基督教台灣浸會神學院

資訊安全維護計畫

機密等級：一般

文件編號：教 1111G0101 資訊安全維護計畫 0926

版 次：1.0

發行日期：2022.9.26

民國一一０年九月二十三日資訊安全委員會議通過

目　　錄

壹、依據及目的

依據資通安全管理法(以下簡稱本法)第 10 條及施行細則第 6 條訂定資通安全維護計畫，作為資訊安全推動之依循及應符合其所屬資通安全責任等級之要求，訂定、修正及實施資通安全維護計畫(以下簡稱本計畫)。

貳、適用範圍

本計畫適用範圍涵蓋基督教台灣浸會神學院(以下簡稱本校)。

參、核心業務及重要性

- 依據行政院資通安全責任等及分級辦法，本校資安責任等級為C級機關。
- 資通安全責任等級C級之學校機關應辦事項如下表：

制度面向	辦理項目	辦理項目 細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，其後應每年至少檢視一次資通系統分級妥適性；系統等級為「高」者，應於初次受核定或等級變更後之二年內，完成附表十之控制措施。
	資訊安全管理系統之導入		初次受核定或等級變更後之二年內，全部核心資通系統導入 ISO27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並持續維持導入。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置一人；須以專職人員配置之。
	內部資通安全稽核		每二年辦理一次。
	業務持續運作演練		全部核心資通系統每二年辦理一次。
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每二年辦理一次。
		系統滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	

		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄伺服器設定及防火牆連線設定檢視	
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
認知與訓練	資通安全教育訓練	資通安全及資訊人員	每年至少一名人員接受十二小時以上之資通安全專業課程訓練或資通安全職能訓練。
		一般使用者及主管	每人每年接受三小時以上之一般資通安全教育訓練。
	資通安全專業證照及職能訓練證書	資通安全專業證照	資通安全專職人員總計應持有一張以上。
		資通安全職能評量證書	初次受核定或等級變更後之一年內，資通安全專職人員總計應持有一張以上，並持續維持證書之有效性。

一、 資通業務及重要性：

本校之核心業務及重要性如下表：

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
教務 學務 總務 會計 人事	校務系統	■為本校依組織法執掌，足認為重要者	影響校務營運，含個人資料	8 小時
學術網路主幹	網路管理系統	■為本校依組織法執掌，足認為重要者	影響校務營運	8 小時

Domain name server		■為本校依組織法執掌，足認為重要者	影響本校與外界聯繫	8 小時
郵件伺服器		■為本校依組織法執掌，足認為重要者	影響校務及聯繫	8 小時
網站伺服器		■為本校依組織法執掌，足認為重要者	影響本校對外資訊公布	8 小時

二、 非核心業務及說明：

除核心資通系統外之其他資通系統即為非核心系統，最大可容忍中斷時間皆為 24 小時。

肆、資通安全政策及目標

1. 目的

為確保基督教台灣浸會神學院（以下簡稱「本校」）所屬之資訊資產的機密性、完整性及可用性，以符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅，並參酌本校之業務需求，訂定本政策。

2. 適用範圍

2.1. 本政策適用範圍為本校之教職員工生、連線作業之公私機構、提供資訊服務廠商等資訊安全管理事宜。

2.2. 資訊安全管理範疇涵蓋 11 項領域，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，對本校造成 各種可能之風險及危害，各領域分述如下：

2.1.1 資訊安全政策訂定與評估。

2.1.2 資訊安全組織。

2.1.3 資訊資產分類與管制。

2.1.4 人員安全管理與教育訓練。

2.1.5 實體與環境安全。

2.1.6 通訊與作業安全管理。

2.1.7　存取控制安全。

2.1.8　系統開發與維護之安全。

2.1.9　資訊安全事件之反應及處理。

2.1.10 業務永續運作管理。

2.1.11 相關法規與施行單位政策之符合性。

3. 目標

為維護本校資訊資產之機密性、完整性與可用性，並保障使用者資料隱私之安全。期藉由本校全體同仁共同努力以達成下列目標：

3.1. 保護本校業務服務之安全，確保資訊需經授權人員才可存取資訊，以確保其機密性。

3.2. 保護本校業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。

3.3. 建立本校業務永續運作作業規範，以確保本校業務服務之持續運作。

3.4. 確保本校各項業務服務之執行須符合相關法令或法規之要求。

3.5. 網路服務服務品質，需達全年上班時間網路正常服務時間可用性90%。

4. 責任

4.1. 本校應成立資訊安全委員會統籌本校資訊安全政策制定；負責資訊安全政策及本校資訊安全管理制度認證事宜之執行工作。

4.2. 管理階層應積極參與及支持資訊安全管理制度，並透過適當的標準和程序實施本政策。

4.3. 本校之教職員生、連線作業之公私機構、提供資訊服務廠商等皆應遵守本政策。

4.4. 本校之教職員生、連線作業之公私機構、提供資訊服務廠商等均有責任透過適當通報機制，通報資訊安全事件或弱點。

4.5. 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本校之相關規定進行議處。

5. 審查

本政策應每年至少審查乙次，以反映政府法令、技術及業務等最新發展現

況， 並確保本校業務永續運作之能力。

6. 實施

本政策經資訊安全委員會核定後實施，修訂時亦同。

伍、資通安全推動組織

第一條、 設置依據

依據行政院國家資通安全會報法規設置基督教台灣浸會神學院資訊安全委員會(以下簡稱本會)，擬定並執行本校資訊安全政策、技術服務與防護管理等事項。

第二條、 職掌

本會掌理下列事項：

一、訂定資訊安全政策及資訊安全管控機制。

二、督導資訊安全政策之實施。

三、稽核校內資訊安全。

四、資訊安全事件通報、緊急應變及危機處理。

五、規劃資訊安全教育訓練。

六、其它資訊安全事項。

第三條、 組織

本會置委員五人,由主任秘書擔任資訊安全官;行政管理中心主任為執行安全官,行政及技術相關事宜由行政管理中心資訊組負責。使用者代表為教師代表及行政人員代表各一位擔任。本會視需要另聘校內外資訊安全專長或具有資訊安全證照之專業人員為顧問。

第四條、 本辦法經資訊安全委員會會議通過後實施，修訂時亦同。

陸、人力及經費配置

一、專職人力資源之配置

（一） 本校依資通安全責任等級分級辦法之規定，屬資通安全責任等級C級，最低應設置資通安全專職人員1人。

（二） 本校之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升機關內資通安全專業人員之資通安全管理能力。本

校之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。

（三） 資安職人員專業職能之培養(如證書、證照、培訓紀錄等)，應依據資通安全責任等級分級辦法之規定。

（四） 本校負責重要資通系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽屬書面約定。

（五） 本校之首長及相關業務主管人員，應負責督導資訊人員之資通安全作業，防範不法及不當行為。

（六） 專業人力資源之配置情形應定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

二、經費之配置

（一） 資訊安全委員會於規劃配置相關經費及資源時，應考量本校之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。

（二） 規劃建置資通系統建置時，應一併規劃資通系統之資安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。

（三） 資通安全經費、資源之配置情形應定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

柒、資訊及資通系統之盤點

一、資訊及資通系統盤點

(一)本校辦理資訊及資通系統資產盤點，並依資產屬性進行分類，分別為軟體資產、實體資產等。

(二)資訊及資通系統資產項目如下：

1. 軟體資產：應用軟體、系統軟體、開發工具、套裝軟體及電腦作業系統等。

2. 實體資產：電腦及通訊設備、可攜式設備及資通系統相關之設備等。

(三)資通系統應界定其可容忍之故障發生至修復正常運轉所需時間(RTO, Recovery Time Object)及復原之時間點(RPO, Recovery Point Object)。

(四)本校每年度應依資訊及資通系統盤點結果，製作「資訊財產清冊」，欄位應包含：資訊及資通系統名稱、資產名稱、資產類別、擁有者、使

用者、存放位置，是否屬核心資通系統及相關資產等。

(五)資訊及資通系統資產應以標籤標示於設備明顯處，並於清冊上載明財產編號、保管人、廠牌、型號等資訊。

二、機關資通安全責任等級分級

本校因業務涉及維運自行或委外開發之資通系統者，其資通安全責任等級為 C 級。

捌、資通安全風險評估

一、資通安全風險評估

(一)本校應每年針對資訊及資通系統資產進行風險評估。

(二)執行風險評估時應參考行政院國家資通安全會報頒布之最新「資訊系統風險評鑑參考指引」，並依其中之「詳細風險評鑑方法」進行風險評估之工作。

(三)本校應每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估自行或委外開發之資通系統防護需求分級。

二、資通安全風險之因應

(一)本校之資通系統於完成資通系統分級後，應依資通安全責任等級分級辦法之規定，並考量本校可接受之風險，選擇並採行相關之防護及控制措施。

(二)選擇防護及控制措施時，亦應考量採行該項措施可能對資通安全風險之影響。

玖、資通安全防護及控制措施

本校依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及資通系統之防護基準，採行相關之防護及控制措施如下:

一、 資訊及資通系統之管理

(一) 資訊及資通系統之保管

1. 資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。

2. 資訊及資通系統管理人應確保資訊及資通系統被妥善的保存或備份。

3. 資訊及資通系統管理人應確保重要之資訊及資通系統已採取適當之存取控制政策。

（二）資訊及資通系統之使用

1. 本校同仁使用資訊及資通系統前應經其管理人授權。

2. 本校同仁使用資訊及資通系統時，應留意其資通安全要求事項，並負對應之責任。

3. 本校同仁使用資訊及資通系統後，應依規定之程序歸還。資訊類資訊之歸還應確保相關資訊已正確移轉，並安全地自原設備上抹除。

4. 非本校同仁使用本校之資訊及資通系統，應確實遵守本校之相關資通安全要求，且未經授權不得任意複製資訊。

5. 對於資訊及資通系統，宜識別並以文件記錄及實作可被接受使用之規則。

（三）資訊及資通系統之刪除或汰除

1. 資訊及資通系統之刪除或汰除前應評估機關是否已無需使用該等資訊及資通系統，或該等資訊及資通系統是否已妥善移轉或備份。

2. 資訊及資通系統之刪除或汰除時宜加以清查，以確保所有機敏性資訊及具使用授權軟體已被移除或安全覆寫。

3. 具機敏性之資訊或具授權軟體之資通系統，宜採取實體銷毀，或以毀損、刪除或覆寫之技術，使原始資訊無法被讀取，並避免僅使用標準刪除或格式化功能。

二、 存取控制與加密機制管理

（一）網路安全控管

1. 網路區域劃分如下：

（1）外部網路：對外網路區域，連接外部廣網路(Wide Area Network, WAN)。

（2）內部區域網路（Local Area Network, LAN）：機關內部單位人員及內部伺服器使用之網路區段。

2. 外部網路及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。

3. 應定期檢視防火牆政策是否適當，並適時進行防火牆軟、硬體之必要更新

或升級。

4. 內部網路之區域應做合理之區隔，使用者應經授權後在授權之範圍內存取網路資源。

5. 使用者應依規定之方式存取網路服務，不得於辦公室內私裝電腦及網路通訊等相關設備。

6. 網域名稱系統(DNS)防護

（1）一般伺服器應關閉 DNS 服務，防火牆政策亦應針對 DNS 進行控管，關閉不需要的 DNS 服務存取。

（2）DNS 伺服器應經常性進行弱點漏洞管理與修補、落實存取管控機制。

7. 無線網路防護

（1）機密資料原則不得透過無線網路及設備存取、處理或傳送。

（2）用以儲存或傳輸資料且具無線傳輸功能之個人電子設備與工作站，應安裝防毒軟體，並定期更新病毒碼。

(二) 資通系統權限管理

1. 資通系統應設置通行碼管理，通行碼之要求需滿足：

（1）通行碼長度 8 碼以上。

（2）通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。

（3）使用者每 180 天應更換一次通行碼。

2. 使用者使用資通系統前應經授權，並使用唯一之使用者 ID，除有特殊營運或作業必要經核准並紀錄外，不得共用 ID。

3. 使用者無繼續使用資通系統時，應立即停用或移除使用者 ID，資通系統管理者應定期清查使用者之權限。

(三) 特權帳號之存取管理

1. 資通系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

2. 資通系統之特權帳號不得共用。

3. 資通系統之管理者每季應清查系統特權帳號。

（四）加密管理

1.機密資訊於儲存或傳輸時應進行加密。

2.加密保護措施應遵守下列規定：

（1）應落實使用者更新加密裝置並備份金鑰。

（2）一旦加密資訊具遭破解跡象，應立即更改之。

三、 作業與通訊安全管理

（一）防範惡意軟體之控制措施

1.主機及個人電腦應安裝防毒軟體，並時進行軟、硬體之必要更新或升級。

2.使用者未經同意不得私自安裝應用軟體，管理者並應每年定期針對管理之設備進行軟體清查。

3.使用者不得私自使用已知或有嫌疑惡意之網站。

（二）遠距工作之安全措施

（1）提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。

（2）遠距工作終止時之存取權限撤銷，並應返還相關設備。

（三）確保實體與環境安全措施

1.電腦機房之門禁管理

（1）電腦機房應進行實體隔離。

（2）機關人員或來訪人員應申請及授權後方可進入電腦機房，管理者並應定期檢視授權人員之名單。

（3）人員及設備進出應留存記錄。

2.電腦機房之環境控制

（1）電腦機房之空調、電力應建立備援措施。

（2）電腦機房應有安全偵測及防護措施，包括火災警報設備、照明設備、預防入侵者進入，以減少環境不安全之危險。

3.辦公室區域之實體與環境安全措施

（1）應考量採用辦公桌面的淨空政策，以減少文件及可移除式媒體等在辦公時間之外遭未被授權的人員取用、遺失或是被破壞的機會。

（2）機密性及敏感性資訊，不使用或下班時應該上鎖。

（四）資料備份

1. 重要資料及資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。

2. 敏感或機密性資訊之備份應加密保護。

（五）媒體防護措施

1. 使用隨身碟存放資料時，具機密性、敏感性之資料應與一般資料分開儲存，不得混用並妥善保管。

2. 對機密與敏感性資料之儲存媒體實施防護措施，包含機密與敏感之紙本或備份隨身碟，應保存於上鎖之櫃子，且需由專人管理鑰匙。

（六）電腦使用之安全管理

1. 連網電腦應隨時配合更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

2. 筆記型電腦及實體隔離電腦應定期以人工方式更新作業系統、應用程式漏洞修補程式及防毒病毒碼等。

3. 下班時應關閉電腦及螢幕電源。

4. 如發現資安問題，應主動循機關之通報程序通報。

（七）行動設備之安全管理

1. 機密資料不得由未經許可之行動設備存取、處理或傳送。

2. 機敏會議或場所不得攜帶未經許可之行動設備進入。

四、 資通安全防護設備

1. 應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。

2. 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

壹拾、資通安全事件通報、應變及演練

為即時掌控資通安全事件，並有效降低其所造成之損害，本校應訂定資通安全事件通報、應變及演練，依本校資通安全事件通報應變程序辦理。

壹拾壹、資通安全情資之評估及因應

本校接獲資通安全情資，應評估該情資之內容，並視其對本校之影響、可接受之風險及本校之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

一、 資通安全情資之分類評估

本校接受資通安全情資後，應指定資通安全人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

（一）資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

（二）入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

（三）機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

二、 資通安全情資之因應措施

本校於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

（一）資通安全相關之訊息情資

由資通安全委員會彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

（二）入侵攻擊情資

由資通安全人員判斷有無立即之危險，必要時採取立即之通報應變措施，並

依據資通安全維護計畫採行相應之風險防護措施，另通知相關單位進行處理。

（三）機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

壹拾貳、資通系統或服務委外辦理之管理

本校委外辦理資通系統之建置、維運或資通服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

一、 選任受託者應注意事項

1. 受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。
2. 受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

二、 監督受託者資通安全維護情形應注意事項

1. 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。
2. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。
3. 本校應定期或於知悉受託者發生可能影響受託業務之資通安全事件。

壹拾參、資通安全教育訓練

一、 資通安全教育訓練要求

（一）本校依資通安全責任等級分級屬 C 級，資安及資訊人員每年至少一名人員接受十二小時以上之資安專業課程訓練或資安職能訓練。

（二）本校之一般使用者與主管，每人每年接受 3 小時以上之一般資通安全教育訓練。

二、 資通安全教育訓練辦理方式

（一）承辦單位考量管理、業務及資訊等不同工作類別之需求，擬定資通安全

認知宣導及教育訓練計畫，以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。

（二）本校資通安全認知宣導及教育訓練之內容得包含：

1. 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等)。
2. 資通安全法令規定。
3. 資通安全作業內容。
4. 資通安全技術訓練。

（三）員工報到時，應使其充分瞭解本校資通安全相關作業規範及其重要性。

（四）資通安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，亦應一體適用。

壹拾肆、公務機關所屬人員辦理業務涉及資通安全事項之考核機制

本校人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法審酌辦理，及本校各相關規定辦理之。

壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制

一、 資通安全維護計畫之實施

為落實本安全維護計畫，使本校之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本校之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

二、 資通安全維護計畫之持續精進及績效管理

(一) 稽核機制之實施

1. 本校應定期(每年一次)或於系統重大變更或組織改造後執行一次內部稽核作業，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。
2. 辦理稽核前本校應擬定資通安全稽核計畫並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。

3. 辦理稽核時，本校應於執行稽核前 90 日，通知受稽核單位，並將稽核期程、稽核項目紀錄表及稽核流程等相關資訊提供受稽單位。

4. 本校之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性；另於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至稽核結果及改善報告中，並提供給受稽單位填寫辦理情形。

5. 稽核結果應對相關管理階層(含資安長)報告，並留存稽核過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。

6. 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如是否瞭解資訊安全政策及應負之資安責任、是否訂定人員之資訊安全作業程序與權責、是否定期更改密碼）。

(二) 稽核改善報告

1. 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。

2. 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。

3. 受稽單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。

4. 本校應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。

5. 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報告。

三、 資通安全維護計畫之持續精進及績效管理

(一) 本校之資通安全安全委員應召開資通安全委員會議， 確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。

(二) 管理審查議題應包含下列討論事項：

1. 過往管理審查議案之處理狀態。

2. 與資訊安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、本校決議事項等。

3. 資通安全維護計畫內容之適切性。

4. 資訊安全績效之回饋，包括：

(1) 資通安全政策及目標之實施情形。

(2) 資通安全人力及資源之配置之實施情形。

(3) 資通安全防護及控制措施之實施情形。

(4) 內外部稽核結果。

(5) 不符合項目及矯正措施。

5. 風險評鑑結果及風險處理計畫執行進度。

6. 重大資通安全事件之處理及改善情形。

7. 利害關係人之回饋。

8. 持續改善之機會。

(三) 持續改善機制之管理審查應做成改善績效追蹤報告，相關紀錄並應予保存，以作為管理審查執行之證據。

壹拾陸、資通安全維護計畫實施情形之提出

本校依據本法之規定，應於年底前向上級或監督機關，提出資通安全維護計畫實施情形，使其得瞭解本校之年度資通安全計畫實施情形。

壹拾柒、相關附件

附件表單。

資通安全維護計畫附件

目　次

1. 資訊安全委員會成員及分工表

基督教台灣浸會神學院資訊安全委員會成員及分工表

編號：001

製表日期：109 年 2 月 5 日

單位職級	職掌事項	分機	備註
校長室 校長	資訊安全長：擬訂資安計劃與推動	111	
行政管理中心 主任	資安執行官：責綜理資訊安全管理作業協調與督導工作	104	
資訊組 職員	執行資安技術相關事宜	160	
學務處 主任	使用者代表：提供相關建議	106	
秘書暨公關室 秘書	使用者代表：提供相關建議	143	

2. 校內教職員保密切結書

基督教台灣浸會神學院

11045 台北市吳興街 394 巷 1 號
NO.1, LANE 394, WU HSING ST., TAIPEI, TAIWAN, ROC 11045
郵政劃撥：50158603
網址：www.tbts.edu.tw

電話 ：02-2723-8197
02-2720-7824
02-2720-3140
傳真 ：02-2722-4646

校內教職員保密切結書

本人 _____將嚴守工作保密規定與國家相關法對業務機密負完全保密之責，並尊重智慧財產權。絕不擅自洩漏、傳播職務上任何業務相關資料及任職期間經辦、保管或接觸之所有須保密訊息資料；絕不擅自複製他人個資及校方業務重要資料、傳播任何侵害智慧財產權之任何程式、軟體，違者願自負法律責任。

此致 學校財團法人中華浸信會基督教台灣浸會神學院

立　同　意　書　人：_____

電　　話：_____

中　華　民　國　　年　　月　　日

3. 資訊服務申請表

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) 從 年　月　日 至 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				
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 □密碼遺失:　□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	

4. 進出機房登記表

基督教台灣浸會神學院人員進出機房登記表					
文件編號		機密等級		版次	

紀錄編號：___________________

日　期 （民國年月日）	進入機房人員 登記時間	進入機房人員 簽　　名	進 出 事 由	主　管 簽　名
年　月　日	進入： 離去：	單 位： 姓 名：		
年　月　日	進入： 離去：	單 位： 姓 名：		
年　月　日	進入： 離去：	單 位： 姓 名：		
年　月　日	進入： 離去：	單 位： 姓 名：		
年　月　日	進入： 離去：	單 位： 姓 名：		
年　月　日	進入： 離去：	單 位： 姓 名：		
年　月　日	進入： 離去：	單 位： 姓 名：		
年　月　日	進入： 離去：	單 位： 姓 名：		
年　月　日	進入： 離去：	單 位： 姓 名：		

1

5. 委外廠商保密切結書

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

「＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿」業務（或專案） 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

6.資通安全教育訓練計畫

基督教台灣浸會神學院　年度

資通安全教育訓練計畫

壹、依據

基督教台灣浸會神學院之資通安全維護計畫辦理。

貳、目的

為精進本校所屬人員之資通安全意識及職能，並敦促該等人員得以瞭解並執行本校之資通安全維護計畫，以強化資通安全管理能量，爰擬定本校教育訓練計畫，要求所屬人員應接受資通安全之教育訓練。

參、實施範圍

本校所屬人員：

人員類別	人數
資通安全專責人員	1人
主管人員	1人
共計	2人

肆、訓練項目

人員類別	訓練課程	時數
資通安全專責人員		
主管人員		

伍、訓練期程

陸、訓練方式

7. 委外廠商開放防火牆申請表

基督教台灣浸會神學院開放防火牆申請表

<table>
<tr><td>*申請廠商</td><td colspan="2"></td><td>*申請日期</td><td colspan="2"></td></tr>
<tr><td>*主機名稱</td><td colspan="2"></td><td>*OS 版本</td><td colspan="2"></td></tr>
<tr><td>*負 責 人</td><td colspan="2"></td><td>*聯絡電話</td><td colspan="2"></td></tr>
<tr><td colspan="2">*URL 完整路徑
瀏覽器所輸入網路位址</td><td colspan="4"></td></tr>
<tr><td colspan="6">*申請目的：</td></tr>
<tr><td rowspan="4">*防火牆
授權</td><td>*有效日期</td><td colspan="2">自 年 月 日
至 年 月 日</td><td>*Port</td><td></td></tr>
<tr><td>*來源 IP</td><td colspan="4"></td></tr>
<tr><td>*目的 IP</td><td colspan="4"></td></tr>
<tr><td>是否做 NAT</td><td colspan="4">□是 □否</td></tr>
<tr><td colspan="6">行政管理中心主任評估：</td></tr>
<tr><td colspan="6">處理說明：</td></tr>
<tr><td colspan="3">設定檔備份 □是</td><td colspan="3">Firewall Check □是</td></tr>
<tr><td>承辦人</td><td colspan="2"></td><td>行政管理中心
主任核章</td><td colspan="2"></td></tr>
</table>

（*表必填寫欄位）

8 資通安全認知宣導簽到表

基督教台灣浸會神學院資通安全認知宣導

簽到表

編號：

課程名稱：

時　　間：

地　　點：

單　位	職　稱	姓　名	簽　名

9 資通安全維護計畫實施情形

基督教台灣浸會神學院資通安全維護計畫實施情形

編號：

本校之業務因涉及全國性民眾個人資料檔案之持有及處理，經主管機關核定後本校之資通安全責任等級為 C 級 ，依資通安全管理法第 12 條之規定，向 鈞部提出本校 年度資通安全維護計畫實施情形、執行成果及相關說明如下表所示：

實施項目	實施內容	實施情形說明
1. 核心業務及其重要性	1.1 核心業務及重要性盤點	
2. 資通安全政策及目標之訂定	2.1 資通安全政策訂定及核定	
	2.2 資通安全目標之訂定	
	2.3 資通安全政策及目標宣導	
	2.4 資通安全政策及目標定期檢視	
3. 設置資通安全推動組織	3.1 設定資通安全長	
	3.2 設置資通安全推動小組	
4. 專責人力及經費之配置	4.1 專職(責)人員配置	
	4.2 經費之配置	
5. 資訊及資通系統之盤點及核心資通系統、相關資產之標示	5.1 資訊及資通系統之盤點	
	5.2 機關資通安全責任等級分級	
6. 資通安全風險評估	6.1 資通安全風險評估	
	6.2 資通安全風險之因應	
7. 資通安全防護及控制措施	7.1 資通安全防護及控制措施	
	7.1 資訊及通系統之保管	
	7.2 存取控制與加密機制管理	
	7.3 作業及通訊安全管理	
	7.4 系統獲取、開發及維護	
	7.5 執行資通安全健診	
8. 資通安全事件通報、應變及演練相關機制	8.1 訂定資通安全事件通報、應變及演練相關機制	
	8.2 資通安全事件通報、應變及演	

	練	
9. 資通安全情資之評估及因應機制	9.1 資通安全情資之分類評估	
	9.2 資通安全情資之因應措施	
10. 資通系統或服務委外辦理之管理	10.1 選任受託者應注意事項	
	10.2 監督受託者資通安全維護情形應注意事項	
11. 資通安全教育訓練	11.1 資通安全教育訓練要求	
	11.2 辦理資通安全教育訓練	
12. 公務機關所屬人員辦理業務涉及資通安全事項之考核機制	12.1 訂定考核機制並進行考核	
13. 資通安全維護計畫及實施情形之持續精進及績效管理機制	13.1 資通安全維護計畫之實施	
	13.2 資通安全維護計畫實施情形之稽核機制	
	13.3 資通安全維護計畫之持續精進及績效管理	
其他說明		

單位主管：　　資通安全長：

10 資通安全稽核計畫

基督教台灣浸會神學院年度資通安全稽核計畫

壹、依據

一、基督教台灣浸會神學院之資通安全維護計畫辦理。

二、資通安全管理法第十三條規定辦理。

貳、目的

為瞭解本校資通安全維護計畫執行之有效性，爰擬定本稽核計畫，執行稽核作業。

參、稽核期程

肆、稽核團隊成員

伍、稽核範圍

陸、稽核項目及內容

一、核心業務及其重要性：

二、資通安全政策及目標：

三、資通安全推動組織：

四、專責人力及經費之配置：

五、公務機關資通安全長之配置：

六、資訊及資通系統之盤點，並標示核心資通系統及相關資產：

七、資通安全風險評估：

八、資通安全防護及控制措施：

九、資通安全事件通報、應變及演練相關機制：

十、資通安全情資之評估及因應機制：

十一、資通系統或服務委外辦理之管理措施：

十二、公務機關所屬人員辦理業務涉及資通安全事項之考核機制：

柒、資通安全維護計畫及實施情形之持續精進及績效管理機制：

11 稽核項目紀錄表

基督教台灣浸會神學院
OOO 學年度內部稽核檢核表

受稽核單位：_____ 編號：_____

稽核時間：_____ 頁次：_____

項次	稽核項目	稽核目的	稽核方式	稽核結論	建議意見
1					
3					
4					

受稽核單位人員簽章	單位主管簽章	稽核人員簽章

12.稽核委員聘任同意暨保密切結書

基督教台灣浸會神學院資安維護計畫

稽核委員聘任同意暨保密切結書

本人＿＿＿＿＿＿＿＿（以下簡稱甲方）為協助基督教台灣浸會神學院執行「資安維護計畫」（以下簡稱本計畫），接受乙方之邀請，擔任　年資安稽核團隊之稽核委員，特立書同意事項如下：

一、 甲方應遵守國家機密保護法、個人資料保護法、行政院及所屬各機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、著作權法及其他相關法令之規定，並對因執行本計畫或因執行本計畫之機會所知悉之機密資訊負有保密義務;且上開各義務不因甲方與乙方或與技服中心間，就本年度擔任稽核委員相關事宜之法律關係解除、終止或完成而失其效力。

二、 甲方就因執行本計畫或因執行本計畫之機會，所知悉或接觸之乙方、受稽機關或其他第三人之機密資訊，除因執行本計畫所必須，且事先經乙方書面同意者，或法律另有明文規定外，不得有下列行為：

（一）全部或一部重製或留存上開機密資訊；

（二）以任何方式向任何第三人揭露上開機密資訊之全部或一部；

（三）以任何方式使任何第三人知悉、持有或使用上開機密資訊之全部或一部；

（四）以任何方式使自己或任何第三人就上開機密資訊之全部或一部取得任何權利；

（五）揭露、公開或使用上開機密資訊之全部或一部。

三、 甲方因執行本計畫所製作之報告、文件或其他產出，其智慧財產權及其他權利均歸屬乙方所有。

四、 甲方與受稽機關有下列情形之一者，就與該受稽機關之稽核相關事宜，應主動迴避，或事先以書面告知乙方，以確認是否得免予迴避：

（一）甲方、甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬、或上開人員財產信託之受託人，與受稽機關間，有財產上或非財產上利益之利害關係者；

（二）甲方、甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬，與受稽機關或其負責人間現有或於過去兩年間曾有僱傭、承攬、委任、代理或其他類似之關係者；

（三）甲方或其現任職或於過去兩年內曾任職之機關，於民國　年至本次稽核期間，曾為受稽機關進行與受稽事項相關之顧問輔導者。

五、 前條所稱財產上利益，係指動產、不動產、現金、有價證券、債權、其他財產上權利、具有經濟價值或得以金錢交易取得之利益；所稱非財產上利益，係指有利於甲方之配偶、甲方三親等以內血親或姻親、與甲方有共同生活關係之家屬、或上開人員財產信託之受託人於受稽機關或其關聯機關之任用、陞遷、調動及其他人事措施。

六、 有其他情形足認甲方有不能公正執行職務之虞，經受稽機關敘明理由，並由乙方作成迴避決定者，甲方應迴避之。

七、 甲方有第四條各款情形之一，而未自行迴避，亦未事先以書面告知乙方相關情事，並經乙方書面同意免予迴避者，乙方得終止本契約，甲方應返還已收取之報酬，如乙方，因此認有必要對受稽核機關重為全部或一部稽核，或受有其他不利益時，甲方並應賠償乙方因此所生之一切損失及費用（包括但不限於賠償金、和解金、律師費及訴訟費用等）。

八、 甲方如違反第二條或就相關事宜涉及其他不法情事，將移送司法機關處理；如致乙方、受稽機關，遭受任何不利益，或受第三人法律上請求或訴追者，甲方應賠償乙方、受稽機關，因此所生之一切損失及費用（包括但不限於賠償金、和解金、律師費及訴訟費用等）。

九、 甲方應公正執行職務，並應避免使人誤認推薦特定廠商、產品或服務；且處理稽核相關事務或出席會議，應親自為之。

此　致

基督教台灣浸會神學院

立 同 意 書 人

姓　　名：　　（簽章）

身 份 證 字 號：

中 華 民 國　　年　　月　　日

13.稽核結果及改善報告暨追蹤改善結果

基督教台灣浸會神學院

000 學年度內部稽核報告

【行政管理中心-資訊組】		
稽核項目	**稽核目的及方式**	**稽核說明及建議**