國立嘉義特殊教育學校
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嘉義特殊教育學校全校（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	管理單位
學務、教務、輔導業務	教育部特殊教育通報網(連外部系統網站)	為本校依組織職掌，足認為重要者。	影響校務運作	24小時	上級主管機關

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. 管理單位：實際管理單位。

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
學校網頁主機和DNS Server	學校網站無法公布學校資訊與訊息	48小時
公文交換	電子公文無法及時送達機關，影響機關行政效率	48小時
人事室業務	影響人事業務進行	48小時
主計室業務	影響主計業務進行	48小時
薪資系統	影響機關行政效率	48小時

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。

肆、資通安全政策及目標

一、 資通安全政策

為確保本校所屬之資訊資產的機密性、完整性、可用性及符合相關法規之要求，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。

二、 資通安全目標

1. 資安事件發生時，能於規定的時間，完成通報、應變及復原作要。
2. 因應法令與技術之變動調整資通安全維護計畫內容，避免資通系統或資訊遭受未經授權侵害，以確保其機密性、完整性及可用性。
3. 達成資通安全責任等級分級要求，並降低遭受資通安全風險之威脅。

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。

一、 資通安全長

依本法第11條之規定，本校由校長為資通安全長，負責督導機關資通安全相關事項，其任務包括：

1. 資通安全管理政策及目標之核定、核轉及督導。
2. 資通安全責任之分配及協調。
3. 資通安全資源分配。
4. 資通安全防護措施之監督。
5. 資通安全事件之檢討及監督。
6. 資通安全相關規章、程序與制度文件核定。
7. 資通安全維護計畫之核定。

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、學部代表與相關業務人員成立資通安全推動小組，其任務包括：

1. 跨業務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. 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、程序與制度文件，並確保相關規章、程序與制度合乎法令及契約之要求。
3. 傳達本校資通安全政策與目標。

4. 資通安全相關規章、程序與制度之執行。

5. 資料及資通系統之安全防護事項之執行

6. 資通安全事件之通報及應變機制之執行。

7. 其他資通安全事項之規劃與推動。

8. 每年至少召開 1 次會議，確認資通安全事項執行情形。

陸、專責人力及經費配置

一、專責人力及資源之配置

(一)本校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，最低應設置資通安全兼辦人員 1 人，其分工如下，本機關現有資通安全專責人員名單及職掌應列冊，並適時更新。

1. 負責推動內部資通安全稽核及教育訓練等業務之推動。

2. 負責資通安全防護設施建置、資通安全事件通報及應變業務之推動。

(二)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，並提升機關內資通安全專業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，得洽請縣政府資管科、相關學者專家或專業機關（構）提供顧問諮詢服務。

(三)本校負責重要資通設備之管理、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。

(四)本校之首長及各業務人員，應負責所屬業務資料之資通安全作業，防範不法及不當行為。

(五)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. 各單位如有資通安全資源之需求，應配合本校預算規劃期程向資通安

全小組提出，由資通安全推動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。

3. 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、資通安全防護及控制措施

本校依據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、 存取控制與加密機制管理

(一)網路安全控管

1. 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。

2. 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。

3. 本機關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。

4. 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。

5. 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) 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。

(3) 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 6 碼以上。

(2) 通行碼複雜度應包含英文、數字二種以上。

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. 使用者若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。

二、 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。

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)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. 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。

3. 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。

4. 使用者應確保電子郵件傳送時之傳遞正確性。

(三)確保實體與環境安全措施

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. 具有機密性或敏感性資訊的文件及可移除式媒體在不使用或不上班時，應妥善存放。

3. 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。

4. 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。

5. 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。

(四)電腦使用之安全管理

1. 電腦超過 30 分鐘不使用時，應啟動螢幕保護功能。

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. 如發現資安問題，應主動循機關之通報程序通報。

(五)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

捌、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，詳見本校「資通安全事件通報應變程序」。

玖、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。

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。

壹拾、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，格式如附件表單(二)。

壹拾壹、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。

壹拾貳、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及本校相關規定辦理之。

壹拾參、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」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」，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. 本校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。

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。

壹拾肆、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，使其得瞭解本校之年度資通安全計畫實施情形。

壹拾伍、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

二、附件資料表單

(一)：資訊安全推動小組成員及分工表
(二)：資訊安全保密同意書
(三)：資訊安全需求申請表
(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)：資通安全稽核計畫
(九)：稽核項目紀錄表
(十)：稽核結果及改善報告
(十一)：改善績效追蹤報告