XXXX　學校

資通安全維護計畫

目　　錄

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。

適用範圍

本計畫適用範圍涵蓋 XXXX 學校全機關（以下簡稱本校）

核心業務及重要性

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
校務學生資料管理	校務系統	□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	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受罰。 影響校務運作	4 小時

各欄位定義：

1. 核心業務名稱：請參考資通安全管理法施行細則第 7 條之規定列示。

作業名稱：該項業務內各項作業程序的名稱。

重要性說明：說明該業務對機關之重要性，例如對機關財務及信譽上影響，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。

最大可容忍中斷時間單位以小時計。

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
公文交換	電子公文無法即時送達機關，影響機關行政效率	24 小時
校務基金系統	影響機關行政效率	24 小時
財管系統	影響機關行政效率	24 小時

各欄位定義：

1. 業務名稱：公務機關之非核心業務至少應包含輔助單位之業務名稱，如差勤服務、郵件服務、用戶端服務等。

1. 作業名稱：該項業務內各項作業程序的名稱。

2. 說明：說明該業務之內容。

3. 最大可容忍中斷時間單位以小時計。

資通安全政策及目標

依本校資通安全管理制度文件「ISMS-A-001 資訊安全政策」施行。

資通安全推動組織

依本校資通安全管理制度文件「ISMS-B-001 資訊安全組織程序書」、「ISMS-D-001 資訊安全組織成員表」施行。

專職(責)人力及經費配置

專職(責)人力及資源之配置

1. 本機關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，其分工如下，本校現有資通安全專責人員名單及職掌應表列於「ISMS-D-001 資訊安全組織成員表」，並適時更新。

(1) 資通安全管理面業務１人，負責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、機關資安治理成熟度評估及教育訓練等業務之推動。

資通系統安全管理業務1人，負責資通系統分級及防護基準、安全性檢測、業務持續運作演練等業務之推動。

資通安全防護業務1人，負責資通安全監控管理機制、政府組態基準導入，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。

資通安全管理法法遵事項業務1人，負責本機關對所屬公務務機關或所管特定非公務機關之法遵義務執行事宜。

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。

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。

(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。

(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。

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「ISMS-D-016保密切結書」，並視需要實施人員輪調，建立人力備援制度。

校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。

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。

經費之配置

1. 資訊安全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。

各單位於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。

各單位如有資通安全資源之需求，應配合機關預算規劃期程向資訊安全小組提出「資通安全需求申請單」，由資訊安全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。

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

資訊及資通系統之盤點

資訊及資通系統盤點

依本校資通安全管理制度文件「ISMS-B-003 資訊資產管理程序書」施行。

機關資通安全責任等級分級

本機關委外維運核心資通系統，為資通安全等級分類C級機關。

資通安全風險評估

資通安全風險評估

依本校資通安全管理制度文件「ISMS-B-004-風險評鑑與管理程序書」施行。

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
校務系統	網站前台主機計1台 網站後台主機計1台 骨幹網路交換器(HPE 5820)	4小時	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受罰。 影響機關業務運作

最大可容忍中斷時間以小時計。

資通安全防護及控制措施

本機關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如下:

資訊及資通系統之管理

依本校資通安全管理制度文件「ISMS-B-007 通信與作業管理程序」、「ISMS-C-001 資訊資產異動作業說明書」施行。

存取控制與加密機制管理

依本校資通安全管理制度文件「ISMS-B-008 存取控制管理程序書」施行。

作業與通訊安全管理

依本校資通安全管理制度文件「ISMS-006 實體安全管理程序書」、「ISMS-B-007 通信與作業管理程序書」施行。

系統獲取、開發及維護

1. 本校之資通系統應依「資通安全責任等級分級辦法」附表九之規定完成系統防護需求分級，依分級之結果，完成附表十中資通系統防護基準，並注意下列事項：

   (1) 開發過程請依安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)納入資安要求，並參考行政院國家資通安全會報頒布之最新「安全軟體發展流程指引」、「安全軟體設計指引」及「安全軟體測試指引」。

   於資通系統開發前，設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形。

   於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形。

   執行資通系統源碼安全措施，包含源碼存取控制與版本控管，並檢討執行情形。

   餘依本校資通安全管理制度文件「ISMS-B-009 系統開發與維護程序書」施行。

業務持續運作演練

本機關應針對核心資通系統制定業務持續運作計畫，並每二年辦理一次核心資通系統持續運作演練。

執行資通安全健診

1. 本機關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：

(1) 網路架構檢視。

(1) 網路惡意活動檢視。

(2) 使用者端電腦惡意活動檢視。

(3) 伺服器主機惡意活動檢視。

(4) 安全設定檢視。

資通安全防護設備

1. 本機關應建置防毒軟體、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。

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。

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，本機關應訂定資通安全事件通報、應變及演練相關機制，詳資通安全事件通報應變程序。

資通安全情資之評估及因應

本機關接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、本機關可接受之風險及本機關之資源，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。

資通安全情資之分類評估

本機關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：

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。

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。

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。

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機關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。

資通安全情資之因應措施

本機關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。

資通安全相關之訊息情資

由資訊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。

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。

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。

涉及核心業務、核心資通系統之情資

資訊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機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

資通系統或服務委外辦理之管理

本機關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。

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。

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。

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。

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。

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。

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。

受託者應採取之其他資通安全相關維護措施，簽署「委外廠商執行人員保密同意書」、「委外廠商執行人員保密切結書」。

本機關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，以本校「委外廠商查核項目表」進行稽核以確認受託業務之執行情形。

資通安全教育訓練

資通安全教育訓練要求

1. 本機關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 1 名人員接受 12 小時以上之資安專業課程訓練或資安職能訓練。

本機關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。

資通安全教育訓練辦理方式

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，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（ISMS-D-018 教育訓練簽到表教」）。

本機關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)。

資通安全法令規定。

資通安全作業內容。

資通安全技術訓練。

員工報到時，應使其充分瞭解本機關資通安全相關作業規範及其重要性。

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。

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

本機關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、國立華南高級商業職業學校教職員獎懲實施要點，及本機關各相關規定辦理之。

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

資通安全維護計畫之實施

為落實本安全維護計畫，使本機關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，應與本機關之資通安全政策、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。

資通安全維護計畫實施情形之稽核機制

稽核機制之實施

1. 資訊安全稽核小組應定期(至少每年一次)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. 辦理稽核前資訊安全小組應擬定「ISMS-C-004 資訊安全管理制度內部稽核計畫」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（稽核委員簽署「ISMS-D-016 保密切結書」）、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。

辦理稽核時，資訊安全稽核小組應於執行稽核前 30 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。

本機關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「ISMS-D-041 資訊安全管理制度內部稽核報告」中，並提供給受稽單位填寫辦理情形。

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。

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

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。

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。

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。

機關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。

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。

資通安全維護計畫之持續精進及績效管理

1. 本機關之資訊安全小組應於十二月(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。

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。

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。

資通安全維護計畫內容之適切性。

資通安全績效之回饋，包括：

資通安全政策及目標之實施情形。

資通安全人力及資源之配置之實施情形。

資通安全防護及控制措施之實施情形。

內外部稽核結果。

不符合項目及矯正措施。

風險評鑑結果及風險處理計畫執行進度。

重大資通安全事件之處理及改善情形。

利害關係人之回饋。

持續改善之機會。

持續改善機制之管理審查應做成「HNVS-ISMS-D-040 矯正與預防處理單」，相關紀錄並應予保存，以作為管理審查執行之證據。

資通安全維護計畫實施情形之提出

本機關依據本法第 11(16,17)條之規定，應於一月前向上級或監督機關，提出「資通安全維護計畫實施情形」，使其得瞭解本機關之年度資通安全計畫實施情形。

相關法規、程序及表單

相關法規及參考文件

1. 資通安全管理法

資通安全管理法施行細則

資通安全責任等級分級辦法

資通安全事件通報及應變辦法

資通安全情資分享辦法

公務機關所屬人員資通安全事項獎懲辦法

資訊系統風險評鑑參考指引

政府資訊作業委外安全參考指引

無線網路安全參考指引

網路架構規劃參考指引

行政裝置資安防護參考指引

政府行動化安全防護規劃報告

安全軟體發展流程指引

安全軟體設計指引

安全軟體測試指引

資訊作業委外安全參考指引

本機關資通安全事件通報及應變程序

附件表單

1. ISMS-A-001 資訊安全政策
2. ISMS-B-001 資訊安全組織程序書
3. ISMS-B-003 資訊資產管理程序書
4. ISMS-B-004 風險評鑑與管理程序書
5. ISMS-B-006 實體安全管理程序書
6. ISMS-B-007 通信與作業管理程序
7. ISMS-B-008 存取控制管理程序書
8. ISMS-B-009 系統開發與維護程序書
9. ISMS-C-001 資訊資產異動作業說明書
10. ISMS-C-004 資訊安全管理制度內部稽核計畫
11. ISMS-D-001 資訊安全組織成員表
12. ISMS-D-009 資訊資產清單
13. ISMS-D-016 保密切結書
14. ISMS-D-018 教育訓練簽到表
15. ISMS-D-019 人員進出機房登記表
16. ISMS-D-040 矯正與預防處理單
17. ISMS-D-041 資訊安全管理制度內部稽核報告
18. 資通安全需求申請單
19. 委外廠商執行人員保密切結書
20. 委外廠商執行人員保密同意書
21. 委外廠商查核項目表
22. 稽核項目紀錄表
23. 資通安全維護計畫實施情形