至善資訊安全政策

機密等級：一般使用

初版日期：2021.11.01

1. **目的**

本政策規範至善基金會(本會)資訊安全管理制度，以確保本會管轄資訊資產之機密性、完整性、可用性及符合相關法規之要求，進而保障機構同仁及捐款人之權益。

2. **適用範圍**

本機構同仁、接觸本機構業務資料之外部人員、委外服務提供廠商人員及訪客。

3. **名詞定義**

3.1. 機密性（Confidentiality）：使資訊不可用或不揭露給未經授權之個人、個體或過程的性質。

3.2. 完整性（Integrity）：保護資產的準確度（Accuracy）和完全性（Completeness）的性質。

3.3. 可用性（Availability）：經授權個體因應需求之可存取及可使用的性質。

3.4. 法律遵循性：系統運作、資料保護、資訊資產使用等若未依循法律規範辦理，造成可預期的負面影 響較輕微。

3.5. 資訊安全：係避免因人為疏失、蓄意或自然災害等風險，運用系統化之控制措施，包含政策、實施、稽核、組織結構和軟硬體功能等，以確保本機構資訊資產受到妥善保護。

3.6. 資訊資產：凡本機構作業流程中使用之資訊資產，如內部人員、外部人員、紙本文件、電子文件、網路服務、電腦應軟體、應用系統、電腦硬體、網路設備、環控系統、建築保護設施與便利設施等皆屬之。

4. **權責**

設置本機構「資訊安全暨捐款人個人資料保護專案小組」，負責政策之核定及監督、資訊安全預防及危機處理。

5. **要求事項**

5.1. 資訊安全目標

5.1.1. 本機構每年無捐款人及同仁密級資料外洩。

5.1.2. 本機構每年無捐款人及同仁資料(如:同仁薪資或捐款人個人資料)遭竄改或外洩。

5.1.3. 確保本機構關鍵業務系統資訊系統維運服務達全年上班時間95%以上之可用性，並確保：

A. 因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每年不得超過 8 次。

B. 因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過 8 工作小時。

5.1.4. 本機構關鍵業務系統服務達全年上班時間 98%以上之可用性，中心關鍵業務系統因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過 4 工作小時。

5.2. 資訊安全管理事項

避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本機構帶來各種可能之風險及危害。資訊安全管理應涵蓋 14 項管理事項：

1.資訊安全政策。

2. 資訊安全組織。

3. 人力資源安全。

4. 資產管理。

5. 存取控制。

6.金鑰加密控制。

7. 實體與環境安全。

8. 運作安全。

9.通訊安全。

10.資訊系統取得、開發及維護。

11. 系統廠商關係。

12.資訊安全事故管理。

13. 營運持續管理之資訊安全層面。

14.遵循性。

5.3. 資訊安全管理原則

5.3.1. 重要之資訊資產應定期清查、分類分級與進行風險評鑑，並據以實施適當的防護措施。

5.3.2. 重要資訊資產存取權限應予以區分，考量人員職務授予相關權限，必要時得採行加解密(金鑰)及身分鑑別機制，以加強資訊資產之安全。

5.3.3. 對於資訊安全事件須有完整的通報及應變措施，以確保資訊系統、業務的持續運作。

5.3.4. 應訂定營運持續計畫並定期演練，以確保重要系統、業務於資安事故發生時能於預定時間內恢復作業。

5.3.5. 相關人員應依規定接受資訊安全教育訓練與宣導，以加強資訊安全認知。

5.3.6. 定期執行資訊安全稽核作業，檢視存取權限及資訊安全管理制度之落實。

5.3.7. 違反本政策與資訊安全相關規範，依相關法規或本機構懲戒規定辦理。

5.3.8. 本政策每年至少評估一次，依業務變動、技術發展及風險評鑑的結果修訂。

6. 修訂

6.1. 管理階層審查

確保「資訊安全管理系統」實務運作之可用性、安全性及有效性。本政策每年依業務變動、技術發展及風險評鑑的結果或配合政府資訊安全管理要求、法令、技術及最新業務發展現況至少評估或修訂一次。

7. 施行

7.1. 本政策須經「資訊安全暨捐款人個人資料保護專案小組」審核，核定後依據「文件暨紀錄管理辦法」公告或傳達給本機構各單位同仁與相關外部單位實施，修訂時亦同。