國立斗六高級中學

資通安全維護計畫

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斗六高級中學全機關（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
校務學生資料管理	校務行政系統（預計111年完成向上集中）	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	24	中
學校官網	網頁伺服器(110年7月已完成向上集中)	為本校依組織法執掌，足認為重要者	影響校務運作	24	中

DNS 服務	DNS 伺服器（已於109年完成向上集中）	為本校依組織法執掌，足認為重要者	影響校務運作	24	中
學習歷程檔案	學習歷程檔案伺服器（預計111年完成向上集中）	為本校依組織法執掌，足認為重要者	影響校務運作	24	中
電子郵件系統	電子郵件系統伺服器（完成向上集中，使用教育部校園雲端郵件）	為本校依組織法執掌，足認為重要者	影響校務運作	24	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
公文交換	電子公文無法即時送達機關，影響機關行政效	48	普

	率		
校務基金系統	無法完成會計相關作業，影響機關行政效率	48	普
圖書館管理系統	無法進行圖書借閱，歸還等作業	48	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110年11月19日院臺護字第1100036460號函，依據資通安全責任等級分級辦法第6條辦理，因本校尚有核心系統未完成向上集中規劃，依資定核定本校資案等級為C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110年11月19日院臺護字第1100036460號函，依據資通安全責任等級分級辦法第6條辦理，因本校尚有核心系統未完成向上集中規劃，依資定核定本校資案等級為C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	網站主機計1台 ASUS TS300 Win Server 2012R2 SQL SERVER 2014 防火牆 Fortinet 100D 核心交換器 EXTREME X460G2-24t-G4 中繼交換器 HP HPE1920S	學籍管理、學生修課、出缺席、輔導狀況資料	24
網頁伺服器	已於2021/07/16完成上集中至成大	學校資訊呈現及公告	24
學習歷程檔案	同校務行政系統	學生學習歷程檔案收集	24

DNS 伺服器檔案	109年已完成向上集中	DNS 查詢服務	24
郵件伺服器	完成向上集中，採用教育部校園雲端電子郵件系統	郵件傳遞	24

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、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. 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」如附件十八，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
附件二：資訊安全組織
附件三：資訊安全組織成員表
附件四：保密切結書
附件五：資訊資產管理
附件六：風險評鑑與管理
附件七：資訊資產異動作業
附件八：存取控制管理
附件九：實體安全管理
附件十：通信與作業管理
附件十一：系統開發與維護
附件十二：資通安全事件通報及應變程序
附件十三：委外廠商執行人員保密切結書
附件十四：委外廠商查核項目表
附件十五：內部稽核計畫
附件十六：稽核項目紀錄表
附件十七：內部稽核報告
附件十八：矯正與預防處理單

承辦人/專責人員　　單位主管　　校長

國立斗六高級中學

資訊安全政策

修 訂 紀 錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目　錄

1 目的

為確保國立斗六高級中學（以下簡稱本校）所屬之資訊資產的機密性、完整性與可用性，導入資訊安全管理系統，強化本校資訊安全管理，保護資訊資產免於遭受內、外部蓄意或意外之威脅，維護資料、系統、設備及網路之安全，提供可靠之資訊服務，訂定本政策。

2 依據

1.1 個人資料保護法（及施行細則）

1.2 行政院及所屬各機關資訊安全管理要點

1.3 教育體系資通安全暨個人資料管理規範

1.4 資通安全法(及施行細則、相關辦法)

3 適用範圍

3.1 本政策適用範圍為本校之全體人員、委外服務廠商與訪客等。

3.2 資訊安全管理範疇涵蓋 14 項領域，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本校造成各種可能之風險及危害，各領域分述如下：

3.2.1 資訊安全政策訂定與評估。

3.2.2 資訊安全組織。

3.2.3 人力資源安全。

3.2.4 資產管理。

3.2.5 存取控制。

3.2.6 密碼學(加密控制)。

3.2.7 實體及環境安全。

3.2.8 運作安全。

3.2.9 通訊安全。

3.2.10 系統獲取、開發及維護。

3.2.11 供應者關係。

3.2.12 資訊安全事故管理。

3.2.13 營運持續管理之資訊安全層面。

3.2.14 遵循性。

4 目標

維護本校資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由本校全體同仁共同努力來達成下列目標：

4.1 保護本校業務服務之安全，確保資訊需經授權，人員才可存取，以確保其機密性。核心業務系統遭非法存取之事件，每年發生次數不得超過 1 次。

4.2 保護本校業務服務之安全，避免未經授權的修改，以確保其正確性與完整性。核心業務系統資料異動經查核異常案件應為 1 件。

4.3 建立本校業務永續運作計畫，以確保本校業務服務之持續運作。提供核心業務系統之平台因資安事件導致服務停頓，每次不得超過 72 小時，每年中斷服務率不得超過 2% 以上（計算方式：全年中斷服務之總工作小時／一年總工作小時）。

4.4 每年依本校全體人員之工作職務、責任，適當授與資訊安全相關訓練。

4.5 確保本校各項業務服務之執行須符合相關法令或法規之要求。

5 責任

5.1 本校應成立「資訊安全暨個人資料保護推動委員會」統籌資訊安全事項推動。

5.2 管理階層應積極參與及支持資訊安全管理制度，並授權資訊安全組織透過適當的標準和程序以實施本政策。

5.3 本校全體人員、委外服務廠商與訪客等皆應遵守相關安全管理程序以維護本政策。

5.4 本校全體人員及委外服務廠商均有責任透過適當通報機制，通報資訊安全事件或弱點。

5.5 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本校之相關規定進行議處。

6 審查

本政策應每年至少審查乙次，以反映政府法令、技術及業務等最新發展現況，並確保本校業務永續運作之能力。

7 實施

本政策經「資訊安全委員會」審核、資安長核定後實施，修正時亦同。

國立斗六高級中學

資訊安全組織

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目錄

1　目的

確保國立斗六高級中學（以下簡稱「本校」）資訊安全管理制度之資訊安全責任，落實資訊安全政策之推行，並符合下列「教育體系資通安全管理規範」之控制目標：

1.1　為確保本校內部資訊安全管理事項之推動，應建立適當管理架構，以審核資訊安全政策、分配安全責任，並協調本校各項資訊安全措施之實施。

1.2　建立與外部資訊安全專家之聯繫管道，以利於安全事件處理及專家意見徵詢。

2　適用範圍

本校承辦之資訊安全相關業務作業流程。

3　權責

無。

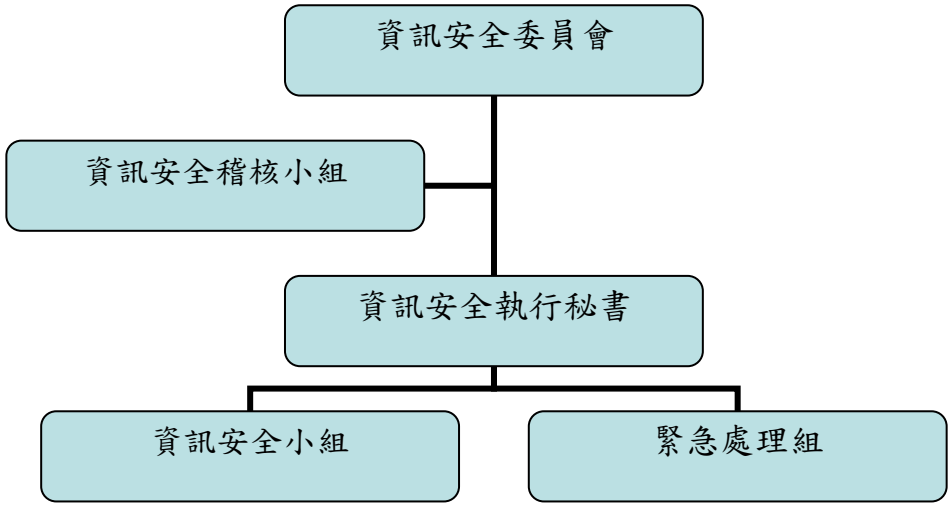
4　名詞定義

無。

5　作業說明

5.1　資訊安全組織架構與工作執掌

5.1.1資訊安全組織架構如下圖所示，資訊安全組織成員應填寫於「資訊安全組織成員表」，若遇人員異動應加以更新。



5.1.2資訊安全員會：由本校校長擔任召集人，各單位一級主管及各科主任為委員會委員，負責資訊安全管理制度相關事項之決議。

5.1.2.1 每年定期或視需要召開會議，審查資訊安全管理相關事宜。

5.1.2.2 視需要召開跨部門之資源協調會議，負責協調資訊安全管理制度執行所需之相關資源分配。

5.1.3資訊安全執行秘書：由資訊安全委員會召集人指派專人擔任。

5.1.3.1 負責協調資訊安全小組與緊急處理組執行資訊安全相關作業。

5.1.3.2 負責對資訊安全狀況進行預警、監控，並對資訊安全狀況與事件進行處置。

5.1.3.3 對於資訊安全管理之改善提出建議，以及協助執行資訊安全之自我檢核。

5.1.3.4 對於存取控制管理定期進行事件紀錄檢核，以及管理程序檢核。

5.1.4資訊安全小組：由資訊安全委員會召集人指派人員組成，負責規劃及執行各項資訊安全作業。

5.1.4.1 制定資訊安全管理相關規範。

5.1.4.2 推動資訊安全相關活動。

5.1.4.3 辦理資訊安全相關教育訓練。

5.1.4.4　建立風險管理制度，執行風險管理。

5.1.4.5　建立安全事件緊急應變暨復原措施。

5.1.4.6　執行稽核改善建議事項。

5.1.4.7　執行預防措施之改善。

5.1.4.8　研討新資訊安全產品或技術。

5.1.4.9　執行資訊安全委員會決議事項。

5.1.4.10 鑑別資訊安全相關之法規。

5.1.4.10.1 資訊安全小組應針對本校所提供之資訊服務，識別資訊安全相關法令、法規及相關要求，明確定義至「外來文件一覽表」中，並定期檢討與更新。

5.1.5緊急處理組：緊急處理組為任務編組，由資訊安全暨個人資料保護委員會召集人指派人員組成。成員相關權責及作業內容分述如下：

5.1.5.1　緊急處理組組長：

5.1.5.1.1 當重大資安事件發生時，負責聯絡及召集緊急處理組。

5.1.5.1.2 協調及督導各關鍵業務流程負責人執行作業，並協調資源之調派使用。

5.1.5.1.3 依據事件評估之結果，得依現況建請資訊安全委員會召集人決議是否宣布災變並啟動業務永續運作計畫。

5.1.5.1.4 當災變發生時，配合救災單位負責搶救人員、物資與設備等，以及現場指揮工作。

5.1.5.1.5 負責災後協調、指揮清理災害現場。

5.1.5.1.6 負責規劃原營運場所之現場復原工作。

5.1.5.2　各關鍵業務流程負責人員：

5.1.5.2.1 負責召集相關人員，發展、維護、更新修訂及執行各災害復原程序。

5.1.5.2.2 每年負責召集相關人員進行業務永續運作計畫之測試演

練。

5.1.5.2.3 負責原營運場所或異地備援場所之應變、處理、復原及運轉測試工作。

5.1.5.2.4 負責災害現場證據收集,俾利未來訴訟與損害求償事宜。

5.1.5.2.5 災害現場評估損害狀況及執行原營運場所之現場復原工作。

5.1.6資訊安全稽核小組：由資訊安全委員會召集人指派，負責評估資訊安全管理制度之執行情形。

5.1.6.1 擬定資訊安全內部稽核計畫。

5.1.6.2 執行資訊安全內部稽核。

5.1.6.3 撰寫資訊安全內部稽核報告。

5.1.6.4 追蹤不符合事項之改善執行情形。

5.2 管理審查會議

5.2.1資訊安全委員會應每年至少召開一次管理審查會議，必要時得召開臨時會議。

5.2.2管理審查會議審查內容建議如下：

5.2.2.1 資訊安全稽核結果及建議改善事項。

5.2.2.2 上級指導單位、內部同仁及外部單位等利害相關團體的建議。

5.2.2.3 新資訊安全產品或技術導入之審查。

5.2.2.4 矯正及預防措施檢討。

5.2.2.5 風險評鑑適切性審查。

5.2.2.6 前次管理審查會議決議執行狀況。

5.2.2.7 影響資訊安全制度之任何變更事項。

5.2.2.8 資訊安全組織成員所提出之改善建議。

5.2.2.9 資訊安全目標執行狀況報告。

本校依據「資訊安全政策」所列之範圍及目標制定「ISMS

有效性量測表」,並以該量測結果做為評估本校資訊安全目標達成情形。

5.2.3管理審查會議之結論建議如下：

5.2.3.1 資訊安全制度執行之各項改進措施。

5.2.3.2 更新風險評鑑與風險改善計畫。

5.2.3.3 針對可能影響資訊安全制度之內、外部事件，修正資訊安全管理流程與控制措施，包括：

5.2.3.3.1 營運需求的變更。

5.2.3.3.2 安全需求的變更。

5.2.3.3.3 影響現行營運需求的業務程序變更。

5.2.3.3.4 管理或法規需求的變更。

5.2.3.3.5 契約要求的變更。

5.2.3.3.6 可接受風險等級或標準的變更。

5.2.3.4 針對資訊安全制度之需要，協調所需之資源。

5.2.3.5 控制措施有效性評量方式的改善。

應每年檢視「ISMS 有效性量測表」之量測結果與執行情形，並檢討量測項目與目標水準是否需進行調整之必要，做成改善決議。

5.2.4管理審查紀錄

管理審查會議為資訊安全管理制度重要之活動,「資訊安全管理審查會議紀錄」應依「文件管理程序書」辦理。

5.3 組織間的合作及協調

須建立與資訊安全管理制度相關之「外部單位聯絡清單」,並由資訊安全小組負責維護及更新。

6 相關文件

6.1 資訊安全政策。

6.2 資訊安全組織成員表。

6.3 資訊安全管理審查會議紀錄。

國立斗六高級中學
資通安全推動小組成員及分工表

編號：01

製表日期：111年08月01日

職務	職稱	姓名	分機	電子郵件
資安長	校長	羅聰欽	110	tlsh_110@mail.edu.tw
資安執行秘書	資訊組長	陳俊利	161	alec5106@mail.edu.tw
委員	秘書	鍾源旺	111	tlsh_111@mail.edu.tw
委員	輔導主任	連約瑟	170	pre2486viasdf@mail.edu.tw
委員	圖書館主任	李惠娟	160	lhc600122@mail.edu.tw
委員	人事主任	陳彩緞	190	tlsh_190@mail.edu.tw
委員	主計主任	林維泰	180	investing_905@mail.edu.tw
委員	主任教官	林啟文	210	g9521204@mail.edu.tw
策略規劃組	教務主任	董季樺	120	tlsh_120@mail.edu.tw
組員	教學組長	佟以群	121	atong81@mail.edu.tw
組員	註冊組長	葉宗達	122	dionysus0406@mail.edu.tw
組員	試務組長	黃子溶	127	cathy0619@mail.edu.tw
組員	設備組長	劉國保	123	hbow520@mail.edu.tw
組員	特教組長	蔡昀伶	125	slimshgk@mail.edu.tw
資安防護組	學務主任	潘澤黃	130	panth5799999@mail.edu.tw
組員	訓育組長	林志豪	131	tlsh_132@mail.edu.tw
組員	生活組長	李文進	221	qsxdrf48@mail.edu.tw
組員	體育組長	林宗祺	132	ltcl210@mail.edu.tw
組員	活動組長	張季倩	139	chi_chien_chang@mail.edu.tw
組員	衛生組長	連惠卿	133	candylien8@mail.edu.tw
績效管理組	總務主任	陳嘉彬	150	stuaffair@mail.edu.tw

組員	庶務組長	詹聖偉	151	terrychan5128@mail.edu.tw
組員	出納組長	陳盈安	152	et580602@mail.edu.tw
組員	文書組長	賴文彬	153	lwp570416@mail.edu.tw

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，保護所接觸到的個人資料，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，違者願負法律責任。

此致

國立斗六高級中學

立 同 意 書 人：_____

身 分 證 字 號：_____

電　　話：_____

住　　址：_____

中　華　民　國　　年　　月　　日

《後續--個人資料提供同意書》

個人資料提供同意書

本同意書說明國立斗六高級中學（以下簡稱本校）將如何處理本表單所蒐集到的個人資料，當您勾選「我同意」並簽署本同意書時，表示您已閱讀、瞭解並同意接受本同意書之所有內容及其後修改變更規定。

1. 本校因執行業務蒐集您的個人資料包括姓名、身分證字號、電話、地址等。
2. 若您的個人資料有任何異動，請主動向本校申請更正，使其保持正確、最新及完整。
3. 若您提供錯誤、不實、過時或不完整或具誤導性的資料，您將損失相關權益。
4. 您可依中華民國「個人資料保護法」，就您的個人資料行使以下權利：
   (1) 請求查詢或閱覽。
   (2) 製給複製本。
   (3) 請求補充或更正。
   (4) 請求停止蒐集、處理及利用。
   (5) 請求刪求。
5. 本校利用您的個人資料期間為即日起至您離職之日，利用地區為台灣地區。
6. 除非取得您的同意或其他法令之特別規定，本校絕不會將您的個人資料揭露予第三人或使用。
7. 僅有經過授權的人員才能接觸您的個人資料，相關處理人員皆簽有保密合約，如有違反保密義務者，將會受到相關的法律處分。
8. 本同意書可能會因應個人資料保護法或其他相關法規、以及實際需求進行修正。

☐ 我瞭解與同意以上文字

_____簽章

中　　華　　民　　國　　年　　月　　日

國立斗六高級中學

資訊資產管理

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目錄

1　目的

建立國立斗六高級中學（以下簡稱「本校」）資訊資產管理規範，訂定資訊資產分類、分級、價值評估、標示及處理之遵循原則，並據以辦理各項資訊資產管理及作業方法。用以保護各類資訊資產，避免因人為疏失、蓄意或自然災害等風險所造成之傷害。

2　適用範圍

本校承辦相關資訊業務作業流程之資訊資產。

3　權責

3.1　資訊安全執行秘書：

負責定期審議資訊資產清單及價值評估結果，並督導相關活動之進行。

3.2　資訊安全小組：

負責定期辦理資訊資產異動調查與彙整，提供最新之資訊資產清單，並陳報資訊安全委員會。

3.3　資訊資產權責單位：

負責所管轄內資訊資產之存取授權，並評估與審核資訊資產分類分級及價值之結果，得另指定資訊資產保管單位。

3.4　資訊資產保管單位：

對於指定資訊資產，具有落實資訊資產權責單位所委託之保護管理責任。

3.5　資訊資產使用單位：

對於資訊資產之使用，必須依據權責單位要求，並具有正確使用操作之責任。

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 資訊資產權責單位

對該項資訊資產具有判斷資產價值、決定存取權限或新增、刪除、修改權限之單位，同時也是資訊資產的擁有單位。

4.5 資訊資產保管單位：

依據權責單位之需求標準，執行資訊資產日常保護、異動與維護之執行單位。

4.6 資訊資產使用單位：

因業務需求，經授權可直接或間接使用該資訊資產之單位。

5 作業說明

5.1 資訊資產鑑別

5.1.1各資訊資產權責單位應鑑別所管轄之資訊資產，並建立「資訊資產清單」。

5.1.2各資訊資產權責單位應定期更新與維護所管轄之資訊資產清單。

5.1.3資訊資產清單由各權責單位提供，資訊安全小組負責彙整，並陳報至資訊安全委員會，以確保資訊資產編號及清單之完整性。

5.2 資訊資產分類

5.2.1資訊資產依其性質不同，分為 7 類：人員、文件、軟體、通訊、硬體、資料、環境。

5.2.1.1 人員（People / PE）：包含全體同仁，以及委外廠商。

5.2.1.2 文件（Document / DC）：以紙本形式存在之文書資料、報表

等相關資訊，包含公文、列印之報表、表單、計畫等紙本文件。

5.2.1.3 軟體（Software / SW）：作業系統、應用系統程式、套裝軟體等，包含原始程式碼、應用程式執行碼、資料庫等。

5.2.1.4 通訊（Communication / CM）：網路設備、網路安全設備、提供資訊傳輸、交換之線路或服務。

5.2.1.5 硬體（Hardware / HW）：主機設備等相關硬體設施。

5.2.1.6 資料（Data / DA）：儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。

5.2.1.7 環境（Environment / EV）：相關基礎設施及服務，包含辦公室實體、實體機房、電力、消防設施等。

5.2.2各類資訊資產機密等級分為 4 級：一般、限閱、敏感、機密。各等級之評估標準如下：

5.2.2.1 一般：無特殊之機密性要求，可對外公開之資訊。

5.2.2.2 限閱：僅供組織內部人員或被授權之單位及人員使用。

5.2.2.3 敏感：僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用。

5.2.2.4 機密：為組織、主管機關或法律所規範之機密資訊。

5.2.3資訊資產之機密等級應定期審核，視實際需要予以調整。

5.2.4不同等級之資訊資產合併使用或處理時，以其中最高之等級為機密等級。

5.3 資訊資產價值鑑別

5.3.1資訊資產權責單位應鑑別其所管轄內所有資訊資產之價值。

5.3.2資訊資產價值除考量資訊資產機密等級之外，尚需考量資訊資產之可用性及完整性，其評估標準如下：

5.3.2.1 機密性評估標準

評估標準	數值
此資訊資產無特殊之機密性要求	1
此資訊資產僅供組織內部人員或被授權之單位及人員使用	2
此資訊資產僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用	3
此資訊資產所包含資訊為組織或法律所規範的機密資訊	4

5.3.2.2　完整性評估標準

評估標準	數值
該資訊資產本身完整性要求極低	1
該資訊資產本身具有完整性要求，當完整性遭受破壞時，不會對組織造成傷害	2
該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，但不至於太嚴重	3
該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，甚至造成業務終止	4

5.3.2.3　可用性評估標準

評估標準	數值
該資訊資產可容許失效 3 工作天以上	1
該資訊資產可容許失效 8 工作小時以上，3 工作天以下	2
該資訊資產僅容許失效 4 工作小時以上，8 工作小時以下	3
該資訊資產僅容許失效 4 工作小時以下	4

5.3.2.4　資訊資產價值之決定將依據資訊資產之機密性、完整性及可用性評估之後，取 3 者之最大值以為資訊資產之價值。

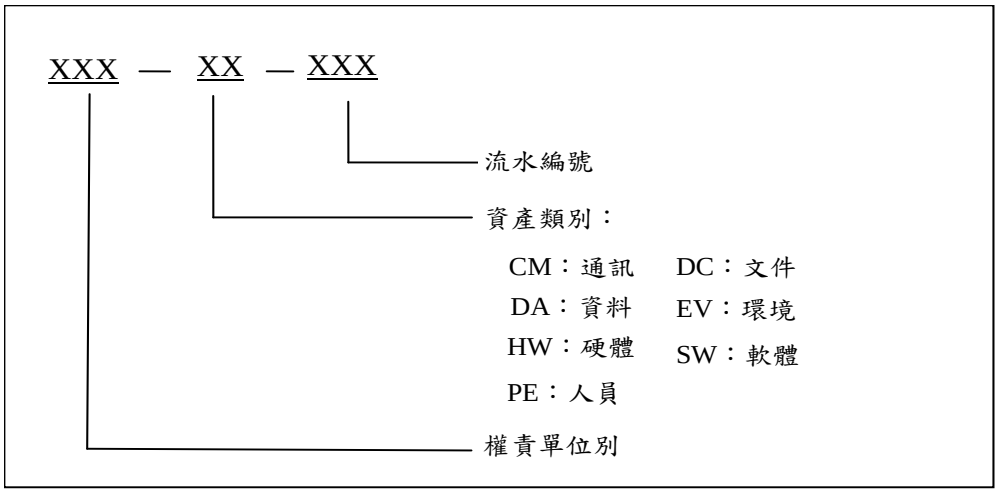
5.4　資訊資產清單及價值確認

5.4.1資訊資產權責單位應依據資訊資產清單之機密性、可用性及完整性之評估標準，確認資產價值。

5.4.2資訊資產清單及價值評估結果，應陳報至資訊安全委員會審議。

5.5 資訊資產編號及標示

5.5.1除「資訊安全管理制度文件」外的資訊資產編碼方式，第 1~3 碼為權責單位別，第 4~5 碼為資產類別，第 6~8 碼為資訊資產流水編號。



資訊資產編碼方式圖

5.5.2已列入機密等級分類的資訊資產，應明確標示其機密等級，避免其機密性遭破壞。

5.5.3實體設備之重要等級標示方式：

5.5.3.1 實體設備之重要等級應以不同顏色標籤區分（資產價值 2 為綠色標籤，資產價值 3 為黃色標籤，資產價值 4 為藍色標籤）。

5.5.3.2 文件之機密等級應於文件封面做明確的標示。系統輸出機密等級為敏感以上的報表，如系統未自動標示，則由資訊資產權責單位做額外的明顯註記。

5.6 資訊資產管理作業

5.6.1有關文件、紀錄、相關電子檔及儲存媒體控管原則及方式，請參閱「文件管理程序書」。

5.6.2有關人員之控管原則及方式，請參閱「人員安全與教育訓練程序書」。

5.6.3有關實體資產，包括：軟體、硬體、通訊及環境等之控管原則及方式，請參閱「實體安全管理程序書」。

5.6.4資訊資產異動管理，如：新增、刪除、修改等控管原則，請參閱「資

訊資產異動作業說明書」。

5.7 覆核

5.7.1權責單位每年至少進行 1 次資產盤點與資訊資產清單覆核，以更新及確保資訊資產清單的正確性及完整性。

5.7.2當範圍內有以下的狀況發生時，則實施不定期的覆核，以更新及確保資訊資產清單的正確性及完整性。

5.7.2.1 有新增、變更或移除資訊資產。

5.7.2.2 系統有重大異動。

5.7.2.3 作業環境改變。

5.8 資訊資產之報廢

資訊資產之報廢（或銷毀）應依「資訊資產異動作業說明書」之相關規定，採取適當之方式進行銷毀。

5.9 資訊資產之處理規範

5.9.1針對價值 3 或 4 之資訊資產，應加強安全保護及存取控制管控措施，以防止洩漏或不法及不當的使用。

5.9.2價值 3 或 4 文件類資訊資產之安全處理應符合以下作業要求：

5.9.2.1 紙類文件不再使用時，應銷毀處理。

5.9.2.2 系統流程、作業流程、資料結構及授權程序等系統相關文件，應予適當保護，以防止不當利用。

5.9.2.3 系統文件應指定專人管理，並鎖在安全的儲櫃或其他安全場所，且發送對象應以最低必要的人員為限。

5.9.2.4 電腦產製的文件，應與其應用檔案分開存放，且應建立適當的存取保護措施。

5.9.3價值 3 或 4 軟體類資訊資產之安全處理作業，請參閱「存取控制管理程序書」及「系統開發與維護程序書」之相關程序。

5.9.4價值 3 或 4 硬體類資訊資產之安全處理作業，請參閱「實體安全管

理程序書」中重要設備之相關程序。

5.9.5應定期檢討價值 3 或 4 之資訊資產清單內容，以確保重要資產受到適當的安全保護。

6 相關文件

6.1 資訊資產清單

國立斗六高級中學

風險評鑑與管理

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目錄

1 目的

建立國立斗六高級中學（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。

3.2 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。

3.3 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。

3.4 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

國立斗六高級中學

資訊資產異動作業

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目錄

1　目的

本作業說明書制訂之目的，在於保護國立斗六高級中學（以下簡稱本校）之資訊資產於新增、異動、報廢時，能依據適當之程序，進行安全可靠之處置。

2　適用範圍

本校承辦相關資訊業務之資訊資產新增、異動、報廢作業。

3　權責

本校相關人員、約聘（僱）人員與工讀生：遵守本作業說明書之相關規定，確實執行資訊資產新增、異動、報廢作業之程序。

4　名詞定義

無。

5　作業說明

5.1　資訊資產之新增、異動

5.1.1　資訊資產新增或異動時，資訊資產使用單位應填寫「資訊資產異動申請表」，資訊資產價值為 4 者，須呈核至資訊安全執行秘書；其餘由權責主管核定。

5.1.2　「資訊資產異動申請表」經審核後，交由文件管理人員保管，並定期更新「資訊資產清單」。

5.2　資訊資產之報廢

5.2.1　硬體及通訊資產報廢

5.2.1.1　硬體及通訊資訊資產需報廢或移作他用，硬體及通訊資產之相關設定與儲存媒體之資料必須清除。

5.2.1.2　硬體及通訊資訊資產報廢時，資訊資產使用單位應填寫「資訊資產異動申請表」，經本校審核並確認資料清除後，方可進行資訊資產報廢程序。

5.2.1.3　資訊資產保管單位依據「資訊資產異動申請表」經本校審核

後，辦理更新「資訊資產清單」，可重複使用之資料儲存媒體，於不再繼續使用時，應將儲存之內容完全消除，敏感級以上的資料必須確認資料清除後無法還原其內容。

5.2.1.4 硬體及通訊資訊資產價值為 4 者，經呈報資訊安全官核准後，方可執行報廢；資訊資產價值為 4 以下者，經各權責主管核准後，方可執行報廢。

5.2.2 儲存媒體報廢

5.2.2.1 儲存媒體如要報廢或移作他用時，儲存媒體上之資料必須清除。

5.2.2.2 當儲存媒體須報廢時，應採用以下任一種合宜之措施進行銷毀：

5.2.2.2.1 清除硬碟資料

以覆寫方式覆蓋硬碟資料或以工具進行實體之破壞，使其無法使用。

5.2.2.2.2 光碟

於光碟表面塗抹層製造刮痕後，再進行絞碎作業。

5.2.2.2.3 磁帶或磁片

使用強力磁鐵消磁後，磁帶應抽出後剪斷，磁片則進行絞碎作業。

5.2.2.3 儲存機密級以上資料之儲存媒體，嚴格禁止使用格式化方式進行資訊資產之報廢程序，應採用上述之方式進行銷毀。

5.2.3 軟體版權到期與移除

5.2.3.1 當軟體版權到期而需移除時，資訊資產使用單位應填寫「資訊資產異動申請表」，經本校審核後，方可進行軟體移除程序。

5.2.3.2 資訊資產保管單位依據「資訊資產異動申請表」經本校審核後，辦理更新「資訊資產清單」。

5.2.3.3 軟體資訊資產價值為 4 者，經呈報資訊安全官核准後，方可執行移除；資訊資產價值為 4 以下者，經各權責主管核准後，方可執行移除。

5.2.4 文件報廢

當資訊安全管理制度相關文件報廢時，依照文件管理程序書辦理。

6 相關文件

6.1 資訊資產異動申請表

6.2 資訊資產清單

國立斗六高級中學

存取控制管理

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目錄

1　目的

為保護資訊資產，降低未經授權存取系統之風險，以達成國立斗六高級中學（以下簡稱「本校」）安全控管之目的。

2　適用範圍

本校資訊資產之存取控管原則。

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　存取控制政策

5.1.1　資訊資產之存取應與本身業務相關之範圍為主，任何人未經授權不得存取業務範圍外之資訊資產。

5.1.2　應正確地使用資訊資產，以維護資訊資產之可用性、完整性與機密性。

5.1.3　非因業務需求不得將系統存取帳號提供給外部人員，若因業務需要開放帳號予外部人員，應有適當安全控管措施，該安全控管措施應考量業務需求及資訊資產之機密性，授與適當之存取權限及有效日期。

5.1.4　被賦予系統管理最高權限之人員、掌理重要技術及作業控制之特定人員，應經審慎之授權評估。

5.1.5　因處理系統當機與異常狀況需視狀況授與適當存取權限，並避免共用帳號。

5.1.6　可攜式電腦儲存媒體，例如：筆記型電腦、隨身碟、外接式硬碟、

光碟、磁帶等，應採取適當之控管措施，以防止未經授權之資料、系統、網路存取或病毒傳播。

5.1.7 資料、資訊之存取，必須符合「個人資料保護法」、「電子簽章法」及「智慧財產權」等相關法規、法令之規定，或契約對資料保護及資料存取使用控管之規定。

5.1.8 系統主機之公用程式路徑之存取權限應適當控管，禁止一般使用者存取。

5.1.9 針對無人看管的資訊資產設備，應有適當控管程序，以防未經授權之存取或濫用。

5.1.10 個人桌上型電腦、可攜式電腦應設定於一定時間不使用或離開後，應自動清除螢幕上的資訊並登出或鎖定系統，以避免被未經授權之存取。

5.2 帳號與密碼管理

5.2.1 新購置之應用軟體或系統，安裝完成後應立即更新預設之密碼，並刪除或關閉不必要之帳號。

5.2.2 使用者帳號管理

5.2.2.1 使用者帳號申請應填寫「資訊服務申請表」，經部門主管核准後，由帳號管理人員進行使用者帳號建立作業。

5.2.3 管理者帳號管理

5.2.3.1 系統管理者應避免共用系統管理者帳號，系統管理者帳號與密碼應存放於安全之處。

5.2.3.2 系統管理者密碼設置，至少 8 碼，且應符合密碼設置原則。

5.2.4 密碼管理

5.2.4.1 使用者首次使用系統時，應要求更改密碼設定，並妥善保管帳號與維持密碼之機密性，保存帳號密碼之檔案應以加密方式處理。

5.2.4.2 使用者應避免將帳號密碼記錄在書面上，張貼在個人電腦、螢幕或其他容易洩漏秘密之場所。

5.2.4.3 使用者禁止共用帳號密碼。

5.2.4.4 使用者發現密碼可能遭破解時，應立即更改密碼。

5.2.4.5 使用者每次存取系統時應輸入密碼登入系統，避免使用記錄密碼功能，導致開機時自動登入系統。

5.2.4.6 資訊資產價值為 4 以上之資訊系統，系統管理者應至少 3 個月更換密碼一次，學籍系統之使用者(學校行政人員)應至少 6 個月更換密碼一次，並禁止重複使用相同的密碼。

5.2.4.7 使用者密碼設置至少 8 碼，且應符合密碼設置原則。

5.2.4.8 密碼設置原則

應儘量避免使用易猜測或公開資訊為設定，例如：

A. 個人姓名、出生年月日、身分證字號

B. 機關、單位名稱或其他相關事項

C. 使用者 ID、其他系統 ID

D. 電腦主機名稱、作業系統名稱

E. 電話號碼

F. 空白

密碼設定可考慮下列原則：

A. 參雜數字、英文字母、特殊符號、大小寫

B. 特殊意義詞彙

5.2.4.9 使用者遺忘密碼時，須填具「資訊服務申請表」，經部門主管核准後，由帳號管理人員重新設定。

5.3 使用者存取管理

5.3.1 各項系統資源使用權限之申請、註冊及註銷應遵循作業管理程序，並維護相關之申請、註冊、註銷資料與紀錄，以備查核。

5.3.2 使用者職務異動或離職時,部門主管應即時通知相關單位調整或終止使用者之存取權限。

5.3.3 特殊權限之使用者必須與一般權限之使用者區分管理;針對特殊權限帳號，應妥善管理。

5.3.4 特殊權限之授權管理，必須依執行業務系統別之需求，例如作業系統、資料庫管理系統、網路服務系統、監控管理系統等賦予系統存取特殊權限的授權,且以執行業務及職務所必要的最低資源存取授權為限。

5.3.5 系統相關作業人員需經正式授權存取業務相關之資訊資產,其識別資料與帳號必須為唯一，禁止借用他人之帳號或共用帳號。

5.3.6 各項設備與系統相關之使用權限（例如使用者帳戶與作業權限）應留存紀錄。

5.3.7 應妥善管理久未登錄系統之帳戶，若超過 6 個月未曾登錄，則視需要清除閒置帳號。

5.3.8 應要求使用者變更初始密碼並定期變更密碼;重要資訊系統及特殊權限之存取帳號之密碼變更期間應較一般權限之帳號頻繁。

5.3.9 使用者存取權限應定期審查，週期不得超過 6 個月。

5.3.10 重要系統稽核資料應由專人定期審核，系統管理者不得新增、刪除或修改稽核資料，審查週期不得超過 6 個月。

5.4 作業系統存取控制

5.4.1 系統設定應避免於終端機登入程序中以明碼方式顯示密碼相關資訊。

5.4.2 只有在完成所有的登入資料輸入後,系統才開始查驗登入資訊的正確性；若登入發生錯誤，系統不應顯示錯誤發生之原因。

5.4.3 在系統登入被拒絕後，應立即中斷登入程序，並不得給予任何的協助。

5.4.4 應設定系統登入程序之時間限制，如果超出時間限制，系統將自動中斷登入。

5.4.5 使用者帳號避免顯示任何足以辨識使用者特別權限的訊息，例如：顯示其為管理者或監督者。

5.4.6 系統管理人員結束系統維護作業後，應結束應用系統及網路連線，清除螢幕上的資訊，登出系統，並鎖定主控台螢幕。

5.4.7 系統之存取使用應留存查核紀錄。

5.5 應用系統之存取控制

5.5.1 資訊存取之限制

5.5.1.1 應用系統資訊之使用，僅限業務相關之授權使用者，並應適當控制。例如：新增、刪除或執行等。

5.5.1.2 應用系統之敏感與機密性資訊，應與一般資訊作適當區隔，並加強權限控管措施。

5.5.2 原始程式資源之存取控制

5.5.2.1 應用程式原始碼，應集中存放，並由系統負責人管理程式之增修作業。

5.5.2.2 開發中之原始程式碼，應與線上程式碼分開放置與控管。

5.5.2.3 舊版的原始程式應妥慎保管，並詳細記錄使用的明確時間，以備新版失敗回復使用。

5.5.2.4 應用程式之異動需經適當控管。

5.5.2.5 應用程式管理人員，應檢視程式目錄清單，如有異常情形，應即查明原因及處理。

5.6 網路存取控制

5.6.1 網路系統應依其性質之不同，分開成不同的領域，各領域應以特定的安全設施（如防火牆及網路閘門）加以保護，以降低可能的安全風險。

5.6.2 網路管理人員應定期檢視網路存取之紀錄，並留存查核紀錄。

5.6.3 對於開放提供外部客戶或廠商存取之服務，必須限制使用者之網路功能以確保網路安全。

5.6.4 網路路由之規劃必須確保任何網路連線或資訊傳輸符合網路存取之安全需求。

5.7 遠端存取之限制

5.7.1 所有資訊資源使用者，非經主管授權或允許，禁止執行遠端存取作業。

5.8 資料庫存取控制

5.8.1 資料庫之存取權限，應經適當程序之授與及移除，且須使用獨立之帳號及密碼登入。

5.8.2 資料庫存取之身分驗證機制，須由系統內部安全機制提供。

5.8.3 資料庫使用者之帳號密碼設定必須符合本程序書及相關系統之帳號密碼管理規範之要求。

5.8.4 資料庫公用程式路徑之存取權限應適當控管，禁止一般使用者存取。

5.8.5 資料庫最高權限帳號之存取授權應僅限於資料庫管理員。

5.8.6 資料庫預設帳號應變更密碼，或是關閉使用。

5.8.7 資料庫之存取紀錄應留存查核紀錄。

5.9 系統被入侵時的異常處理

5.9.1 立即拒絕入侵者任何存取動作（例如關閉可疑帳號），防止災害繼續擴大。

5.9.2 關閉受侵害的主機，或立即與網路離線。

5.9.3 檢查防火牆及系統紀錄，研判入侵管道之方式，必要時作安全漏洞修補。

5.9.4 通知主機供應商提供必要的回復協助。

5.9.5 如伺服主機的完整性受侵害，應將完整的系統備份資料存回受害主機上，並測試其功能，直至完全回復為止，最後再將該主機重新上線。

6 相關文件

6.1 個人資料保護法

6.2 智慧財產權相關法令

6.3 電子簽章法

6.4 資訊服務申請表

國立斗六高級中學

實體安全管理程序書

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目錄

1　目的

本程序書制訂之目的，在於保護國立斗六高級中學（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或經由監控畫面隨時監控安全並填寫「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 委外廠商保密切結書

國立斗六高級中學

通信與作業管理程序書

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目錄

1　目的

為防止國立斗六高級中學（以下簡稱「本校」）資訊在不安全之網路環境下，遭致可能之破壞，或非預期及非經授權之修改，以確保資訊系統與資料之安全性、可用性及完整性。

2　適用範圍

本校所轄之範圍內，相關網路服務與設備及核心業務系統之管理。

3　權責

本校網路管理人員應遵守本程序書之相關規定，以確保本校網路之安全。

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。

4.9 行動計算與通信設施

如筆記型電腦、掌上型電腦、行動電話等。

4.10 儲存媒體

如磁片、磁碟、磁帶、IC 卡、匣式磁帶、外接式硬碟、光碟、隨身碟、各式記憶卡、錄影帶、錄音帶等。

5 作業說明

5.1 資訊系統安全規劃作業

5.1.1 應建立資訊系統之安全控管機制，以確保資訊資料之安全，保護系統及網路作業，防止未經授權之系統存取。

5.1.2 資訊系統管理職務與責任應加以區隔，足以影響業務經營管理的資訊，不可只由單獨一人知悉。如因人力資源限制，無法區隔責任，則應加強監督與稽核等措施。

5.1.3 伺服主機及網路設備應指定負責人，負責該主機之正常運作，包括應用程式之執行、資料庫之維護及相關作業系統與主機硬體資源之分配管理。主機或網路設備負責人無法進行管理時應由代理人負責，未指定負責人之主機及網路設備由機房管理負責人員負責。

5.1.4 網路管理人員應妥為規劃網路架構、設定網路參數，並依規定備份相關檔案。

5.1.5 應規劃系統與設備的開發與測試環境，避免於已上線運作設備及環境進行開發或測試工作。

5.1.6 系統及設備建置前，主辦單位應對系統需求做適當規劃，以確保足夠的電腦處理及儲存容量。如需委外開發或採購，則依「委外管理程序書」辦理。

5.1.7 系統設備與軟體之建置，均應依照「系統開發與維護程序書」之程序進行測試及驗收。

5.2 變更管理

5.2.1 新增設備及網路變動，應即時修改網路架構圖及設備資料。

5.2.2 架構調整：架構變動之影響性甚大者應經資訊安全官以上核准，並遵循下列規定：

5.2.2.1 設備之功能性及設定方式應熟悉掌握。

5.2.2.2 新增對外網路連線，需注意安全性考量，從嚴審核對外網路連線與內部之連接之方式。

5.2.2.3 如有廠商參與安裝或設定，必須全程陪同參與並記錄。

5.2.3 系統若有相關文件（如系統文件、參考文件或作業準則）時，系統相關負責人員於變更程序同時，應同步修改維護相關文件。

5.2.4 各項系統變更作業依據「系統開發與維護程序書」變更作業控制措施辦理。

5.3 惡意軟體之防範

5.3.1 禁止使用或下載未經授權或與業務無關之軟體。

5.3.2 應安裝病毒偵測與修復軟體，並定期更新病毒資訊，以防止病毒之攻擊。伺服器主機防毒軟體系統應設定主動掃瞄檢查，或由網路管理人員定期執行掃瞄檢查作業。

5.3.3 應定期檢查支援重要業務之作業系統是否有任何未核准的檔案或未經授權的修改。

5.3.4 應於使用來源不明、來源未經授權、或從未經信任網路接收之檔案前，檢查該檔案是否藏有病毒。

5.3.5 應於使用前檢查電子郵件附件和下載檔案有無惡意軟體。

5.3.6 使用者如偵測到電腦病毒入侵或其他惡意軟體，應立即通知系統或網路管理人員；管理者亦應將已遭病毒感染的資料及程式等資訊隨時提供使用者，以避免電腦病毒擴散。

5.3.7 系統或電腦設備如遭病毒入侵感染，應立即與網路離線並隔離，直到網路管理人員確認病毒已消除後，才可重新連線，並留存處理紀錄。

5.4 電腦軟體與程式著作權保護

5.4.1 應訂定使用授權軟體與遵守著作權規範，違反規範者應依相關程序議處。

5.4.1.1 使用軟體與資訊產品不得超過允許的最高使用人數。

5.4.1.2 使用軟體與資訊產品應遵守相關規定，例如限制於指定之機器使用、限制僅於備份時方可複製等。

5.4.1.3 取得之合法軟體不得從事或轉讓予非授權範圍之使用。

5.4.1.4 從公共網路取得之合法軟體與資訊須遵守原著作權者與電腦處理個人資料保護法之規定。

5.4.1.5 對公共系統的存取不得擅自存取其所相連的網路。

5.4.2 應妥善保管採購軟體產品之授權書、原版光碟、手冊等等證明。

5.4.3 經由網際網路下載之公開授權軟體，應在確認安全無虞及不違反智慧財產權前提下，方得下載執行。

5.5 網路安全管理

5.5.1 網路服務之管理

5.5.1.1 避免利用公共網路傳送敏感等級（含）以上資訊，應保護資料在公共網路傳輸之完整性及機密性，並保護連線作業系統之安全性。

5.5.1.2 網路管理人員應利用網路管理工具，偵測及分析網路流量。

5.5.1.3 開放相關人員從遠端登入內部網路系統之網路服務，應執行嚴謹之身分辨識作業，或提供連線設備之識別機制。

5.5.1.4 如果系統使用者為非合法授權之使用者時，應立即撤銷其系統使用權限；離（休、退）職人員應依資訊安全規定及程序，調整或終止其存取網路及系統之權限。

5.5.1.5 網路管理人員除依相關法令或規定，不得閱覽使用者之私人檔案；但如發現有可疑之網路安全情事，網路系統管理人員得依授權規定，使用工具檢查檔案。

5.5.1.6 網路管理人員除有緊急狀況外，未經使用者同意，不得增加、刪除及修改私人檔案。

5.5.1.7 網路設備軟硬體應限定由網路系統管理人員依規定辦理設定異動，並應留存紀錄備查。

5.5.1.8 對任何網路安全事件，網路管理人員應依「安全事件管理程序書」辦理。

5.5.1.9 網路管理人員應於每工作日檢查所有網路設備並記錄於「巡查紀錄表」，每月送主管簽核。如發現異常應依本程序之異常處理流程辦理。

5.5.2 網路使用者之管理

5.5.2.1 經授權之網路使用者，只能在授權範圍內存取網路資源。

5.5.2.2 網路使用者於使用行動碼（如 ActiveX、JAVA Applet）之前，應先確認其授權資料，並禁止執行未經授權之行動碼。

5.5.2.3 網路使用者應遵守網路安全規定，並確實瞭解其應負之責任；如有違反網路安全情事，應依資訊安全規定，限制或撤銷其網路資源存取權利，並依相關規定處理。

5.5.2.4 網路使用者不得將自己之登入身分識別與登入網路之密碼交

付他人使用。

5.5.2.5 禁止網路使用者以任何方法竊取他人之登入身分與登入網路密碼。

5.5.2.6 禁止網路使用者以任何儀器設備或軟體工具竊聽網路上之通訊。

5.5.2.7 禁止網路使用者在網路上取用未經授權之檔案。

5.5.2.8 網路使用者不得將色情檔案建置在網路，亦不得在網路上散播色情文字、圖片、影像、聲音等不法或不當之資訊。

5.5.2.9 禁止網路使用者發送電子郵件騷擾他人，導致其他使用者之不安與不便；或以任何手段蓄意干擾或妨害網路系統之正常運作。

5.5.2.10 網路使用者不得任意修改網路相關參數。

5.5.2.11 為維護本校網路安全，網路管理人員於發現網路使用者之電腦發送異常封包或使用非經允許之服務時，依『校園網路使用規範』相關規定辦理。

5.5.3 無線網路使用之管理

5.5.3.1 無線網路基地台之使用應經適當控管。

5.5.3.2 無線網路設備之安裝設定應經核准。

5.5.3.3 無線網路設備之使用應取得授權，禁止於內部網路私自使用任何無線網路產品。

5.5.3.4 無線網路設備之使用應有適當管理機制，例如：授權使用之IP 數量、連接埠、網卡位址（MAC）過濾等。

5.5.3.5 無線網路之資料傳輸應使用加密機制，並就安全與資訊風險之考量，增加適當之防護機制以避免資料外洩。

5.5.4 防火牆之安全管理

5.5.4.1 所有與外界網路連接之連線，應透過加裝防火牆，以控管外

界與本校內部網路間之資料傳輸與資源存取。

5.5.4.2 防火牆設定異動時，應填寫「防火牆進出規則申請表」，經主管簽准後，交由網路管理人員設定。

5.5.4.3 防火牆應由網路管理人員執行控管設定，並依制定之資訊安全規定、資料安全等級及資源存取之控管策略，建立包含身分辨識機制與系統稽核之安全機制。

5.5.4.4 防火牆設置完成時，應測試防火牆是否依設定之功能正常及安全地運作。如有缺失，應立即調整系統設定，直到符合既定之安全目標。

5.5.4.5 網路管理人員應配合資訊安全政策及規定之修正，以及網路設備之變動，隨時檢討及調整防火牆系統設定，調整系統存取權限，以反映最新狀況。

5.5.4.6 視業務需要及設備功能，對於通過防火牆之特定網路服務，應予確實紀錄。

5.5.4.7 網路管理人員應避免採取遠端登入方式登入防火牆主機，以避免登入資料遭竊取，危害網路安全。如果必須使用遠端登入方式管理，應訂定嚴謹之遠端登入控管措施。

5.5.4.8 若資源許可應建立防火牆設備之備援機制；防火牆之環境建置檔等需定期執行備份作業。

5.5.4.9 防火牆政策及設定應每月定期覆核，並記錄於「巡查紀錄表」中，若已屆期限或該 IP 不再使用，請系統負責人確認後刪除，並填寫「防火牆進出規則申請表」。

5.5.4.10 網路管理人員每週將防火牆之 log 轉出存放於備份機器上，並記錄於「巡查紀錄表」。

5.5.4.11 於防火牆設定變更之前，將各防火牆之設定檔備份，並依「備份狀況紀錄表」之表列進行備份，存放於備份設備上。

5.5.5 網路資訊之管理

5.5.5.1 敏感等級（含）以上之業務資料或文件不得存放於對外開放之資訊系統中，若因特殊業務功能之需求，必須採取加強之安全管控機制，如：資料加密。

5.5.5.2 網路管理人員應負責監督網路流量及使用情形，並對可能導致系統作業癱瘓等情事，預作有效的防範，以免影響網路服務品質。

5.5.5.3 對外開放的資訊系統所提供之網路服務，如：HTTP、FTP等，應採取適當之存取控管機制。

5.5.5.4 對校外開放的資訊系統，如：存放教職員、學生或家長申請或註冊之個人資料檔案，其傳輸過程應考量以加密方式處理，並妥善保管資料，以防止被竊取或移作他途之用，侵犯個人隱私。

5.5.5.5 網路管理人員於偵測收到資訊系統異常狀況或駭客入侵之警示訊息時，應立即通報權責主管，依據相關作業管理規範採取適當之緊急應變處理，並留存系統異常處理紀錄。

5.5.6 網路管理作業流程

5.5.6.1 網路檢查作業

5.5.6.1.1 以指令方式 ping 各網段之 Gateway，以回應時間初步判斷網路狀態。

5.5.6.1.2 檢查防火牆之 log 及狀態。

5.5.6.1.3 防火牆發現異常情形應設定自動寄發通知信給網路管理人員，嚴重時網路管理人員應立即採取阻擋作為，並通知主管。

5.5.6.2 網路監控作業

5.5.6.2.1 利用工具自動 ping 各 IP，用以監控網路各節點，由其回

應數值判斷網路狀態是否正常。

5.5.6.2.2 收集防火牆之 log，並統計 log 資料。

5.5.6.2.3 監控內部網路頻寬使用狀況，於頻寬使用率達 60%以上時，應評估增加頻寬之必要性。

5.5.6.3 異常監控作業

5.5.6.3.1 定期監控各伺服器提供之各項服務是否正常，若設備服務狀態不正常時，應通知相關負責人員處理。

5.5.6.4 異常處理作業

5.5.6.4.1 以節點方式由內而外檢測，由回應數值推知問題點。

5.5.6.4.2 確認與問題點相關之實體設備和網路線是否正常。

5.5.6.4.3 如為設備問題可尋找替用設備更換，並連絡廠商維修，並將處理情形記錄於「異常事件紀錄表」。

5.5.7 網路入侵之處理

5.5.7.1 網路被入侵時，應依「安全事件管理程序書」辦理。

5.5.7.2 應建立網路入侵事件之調查程序，除利用工具及稽核檔案提供之資料外，應協請相關單位（如網路服務提供者），追蹤入侵者。

5.5.7.3 入侵者之行為若觸犯法律規定，構成犯罪事實，應立即告知相關單位，請其處理入侵者之犯罪事實調查。

5.6 電子郵件安全管理

5.6.1 電子信箱帳號之註冊、離職、異動申請，應遵循電子郵件相關管理規範之規定，除學生帳號由本校批次建立外，其餘則填寫「電子郵件帳號申請表」提出申請，經各單位部門主管核准後，再交由系統管理者或經授權之管理者建置相關資料。

5.6.2 應建立電子郵件之安全管理機制，以降低電子郵件可能帶來之業務

上及安全上之風險。

5.6.3 應禁止發送匿名信，或偽造他人名義發送電子郵件騷擾他人，導致其他使用者之不安與不便。

5.6.4 敏感等級（含）以上的資料或文件，應避免以電子郵件傳送。

5.6.5 不得傳遞大量且非必要的資訊，避免網路壅塞及資源浪費。

5.6.6 電子郵件附加之檔案，應事前檢視內容有無錯誤後方可傳送。

5.6.7 對來路不明之電子郵件，不宜隨意打開電子郵件，以免啟動惡意執行檔，使網路系統遭到破壞。

5.6.8 郵件伺服器異常處理及故障排除作業

5.6.8.1 發現郵件伺服器系統異常，資訊人員應進行診斷，辨識異常原因及影響範圍，評估系統回復時間，並進行排除作業。

5.6.8.2 異常處理人員應定時回報權責主管最新狀況及處理進度。

5.6.8.3 如異常發生無法立即排除故障時，應通知相關部門異常影響程度及預估回復時間，並採取因應措施。

5.6.8.4 如診斷可能係硬體設備故障造成，則通知廠商人員到場檢測。

5.6.8.5 系統經復原並確實檢查測試後，終止緊急應變作業，並通知相關部門及主管。

5.6.8.6 將處理過程及結果記錄於「異常事件紀錄表」中。

5.7 全球資訊網（WWW）

5.7.1 對 HTTP 伺服器開放可存取的範圍，應限制僅能存取資訊系統之某一特定區域之功能與權限，HTTP 伺服器應透過組態的設定，使其啟動時不具備系統管理者身分。

5.7.2 公告之資訊，應經由權責管理人員之審查與核定，確認未含機密性或敏感性的資訊、違反本系統資訊安全管理之相關資訊，以及違反智慧財產權或法令所明定禁止之資訊。

5.7.3 開放外界連線作業之資訊系統，應避免外界直接進入資訊系統或資料庫存取資料。

5.7.4 內部使用的瀏覽器，對下載之檔案應設定掃描是否隱藏電腦病毒或惡意內容。

5.7.5 當伺服器執行之應用程式需接收自使用者回傳資料時，應予嚴密監控，以防止不法者利用來執行系統指令，獲取系統內重要的資訊或破壞系統。

5.8 電腦管理及安全防護

5.8.1 系統負責人應定時檢查作業系統及硬體設備之效能，並注意作業系統版本更新及問題資訊，做最適建議及導入。

5.8.2 主機負責人應進行伺服器主機監控，檢查系統、安全及應用程式日誌紀錄、或其它有關之系統狀況。一旦發現任何問題得請相關人員協同處理，必要時並通知廠商處理。

5.8.3 為提升伺服器主機連線作業之安全性，應視需要使用加密通道（如VPN、SSH）等各種安全控管技術。

5.8.4 應關閉不需要之服務。

5.8.5 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。

5.8.6 應保存稽核紀錄，並定期審查。

5.8.7 系統負責人應於每週上班時至少一次依「巡查紀錄表」所列項目檢查各主機狀況，以確保系統正常運作。

5.8.8 軟體由系統負責人安裝，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。

5.8.9 系統軟體測試由系統負責人辦理，測試時應事先公告並通知及協調相關人員支援，且視狀況需要通知相關人員及使用者以避免因資訊

服務中斷而影響業務。

5.8.10 異常狀況排除

5.8.10.1 遇異常狀況時系統負責人應先行回報資訊安全官，視需要採適當方式處理。

5.8.10.2 通知本校相關人員協助，並說明詳細原因、先行處理步驟及相關資料。如無法自行排除則向維護廠商報修維護，並將故障情形公告及通知使用者及相關人員。

5.8.10.3 將處理過程及結果記錄於「異常事件紀錄表」中。

5.8.11 系統入侵之處理

5.8.11.1 立即拒絕入侵者任何存取動作(例如關閉可疑帳號)，以防止災害繼續擴大。

5.8.11.2 關閉受侵害的主機，並立即與網路離線。

5.8.11.3 檢查防火牆及系統紀錄，研判入侵管道之方式，必要時作安全漏洞修補。

5.8.11.4 通知主機供應商提供必要的回復協助。

5.8.11.5 如伺服主機的完整性受侵害，應將完整的系統備份資料存回受害主機上，並測試其功能，直至完全回復止，最後再將該主機重新上線。

5.8.11.6 將處理過程及結果記錄於「異常事件紀錄表」中。

5.9 可攜式電腦儲存媒體管理

5.9.1 系統資料若需以可攜式媒體保存時，該媒體應存放於安全設備或處所。

5.9.2 儲存媒體所使用之密碼或編碼技術不應透露予遞送人員或與業務無關之人員。

5.9.3 儲存媒體遞送前應加以妥善包裝保護，避免發生實體損壞。

5.9.4 儲存媒體如委由外部單位（例如：郵局或快遞公司）運送，應選擇具有信譽之廠商，並採取以下控制措施：

5.9.4.1 放置於上鎖之容器或以彌封方式處理。

5.9.4.2 當面送達並簽收。

5.9.4.3 資料內容應使用密碼保護。

5.9.5 該儲存媒體之報廢，請詳「資訊資產異動作業說明書」，且須經核准。

5.10 資料備份

5.10.1 各項系統設定檔、伺服器檔案及資料庫資料均應由各系統負責人員訂定備份週期，並依據週期執行系統排程或手動備份，備份狀況應記錄於「備份狀況紀錄表」。

5.10.2 應定期於測試主機上測試備份復原是否正確。

5.10.3 重要系統資料應考量建立異地備份機制。

5.11 安全稽核事項

5.11.1 對各項系統視需要留存系統最新參數設定檔。

5.11.2 系統管理、技術諮詢與機房操作人員工作應依職務與相關規定確實記錄其工作內容於「巡查紀錄表」內。

5.11.3 每月應檢視一次各設備中系統時間是否一致，並進行校正及同步作業。

5.11.4 系統稽核資料應依系統重要性進行備份保護作業，並由專人定期審核，系統管理者不得新增、刪除或修改稽核資料，審查週期不得超過 6 個月。

5.11.5 應定期查核技術符合性，進行弱點掃描或滲透測試，以確定資訊系統及網路環境符合安全實施標準。掃描週期如下：

5.11.5.1 每半年至少針對伺服器及網管設備執行一次。

5.11.5.2 當系統有重大變動時。

5.11.5.3 新系統上線前。

5.11.6 系統異常及安全事件記錄與分析，依據「矯正及預防管理程序書」辦理。

5.11.7 弱點掃瞄報告與修補作業

5.11.7.1 執行弱點掃描應產出弱點掃描報告，弱點掃描報告格式不拘，惟應包含下列內容：

5.11.7.1.1 弱點掃描檢測範圍。

5.11.7.1.2 弱點掃描檢測時程。

5.11.7.1.3 弱點風險等級說明。

5.11.7.1.4 安全弱點列表與建議修補措施。

5.11.7.2 掃描出之弱點應限期改善，並填寫「弱點處理報告單」，且於修補後進行複掃。

5.11.7.3 於安裝修正程式前，需先行測試並確認運作正常後，方可進行安裝。

5.11.8 殘餘弱點管理

5.11.8.1 弱點若因故無法修補，應於「弱點處理報告單」說明無法修補之原因與防禦因應方法。

6 相關文件

6.1 資訊安全政策

6.2 委外管理程序書

6.3 系統開發與維護程序書

6.4 安全事件管理程序書

6.5 資訊資產異動作業說明書

6.6 矯正及預防管理程序書

6.7 巡查紀錄表

6.8 防火牆設定變更申請表

6.9 弱點處理報告單

國立斗六高級中學

系統開發與維護

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目錄

1　目的

本程序書制訂之目的在於確保國立斗六高級中學（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 系統程式碼清冊

6.5 資料需求申請表

國立斗六高級中學

資通安全事件通報及應變管理程序

目錄

壹、 目的

國立斗六高級中學(以下簡稱本校)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：(05)5322039#161

(二)聯絡單位：資訊媒體組

(三)聯絡人：陳俊利

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；接獲本校所屬單位或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、 通報作業程序

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). 事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

委外廠商保密切結書

具保密切結廠商(人員)　　於民國　　年　　月　　日起於國立斗六高級中學執行「　　」業務(或專案)，因而知悉　貴校機密或任何不公開之文書、電子資料、圖畫、消息、物品或其他資訊，將恪遵保密規定，未經　貴校書面授權，不得以任何形式利用或洩漏、告知、交付、移轉予任何第三人；合約執行期間應配置適當有受過訓練取得資通安全證照的資通安全人員，若有違反資通安全相關規定或知悉發生資通安全事件，應立即通知貴校；合約結束後因業務得知或持有本校的相關資料應確實移交、刪除或銷毀，如有違誤願負法律上之責任。

此致

國立斗六高級中學

具切結書委外廠商(人員)：＿＿＿＿＿＿＿＿＿＿

身分證字號/護照號碼(人員)：＿＿＿＿＿＿＿＿＿＿

代　表　人(委外廠商)：＿＿＿＿＿＿＿＿＿＿

統 一 編 號：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

地　　址：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

中　　華　　民　　國　　年　　月　　日

國立斗六高級中學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點及風險評估	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。
	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。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	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。
	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。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	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。
	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	5.1 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。

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
變之程序及機制	5.2 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。
	5.3 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	10.1 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。
	10.2 是否追蹤過去缺失之改善情形？	□	□	□	有追蹤缺失改善之情形。
	10.3 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

國立斗六高級中學

內部稽核計畫

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要

目錄

1　主旨

為落實國立斗六高級中學（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：祕書

組員：教務主任、學務主任、總務主任、主任輔導教師、圖書館主任、人事

主任、會計主任

6 稽核時程；

6.1 每年度 9 月實施自我檢核，要求每位行政同仁自我檢核相關資安事項是否依規定辦理

6.2 配合本校內部控制計劃，每年度由各處室主任抽籤決定受稽核單位，由稽核小組成員針對分配處室進行相關事項的訪談和查核

7 稽核項目

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

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

8 稽核程序

8.1 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

8.2 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

8.3 改善及總結

- 資訊安全稽核小組報告發現之缺失事項
- 改善建議
- 稽核總結
- 提交資通安全管理審查會討論與問題澄清

9 附件

9.1 矯正與預防處理單

國立斗六高級中學稽核項目紀錄表

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：

資訊安全管理制度內部稽核報告

1　稽核目的

為落實及評估國立斗六高級中學（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：祕書

組員：教務主任、學務主任、總務主任、主任輔導教師、圖書館主任、人事主任、會計主任

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		資訊安全執行秘書	
日期	/　/	日期	/　/	日期	/　/

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="6">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>