113年國立嘉義大學資通安全維護計畫

目　　錄

壹、依據及目的

本計畫依據資通安全管理法第 10 條及施行細則第 6 條訂定。

目的為確保核心業務營運穩定。

貳、適用範圍

本計畫適用範圍涵蓋國立嘉義大學全機關(以下簡稱本校)。

參、核心業務及重要性[1]

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
本校校務行政系統	校務行政系統及相關業務支援系統	□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 ■為本機關依組織法執掌，足認為重要者	民眾權益受損：業務失效可能使教職員生無法操作個人資料維護作業、課程相關作業、差勤作業等，嚴重影響教職員生權益。 違反法遵義務:依個人資料保護法應善盡個人資料保護責任，如違反該法致足生損害他人者將依法受罰。 其他：業務失效將使本校行政效率大幅降低。	8 小時

[1] 所填之核心與非核心業務係依據本校 ISMS 之業務流程衝擊分析表[NCYU-ISMS-D-038]記錄編號:113-001 填寫。

各欄位定義：

1. 核心業務名稱：參考資通安全管理法施行細則第 7 條[2]之規定列示。
2. 核心資通系統：列出支持核心業務運作必要之系統。
3. 重要性說明：說明該業務對學校之重要性，例如對學校財務及信譽上影響，對民眾影響，對社會經濟影響，對其他機關業務運作影響，法律遵循性影響或其他重要性之說明。
4. 最大可容忍中斷時間單位以小時計。

二、非核心業務及說明：

本校之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
電子公文交換	電子公文無法即時送達機關，影響機關行政效率	8 小時
電子郵件系統	機關內外無法以電子郵件形式告知各項事務，影響機關行政效率	8 小時
本校全球資訊網系統	無法以網站即時公告本校各項事務，影響機關行政效率	8 小時
會計管理系統及	各項會計、請購等作業無法以線	8 小時

[2] 一、公務機關依其組織法規，足認該業務為機關核心權責所在。
二、公營事業及政府捐助之財團法人之主要服務或功能。
三、各機關維運、提供關鍵基礎設施所必要之業務。
四、各機關依資通安全責任等級分級辦法第四條第一款至第五款或第五條第一款至第四款涉及之業務。
前條第一項第六款所稱核心資通系統，指支持核心業務持續運作必要之系統，或依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之規定，判定其防護需求等級為高者。

網路請購系統	上方式處理，影響機關行政效率	
出納帳務管理系統	機關支出、收入、帳務作業無法以線上方式處理，影響機關行政效率	24 小時
其他-非屬上開業務範疇及核心業務者(同本校資訊安全管理系統 編號：NCYU-ISMS-D-038 名稱：業務流程衝擊分析表)	影響機關行政效率	依其業務性質容許中斷24 小時至72 小時

肆、資通安全政策及目標

一、資通安全政策

同本校資訊安全管理系統(ISMS) 編號: NCYU-ISMS-A-001，

名稱:資訊安全政策，第三章：目標。

二、資通安全目標

同本校資訊安全管理系統(ISMS) 編號: NCYU-ISMS-A-001，

名稱: 資訊安全政策，第五章：管理指標。

三、資通安全政策及目標之核定程序

同本校資訊安全管理系統(ISMS) 編號: NCYU-ISMS-A-001，

名稱: 資訊安全政策，第七章：實施。

四、資通安全政策及目標之宣導

本校資訊安全政策公布於本校全球資訊網資訊安全專區。

五、資通安全政策及目標定期檢討程序

同本校資訊安全管理系統(ISMS) 編號: NCYU-ISMS-A-001，名稱: 資訊安全政策，第六章：審查。

伍、資通安全推動組織[3]

同本校資訊安全管理系統(ISMS) 編號:NCYU-ISMS-B-001，名稱:資訊安全組織程序書。

陸、專職(責)人力及經費配置

一、專職(責)人力及資源之配置

1. 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(責)人員 1 人，其工作如下，本校現有資通安全專職(責)人員名單及職掌應列冊，並適時更新[4]。

   (1) 資通安全管理面業務：推動資通系統防護需求分級、資通安全管理系統導入及驗證、內部資通安全稽核、本校資安弱點通報機制及教育訓練等業務之推動。

   (2) 資通安全防護業務：包含資通安全監控管理機制、安全性檢測、業務持續運作演練、資通安全防護設施建置及資通安全事件通報及應變業務之推動。

2. 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，並提升校內資通安全專業人員之資通安全管理能力。校內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。

[3] 本校資通安全推動組織將於核定後，將再參酌本校 ISMS 之資訊安全組織程序書 [NCYU-ISMS-B-001]進行相關調整。

[4] 各公務機關應製作「資通安全專職人員分工表」,說明專職人員及相關職掌。本校採用本校 ISMS 之資訊安全組織成員表[NCYU-ISMS-D-001]進行列冊，並將於核定後再進行相關細部調整。

3. 資安專職(責)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[5]。

(1) 資安專職(責)人員總計應持有 1 張以上資通安全專業證照[6]。

(2) 資安專職(責)人員總計應持有 1 張以上資通安全職能評量證書[7]。

4. 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[8]。

5. 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。

6. 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

1. 資通安全推動小組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[9]。

2. 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占之比例。

3. 各單位如有資通安全資源之需求，應配合本校預算規劃期程向資通安全推動小組提出[10]，由資通安全推動小組視整體資通安全資源進行分配，並經資通安全長核定後，進行相關之建置。

4. 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安

---

[5] 各機關應依據其資通安全責任等級分級辦法所規範之資通安全專責人員、認知與訓練之要求，配置適當之資源於資安人員專業職能之培養。

[6] 視各機關之資通安全責任等級之分級要求。

[7] 視各機關之資通安全責任等級之分級要求。

[8] 本校採用本校ISMS之人員資訊安全守則[NCYU-ISMS-C-006]及保密切結書[NCYU-ISMS-D-016]作為書面約定文件，並將於核定後再進行相關細部調整。

[9] 為有效建置機關之資通安全風險防護機制，公務機關應投入相當之資源，故機關之資通安全推動小組於資源規劃或編制預算時，應考量機關之責任等級、資通安全政策及目標。

[10] 各機關可填具資通安全需求申請單。本校採用本校 ISMS 之人員資訊安全守則[NCYU-ISMS-C-006]作為申請表單，並將於核定後再進行相關細部調整。

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

同本校資訊安全管理系統(ISMS) 編號: NCYU-ISMS-B-003，

名稱:資訊資產管理程序書。

二、本校資通安全責任等級分級

依教育部 112 年 10 月 18 日臺教資通字第 1122704063A 號來函轉知本校業經行政院核定為資通安全責任等級 C 級機關。

捌、資通安全風險評估

一、資通安全風險評估

同本校資訊安全管理系統(ISMS) 編號: NCYU-ISMS-B-004，

名稱:風險評鑑與管理程序書。

二、核心資通系統及最大可容忍中斷時間

核心資通系統	資訊資產	最大可容忍中斷時間	核心資通系統主要功能
校務行政系統	1.網站主機計 3 台 2.網路交換設備 1 台 (Extreme X620t)	8 小時	提供本校教職員工生線上差勤、個人相關申請、活動報名、場地借用、修繕申請，學生各種申請作業、學籍及選課作業、成績與抵

			免作業、畢業、學務、學習歷程等服務

最大可容忍中斷時間以小時計。

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核心資通系統之防護基準，採行相關之防護及控制措施，由於本校核心資通系統已導入 ISMS，核心之防護及控制措施詳如 ISMS 資通安全管理系統文件。

壹拾、資通安全事件通報、應變及演練相關機制

同本校資訊安全管理系統(ISMS) 編號: NCYU-ISMS-B-011，

名稱:安全事件管理程序書。

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，應指定資通安全專職人員進行情資分析，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。

(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，並配合教育機構資安平台（TANet CERT）資安預警之執行，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

由資通安全小組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(責)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

資通安全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，並依據資通安全維護計畫採行相應之風險管理機制。

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

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[11]。

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。

3. 受託者辦理受託業務得否重複委託、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

1. 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。

2. 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

[11] 委外單位之管理措施是否完善，可視其人員資格是否具有相關證照、訓練或認證（如 ISO 27001、CISSP、SSCP、各資安教育訓練單位所辦之課程等）做為參考。

件時，應立即通知委託機關及採行之補救措施。

3. 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。

4. 受託者應採取之其他資通安全相關維護措施[12]。

5. 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，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

本校依資通安全責任等級分級屬C級，

1. 資通安全專職人員每人每年至少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。
2. 資通安全專職人員以外之資訊人員，每人每二年至少接受三小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受三小時以上之資通安全通識教育訓練。
3. 一般使用者及主管，每人每年接受三小時以上之資通安全通識教育訓練。

二、資通安全教育訓練辦理方式

1. 承辦單位應於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全教育訓練計畫[13]，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教育訓練紀錄[14]。

2. 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、

[12] 公務機關與委外廠商簽訂契約時，應審查契約中保密條款，並要求委外廠商之業務執行人員簽署委外廠商執行人員保密切結書、保密同意書。本校採用本校 ISMS 之委外廠商保密切結書[NCYU-ISMS-D-019]進行簽署，並將於核定後再進行相關細部調整。

[13] 格式可參附件：年度資通安全教育訓練計畫。

[14] 公務機關辦理教育訓練時，參加人員應簽名留存紀錄，格式可參附件：資通安全教育訓練簽到表。

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。

3. 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。

4. 資通安全教育及訓練之政策，除適用所屬員工外，對學校外部的使用者，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，依據公務機關所屬人員資通安全事項獎懲辦法、國立嘉義大學職員獎懲實施要點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、資通安全維護計畫實施情形之稽核機制

(一) 稽核機制之實施

同本校資訊安全管理系統(ISMS) 編號: NCYU-ISMS-B-013，

名稱:資訊安全稽核作業程序書。

(二) 稽核改善報告

同本校資訊安全管理系統(ISMS) 編號: NCYU-ISMS-B-014，

名稱:矯正及預防管理程序書。

三、資通安全維護計畫之持續精進及績效管理

1. 本校之資通安全推動小組應每年至少一次召開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。

2. 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、資通安全推動小組決議事項等。

(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：

A. 資通安全政策及目標之實施情形。

B. 資通安全人力及資源之配置之實施情形。

C. 資通安全防護及控制措施之實施情形。

D. 內外部稽核結果。

E. 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。

3. 持續改善機制之管理審查應做成改善績效追蹤報告[15]，相關紀錄並應予保存，以作為管理審查執行之證據。

[15] 本校採用本校 ISMS 之矯正處理[NCYU-ISMS-D-042]進行追蹤，並將於核定後再進行相關細部調整。

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第 12 條之規定，應每年向教育部提出資通安全維護計畫實施情形[16]，使其得瞭解本校之年度資通安全計畫實施狀況。

壹拾柒、相關法規、程序及表單

一、相關法規及參考文件

1. 資通安全管理法
2. 資通安全管理法施行細則
3. 資通安全責任等級分級辦法
4. 資通安全事件通報及應變辦法
5. 資通安全情資分享辦法
6. 公務機關所屬人員資通安全事項獎懲辦法
7. 安全軟體發展流程指引
8. 資訊作業委外安全參考指引
9. 本校資通安全事件通報及應變程序
10. 本校資訊安全管理制度

二、本校現有 ISMS 四階文件(表單)

同本校資訊安全管理系統(ISMS) 編號: NCYU-ISMS-D-008，名稱:資訊安全管理文件列表。

[16] 資通安全維護計畫實施情形之內容，包含上開定期評估、稽核機制、缺失之消除或改正及機關辦理資通安全計畫之相關實施事項，參附件：資通安全維護計畫實施情形。