銘傳大學資訊網路處

資訊安全政策

ISMS-1-001

V1.2

機密等級: ■一般□限閱□密

文件修訂履歷

發行／修訂版本	發行／修訂生效日期	發行／修訂人員	發行與變更說明	核准人員
V0.1	97/01/21	陳建伯	初稿	
V1.0	97/04/21	陳建伯	正式發行	王金龍
V1.1	97/07/02	陳建伯	修改「系統範圍」第一項內容	王金龍
V1.2	97/07/14	陳建伯	修改 6.3(c)；修改第 7 項內稽時間；增加 8.3(a)小項	王金龍

目 錄

1 目的

銘傳大學資訊網路處（以下簡稱資訊網路處)為推動強化資訊安全管理，建立安全及可信賴之資訊作業環境，確保資訊網路處資料、系統、設備及網路等資訊資產之安全，保障資訊網路處權益，特依據「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」及「電腦處理個人資料保護法」等相關法令及法規，並考量相關業務需求，據以訂定本資訊安全政策，使其成為資訊網路處推動資訊安全管理及實施各項資訊安全措施之準則。透過本資訊安全政策之制定，明確宣示資訊網路處支持資訊安全之決心，期使相關人員有所依循，並能適切合乎法令、法規及資訊網路處對於資訊安全之要求，以降低資訊安全事件所可能帶來之衝擊。
依據資訊網路處核心業務之特性及願景，確保資訊網路處及其相關業務資訊資產之完整性、可用性與機密性。

a) 機密性：確保被授權之人員才可使用資訊。
b) 完整性：確保使用之資訊正確無誤、未遭竄改。
c) 可用性：確保被授權之人員能取得所需資訊。

2 範圍

為強化資訊網路處資安環境，故以資訊網路處為本資訊安全管理系統（Information Security Management System，簡稱 ISMS)之基礎，並逐漸擴大其範圍。本文件描述資訊網路處資訊安全管理系統的架構，並闡明資訊網路處全體人員應遵循的資訊安全政策，以及在資訊安全工作規劃、實踐與持續改進過程中所應扮演的角色與權責。其適用範圍如下：

a) 系統範圍
    1) 提供銘傳大學校園資訊服務之主機暨應用系統。
    2) 機房網路維運作業。
    3) 校務系統開發及維運作業。
    4) 臺灣學術網路之連線作業。
b) 實體範圍
    1) 資訊網路處所屬之台北校區資訊機房及辦公室。
    2) 資訊網路處所屬之桃園校區資訊機房及辦公室。
c) 組織/人員範圍

1)　資訊網路處全體人員。

3　資訊安全聲明

a) 資訊安全是確保資訊網路處永續經營的要素之一。

b) 應確保資訊網路處提供之服務不中斷。

c) 管理階層必須清楚地界定資訊網路處對於資訊安全的權責，以避免資訊或服務遭受未授權之修改或誤用。

d) 應依據業務需求考量，定期測試演練營運持續計劃，以維持其可用性。

e) 對於資訊安全事件應隨時保持警戒，並依程序進行通報。

f) 禁止於內部網路上安裝、使用、下載非法或未授權之軟體。

g) 如違反本資訊安全政策及相關安全規定者，將視情節追訴其法律責任。

4　組織與權責

資訊網路處為確保依據 ISO/IEC 27001:2005 標準所擬定之資訊安全管理系統能有效運作與實踐，故明訂相關組織及權責，以推動及維持資訊安全管理系統各類管理、執行與稽核等工作之進行。為負責執行各項資訊安全管理系統之活動，資訊網路處特設立資訊安全推行組織，其組織架構及權責請參考「資訊安全推行組織設置程序書」。

5　資訊安全管理系統架構

5.1　資訊安全管理系統

資訊網路處為貫徹資訊安全管理，並確保所有資訊與資訊系統獲得適當保護，特依照 ISO/IEC 27001:2005 標準之要求規劃、建立、實施、運作、監督、稽核、維護與改進資訊安全管理系統，並持續改進本系統之有效性。

5.2　運作機制

資訊網路處係依照 ISO/IEC 27001:2005 標準, 採用“Plan-Do-Check-Act”(PDCA)之循環運作模式，建立整個資訊安全管理系統，並維繫其有效運作與持續改進。

a) 規劃與建立 (Plan)

1) 制定風險評鑑程序。

2) 找出資訊安全管理系統範圍內之資產，界定其擁有者，分析其弱點與威脅，並評鑑風險發生之機率與對於機密性（Confidential)、完整性（Integrity)、可用性（Availability)之影響程度。

3) 列舉評鑑各種風險處理方式（例如：採行合適之控制措施、接受、規避或轉嫁等)，選擇適當之管制目標與措施。

4) 研擬「適用聲明」(Statement of Applicability)，載明所選定之安全管制目標、控制措施與選用原因等資料。

5) 風險評鑑結果呈報維運權責單位核可，並取得系統運作所需之授權。

b) 實施與運作 (Do)

1) 研擬風險處理計畫，詳述資訊安全風險管理相關之行動方案、負責單位與執行順序。

2) 落實執行風險處理計畫，管理相關作業與資源，以達成預期之管制目標。

3) 定義如何量測所選擇控制措施或控制措施群的有效性，並具體說明如何使用這些量測去評鑑控制措施的有效性，及產生可比較與可再製的結果。

4) 實施資訊安全認知宣導與教育訓練。

5) 採行適當之控制措施與程序，以利及早發現安全事件並迅速因應處理。

c) 監督與稽核 (Check)

1) 定期執行資訊安全稽核，並依據稽核結果、安全事件與相關單位之建議與回應，檢討資訊安全管理系統之有效性。

2) 因應組織、技術、業務目標或外部環境之變動，檢討剩餘風險值與風險可接受水準。

3) 定期辦理管理審查，以確認資訊安全管理系統之範圍是否合宜，相關作業是否持續改進。

4) 記錄可能影響資訊安全管理系統運作或效率之活動或事件。

5) 量測控制措施的有效性，以證實安全需求已得到滿足。

d) 維護與改進 (Action)

1) 落實系統改進作業，採行適當之矯正與預防措施。

2) 與所有相關單位溝通協調系統改進作業之行動與結果，以確保達成預期目標。

3) 持續維護資訊安全管理系統之運作。

6 管理責任

6.1 管理承諾

資訊安全長應通過以下方式對於資訊網路處資訊安全管理系統之規劃、建立、實施、運作、監督、稽核、維護與改進各項作業，具體展現其承諾。

a) 制定資訊安全政策。

b) 確保資訊安全目標與計畫之建立。

c) 訂定資訊安全之角色與職責。

d) 宣導遵守資訊安全政策與法令規章、達成資訊安全目標及持續改善之重要性。

e) 對於資訊安全管理系統各項作業提供充足之資源。

f) 決定接受風險的準則及可接受的風險等級。

g) 確保資訊安全管理系統內部稽核作業之執行。

h) 執行資訊安全管理系統審查作業。

6.2 資源管理

資訊網路處應確認並提供執行下列事項所需之資源，以利資訊安全推行組織於進行各項工作時，得以順利推展：

a) 資訊安全管理系統之建立、實施、運作與維護。

b) 確認資訊安全程序可符合業務需求。

c) 闡明法令規章之要求與契約之安全義務。

d) 正確運用控制措施，以確實維護資訊安全。

e) 執行必要之審查，並對結果做適當之反應與處理。

f) 改善資訊安全管理系統之有效性。

6.3 訓練、認知及職能

資訊網路處應依下列程序確認參與資訊安全管理系統作業之人員，均具備工作所需之相關職能，並認知其工作之重要性與對資訊安全管理系統之目標達成有所貢獻。

a) 定義資訊安全之角色與職責。確立資訊安全管理系統運作相關人員必須具備之職能。

b) 提供職能訓練，必要時應聘任可滿足職能需求的人員。

c) 評鑑職能訓練與相關措施之有效性，例如以筆試、口試、証照、報告或其他方法來進行評鑑。

d) 建立並維護教育訓練、技能、經驗與資格之相關紀錄。

7 內部稽核

資訊網路處資訊安全管理系統每半年至少進行 1 次資訊安全內部稽核作業，以檢討資訊安全目標、控制措施與程序是否遵循相關標準、法令、法規或資訊安全需求，並依預期規劃有效執行與維持。內部稽核作業之規劃應考量稽核對象或範圍之重要性與現況，定義稽核之標準、範圍、頻率與方法，確認稽核人員之客觀與公正，並妥善保存相關紀錄。受稽核單位對於不符合事項應及時採行改善措施，並追蹤驗證其適當性、充分性及有效性。內部稽核結果應清楚地於文件中陳述，並保持相關稽核紀錄。詳細作業請詳閱「資訊安全稽核作業程序書」。

8 管理審查

8.1 目的

為確保資訊網路處資訊安全管理系統運作之程序適切與有效，故制訂此審查程序，針對資訊網路處之資訊安全管理系統定期召開管理審查會議審查，並對矯正措施予以追蹤、檢討與結案。

8.2 會議召開

資訊網路處管理審查會議應定期由資訊安全長召開，每半年至少進行 1 次，以持續確保資訊網路處資訊安全管理系統運作之適切性、充足性及有效性。審查範圍包括管理系統改進方案與變革需求之評鑑，審查結果應予詳實記錄並妥善保存。詳細作業請詳閱「資訊安全推行組織設置程序書」。

8.3 審查輸入

管理審查作業進行前應明訂各項審查內容之需求，使資訊安全推行組織明確瞭解並充分進行相關資訊之準備工作，其輸入項目包括下列資訊，：

a) 審核資訊安全政策之適切性。

b) 資訊安全管理系統稽核與審查之結果。

c) 來自利害相關團體之回饋。

d) 可以改善資訊安全管理系統運作有效性及效率之技術、產品或程序。

e) 預防與矯正措施之執行現況。

f) 前次風險評鑑未能指明之弱點或威脅。

g) 有效性測量的結果

h) 前次管理審查之後續追蹤。

i) 任何可能影響資訊安全管理系統之變更。

j) 改善建議。

8.4 審查輸出

管理審查作業完成後，需要明確定義各項具體的審查結果，以利資訊安全推行組織持續進行各項相關的工作，其輸出項目應包括關於下列事項之決策或行動：

a) 資訊安全管理系統有效性的改善。

b) 更新風險評鑑及風險處理計畫。

c) 必要時應修訂影響資訊安全的程序及控制措施，以反映可能影響本資訊安全管理系統的內外部事件，包含下列變化：

   1) 業務需求。

   2) 安全需求。

   3) 影響現有業務需求的業務程序。

   4) 法律法規要求。

   5) 合約責任。

   6) 風險等級或風險可接受水準。

d) 資源需求。

e) 改進量測控制措施的有效性。

9 資訊安全管理系統改進

9.1 持續改善

資訊網路處應透過資訊安全政策、資訊安全目標、稽核結果、事件監控分析、矯

正預防措施及管理審查等機制，持續增進本資訊安全管理系統之有效性，詳細作業請參考「矯正預防措施管理程序書」。

9.2 矯正措施

資訊網路處應採取適當的控管措施，以減少資訊安全管理系統建置與運作過程中所發現之不符合事項，並防止再度發生。矯正措施之作業程序文件應規定如下列之要求：

a) 指出資訊安全管理系統建置與運作之不符合事項。

b) 確認不符合事項的原因。

c) 評鑑為防範再發生所需採行之措施。

d) 決定及實作所需之矯正措施。

e) 記錄矯正措施之執行結果。

f) 審查矯正措施之執行結果。

9.3 預防措施

資訊網路處應採取適當的控管措施，以預防本資訊管理系統潛在不符合事項之發生。預防措施之作業程序文件應規定如下之要求：

a) 指出潛在之不符合事項及其原因。

b) 評鑑預防不符合事項發生所需之措施。

c) 確定並實施所需執行之預防措施。

d) 記錄預防措施之執行結果。

e) 審查預防措施執行之結果。

f) 資訊網路處應識別風險變化情形，並特別注意明顯變化之風險以識別預防措施。另應根據風險評鑑的結果來確定預防措施的優先等級。