銘傳大學
資通安全維護計畫

V1.0

機密等級: ■一般□限閱□密

文件修訂履歷

發行／修訂版本	修訂日期	修訂人員	發行與變更說明	核准人員
V1.0	112/11/20	林佩穎	正式發行	陳振南

目　錄

壹、依據及目的

本計畫依據政府資通安全管理法施行細則第 6 條訂定。

貳、適用範圍

本計畫適用私立銘傳大學（以下簡稱本校）所有單位。

參、核心業務及重要性

一、核心業務及重要性

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
教職員資訊系統	教職員資訊系統	□為主管機關指定之關鍵基礎設施 □為主管機關核定資通安全責任等級 A 級或 B 級機關所涉業務 ■為本校依組織法執掌，足認為重要者	機關信譽：影響本校教職員管理相關業務及其運作。	8 小時 (工作日)
學生資訊系統	學生資訊系統	□為主管機關指定之關鍵基礎設施 □為主管機關核定資通安全責任等級 A 級或 B 級機關所涉業務 ■為本校依組織法執掌，足認為重要者	機關信譽：影響本校學生管理相關業務及其運作。	8 小時 (工作日)
Moodle 數位教學平台	Moodle數位教學平台	□為主管機關指定之關鍵基礎設施 □為主管機關核定資	機關信譽：影響本校師生教學相關業務及	8 小時 (工作日)

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
		通安全責任等級 A 級或 B 級機關所涉業務 ■為本校依組織法執掌，足認為重要者	其運作。	
電子公文	電子公文	□為主管機關指定之關鍵基礎設施 □為主管機關核定資通安全責任等級 A 級或 B 級機關所涉業務 ■為本校依組織法執掌，足認為重要者	機關信譽：影響本校教職員電子公文收發無法正常運作。	8 小時 (工作日)
電子表單	電子表單	□為主管機關指定之關鍵基礎設施 □為主管機關核定資通安全責任等級 A 級或 B 級機關所涉業務 ■為本校依組織法執掌，足認為重要者	機關信譽：影響本校師生申請表單相關業務及其運作。	8 小時 (工作日)

為確保營運持續運作，並降低關鍵性業務流程受重大故障或災害之影響，訂定相關營運持續運作管理程序。請參閱「ISMS-2-003實體及環境安全管理程序書」、「ISMS-2-013業務持續營運管理程序書」。

二、非核心業務及說明

在核心業務系統之外所屬資訊系統、各單位架設之伺服器等，其應遵守本校的資訊安全規範，詳請參閱「壹拾柒、相關法規、程序及表單」。

肆、資通安全政策及目標

一、資通安全政策

為強化資通安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本校之資通業務持續運作之資通環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，訂定「銘傳大學資通安全政策」，確保本校資料、系統、設備及網路等資訊資產之安全，保障所有教職員生之權益。

二、資通安全目標

(一) 確保相關資通安全措施或規範符合政策與現行法令之要求，每年至少進行一次內部稽核。

(二) 確保業務得以持續運作，每年至少須執行營運持續計畫演練一次，確保本校業務持續運作。

(三) 依員工之職務及責任符合資通安全管理法教育訓練時數要求，且完成人數比例須達 95%以上。

(四) 強化主機網路安全防護機制、阻斷駭客入侵，完善通報機制與緊急應變處理程序，定期完成弱點掃描、安全漏洞檢測，規劃備援系統，以維持正常營運，確保每半年網路服務異常中斷 10 分鐘以上次數在 3 次以內。

三、資通安全政策及目標之核定程序

「銘傳大學資通安全政策」由「銘傳大學資安暨個資保護推行委員會」每年於資通安全管理審查會議定期審議，另組織、業務、法令或實體環境等因素之變迭時，予以適當修訂。經「銘傳大學資安暨個資保護推行委員會」召集人核定後公布施行。

四、資通安全政策及目標之宣導

資通安全政策及目標得以透過教育訓練、電子郵件（E-MAIL）、公告於網站、或其他等方式公告周知向所有人員、利害關係人（例如 IT 服務供應商）進行宣導。

伍、資通安全推動組織

資通安全推動組織與分工及職責，已於「銘傳大學資安暨個資保護推行委員會設置要點」及「銘傳大學資安暨個資保護管理要點」說明。

陸、專職人力及經費配置

一、專職人力及資源之配置

(一) 本校設置資通安全專職人員1人，負責統籌資安業務，其負責工作如下，

1. 資通安全管理面業務：負責全校性資通安全導入、資訊及資通系統資產盤點、內部資通安全稽核及教育訓練等業務之推動。

2. 資通系統安全管理業務：業務持續運作演練等業務之推動。

3. 資通安全管理法法令遵循業務：負責本校資通安全管理法法令遵循義務執行事宜。

(二) 資訊資產分級、資通安全防護業務之防護基準規範及安全監控管理，由資訊網路處核心資通系統維運小組訂定，參閱「ISMS-2-012_資訊資產管理程序書」。

(三) 本校資通安全系統驗證，賡續ISO27001國際認證，由資訊網路處核心資通系統維運小組持續改善。

(四) 本校安全性檢測及資安事件通報，由各單位資安種子人員負責。

(五) 本校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，並提升校內資通安全專業人員之資通安全管理能力。

(六) 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。

(七) 資安專職人員應持有1張資通安全專業證照。

(八) 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，應簽署並視需要實施人員輪調，建立人力備援制度。

(九) 本校之首長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。

(十) 專業人力資源之配置情形應每年定期檢討，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) 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) 各單位於規劃建置資通系統時，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、資源之配置情形應每年一次定期檢討，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

每年至少辦理一次資訊及資通系統資產盤點。應依資訊及資通系統盤點結果，製作「資訊及資通系統資產清冊」，評估資通系統防護需求分級，並以此防護需求分級的等級(高/中/普)作為高階風險評鑑的風險等級。

各單位管理之資訊或資通系統如有異動，應依各單位內部作業流程立即更新資訊及資通系統資產清冊或於資通系統資產風險評估前完成更新，以維護資訊資產清冊之正確性及完整性。

捌、資通安全風險評估

每年辦理一次資訊及資通系統資產風險評估，依據「資通安全責任等級分級辦法」附表九、資通系統防護需求分級原則，分別就機密性、完整性、可用性及法律遵循性四大影響構面，分別考量資通系統發生資安事件時，在各個影響構面可能造成之衝擊與後果嚴重程度，進行「高階風險評鑑」，檢視評估防護需求分級(高/中/普)妥適性，評鑑結果提交單位主管核章，並以此防護需求分級的等級(高/中/普)作為高階風險評鑑的風險等級，再由資通安全專職人員彙整成「資通系統與服務資產清冊」呈報資安長備查。

「高階風險評鑑」被評估為「高」風險等級或支援核心業務之資通系統，需依據「ISMS-2-011風險評鑑暨管理程序書」再進行「詳細風險評鑑」。

玖、資通安全防護及控制措施

依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核心資通系統之防護基準，採行相關之防護及控制措如下：

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. 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。

(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

在核心業務系統之外所屬資訊系統、各系所院網頁、各單位架設之主機、伺服器等，請參閱「ISMS-2-009系統開發與維護安全程序書」。

(一) 資通系統權限管理

1. 本校之資通系統應設置密碼管理，密碼之要求需滿足：

設有8碼以上密碼(需含有英數字)。

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。

(二) 特權帳號之存取管理

1. 資通系統之特權帳號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，其授權及審查紀錄應留存。資通系統之特權帳號不得共用。

2. 資通系統之特權帳號應妥善管理，並應留存特殊權限帳號之使用軌跡。

3. 資通系統之管理者應清查系統特權帳號並將逾期特權帳號刪除。

三、作業與通訊安全管理

(一) 防範惡意軟體之控制措施

1. 本校個人電腦應安裝防毒軟體，並進行軟、硬體之必要更新或升級。

(1) 經任何形式之儲存媒體所取得之檔案，於使用前應先掃描有無惡意軟體。

(2) 電子郵件附件及下載檔案於使用前，宜先掃描有無惡意軟體。

(3) 確實執行網頁惡意軟體掃描。

2. 使用者不得私自使用已知或有嫌疑惡意之網站。

3. 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

(二) 遠距工作之安全措施

1. 針對遠距工作之連線應透過VPN進行連線。

(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解除。

2. 辦公室區域之實體與環境安全措施

(1) 文件及可移除式媒體在不使用或非上班時，應存放在櫃子內。

(2) 機密性及敏感性資訊，不使用或下班時應該上鎖。

(3) 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。

(三) 資料備份

重要資料應進行資料備份，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。

(四) 媒體防護措施

1. 使用隨身碟或硬碟等存放資料時，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. 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之紀錄。

3. 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。

4. 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硬碟，應保存於上鎖之櫃子。

(五) 電腦使用之安全管理

1. 電腦或業務系統，若超過十分鐘不使用時，應立即登出或啟動螢幕保護功能。

2. 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。

3. 如發現資安問題，應主動循本校之通報程序通報。

4. 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低及減少敏感性資訊遭破解或洩漏之機會。

(六) 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。

(七) 即時通訊軟體之安全管理

使用即時通訊軟體傳遞本校內部公務訊息，其內容不得涉及機密資料。

四、執行資通安全健診

本校每二年應辦理資通安全健診，其至少應包含下列項目，並檢討執行情形：

(一) 網路架構檢視。

(二) 網路惡意活動檢視。

(三) 使用者端電腦惡意活動檢視。

(四) 伺服器主機惡意活動檢視。

(五) 安全設定檢視。

五、資通安全防護設備

(一) 本校應建置防毒軟體、網路防火牆，持續使用並適時進行軟、硬體之必要更新或升級。

(二) 資安設備應定期備份日誌紀錄及定期檢視。

壹拾、資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，本校訂定資通安全事件通報、應變及演練相關機制，核心業務系統請參閱「ISMS-2-008安全事故緊急應變程序書」，在核心業務系統之外所屬資訊系統、各單位架設之伺服器等通報應變程序如下：

(一) 收到資安事件通報，負責業務同仁回覆通報，並封鎖IP。

(二) 資安專職人員通知單位同仁處理。

(三) 單位處理完畢後填寫電子表單，才可解鎖IP。

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、本校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，由資訊網路處系統組同仁進行情資分析，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、特定系統遭受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。

(四) 涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含本校內部之核心業務資訊、核心資通系統、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作等內容，屬涉及核心業務、核心資通系統之情資。

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防護及控制措施。

(一) 資通安全相關之訊息情資

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

由資通安全專職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，另通知各單位進行相關之預防。

(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。

(四) 涉及核心業務、核心資通系統之情資

核心資通系統維運小組應就涉及核心業務、核心資通系統之情資評估其是否對於本校之運作產生影響，並依據相對應之程序書採行相關之風險管理機制。

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

(一) 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並禁止使用大陸設備。

(二) 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。

(三) 受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

二、監督受託者資通安全維護情形應注意事項

(一) 受託業務包括客製化資通系統開發者，受託者應提供該資通系統之第三方安全性檢測證明；涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。

(二) 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取補救措施。

(三) 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。

(四) 受託者應採取其他資通安全相關維護措施。

(五) 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時，以稽核或其他適當方式確認受託業務之執行情形。

壹拾參、資通安全教育訓練

一、資通安全教育訓練要求

(一) 本校資安專職人員每年至少接受12小時之資安專業課程訓練或資安職能訓練。

(二) 本校資訊人員每年至少接受6小時之資通安全專業課程。

(三) 本校主管每年至少接受3小時之資通安全通識教育訓練。

(四) 本校職員每人每年至少接受3小時之資通安全通識教育訓練。

二、資通安全教育訓練辦理方式

(一) 本校應每年考量管理、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，提升本校資通安全水準，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。
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，對本校外部的使用者，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

本校所屬人員之平時考核或聘用，依據銘傳大學所屬人員資通安全事項獎懲辦法辦理之。

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紀錄。

二、資通安全維護計畫實施情形之稽核機制

(一) 本校之稽核人員應定期參加教育訓練，以持續加強資安專業能力與稽核技巧，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。

(二) 內部稽核應每年至少辦理一次，當系統重大變更或組織改造後，應立即執行內部稽核作業，以確認人員是否遵循本規範與校之管理程序要求，並有效實作及維持管理制度。

(三) 辦理稽核前內部稽核組應於1週前擬定資通安全稽核計畫並安排稽核成員，稽核計畫應闡明稽核範圍與項目，陳核「銘傳大學資安暨個資保護推行委員會執行長」核可後，方得實施。

(四) 內部稽核報告由「內部稽核組」彙整後，呈報「銘傳大學資安暨個資保護推行委員會」核定。內部稽核報告所列建議改善事項，應辦理追蹤複檢。

(五) 受稽單位應尊重及支持「內部稽核組」人員，誠實答覆稽核人員所提問題，並接受調閱有關紀錄、報告及文件。

(六) 稽核人員應依照查核發現之情況於內部稽核底稿中，並概略描述各查核項目之現況說明及結果。

(七) 「內稽報告」之缺失與建議事項，應訂定改善方案據以執行，並由「內部稽核組」辦理複核工作。

三、資通安全維護計畫之持續精進及績效管理

(一) 本校「銘傳大學資安暨個資保護推行委員會」應每年至少召開一次資通安全管理審查會議，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. 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求等。
3. 資通安全維護計畫內容之適切性。
4. 資通安全績效之回饋，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「資通安全管理法」規定，應依教育部規定時程，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、相關法規、程序及表單

一、相關法規及參考文件

(一) 資通安全管理法

(二) 資通安全管理法施行細則

(三) 資通安全責任等級分級辦法

(四) 資通安全事件通報及應變辦法

(五) 資通安全情資分享辦法

(六) 教育部人員資通安全事項獎懲基準

(七) 銘傳大學資通安全政策

(八) 銘傳大學資安暨個資保護推行委員會設置要點

(九) 銘傳大學資安暨個資保護管理要點

(十) 實體及環境安全管理程序書(ISMS-2-003)

(十一) 安全事故緊急應變程序書(ISMS-2-008)

(十二) 系統開發與維護安全程序書(ISMS-2-009)

(十三) 風險評鑑暨管理程序(ISMS-2-011)

(十四) 資訊資產管理程序書(ISMS-2-012)

(十五) 業務持續營運管理程序書(ISMS-2-013)

二、附件表單

(一) 資訊及資通系統資產清冊

(二) 稽核計畫

(三) 內部稽核底稿

(四) 內稽報告

(五) 固定進出管制區域人員名冊(ISMS-4-006)

(六) 管制區域進出登記簿(ISMS-4-007)

(七) 緊急聯絡清單(ISMS-4-029)

(八) 資訊安全事件通報單(ISMS-4-030)

(九) 資訊資產清冊_人員類(ISMS-4-049)

(十) 資訊資產清冊_資料類(ISMS-4-050)

(十一) 資訊資產清冊_軟體類(ISMS-4-052)

(十二) 資訊資產清冊_硬體類(ISMS-4-053)

(十三) 資訊資產清冊_通訊類(ISMS-4-054)

(十四) 資訊資產清冊_環境類(ISMS-4-055)

(十五) 風險評鑑報告(ISMS-4-070)

(十六) 風險處理計畫(ISMS-4-071)

(十七) 業務持續運作管理計畫(ISMS-4-072)

(十八) 資訊資產清冊_虛擬主機類(ISMS-4-083)