佛教慈濟慈善事業基金會

Taiwan Buddhist Tzu Chi Foundation

資訊安全政策

1.目的

隨著資訊化作業及個人資料保護法之實施，為確保個人資料及勸募資料安全性，建置完善資訊安全系統已成為不可或缺之重要措施，因此為確保佛教慈濟慈善事業基金會（以下簡稱本會）資訊系統服務正常且安全穩定的運作，特制定資訊安全政策（以下簡稱本政策）以作為規範本會之資訊安全管理制度最高指導方針，以建立安全、可信賴之資訊系統服務，並確保本會之資訊資產之機密性、完整性、可用性及適法性，以維持本會業務持續運作，降低資訊作業風險，進而保障本會資訊系統服務使用者之權益及資產安全。同時建立資訊安全人人有責之觀念，共同遵循本會資訊安全相關規範。

2.適用範圍

2.1 基於保護本會資訊資產機密性、完整性、可用性與適法性為目標，資訊處、資訊機房、資訊系統及網路系統維運安全管理作業為本會資訊系統服務之核心所在，故以資訊機房、台灣勸募資訊系統（以下簡稱勸募系統）作業定為本會資訊安全管理範圍，推動建置完善資訊安全管理制度與服務系統，以保障本會資訊資產安全。

2.2 參照ISO27001/CNS27001 本文及資訊安全要項，資訊處、資訊機房、資訊系統及網路系統維運安全管理作業之資訊安全要項涵蓋14項管理事項，其目的在於避免因人為疏失、蓄意或天然災害等因素，導致資訊資產不當使用、洩漏、竄改、破壞等情事發生，進而對本會帶來可能之風險及危害。管理事項如下：

資訊安全政策、資訊安全的組織、人力資源安全、資產管理、存取控制、密碼學、實體及環境安全、運作安全、通訊安全、系統獲取、開發及維護、供應商關係、資訊安全事故管理、營運持續管理、遵循性管理。

2.3 適用人員: 於本會服務之員工、約聘人員、工讀生及外包供應商

3.相關文件

3.1 資訊安全管理作業程序

3.2 慈善志業資訊保密辦法

4.名詞定義

4.1 資訊安全

保存資訊的機密性、完整性、可用性、適法性；此外亦能涉及如鑑別性、可歸責性、不可否認性及可靠度等性質；亦避免因人為或自然災害等風險，運用系統化之控制措施，以確保資訊安全管理制度範圍內之資訊資產受到妥善保護。

4.2 資訊資產

凡資訊處、資訊機房、資訊系統及網路系統之資產，如文件、人員、軟體、硬體、服務與建築等皆屬之。

4.3 資訊安全異常事件

凡因人為或自然災害因素，造成本會資訊系統服務中斷，或本會資訊資產遭竄改、刪除或竊取等，皆屬之。

4.4 基金會方針

深入法脈精神，發揮粽頭良能；加強宗門連結，展現四大一體；

活絡組織合和，培育人才傳承；善用資訊整合，精實流程效率。

5. 作業說明

5.1 權責

5.1.1 資訊發展暨安全管理委員會

本會資訊系統發展暨安全管理階層決策組織。

5.1.2 資訊安全推動組

本會資訊處、資訊機房、勸募資訊系統及網路系統資訊安全管理制度規劃、建立、實施、維護、審查與持續改善，並將資訊安全相關議題於資訊發展暨安全管理委員會提報。

5.1.3 所有員工、約聘人員及外包供應商

皆應遵循本資訊安全政策，共同維護本會資訊安全。

5.2 通則

5.2.1 應考量相關法律規章及營運要求，進行資訊資產之資訊風險評鑑，確定資訊作業安全需求，採取適當資訊安全措施，確保資訊資產安全。

5.2.2 依角色及職能為基礎，建立評估或考核制度，並視實際需要辦理資訊安全教育訓練及宣導。

5.2.3 定期執行資訊安全稽核作業，檢視資訊安全管理制度之落實。

5.2.4 資訊資產存取權限之賦予，應業務需求並考量最小權限與權責區隔。

5.2.5 建立資訊安全事故通報及應變程序，以確保本會資訊服務能持續運作。

5.2.6 訂定業務持續計畫並定期演練，以確保本會重大資安事故發生時，能妥善回應。

5.2.7 依據個人資料保護法與著作權法等相關規定，審慎處理及保護勸募電子紀錄、個人資訊與著作權。

5.2.8 為確保本會同仁皆知悉本會資訊安全要求，公告本會同仁周知。

5.2.9 辦理資訊安全宣導課程，強化員工資訊安全之認知，建立資訊安全人人有責之觀念。

5.2.10 若違反本政策與資訊安全相關規範,依相關法規或本會人事規定辦理。

5.3目標

5.3.1 維持本會營運資訊系統服務持續順暢正常運作。

5.3.2 保護本會資訊資產，防止人為意圖不當或不法使用，遏止駭客、病毒等入侵及破壞之行為，以保障勸募及個人資料等資訊資產之機密性、完整性、可用性。

5.3.3 建立本會資訊系統服務之標準作業程序，避免人為作業疏失及意外，同時加強同仁資訊安全意識。

5.3.4 辦理本會資訊安全目標之規劃、量測、審查及改善，以因應不同資訊安全之要求與期望，力求達成資訊安全管理之目標。

5.3.5 為確保上述政策目標實務作業的可行性及有效性，並符合基金會方針，依據資訊安全管理作業程序訂定有效性量測表，每年針對各項政策目標實施有效性量測。

5.3.6 資訊安全目標量測

5.3.6.1 未經授權存取，機密資料(個人資料)外洩：不得發生

5.3.6.2 未經授權存取，機密資料(個人資料)遭篡改：不得發生

5.3.6.3 資訊安全異常事故4級：每年不得超過1件

5.3.6.4 資訊安全異常事故3級：每年不得超過12件

5.3.6.5 勸募系統線上資訊服務可用率(業務期間)：每年達95%以上

5.3.6.6 勸募系統相關主機群設備運轉使用良率：每年達95%以上

5.4 審查

5.4.1 本政策應至少每年審查一次，以反映相關法令、技術及資訊服務等最新發展現況，並予以適當修訂。

5.4.2 本政策經本會資訊發展暨安全管理委員會核准，於公告日施行，並以書面、電子或其他方式通知所有員工及提供資訊服務之相關廠商與關注方，修正亦同。