國立臺灣大學醫學院臺灣腦神經組織人體生物資料庫

文件名稱	資訊安全管理辦法	權責單位		腦庫	頁碼/總頁數	1/9
文件編號	8.1	版次	4	修制訂日期	2025/11/5	
				檢視日期	2025/11/5	

民國 111 年 03 月 24 日倫理委員會審查通過
民國 112 年 05 月 22 日倫理委員會審查通過
民國 114 年 11 月 05 日倫理委員會審查通過

壹、 目的

「國立臺灣大學醫學院臺灣腦神經組織人體生物資料庫」(以下簡稱本庫)為管理與生物檢體有關之資訊，保護參與者之隱私及權益，使其在合乎主管機關之法令下作保存與運用，特訂定本庫資訊安全管理辦法。

貳、 依據

本管理辦法依據「人體生物資料庫管理條例」、「人體生物資料庫資訊安全規範」及國立臺灣大學(下稱本校)醫學院與附設醫院之資訊安全相關規定。

參、 適用範圍

本管理辦法適用於接觸人體生物資料庫相關資訊之本校醫學院與附設醫院所有正式員工、約聘員工及外部人員(含工程、設備、運送等)等相關人員與設備。

肆、 資訊管理工作之權責及分工

一、本庫設有資訊中心，由資訊主管負責。

二、本庫依據所屬人員之業務特性，於工作職掌中載明資訊安全相關作業職責，並辦理資訊安全教育。參與本庫相關工作之人員離（退）職時，應立即取消其所有權限。

三、與本庫資料與資訊有接觸之工作人員，需簽屬保密協議。

四、本庫對與資訊有關業務及人員，應進行安全評估，並作員工個人資料管理。

五、本庫資訊安全相關工作人員權責分工說明如下：

(一)資訊主管：負責資訊安全管理事項之協調及推動，並辦理資訊安全政策、規劃、執行等審議、督導事項。

(二)資訊管理人員：建置並管理相關軟硬體設備以及管控使用者權限，但不接觸生物檢體。

(三)資訊處理人員：負責行政業務與資訊處理，但不接觸生物檢體。

以上各類人員不得互為兼任。

六、生物檢體其相關資料、資訊之資訊硬體系統與生物檢體本身，應分別指定專人管理；該專人不得兼任前項相關資料、資訊之管理人員。

七、本庫資訊主管、資料管理、資訊處理相關人員，每年應接受資訊安全相關教育訓練課程。

八、本庫若將資訊業務委託其他廠商辦理，應於委託契約中明定廠商之資訊安全、管理責任、保密規定及建立定期稽核機制；並將本規範納入成為契約之一部分。委託契約應明定機密保持之範圍、契約期間及契約終了時所應負之義務。

伍、 電腦系統安全管理

一、本庫之電腦，由資訊管理人員，依國立臺灣大學智財權與個人資料保護暨安全管理相關規範，負責安裝合法軟體。未經合法授權使用之軟體，不得安裝。其他使用者不得任意安裝轉體；使用者若有新軟體需求，需經資訊中心核准，由資訊管理人員負責安裝。資訊管理人員需定期確認授權軟體及免費軟體之使用情形。

二、為防範電腦病毒與惡意軟體之侵入，本庫電腦系統需安裝防毒軟體、更新病毒定義檔和定期掃瞄電腦系統及資料儲存媒體；員工需認知電腦病毒及惡意行動碼的威脅，提升警覺性，禁止使用來路不明及內容不確定的儲存媒體。

三、本庫監控並稽核電腦資料的使用情形，措施如下：

(一)使用者登入登出紀錄。

(二)使用者帳號與群組之異動。

(三)特殊權限帳號之異動與存取紀錄。

(四)系統參數之異動。

(五)系統錯誤事件(如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等)之紀錄與檢討。

四、與本相關之伺服器等重要資訊設備，在操作及異動時，應留下紀錄，以供日後備查。

五、本庫系統主機應定期進行效能及容量檢查，系統弱點檢測，並執行系統漏洞修補作業。

六、本庫所屬設備、資訊或軟體，未經資訊主管或生物醫學主管授權，禁止移動。

陸、 網路安全管理及通訊管理

一、建置於本庫之個人資料，存於實體隔離之資訊安全室內，其資訊系統不得與網際網路連接。進出資訊安全室者需經授權並受門禁管制。

二、本庫網路之連線，基於業務需求、效能及安全性等考量，應作適當的實體或邏輯劃分，各網段之間應設定適當之存取控制清單，以避免未經授權之存取。若有未經許可擅接網路之情事，應立即通知網路管理人員。

三、若因業務需要需與院外單位進行資料交換時，應簽訂合作協議書，規範單位間交換資訊安全之保護措施。

四、網路服務安全控制措施，包含：網路分隔控制規定、遠端連線使用者之存取須身分鑑別、無線網路服務之存取及應用之安全管控程序等。

五、本庫之網路連線受本校醫學院附設醫院網路安全管制，透過安全閘道設備積極控制資訊源到目的地之間的通訊，如防火牆機制等。

六、於核心路由器、核心交換器或防火牆當中設定存取控制清單，以過濾並控制本庫資料封包流向、通訊協定或流量。

七、網路傳輸之安全管理要點如下：

(一)透過網路傳輸資訊時，應考量傳輸時正確性與完整性，網路傳輸之內容需經授權存取。傳輸重要資料時，應視傳輸資料之機密等級與傳輸途徑予以適當之加密與安全機制防護。

(二)與人體生物資料庫有關之資訊，非經設置者倫理委員會認可之技術加以處理，不得以電子郵件或其他電子方式對外傳送；且經倫理委員會認定有特別保密必要之機密文件，不得以電子方式傳輸之規定。

(三)本庫針對全部資通系統，定期辦理網站安全弱點檢測並檢測網路運作環境之安全漏洞。資訊檔案室已實體隔離區且單機不連網，資訊系統得免實施網路弱點掃描。

八、本庫訂定網路監控措施與適當之保護機制，並建立日誌以保留紀錄。

柒、 資訊系統存取控制管理

一、本庫應訂定系統存取政策及授權規定，依不同工作職責，明確訂定可存取之系統資源內容，經倫理委員會審查通過後，以書面、電子或其他方式告知員工及使用者相關之權限及責任。

二、使用生物檢體及相關資料、資訊之第三人，其資訊管理人員與研究人員間，不得互為兼任。

三、系統存取權限，以執行其職務所必要者為限；對系統管理最高權限之人員及掌理重要技術及作業控制之特定人員，應經審慎之授權，並定期查核其權限及活動日誌，前項最高權限人員，至少應有二人。

四、本庫系統管理最高權限人員，可執行之權限與管理規範如下：

(一)生物醫學主管：具有自本庫取得已去除個資之相關檢體資料權限。

(二)資訊中心主管：具取得實體隔離之個資權限，可將外部資料匯入人體生物資料庫，但無權檢視人體生物資料庫內容。若計畫主持人通過外部資料庫串聯申請審核，由資訊中心主管授權，向外部資料庫取得計畫主持人申請之研究資料，去除個資後匯入人體生物資料庫。

(三)系統應自動記錄所有相關操作歷程軌跡。

五、建立使用者註冊管理制度，設定帳號密碼登入管制，並加強密碼管理，措施如下：

(一)帳號管理：

1. 申請人依檢體使用與資訊安全相關辦法，向本庫申請帳號，需善盡保管帳號及密碼之責，如有洩漏,須承擔與實際使用人同等的責任;不得將帳號借予他人或盜用他人帳號及密碼。
2. 本庫人員之帳號與權限由資訊管理人員管控。人員離（休）職時，應立即取消使用各項資訊資源之所有權限，並列入離（休）職之必要手續。

(二)密碼設定：

1. 本庫要求使用者之密碼長度及複雜度：不得太短(六個以上字元)、不得全部為字母或全部為數字、不得與個人有關資料(如身份證字號、生日等)相同等，以確保密碼安全性。
2. 密碼之更新周期，視系統及安全管理需求決定，最長以六個月為限。

(三)特殊權限：

1. 應建立具有特殊權限之人員名冊，加強安全控管，並縮短通行密碼更新周期。
2. 應監控具有資訊設備管理權限、特殊資料存取權限、其他系統資源控制權限及存取稽核軌跡之帳號。
3. 特殊權限帳號之使用應僅限於經授權核准之事項，並留存適當之稽核軌跡。帳號管理人員需定期檢視稽核軌跡是否有異常之處，並視情況限制使用特殊權限之有效時間。

六、可攜式資訊設備作業安全管制措施如下：

(一)本庫專屬可攜式資訊設備應列冊管理;相關人員使用可攜式資訊設備，應注意使用環境之封閉性，儘量避免與本庫外之電腦媒體設備進行檔案傳輸及交換。

(二)相關人員以可攜式資訊設備到本庫以外之場所使用時，須經適當主管之授權，並避免可攜式資訊設備遺失、無人管理或可攜式資訊設備內之檔案或資料遭竊取等。

(三)儲存於可攜式資訊設備之機密資料應考量經適當加密後再行儲存。可攜式資訊設備必要時須考量相關實體保護，例如上鎖或設定開機/檔案密碼等。

七、為確保本庫資料之安全性,需建立資料以及業務處理記錄的異地備份機制,並做備份回存測試,以確保備份資料之可讀性與儲存媒體之可用性。

八、各類人員對於本庫資訊之存取、增刪、查閱、複製時，系統應將執行人員、時間等訊息加以記錄。資訊之存取紀錄，應保留至少六個月，並限制紀錄之存取活動，以維持其完整性。

捌、　資訊系統購置、發展及維護安全管理

一、各項設備採購依政府採購法規定辦理。資訊設備、資料庫或應用程式須經授權後方可使用。

二、本庫資訊系統之發展及維護依照本校醫學院與附設醫院資訊室之規定辦理。若由委託廠商辦理資訊系統之開發與維護，須符合下列規定：

(一)依照本校醫學院委外作業相關規定辦理。

(二)系統開發作業，應考量權限管理、稽核軌跡、加密機制、可擴充性、備份與恢復等，應經過適當之需求分析、可行性及容量評估，並產生相關之系統分析文件或紀錄。

(三)開發、測試環境應與正式環境分別獨立於不同電腦作業系統。

(四)應規範及限制其可接觸之系統與資料範圍，嚴禁核發長期之系統辨識碼及通行密碼。

(五)委外廠商負責資訊系統之建置與維護作業時，應在本庫所屬人員監督下為之。

(六)委外廠商服務異動時，應考量變更對對本庫運作與資訊安全的影響。

玖、 資訊資產之管理

一、各項資訊資產需經測試、完成驗收並列入財產清冊，由資訊主管指定專人管理，至少每年盤點一次。

二、本庫資訊中心指定資訊資產適當之管理者與使用者。相關人員之權責說明如下：

(一)管理者：對於人體生物資料庫擁有最高的權責，得賦予其他人員存取及使用人體生物資料庫的權限。

(二)處理者：負責資訊處理與保管工作並得檢視、使用、存取或異動人體生物資料庫，但不直接接觸檢體。

三、資訊設備移出設置者時，須經資訊安全主管核定，始得放行。

四、各項儲存設備報廢時，應評估其堪用狀況並進行必要之清除動作，避免內存資料外洩，始得辦理報廢。

壹拾、實體及環境安全管理

一、本庫資訊存放於資訊安全室內之機房，並備份於附設醫院資訊室內之異地機房。

二、資訊安全室設有門禁管理與 24 小時攝影監控系統，避免非法進出、存取或破壞行為。

三、資訊安全室設有 24 小時空調、不斷電系統與溫溼度監控設備，以保持穩定之電力與適當的溫濕度。

四、資訊設備之維護由資訊設備處理者執行並留下紀錄。

五、門禁之管制措施：

(一)本庫之各區域(含入口、檢體室與資訊安全室)均設有門禁管制，人員經授權使得刷卡進入，出入之人員與時間均有紀錄。

(二)非經授權之人員欲進入資訊安全室，需先告知並登記，並由本庫相關資訊人員陪同，方可進入。

六、人體生物資料庫各項資料、資訊之安全措施，應依參與者之同意範圍，進行不同等級之保護，並依同意書之變更，更改至適當等級。若因同意書之變更致應銷毀其資料時，應以不可回復之方式銷毀。

七、辦公室桌面管理，重點如下：

(一)使用電腦處理個人資料完畢即應清除畫面，不得將個人資料殘留於電腦終端機上。

(二)個人電腦及終端機不使用時，應有關機、登出、或設定有密碼保護之螢幕保護程式或以其他控制措施進行保護。

(三)公文及檔案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。

(四)棄置之手寫或影印公文廢紙及已過保存期限之公文，若為機密性、敏感性者，應依機密文件管理辦法予以銷毀。

八、發現有不明人士未經許可擅接網路之情事，應立即通知。

九、重要之資訊設備必須上鎖，且保存於合於電腦機房安全之空間。

壹拾壹、　資訊安全事件發生之通報及保全處理程序

一、資訊異常事件通報與處理，原則如下：

(一)為掌握時效正確處理，以降低對本庫作業的危害與損失，工作人員發現資訊異常事件時應立即向資訊主管報告，並通知本校醫學院附設醫院資訊室，說明發生之徵兆與可能來源，以提供主管判斷是否為緊急事件以及受影響之資訊作業範圍。

(二)接獲事件通報後，應依相關作業程序之規定，立即進行回應與處理，並紀錄事件發展與處理情況。

(三)公文及檔案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。

(四)棄置之手寫或影印公文廢紙及已過保存期限之公文，若為機密性、敏感性者，應依機密文件管理辦法予以銷毀。

二、資訊異常事件之記錄及追蹤措施

(一)本庫與本校醫學院附設醫院資訊室相關負責單位應根據相關紀錄，瞭解事件發生之種類、發生頻率、影響範圍、損耗成本等，加以適當評估檢討後，找出問題癥結，並採取相關矯正預防措施。

(二)資訊異常事件如涉及法規或犯罪部份，須確認處理措施符合法規要求，注意處理過程中證據留存事宜，並通報主管機關。

(三)事件處理紀錄，應供日後教育訓練之案例學習使用。

三、若因資訊異常事件影響參與者權益，應於查明後以書面、電話(簡訊)、電子郵件等方式通知相關參與者。參與者可依本庫「遭受侵害情事通報機制及救濟措施規範」，請求救濟措施。

四、資訊安全事件通報及處理程序每年應進行檢討修正。

壹拾貳、　業務持續及回復管理

一、應擬定永續營運管理計畫，包含本庫之營運衝擊分析，遭遇災害時之營運復原計畫，及計畫之測試與演練等。

二、營運衝擊分析及風險評估，內容包含：

(一)瞭解本庫資訊作業活動、資料應復原之時間、復原時所需之資源等。

(二)辨識可能造成資訊作業中斷之各項威脅，評估風險。

三、本庫資訊之備份作業管理程序如下：

(一)每天進行系統自動備份作業至少一次。

(二)每兩個月至少有一備份於附設醫院資訊室作異地儲存，執行人員於完成後填寫備份紀錄，以確保備份媒體安全。

四、本庫每年應至少進行一次備份回復測試作業，並於完成後填寫回復測試紀錄。

壹拾參、　相關法令規定事項，及其他有關資訊安全事項

一、本庫訂定年度資訊安全稽核計畫，並應視需要不定期進行專案稽核；稽核紀錄為永久保存且不允許更改。原則如下：

(一)本庫各資訊相關軟硬體設備與資產之運作狀況。

(二)資訊安全風險評估、備份回復作業等之演練結果與規範之檢討。

(三)資訊異常事件之處理與檢討。

(四)去識別化之資訊再連結的機制。

(五)第三人使用之生物檢體及相關資料、資訊，應於契約內納入資訊安全之要求，且得對第三人進行資訊安全稽核。

(六)稽核計畫、稽核報告結果及改善計畫，應送倫理委員會審查。倫理委員會得視必要，指派人員會同稽核。

二、密碼管理、電子簽章及資料加解密管理

(一)密碼與電子簽章管理，包括加密金鑰與電子憑證的產生及效期，由資訊管理人員依本校醫學院及附設醫院資訊安全規範辦理。

(二)資料之加解密程序統一由系統執行，避免個資外洩。

(三)加、解密作業程序：

1. 個案產生時，系統依個案使用密鑰，並於產生當下即將相關個資加密後儲存。
2. 系統運行中產生之相關記錄，若其中含敏感內容，則以系統密鑰加密後儲存。
3. 系統於產生交換資料時，透過非對稱加密演算法將轉出資訊系統私鑰簽章後，依訊息接收者公鑰進行加密後，以可攜式儲存設備交給訊息接收者，以確保只有訊息接收者可解開(匯出者也無法得知匯出後之內容)。
4. 訊息接收者，至後續系統處理時，系統將以訊息接收者之私鑰解密，且經驗章成功後，執行匯入或後續處理作業，處理後之輸出資料仍須依資料交換規範進行加密後輸出，後續交由其他系統進行處理。

(四)機密性及敏感性資料應有分類管理政策及特殊加密型式需求，如：實體隔離、非對稱式加解密、對稱式加解密、雜湊運算、多重加解密…等。

(五)加密金鑰由兩人(含以上)負責保管，由資訊中心規劃建置備援措施、系統自動加解密作業及人員介入之加解密作業。

三、個人資料管理及去識別管理

(一)參與者個資管理規定及程序，需注意以下事項：

1. 參與者個人資料由資訊處理人員負責管理，需遵守保密規定。
2. 參與者個人資料如需作鑑別，應有授權與處理機制並列管。
3. 如有個人資料的揭露，需研議並經授權方得執行，並有軌跡追蹤管理。
4. 有個人資料保存及備援措施。

(二)資料去識別管理規定及程序，需注意以下事項：

1. 按個人資料保護相關法規，個人資料可分為直接辨識與間接辨識兩大類，應設計相應之去識別措施。
2. 應規劃去識別之個資替代型式，如：編碼、加密或其他無法辨識參與者身分之方式。
3. 生物檢體、資料及資訊進入本庫時，均需與個人資料抽離，以代碼方式取代可辨識之個人資料。

四、去識別資料之再連結

(一)因資料彙整、接受委託或內部資料稽核等原因，經倫理委員會同意，本庫可進行將已去識別之資料與參與者個人資料再連結之作業。

(二)需由本庫資訊最高權限者兩人(含以上)，以金鑰進行解密與再連結作業。

(三)工作完成之後應恢復原本狀態。

五、本管理辦法應經本庫之倫理委員會審查通過後，報主管機關備查，修正時亦同；倫理委員會審查時，應有資訊安全專家參與。

六、本管理辦法應逐年檢討，並作必要之修正。