臺東縣立鹿野國民中學

資通安全維護計畫

機密等級：一般

承辦人簽章：教師兼教學主任林彥仲

單位主管簽章：教師兼教學主任林彥仲

資安長簽章：臺東縣立鹿野國民中學校長李紹平

校長簽章：臺東縣立鹿野國民中學校長李紹平

資通安全維護計畫

目　　錄

壹、依據及目的 4
貳、適用範圍 4
參、核心業務及重要性 4
肆、資通安全政策及目標 6
一、資通安全政策 6
二、資通安全目標 6
三、資通安全政策及目標之核定程序 6
四、資通安全政策及目標之宣導 6
五、資通安全政策及目標定期檢討程序 6
伍、資通安全推動組織 6
一、資通安全長 6
二、資通安全推動組織 7
陸、專職(責)人力及經費配置 8
一、專職(責)人力及資源之配置 8
二、經費之配置 8
柒、資訊及資通系統之盤點 9
一、資訊及資通系統盤點 9
二、機關資通安全責任等級分級 9
捌、資通安全風險評估 9
一、資通安全風險評估 9
二、核心資通系統及最大可容忍中斷時間 10
玖、資通安全防護及控制措施 10
一、資訊及資通系統之管理 10
二、存取控制與加密機制管理 11
三、作業與通訊安全管理 122
四、業務持續運作演練 165

五、資通安全防護設備.....166
壹拾、資通安全事件通報、應變及演練相關機制..... 166
壹拾壹、資通安全情資之評估及因應..... 166
一、資通安全情資之分類評估.....166
二、資通安全情資之因應措施.....177
壹拾貳、資通系統或服務委外辦理之管理 188
壹拾參、資通安全教育訓練..... 18
一、資通安全教育訓練要求 18
二、資通安全教育訓練辦理方式 18
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... 19
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... 19
一、資通安全維護計畫之實施 19
二、資通安全維護計畫之持續精進及績效管理..... 19
壹拾陸、資通安全維護計畫實施情形之提出 200
壹拾柒、相關法規、程序及表單..... 200
一、相關法規及參考文件.....200
二、附件表單.....200

壹、依據及目的

本計畫依據下列法規訂定：

一、 資通安全管理法第10條及其施行細則第6條。

二、 臺東縣政府資訊安全政策。

三、 其他相關業務法規名稱。

貳、適用範圍

本計畫適用範圍涵蓋臺東縣立鹿野國民中學（以下簡稱本機關）。

參、核心業務及重要性

一、核心業務及重要性：

(一)本機關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
教務業務：課程發展、課程編排、教學實施、學籍管理、成績評量、教學設備、教具圖書資料供應、教學研究及教學評鑑，並與輔導單位配合實施教育輔導等事項	國中學籍系統（向上集中） 國中成績系統（向上集中）	為本機關依組織法執掌，足認為重要者。	可能使本校部分業務中斷	由上級管理單位訂之
學生事務：公民教育、道德教育、生活教育、體育衛生保健、學生團體活動及生活管理，並與輔導單位配合實施生活輔導等事項。	國中學務系統（向上集中）	為本機關依組織法執掌，足認為重要者。	可能使本校部分業務中斷	由上級管理單位訂之
總務業務：學校文書、事務及出納等事項	公文系統（向上集中）	為本機關依組織法執掌，足認為重要者。	可能使本校部分業務中斷	由上級管理單位訂之
輔導業務：學生資料蒐集與分析、學生智力、	國中輔導心測系統(向上集中)	為本機關依組織法執掌，足認為	可能使本校部分業務中	由上級管理單

性向、人格等測驗之實施，學生興趣、學習成就與志願之調查、輔導諮商之進行，並辦理特殊教育及親職教育等事項。		重要者。	斷	位訂之

(二)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：該項核心業務所必須使用之資通系統名稱。

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：該項業務使用之系統失效後，機關業務運作有何影響。

5. 最大可容忍中斷時間單位以小時計(對外服務以小時，對內服務以工作小時計)。

二、 非核心業務及說明：

(一)本機關之非核心業務及說明如下表：

非核心業務	業務失效影響說明	最大可容忍中斷時間
學校首頁(向上集中)	可能使本校部分業務中斷	由上級管理單位訂之

(二)各欄位定義：

1. 非核心業務系統：公務機關非核心業務相關之資通系統，如差勤服務、郵件服務、用戶端服務等。(請依機關實際情形列出)

2. 業務失效影響說明：該項業務使用之系統失效後，機關業務運作有何影響。

3. 最大可容忍中斷時間單位以小時計(對外服務以小

時，對內服務以工作小時計)。

肆、資通安全政策及目標

一、資通安全政策

為使本機關業務順利運作，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：

(一)安全：確保資訊不遭竊取、竄改、滅失或遺漏。

(二)正確：資訊內容及處理過程精準無誤。

(三)迅速：對資安事件之處理、通報與回復能快速完成。

二、資通安全目標

(一)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。

(二)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。

三、資通安全政策及目標之核定程序

資通安全政策由本機關簽陳資通安全長核定。

四、資通安全政策及目標之宣導

本機關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，向機關內所有人員進行宣導。

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、資通安全長

依本法第11條之規定，本機關擇請_校長___兼任本機關資通安全長，負責督導機關資通安全相關事項，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、資通安全推動組織

(一)本機關設置「資通安全推動小組」負責督導機關資通安全相關事項，為推動本機關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，由資通安全長召集人員代表成立資通安全推動小組，其任務宜包括：

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

1. 本機關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，本機關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。

2. 資通安全推動小組，其工作內容得參考下列事項：

(1) 資通安全政策及目標之研議。

(2) 訂定機關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機關年度工作計畫。

(4) 傳達機關資通安全政策與目標。

(5) 其他資通安全事項之規劃。

(6) 資通安全相關規章與程序、制度之執行。

(7) 資訊盤點及風險評估。

(8) 資料安全防護事項之執行。

(9) 資通安全事件之通報及應變機制之執行。

(10) 其他資通安全事項之辦理與推動。

陸、專職(責)人力及經費配置

一、專職(責)人力及資源之配置

(一) 本機關依資通安全責任等級分級辦法之規定，屬資通安全責任等級D級，其分工如下。

1. 資通安全認知與訓練業務，負責推動資通安全教育訓練等業務之推動。

2. 資通安全防護業務，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。

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

(二) 本機關之承辦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。

(三) 本機關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。

(四) 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

(一) 資通安全推動小組於規劃配置相關經費及資源時，應考量本機關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。

(二)各單位如有資通安全相關設備之需求，可向上級機關提出相關申請，由上級機關審核申請需求及相關資源來決議。

(三)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

(一)本機關每年辦理資訊資產盤點，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機關內部之支援服務，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。

二、機關資通安全責任等級分級

本機關自行辦理資通業務，未維運自行或委外開發之資通系統者，其資通安全責任等級為D級。

捌、資通安全風險評估

一、資通安全風險評估

(一)本機關應每年針對資訊及資通系統資產進行風險評估，若配合資訊資源向上集中計畫，資訊系統由上級或監督機關兼辦或代管，則不需進行。

(二)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。

(三)本機關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

本機關配合資訊資源向上集中計畫，核心資訊系統均由上級或監督機關兼辦或代管，不再另行訂定。

玖、資通安全防護及控制措施

本機關依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項，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

(一)資訊保管

1. 資訊管理人應確保資訊已盤點造冊並適切分級，並持續更新以確保其正確性。

2. 資訊管理人應確保資訊被妥善的保存或備份。

3. 資訊管理人應確保重要之資訊已採取適當之存取控制政策。

(二)資訊及資通系統之使用

1. 本機關同仁使用資訊及資通系統前應經其管理人授權。

2. 本機關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. 本機關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. 非本機關同仁使用本機關之資訊及資通系統，應確實遵守本機關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)資訊之刪除或汰除

1. 資訊之刪除或汰除前應評估機關是否已無需使用該等資訊，或該等資訊是否已妥善移轉或備份。

2. 資訊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，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。

二、存取控制與加密機制管理

(一)網路安全控管

1. 本機關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。若為向上集中管理，則由上級單位統一辦理更新與升級。

2. 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。

3. 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。

4. 無線網路防護

(1)機密資料原則不得透過無線網路及設備存取、處理或傳送。

(2)無線設備應具備安全防護機制以降低阻斷式攻擊風險，且無線網路之安全防護機制應包含外來威脅及預防內部潛在干擾。

(3)行動通訊或紅外線傳輸等無線設備原則不得攜入涉及或處理機密資料之區域。

(4)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)加密管理

1. 本機關之機密資訊於儲存或傳輸時應進行加密。

2. 本機關之加密保護措施應遵守下列規定：

(1) 應避免留存解密資訊。

(2) 一旦加密資訊具遭破解跡象，應立即更改之。

三、作業與通訊安全管理

(一)防範惡意軟體之控制措施

1. 本機關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。

4. 設備管理者應定期進行作業系統及軟體更新，以避免惡意軟體利用系統或軟體漏洞進行攻擊。

(二)遠距工作之安全措施

1. 本機關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。

(三)電子郵件安全管理

1. 本機關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. 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，若為向上集中管理，則由上級單位統一辦理。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。

4. 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。

5. 使用者不得利用機關所提供電子郵件服務從事侵害他人權益或違法之行為。

6. 使用者應確保電子郵件傳送時之傳遞正確性。

7. 使用者使用電子郵件時，應注意電子簽章之要求事項。

8. 本機關應配合上級機關舉辦電子郵件社交工程演練，並檢討執行情形。

(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(有機房之機關參考)

(1) 資料中心及電腦機房應進行實體隔離。

(2) 機關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) 機關人員應隨時注意身分不明或可疑人員。

(4) 僅於必要時，得准許外部支援人員進入資料中心及電腦機房。

(5) 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(有機房之機關參考)

(1) 資料中心及電腦機房應安裝之安全偵測及防護措施，如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。

(2) 各項安全設備應定期執行檢查、維修。

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) 文件及可移除式媒體在不使用或不上班時，應存放在櫃子內。

(3) 機密性及敏感性資訊，不使用或下班時應該上鎖。

(4) 機密資訊或處理機密資訊之資通系統應避免存放或設置於公眾可接觸之場域。

(5) 顯示存放機密資訊或具處理機密資訊之資通系統地點之通訊錄及內部人員電話簿，不宜讓未經授權者輕易取得。

(6) 資訊或資通系統相關設備，未經管理人授權，不得被帶離辦公室。

(五) 資料備份

1. 重要資料應進行資料備份，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. 資訊如以實體儲存媒體方式傳送，應留意實體儲存媒體之包裝，選擇適當人員進行傳送，並應保留傳送及簽收之記錄。

3. 為降低媒體劣化之風險，宜於所儲存資訊因相關原因而無法讀取前，將其傳送至其他媒體。

4. 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. 禁止私自安裝點對點檔案分享軟體及未經合法授權軟體。

3. 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。

4. 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。

5. 下班時應關閉電腦及螢幕電源。

6. 如發現資安問題，應主動循機關之通報程序通報。

7. 支援資訊作業的相關設施如影印機、傳真機等，應安置在適當地點，以降低未經授權之人員進入管制區的風險，及減少敏感性資訊遭破解或洩漏之機會。

(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機關內部公務訊息，其內容不得涉及機密資料。但有業務需求者，應使用經專責機關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宜考量下列安全性需求：

(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。

四、業務持續運作演練

本機關為D級機關無需針對核心資通系統制定業務持續運作計畫與演練。

五、資通安全防護設備

(一) 本機關應建置防毒軟體、防火牆，如有設置電子郵件伺服器應建立電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。前項之防火牆、電子郵件伺服器若為向上集中管理，則由上級單位統一辦理更新與升級。

(二) 資安設備設定異動應保留相關修改紀錄，並定期檢討執行情形。

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

壹拾壹、資通安全情資之評估及因應

本機關接獲資通安全情資，應評估該情資之內容，並視其對本機關之影響、本機關可接受之風險及本機關之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

一、資通安全情資之分類評估

本機關接受資通安全情資後，應指定人員進行情資分析，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

本機關於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

(一)資通安全相關之訊息情資

由資通安全推動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

由經指派之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

資通安全推動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

本機關委外辦理資通系統之建置、維運或資通服務之提供時，可由上級機關認證後，考量其之專業能力與經驗、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。

壹拾參、資通安全教育訓練

一、資通安全教育訓練要求

本機關依資通安全責任等級分級屬D級，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

(一)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。

(二)本機關資通安全認知宣導及教育訓練之內容得包含：

1. 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等)。

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。

(三)員工報到時，應使其充分瞭解本機關資通安全相關作業規範及其重要性。

(四)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

本機關所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法，及本機關各相關規定辦理之。

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，使本機關之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本機關之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

二、資通安全維護計畫之持續精進及績效管理

(一)本機關之資通安全推動小組應每年定期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。

(二)管理審查議題應包含下列討論事項：

1. 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。

2. 資通安全維護計畫內容之適切性。

3. 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. 不符合項目及矯正措施。

4. 風險評鑑結果及風險處理計畫執行進度。

5. 重大資通安全事件之處理及改善情形。

6. 利害關係人之回饋。

7. 持續改善之機會。

(三)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

本機關依據本法第12條之規定，應於次年向上級或監督機關，提出上年度資通安全維護計畫實施情形，使其得瞭解本機關上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

(一)本機關資通安全事件通報及應變程序

二、 附件表單

(一)資通安全推動小組成員及分工表

(二)資通安全保密同意書

(三)管制區域人員進出登記表

(四)委外廠商執行人員保密切結書、保密同意書

(五)年度資通安全教育訓練計畫

(六)資通安全認知宣導及教育訓練簽到表

(七)資通安全維護計畫實施情形

(八) 審查結果及改善報告

(九)改善績效追蹤報告

臺東縣立鹿野國民中學
資通安全維護計畫範本參考附件

目　次

1. 資通安全推動小組成員及分工表 1
2. 資通安全保密同意書 2
3. 管制區域人員進出登記表 3
4. 委外廠商執行人員保密切結書、保密同意書 4
5. 年度資通安全教育訓練計畫 6
6. 資通安全認知宣導及教育訓練簽到表 8
7. 資通安全維護計畫實施情形 9
8. 審查結果及改善報告 12
9. 改善績效追蹤報告 13

1. 資通安全推動小組成員及分工表

鹿野國民中學資通安全推動小組成員及分工表

編號：

製表日期：　　年　月　日

單位職級	名稱	職掌事項	分機	備註 （代理人）
教導主任	林彥仲	資通安全事件通報	231	楊淑如

資通安全長：李紹平

註：陳核層級請機關依需求調整

2. 資通安全保密同意書

台東縣立鹿野國民中學資通安全保密同意書

編號：

立同意書人_____於民國_____年____月____日起於_____任職，因業務涉及單位重要之資訊及資通系統，故同意下列保密事項：

一、於業務上所知悉之機敏資料及運用之資通系統等，應善盡保管及保密之責。

二、相關業務之資訊、文件，不得私自洩漏與業務無關之人員。

三、遵守其他本單位資通安全相關之法令及規定。

四、如有危害本單位資通安全之行為，願負相關之責任。

立同意書人：_____(簽章)

身份證字號：_____

服務機關：_____

機關首長：_____

中　華　民　國　　年　　月　　日

3. 管制區域人員進出登記表

台東縣立鹿野國民中學管制區域人員進出登記表

編號：

製表日期：　年　　月　　日

編號	姓名	單位	配同人員	日期	進入時間	離開時間	事由	權限	進出設備	攜帶物品
1 (範本)	陳○○	○○室	李○○	106.3.1	8：00	9：00	借用電腦設備	普	手提電腦	手機

承辦人員：　　單位主管：

註：陳核層級請機關依需求調整

4. 委外廠商執行人員保密切結書、保密同意書

台東縣立鹿野國民中學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_____（機關名稱，以下稱機關）處理業務，謹聲明恪遵機關下列工作規定，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，非經機關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，不得私自將機關之資訊設備、媒體檔案及公務文書攜出。

二、 未經機關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機關網路。若經申請獲准連接機關網路，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機關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機關配發之個人電腦與週邊設備，並僅開放使用機關內部網路。若因業務需要使用機關電子郵件、目錄服務，應經機關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機關業務相關人員之確認並代為申請核准。

五、 機關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	聯絡電話及戶籍地址
_____	_____	_____

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	廠商聯絡電話及地址
_____	_____	_____

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（以授課時需連結機關網路者為限）及經常到機關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機關洽公之業務人員每年簽署本切結書乙次。

中　華　民　國　　年　　月　　日

台東縣立鹿野國民中學委外廠商執行人員保密同意書

茲緣於簽署人 ----------（簽署人姓名，以下稱簽署人）參與----------（廠商名稱，以下稱廠商）得標----------（機關名稱）（以下稱機關）資通業務委外案----------（案名）（以下稱「本案」），於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

第一條　簽署人承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至機關或機關所指定處所以外之處所。

第二條　簽署人知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員。

第三條　簽署人在下述情況下解除其所應負之保密義務：

原負保密義務之資訊，由機關提供以前，已合法持有或已知且無保密必要者。

原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所知之資訊。

原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。

第四條　簽署人若違反本同意書之規定，機關得請求簽署人及其任職之廠商賠償機關因此所受之損害及追究簽署人洩密之刑責，如因而致第三人受有損害者，簽署人及其任職之廠商亦應負賠償責任。

第五條　簽署人因本同意書所負之保密義務，不因離職或其他原因不參與本案而失其效力。

第六條　本同意書一式叁份，機關、簽署人及----------（廠商）各執存一份。

簽署人姓名及簽章：

身分證字號：

聯絡電話：

戶籍地址：

所屬廠商名稱及蓋章：

所屬廠商負責人姓名及簽章：

所屬廠商地址：

中　華　民　國　　年　　月　　日

5. 年度資通安全教育訓練計畫

台東縣立鹿野國民中學_____年度資通安全教育訓練計畫

壹、依據

台東縣立鹿野國民中學之資通安全維護計畫辦理。

貳、目的

為精進所屬人員之資通安全意識及職能，並敦促該等人員得以瞭解並執行（本機關）之資通安全維護計畫，以強化（本機關）之資通安全管理能量，爰要求該等人員應接受資通安全之教育訓練，爰擬定本教育訓練計畫。

參、實施範圍（各機關自行定義）

本機關所屬人員：

人員類別	人數
資通安全專責人員	1
一般人員	5
主管人員	2
共計	8

肆、訓練項目（各機關自行定義）

人員類別	訓練課程[1]	時數
資通安全專責人員	電子郵件安全	
資訊人員	資訊系統風險管理	
一般人員	資訊安全通識	
主管人員	資訊系統風險管理	

[1] 可參考行政院國家資通安全會報技術服務中心之資安職能課程項目，網址：https://www.nccst.nat.gov.tw/Capacity?lang=zh

伍、訓練期程（各機關自行定義）

由各機關自行排定教育訓練期程。

陸、訓練方式（各機關自行定義）

由各機關自行決定教育訓練方式(實體課程、線上課程...)。

6. 資通安全認知宣導及教育訓練簽到表

台東縣立鹿野國民中學資通安全認知宣導及教育訓練簽到表

編號：

課程名稱：資安宣導課程-案例分享、資安防護重點及社交工程等

時　　間：　年　月　日　　－

地　　點：

單　位	職　稱	姓　名	簽　名

7. 資通安全維護計畫實施情形

台東縣立鹿野國民中學資通安全維護計畫實施情形

編號：

本機關經主管機關核定後本機關之資通安全責任等級為 D 級，依資通安全管理法第 12 條之規定，向上級機關提出本○○○年度資通安全維護計畫實施情形、執行成果及相關說明如下表所示：

實施項目	實施內容	實施情形說明 （下列內容為範例，請機關依自身情形填寫對應的說明，並提供證明，如計畫、程序、記錄或相關公文等）
1. 核心業務及其重要性	1.1 核心業務及重要性盤點	本機關核心業務及重要性詳參資通安全維護計畫（詳附件，下同）。
2. 資通安全政策及目標之訂定	2.1 資通安全政策訂定及核定	本機關已訂定資通安全政策，詳參資通安全維護計畫，並經資安長核定(詳公文附件)。
	2.2 資通安全目標之訂定	本機關已訂定資通安全目標，詳參資通安全維護計畫。
	2.3 資通安全政策及目標宣導	本機關為推動資通安全政策，已定期向同仁及利害關係人進行宣達。
	2.4 資通安全政策及目標定期檢視	本機關已定期召開資通安全管理審查會議中檢討資通安全政策及目標之適切性 (詳會議記錄) 。
3. 設置資通安全推動組織	3.1 設定資通安全長	本機關已指定○○長為資通安全長，其職掌詳參資通安全維護計畫。
	3.2 設置資通安全推動小組	本機關已設置資通安全推動小組，其組織、分工及職常詳參資通安全維護計畫。
4. 專責人力及經費之配置	4.1 專職(責)人員配置	本機關依規定配置資通安全專職人員四人，並具備資通安全專業證照及資通安全職能評量證書各四張。另因其業務內容將涉及機密性資料，故已進行相關安全評估。
	4.2 經費之配置	本機關今年視需求已合理分資安經費，資安經費佔資訊經費之○○%。

5. 資訊及資通系統之盤點及核心資通系統、相關資產之標示	5.1 資訊及資通系統之盤點	本機關已於今年○月盤點本機關之資訊、資通系統，建立資產目錄。
	5.2 機關資通安全責任等級分級	本機關依資通安全責任等級分級辦法，為資通安全責任等級 A 級機關。
6. 資通安全風險評估	6.1 資通安全風險評估	本機關已於今年○月完成本機關之資訊、資通系統及相關資產之風險分析評估及處理。
	6.2 資通安全風險之因應	本機關已依資通安全風險評估之結果擬定對應之資通安全防護及控制措施。
7. 資通安全防護及控制措施	7.1 資通安全防護及控制措施	本機關已依依安全維護計畫辦理，詳附件資料。
	7.1 資訊及通系統之保管	本機關已依依安全維護計畫辦理，詳附件資料。
	7.2 存取控制與加密機制管理	本機關已依依安全維護計畫辦理。
	7.3 作業及通訊安全管理	本機關已依依安全維護計畫辦理。
	7.4 系統獲取、開發及維護	本機關已依依安全維護計畫辦理。
	7.5 執行資通安全健診	本機關已依依安全維護計畫辦理。
8. 資通安全事件通報、應變及演練相關機制	8.1 訂定資通安全事件通報、應變及演練相關機制	本機關已依規定訂定資通安全事件通報應變程序。(詳附件)
	8.2 資通安全事件通報、應變及演練	本機關已依規定進行資通安全事件通報。 本機關已依規定於今年○、○月辦理社交工程演練，並於○月辦理通報應變演練。
9. 資通安全情資之評估及因應機制	9.1 資通安全情資之分類評估	本機關接受情資後，已進行分類評估。
	9.2 資通安全情資之因應措施	本機關已接受情資之分類，採取對應之因應措施。
10. 資通系統或服務委外辦理之管理	10.1 選任受託者應注意事項	本機關資通系統或服務委外辦理時，已將選任受託者應注意事項加入招標文件中。
	10.2 監督受託者資通安全維護情形應注意事項	本機關已依規定監督受託者資通安全維護情形，客製他資通系統開發者，已要求其出具安全性檢測證明....(請機關依實際情形列出)。

11. 資通安全教育訓練	11.1 資通安全教育訓練要求	本機關人員已規定進行資通安全教育訓練。
	11.2 辦理資通安全教育訓練	本機關已於今年○月辦理資通安全教育訓練。
12. 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	12.1 訂定考核機制並進行考核	本機關已建立考核機制，並已依規定進行平時及年終考核。
13. 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	13.1 資通安全維護計畫之實施	本機關已依規定訂定各階文件、流程、程序或控制措施，據以實施並保存相關之執行成果記錄。
	13.2 資通安全維護計畫實施情形之稽核機制	本機關已依規定辦理內部稽核。
	13.3 資通安全維護計畫之持續精進及績效管理	本機關已依規定辦理內部召開管理審查會議，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。
其他說明		

承辦人：　　單位主管：　　資通安全長：

註：陳核層級請機關依需求調整

8. 審查結果及改善報告

臺東縣立鹿野國民中學審查結果及改善報告

範圍	全機關			
日期	107 年 ○○ 月 ○○ 日			
審查日期	107 年 ○○ 月 ○○ 日			
項目				
編號	建議或待改善項目	改善措施	改善期程規劃	相關佐證資料
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				

9. 改善績效追蹤報告

臺東縣立鹿野國民中學改善績效追蹤報告

編號：○○

製表日期：○○○年○○月○○日

審查發現			
審查日期	107 年 10 月 20 日 08 時	受審查單位	○○○
審查區域	■ 電腦機房　委外業務之監督措施　自動備份系統之安全措施		
建議或待改善項目與內容	待改善項目：電腦機房所設置之預備電源設備老舊。 建議項目：委外廠商未定期為保養相關設備。		
影響範圍評估	將影響電腦機房之運作及相關非核心系統之線上服務之提供。		
發生原因分析	未落實監督委外廠商管理之責任。		

改善措施成效追蹤			
改善措施		預計成效	執行情況
管理面	定期進行委外廠商承辦人員之教育訓練，已落實對委外廠商之監督責任。	要求委外廠商每季進行保養，並提供相關保養紀錄。	已與委外廠商接洽。
技術面			
人力面			
資源面	更新相關電腦	電腦機房電源設備更新，並採用不斷電	已進行採購作業。

	機房設備，並確保備份設備及機制運作效果。	系統，於停電時可維持 12 小時運作。	
作業程序			
其他			

績效管考			
改善措施確認	■合格／完成 □待追蹤(追蹤期限：_____年_____月_____日) □不合格(說明：_____)		
經費需求或編列執行金額	○○○萬元。	經費執行情形	已進行相關電腦機房設備更新採購，共執行○○萬元。
預定完成日期	107 年 12 月 20 日	實際完成日期	107 年 12 月 20 日
完成進度或情形說明	定期檢視委外廠商之監督維護責任。		
改善成效考核			
後續成效追蹤			
資通安全推動小組承辦人員	○○○	機關首長(或資通安全管理代表)	○○○

註：陳核層級請學校依需求調整