新北市五股區成州國民小學

資通安全維護計畫

機密等級：一般

承辦人簽章：教師兼資訊組長蔡靖萱

單位主管簽章：教師兼教務主任蘇建誠

校長(資安長)簽章：成州國小校長王淑玲

中華民國 108 年 05 月 20 日
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。

貳、適用範圍

本計畫適用範圍涵蓋新北市五股區成州國民小學(及附設幼兒園)。

參、核心業務及重要性

一、 資通業務及重要性：

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	校務行政系統	為本校依組織法執掌，足認為重要者	影響學校部分教學業務運作	1 個工作天
學生事務業務	校務行政系統	為本校依組織法執掌，足認為重要者	影響學校部分教學業務運作	1 個工作天
總務業務	校務行政系統	為本校依組織法執掌，足認為重要者	影響學校部分教學業務運作	1 個工作天
輔導業務	校務行政系統	為本校依組織法執掌，足認為重要者	影響學校部分教學業務運作	1 個工作天
幼教業務	校務行政系統	為本校依組織法執掌，足認為重要者	影響學校部分教學業務運作	1 個工作天

二、 非核心業務及說明：

非核心業務及說明如下表:

非核心業務	非核心資通系統	業務失效影響說明	最大可容忍中斷時間
人事業務	行政院人事行政總處人事服務網	人事部份業務無法運作	3 個工作天
會計業務	地方教育發展基金會計資訊系統	會計部分業務無法運作	3 個工作天
資訊組業務	校園網站	對外公告資訊無法運作	3 個工作天
出納組業務	薪資管理系統	出納部分業務無法運作	3 個工作天

肆、資通安全政策及目標

一、資通安全政策

為使本校業務順利運作，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. 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. 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. 因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高本校同仁之資通安全意識，本校同仁亦應確實參與訓練。
4. 針對辦理資通安全業務有功人員應進行獎勵。
5. 勿開啟來路不明或無法明確辨識寄件人之電子郵件。
6. 禁止多人共用單一資通系統帳號。
7. 校內同仁及外部廠商須簽屬相關資通安全保密切結與同意書。

二、資通安全目標

(一)量化型目標

1. 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。
2. 校園電腦防毒軟體100%啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
3. 每人每年接受三小時以上之一般資通安全教育訓練。

(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、防止發生中毒或入侵事件。

三、資通安全政策及目標之核定程序

資通安全政策由本校校長核定並公告之。

四、資通安全政策及目標之宣導

1. 本校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，向所有人員進行宣導，並檢視執行成效。

2. 本校應每年進行資安政策及目標宣導，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

依資通安全法第 11 條之規定，本校訂定校（園）長為資通安全管理代表，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. 資通安全相關規章與程序、制度文件核定。

7. 資通安全管理年度工作計畫之核定

8. 資通安全相關工作事項督導及績效管理。

9. 其他資通安全事項之核定。

二、資通安全推動小組

(一)組織

本校設置「資通安全推動小組」負責督導校內資訊安全相關事項，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，由資通安全管理代表召集各業務人員代表成立資通安全推動小組，其任務包括：

1. 跨處室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下列分工進行責任分組，並依資通安全管理代表指示負責下列事項，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. 資通安全推動小組：

(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年度工作計畫。

(4) 傳達資通安全政策與目標。

(5) 其他資通安全事項之規劃。

(6) 資訊及資通系統之盤點及風險評估。

(7) 資通安全相關規章與程序、制度之執行。

(8) 資料及資通系統之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) 每年得須參加縣市辦理之相關資訊安全研習。

陸、專責人力及經費配置

一、專責人力及資源之配置

1. 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，本校現有資通安全人員名單及職掌應列冊，並適時更新。

2. 本校之承辦單位於辦理資通安全業務時，應加強資通安全人員之培訓，並提升校內資通安全專業人員之資通安全管理能力。如資通安全人力或經驗不足，得洽請新北市教育局(處)或相關專業機關（構）之人員，提供顧問諮詢服務。

3. 本校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。

4. 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. 資通安全推動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. 校內如有資通安全資源之需求，應向上級機關提出申請，由上級機關審核後，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、資訊及資通系統之盤點

一、資訊及資通系統盤點

1. 本校每年辦理資訊及資通系統資產盤點，依管理責任及使用人員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：

(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：校內各項資訊系統與設備使用人員清冊，以及委外廠商駐點人員清冊等。

(6) 資料資產：以紙本形式儲存之資訊，如程序、清單、計畫、報告、指引手冊、政策、公文、作業紀錄、作業規範、各種應用系統文件及管理手冊，契約、法律文件、軟體使用授權等等。

二、機關資通安全責任等級分級

依據教育部臺教資(四)字第 1070202157 號函文，本校為公立高級中等以下學校，且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，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

本校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、資通安全風險之因應

本校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

(一)資訊及資通系統之保管

1. 資訊及資通系統管理人應確保資訊及資通系統已盤點造冊並適切分級，並持續更新以確保其正確性。
2. 資訊及資通系統管理人應確保資訊及資通系統被妥善的保存或備份。
3. 資訊及資通系統管理人應確保重要之資訊及資通系統已採取適當之存取控制政策。

(二)資訊及資通系統之使用

1. 本校同仁使用資訊及資通系統前應經其管理人授權。
2. 本校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. 非本校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)資訊及資通系統之刪除或汰除

1. 資訊及資通系統之刪除或汰除前應評估機關是否已無需使用該等資訊及資通系統，或該等資訊及資通系統是否已妥善移轉或備份。

2. 資訊及資通系統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. 具機敏性之資訊或具授權軟體之資通系統，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. 網路區域劃分如下：

(1) 外部網路：對外網路區域，連接外部廣網路(Wide Area Network, WAN)。

(2) 內部區域網路 (Local Area Network, LAN) ：機關內部單位人員及內部伺服器使用之網路區段。

2. 外部網路及內部區域網路間連線需經防火牆進行存取控制，非允許的服務與來源不能進入其他區域。

3. 本校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。

4. 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。

5. 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。

6. 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) 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. 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 8 碼以上。

(2) 通行碼複雜度應包含英文大寫小寫、特殊符號或數字三種以上。

(3) 使用者每 90 天應更換一次通行碼。

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。

(三)特權帳號之存取管理

1. 資通系統之特權帳號請應經正式申請授權方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。

2. 資通系統之特權帳號不得共用。

3. 資通系統之管理者每季應清查系統特權帳號。

(四)加密管理

1. 機密資訊於儲存或傳輸時應進行加密。

2. 加密保護措施應遵守下列規定：

(1) 應落實使用者更新加密裝置並備份金鑰。

(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. 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)遠距工作之安全措施

(1) 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。

(2) 遠距工作終止時之存取權限撤銷，並應返還相關設備。

(三)確保實體與環境安全措施

1. 電腦機房之門禁管理

(1) 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電腦機房，管理者並應定期檢視授權人員之名單。

(3) 人員及設備進出應留存記錄。

2. 電腦機房之環境控制

(1) 電腦機房之空調、電力應建立備援措施。

(2) 電腦機房應安裝之安全偵測及防護措施，包括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，以減少環境不安全之危險。

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) 機密性及敏感性資訊，不使用或下班時應該上鎖。

(四)資料備份

1. 重要資料及資通系統應進行資料備份，並執行異地存放。

2. 敏感或機密性資訊之備份應加密保護。

(五)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. 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。

(六)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。

(七)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

(八)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應具備下列安全性需求：

(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、資通安全防護設備

1. 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。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。

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

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，依本校資通安全事件通報應變程序辦理。

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、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

由資通安全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。

二、監督受託者資通安全維護情形應注意事項

1. 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。

2. 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。

3. 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。

壹拾參、資通安全教育訓練

一、資通安全教育訓練要求

本校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

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，以建立人員資通安全認知，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. 員工報到時，應使其充分瞭解本校資通安全相關作業規範及其重要性。

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，及本校各相關規定辦理之。

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、資通安全維護計畫之持續精進及績效管理

1. 本校之資通安全推動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) 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. 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) 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。

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

本校依據資通安全管理法第 12 條之規定，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. 本機關資通安全事件通報及應變程序

二、附件表單

1. 資通安全推動小組成員及分工表

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. 資訊資產價值評定標準

8. 風險事件發生可能性評定標準

9. 管制區域人員進出登記表

10. 委外廠商執行人員保密切結書、保密同意書

11. 委外廠商查核項目表

12. 資通安全認知宣導及教育訓練簽到表

13. 資通安全維護計畫實施情形

14. 審查結果及改善報告

15.改善績效追蹤報告

新北市五股區成州國民小學資通安全維護計畫相關附件

目　次

1. 資通安全管理代表及推動小組成員分工表

新北市五股區成州國民小學

資通安全管理代表及推動小組成員及分工表

編號：○○

製表日期：○○○年○○月○○日

單位職級	姓名	業務事項	分機	備註 （代理人）
校長		督導學校資通安全相關事項		
教務處 教務主任		資通安全相關規章與程序、制度之執行		
教務處 資訊組		資通安全事件通報		
總務處 總務主任		資訊及資通系統之盤點及風險評估		
總務處 事務組		資料及資通系統之安全防護事項之執行		
學務處 學務主任		傳達資通安全政策與目標		
教務處 教學組		其他資通安全事項之規劃		

承辦人:　　單位主管：　　校長:

2. 資通安全保密同意書

新北市五股區成州國民小學　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：＿＿＿＿＿＿＿＿＿＿

機關校長：＿＿＿＿＿＿＿＿＿＿

中　　華　　民　　國　　年　　月　　日

3. 資通安全需求申請單

新北市五股區成州國民小學　資通安全需求申請單

編號：○○

申請單位	○○處(室)	申請日期	108 年○○月○○日
申請項目	■軟體 □硬體 □其他	項目名稱	○○防毒軟體
申請數量	1	需用日期	108 年○○月○○日
申請類別	■新購 □變更 □廢除	使用設備	■伺服器 □個人電腦/筆電 □其他
安裝單位	資訊組	安裝位置	□機房 □辦公室 □其他
用途說明	防毒軟體更新		
申請人	○○○	單位主管	○○○
資通安全推動小組	處理情形說明：		
資通安全推動小組承辦人員	○○○	校長	○○○

4. 資訊及資通系統資產清冊

新北市五股區成州國民小學　資訊及資通系統資產清冊

編號：○○

製表日期：○○○年○○月○○日

項次	資產名稱	類別	擁有者/職稱	管理者（部門）	使用者（部門）	存放位置	數量	說明	備註
1.	EVO 派送軟體	軟體資產	資訊組	教務處	全校師生	電腦教室/機房	○○套		
2.	個人電腦	實體資產	全體教職員	資訊組	全體教職員	教室/辦公室	○○台		
3.	行動裝置	實體資產	全體教職員	資訊組	全體教職員	教室/辦公室	○○台	筆電、平板、手機	
4.	可攜式媒體	實體資產	全體教職員	全體教職員	全體教職員	教室/辦公室	○○式	有資料的光碟、外接式硬碟、隨身碟	
5.	學校網站	軟體資產	資訊組	資訊組	全體教職員	教育局	○○式	局端雲端機房	
6.	NAS 儲存裝置	實體資產	資訊組	資訊組	全體教職員	機房	○○台		
7.	AD 系統	軟體資產	資訊組	資訊組	資訊組	教育局	○○套	局端雲端機房	
8.	主管人員	人員資產	校長	校長	校長	辦公室	○○式	主任以上	
9.	教職人員	人員資產	校長	校長	校長	辦公室	○○式	主任以下	
10.	資訊組長	人員資產	教務主任	教務主任	教務主任	辦公室	○○式		

項次	資產名稱	類別	擁有者/職稱	管理者（部門）	使用者（部門）	存放位置	數量	說明	備註
11.	圖書志工	人員資產	教務主任	設備組	教務處	圖書室	○○式	接觸學生資料	
12.	教務處 教學資料	資訊資產	教學組	教務處	全校教師	NAS	○○式		
13.	教務處 專案計畫、公文	資料資產	教務主任	教務處	教務處	教務處	○○式		
14.	學生註冊 資料	資料資產	註冊組長	註冊組	註冊組	教務處	○○式		
15.	學務處 學生健康系統	軟體資產	校護	學務處	校護	健康中心	○○式	學生個資資料	
16.	學務處 專案計畫、公文、 校安通報、 性平案與霸凌案件	資料資產	學務主任	學務處	學務處	學務處	○○式		
17.	總務處 專案計畫、公文、 財管資料、地籍資料、 出納憑證	資料資產	總務主任	總務處	總務處	總務處	○○式		
18.	輔導室 專案計畫、公文、 個案輔導記錄	資料資產	輔導主任	輔導室	輔導室	輔導室	○○式		
19.	人室事 履歷資料	資料資產	人事主任	人事室	人事室	人事室	○○式	教職員工人事履歷	
20.	幼兒園 幼兒個資、	資料資產	園長	幼兒園	幼兒園	幼兒園	○○式		

項次	資產名稱	類別	擁有者/職稱	管理者（部門）	使用者（部門）	存放位置	數量	說明	備註
	教師獎懲文件								

承辦人：　　單位主管：　　校長:

5. 風險評估表

新北市五股區成州國民小學　風險評估表

編號：○○

製表日期：○○○年○○月○○日

項次	資產名稱	類別	擁有者/職稱	機密性©	完整性(I)	可用性(A)	資訊資產價值(T)(C,I,A取最大值)	潛在風險事件	風險發生可能性(V)	風險值 資訊資產價值*(T*V)
1.	EVO派送軟體	軟體資產	資訊組	1	1	3	3	1.3.2	2	6
2.	個人電腦	實體資產	全體教職員	1	1	2	2	2.3.3	2	4
3.	行動裝置	實體資產	全體教職員	1	1	1	1	2.4.3	2	2
4.	可攜式媒體	實體資產	全體教職員	1	1	1	1	2.5.2	2	2
5.	學校網站	軟體資產	資訊組	1	1	1	1	1.2.2	1	1
6.	NAS儲存裝置	實體資產	資訊組	2	1	2	2	2.1.3	1	2
7.	AD系統	軟體資產	資訊組	3	2	2	3	1.1.4	1	3
8.	主管人員	人員資產	校長	1	1	1	1	4.2.1	1	1
9.	教職人員	人員資產	校長	1	1	1	1	4.3.1	2	2
10.	資訊組長	人員	教務	2	2	1	2	4.1.2	1	2

項次	資產名稱	類別	擁有者/職稱	機密性©	完整性(I)	可用性(A)	資訊資產價值(T)(C,I,A取最大值)	潛在風險事件	風險發生可能性(V)	風險值資訊資產價值*(T*V)
		資產	主任							
11.	教務處教學資料	資訊資產	教學組	1	1	1	1	3.1.2	1	1
12.	教務處專案計畫、公文	資料資產	教務主任	2	1	1	2	3.1.2	1	2
13.	學生註冊資料	資料資產	註冊組長	3	1	1	3	3.1.4	2	6
14.	學務處學生健康系統	軟體資產	校護	2	1	1	2	1.1.1	2	2
15.	學務處專案計畫、公文、校安通報、性平案與霸凌案件	資料資產	學務主任	2	1	1	2	3.1.2	1	2
16.	總務處專案計畫、公文、財管資料、地籍資料、出納憑證	資料資產	總務主任	2	1	1	2	3.1.2	1	2
17.	輔導室專案計	資料	輔導主	2	1	1	2	3.1.2	1	2

項次	資產名稱	類別	擁有者/職稱	機密性©	完整性(I)	可用性(A)	資訊資產價值(T)(C,I,A取最大值)	潛在風險事件	風險發生可能性(V)	風險值資訊資產價值*(T*V)
	畫、公文、個案輔導記錄	資產	任							
18.	人室事履歷資料	資料資產	人事主任	3	1	1	3	3.1.4	1	3
19.	幼兒園幼兒個資、教師獎懲文件	資料資產	園長	3	1	1	3	3.1.4	1	3

註：

1. 本表可與資訊及資通系統資產清冊合併使用。
2. 陳核層級請學校依需求調整

承辦人：　　單位主管：　　校長：

6. 風險類型暨風險對策參考表

資產大類	資產小類	潛在風險事件	管控措施範例說明
1.軟體資產類	1.1 作業系統	1.1.1 未落實作業系統更新/漏洞修補，致使遭受惡意攻擊、資料外洩或其他侵害。	-WSUS 機制失效 -定期檢查漏洞更新狀態 -資訊單位定期彙整提供發佈更新資訊(，供業務單位進行比對
1.軟體資產類	1.1 作業系統	1.1.2 未購買妥適的作業系統授權/使用授權超過購買數，致使遭受廠商求償或抗議。	-作業系統授權清單
1.軟體資產類	1.1 作業系統	1.1.3 未汰換原廠公告停止技術支援之作業系統，進而無法修補漏洞，致使遭受惡意攻擊、資料外洩或其他侵害。	
1.軟體資產類	1.1 作業系統	1.1.4 未加入組織之網域，進而無法套用 GCB 或群組原則政策，致使無法有效管控。	-套用 GCB 設定，或設定適當權組原則
1.軟體資產類	1.1 作業系統	1.1.5 個人電腦或伺服器等資訊設備，未安裝適當之防毒軟體或安全防護軟體，於網路連線時遭電腦病毒入侵或被植入惡意程式，致使資料外洩或遭受其他侵害。	
1.軟體資產類	1.1 作業系統	1.1.6 作業系統最高管理權限管制不當，有共用或浮濫設定的情形。	
1.軟體資產類	1.2 套裝軟體	1.2.1 未購買妥適的套裝軟體授權或使用超過購買授權數量，致使可能違反智慧財產權，遭受廠商求償。	-軟體管制清單 -軟體授權資料 -資產管理工具
1.軟體資產類	1.2 套裝軟體	1.2.2 未定期進行套裝軟體更新(含防毒軟體)/漏洞修補，致使遭受惡意攻擊、資料外洩或其他侵害。	-軟體原廠發佈更新及安裝紀錄 -資訊單位定期彙整提供發佈更新資訊，供業務單位進行比對 -定期檢查原廠公告漏洞修補狀態
2.實體資產類	2.1 伺服器	2.1.1 未安裝於機櫃中或實體管制隔離區(如：機房)，可能因人員誤觸或未經	-機房環境管控

資產大類	資產小類	潛在風險事件	管控措施範例說明
		授權人員有機會碰觸，而造成設備損壞、資料外洩或服務中斷。	
2.實體資產類	2.1 伺服器	2.1.2 伺服器擺放位置，未考量安全環境(如：溫度、濕度、電力、監控等)，可能因安全環境背景，造成伺服器損壞或服務中斷。	-機房環境管控
2.實體資產類	2.1 伺服器	2.1.3 伺服器超過廠商保固期限，未定期編列經費維護或汰換，造成設備可能因零件損壞時無料可維修，致使服務中斷。	-超過保固期限
2.實體資產類	2.1 伺服器	2.1.4 伺服器於報廢前未妥善清除資料，致使資料外洩或遭受其他侵害。	-相關設定與儲存媒體之資料必須清除 -如專業資料清除軟體或實體破壞
2.實體資產類	2.1 伺服器	2.1.5 重要伺服器無適當之備援措施。	-設備備援措施
2.實體資產類	2.1 伺服器	2.1.6 設備安裝或變更無適當管控措施。	-安裝或變更管制措施
2.實體資產類	2.1 伺服器	2.1.7 設備未定期維護或缺乏備援設備，致使設備故障時未能及時修復影響業務。	-定期維護
2.實體資產類	2.2 網路設備	2.2.1 骨幹網路設備未安裝於機櫃中或實體管制隔離區(如：機房)，造成因人員誤觸或未經授權人員有機會接觸設備，而致使設備損壞、資料外洩或服務中斷。	
2.實體資產類	2.2 網路設備	2.2.2 網路設備擺放位置，未考量安全環境(如：溫度、濕度、電力、監控等)，造成因安全環境背景，致使伺服器損壞或服務中斷。	
2.實體資產類	2.2 網路設備	2.2.3 網路設備超過廠商保固期限，未定期編列經費維護或汰換，造成設備可能因零件損壞時無料可維修，致使服務中斷。	

資產大類	資產小類	潛在風險事件	管控措施範例說明
2.實體資產類	2.2 網路設備	2.2.4 設備於報廢前未妥善清除資料，致使資料外洩或遭受其他侵害。	-相關設定與儲存媒體之資料必須清除 -如專業資料清除軟體或實體破壞
2.實體資產類	2.2 網路設備	2.2.5 核心網路設備架構上具有單點失效之問題。	
2.實體資產類	2.2 網路設備	2.2.6 網路纜線接合不良或未做適當防護措施。	
2.實體資產類	2.3 個人電腦	2.3.1 個人電腦超過廠商保固期限，未定期編列經費汰換，造成設備因零件損壞時無料可維修，致使服務中斷。	
2.實體資產類	2.3 個人電腦	2.3.2 個人電腦未進行適切的資產管理及管制硬體規格數量，造成零組件遭置換或遺失，致使硬體效能降低，影響作業效率。	
2.實體資產類	2.3 個人電腦	2.3.3 處理機敏性資料之個人電腦未進行適切的隔離或存取控制措施，可能發生資料外洩。	
2.實體資產類	2.3 個人電腦	2.3.4 未管制個人電腦內建式燒錄機或USB 連接埠，透過可攜式媒體將資料複製攜出，致使資料於未授權情況下，造成資料外洩、遺失或遭受其他侵害。	-如全面控管，禁止使用 -或設定 USB 僅能讀取資料，禁止寫出 -或特別申請 USB 開放使用，並保存讀取/寫出紀錄 -或僅能使用經組織登錄配發之可攜式媒體(並使用加密功能)
2.實體資產類	2.3 個人電腦	2.3.5 個人電腦於報廢前未妥善清除資料，致使資料外洩或遭受其他侵害。	-相關設定與儲存媒體之資料必須清除 -如專業資料清除軟體或實體破壞
2.實體資產類	2.4 可攜式設備	2.4.1 存放設備之實體門禁未進行出入管制或長時間不使用時未將設備妥善收存，造成同仁、外部訪客或廠商可能無意/故意將設備攜出，致使設備遺失、資料外洩或遭受其他侵害。	

資產大類	資產小類	潛在風險事件	管控措施範例說明
2.實體資產類	2.4 可攜式設備	2.4.2 設備遺失未即時通報，造成組織未能即時處置，致使資料外洩或遭受其他侵害。	
2.實體資產類	2.4 可攜式設備	2.4.3 未管制筆記型電腦內建式燒錄機或 USB 連接埠，透過可攜式媒體將資料複製攜出，致使資料於未授權情況下，造成資料外洩、遺失或遭受其他侵害。	-如全面控管，禁止使用 -或設定 USB 僅能讀取資料，禁止寫出 -或特別申請 USB 開放使用，並保存讀取/寫出紀錄 -或僅能使用經組織登錄配發之可攜式媒體(並使用加密功能)
2.實體資產類	2.4 可攜式設備	2.4.4 可攜式設備於報廢前未妥善清除資料，致使資料外洩或遭受其他侵害。	-相關設定與儲存媒體之資料必須清除 -如專業資料清除軟體或實體破壞
2.實體資產類	2.4 可攜式設備	2.4.5 筆記型電腦、平板電腦或智慧型手機等可攜式設備，未安裝適當之防毒軟體或安全防護軟體，於網路連線時遭電腦病毒入侵或被植入惡意程式，致使資料外洩或遭受其他侵害。	
2.實體資產類	2.5 可攜式媒體	2.5.1 可攜式媒體未妥善保管，造成同仁、外部訪客或廠商無意/故意將可攜式媒體攜出，致使媒體遺失、資料外洩或遭受其他侵害。	-如可攜式媒體經申請或借用後，應妥為收藏或上鎖存放 -或機敏資訊儲存於可攜式媒體，應予以加密
2.實體資產類	2.5 可攜式媒體	2.5.2 可攜式媒體攜出組織場所，未妥善保管，致使資料外洩或遭受其他侵害。	-攜出組織場所以外，須將可攜式媒體放置於放置於包裝袋中
2.實體資產類	2.5 可攜式媒體	2.5.3 可攜式媒體於報廢前未妥善清除資料，致使資料外洩或遭受其他侵害。	-如專業資料清除軟體或實體破壞 -或將磁碟/磁帶/磁片予以消磁
2.實體資產類	2.6 週邊設備	2.6.1 列(影)印、傳真機密文件，未即時將紙本文件取走，留置於設備上，造致使資料外洩或遭受其他侵害。	

資產大類	資產小類	潛在風險事件	管控措施範例說明
2.實體資產類	2.6 週邊設備	2.6.2 設備未定期維護或缺乏備品，致使設備故障時未能及時修復影響作業效率。	
2.實體資產類	2.6 週邊設備	2.6.3 設備於報廢前未妥善清除資料，致使資料外洩或遭受其他侵害。	-相關設定與儲存媒體之資料必須清除 -如專業資料清除軟體或實體破壞
2.實體資產類	2.6 週邊設備	2.6.4 保存紙本文件資料或可攜式媒體之文件櫃或硬體設備，應上鎖而未上鎖或上鎖功能損壞，致使資料外洩或遭受其他侵害。	
2.實體資產類	2.6 週邊設備	2.6.5 設備放置於外部網路，未進行適當防護，可能遭駭客入侵，做為進入內部網路的跳板。	
3.資料資產類	3.1 紙本文件	3.1.1 資訊系統相關技術說明、設定或規劃文件，未有適當控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-如文件櫃上鎖存放
3.資料資產類	3.1 紙本文件	3.1.2 業務資料或其它包含機敏資訊之文件，未依安全等級控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-依資訊資產安全等級限閱或敏感等級進行管理
3.資料資產類	3.1 紙本文件	3.1.3 業務資料或其它包含一般資訊之文件，違反組織作業程序或法令法規之要求，致使資料遭不當使用後，影響法律規章遵循或損害組織信譽。	-依資訊資產安全等級一般或公開等級進行管理
3.資料資產類	3.1 紙本文件	3.1.4 包含個人資料之文件，未有適當控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-依個人資料檔案機密等級進行管理
3.資料資產類	3.1 紙本文件	3.1.5 逾保存期限之紙本文件、表單或紀錄，未能適度予以銷毀，造成保存之文件與資料過多，致使發生遺失或外洩情況時，增加組織遭損害求償之風險或損害組織信譽。	-依文件與紀錄管理程序書進行管理
4.人員資產類	4.1 資訊人員	4.1.1 資訊人員未訂定或落實代理人制度，致使組織遇緊急資安事件時無法即時處置。	-資安事件如：網路斷線、系統無法正常使用等

資產大類	資產小類	潛在風險事件	管控措施範例說明
4.人員資產類	4.1 資訊人員	4.1.2 資訊人員未進行適當職務區隔，造成特定人員權限過大，增加組織之營運風險。	
4.人員資產類	4.1 資訊人員	4.1.3 人員的疏失、操作錯誤或惡意行為，致使作業過程中資料外洩或遭受其他侵害。	
4.人員資產類	4.2 主管人員	4.2.1 缺乏職務代理機制，影響組織行政效率或造成管理弊端。	
4.人員資產類	4.2 主管人員	4.2.2 主管人員遭受脅迫、賄絡或社交工程影響，造成機敏資訊外洩或遭受其它侵害，違反組織作業程序或法令法規之要求，致使資料遭不當使用後，影響法律規章遵循、損害組織利益或信譽。	-主管人員擁有較多機敏資訊權限，若其資料外洩或遭受其它侵害時，影響層面較廣
4.人員資產類	4.3 一般人員	4.3.1 人員未瞭解組織資訊安全政策、內部制度規範及應負之資安責任，造成人員資安認知不足，致使作業過程中資料外洩或遭受其他侵害。	
4.人員資產類	4.3 一般人員	4.3.2 人員的疏失、操作錯誤或惡意行為，致使作業過程中資料外洩或遭受其他侵害。	
4.人員資產類	4.3 一般人員	4.3.3 缺乏職務區隔機制，造成承辦人員被賦予之權限過大或不適當，致使產生管理弊端。	-如審查者與設定者需進行適當區隔 -如會計與出納需明確區隔
4.人員資產類	4.3 一般人員	4.3.4 缺乏職務代理機制，造成發生突發狀況時無法及時反應，致使營運中斷或發生資安事故。	
4.人員資產類	4.4 外部人員	4.4.1 未告知外部人員本組織之資訊安全政策及資安要求，造成外部人員資安認知不足或作業疏失，致使組織資料外洩或遭受其他侵害。	
4.人員資產類	4.4 外部人員	4.4.2 人員未能配合、疏失、操作錯誤或惡意行為，致使作業過程中資料外洩或遭受其他侵害。	

資產大類	資產小類	潛在風險事件	管控措施範例說明
4.人員資產類	4.4 外部人員	4.4.3 人員接觸組織資料前未簽訂保密切結或協議，致使人員將組織資料攜出或惡意揭露。	
5.資訊資產類	5.1 電子資料	5.1.1 業務資料或其它包含機敏資訊之電子資料，未依安全等級控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-如限閱或敏感等級存取權限控管 -或加密存放 -或機敏資訊儲存於可攜式媒體，應予以加密。
5.資訊資產類	5.1 電子資料	5.1.2 業務資料或其它包含一般資訊之電子資料，違反組織作業程序或法令法規之要求，致使資料遭不當使用後，影響法律規章遵循或損害組織信譽。	-如一般等級資料存取權限控管 -如公開資料覆核
5.資訊資產類	5.1 電子資料	5.1.3 包含個人資料之電子資料，未有適當控管，致使資料遺失、毀損、外洩或遭受其它侵害。	-依個人資料檔案機密等級進行管理
5.資訊資產類	5.1 電子資料	5.1.4 資料庫包含之各項資料，未有適當控管，致使資料不正確、毀損、外洩或遭受其它侵害。	-如透過 DBMS 寫入、修改或查詢等功能權限控管 -或資料庫加密/欄位加密

7. 資訊資產價值評定標準

評分 類型	0	1	2	3
機密性	無此特性或可公開。	僅供本校內部人員使用。	僅供業務相關人員存取。	具特殊權限人員方可存取。
完整性	無此特性或不影響本校運作。	將造成部份業務運作效率降低。	將造成部份業務運作停頓。	將造成全部業務運作停頓。
可用性	無此特性或最大可容忍中斷時間 5 天以上。	最大可容忍中斷時間 3 天以上，5 天以下。	最大可容忍中斷時間 1 天以上，3 天以下。	最大可容忍中斷時間 1 天以內。
適法性	無此特性或不影響本校運作。	須符合本校或市府內部規定的要求。	須符合行政法規（如：國家資通安全會報等）或外部合約規範的要求。	須符合國家法律（如：資通安全管理法、個人資料保護法、著作權法等）規範的要求。

8. 風險事件發生可能性評定標準

評分	評定標準
1	風險發生可能性低，每年至多可能發生 1 次。
2	風險發生可能性中，每季有可能發生 1 次。
3	風險發生可能性高，每月有能發生 1 次。

9. 管制區域人員進出登記表

新北市五股區成州國民小學　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	王○○	○○室	陳○○	108.05.2	8：00	9：00	借用電腦設備	普	手提電腦	手機

註：陳核層級請學校依需求調整

承辦人：　　單位主管：

10. 委外廠商執行人員保密切結書、保密同意書

新北市五股區成州國民小學　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

新北市五股區成州國民小學　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

11. 委外廠商查核項目表

新北市五股區成州國民小學　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？	■	□	□	指派本校校長擔任資安長。
	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ISO 27001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。
	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。

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

查核項目	查核內容	查核結果			說明
		符合	不符合	不適用	
	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變之程序及機制	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。
	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	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。

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

註：陳核層級請學校依需求調整

承辦人:　　單位主管：　　校長：

12. 資通安全認知宣導及教育訓練簽到表

新北市五股區成州國民小學　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（範例）

時　　間：108 年○○月○○日 8：00 — 9：00

地　　點：＿＿會議室＿＿＿＿＿＿＿＿＿＿＿＿

單　位	職　稱	姓　名	簽　名
人事室	組長	○○○	

13. 資通安全維護計畫實施情形

新北市五股區成州國民小學　資通安全維護計畫實施情形

編號：○○

本校經主管機關核定後本校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108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
1. 資通業務及其重要性	1.1 資通業務及重要性盤點	本校資通業務及重要性詳參資通安全維護計畫（詳附件）。
2. 資通安全政策及目標	2.1 資通安全政策訂定及核定	本校已訂定資通安全政策，詳參資通安全維護計畫，並經校長核定(詳附件)。
	2.2 資通安全目標之訂定	本校已訂定資通安全目標，詳資通安全維護計畫。
	2.3 資通安全政策及目標宣導	本校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	本校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. 設置資通安全推動代表	3.1 設定資通安全管理代表	本校已指定○○○為資通安全管理代表，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	本校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. 人力及經費之配置	4.1 人員配置	本校依規定配置資通安全人員7名。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	本校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資通系統、相關資產之標示	5.1 資訊及資通系統之盤點	本校已於今年七月盤點資訊、資通系統，建立資產目錄。
	5.2 資通安全責任等級分級	本校依資通安全責任等級分級辦法，為資通安全責任等級D級機關。
6. 資通安全風險評估	6.1 資通安全風險評估	本校已於今年○月完成資訊、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	本校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 資訊及資通系統之保管	本校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	本校已依資通安全維護計畫辦理。
	7.3 作業及通訊安全管理	本校已依資通安全維護計畫辦理。
	7.4 資通安全防護設備	本校已依資通安全維護計畫辦理。
8. 資通安全事件通報、應變及演練	8.1 訂定資通安全事件通報、應變及演練相關機制	本校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	本校已依規定進行資通安全事件通報。 本校已依規定於今年○、○月辦理社交工程演練，並於九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	本校接受情資後，已進行分類評估。
	9.2 資通安全情資之因應措施	本校已接受情資之分類，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	本校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	本校已依規定監督受託者資通安全維護情形。
11. 資通安全教育訓練	11.1資通安全教育訓練要求	本校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	本校已於今年0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	本校已建立考核機制，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	13.1資通安全維護計畫之實施	本校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	本校已依規定辦理內部自我檢核。

制	形之檢核機制	
	13.3資通安全維護計畫之持續精進及績效管理	本校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		

註：陳核層級請學校依需求調整

承辦人:　　單位主管：　　校長：

14. 審查結果及改善報告

新北市五股區成州國民小學　審查結果及改善報告

範圍	全機關
日期	108 年 ○○ 月 ○○ 日
審查日期	108 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				

15. 改善績效追蹤報告

新北市五股區成州國民小學　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	108年___月___日___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。

<table>
<tr><td></td><td>機房設備，並確保備份設備及機制運作效果。</td><td colspan="2">系統，於停電時可維持 12 小時運作。</td><td></td></tr>
<tr><td>作業程序</td><td></td><td colspan="2"></td><td></td></tr>
<tr><td>其他</td><td></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="5">績效管考</td></tr>
<tr><td colspan="2">改善措施確認</td><td colspan="3">■合格／完成
□待追蹤(追蹤期限：_______年______月______日)
□不合格(說明：____)</td></tr>
<tr><td colspan="2">經費需求或編列執行金額</td><td>○○○萬元。</td><td>經費執行情形</td><td>已進行相關電腦機房設備更新採購，共執行○○萬元。</td></tr>
<tr><td colspan="2">預定完成日期</td><td>108 年 12 月 20 日</td><td>實際完成日期</td><td>108 年 12 月 20 日</td></tr>
<tr><td colspan="2">完成進度或情形說明</td><td colspan="3">定期檢視委外廠商之監督維護責任。</td></tr>
<tr><td colspan="2">改善成效考核</td><td colspan="3"></td></tr>
<tr><td colspan="2">後續成效追蹤</td><td colspan="3"></td></tr>
<tr><td colspan="2">資通安全推動小組
承辦人員</td><td>○○○</td><td>校長</td><td>○○○</td></tr>
</table>

註：陳核層級請學校依需求調整