基督教台灣浸會神學院

資訊安全作業要點

機密等級：一般

文件編號：教 1082G0101 資訊安全作業要點 0205

版 次：1.0

發行日期：2020.2.5

民國一０九年二月五日資訊安全委員會議通過

1. 目的

為確保基督教台灣浸會神學院（以下簡稱「本校）資訊安全管理作業推行，符合資訊安全政策之目標，特訂定本作業要點。

2. 適用範圍

本作業要點適用之管理範圍為本校教職員與學生個人資料處理及其相關資訊服務。

3. 權責

3.1. 資訊安全長：由校長擔任，負責綜理資訊安全管理作業協調與督導工作。

3.2. 資訊安全官：由行政管理中心主任擔任，負責規劃及管理資訊安全管理作業相關事宜。

3.3. 執行單位：由行政管理中心資訊組擔任，負責執行資訊安全管理作業相關事宜。

3.4. 稽核小組：由校方指派人員擔任，負責規劃及執行資訊安全管理作業稽核工作。

3.5. 全體人員（含委外廠商）：配合及遵守資訊安全各項要求及規定。

4. 相關文件

4.1. 教育體系資通安全管理規範

4.2. 資訊安全政策

4.3. 外部連絡清單

4.4. 資訊服務申請表

4.5. 委外廠商保密切結書

4.6. 資訊安全事件報告單

4.7. 人員安全守則

4.8. 防火牆進行規則申請表

4.9. 資訊異常事件表

4.10. 資訊資產清冊

5. 作業說明

5.1. 資訊安全組織

5.1.1. 資訊安全長須每年至少召開一次資訊安全管理審查會議，討論內容包括如下：

5.1.1.1. 資訊安全稽核與審查之結果。

5.1.1.2. 來自利害相關者之回饋。

5.1.1.3. 可用於組織以改進資訊安全績效與有效性之技術、產品或程序。

5.1.1.4. 預防與矯正措施之執行狀況。

5.1.1.5. 資安政策目標達成性衡量結果。

5.1.1.6. 前次相關會議結論之跟催結果。

5.1.1.7. 可能影響資訊安全管理作業之任何變更。

5.1.1.8. 加強或改進資訊安全的其他各項建議。

5.1.2. 管理審查會議討論結果應包含：

5.1.2.1. 資安政策目標之改進。

5.1.2.2. 因為下列項目之變更，所進行之因應措施。

5.1.2.2.1. 各項營運要求。

5.1.2.2.2. 各項安全要求。

5.1.2.2.3. 影響既有各項營運要求之營運過程。

5.1.2.2.4. 法律或法規各項要求。

5.1.2.2.5. 契約的各項義務。

5.1.2.3. 資源需求。

5.1.3. 管理審查會議應留存相關會議紀錄備查。

5.1.4. 資訊處理設備之使用，應具授權程序。

5.1.5. 為確保資訊安全作業的順利運行，應建立能與相關外部團體（主管機關、廠商等）即時連繫之「外部連絡清單」（如附件一）。

5.1.6. 任何資訊委外業務，皆應考量與包含資訊安全需求，且明訂 廠商之資訊安全責任及保密規定，並列入契約。

5.2. 資訊資產分類與管制

5.2.1. 為確實掌控資訊資產現況，行政管理中心資訊組須編製資訊資產清冊並定期更新(附件二：資訊資產清冊)。

5.3. 人員安全管理與教育訓練

5.3.1. 行政管理中心資訊組應依主管機關要求，辦理資訊安全教育 訓練及宣導，強化教職員資訊安全認知，必要時應請委外廠商人員一同參與資訊安全教育訓練。

5.3.2. 人員離職，須依流程辦理資訊資產移交，並即時移除相關存取權限。

5.3.3. 各單位若有資訊服務需求（如：帳號申請、電腦維修、系統開發或程式修改等），應填寫「資訊服務申請表」（附件三），經行政管理中心主任核准後，交由行政管理中心資訊組依需求處理。

5.3.4. 本校教職員工之資訊安全管理相關規定，須遵守「資訊安全守則」。

5.3.5. 本校委外廠商所執行之業務，若涉及個人隱私資料，承辦人員應要求其簽訂「委外廠商保密切結書」（附件四）。

5.3.6. 對於委外廠商提供之服務，行政管理中心資訊組應監視和審查，確認服務內容滿足合約之要求。

5.3.7. 委外廠商(人員)異動、合約到期或其他因素服務終止時，行政管理中心資訊組須確認其歸還各項設備、軟體、文件或鑰匙等，並取消存取權限。

5.4. 實體與環境安全

5.4.1. 學校應採取適當防護措施以保障人員辦公處所安全。

5.4.2. 重要資訊設施應設置於機房，並確保經授權人員方可進出。

5.4.3. 機房應採取適當的控制措施與指引，確保其安全性。

5.4.4. 機房內應保持整齊清潔，並嚴禁飲食或堆置易燃物。

5.4.5. 機房宜設置足量之不斷電系統（UPS），確保重要資訊設備在非預期斷電情

況下能具足夠電源完成緊急處置。

5.4.6. 冷氣機、不斷電系統（UPS）等機電設備之使用，應依照設備說明書指示操作，並施行檢查作業。

5.4.7. 資訊設備報廢與再使用時，應將含有個人隱私資料及有版權的軟體移除。

5.4.8. 禁止資訊設備在未經授權之情況下攜離所屬區域，若需將設備攜出，應填寫「設備進出紀錄表」（附件五）。

5.5. 通訊與作業安全管理

5.5.1. 資訊單位應建立資訊系統之安全控管機制，保護資料、系統及網路作業，防止未經授權之存取。

5.5.2. 伺服主機及網路設備應指定負責人，確保設備正常運作。

5.5.3. 新資訊系統、系統升級，正式上線前應適當的測試，並依驗收規定完成驗收。

5.5.4. 學校內電腦（伺服主機、個人電腦、筆記型電腦等）應安裝防毒軟體，定期更新病毒碼並定期掃描。

5.5.5. 各項系統資料（如：設定檔、網頁資料、伺服器日誌、資料庫等）應由行政管理中心資訊組執行定期備份。

5.5.6. 系統資料以可攜式儲存媒體保存時，應將該儲存媒體存放於上鎖儲櫃或安全處所。

5.5.7. 可攜式儲存媒體若存有個人隱私資料，應加密儲存或實施安全控管措施。

5.5.8. 可攜式儲存媒體的遞送，應妥善包裝保護。

5.5.9. 行政管理中心資訊組變更系統作業程序時，應適時修改維護相關文件（如：系統文件、操作手冊等）。

5.5.10. 對外開放之資訊系統，其帳號密碼、個人資料等機密性資料傳輸過程應以加密方式處理，並妥善保管該資料，防止遭竊取或擅自挪作他途之用。

5.5.11. 以電子郵件傳送含有個人隱私之資料時，宜以加密機制保護。

5.5.12. 學校網頁資訊之公布，應經權責管理人員審查，確認內容未含個人隱私之資料及無違反學校規定與法令、法規之要求。

5.5.13. 重要系統應留存電腦稽核紀錄，並妥善保護與保存，以作為日後調查及監督之用。

5.5.14. 行政管理中心資訊組發現資訊系統異常、駭客入侵等異狀時，應進行緊急應變處置並通報行政管理中心主任，並填寫「異常事件紀錄表 」（附件六），留存系統異常處理紀錄備查。

5.6. 存取控制安全

5.6.1. 資訊系統使用權限之申請、異動應依「資訊服務申請表」流程辦理。

5.6.2. 使用者職務異動或離職時，使用單位應填寫「資訊服務申請表」提供給行政管理中心，終止使用者之存取權限。

5.6.3. 各項設備與系統相關之使用權限（例如使用者帳戶與作業權限）宜有授權紀錄，以備查核。

5.6.4. 系統管理人員結束系統操作應登出系統，並鎖定主控台螢幕。

5.6.5. 宜依業務性質之不同，區分不同內部網路網段，例如：行政、 宿網、資

訊中心等，以降低未經授權存取之風險。

5.6.6. 行政管理中心資訊組應定期監控網路使用狀況，例如：網路流量、封包等，以及早發現異常狀況。

5.6.7. 對於開放提供外部使用者或廠商存取之服務，必須限制使用者之網路功能以確保網路安全。

5.6.8. 避免委外廠商使用系統管理者帳號（例如：Root、Administrator）或共用帳號，以釐清責任。

5.7. 系統開發與維護之安全

5.7.1. 系統開發應包含安全性功能之規劃。

5.7.2. 應用系統之資料輸入，應檢核、過濾主要欄位之資料輸入或資料內容，以確保資料的有效性及真確性。

5.7.3. 輸出之資料，應確認其正確性；對於系統內之資料處理，則須保護其完整性。

5.7.4. 作業系統變更，應審查與測試，以確保現行資訊系統與服務正常運作。

5.7.5. 系統軟體應由行政管中心資訊組進行安裝，避免使用者自行安裝錯誤造成營運異常。

5.8. 資訊安全事件之反應及處理

5.8.1. 資訊安全事件依影響等級區分為 4 個級別，由重至輕分別為「4 級」、「3 級」、「2 級」及「1 級」。

5.8.1.1. 「4」級事件，符合下列任一情形者：

5.8.1.1.1. 法令、法規所規範應保護之資料外洩（例如：個人隱私資料）。

5.8.1.1.2. 重要系統或資料遭竄改、破壞或嚴重毀損。

5.8.1.2. 「3」級事件，符合下列任一情形者：

5.8.1.2.1. 敏感資料外洩（如：財會資料、系統文件）。

5.8.1.2.2. 重要系統運作停頓，影響業務正常運作。

5.8.1.3. 「2」級事件，符合下列任一情形者：

5.8.1.3.1. 內部行政資料外洩（如：校內行政資料）。

5.8.1.3.2. 非重要系統運作遭影響或系統停頓，已影響業務正常運作。

5.8.1.4. 「1」級事件，符合下列情形者：

5.8.1.4.1. 系統運作遭影響或系統停頓，不致影響業務正常運作。

5.8.2. 人員發現資訊安全事件，應即時通報，並記錄於「資訊安全事件通報單」（附件七）。

5.8.3. 資訊安全事件確認處理完成後，行政管理中心應檢討現行管理措施之完整性，必要時進行檢討會議，討論改善之事宜。

5.9. 相關法規與施行單位政策之符合性

5.9.1. 學校應蒐集相關法律條文（如：智慧財產權、資料隱私保護 及其他相關法規）、管理規定及合約要求，以確保相關作業符合要求。

5.9.2. 學校應定期進行弱點掃描或滲透測試，確保資訊系統之運行符合既定之安全實施標準，執行結果應留存紀錄。

5.9.3. 系統稽核工具之使用應審慎進行，避免造成系統中斷。

6. 違反規定之處理

6.1. 人員未遵循上述規定者，視情節重大，提報資訊安全委員會議處。

6.2. 本作業要點經資訊安全委員會會議通過後，陳請校長核定後公布實施，修訂時亦同。

【附件一】

基督教台灣浸會神學院

外部連絡清單

單　位	聯絡人					備　註
	職稱	姓名	電話	行動電話	電子郵件／地址	

基督教台灣浸會神學院資訊資產清單

機密等級：

文件編號：

版　　次：

紀錄編號：

填表日期：　　年　　月　　日

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值

資產類別：通訊（CM）、資料（DA）、文件（DC）、環境（EV）、硬體（HW）、人員（PE）、軟體（SW）

使用本表單之前，請確認表單版本是否已更新

【附件三】

基督教台灣浸會神學院資訊服務申請表

申請人		所屬單位		申請日期	年　　月　　日

以下為申請單位填寫

1.應用系統權限申請

☐系統後端權限	☐課程管理　☐課程標準　☐開課　☐排課　☐自動選課　☐線上選課　☐成績管理 ☐畢業管理　☐課程抵免　☐自我評量　☐教學評量 ☐其他： 開始日期：　　年　　月　　日　結束日期：　　年　　月　　日

2.新進人員帳號申請

人事編號 (此部份人事組填寫)		個人電子郵件信箱 (此部份申請者填寫)	

☐校內系統帳號 ☐臨時使用無線網路 (請填寫使用期限) 年　　月　　日	電子郵件帳號：(此欄由申請者自行設定，無線線路臨時使用申請者勿填) 西元出生年月日　　年　　月　　日
	備註： 1. 電子郵件帳號請設定英文字母(區分大小寫)或數字，不可包含特殊字元及空白；電子郵件密碼預設值為西元出生年月日共八碼 2. EIP 系統、校內全區無線帳號密碼同電子郵件預設值 3. 臨時使用之無線帳號密碼以本中心核發為主 4. 校務系統、線上請款、浸神之友預設帳號密碼為人事編號 5. 資料及操作手冊會以電郵方式寄至個人信箱，故請確認個人電子郵件信箱為可正常接收狀況

3.權限/帳號變更或停用

☐權限變更　☐權限停用　☐帳號變更　☐帳號停用

申請事由	

4.資訊服務申請

☐電腦維修　☐軟體安裝　☐系統需求　☐系統問題　☐網路問題　☐網頁資料

☐其他：

申請事由		單位主管核章	

以下為行政管理中心填寫

行政管理中心主任評估：	處理結果：

完成日期	年　　月　　日	承辦人簽章		行政管理中心主任核章	

【附件四】

基督教台灣浸會神學院
委外廠商保密切結書

具保密切結廠商（人員）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿於

民國＿＿＿年＿＿＿＿月＿＿＿＿日起於基督教台灣浸會神學院執行

「＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿」因而知悉貴校機密或任何不公開之文書、電子資料、圖畫、消息、物品或其他資訊，將恪遵保密規定， 未經 貴校書面授權，不得以任何形式利用或洩漏、告知、交付、移 轉予任何第三人，如有違誤願負法律上之責任。

此致

基督教台灣浸會神學院

具切結書委外廠商（人員）＿＿＿＿＿＿＿＿＿＿＿＿

代　表　人（委外廠商）＿＿＿＿＿＿＿＿＿＿＿＿

統　一　編　號：＿＿＿＿＿＿＿＿＿＿＿＿

地　　址：＿＿＿＿＿＿＿＿＿＿＿＿

中　　華　　民　　國　　年　　月　　日

【附件五】

基督教台灣浸會神學院
設備進出記錄表

填表日期：　年　　月　　日

	單位		申請人	
攜出時間	年　　月　　日		歸還簽名	
設備 名稱/序號				
攜入/出方式	□自行攜入/出 □貨運代送(公司名稱/電話：＿＿＿＿＿＿＿＿ 貨運編號：＿＿＿＿＿＿＿＿) □其他(請說明：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿)			
攜入/出原因	□課程教學使用 □崇拜聚會 □設備送修(預計修復完成日期：/　　/　　) □其他:＿＿＿＿＿＿＿＿ □調 / □借 / □還 其他單位：＿＿＿＿＿＿＿＿ 聯 絡 人：＿＿＿＿＿＿＿＿ 聯絡電話：＿＿＿＿＿＿＿＿ （預計歸還日期：　　/　　/　　） □其他(請說明：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿)			
覆核單位				
承辦人		行政管理中心主任		

【附件六】

基督教台灣浸會神學院

異常事件紀錄表

紀錄編號：_____　　填表日期：　　年　　月　　日

異常原因	異常項目：資產名稱：_____ 異常發現時間：　　年　月　日　時　分	
處理說明	異常排除時間：　　年　月　日　時　分	
執行單位 行政管理中心資訊組		行政管理中心主任

【附件七】

基督教台灣浸會神學院資安事件報告單

紀錄編號：　　填表日期：　年　　月　　日

通報單位聯絡資料			
單位名稱		通 報 人	
電　　話		電子郵件	

資訊安全事件通報事項	
發生時間	年___月___日____時___分
設備資料	IP 位址（無；可免填）： Web 位址（無；可免填）： 設備廠牌、機型： 作業系統名稱、版本： 已裝置之安全機制：

資訊安全事件資料				
事件影響等級	□4 級	□3 級	□2 級	□1 級　□資安預警
事件分類	□非法入侵	□感染病毒	□阻斷服務	□其他(誤判)
破壞程度	□系統當機	□資料庫毀損	□網頁遭篡改	□其他(無)
事件說明				
可能影響範圍及損失評估				
應變措施				

期望支援項目

解決辦法	
解決時間	年__月___日___時__分

承辦人	資安執行官