

國立岡山高級農工職業學校

資通安全維護計畫

目 錄

壹、 依據及目的	3
貳、 適用範圍	3
參、 核心業務及重要性	3
一、 核心業務及重要性：	3
二、 非核心業務及說明：	4
肆、 資通安全政策及目標	5
伍、 資通安全推動組織	5
陸、 專職(責)人力及經費配置	5
一、 專職(責)人力及資源之配置	5
二、 經費之配置	6
柒、 資訊及資通系統之盤點	6
一、 資訊及資通系統盤點	6
二、 機關資通安全責任等級分級	6
捌、 資通安全風險評估	6
一、 資通安全風險評估	6
二、 核心資通系統及資料復原點目標 (RPO)	6
玖、 資通安全防護及控制措施	7
一、 資訊及資通系統之管理	7
二、 存取控制與加密機制管理	8
三、 作業與通訊安全管理	8
四、 系統獲取、開發及維護	8
五、 業務持續運作演練	9
六、 執行資通安全健診	9
七、 資通安全防護設備	9
八、 備份資料回復測試	9
壹拾、 資通安全事件通報、應變及演練相關機制	9
壹拾壹、 資通安全情資之評估及因應	9
一、 資通安全情資之分類評估	10
(一) 資通安全相關之訊息情資	10
(二) 入侵攻擊情資	10
(三) 機敏性之情資	10
(四) 涉及核心業務、核心資通系統之情資	10
二、 資通安全情資之因應措施	10
(一) 資通安全相關之訊息情資	10

(二) 入侵攻擊情資	11
(三) 機敏性之情資	11
(四) 涉及核心業務、核心資通系統之情資	11
壹拾貳、資通系統或服務委外辦理之管理	11
一、選任受託者應注意事項	11
二、監督受託者資通安全維護情形應注意事項	12
壹拾參、資通安全教育訓練	12
一、資通安全教育訓練要求	12
二、資通安全教育訓練辦理方式	12
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	13
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	13
一、資通安全維護計畫之實施	13
二、資通安全維護計畫實施情形之稽核機制	13
(一) 稽核機制之實施	13
(二) 稽核改善報告	14
三、資通安全維護計畫之持續精進及績效管理	14
壹拾陸、資通安全維護計畫實施情形之提出	15
壹拾柒、相關法規、程序及表單	15
一、相關法規及參考文件	15
二、附件資料表單	16
三、相關網站	17

壹、依據及目的

依據資通安全管理法第13條及施行細則第9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岡山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	維護廠商	業務失效影響說明
校務行政與學生資料管理	校務行政整合系統(向上集中)	為本校依組織法執掌，足認為重要者	亞昕資訊股份有限公司	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
學校首頁	校園網頁系統(向上集中)	為本校依組織法執掌，足認為重要者	成功大學向上集中辦公室	影響校務運作及機關行政效率
網域名稱轉址	DNS 網域名稱系統(向上集中)	為本校依組織法執掌，足認為重要者	成功大學向上集中辦公室	影響網路網域名稱解譯

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10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。

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	維護廠商	最大可容忍中斷時間(MTPD)	資通系統防護需求等級
校務基金系統	影響機關行政效率	艾富資訊	48小時	普
公文交換	電子公文無法及時送達機關，影響機關行政效率	帝緯系統整合股份有限公司	48小時	普
財管系統	影響機關行政效率	奇勁科技	48小時	普
圖書查詢管理系統	影響師生借還書及圖書館館藏查詢功能，但可手動借閱	寶慶文化科技股份有限公司	48小時	普
人事差勤系統	降低行政效能。	宏權科技有限公司	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. 資通系統防護需求等級：依據「資通安全責任等級分級辦法」之附件九資通系統防護需求分級原則定義，以與該系統相關之機密性、完整性、可用性、法律遵循性構面中，任一構面之防護需

求等級之最高者定之。

肆、資通安全政策及目標

依本校「資通安全政策」如附件1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2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3。

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3，並適時更新，資安業務內容如下：
 - (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5施行。

二、機關資通安全責任等級分級

行政院114年11月3日院授數資安字第11450003261號函，依據資通安全責任等級分級辦法第6條，茲考量學校核心資通系統向上集中，依同辦法第10條第4款調為D級。

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6施行。

二、核心資通系統及資料復原點目標（RPO）

依據「資通安全責任等級分級辦法」附表十資通系統防護基準之控制措施，本校依教育部五大核心資通系統向上集中，訂定核心資通系統「最大可容忍中斷時間」（MTPD）、資料復原點目標（RPO）及系

統中斷時取代提供服務方式

核心資通系統	資通系統防護需求等級	最大可容忍中斷時間(小時)	資料復原點目標(小時)	取代提供服務方式
校務行政整合系統(向上集中)	無(已向上集中)	24	24	以靜態網頁方式
校園網頁系統(向上集中)	無(已向上集中)	24	24	以靜態網頁方式
DNS 網域名稱系統(向上集中)	無(已向上集中)	24	24	以靜態網頁方式

各欄位定義：

1. 資通系統防護需求等級：依據「資通安全責任等級分級辦法」之附件九資通系統防護需求分級原則定義，以與該系統相關之機密性、完整性、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。
2. 資料復原點目標 (Recovery Point Objective, RPO)：資通安全事故發生後，業務流程中所有相關之利害關係者，可接受資料滅失或遺漏之資料時間差，以小時計，如學校官網為24小時。
3. 最大可容忍中斷期間 (Maximum Tolerable Period of Disruption, MTPD)：資通安全事故發生後，造成關鍵業務流程中斷，關鍵業務流程中所有相關聯之利害關係者所能容忍業務流程中斷之最大可接受時間，以小時計，如學校官網24小時。
4. 取代提供服務方式：如系統中斷於最大可容忍中斷時間內，其他方式取代提供服務，如學校官網可使用電話、電子郵件方式公告。

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7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8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9、

「通信與作業管理」規定如附件10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10中資通系統防護基準，並注意下列事項：
 - (1) 本校資訊及資通系統開發過程依據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。
 - (5) 針對非向上集中且有對外營運服務資通系統之系統開發、增修功能，依據「資通安全責任等級分級辦法」附表10資通系統防護基準之控制措施—系統發展生命週期測試階段，須執行「弱點掃描」，本校使用國立成功大學教育單位弱點檢測平台、國立陽明交通大學教育體系弱點掃描服務平台或向教育部國民及學前教育署資訊中心申請網頁弱掃服務。
2. 餘依本校「系統開發與維護」規定如附件11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，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、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。

八、備份資料回復測試

本校針對非核心且對外服務之資通系統，每年辦理一次備份資料回復測試紀錄（附件12）。

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13「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. 訂定委外服務案需求規格書或合約，應載明資安條款或附約及相關表件，例如委外廠商資安管理作業自評表(附件14)、委外廠商保密同意書(附件15)、委外廠商執行人員保密切結書(附件16)、委外廠商查核暨自我檢核項目表(附件17)。
2. 委外服務案招標、投標時，請廠商提供「委外廠商資安管理作業自評表」(附件14)。
3. 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。
4. 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。
5. 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，並要求委外廠商簽署「委外廠商保密同意書」(附件15)及業務執行人員簽署「委外廠商執行人員保密切結書」(附件16)
5. 本校應於簽約時、維運期間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「委外廠商查核暨自我檢核項目表」(附件17)，進行稽核以確認受託業務之執行情形。
6. 契約終止、解除、屆期時，請受託者提供「委外廠商查核暨自我檢核項目表」(附件17)，檢視是否符合資安條款或附約各項作業如完成稽核結果矯正、完成處理資安事件等；倘有違約事項，應依罰則處置。

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。
3. 本校資通安全專職人員以外之資訊人員，指其他實際從事資通安全業務或資訊業務之人員，每人每二年接受3小時以上資通安全專業課程訓練或資通安全職能訓練且每年完成3小時以上資通安全通識教育訓練。
4. 詳資通安全教育訓練統計表(附件18)。

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、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、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. 本校每年配合教育部國民及學前教育署實地稽核訪視或書面審查，且依據實地稽核訪視報告或書面審查報告，後續提出具體改善報告呈報資通安全長，並於資通安全管理審查會議追蹤辦理情形。
2. 本校發生資安事件時，資通安全稽核小組應依據「內部稽核計

畫」(附件19)，對事件相關單位進行實地稽核，「稽核項目紀錄表」(附件20)。

3. 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(附件20)，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」(附件21)，並提供給受稽單位填寫辦理情形。
4. 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。
5. 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。

(9) 委外廠商查核暨自我檢核項目表、委外廠商資安管理作業自評表及委外服務案需求規格書之資安條款、資安能力要求項目、之適切性。

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 22，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14條規定，應每年向上級或監督機關，提出資通安全維護計畫實施情形；及依據資通安全維護計畫實施情形稽核辦法第3條規定，應至主管機關指定之系統平臺，提出資通安全維護計畫實施情形，以符合法遵要求。

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. 資通安全事件通報應變及演練辦法

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. 行動裝置資安防護資安參考指引
12. 安全軟體發展流程指引
13. 安全軟體設計參考指引
14. 安全軟體測試參考指引
15. 政府資訊服務採購作業指引

二、附件資料表單

- 附件1：資訊安全政策
- 附件2：資訊安全組織
- 附件3：資訊安全組織成員表
- 附件4：經費配置表
- 附件5：資通資產管理
- 附件6：風險評鑑與管理
- 附件7：資通資產異動作業
- 附件8：存取控制管理
- 附件9：實體安全管理
- 附件10：通信與作業管理
- 附件11：系統開發與維護
- 附件12：備份資料回復測試紀錄
- 附件13：資通安全事件通報應變程序
- 附件14：委外廠商資安管理作業自評表
- 附件15：委外廠商保密同意書
- 附件16：委外廠商執行人員保密切結書
- 附件17：委外廠商查核暨自我檢核項目表
- 附件18：資通安全教育訓練統計表
- 附件19：內部稽核計畫
- 附件20：稽核項目紀錄表

附件21：內部稽核報告

附件22：矯正與預防處理單

三、相關網站

1. 國立成功大學教育單位弱點檢測平台：提供免費網頁及主機弱掃服務（網址：<https://evs.ncku.edu.tw>）。
2. 國立陽明交通大學教育體系弱點掃描服務平台：提供免費網頁弱掃服務（網址：<https://va.nycu.edu.tw>）。
3. 數位發展部資通安全署資通安全作業管考系統（網址：<https://spm.nat.gov.tw/Account/Login>）。
4. 新增資安人員身分驗證系統（網址：<https://www.ncert.nat.gov.tw/iAuth2/getOidInfo.jsp>）。

承辦人/專責人員

資訊媒體組 長 陳界任

單位主管

圖書館 主任 洪佳玲

校長

國立岡山農工學校 校長 黃銘福
115-0510

