考量的安控措施如下：

(1)檢查是否有以下的錯誤：

- 是否有超出設定範圍的數值。
- 資料檔案是否有錯誤的文數字。
- 資料是否有毀損或是不正確。
- 是否有超出設定數值的上限或是下限。
- 是否有未經授權的資料或是不一致的控制性資料。

(2)定期檢查主要欄位或資料檔案的內容，以確保資料的有效性及真確性。

(3)檢查輸入的書面資料是否有被竄改情形。

(4)建立資料檢驗證程序及資料錯誤更正的作業程序。

(5)明定資料輸入過程中相關人員的責任。

(二) 系統內部作業處理之驗證

- 1、針對系統內部的作業，建立驗證資料正確性的作業程序，避免正確輸入資料到應用系統中，卻因系統處理錯誤或是人為因素而遭受破壞。
- 2、系統內部作業是否採取特別的資料處理控制程序，視應用系統的性質及資料遭破壞，將對人體生物資料庫業務的影響程度而定。
- 3、系統內部作業處理之驗證方法如下：(1)利用系統提供的功能，做資料處理作業控制或批次控制，以達到檔案資料更新處理後的一致性。(2)比對本次開始作業與前次結束作業的檔案資料是否一致。(3)查證系統產生的資料是否正確。(4)查證電腦系統之資料、下載及上傳軟體，或軟體更新後系統之真確性。

(三) 訊息真確性之鑑別

- 1、依安全風險評估結果，採行最適當的訊息鑑別方法，以偵測資料內容是否遭受未經授權的竄改，或驗證傳送之訊息內容是否遭受破壞。
- 2、對重要的應用系統，使用訊息鑑別技術保護資料內容之真確性。

三、應用系統檔案之安全

(一)作業軟體之控制

- 1、在作業系統上執行應用軟體，嚴格執行下列控制程序，減少可能危害作業系統的風險：
 - (1)作業用的應用程式更新作業，限定只能由授權的管理人員才可執行。
 - (2)須將執行碼存放在作業系統內。

- (3)執行碼尚未測試成功，且未被使用者接受前，不可在作業系統執行。
- (4)建立應用程式館的更新稽核紀錄。
- (5)必須保留舊版的軟體或實施版管控管機制，以作為緊急應變措施之用。

(二)系統測試資料之保護

- 1、須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；如須應用真實的資料，必須於事前將足以辨識個人的資料去除。
- 2、在使用真實的資料進行測試時，採行下列的保護措施：
 - (1)適用在實際作業系統的存取控制措施，亦適用在測試用的系統。
 - (2)真實資料被複製到測試系統時，依複製作業的性質及內容，在取得授權後始能進行。
 - (3)測試完畢後，真實資料必須立即從測試系統中刪除。
 - (4)記錄真實資料的複製情形，以備日後稽核之用。

(三)應用系統及其資料之保護

- 1、對生物資料庫系統具有維護及更新能力之應用系統開發人員須禁止其對生物資料庫系統的使用權限及資料讀取存取權限。
- 2、該系統之修改更新，需依規定於「陸、資訊系統購置、發展及維護安全管理」之「陸.四、系統變更及支援環境之安全」的變更作業之控制程序取得核准後，由具有生物資料庫系統操作權限之系統人員在資訊組組長之監督下執行更新。

四、系統變更及支援環境之安全

(一)變更作業之控制程序

- 1、建立正式的變更控制程序，並嚴格執行，以降低可能的安全風險；變更作業之控制程序，要確保系統安全控制程序不會被破壞，並確保程式設計人員只能存取系統作業所需的項目，且任何的系統變更作業，皆獲得權責主管人員的同意。
- 2、建立變更控制程序，依事前訂定的授權規定，執行變更作業
 - (1)規定系統使用者提出變更需求之權責，以及接受系統變更建議之授權程序。
 - (2)規定系統完成變更作業後，系統使用者是否認可之權責。
 - (3)規定只有被授權的使用者可提出系統變更之請求。
 - (4)規定檢視系統安全控制及檢視系統真確性的程序，以確保系統變更作業不致影響或破壞系統原有的安全控制措施。
 - (5)找出系統變更作業需要修正的電腦軟體、資料檔案、資料庫及硬體項目。
 - (6)在實際執行變更作業前，變更作業的細項建議，須取得權責主管人員之核

准。(7)在執行變更作業前，確保系統變更作業能為使用者接受。(8)系統文件在每次完成變更作業後，須立即更新，舊版的系統文件亦要妥善保管及處理。(9)建立軟體更新的版本控制機制。(10)所有的系統變更作業請求，皆須建立稽核紀錄。(11)所有的系統變更作業請求更新，於核准後，皆要建立稽核紀錄。

(二) 作業系統變更之技術評估

- 1、規範作業系統定期更新辦法（例如：安裝新的版本）；作業系統變更時，須評估其對應用系統是否造成負面的影響，或是產生安全上的問題。
- 2、作業系統變更之評估程序，考量的事項如下：(1)評估應用系統的安全控制措施及查驗系統真確性，以確保其未受作業系統變更之影響。(2)作業系統變更的評估及測試結果，如須進行必要的調整，要納入年度計畫及預算。(3)作業系統的變更所需即時通告相關人員，以便在作業系統變更前，相關人員可以進行適當及充分的評估作業。

(三) 套裝軟體變更之限制

- 1、廠商提供的套裝軟體，要減少自行變更或修改，如因特殊需要須修改，要考量以下的事項：
(1)是否會破壞系統內建的安全控制，以及危害鑑別系統真確性作業的風險。(2)取得套裝軟體開發廠商的同意。(3)考量以標準化的系統更新方式，請廠商進行必要的變更。(4)考量如自行變更套裝軟體，日後進行軟體維護的可能性。(5)套裝軟體如須變更，須保留原始的軟體，並將變更的資料予以記錄，以備日後軟體再更新之用。

五、系統委外開發管理之安全

1. 當生物資料庫系統的部分運作功能或程序進行委外時，必須對資訊安全的風險加以評估，並且建置相關的安全措施，此措施必須被載明在委外合約中。必須納入資訊委外服務契約的資訊安全事項如下：(1)應限制委外廠商存取之機密性、敏感性或是關鍵性的應用系統或資料項目。(2)廠商需配合執行業務永續運作計畫之系統範圍。(3)廠商應遵守之資訊安全規範及評鑑作業程序。(4)廠商處理及通報資訊安全事件的責任及作業程序。
2. 對於委外廠商的內部作業程序及系統作業程序安全性，需進行初始及定期的了解並評估是否符合生物資料庫的資安規定或有其危害風險。
3. 於每一委外建置或管理之系統合約中明定系統的使用權責歸屬，以釐清資訊安全的責任，並避免誤解。
4. 廠商系統人員如有涉及可能接觸生物資料庫系統的資料之可能性，要求相關人員簽訂保密協定。

5. 系統建置委託之合約簽訂時，對可能的資料外洩或未經授權的存取之風險審慎評估，並於契約中針對該風險制定防範之規定。
6. 於實體辦公室安全管控及資料存取的規定中，納入各系統委外廠商的授權及安全管控內容。
7. 應限制廠商永久存取權限及遠端存取權限。
8. 對所委外的系統並執行定期的權限稽查，確保委外授權人員的必要性及授權期間是否與合同明定相符，廠商的系統使用權限須於系統委任開始、結束或變更內容時由稽核小組進行稽核檢視。
9. 明確限制委外廠商對生物資料庫實體資料的存取權限及應用系統的修改權限。任何因業務及變更所需的修改，需經由使用單位提出，相關系統人員檢視其修改範圍無誤並符合業務需求後，經由所規範的系統變更修改程序執行其異動。

捌、資訊資產之管理

一、人體生物資料庫資訊資產之保護

(一) 資訊資產目錄之建立

- 1、需建立一份與資訊系統有關的資訊資產目錄，訂定人體生物資料庫資訊資產的項目、擁有者及安全等級分類等。
- 2、資訊資產參考項目如下：
 - (1) 資訊資產：資料庫及資料檔案、系統文件、使用者手冊、訓練教材、作業性及支援程序、業務永續運作計畫、預備作業計畫等。
 - (2) 軟體資產：應用軟體、系統軟體、發展工具及公用程式等。
 - (3) 實體資產：電腦及通訊設備、磁性媒體資料及其他技術設備。
 - (4) 技術服務資產：電腦及通信服務、其他技術性服務（電源及空調）。

(二) 資訊安全之等級分類

1、資訊安全分類原則

- (1) 依據國家機密保護、電腦處理個人資料保護及政府資訊公開等相關法規，建立資訊安全等級之分類標準，以及相對應的保護措施。
- (2) 資訊安全分類標準，首要考量資訊分享及限制的影響、未經授權的系統存取或是系統損害對人體生物資料庫業務的衝擊，尤其要考量資料的機密性、資料真確性及可用性。
- (3) 人體生物資料庫資訊安全分類，可依據相關法規，區分機密性、敏感性及一般性等三類。
- (4) 界定資訊安全等級之責任，依客戶所簽訂的同意書所要求，記錄於生物資料庫當中。
- (5) 依客戶變更同意書所需移除之資料，需確保於線上儲存及備份儲存的所有資料媒介中即時更新移除並依特定技術無法再行回復。

2、資訊安全等級標示

- (1) 已列入安全等級分類的資訊及系統之輸出資料，標示適當的安全等級以利使用者遵循。
- (2) 應納入安全等級分類的項目，包括：書面報告、螢幕顯示、磁性媒體、電子訊息及檔案資料等。

玖、實體及環境安全管理

一、設備安全管理

(一) 設備安置地點之保護

- 1、設備必須安置在適當的地點並予保護，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。
- 2、設備安置遵循的原則如下：
 - (1)設備盡量安置在可減少人員不必要經常進出的工作地點。處理機密性及敏感性資料的工作站，應放置在員工可以注意及照顧的地點。
 - (2)需要特別保護的設備，需與一般的設備區隔，安置在獨立的區域。
 - (3)檢查及評估火災、煙、水、灰塵、震動、化學效應、電力供應、電磁幅射等可能的風險。
 - (4)電腦作業區嚴禁抽煙及飲用食物。
 - (5)在特定的作業環境下，可考慮使用鍵盤保護膜。
 - (6)除了考量同一樓層地板可能導致的危險外，也需考量鄰近建築樓層地板可能導致的危險。

(二) 電源供應

- 1、電腦設備之設置，規範其電源保護措施，以防止斷電或其他電力不正常導致的傷害；電源供應依據製造廠商提供的規格設置。
- 2、人體生物資料庫主要系統安置預備電源，且不斷電系統屬必要之配置。**
- 3、人體生物資料庫的資訊安全事件緊急處理應變計畫，應將不斷電系統失效之後的應變措施納入；不斷電系統應依據製造廠商的建議，定期進行測試。
- 4、謹慎使用電源延長線，以免電力無法負荷導致火災等安全情事。

(三) 電纜線安全

- 1、電力及通信用的電纜線給予適當的保護，以防止被破壞或是資料被截取。
- 2、電力及通信纜線的保護原則如下：
 - (1)連接資訊設施的電源及通信線路，盡可能地下化；如果不能地下化，則需採取足夠的替代保護措施。
 - (2)應該考量保護網路通信線路的措施，以防止遭截取或是受到破壞。
 - (3)對於特別敏感性或是特別重要的系統，採取額外強化的安全措施。

(四) 設備維護

- 1、妥善地維護設備，以確保設備的完整性及可以持續使用。

- 2、設備維護的原則如下：(1)依據廠商建議的維修服務期限及說明進行設備維護。(2)設備的維護只能由授權的維護人員執行。(3)將所有的錯誤或是懷疑的錯誤予以記載。

(五) 設備放置在人體生物資料庫外部空間之安全管理

- 1、設置在人體生物資料庫外支援人體生物資料庫業務運作的資訊設備，需同樣遵守資訊安全管理授權規定，維持與人體生物資料庫內部資訊設備一樣的安全水準。
- 2、設置在人體生物資料庫外的資訊設備安全措施原則如下：(1) 執行人體生物資料庫業務使用之個人電腦，僅限在業務執行場所使用。(2)外出差勤時，電腦設備及資料儲存媒體在公共場所需有人看管。(3)外勤使用之攜帶型電腦，易於被偷取、遺失或是遭未經授權的取用，規範其適當的存取保護措施，例如設定通行碼或是將檔案資料加密。(4)應隨時注意設備製造廠商提供的保護使用說明書。(5)各種安全風險如損害、偷竊或竊聽等，可能會因不同的安置地點而有所不同；在決定最適當的安全措施時，必須將不同地點的安全風險納入考量。

(六) 設備處理之安全措施

儲存媒體在報廢前，除詳加檢查並移除相關機密性、敏感性的資料及有版權的軟體外，更應採以不可回復的破壞方式處理必須採取破壞性且不可回復之處理方式，以確保該媒體所儲存之資料不會被非法還原。

(七) 資訊設施誤用之防止

- 1、人體生物資料庫提供的資訊設施，如有業務目的以外的使用，或是超出授權目的以外的使用需求，需經權責主管人員的核准，並課予相關人員的責任。
- 2、如從監督性的資訊或是從其他方法發現資訊設施有不當使用情形，必須作適當及立即的紀律處理。
- 3、清楚以書面或其他電子方式明確告知使用者的系統存取授權範圍。
- 4、人體生物資料庫員工以及其他第三者，除非獲得正式的授權，任何人皆不得進行系統存取。

二、周邊安全管理

(一) 周圍環境之安全

- 1、實體環境的安全保護，以事前劃定的各項周邊設施為基礎，並以設置必要的障礙（例如：使用身分識別卡之安全門），達成安全控管的目的。
- 2、每項資訊設施的實體保護程度，以及實體障礙設置的位置，需依資訊資產及服務系統的價值及安全的風險決定。

3、實體環境的安全保護原則如下：(1)周圍設施的安全措施，視擬保護的資訊資產或資訊服務系統的價值而定。(2)明確界定有那些周邊設施須列為安全管制的對象。(3)支援資訊作業的相關設施如影印機、傳真機等，安置在適當的地點，以降低未經授權的人員進入管制區的風險，及減少敏感性資訊遭破解及洩漏的機會。(4)不可對非相關的人員提供過多有關管制區的作業細節。(5)為了安全的目的，以及防止可能的不當行動，未經授權的人員在辦公室單獨作業需予適當的管理。(6)人體生物資料庫資訊作業如有委外者，自行管理的設備必須安置在特定的區域，並與資訊服務提供者管理的設備分開。(7)資訊支援人員或維護服務人員，只有在被要求或是被授權的情形下，才能進入管制區域，並視需要限制（例如限制存取敏感性的資料）及監督其活動。(8)非經授權，管制區內不得設置照像、錄音及錄影等設備。

(二) 人員進出管制

1、管制區內應有適當的進出管制保護措施，以確保只有被授權的人員始得進入。

2、進出管制考量的事項如下：

- (1)來訪人員進入管制區予適當的管制，並記錄進出時間；來訪人員只有在特定的目的或是被授權情形下，才能進入管制區。
- (2)在管制區內，所有的人員必須配戴身分識別標示，並隨時注意身分不明或可疑的人員。
- (3)人體生物資料庫員工離職後，立即撤銷進入管制區的權利。

(三) 資料中心及機房之安全管理

- 1、支援人體生物資料庫重要業務運作的資料中心及電腦機房，必須設立良好的實體安全措施；資訊中心及電腦機房地點的選定，應考量火災、水災、地震等自然及人為災害的可能性，並考量鄰近空間的可能安全威脅。
- 2、資料中心及機房安全考量的事項如下：
 - (1)主要的設施應遠離大眾或是公共運輸系統可直接進出的地點。
 - (2)資料中心及電腦機房的建築，盡可能不要有過於明顯的標示；在建築物內部及外部的說明，以提供最低必要的指引或配置說明為限。
 - (3)各樓層的配置說明及內部的電話聯絡簿，以不讓有心人士循線找出電腦設施的所在地為原則。
 - (4)危險性及易燃性的物品，必須存放在遠離資料中心或電腦機房的安全地點。非有必要，電腦相關文具設備不可存放在電腦機房內。
 - (5)備援作業用的設備及備援媒體，要存放在安全距離以外的地點，以免資料中心或電腦機房受到損害時也一併受到毀損。
 - (6)應安裝適當的安全偵測及防制設備，例如熱度及煙霧偵測設備，火災警報設備、滅火設備及火災逃生設備；各項安全設備需依廠商的使用說明書定期檢查；人體生物資料庫的員工須施予適當的安全設備使用訓練。
 - (7)人體生物資料庫資訊安全緊急處理作業程序必須以書面方式記載，並定期演練及測試。
 - (8)人體生物資料庫不上

班或沒有人看護時，門窗必須閉鎖，並考量窗戶的外部保護措施。

(四) 物品及設備配送及裝載之管理

- 1、電腦機房需設置適當的保護措施，防止未被授權的人員進出；為降低未被授權的人員進入電腦機房的風險，可視需要設立一個獨立的物品及設備配送及裝載作業區域。
- 2、物品及設備作業區的安全需求需依風險評估的結果而決定。

(五) 辦公桌面之安全管理

- 1、考量採用辦公桌面的淨空政策，以減少文件及磁碟片等在正常的辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。
- 2、考量的事項如下：
 - (1)文件及磁碟片在不使用或是不上班時，存放在櫃子內。
 - (2)人體生物資料庫的機密性及敏感性資訊，不使用或下班時應該上鎖，最好是放在防火櫃之內。
 - (3)個人電腦及電腦終端機不再使用時，于以上鎖、通行碼或是其他控制措施保護。
 - (4)考量保護一般郵件進出的地點，以及無人看管的傳真機。

(六) 財產移轉之安全管理

電腦設備、資料或是軟體，在沒有資訊安全主管書面授權的情形下，不可被帶離辦公室。

拾、資訊安全事件發生之通報及保全處理程序

一、資訊安全事件之通報

- (一) 建立資訊安全事件的正式通報程序及管道，訂定資訊安全事件通報應採行之行動及措施。
- (二) 如發現或懷疑有資訊安全事件時（包括系統有安全漏洞、受威脅、系統弱點及功能不正常事件等），立即依事前訂定的通報管道，迅速通報權責主管單位及人員立即處理。
- (三) 人體生物資料庫員工及與人體生物資料庫簽訂資訊安全協定的外部人員，皆需確實明瞭各種資訊安全事件的反應及報告程序。

二、資訊安全弱點之反映

- (一) 人體生物資料庫員工需隨時注意資訊系統或是資訊服務設施內部之安全弱點、可能面臨的威脅，並迅速向直屬業務主管或是系統服務廠商報告。
- (二) 系統安全上的弱點，必須由專業人員處理，不可任由系統使用者自行修改。

三、軟體功能不正常之反映

- (一) 使用者發現軟體功能有異常時，需迅速告知資訊支援單位或是服務廠商處理。
- (二) 建立軟體功能不正常之反映及處理程序：
 - 1、注意螢幕上出現的徵兆或是訊息。
 - 2、立即停止使用電腦，迅速通知資訊支援單位。
 - 3、檢視軟體功能不正常的設備，再次啟動前，則以離線方式處理。
 - 4、在任何狀況下，使用者不應自行移除功能不正常的軟體；系統回復作業應由受過適當訓練及有經驗的人員執行。

四、資訊安全事件分級

- (一)『A』級：影響生物資料庫個人資料安全。
- (二)『B』級：系統停頓，業務無法運作。
- (三)『C』級：系統短暫停頓，業務中斷，短時間可修復。
- (四)『D』級：系統效能降低，業務遲滯，可立即修復。
- (五)『E』級：違反網路使用規範或其他公約。

五、資訊安全事件之通報程序

(一) 事件鑑定與確認：

- 1、系統管理人員或使用者發現資訊及網路系統服務及功能異常反應，應立即通知資訊主管進行鑑定。
- 2、資訊主管協同系統管理人員分析資安徵兆或對外通知，確認為資安事件後，依據事件類別及對業務影響程度，區分資訊安全事件等級。
- 3、必要時系統管理人員得採取緊急應變措施，防止事件影響擴大。
- 4、系統管理人員應記錄事件狀況、應變措施等相關資訊，交資訊主管人進行通報。

(二) 事件通報：

- 1、資訊主管立即依循內部行政程序，將事件狀況、應變措施等相關資訊向生物醫學組主管及基金會代表人報告。
- 2、屬『A』、『B』、『C』、『D』級之資安事件，資訊組主管應於確認資安事件1小時內向生物組主管報告。
- 3、屬『A』級之資安事件，資訊組主管應於確認資安事件2小時內向衛生署資安聯絡人通報，並提供事件細節內容。

六、資訊安全事件之處理程序

- (一)系統管理人員進行損害評估，並分析系統復原所需資源。
- (二)資訊組主管協調組織資通安全處理小組成員進行應變處理作業。
- (三)資通安全處理小組依組織、人力、應變措施與所需資源，判定是否自行處理或需請求上級支援。
- (四)若判定需請求上級支援，經基金會代表人核定後，應於確認資安事件12小時內向衛生署提出申請支援。
- (五)系統管理人員進行資安事件處理前，應先儲存或備份系統記錄與稽核軌跡等相關資訊，保全事件證據。
- (六)系統管理人員應記錄事件處理過程，以供後續稽核改善之參考。

拾壹、業務持續及回覆管理

一、業務永續運作之規劃

(一) 業務永續運作之規劃程序

- 1、必須建立跨部門的業務永續運作計劃程序，研訂及維護人體生物資料庫業務持續運作之計畫。
- 2、業務永續運作的規劃作業，詳細研析並降低人為或是意外因素對人體生物資料庫重要業務運作可能導致的威脅，使重要業務在系統發生事故、設施失敗或是受損害時，仍可持續運作。
- 3、人體生物資料庫業務永續運作計畫，必須考量下列事項：
 - (1)界定重要的業務作業程序，並訂定其優先順序。
 - (2)評估各種災害對人體生物資料庫業務可能的衝擊。
 - (3)維持人體生物資料庫永續運作之人員責任界定，以及緊急應變措施之安排。
 - (4)建立人體生物資料庫永續運作之作業程序及流程，並以書面或其他電子方式記載。
 - (5)定期就緊急應變程序及作業流程，進行員工教育及訓練。
 - (6)定期測試緊急應變計畫。
 - (7)定期更新緊急應變計畫。
 - (8)定期更新備份計畫。

資料備份作業原則如下：

- 正確及完整的備份資料，除存放在主要的作業場所外，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損失。如：人體生物資料庫與第三方備援中心。
- 人體生物資料庫的備份，以維持三代為原則。
- 備份資料需有適當的實體及環境保護，其安全標準應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，應適用到備援作業場所。
- 定期測試備份資料，以確保備份資料之可用性。
- 資料的保存時間，以及檔案永久保存的需求，由設置者研提。

(二) 業務永續運作規劃架構

- 1、持續建立及維持單一的永續作業計畫架構，使各種不同層次及等級的計畫相互連貫，並訂定測試計畫及維護計畫之優先順序。
- 2、每項業務之永續運作計畫，需明定行動之條件，以及員工執行計畫之責任；人體生物資料庫研擬新的資訊計畫，必須與人體生物資料庫緊急應變計畫程序相一致（例如：疏散

計畫、現有電腦服務系統的預備作業安排，以及通信及空間的配置。)

- 3、目前作業並無對國際傳輸或處理的範圍，特別是生物資料庫的系統及資料也無國際服務的需求，因此永續運作計畫未包含國際傳輸相關之管理規定及作業辦法，但如此業務開通，則須檢視此資安規範對國際傳輸的可能風險並加入該作業之永續運作規畫。
- 4、在業務永續運作之整體架構內，訂定不同層次及等級的計畫，每一層次及等級的計畫，涵蓋不同的計畫重點及負責回復作業的人員安排。
- 5、業務永續運作計畫，考量的作業程序如下：(1)訂定緊急應變作業程序，規定如何在發生危害人體生物資料庫業務運作或危及生命的重大事件發生時，立即採取的行動。(2)訂定預備作業程序，規定如何將必要的人體生物資料庫業務活動或是支援性的服務，移轉至另外一個臨時的作業地點。(3)訂定回復作業程序，規定如何採取回復作業，使人體生物資料庫的業務回復到原來正常的業務運作。(4)訂定測試作業程序，規定如何及什麼時間執行測試作業。
- 6、每一層次的計畫以及每一項個別計畫，都指定一位計畫執行督導人員。
- 7、緊急應變作業、人工預備作業及回復作業計畫等，指定適當的單位或人員負責。
- 8、技術服務的預備作業安排(例如電腦及通信系統)應由資訊人員或該系統之委外廠商負責。
- 9、根據回復之業務範圍及時間需求訂定系統備份計畫，此計畫應考量的重點如下：
(1)一套兩份以上的完整系統備份 (2)增量資料庫備份及備份頻率 (3)備份排程 (4)安全及可及時執行回復的備份資料保存地點 (5)備份執行的系統紀錄及監督流程。

二、業務永續運作計畫之測試

(一) 業務永續運作計畫之測試

- 1、業務永續運作計畫可能因事前的假設不正確、規劃不周全或設備及人員的職務調整變更，而無法發揮預期的作用，必須定期測試及演練，以確保計畫的有效性，並使相關人員確實瞭解計畫的最新狀態。
- 2、擬訂測試作業的時程，定期進行測試，使應變計畫維持在有效及最新的狀態；測試計畫可以定期測試個別計畫的方式進行，以減少測試完整計畫的需求及頻率。

三、業務永續運作計畫之變更

(一) 業務永續運作計畫之變更

- 1、業務永續運作計畫要配合業務、組織及人員的調整變更而定期更新，以發揮計畫投資的效益及確保計畫持續有效。

- 2、需納入計畫更新之事項如下：(1)採購新的設備，或是更新作業系統。(2)使用新的問題偵測及控制技術（例如火災偵測）。(3)使用新的環境控制技術。(4)人員及組織上的調整變動。(5)人體生物資料庫及人員地址及電話號碼的變動。(6)契約當事者或是供應商的調整變動。(7)業務流程的變動，新建或是撤銷作業流程。(8)實務作業的變更。(9)法規上的變更。
- 3、需指定專人負責計畫變更事宜，個別計畫原則上至少每一個月要檢查評估一次，完整的計畫至少每年檢討評估一次。
- 4、需建立計畫變更的控制機制，以確保計畫變更前，以及賦予員工相關責任前，能將相關的訊息告知相關人員。

拾貳、其他有關資訊安全事項

其他資訊安全事項依相關規範納入本計畫附件項目辦理的管理應與前揭拾壹大項具有系統性及一貫性。