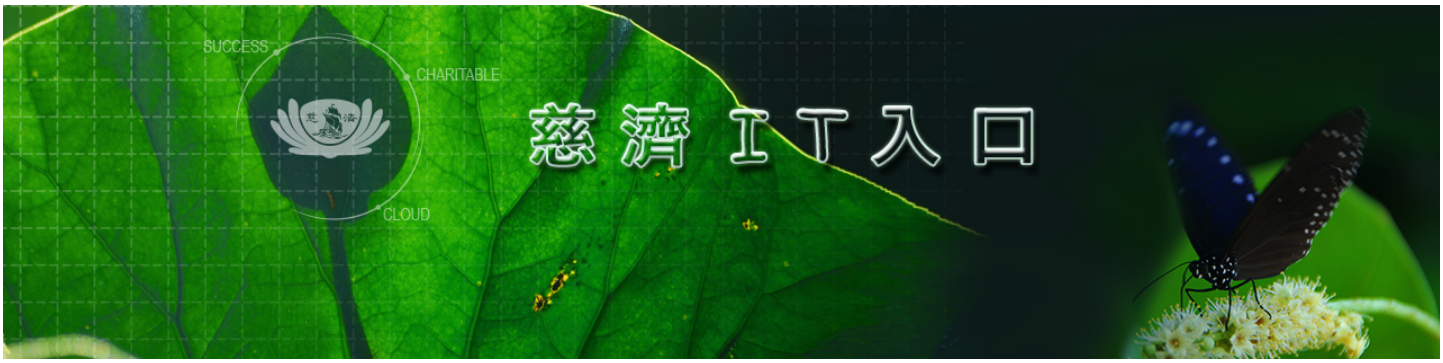
慈濟IT入口



公告

資安政策

強化資安防護能力，提升系統與網路作業環境安全。

1. 目的
   為確保本會驗證範圍資訊資產之機密性、完整性、可用性，並符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅。
2. 目標
   ● 確保本會營運資訊系統服務持續順暢正常運作，維持資訊資產之可用性。
   ● 建立資訊系統服務之標準作業程序，以降低人為疏失與意外風險，並透過教育訓練與宣導活動，強化全體同仁之資訊安全意識。
   ● 依據資通安全管理範疇，辦理資訊安全目標之規劃、量測、審查及持續改善，以因應不同資訊安全需求與期望，提升整體資安管理效能。
   ● 每年依資訊安全管理作業程序，執行政策目標之有效性量測與檢討，以確保各項措施之可行性與成效，並符合本會方針與法令規章要求。
3. 2026年資安目標
   勸募系統與慈善個案系統上班期間資訊服務可用率：
   扣除因系統維護得停止服務時間，全年服務可用率達98%以上
   勸募系統與慈善個案系統AP主機發生異常次數：每年不得超過14件。
   資通安全事件、事故時， 不得有未通報情形。

慈濟IT入口

多層次資安落實方案說明：

我們將資安措施分成 **網路設備與資源**、 **伺服器儲存安全**、 **備份安全**、 **資料庫安全**、 **專案開發安全**、 **用戶端安全**、 **管理特權**、 **災難緊急應變措施** 等層面。每個層面皆呼應先前提到的「六大防護」：

1. **網路設備與資源：** 對應「六大防護」中的 *「網路入侵防護」* 與 *「網站滲透測試」*。 我們透過防火牆、入侵偵測系統（IDS/IPS）及定期滲透測試， 強化網路層安全。
2. **伺服器儲存安全：** 對應 *「內部異常行為偵測」* 與 *「委外與開發資安健檢」*。 除加強系統日誌監控，也確保第三方或內部開發符合資安規範。
3. **備份安全：** 對應 *「ISO27001資安驗證」* 及 *「雙因認證與異地連線安全」*。 確保備份資料異地存放、權限管控與檢測。
4. **資料庫安全：** 呼應 *「網站滲透測試」* 與 *「委外與開發資安健檢」*， 從程式碼層面與 DB 層面落實 SQL Injection 防禦、權限最小化等。
5. **專案開發安全：** 對應 *「委外與開發資安健檢」*， 在專案開發全流程進行資安審核與程式碼檢測。
6. **用戶端安全：** 呼應 *「網路入侵防護」* 與 *「內部異常行為偵測」*， 加強終端防毒、防惡意程式、防社交工程訓練等。
7. **管理特權：** 對應 *「雙因認證與異地連線安全」*， 透過多因子認證、權限分層與審計， 降低高權限帳號被盜用風險。
8. **災難緊急應變措施：** 呼應 *「ISO27001資安驗證」* 中的營運持續與災難復原規範， 確保在突發狀況時能迅速回復關鍵服務。

六大資安防護

網路入侵防護

發現異常行為或攻擊事件，進行阻擋防禦，建立防火巷

委外與開發資安健檢

委外與內部開發資安檢測，開發安全。

內部異常行為偵測

發現內部異常行為或內部攻擊事件，杜絕內部惡意行為

ISO27001資安驗證

提升慈濟品牌形象；遵守法規、確保營運持續；證明善盡管理責任，讓會員確信個資受保護；彰顯資安公信力，展現最佳實務。

網站滲透測試

以駭客思維及攻擊模式進行安全測試，藉此了解系統主機及程式存在漏洞，並提供修復及防禦建議。

雙因認證與異地連線安全

降低管理員帳號密碼遭竊風險，導致全資訊服務帳密淪陷，增加高權限帳號之安全性。

透過上述層面與「六大防護」的對應，可以看出本方案從網路、系統、應用到人員與災難應變 都進行了全面落實，確保資安風險降到最低。