人體生物資料庫資訊安全規範

一、 設置者訂定之資訊安全管理規定（以下稱資安規定），應包括下列事項：

（一）資訊管理單位之組織、權責及分工。
（二）人員管理及資訊安全訓練。
（三）電腦系統安全管理。
（四）網路安全管理。
（五）資訊系統存取控制管理。
（六）資訊系統購置、發展及 維護安全管理。
（七）資訊資產之管理。
（八）實體及環境安全管理。
（九）資訊安全事件發生之通報及保全處理程序。
（十）業務持續及回復管理。
（十一）本規範與相關法令規定事項，及其他有關資訊安全事項。

資安規定應經設置者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。資安規定應逐年檢討，並為必要之修正。

二、 設置者應指定主管人員負責資訊安全管理事項之協調及推動，並得成立資訊安全推行小組，辦理資訊安全政策、規劃、執行等審議、督導事項。

三、 設置者對資訊有關業務及人員，應進行安全評估。

四、 設置者應依所屬人員之業務特性，定期辦理資訊安全教育。

五、 設置者、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。

六、 設置者得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。

七、 設置者應定期更新漏洞、電腦病毒碼及其他惡意軟體防範之程式，確保應用系統正常運作。

八、 收案後所建置之生物資料庫之個人資料，應以實體隔離之方式建構及使用，其資訊系統不得與網際網路連接。

九、 生物資料庫有關資訊，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。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。

十、 設置者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。

十一、 設置者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，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。

十二、 設置者離（休）職人員，應立即取消使用設置者各項資訊資源之所有權限，並列入離（休）職之必要手續。

十三、 設置者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，由設置者視運用系統及安全管理需求決定，最長以六個月為限。

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周期。

資訊之存取紀錄，應保留一定期間，並限制紀錄之存取活動，以維持其完整性。

十四、 設置者對生物資料庫資訊系統之建置與維護之承作者，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期之系統辨識碼及通行密碼；承作者執行建置維護作業，應在設置者所屬人員監督下為之。

十五、 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。

十六、 生物資料庫各項資訊設備移出設置者時，應經資訊安全管理主管人員之核定，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。

發現有不明人士，未經許可擅接網路之情事，應立即通知。

重要之資訊設備，必須上鎖，且保存於合於電腦機房安全空間。

十七、設置者為辦理人體生物資料庫管理條例（以下簡稱本條例）第十一條第一項所定之事宜，應事前擬訂建立資訊安全事件通報機制，作成事件處理紀錄，並應供日後教育訓練學習使用，且併同本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。

十八、設置者應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，應永久保存。

設置者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。

前二項之稽核計畫、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。