資訊安全政策

文件制/修訂紀錄

版本	發行日期	修訂說明	撰寫者	審閱者
V1	2015.06.05	新制訂文件	黃毓婷	李金美

壹、 目的

人體生物資料庫之人體生物資料保存庫(以下簡稱本資料保存庫)導入資訊安全管理系統(簡稱 ISMS)，以保護資訊免受內部或外部、蓄意或意外之威脅，以強化資訊安全管理，特訂定本政策。

貳、 適用範圍

本政策適用本資料保存庫之資訊安全管理，需遵守人員包括本資料保存庫內部人員、本中心委外與往來之外部廠商或機關、使用檢體相關資料、資訊之人員。

參、 資訊安全目標

一、 確保使用檢體相關資料、資訊之機密性，以及人員符合衛生福利部規定，確保生物資料庫資訊系統管制人員權限並嚴禁開放遠端維護。

二、 針對參與者提供之個人資料及其他相關資料、資訊，建立適當保護，在安全作業區內設置門禁管制並具錄影監視設備確保僅有授權人員進出。

肆、 政策推動

一、 本資料保存庫成立資訊安全管理小組，負責資訊安全管理系統之研議、建置及評估。本資料保存庫主管由本院院長擔任，資訊室主任擔任資訊安全管理代表。

二、 資訊安全管理小組設置、管理階層輸入與輸出審查，將依據「資訊安全管理小組運作程序書」辦理。

三、 本資料保存庫資訊安全管理系統應依據下列原則建立：

（一） 鑑別外部與內部會影響本資料保存庫資訊安全管理目的。

（二） 鑑別與有關的利害相關者，以及其對資訊安全要求。

（三） 遵守政府法令要求，例如：政府資訊公開法、個人資料保護法及其施行細則等。

（四） 遵守主管機關規定，例如：衛生福利部「人體生物資料庫管理條例」、「人體生物資料庫資訊安全規範」等。

（五） 參考國際資訊安全管理標準，例如：ISO/IEC 27001：2013（以下簡稱 ISO 27001）、ISO/IEC 27002：2013 等。

四、 為有效推動資訊安全管理相關工作，資訊安全管理小組得委請學者專家或民間專業組織及團體，提供顧問諮詢服務。

五、 在規劃 ISMS 時，應考慮本資料保存庫面臨的資訊安全問題與要求，決定需要解決的風險和機會，提供適切資源。

（一） 確保 ISMS 實現本資料保存庫預期結果。

（二） 防止或減少對本資料保存庫不利的影響。

（三） 實現持續改進 ISMS 承諾。

六、針對 ISMS 面臨的風險和機會，應規劃需要採取的行動，並滿足以下要求：

（一） 在本資料保存庫落實 ISMS 所建立的管理系統中，整合與實施這些行動。

（二） 透過量測評估相關行動的有效性。

七、 有效性量測

（一） 資訊安全規劃人員應依據以下規定，設計「資訊安全管理有效性量測單」，規劃各項資訊安全管理量測指標：

1. 依據資訊安全目標，設計評量目標達成之指標。
2. 配合資訊安全管理小組會議決議，規劃與調整有

效性量測指標。

（二） 資訊安全人員每年應填寫「資訊安全管理有效性量測單」，進行資訊安全管理量測，並出席資訊安全管理小組，報告量測結果。

（三） 本資料保存庫應針對未達到有效性量測指標之案件，依據「改善措施管理程序書」之程序，提出改善措施。

八、 人員於本資料保存庫發現資訊安全事件，或明顯、可疑之安全弱點時，應依據「資安事故與營運持續管理程序書」規定，向本資料保存庫進行通報。

九、 本政策適用範圍之人員，應遵守本政策及資訊安全管理系統各項文件規定。

十、 人員違反資訊安全管理規定者，或行使其他任何危及本資料保存庫資訊安全之行為，都將訴諸適當之懲罰程序或法律行動。

伍、實行和修正

一、 本政策應每年定期或依組織、業務和環境等變動因素之適當性予以修訂。

二、 本政策應以書面、電子郵件或其他方式告知適用範圍之人員，以共同遵行。

三、 本政策經本**資料**保存庫主管核可後實施，修正時亦同。

陸、使用表單

一、資訊安全改善措施單(文件編號:ISMS-4-01)

二、資訊安全管理有效性量測單(ISMS-4-02)