

佛教慈濟慈善事業基金會
Taiwan Buddhist Tzu Chi Foundation

資 訊 安 全 政 策

編號：TCF-ISMS-A-01

版次：1.0

實施日期：2022年11月1日

<h1 style="margin: 0;">佛教慈濟慈善事業基金會</h1> <p style="margin: 0;">Taiwan Buddhist Tzu Chi Foundation</p>				機密 等級	內部使 用
文件 編號	TCF-ISMS-A-01	文件 名稱	資訊安全政策	頁次	1/4
				版次	1.0

1. 目的

為確保財團法人中華民國佛教慈濟慈善事業基金會（以下各階文件均簡稱本會）勸募系統及捐款者資料安全，制定本資訊安全政策作為規範本會資訊安全管理程度最高指導方針，以建立安全、可信賴之資訊系統服務與資訊安全人人有責之觀念，確保本會之資訊資產之機密性、完整性、可用性及適法性，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。

2. 目標

2.1 維持本會營運資訊系統服務持續順暢正常運作。

2.2 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、惡意程式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。

2.3 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。

2.4 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。

2.5 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。

2.6 資訊安全目標量測

2.6.1 勸募系統線上資訊服務可用率(業務期間：上午 07 時至下午 19 時，每周 7 天，線上資訊服務)：每年達 95%以上。

佛教慈濟慈善事業基金會				機密 等級	內部使 用
Taiwan Buddhist Tzu Chi Foundation					
文件 編號	TCF-ISMS-A-01	文件 名稱	資訊安全政策	頁次	2/4
				版次	1.0

- 2.6.2 勸募系統AP主機發生異常次數：每年不得超過 18 件。
- 2.6.3 未經授權存取，機密資料(個人資料)外洩：不得發生。
- 2.6.4 未經授權存取，機密資料(個人資料)遭篡改：不得發生。
- 2.6.5 資訊安全異常事故 4 級：每年不得超過 1 件。
- 2.6.6 資訊安全異常事故 3 級：每年不得超過 12 件。

3. 適用範圍

3.1 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。

3.2 位於花蓮縣新城鄉本會精舍資訊機房、勸募資訊系統(台灣)(以下簡稱勸募系統)，定為資訊安全管理範圍，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。

3.3 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。

4. 作業說明

4.1 本項政策制定應考量組織特性與法令、法規要求，建立資訊安全各項原則，並由資訊安全管理審查委員會所核准；依據資訊安全管理制度範圍內資訊資產之風險，實施各項風險控制機制，以保障資訊資產之機密性、完整性、可用性 & 適法性。

佛教慈濟慈善事業基金會				機密 等級	內部使 用
Taiwan Buddhist Tzu Chi Foundation					
文件 編號	TCF-ISMS-A-01	文件 名稱	資訊安全政策	頁次	3/4
				版次	1.0

4.2 資訊安全管理作業方法，依據【TCF-ISMS-B-01 資訊安全管理作業程序書】律定執行，執行作業所需人員及任務，以編組方式成立資訊發展暨安全管理委員會，權責及任務參照【TCF-ISMS-B-02 資訊安全組織管理程序書】。

4.3 通則

- 4.3.1 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。
- 4.3.2 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。
- 4.3.3 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。
- 4.3.4 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。
- 4.3.5 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。
- 4.3.6 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。
- 4.3.7 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。
- 4.3.8 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。
- 4.3.9 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。
- 4.3.10 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。

4.4 審查

- 4.4.1 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。
- 4.4.2 本政策經本會資訊安全管理審查委員會核准，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。

<h1>佛教慈濟慈善事業基金會</h1> <p>Taiwan Buddhist Tzu Chi Foundation</p>				機密 等級	內部使 用
文件 編號	TCF-ISMS-A-01	文件 名稱	資訊安全政策	頁次	4/4
				版次	1.0
<p>5. 相關文件</p> <p>5.1 TCF-ISMS-B-01 資訊安全管理作業程序書</p> <p>5.2 TCF-ISMS-B-02 資訊安全組織管理程序書</p>					