臺南市政府生物資料庫資訊安全管理規定

壹、目的與依據

為推動臺南市政府生物資料庫(以下簡稱本資料庫)之相關營運作業，符合相關法規，使本資料庫作業有所遵循，特訂定本規定，以確保人體生物資料庫資料符合機密性、完整性及可用性之要求。本規定依據「人體生物資料庫管理條例」第十三條、「人體生物資料庫資訊安全管理規範」及「臺南市政府衛生局資通安全維護計畫」相關規定，訂定「臺南市政府生物資料庫資訊安全管理規定」。

貳、資訊管理單位組織、權責及分工

本資料庫設有資訊安全組，其權責依分工說明如下：

一、 設置組長一人擔任資訊主管：負責辦理生物資料庫資訊安全政策之規劃與推動，並對生物資料庫相關人員(即指生物醫學組)進行資訊安全督導與定(或不定)期稽核及其他資訊安全相關工作。

二、 資訊安全幹事若干人，業務如下：

(一)資料及資訊管理幹事：負責資料與資訊之管理。

(二)資訊系統維運幹事：負責管理資訊軟硬體設備、系統運作平臺之維運。

前兩項人員不得互為兼任。

參、人員管理及資訊安全訓練

一、 資訊安全組應對本資料庫相關人員，進行安全性評估及定期安排每年一次至少 3 小時(含)以上之資訊安全相關教育訓練。

二、 本資料庫、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。

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，應分別由資訊安全組與生物醫學組指定專人管理；該專人不得兼任前項相關資料、資訊之管理人員。

三、 本資料庫之資訊業務如委託其他廠商辦理，應於委託契約書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「人體生物資料庫資訊安全管理規範」納入成為契約之一部分。委託契約書中並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。

臺南市政府生物資料庫重要文件 非經同意請勿複製或轉載

肆、電腦系統與網路安全管理

一、資訊安全組應定期更新電腦病毒碼、修補系統漏洞及防範惡意軟體，確保應用系統正常運作。

二、本資料庫伺服器應以實體隔離之方式建置，對外不得與網際網路連接，對內不得加入區域網路。

三、資訊安全組對於生物資料庫之系統變更作業，應先執行評估，以確保系統安全控制程序不會被破壞，且不會影響生物資料庫程式之運作。

四、生物資料庫有關資訊，非經本資料庫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。經本資料庫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。

伍、資訊系統存取控制管理

一、本資料庫相關人員應訂定系統存取政策及授權規定，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、本資料庫所屬人員之系統存取權限，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，其中最高權限之人員，至少應有二人。

三、資訊安全組對於本資料庫所屬之離(休)職人員，應取消使用本資料庫各項資訊資源之所有權限，並列入離(休)職之必要手續。

四、資訊安全組對於本資料庫所屬之相關人員應建立系統使用者註冊管理制度，加強使用者通行密碼管理，並要求使用者之密碼長度及複雜度；使用者通行密碼之更新周期，由資訊安全組視運用系統及安全管理需求決定，以三個月為限。

五、對於具有系統存取特別權限之人員，應建立使用人員名冊，加強安全控管，並縮短通行密碼更新週期。

六、對於本資料庫相關資訊之存取紀錄，應保留十年，並限制紀錄之存取活動，以維持其完整性。

臺南市政府生物資料庫管理中心 非經同意請勿複製或轉載 臺南市政府生物資料庫管理中心 非經同意請勿複製或轉載

陸、資訊資產之管理

一、資訊安全組對本資料庫資訊系統之建置與維護之廠商，應規範及限制其可使用之系統與資料範圍，並核發短期系統辨識碼及通行密碼；廠商執行建置與維護作業應在資訊安全組人員監督下為之。

二、本資料庫各項資料、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。

三、本資料庫各項資訊設備移出本資料庫時，應經資訊安全組組長之核定，始得放行；各項儲存設備報廢時，應核定其堪用狀況後，始得辦理報廢。

四、本資料庫重要資訊設備應上鎖並保存於電腦機房安全空間；發現有不明人士，未經許可擅接網路之情事，應立即通知資訊安全組人員。

柒、業務持續及回復管理

一、當生物資料庫遭受不可抵抗性之天然災害或人為破壞時之資訊安全事件時，應立即通報應變，並於最短時間內回復業務之正常持續運作。

二、本資料庫應依管理條例第十一條第一項所定之事宜，應擬訂緊急應變作業程序，作成事件處理紀錄，並供日後教育訓練學習使用，且併管理條例第十一條第二項關於救濟措施之規範報主管機關核定。

捌、稽核管理

一、本資料庫應訂定一年一次之資訊安全稽核計畫，並不定期進行資訊安全稽核；稽核紀錄，應永久保存。

二、本資料庫若提供第三人使用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，並準用前項規定，對該第三人進行資訊安全稽核。

三、前兩項之稽核計畫、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。

玖、其他

一、本規定及相關作業程序應依據相關法令之調整而進行檢討修正，並提交本資料庫倫理委員會審查通過，呈長官核示後公告實施，修正時亦同。

二、其他資訊安全規定事項悉依臺南市政府現有各類資訊安全管理規定辦理。

臺南市政府生物資料庫重要文件 非經同意請勿複製或轉載