國立大湖高級農工職業學校
資通安全維護計畫

108 年 3 月 12 日行政會報通過
108 年 3 月 14 日湖農工圖字第 1080001785 號公告
108 年 12 月 10 日行政會報修正通過
108 年 12 月 10 日湖農工圖字第 1080008922 號公告修正
109 年 10 月 13 日行政會報修正通過
109 年 10 月 16 日湖農工圖字第 1090007500 號公告修正
110 年 5 月 11日行政會報修正通過
110年 5 月 14日湖農工圖字第1100003886號公告修正

目　　錄

壹、 依據及目的

依據資通安全管理法第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)。為因應資通安全管理法及資通安全責任等級應辦事項要求，以符合法令規定並落實本計畫之資通作業安全。

貳、 適用範圍

本計畫適用範圍涵蓋國立大湖高級農工職業學校全機關(以下簡稱本校)

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	資通系統分級
學籍資料	校務行政系統	為本校依組織法執掌，足認為重要者	成績及出缺勤及排課相關資料不正確，影響校務運作	24小時	中
數位學習歷程檔案(向上集中)	數位學習歷程檔案(向上集中)	為本校依組織法執掌，足認為重要者	學生學習歷程檔案無法上傳	24小時	中
學校首頁	學校首頁	為本校依組織法執掌，足認為重要者	外界無法查看學校公告	24小時	中
電子郵件	電子郵件	為本校依組織法執掌，足認為重要者	無法及時收發電子郵件，影響行政效率	24小時	中
DNS(向上集中)	DNS(向上集中)	為本校依組織法執掌，足認為重要者	外界無法查看學校首頁	24小時	中

各欄位定義：

1. 核心業務：請參考資通安全管理法施行細則第7條之規定列示。
2. 核心資通系統：該項業務內各項作業程序的名稱。
3. 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。
4. 業務失效影響說明：當系統失效時對學校所造成的衝擊及影響。
5. 最大可容忍中斷時間單位以小時計。
6. 資通系統分級：依據資通安全責任等級分級辦法附件九資通系統防護需求分級原則進行分級。

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	最大可容忍中斷時間	資通系統分級
圖書管理系統	無法借還書，影響機關行政效率	72小時	普
公文管理系統	電子公文無法及時送達機關，影響機關行政效率	48小時	普
主計出納管理系統	影響機關行政效率	48小時	普
人事差勤系統	人事差勤、獎懲各項待遇、福利等無法登記	48小時	普

各欄位定義：

1. 非核心業務：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。
2. 業務失效影響：說明該業務失效對機關之影響。
3. 最大可容忍中斷時間單位以小時計。
4. 資通系統分級：依據資通安全責任等級分級辦法附件九資通系統防護需求分級原則進行分級。

肆、 資通安全政策及目標

依本校「資通安全政策」如附件一施行。

伍、 資通安全推動組織

依本校「資通安全組織」辦法如附件二成立資通安全委員會並成立資訊安全小組，「資通安全組織成員表」如附件三。

陸、 專職(責)人力及經費配置

一、 專職(責)人力及資源之配置

1. 依據行政院108年7月24日院臺護字第1080180748號函，依據資通安全責任等級分級辦法第6條辦理，並考量本校已有核心系統向上集中規劃，依同法第10條第4款調降等級為 D 級。在未完成向上集中前本校應設置資通安全專責人員，其業務內容如下，本校現有資通安全專責人員名單及職掌應表列於「資通安全組織成員表」如附件三，並適時更新。

   (1) 資通安全管理面業務，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、內部資通安全稽核及教育訓練等業務之推動。

   (2) 資通系統安全管理業務，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。

   (3) 資通安全防護業務，負責資通安全監控管理機制、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責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。

3. 資安專責人員專業職能之培養(如證書、證照、培訓紀錄等)，應參加主管機關辦理之相關專業研習，並鼓勵取得資通安全專業證照及資通安全職能評量證書。

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「保密切結書」如附件四，並視需要實施人員輪調，建立人力備援制度。

5. 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。

6. 專責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。

2. 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。

3. 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需求，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。

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

依本校「資訊資產管理」規定如附件五施行。

二、 機關資通安全責任等級分級

依據行政院108年7月24日院臺護字第1080180748號函，依據資通安全責任等級分級辦法第6條辦理，並考量本校已有核心系統向上集中規劃，依同法第10條第4款調降等級為D級機關。

捌、 資通安全風險評估

一、 資通安全風險評估

依本校「風險評鑑與管理」規定如附件六施行。

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	核心資通系統主要功能	最大可容忍中斷時間
校務行政系統	網站前台主機1台 ASUS(windows	學校在校成績出缺勤及排課	24小時

	server2003/sql server) (滄學學習股份有限公司 /ischool 1Campus desktop 智慧校園校務系統)		
學校首頁	HP DL165 G5(Centos/Mysql) (數位果子科技有限公司 /ischool 高中E形象系統)	學校各項訊息傳達、業務執行	24小時
學習歷程檔案	非實體資產	學生學習歷程檔案資料	24小時
電子郵件	非實體資產	收發電子郵件、各項訊息傳達	24小時
DNS	非實體資產	Name Resolution	24小時

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如下:

一、 資訊及資通系統之管理

依本校「資訊資產異動作業」規定如附件七施行。

二、 存取控制與加密機制管理

依本校「存取控制管理」規定如附件八施行。

三、 作業與通訊安全管理

依本校資通安全管理制度文件「實體安全管理」規定如附件九、「通信與作業管理」規定如附件十施行。

四、 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」。

(2) 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。

(3) 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。

(4) 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。

2. 餘依本校「系統開發與維護」規定如附件十一施行。

五、 業務持續運作演練

本校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。

六、 執行資通安全健診

1. 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：

(1) 網路架構檢視。

(2) 網路惡意活動檢視。

(3) 使用者端電腦惡意活動檢視。

(4) 伺服器主機惡意活動檢視。

(5) 安全設定檢視。

七、 資通安全防護設備

1. 本校應建置防毒軟體、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，本校應訂定資通安全事件通報、應變及演練相關機制，詳如附件十二「資通安全事件通報應變程序」。

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。

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。

(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。

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。

3. 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

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. 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，格式如：附件十三「委外廠商執行人員保密切結書」、附件十四「委外廠商執行人員保密同意書」。

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，以本校「委外廠商查核項目表」如附件十五進行稽核以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

1. 本校資安及資訊人員每年至少接受12小時以上之資安專業課程訓練或資安職能訓練。

2. 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

1. 資通安全小組應於每年年初，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，以建立教職員生資通安全認知，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（如：「教育訓練簽到表」）。

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、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. 教職員報到時,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,除適用所屬教職員生外,對機關外部的使用者,亦應一體適用。

壹拾肆、 本校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,依據本校所屬人員資通安全事項獎懲辦法、本校教職員獎懲實施要點及各相關規定辦理之。

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

1. 資訊安全稽核小組應定期(至少每二年一次)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. 辦理稽核前資通安全小組應擬定「內部稽核計畫」如附件十六並安排稽核成員,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「保密切結書」如附件四)、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,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」如附件十七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「內部稽核報告」如附件十八中，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）。

(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. 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。

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

1. 本校之資通安全委員會應於二、十月(每年至少二次)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. 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「矯正與預防處理單」如附件十九，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

本校依據資通安全法第12條之規定，應於十月前向上級或監督機關，填報「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

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. 資訊系統風險評鑑參考指引
8. 政府資訊作業委外安全參考指引
9. 無線網路安全參考指引
10. 網路架構規劃參考指引
11. 行政裝置資安防護參考指引
12. 政府行動化安全防護規劃報告
13. 安全軟體發展流程指引
14. 安全軟體設計指引
15. 安全軟體測試指引
16. 資訊作業委外安全參考指引

二、 附件資料表單

附件一：資訊安全政策

國立大湖高級農工職業學校資通安全政策

一、資通安全政策

為使本校業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性(Confidentiality)、完整性(Integrity)及可用性(Availability)，特制訂本政策如下，以供全體同仁共同遵循：

1. 應建立資通安全風險管理機制，定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。
2. 應保護機敏資訊及資通系統之機密性與完整性，避免未經授權的存取與竄改。
3. 應強固核心資通系統之韌性，確保本校業務持續營運。
4. 應因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本校同仁之資通安全意識，本校同仁亦應確實參與訓練。
5. 針對辦理資通安全業務有功人員應進行獎勵。
6. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
7. 禁止多人共用單一資通系統帳號。

二、 資通安全目標

(一) 量化型目標

1. 核心資通系統可用性達 99.99%以上。(中斷時數/總運作時數≤0.1%)(確保本校關鍵業務系統資訊機房維運服務達全年上班時間 96.9%以上之可用性，並確保：因資通安全事件、異常事件、其 他安全事故造成系統、主機異常而中斷營運服務之情事，每年不 得超過 8 次。因資通安全事件、異常事件、其他安全事故造成系統、主機異常而中斷營運服務之情事，每次最長不得超過 8 工作小時。)

2. 知悉資安事件發生(含個資事故通報)，能於規定的時間完成通報、應變及復原作業。

3. 電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於 5%及 2%。

(二) 質化型目標：

1. 適時因應法令與技術之變動，調整資通安全維護之內容，以避免 資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、 竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。
2. 達成資通安全責任等級分級之要求，並降低遭受資通安全風險之 威脅。
3. 提升人員資安防護意識、有效偵測與預防外部攻擊等。

三、資通安全政策及目標之核定程序

資通安全政策由本校圖書館簽請資通安全長核定。

四、 資通安全政策及目標之宣導

(一)本校之資通安全政策及目標應每年透過教育訓練、內部會議、張貼公告等方式，向本校內所有人員進行宣導，並檢視執行成效。

(二)本校應每年向利害關係人(例如IT 服務供應商、與本校連線作業有關單位)進行資安政策及目標宣導，並檢視執行成效。

五、資通安全政策及目標定期檢討程序

資通安全政策及目標應定期於資通安全管理審查會議中檢討其適切性。

附件二：資訊安全組織

國立大湖高級農工職業學校資通安全組織

一、資通安全長

依本法第 11 條之規定,本校訂定教務主任為資通安全長，負責督導本校資通安全相關事項，其任務包括：

（一）資通安全管理政策及目標之核定、核轉及督導。

（二）資通安全責任之分配及協調。

（三）資通安全資源分配。

（四）資通安全防護措施之監督。

（五）資通安全事件之檢討及監督。

（六）資通安全相關規章與程序、制度文件核定。

（七）資通安全管理年度工作計畫之核定。

（八）資通安全相關工作事項督導及績效管理。

（九）其他資通安全事項之核定。

二、資通安全推動小組

(一)組織為推動本校之資通安全相關政策、落實資通安全事件通報及相關應變處理,由資通安全長召集各處室主任成立資通安全推動小組，其任務包括：

1. 跨部門資通安全事項權責分工之協調。
2. 應採用之資通安全技術、方法及程序之協調研議。
3. 整體資通安全措施之協調研議。
4. 資通安全計畫之協調研議。
5. 其他重要資通安全事項之協調研議。

(二)分工及職掌

本校之資通安全推動小組依下列分工進行責任分組,並依資通安全長之指示負責下列事項,本校資通安全推動小組分組人員名單及職掌應列冊，並適時更新之：

1. 策略規劃組：

(1) 資通安全政策及目標之研議。

(2) 訂定本校資通安全相關規章與程序、制度文件，並確保相關規章與程序、制度合乎法令及契約之要求。

(3) 依據資通安全目標擬定本校年度工作計畫。

(4) 傳達本校資通安全政策與目標。
(5) 其他資通安全事項之規劃。

2. 資安防護組：

(1) 資通安全技術之研究、建置及評估相關事項。
(2) 資通安全相關規章與程序、制度之執行。
(3) 資訊及資通系統之盤點及風險評估。
(4) 資料及資通系統之安全防護事項之執行。
(5) 資通安全事件之通報及應變機制之執行。
(6) 其他資通安全事項之辦理與推動。

3. 績效管理組：

(1) 辦理資通安全內部稽核。
(2) 每年定期召開資通安全管理審查會議，提報資通安全事項執行情形。

4. 資安宣導組：

(1) 辦理資通安全宣導。
(2) 維護資安網站。

5. 經費稽核組：

(1) 稽核資通安全經費執行。
(2) 協助編列相關資通安全經費。

附件三：資訊安全組織成員表

國立大湖高級農工職業學校資通安全組織成員表

製表日期：110 年 03 月 24 日

單位職級	職稱	職掌事項	分機	備註(代理人)
校長	召集人	召集並主持會議	300	校長室秘書
教務主任	資訊安全長	統籌全校資通安全	401	圖書館主任
圖書館主任	策略規劃組長	策略規劃及承辦	709	教務主任
設備組長	策略規劃副組長	協助設備規劃	404	圖書館主任
實習主任	資安防護組長	資安防護及稽核	501	總務主任
總務主任	資安防護副組長	協助資安防護及稽核	101	實習主任
學務主任	資安宣導組長	資安宣導規劃	411	主任教官
主任教官	資安宣導副組長	協助資安宣導	701	學務主任
人事主任	績效管理組長	資安執行績效考核	321	主計主任
主計主任	經費稽核組長	資安經費稽核	311	人事主任

附件四：保密切結書

保密切結書

本人 _____ 將嚴守工作保密規定與國家相關法令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、傳播任何侵害智慧財產權之任何程式、軟體。保密之義務，不因調職或離職而終止。如有違反，依法負刑事、民事及行政責任。

此致

國立大湖高級農工職業學校

立 同 意 書 人：_____

電　　話：_____

地　　址：_____

中　華　民　國　　年　　月　　日

附件五：資訊資產管理

國立大湖高級農工職業學校資訊資產管理

一、資訊及資通系統盤點

（一）本校每年辦理資訊及資通系統資產盤點,依管理責任指定對應之資產管理人,並依資產屬性進行分類,分別為資訊資產、軟體資產、實體資產、支援服務資產等。

（二）資訊及資通系統資產項目如下：

1. 資訊資產:以數位等形式儲存之資訊,如資料庫、資料檔案、系統文件、操作手冊、訓練教材、研究報告、作業程序、永續運作計畫、稽核紀錄及歸檔之資訊等。
2. 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。
3. 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。
4. 支援服務資產：相關基礎設施級其他本校內部之支援服務，如電力、消防等。
5. 人員資產：內部設備維運管理人員、主管、使用人員，以及委外廠商駐點人員等。
6. 資料資產：以紙本形式儲存之資訊，如程序、清單、計畫、報告、指引手冊、政策、公文、作業紀錄、作業規範、各種應用系統文件及管理手冊，契約、法律文件、軟體使用授權等。

（三）本校每年度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」,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、管理者、使用者、存放位置、防護需求等級。

（四）資訊及資通系統資產應以標籤標示於設備明顯處,並載明財產編號、保管人、廠牌、型號等資訊。核心資通系統及相關資產，並應加註標示。

（五）各單位管理之資訊或資通系統如有異動,應即時通知資通安全推動小組更新資產清冊。

國立大湖農工資訊及資通系統資產清冊

編號：01

製表日期：110年03月25日

項次	資產名稱	類別	擁有者/職稱	管理者（部門）	使用者（部門）	存放位置	數量	說明	防護需求等級	核心系統	備註
1.	學務系統	實體資產	黃瓊慧老師/教務處教學組長	教務處	教務處與學務處	機房	1	教學課程與學生事務(成績與出缺勤)	中	■是 □否	Asus(windows server 2003/sql server)(鴻學學習股份有限公司 / ischool 1Campus desktop 智慧校園校務系統)
2.	學校首頁	實體資產	林啟鵬老師/圖書館主任	圖書館	全校	機房	1	學校各項訊息傳達、業務執行	中	■是 □否	HP DL165 G5 (Centos/Mysql)(數位果子科技有限公司 / iSchool 高中 E 形象系統)
3.	學習歷程檔案系統(向上集中)	非實體資產	洪德堯老師/教務處註冊組長	教務處	教務處與學務處	教育部國民及學前教育署	1	學生學習歷程檔案資料	中	■是 □否	N/A
4.	電子郵件	非實體資產	林啟鵬老師/圖書館主任	圖書館	教職員	GOOGLE	1	教師各項訊息傳達	中	■是 □否	N/A
5.	DNS(向上集中)	實體資產	林啟鵬老師/圖書館主任	圖書館	全校	教育部	1	Name Resolution	中	■是 □否	N/A
6.	公文管理	實體資產	黃美華組長/總務處文書組長	總務處	總務處	機房	1	公文簽核管理	普	□是 ■否	HP DL20G9 (windows server 2012/sql server)(五福科技有限公司 / 公文簽核系統)
7.	主計出納系統	實體資產	彭倩盈/主計室組員	主計室	主計室	機房	1	經費收支管理	普	□是 ■否	HP DL20G9 (windows server 2012/sql server)(艾富資訊股份有限公司 / 國立社教機構作業基金及國立高級中等學校校務基金系統)
8.	圖書資訊系統	實體資產	謝雨潔/圖書館幹事	教務處	圖書館	機房	1	圖書資訊資料	普	□是 ■否	Dell R210(windows server 2008/sql server)(寶慶文化科技股份有限公司 / M7 圖書館自動化系統)
9.	人事差勤系統	非實體資產	教育部國民及學前教育署	教育部國民及學前教育署	全校	教育部國民及學前教育署	1	人事差勤管理	普	□是 ■否	N/A

附件六：風險評鑑與管理

國立大湖高級農工職業學校風險評鑑與管理

1、目的

建立國立大湖高級農工職業學校（以下簡稱「本校」）資訊安全管理制度（以下簡稱 ISMS）風險評鑑與管理規範，提供本校資訊資產之權責單位、保管單位，以及使用單位，共同遵行之風險評鑑標準，有效執行風險控管，預防資訊安全事件之威脅。

2、適用範圍

本校承辦相關資訊業務作業流程之風險管理。

3、權責

3.1 資訊安全委員會：

負責可接受風險值、風險評鑑結果、風險改善計畫與控制措施之審查及核定。

3.1.1 資訊安全小組：

負責相關資訊資產風險評鑑結果之複核，並針對超過可接受風險值之項目提出建議之控管措施，並產出風險改善計畫。

3.1.2 權責單位主管：

負責所屬單位業務範圍之風險評鑑結果審核作業。

3.1.3 資訊資產權責單位：

負責執行資訊資產之威脅與弱點評估、風險值計算等程序項目。

4、名詞定義

4.1 機密性（Confidentiality）

確保只有經授權的人，才可以存取資訊。

4.2 完整性（Integrity）

確保資訊與處理方法的正確性與完整性。

4.3 可用性（Availability）

確保經授權的使用者在需要時可以取得資訊及相關資產。

4.4 可接受風險值

各類資訊資產之最低風險容忍度。

4.5 殘餘風險（Residual Risk）

在採用相關控制措施之後剩餘的風險。

4.6 威脅（Threat）

可能對系統或組織造成傷害之意外事件。

4.7 弱點（Vulnerability）

因資訊資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。

4.8 風險（Risk）

可能對團體或組織的資產發生損失或傷害的潛在威脅，通常利用弱點所產生之影響及發生可能性來衡量。

5、作業說明

5.1 鑑別資產

5.1.1 資訊資產之鑑別應依據「資訊資產管理程序書」進行鑑別及分類。

5.2 鑑別風險

5.2.1 威脅及弱點評估

參考 ISO 27005 將各類資訊資產可能面臨之威脅與弱點項目，分別建立「威脅及弱點評估表」。

5.2.2 事件發生機率與影響程度評估

5.2.2.1 依威脅的等級對應表（表 1）評估各事件之威脅等級：

表 1 威脅的等級對應表

評估標準	評估值
威脅發生之可能性為低	1
威脅發生之可能性為中	2
威脅發生之可能性為高	3

5.2.2.2 依弱點的等級對應表（表 2）評估各事件之弱點等級：

表 2 弱點的等級對應表

評估標準	評估值
該弱點不容易被威脅利用	1

該弱點容易被威脅利用	2
該弱點非常容易被威脅利用	3

5.2.3 風險值的計算

評估威脅發生之可能性及弱點受到威脅利用之容易度，計算出風險值。

風險值=（資訊資產價值 × 威脅等級 × 弱點等級）

5.3 風險管理

5.3.1 可接受風險值的決定

5.3.1.1 資訊資產之可接受風險值，需經資訊安全委員會開會決議，並記載於會議紀錄中。

5.3.1.2 資訊安全委員會每年召開會議檢討可接受風險值。可接受風險必須考量組織環境及作業之安全需求，並進行適當地調整。

5.3.1.3 資訊安全小組應針對高於可接受風險值項目，產出「風險評鑑彙整表」作為風險管理之依據。

5.3.2 選擇控制措施

5.3.2.1 超出可接受風險值之項目，應選擇適當之控管措施，並產出「風險改善計畫表」，說明風險控管措施之執行辦法。

5.3.2.2「風險改善計畫表」應陳報資訊安全委員會開會審核，並列入追蹤管理程序。

5.3.2.3 資訊安全小組依據風險控管措施產出「適用性聲明書」。

5.3.3 風險改善狀況的後續追蹤

5.3.3.1 資訊安全小組應針對「風險改善計畫表」彙整控管，持續追蹤至完成改善為止。

5.3.3.2 應於各項風險改善措施完成後，應進行風險再評鑑，以確保相關改善措施的有效性。

5.4 覆核

5.4.1 監控

控制措施的實施必須建立相對應的指標或紀錄，以反應出控制措施實施的狀況及成效，便於管理階層及相關人員做定期或不定期審視。

5.4.2 持續改善

為保持本風險評鑑方法之有效性與適用性，資訊安全小組得定期檢討可接受風險值與「威脅及弱點評估表」之項目。以期確保資訊資產均處於最佳保護之下，提供持續不中斷的營運。

5.4.3 風險重新評鑑

5.4.3.1 每年應至少執行 1 次風險評鑑。

5.4.3.2 當有新增系統、系統有重大異動或作業環境改變時則應執行不定期之風險評鑑。

6、附件

6.1 事件風險權值對照表

威脅等級（發生之可能性）		低(1)			中(2)			高(3)		
弱點等級（受到威脅利用之容易度）		低(1)	中(2)	高(3)	低(1)	中(2)	高(3)	低(1)	中(2)	高(3)
資產價值	1	1	2	3	2	4	6	3	6	9
	2	2	4	6	4	8	12	6	12	18
	3	3	6	9	6	12	18	9	18	27
	4	4	8	12	8	16	24	12	24	36

附件七：資訊資產異動作業

國立大湖高級農工職業學校資訊資產異動作業

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本校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。

附件八：存取控制管理

國立大湖高級農工職業學校存取控制管理

一、存取控制與加密機制管理

(一)網路安全控管

1. 本校之網路區域劃分如下：
   (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)：本校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. 對於通過防火牆之來源端主機IP 位址、目的端主機IP 位址、來源通訊埠編號、目的地通訊埠編號、通訊協定、登入登出時間、存取時間以及採取的行動，均應予確實記錄。
5. 本校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。
6. 對網路系統管理人員或資通安全主管人員的操作,均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。
7. 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。
8. 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。
9. 無線網路防護
   (1)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. 本校之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 90 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並劃定特權帳號逾期 之處理方式。

(四)加密管理

1. 本校之機密資訊於儲存或傳輸時應進行加密。
2. 本校之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。

附件九：實體安全管理

國立大湖高級農工職業學校實體安全管理程序書

1、目的

本程序書制訂之目的，在於保護國立大湖高級農工職業學校(以下簡稱「本校」)資訊資產及周邊環境設施，減少環境安全問題所引發的危險，以便達成本校安全控管之目的。

2、適用範圍

本校機房及周邊環境與設備安全管理。

3、權責

本校相關人員、約聘（僱）人員與委外人員：遵守本程序書之相關規定，以確保本校安全區域與人員辦公區域及資訊資產設備之安全。

4、名詞定義

無。

5、作業說明

5.1 安全區域

5.1.1 本校之機房為安全區域。

5.1.2 為確保相關設施之安全，非權責單位授權之人員不得擅自進入安全區域或使用相關資訊設備。

5.1.3 若外部人員或本校未具機房進出權限之人員，因執行業務需求進入機房時，必須由資訊資產權責單位或保管單位指派人員隨行並填寫「人員進出機房登記表」後方可進出機房，並遵守相關設備管理之規定。

5.1.4 安全區域之門禁紀錄，該紀錄應適當保存與定期審閱。

5.2 一般控制措施

5.2.1 無人時或下班最後一人離開時，需將辦公室關門上鎖。

5.2.2 為防止未經授權之存取，同仁應於下班後，遵守桌面淨

空政策，並將敏感等級（含）以上之文件與可攜式資訊設備皆存放於儲櫃並上鎖，避免資訊外洩之機會。

5.2.3 同仁於本校安全區域與辦公室內需隨時注意身分不明或可疑的人員。發現不明身分之人員時，需主動詢問並儘速通知相關部門進行處理。

5.2.4 同仁需隨時清理個人電腦的資源回收筒，以確保已經刪除的重要資料不會因為遺留在資源回收筒未清理，而遭未經授權之使用。

5.2.5 未經授權不得將設備、軟體、儲存資訊之媒體或文件攜出安全區域。如有需要，則須經主管人員核准，始得進行。

5.3 一般設備安全

5.3.1 資訊資產與相關設備安全之維護需考量設備之使用、安置、儲存、監控、移出與報廢等安全管理。

5.3.2 可攜式電腦，需以密碼保護，免於被偷取、遺失而遭未經授權的盜用，並於使用完畢後，刪除電腦中非一般等級之資料及清理資源回收筒內之資料。

5.3.3 個人電腦、伺服器或電腦終端機不使用時，需採用密碼保護、鎖定或登出離線等安全控制措施。

5.4 硬體資訊資產安全維護

5.4.1 重要之儲存媒體，應上鎖或由專人管理，並且僅經授權之使用者方能使用。

5.4.2 謹慎使用電源延長線，以免電力無法負荷而導致火災，於新增硬體設備時，應先評估電力負荷。

5.4.3 設備異動（包含新增、報廢、變更用途），應重新評估相關系統設定。

5.5 機房設備安全維護

5.5.1 重要資訊設備，應放置於機房，並落實安全管理。

5.5.2 電力、網路、通信設備應予以保護，以防止遭有心人士截取或破壞。

5.5.3 機房內應保持整齊清潔，並嚴禁吸菸、飲食或堆置易燃物。

5.5.4 電腦機房應設置專用空調設備以維持電腦主機正常運作。

5.5.5 經評估後，確定將資訊設備（如：伺服器、防火牆…等）委外維護時，應簽訂維護契約，並定期實施保養與維護，以確保設備完整性及可用性之持續使用。

5.5.6 重要電腦主機之資訊設備及警報系統等應定期檢修測試。

5.5.7 冷氣機、不斷電系統（UPS）等機電設備之使用，應依照設備說明書指示操作，並施行定期檢查作業。

5.5.8 機房應設置足量之不斷電系統（UPS），供應重要資訊設備電源之使用，以保障資訊設備之正常作業。

5.5.9 機房溫溼度應維持在機器可正常運轉的範圍內，並需 24 小時維持空調運轉。

5.5.10 資訊設備專用電源插座，不得使用於資訊及空調設備以外之設備，以免耗用電源，發生跳電當機情形，影響正常作業。

5.5.11 資訊設備保管單位應於每工作日檢核各設備之運作狀況，發現異常時，應填寫「異常事件紀錄表」並進行必要之處置。

5.6 移轉資產之安全管理

5.6.1 機房中資訊設備之進出應填寫「設備進出紀錄表」敘明其設備進出原因或目的。

5.6.2 資訊設備、資料或軟體之移轉，應依「資訊資產管理程序書」辦理，並由資訊安全小組負責更新「資訊資產清單」。

5.6.3 硬體資產報廢前應確實清除限閱等級(含)以上之資訊，以避免資訊外露，並確實清點報廢資產後，方可進行報廢，相關作業規範請參閱「資訊資產異動作業說明書」。

5.7 送修作業

5.7.1 資訊設備送修前，資訊設備之權責單位應依該設備之資訊資產價值選擇適當之備援方案，並備註說明於「設備進出紀錄表」。

5.7.2 資訊設備若具敏感等級以上之資料，於送修前應請廠商

簽署「委外廠商保密切結書」。

5.8 維護契約

5.8.1 所有資訊設備維護契約，應由專人負責保管與定期審查契約時間是否過期與該資訊設備是否仍有維護需求，若仍有維護需求則應依「委外管理程序書」簽訂維護契約。

6、相關文件

6.1 資訊資產管理程序書
6.2 委外管理程序書
6.3 資訊資產異動作業說明書
6.4 資訊資產清單
6.5 人員進出機房登記表
6.6 設備進出紀錄表
6.7 異常事件紀錄表
6.8 委外廠商保密切結書

附件十：通信與作業管理

國立大湖高級農工職業學校通訊與作業管理

一、作業與通訊安全管理

(一)防範惡意軟體之控制措施

1. 本校之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。
   (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，宜於他處先掃描有無惡意軟體。
   (3)確實執行網頁惡意軟體掃描。
2. 使用者未經同意不得私自安裝應用軟體,管理者並應每半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. 本校資通系統之操作及維護以現場操作為原則,避免使用遠距工作，如有緊急需求時，應申請並經資通安全推動小組同意後始可開通。
2. 資通安全推動小組應定期審查已授權之遠距工作需求是否適當。
3. 針對遠距工作之連線應採適當之防護措施(並包含伺服器端之集中過濾機制檢查使用者之授權)，並且記錄其登入情形。
   (1)提供適當通訊設備，並指定遠端存取之方式。
   (2)提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。
   (3)遠距工作終止時之存取權限撤銷，並應返還相關設備。

(三)電子郵件安全管理

1. 本校人員到職後應經申請方可使用電子郵件帳號,並應於人員離職後刪除電子郵件帳號之使用。
2. 電子郵件系統管理人應定期進行電子郵件帳號清查。
3. 電子郵件伺服器應設置防毒及過濾機制,並適時進行軟硬體

之必要更新。

4. 使用者使用電子郵件時應提高警覺,並使用純文字模式瀏覽,避免讀取來歷不明之郵件或含有巨集檔案之郵件。
5. 原則不得電子郵件傳送機密性或敏感性之資料,如有業務需求者應依相關規定進行加密或其他之防護措施。
6. 使用者不得利用本校所提供電子郵件服務從事侵害他人權益或違法之行為。
7. 使用者應確保電子郵件傳送時之傳遞正確性。

(四)確保實體與環境安全措施

1. 資料中心及電腦機房之門禁管理
   (1)資料中心及電腦機房應進行實體隔離。
   (2)本校人員或來訪人員應申請及授權後方可進入資料中心及電腦機房,資料中心及電腦機房管理者並應定期檢視授權人員之名單。
   (3)人員及設備進出資料中心及電腦機房應留存記錄。
2. 資料中心及電腦機房之環境控制
   (1)資料中心及電腦機房之空調、電力應建立備援措施。
   (2)資料中心及電腦機房應安裝之安全偵測及防護措施,包括熱度及煙霧偵測設備、火災警報設備、溫濕度監控設備、漏水偵測設備,入侵者偵測系統,以減少環境不安全引發之危險。
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。

(五)資料備份

1. 重要資料及核心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。

(六)媒體防護措施

1. 使用隨身碟或磁片等存放資料時,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. 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磁帶，應保存於上鎖之櫃子，且需由專人管理鑰匙。

(七)電腦使用之安全管理

1. 電腦、業務系統或自然人憑證，若超過十五分鐘不使用時，應立即登出或啟動螢幕保護功能並取出自然人憑證。
2. 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。
3. 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。
4. 下班時應關閉電腦及螢幕電源。
5. 如發現資安問題，應主動循本校之通報程序通報。

(八)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。

(九)即時通訊軟體之安全管理

1. 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。但有業務需求者，應使用經專責本校鑑定相符機密等級保密機制或指定之軟、硬體，並依相關規定辦理。
2. 使用於傳遞公務訊息之即時通訊軟體應具備下列安全性需求：
   (1)用戶端應有身分識別及認證機制。
   (2)訊息於傳輸過程應有安全加密機制。
   (3)應通過經濟部工業局訂定行動化應用軟體之中級檢測項目。
   (4)伺服器端之主機設備及通訊紀錄應置於我國境內。
   (5)伺服器通訊紀錄（log）應至少保存六個月。

二、 資通安全防護設備

(一)本校應建置防毒軟體、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。

(二)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。

附件十一：系統開發與維護

國立大湖高級農工職業學校系統開發與維護

1、目的

本程序書制訂之目的在於確保國立大湖高級農工職業學校(以下簡稱「本校」) 資訊系統開發、測試與維護作業之安全管理。

2、適用範圍

資訊系統之程式開發相關支援活動,如既有線上系統之測試、修改、維護、上線變更、原始碼之管控與儲存等作業。

3、權責

本校相關資訊系統開發、維護人員與委外人員：遵守本程序書之相關規定，以確保本校相關軟體與資料等資訊資產之安全。

4、名詞定義

無。

5、作業說明

5.1 一般控制措施

5.1.1 當發展新資訊系統，或現有系統功能之強化，於系統規劃需求分析階段，即將安全需求要項納入系統功能。

5.1.2 除由系統自動執行之安全控管措施之外，亦可考量由人工執行相關控管措施。

5.1.3 在採購套裝軟體時，視其安全需求，進行分析。除事前經權責單位主管核准外，應避免修改套裝軟體，如需修改應依本程序書之變更作業控制措施加以控管。

5.1.4 系統之安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足，可能帶來之傷害程度。

5.1.5 資訊系統應保護敏感等級（含）以上之資料，防止洩漏或被竄改，必要時應使用資料加密之相關機制保護。

5.1.6 在作業系統上執行應用軟體，應建立控制程序並嚴格執行，為減少可能危害作業系統之風險，應用程式之更新

作業應限定只能由授權之管理人員才可執行，且應建立應用程式之更新稽核紀錄。

5.1.7 真實資料被複製到測試系統時，應依複製作業之性質及內容，在取得授權後始能進行，敏感資料欄位應予模糊化。

5.1.8 系統若需委外建置或維護，請參考「委外管理程序書」之相關管理規範。

5.1.9 系統弱點管理，請參考「通信與作業管理程序書」之相關管理規範。

5.1.10 各單位若有資料需求申請時，申請人視情況應依電子公文程序或填寫『資料需求申請表』經單位主管同意後，呈秘書室或副校長室核決，本校始得提供資料內容。

5.2 軟體控制措施

5.2.1 作業系統變更時，應審查與測試重要營運系統，以確保對組織作業或安全無不利之衝擊。

5.2.2 系統軟體安裝

系統軟體應由系統負責人進行安裝，安裝時應視狀況通知相關技術人員支援或通知使用者，以避免資訊服務中斷或影響業務。

5.2.3 系統軟體測試

5.2.3.1 軟體測試由系統負責人辦理，測試時應事先通知協調相關人員支援。

5.2.3.2 系統負責人應通知相關人員及使用者以避免資訊服務中斷或影響業務。

5.2.4 系統軟體更新

系統負責人需定期檢視更新系統安全修補、防毒軟體及防毒碼，以維持系統正常運作。

5.3 開發作業控制措施

5.3.1 提案與回覆

5.3.1.1 申請單位提出「系統需求申請與回覆單」敘明需求理由。

5.3.1.2 承辦人員於完成與申請單位之訪談與系統分析後，於「系統需求申請與回覆單」中回覆評估結果，

包含功能細項、預估人力與時程、建議方案等。

5.3.1.3 經評估系統修改幅度不大，且不涉及系統流程變更者，於「系統需求申請與回覆單」中回覆處理結果並結案。

5.3.2 分析規劃與程式撰寫

5.3.2.1 程式開發者應於程式開發前進行系統分析，系統分析時應將系統安全需求納入考量。如涉及重要資料之傳輸，應使用 SSL 加密金鑰，並依下列規定管理金鑰：

5.3.2.1.1 金鑰應有明確的啟動與止動日期，並於可用期間，保護其不被修改、遺失和破壞。

5.3.2.1.2 金鑰之使用與存取，應限於使用金鑰之系統管理者，不可由其他非系統管理者任意存取。

5.3.2.1.3 對於金鑰之使用、啟動、止動，皆應留存相關之紀錄。

5.3.2.2 輸入應用系統之資料，應檢查主要欄位或資料檔案的內容，以確保資料的有效性及真確性。

5.3.2.3 對高敏感性的輸入資料，必要時應採用資料保密機制，在傳輸或儲存過程中應採加密方法保護。

5.3.2.4 輸出之資料，應於輸出之前，確認其正確性；對於系統內之訊息，則需保護其完整性。

5.3.3 測試

5.3.3.1 測試環境與線上環境應予以分開。

5.3.3.2 程式設計初步完成後，準備「系統測試記錄表」通知申請單位進行聯合測試，並請申請單位於「系統測試記錄表」中填寫測試結果。

5.3.3.3 程式功能若無法達成申請單位預定需求，則請系統開發人員另行修改程式後，擇期再測試，直至符合預定需求為止。

5.3.4 上線與驗收

5.3.4.1 聯合測試進行順利完成後，進行相關驗收作業，並請申請單位簽收「系統測試記錄表」。

5.3.4.2 若原系統已經存在，應於系統上線前訂定「系統

上線及緊急復原計畫表」,內容包含系統轉換規劃，轉換備援處理等。

5.3.4.3 系統上線後，程式開發者應提出系統設計與功能規格書，內容包含『系統作業流程圖』、『系統資料庫說明表』，以及『系統程式碼清冊』。

5.3.4.4 系統若委由其他單位開發時，應請開發單位交付系統設計與功能規格書，由本校程式開發權責單位審閱，並留存備查。

5.3.5 後續系統增修維護

5.3.5.1 專案上線後功能如需修補，申請單位應填「系統需求申請與回覆單」,程式開發權責單位依需求規格進行訪談規劃設計。

5.3.5.2 程式開發權責單位完成系統增修作業後與申請單位進行測試驗收結案。

5.4 變更作業控制措施

5.4.1 變更作業應考量之事項：

5.4.1.1 在實際執行變更作業前，變更作業之細項建議，應取得權責主管人員之核准。

5.4.1.2 應確保系統變更作業不致影響或破壞系統原有的安全控制。

5.4.1.3 系統開發或變更，應更新系統文件。

5.4.1.4 程式維護時，應在程式內以註解說明異動部分。

5.4.1.5 所有系統變更作業請求，皆應建立紀錄供稽核運用。

5.4.2 變更作業之控制流程：

5.4.2.1 在實際執行變更作業前，申請者應先填具「系統需求申請與回覆單」提出變更需求，並經權責主管人員核准確認。

5.4.2.2 變更作業如有需要，應會辦相關人員配合。

5.4.2.3 上線前應先進行測試，必要時請相關人員配合建置測試環境。

5.4.2.4 除非事先經由權責主管人員核准外，測試不應在線上營運系統執行。

5.4.2.5 測試完成後，程式開發權責單位應擬定「系統上線及緊急復原計畫表」，決定上線日期，經權責主管人員確認後始得上線。

5.4.2.6 上線後應立即於線上營運系統再行測試，以確認系統運作正常。測試人員不宜與程式開發者為同一人，以減少錯誤機會發生。

5.4.2.7 上線後測試如發現狀況，應嘗試可否立即排除，如無法立即排除，應依緊急復原計畫，回復上線前原狀。

5.4.2.8 變更作業完成後應修改相關系統設計與功能規格書。

6、相關文件

6.1 通信與作業管理程序書

6.2 委外管理程序書

6.3 系統需求申請與回覆單

6.4 系統測試紀錄表

6.5 系統作業流程圖

6.6 系統資料庫說明表

6.7 系統上線及緊急復原計畫表

6.8 系統程式碼清冊

6.9 資料需求申請表

附件十二：資通安全事件通報及應變程序

國立大湖高級農工職業學校資通安全事件通報及應變管理程序

壹、目的

國立大湖農工為遵照資通安全管理法第14條及本校資通安全維護計畫之規定，建立資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特制定本資通安全事件通報及應變管理程序(以下稱本管理程序)。

貳、適用範圍

發生於本校之事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通 安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全 政策之威脅者。

參、責任

一、本校於發現資通安全事件時，應依本程序或權責人員之指示，執行通報及 應變事務。

二、本校應視必要性，與受託機關約定，使其制定其資通安全事件通報及應變 管理程序，並於知悉資通安全事件後向本部進行通報，於完成事件之通報 及應變程序後，依本校指示提供相關之紀錄或資料。

三、本校應於知悉資通安全事件後，應依本程序之規定，儘速完成損害控制、 復原與事件之調查及處理作業。完成後，應依教育部指定之方式進行結案 登錄作業，並送交調查、處理及改善報告。

肆、事件通報窗口及緊急處理小組

一、臺灣學術網路資通安全事件委託由臺灣學術網路危機處理中心之教育機構 資安通報應變小組(簡稱通報應變小組)負責，聯繫資訊如下：

(一) 聯絡電話：

(07)525-0211

(二) 網路電話：

98400000

（三） 電子郵件：service@cert.tanet.edu.tw

二、本校應至少指派二位以上資安聯絡人員，並於「教育機構資安通報應變平 台」(https://info.cert.tanet.edu.tw)登錄相關聯絡資料，如有異動亦 應立即上網更新。

三、 本校之資通安全事件通報窗口及聯繫專線為：

（一） 聯絡電話：(037)992216-709

（二） E-mail：dml215@thvs.mlc.edu.tw

四、本校應以適當方式使相關人員明確知悉本機關之通報窗口及聯絡方式。

五、 本校所屬人員知悉資通安全事件後，應立即至教育機構資安通報平台
(https://info.cert.tanet.edu.tw)通報登錄資安事件細節、影響等級及支援申請等資訊。

六、本校應確保通報窗口之聯絡管道全天維持暢通，若因設備故障或其他情形 導致窗口聯絡管道中斷，該中斷情況若持續達一小時以上者，應即將該情 況告知相關人員，並即提供其他有效之臨時聯絡管道。

七、負責事件處理之單位(該事件發生之單位)權責人員應與相關單位密切合作 以進行事件之處理，並使通報窗口適時掌握事件處理之進度及其他相關資 訊。

八、 事件經初步判斷認為可能屬重大(第「三」級、第「四」級)資安事件或事態嚴重時，應即向資通安全長報告，由資通安全長成立緊急處理小組，立即協助進行處理；接獲本校受託廠商所通報之資通安 全事件時，亦同。

九、緊急處理小組成員由資通安全長指派機關之資通安全相關技術人員擔任， 或亦得由其他機關資通安全相關技術人員或外部專家擔任之。

十、各相關權責人員應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

伍、通報程序

一、判定事件等級之流程及權責 本校之權責人員或緊急處理小組應依據以下事項，於知悉資通安全事件後，依規定完成「資通安全事件通報及應變辦法」之資通安全事件等級判斷：

(一)事件涉及核心業務或關鍵基礎設施業務之資訊與否。

(二)事件導致業務之資訊或資通系統遭竄改之影響程度,屬嚴重或輕微。

(三)事件所涉資訊是否屬於國家機密、敏感資訊或一般公務機密。

(四)機關業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復　正常運作。

(五)件其他足以影響資通安全事件等級之因素。

二、 本校因網路或電力中斷等事由，致無法依前項規定方式為通報者，應於確 認資安事件條件成立後 1 小時內，與所隸屬區縣市網路中心及通報應變小 組聯繫，先行提供該次資安事件應通報之內容及無法通報依規定方式通報 之事由，並於事由解除後，依原方式補行通報。

三、 資通安全事件等級如有變更，本校權責人員或通報應變小組應告知通報單 位，使其續行通報作業。

四、 本校於委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合 約中訂定委外廠商於知悉資通安全事件時，應即向委託單位所屬之權責人 員通知，以指定之方式進行通報。

五、 本校於知悉資通安全事件後，如認該事件之影響涉及其他機關或應由其他 機關依其法定職權處理時，權責人員或通報應變小組應於知悉資通安全事 件後一小時內，將該事件依教育部或行政院所指訂或認可之方式，通知該 機關。

六、 本校執行通報應變作業時，得視情形向所隸屬區縣市網路中心人員提出技 術支援或其他協助之需求。

陸、應變程序

一、事件發生前之防護措施規劃 本校應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資安事件之發生。

二、損害控制機制

(一)負責應變之權責人員或緊急處理小組，應完成以下應變事務之辦理，並留存應變之紀錄

1. 資安事件之衝擊及損害控制作業。
2. 資安事件所造成損害之復原作業。
3. 重大(第「三」級、第「四」級)資安事件相關鑑識及其他調查作業。
4. 重大(第「三」級、第「四」級)資安事件之調查與處理及改善報告之方 式。
5. 重大(第「三」級、第「四」級)資安事件後續發展及與其他事件關聯性 之監控。
6. 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷 時，應依據本機關事前擬定之緊急計畫，進行應變措施以恢復業務持續 運作之狀態。
7. 其他資通安全事件應變之相關事項。

(二)對於第一級、第二級資通安全事件，本校應於知悉事件後七十二小時內完成前項事務之辦理，並應留存紀錄；於第三級、第四級資通安全事件，本校應於知悉事件後三十六小時內完成損害控制或復原作業，並執行上述事 項，及留存相關紀錄。

(三)本校完成資安事件處理後，須至教育機構資安通報平台填報資安事件處理 辦法及完成時間。

(四)本校於知悉受託廠商發生與受託業務相關之資通安全事件時，應於知悉委外廠商發生第一、二級資通安全事件後七十二小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第三、四級資通安全事件後三十六小時內，確認委外廠商完成損害控制或復原事項之辦理。

柒、重大(第「三」級、第「四」級)資安事件後之復原、鑑識、調查 及改善機制

一、本校若發生重大(第「三」級、第「四」級)資通安全事件時，於完成資通安全事件之通報及應變程序後，應針對事件所造成之衝擊、損害及影響進行調查及改善，並應於事件發生後一個月內完成資通安全事件調查、處理及改善報告。

二、重大(第「三」級、第「四」級)資通安全事件調查、處理

及改善報告應包括以下項目：

(一)事件發生、完成損害控制或復原作業之時間。

(二)事件影響之範圍及損害評估。

(三)損害控制及復原作業之歷程。

(四)事件調查及處理作業之歷程。

(五)為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

(六)前款措施之預定完成時程及成效追蹤機制。

三、本校應向所隸屬之上級機關及教育部提出前項之報告，以供監督與檢討。

捌、紀錄留存及管理程序之調整

一、本校應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「教育機構資安通報平台」上填報完整之紀錄，該平台事件通報應變紀錄由通報應變小組於年度彙整後，提交至本部資訊及科技教育司覆核備查。

二、本校於完成資通安全事件之通報及應變程序後，應依據實際處理之情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

玖、演練作業

一、本校應配合教育部依資通安全事件通報應變辦法之規定所辦理之社交工程 演練、資通安全事件通報及應變演練。

二、本校應配合行政院依資通安全事件通報應變辦法之規定所辦理之下列資通 安全演練作業：

(一)社交工程。

(二)資安事件通報及應變

(三)網路攻防

(四)情境演練

(五)其他資安演練

附件十三：委外廠商執行人員保密切結書

國立大湖高級農工職業學校委外廠商執行人員保密切結書

立切結書人----------（簽署人姓名）等，受----------（廠商名稱）委派至----------（學校名稱）（以下稱本校）處理業務，謹聲明恪遵本校下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經學校權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

一、未經申請核准，不得私自將本校之資訊設備、媒體檔案及公務文書攜出。

二、未經本校業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接本校網路。若經申請獲准連接學校網路，嚴禁使用數 據機或無線傳輸等網路設備連接外部網路。

三、經核准攜入之資訊設備欲連接網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。

四、廠商駐點服務及專責維護人員原則應使用本校配發之個人電腦與週邊設備，並僅開放使用本校內部網路。若因業務需要使用本校電子郵件、目錄服務，應經本校業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經本校業務相關人員之確認並代為申請核准。

五、本校得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。

六、本保密切結書不因立切結書人離職而失效。

七、立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切 損害，立切結書人所屬公司或廠商應負連帶賠償責任。

立切結書人：　　（姓名及簽章 ）

身分證字號：

聯絡電話：

戶籍地址：

立切結書人所屬廠商：　　（廠商名稱及蓋章）

廠商負責人：　　（姓名及簽章）

廠商聯絡電話：

地址：

填表說明：

一、廠商駐點服務人員、專責維護人員，或逗留時間超過三天以上之突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連 結本校網路者為限）及經常到本校洽公之業務人員皆須簽署本切結 書。

二、廠商駐點服務人員、專責維護人員及經常到本校洽公之業務人員每年簽署本切結書乙次。

中華民國　　年　　月　　日

附件十四：委外廠商執行人員保密同意書

國立大湖高級農工職業學校委外廠商執行人員保密切結書

立切結書人＿＿＿＿＿＿＿＿（簽署人姓名）等，受＿＿＿＿＿＿（廠商名稱）委派至＿＿＿＿＿＿（學校名稱）（以下稱本校）處理業務，謹聲明恪遵本校下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經學校權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

一、 未經申請核准，不得私自將本校之資訊設備、媒體檔案及公務文書攜出。

二、未經本校業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接本校網路。若經申請獲准連接學校網路，嚴禁使用數 據機或無線傳輸等網路設備連接外部網路。

三、經核准攜入之資訊設備欲連接網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發 給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。

四、廠商駐點服務及專責維護人員原則應使用本校配發之個人電腦與週邊設備，並僅開放使用本校內部網路。若因業務需要使用本校電子郵件、目錄服務，應經本校業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經本校業務相關人員之確認並代為申請核准。

五、本校得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。

六、本保密切結書不因立切結書人離職而失效。

七、立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切 損害，立切結書人所屬公司或廠商應負連帶賠償責任。

立切結書人：　　（姓名及簽章 ）

身分證字號：

聯絡電話：

戶籍地址：

立切結書人所屬廠商：　　（廠商名稱及蓋章）

廠商負責人：　　（姓名及簽章）

廠商聯絡電話：

地址：

填表說明：

一、廠商駐點服務人員、專責維護人員，或逗留時間超過三天以上之 突發性維護增援、臨時性系統測試或教育訓練人員（以授課時需連 結本校網路者為限）及經常到本校洽公之業務人員皆須簽署本切結 書。

二、廠商駐點服務人員、專責維護人員及經常到本校洽公之業務人員每年簽署本切結書乙次。

中　華　民　國　　年　　月　　日

附件十五：委外廠商查核項目表

國立大湖高級農工職業學校委外廠商查核項目表

編號：　　填表日期：　　年　　月　　日

查核人員：

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
1.資通安全政策之推動及目標訂定	1.1是否定義符合組織需要之資通安全政策及目標？	□	□	□	已訂定資通安全政策及目標。
	1.2組織是否訂定資通安全政策及目標？	□	□	□	政策及目標符合機關之需求。
	1.3組織之資通安全政策文件是否由管理階層核准並正式發布且轉知所有同仁？	□	□	□	依規定按時進行教育訓練之宣達。
	1.4組織是否對資通安全政策、目標之適切性及有效性，定期作必要之審查及調整？	□	□	□	定期進行政策及目標之檢視、調整。
	1.5是否隨時公告資通安全相關訊息？	□	□	□	將資安訊息公告於布告欄。
2.設置資通安全推動組織	2.1是否指定適當權責之高階主管負責資通安全管理之協調、推動及督導等事項？	□	□	□	指派副首長擔任資安長。
	2.2是否指定專人或專責單位，負責辦理資通安全政策、計畫、措施之研議，資料、資通系統之使用管理及保護，資安稽核等資安工作事項？	□	□	□	有設置內部資通安全推動小組，並制訂相關之權責分工。
	2.3是否訂定組織之資通安全責任分工？	□	□	□	機關內部訂有資安責任分工組織。
3.配置適當之資通安全專業人員及適當之資源	3.1是否訂定人員之安全評估措施？	□	□	□	有訂定人員錄用之安全評估措施
	3.2是否符合組織之需求配置專業資安人力？	□	□	□	機關依規定配置資安人員2人。
	3.3是否具備相關專業資安證照或認證？	□	□	□	專業人員具備 ISO27001之證照
	3.4是否配置適當之資源？	□	□	□	機關並未投入足夠資安資源。
4.資訊及資通系統之盤	4.1是否建立資訊及資通系統資產目錄，並隨時維護更新？	□	□	□	依規定建置資產目錄，並定時盤點。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
點及風險評估	4.2各項資產是否有明確之管理者及使用者？	□	□	□	資產依規定指定管理者及使用者。
	4.3是否定有資訊、資通系統分級與處理之相關規範？	□	□	□	資訊訂有分級處理之作業規範。
	4.4是否進行資訊、資通系統之風險評估，並採取相應之控制措施？	□	□	□	已進行風險評估及擬定相應之控制措施。
5.資通安全管理措施之實施情況	5.1人員進入重要實體區域是否訂有安全控制措施？	□	□	□	機房訂有門禁管制措施。
	5.2重要實體區域的進出權利是否定期審查並更新？	□	□	□	離職人員之權限未刪除。
	5.3電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？	□	□	□	對於進出人員並未監督其活動。
	5.4電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？	□	□	□	按時檢測機房物理面之情況。
	5.5各項安全設備是否定期檢查？同仁有否施予適當的安全設備使用訓練？	□	□	□	依規定定期檢查並按時提供同仁安全設備之使用運練。
	5.6第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？	□	□	□	並未陪同或監視第三方支援人員。
	5.7重要資訊處理設施是否有特別保護機制？	□	□	□	對於核心系統主機並未設置特別保護機制。
	5.8重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？	□	□	□	定期檢查物理面之風險。
	5.9電源之供應及備援電源是否作安全上考量？	□	□	□	有設置備用電源。
	5.10通訊線路及電纜線是否作安全保護措施？	□	□	□	電纜線老舊，並未設有安全保護措施。
	5.11設備是否定期維護，以確保其可用性及完整性？	□	□	□	設備按期維護。
	5.12設備送場外維修，對於儲存資訊是否訂有安全保護措施？	□	□	□	訂有相關之保護措施。
	5.13可攜式的電腦設備是否訂有嚴謹的保護措施(如設通行碼、檔案加密、專人看管)?	□	□	□	攜帶式設備訂有保護措施。
	5.14設備報廢前是否先將機密性、敏感性資料及版權軟體移除或覆寫？	□	□	□	設備報廢前均有進行資料清除程序。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.15公文及儲存媒體在不使用或不在班時是否妥為存放？機密性、敏感性資訊是否妥為收存？	□	□	□	人員下班後並未將機敏性公文妥善存放。
	5.16系統開發測試及正式作業是否區隔在不同之作業環境？	□	□	□	系統開發測試與正式作業區隔。
	5.17是否全面使用防毒軟體並即時更新病毒碼？	□	□	□	按時更新病毒碼。
	5.18是否定期對電腦系統及資料儲存媒體進行病毒掃瞄？	□	□	□	定期進行相關系統之病毒掃瞄。
	5.19是否定期執行各項系統漏洞修補程式？	□	□	□	定期進行漏洞修補。
	5.20是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)?	□	□	□	系統設有檢查之機制。
	5.21重要的資料及軟體是否定期作備份處理？	□	□	□	有定期做備份處理。
	5.22備份資料是否定期回復測試，以確保備份資料之有效性？	□	□	□	備份資料均有測試。
	5.23對於敏感性、機密性資訊之傳送是否採取資料加密等保護措施？	□	□	□	均有設加密之保護措施。
	5.24是否訂定可攜式媒體(磁帶、磁片、光碟片、隨身碟及報表等)管理程序？	□	□	□	訂有可攜式媒體之管理程序。
	5.25是否訂定使用者存取權限註冊及註銷之作業程序？	□	□	□	訂有使用者存取權限註冊及註銷之作業程序。
	5.26使用者存取權限是否定期檢查(建議每六個月一次)或在權限變更後立即複檢？	□	□	□	未定期檢視使用者存取權限。
	5.27通行碼長度是否超過6個字元(建議以8位或以上為宜)?	□	□	□	通行碼符合規定。
	5.28通行碼是否規定需有大小寫字母、數字及符號組成？	□	□	□	通行碼符合規定。
	5.29是否依網路型態(Internet、Intranet、Extranet)訂定適當的存取權限管理方式？	□	□	□	依規定訂定適當之存取權限。
	5.30對於重要特定網路服務，是否作必要之控制措施，如身份鑑別、資料加密或網路連線控制？	□	□	□	對於特定網路有訂定相關之控制措施。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	5.31是否訂定行動式電腦設備之管理政策(如實體保護、存取控制、使用之密碼技術、備份及病毒防治要求)?	□	□	□	有針對行動式電腦訂定管理政策。
	5.32重要系統是否使用憑證作為身份認證?	□	□	□	針對重要系統設有身份認證。
	5.33系統變更後其相關控管措施與程序是否檢查仍然有效?	□	□	□	系統更新後相關措施仍有效。
	5.34是否可及時取得系統弱點的資訊並作風險評估及採取必要措施?	□	□	□	可即時取得系統弱點並採取應變措施。
6.訂定資通安全事件通報及應變之程序及機制	6.1是否建立資通安全事件發生之通報應變程序?	□	□	□	有訂定通報應變程序。
	6.2機關同仁及外部使用者是否知悉資通安全事件通報應變程序並依規定辦理?	□	□	□	同仁及委外廠商均知悉通報應變程序，並定期宣導。
	6.3是否留有資通安全事件處理之記錄文件，記錄中並有改善措施?	□	□	□	有留存相關紀錄。
7.定期辦理資通安全認知宣導及教育訓練	7.1是否定期辦理資通安全認知宣導?	□	□	□	有定期辦理宣導。
	7.2是否對同仁進行資安評量?	□	□	□	按期進行資安評量。
	7.3同仁是否依層級定期舉辦資通安全教育訓練?	□	□	□	有定期辦理教育訓練。
	7.4同仁是否瞭解單位之資通安全政策、目標及應負之責任?	□	□	□	同仁均瞭解單位之資通安全政策及目標。
8.資通安全維護計畫實施情形之精進改善機制	8.1是否設有稽核機制?	□	□	□	訂有稽核機制。
	8.2是否定有年度稽核計畫?	□	□	□	有訂定年度稽核計畫。
	8.3是否定期執行稽核?	□	□	□	有按期執行稽核。
	8.4是否改正稽核之缺失?	□	□	□	訂有稽核後之缺失改正措施。
9.資通安全維護計畫及實施情形之績效管考機制	9.1是否訂定安全維護計畫持續改善機制?	□	□	□	有訂定持續改善措施。
	9.2是否追蹤過去缺失之改善情形?	□	□	□	有追蹤缺失改善之情形。
	9.3是否定期召開持續改善之管理審查會議?	□	□	□	定期召開管理審查會議。

資安官：　　資安長：

註：陳核層級請機關依需求調整

附件十六：內部稽核計畫

國立大湖高級農工職業學校內部稽核計畫

1. 主旨

為落實國立大湖高級農工職業學校學校（以下簡稱「本校」）資通安全計畫執行，以反映政策、法令、技術及現行業務之最新狀況，確保資訊安全政策與資訊安全實務作業之有效性及可行性。

2. 目標

符合本校所訂定之資訊安全政策及各項安全管理規定。

3. 稽核範圍

本校資訊機房維運服務營運相關資訊業務。

4. 稽核項目

4.1 資通安全維護計畫之確認

4.2 核心業務及其重要性

4.3 資通安全政策及目標

4.4 設置資通安全推動組織

4.5 人力及經費之配置

4.6 資訊及資通系統之盤點及核心資通系統、相關資產之標示

4.7 資通安全風險評估

4.8 資通安全防護及控制措施

4.9 資通安全事件通報、應變及演練相關機制

4.10 資通安全情資之評估及因應機制

4.11 資通系統或服務委外辦理之管理

4.12 資通安全教育訓練

4.13 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

4.14 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

5. 資訊安全稽核小組成員

組長：ＸＸＸ

組員：ＸＸＸ、ＸＸＸ

6. 稽核時程

日 期	時 間	項 目	稽核人員	地點
	10:00-10:20	啟始會議		
	10:20-10:30	高階主管訪談		
	10:30-12:00	一、核心業務及其重要性 二、資通安全政策及目標 三、設置資通安全推動組織 四、人力及經費之配置 五、資訊及資通系統之盤點及核心資通系統、相關資產之標示 六、資通安全風險評估 七、資通安全防護及控制措施	ＸＸＸ ＸＸＸ ＸＸＸ	
	12:00-13:00			
	13:00-15:30	七、資通安全防護及控制措施 八、資通安全事件通報、應變及演練相關機制 九、資通安全情資之評估及因應機制 十、資通系統或服務委外辦理之管理 十一、資通安全教育訓練 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 十三、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	ＸＸＸ ＸＸＸ ＸＸＸ	

	15:30-16:00	稽核結果彙整		
	16:00-16:30	結束會議		

7. 稽核程序

7.1 執行日期：XX 年 XX 月 XX 日。

7.2 啟始會議

- 資訊安全稽核小組成員介紹
- 確認稽核目的及範圍
- 稽核程序報告
- 稽核方法說明

7.3 高階主管訪談

- 透過與高階主管訪談方式,瞭解本校推動資訊安全管理制度之決心、資源分配以及所面臨之問題

7.4 實地稽核

- 實地驗證資訊安全管理系統執行之有效性
- 以面談、觀察、抽樣檢查方式進行

7.5 稽核結果彙整

- 資訊安全稽核小組根據稽核事實討論所發現之缺失事項
- 彙整稽核結果
- 總結報告

7.6 結束會議

- 資訊安全稽核小組報告發現之缺失事項
- 改善建議
- 問題澄清與討論
- 稽核總結

8. 附件

8.1 資訊安全管理制度內部稽核表

8.2 矯正與預防處理單

附件十七：稽核項目紀錄表

國立大湖高級農工職業學校稽核項目紀錄表

稽核日期：　　年　　月　　日

稽核範圍：

受稽核單位	稽核項目	稽核結果	備註
		□符合 □不符合 □不適用	
		□符合 □不符合 □不適用	
		□符合 □不符合 □不適用	
		□符合 □不符合 □不適用	
		□符合 □不符合 □不適用	
		□符合 □不符合 □不適用	
附註			
受稽核人員：			受稽核單位主管：

附件十八：內部稽核報告

國立大湖高級農工職業學校資訊安全管理制度內部稽核報告

1 稽核目的

為落實及評估國立大湖高級農工職業學校職業學校（以下簡稱本校)執行資訊安全管理制度之成效，以確保資訊安全政策、法令、技術及現行作業之有效性及可行性。

2 稽核範圍

本校資訊機房維運及核心業務系統。

3 稽核項目

3.1 資通安全維護計畫之確認
3.2 核心業務及其重要性
3.3 資通安全政策及目標
3.4 設置資通安全推動組織
3.5 人力及經費之配置
3.6 資訊及資通系統之盤點及核心資通系統、相關資產之標示
3.7 資通安全風險評估
3.8 資通安全防護及控制措施
3.9 資通安全事件通報、應變及演練相關機制
3.10資通安全情資之評估及因應機制
3.11資通系統或服務委外辦理之管理
3.12資通安全教育訓練
3.13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
3.14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適用性聲明書之確認

4 資訊安全稽核小組

組長：

組員：

5 稽核日期

XX 年 XX 月 XX 日

6 稽核期間

自 XX 年 XX 月 XX 日至 XX 年 XX 月 XX 日

7　稽核結果及其他建議事項

項次	稽核項目	稽核發現	建議事項
1			
2			
3			
其他建議事項			

8　缺失矯正與預防處理

受稽部門於接獲稽核報告後，應依據「矯正預防措施管理」之規定，最晚於十個工作天內將該單位之缺失分析原因及擬採行之矯正與預防措施填列於「矯正與預防處理單」內，且經主管核定後回覆資訊安全稽核小組。

9　附件

資訊安全管理制度內部稽核表

資訊安全稽核小組		受稽單位		資訊安全官	
日期	/　/	日期	/　/	日期	/　/

附件十九：矯正與預防處理單

國立大湖高級農工職業學校矯正與預防處理單

<table>
<tr><td>提出單位</td><td></td><td>提出人員</td><td></td><td>提出日期</td><td></td></tr>
<tr><td>處理單位</td><td></td><td>處理人員</td><td></td><td></td><td></td></tr>
<tr><td>事件分類
（外部稽核）</td><td colspan="2">□主要不符合事項
□觀察事項
□次要不符合事項
□建議事項</td><td>事件來源</td><td colspan="2">□內部稽核
□外部稽核
□資訊安全事件
□自行提出
□其他＿＿＿＿＿＿</td></tr>
<tr><td>問題或不符合事項說明</td><td colspan="5"></td></tr>
<tr><td>原因分析</td><td colspan="5"></td></tr>
<tr><td rowspan="5">矯正與
預防措施評估</td><td colspan="5">暫時性對策：（控制不符合事項的擴大或消除單一事件的影響）</td></tr>
<tr><td>預訂完成日期</td><td></td><td>追 蹤 人</td><td colspan="2"></td></tr>
<tr><td>追 蹤 日 期</td><td></td><td>確認結果</td><td colspan="2"></td></tr>
<tr><td colspan="5">長期性對策：（消除不符合事項或潛在風險的根本原因，防止類似事件發生）</td></tr>
<tr><td>預訂完成日期</td><td></td><td>追 蹤 人</td><td colspan="2"></td></tr>
<tr><td>追 蹤 日 期</td><td></td><td>確認結果</td><td colspan="2"></td></tr>
</table>