國立臺東專科學校
資通安全維護計畫

目　　錄

壹、依據及目的

本計畫依據資通安全管理法第 10 條及施行細則第 6 條訂定。

貳、適用範圍

本計畫適用範圍除國立臺東專科學校圖書資訊中心(以下簡稱本中心)外，另包含 ISMS 組織內部人員、委外服務廠商與一般訪客適用。。

參、核心業務及重要性

本中心之核心業務及重要性如下表：

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間
校務行政	校務行政系統	核心資通系統	關鍵性業務流程受影響	8 小時
校務行政	虛擬系統	核心資通系統	關鍵性業務流程受影響	8 小時
網路服務	核心網路交換器	核心資通系統	關鍵性業務流程受影響	8 小時

肆、資通安全政策及目標

一、資通安全政策

為使本中心業務順利運作，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，確保機關業務持續營運。
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

高本中心同仁之資通安全意識，本中心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%)

2. 知悉資安事件發生，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。

三、資通安全政策及目標之核定程序

資通安全政策由本中心陳資訊安全長核定。

四、資通安全政策及目標之宣導

1. 本中心之資通安全政策及目標應每年透過教育訓練、內部會議等方式，向機關內所有人員進行宣導，並檢視執行成效。

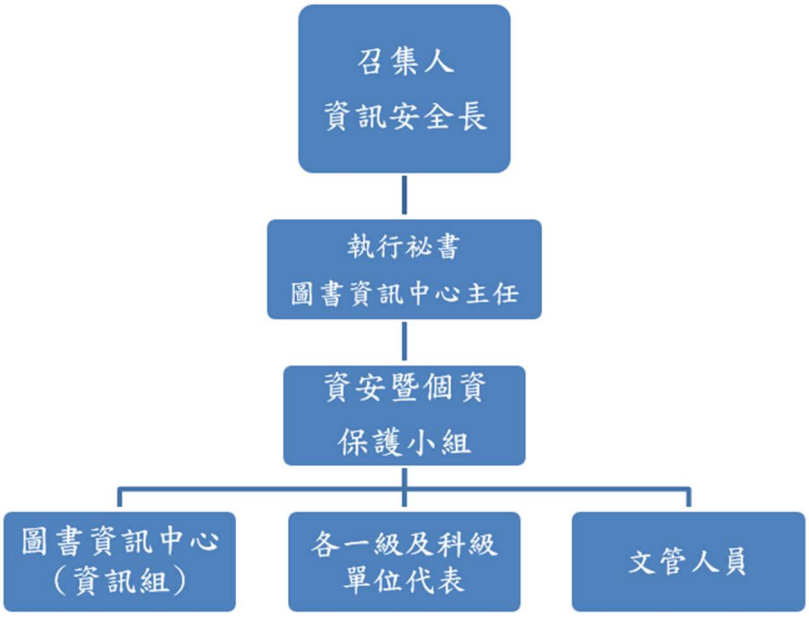
五、資通安全政策及目標定期檢討程序

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。

伍、資通安全推動組織

一、資訊安全暨個人資料保護推動委員會組織架構

本校之資訊安全暨個人資料保護推動委員會組織架構如下圖所示:



二、資訊安全暨個人資料保護推動委員會工作執掌

資訊安全暨個人資料保護推動委員會：為任務編組方式組成，由校長指派副校長擔任召集人；由副校長、一級行政單位及科級教學單位主管為當然委員，如因職務調動應即刻指派遞補人員與辦理交接，其任務包括：

1. 負責本中心資安暨個資保護之政策、目標、資源調度等統籌、協調與研議之整體資通安全維護任務。
2. 每年定期或視需要召開會議，審查資訊安全與個資保護相關事宜。
3. 視需要召開跨部門之資源協調會議，負責協調資訊安全與個資保護執行所需之相關資源分配。

(一) 資訊安全委員會召集人（以下簡稱召集人）：

1. 確保資訊安全政策與目標建立，且切合組織策略方向。
2. 確保整合 ISMS 要求於組織流程中。
3. 確保 ISMS 所需資源得以取用。

4. 溝通有效的 ISMS 與遵循 ISMS 要求的重要性。

5. 確保 ISMS 達成預定成效。

6. 指揮與支援人員貢獻於 ISMS 有效性。

7. 推動持續改善。

8. 支援其他管理角色來展現用於負責領域的領導性。

(二) 執行祕書:

由資訊安全委員會召集人指派圖書資訊中心主任擔任，其任務包括：

1. 負責資安暨個資保護管理制度之推動事宜。
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。
3. 對於資訊安全與個資保護作業之改善提出建議，以及協助執行資訊安全之自我檢核。
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。

(三) 資安暨個資保護小組:

由各一級及科級單位各推派 1 人代表組成，負責規劃資安暨個資保護作業：

1. 由圖書資訊中心主任擔任召集人。
2. 制定資訊安全與個資保護相關規範。
3. 推動資訊安全與個資保護相關活動。
4. 辦理資訊安全與個資保護相關教育訓練。
5. 建立風險管理制度，執行風險管理。
6. 建立資訊安全事件緊急應變暨復原措施。
7. 由圖書資訊中心執行資訊安全稽核作業。
8. 各一級及科級單位共同執行個資保護稽核作業。
9. 執行追蹤不符合事項之與矯正措施執行情形。

10. 研討新資訊安全產品或技術。

11. 執行資訊安全暨個人資料保護推動委員會決議事項。

12. 鑑別資訊安全與個資保護相關之法規。

(四) 指定專人擔任文管一職，負責所有文件管制與發行。

陸、專職(責)人力及經費配置

一、專職(責)人力及資源之配置

1. 本中心依資通安全責任等級分級辦法之規定，屬資通安全責任等級 C 級，最低應設置資通安全專職(責)人員 1 人，本中心現有資通安全專責人員名單及職掌應列冊，並適時更新。

2. 本中心之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升機關內資通安全專業人員之資通安全管理能力。本中心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. 資安專職(責)人員專業職能之培養(如證書、證照、培訓紀錄等)，應依據資通安全責任等級分級辦法之規定。

   (1) 資安專職(責)人員總計應持有 1 張以上資通安全專業證照。

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

4. 本中心負責重要資通系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽屬書面約定，並視需要實施人員輪調，建立人力備援制度。

5. 本中心之首長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。

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

二、經費之配置

1. 資安暨個資保護小組於規劃配置相關經費及資源時，應考量本中心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安暨個資保護小組提出，由資安暨個資保護小組視整體資通安全資源進行分配，並經資訊安全長核定後，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

1. 本中心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。

2. 資訊及資通系統資產項目如下，分為 7 類：人員、文件、軟體、通訊、硬體、資料、環境：

   (1) 人員（People / PE）：包含全體同仁，以及委外廠商。

   (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。

   (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。

   (4) 訊（Communication / CM）：網路設備及提供資訊傳輸與交換之線路或服務。

   (5) 硬體（Hardware / HW）：主機設備及相關硬體設施。

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

   (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。

3. 本中心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。

4. 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。

5. 各單位管理之資訊或資通系統如有異動，應即時通知資安暨個資保護小組更新資產清冊。

二、機關資通安全責任等級分級

依據資通安全責任等級分級辦法第 6 條，本校為 C 級單位。

捌、資通安全風險評估

一、資通安全風險評估

1. 本中心應每年針對資訊及資通系統資產進行風險評估。

2. 執行風險評估時應參考行政院國家資通安全會報頒布之最新「資訊系統風險評鑑參考指引」，並依其中之「詳細風險評鑑方法」進行風險評估之工作。

3. 本中心應每年依據資通安全責任等級分級辦法之規定，分別就機密性、完整性、可用性、法律遵循性等構面評估自行或委外開發之資通系統防護需求分級。

二、核心資通系統及最大可容忍中斷時間

核心資通系統	資訊資產	最大可容忍中斷時間	核心資通系統主要功能
校務行政	校務行政系統	8	核心資通系統
校務行政	虛擬系統	8	核心資通系統
網路服務	核心網路交換器	8	核心資通系統

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

本中心依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及核心資通系統之防護基準，採行相關之防護及控制措施，由於本中心核心資通系統已導入 ISO27001:2013 相關驗證，全機關之防護及控制措施詳如資通安全管理系統文件。

壹拾、資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，本中心應訂定資通安全事件通報、應變及演練相關機制，詳資通安全事件通報應變程序。

壹拾壹、資通安全情資之評估及因應

本中心接獲資通安全情資，應評估該情資之內容，並視其對本中心之影響、本中心可接受之風險及本中心之資源，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

本中心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

本中心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

由資安暨個資保護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

資安暨個資保護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

本中心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. 受託者應採取之其他資通安全相關維護措施。
5. 本中心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，以稽核或其他適當方式確認受託業務之執行情形。

壹拾參、資通安全教育訓練

一、資通安全教育訓練要求

1. 本中心依資通安全責任等級分級屬 C 級，資安及資訊人員每年至少 1 名人員接受 12 小時以上之資安專業課程訓練或資安職能訓練。
2. 本中心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. 承辦單位應於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全認知宣導及教育訓練計畫，以建立員工資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄。

2. 本中心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. 員工報到時，應使其充分瞭解本中心資通安全相關作業規範及其重要性。

4. 資通安全教育及訓練之政策，除適用所屬員工外，對機關外部的使用者，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

本中心所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法、國立臺東專科學校職員獎懲實施要點，及本中心各相關規定辦理之。

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，使本中心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，應與本中心之資通安全政策、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. 資安暨個資保護小組應定期(至少每年一次)或於系統重大變更或組織改造後執行一次內部稽核作業，以確認人員是否遵循本規

範與機關之管理程序要求，並有效實作及維持管理制度。

2. 辦理稽核前資安暨個資保護小組應擬定資通安全稽核計畫並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務、稽核方式、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，資安暨個資保護小組應於執行稽核前通知受稽核單位，並將稽核期程、稽核項目紀錄表及稽核流程等相關資訊提供受稽單位。

4. 本中心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稽核結果及改善報告中，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. 本中心之資安暨個資保護小組應每年至少一次召開資通安全管

理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。

2. 管理審查議題應包含下列討論事項：

(1) 過往管理審查議案之處理狀態。

(2) 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資安暨個資保護小組決議事項等。

(3) 資通安全維護計畫內容之適切性。

(4) 資通安全績效之回饋，包括：

A. 資通安全政策及目標之實施情形。

B. 資通安全人力及資源之配置之實施情形。

C. 資通安全防護及控制措施之實施情形。

D. 內外部稽核結果。

E. 不符合項目及矯正措施。

(5) 風險評鑑結果及風險處理計畫執行進度。

(6) 重大資通安全事件之處理及改善情形。

(7) 利害關係人之回饋。

(8) 持續改善之機會。

3. 持續改善機制之管理審查應做成改善績效追蹤報告，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

本中心應於每年 12 月前向上級或監督機關，提出資通安全維護計畫實施情形，使其得瞭解本中心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

17. 本中心資通安全事件通報及應變程序

二、附件表單

1. 資安暨個資保護小組成員及分工表

2. 資通安全保密同意書

3. 資通安全需求申請單

4. 資訊及資通系統資產清冊

5. 風險評估表

6. 風險類型暨風險對策參考表

7. 管制區域人員進出登記表

8. 委外廠商執行人員保密切結書、保密同意書

9. 委外廠商查核項目表

10. 年度資通安全教育訓練計畫

11. 資通安全認知宣導及教育訓練簽到表

12. 資通安全維護計畫實施情形

13. 資通安全稽核計畫

14. 稽核項目紀錄表

15. 稽核結果紀錄表

16. 稽核委員聘任同意保密切結書

17. 稽核結果及改善報告

18. 改善績效追蹤報告