檔　　號：
保存年限：

簽　於　教務處
電話：047353267#123

日期：113年1月1日

主旨：有關本校資通安全維護計畫，如說明，簽請核示。
說明：依據本縣資通安全維護計畫辦理。
擬辦：奉准後，由職公告於本校全球資訊網供參。

教師兼資訊組長 蘇志祥

裝

訂

第一層決行

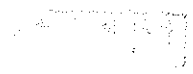
承辦單位　　決行

教師兼資訊組長 蘇志祥
113.01.02

新庄國小 校長 吳文輝

線

教師兼代教務主任 陳建政



彰 化 縣 新 庄 國 民 小 學

資通安全維護計畫

機密等級: 一般

承辦人簽章: 教師兼資訊組長蘇志祥

(資通安全推動小組)單位主管簽章： 教師兼代教務主任陳建政

(資安長)簽章： 新庄國小校長吳文輝

中華民國 113 年 01 月 01 日

資通安全維護計畫

文件制/修訂紀錄表

文件版本	修訂日期 會議名稱	修訂內容	修訂單位	修訂人	核定人 (資安長)
V1.0(初版)	105 年 02 月 01 日	新擬訂文件	教務處 資訊組	陳建政	林俊成
V2.0 版	110 年 08 月 01 日 第一次行政會議	增修訂文件	教務處 資訊組	陳建政	吳文輝
V2.1 版	113 年 05 月 01 日 第一次資通安全管理審查會議	增修訂文件	教務處 資訊組	蘇志祥	吳文輝

目　錄

壹、依據及目的 1
貳、適用範圍 1
參、核心業務及重要性 1
一、核心業務及重要性 1
二、非核心業務及說明 2
肆、資通安全政策及目標 2
一、資通安全政策 2
二、資通安全目標 3
三、資通安全政策及目標之核定程序 4
四、資通安全政策及目標之宣導 4
五、資通安全政策及目標定期檢討程序 4
伍、資通安全推動組織 4
一、資通安全長 4
二、資通安全推動小組 5
陸、人力及經費配置 6
一、專職(責)人力及資源之配置 7
二、經費之配置 7
柒、資訊及資通系統之盤點 7
一、資訊及資通系統盤點 7
二、機關資通安全責任等級分級 8
捌、資通安全風險評估 8
一、資通安全風險評估 8
二、資通安全風險之因應 8
玖、資通安全防護及控制措施 9
一、資訊及資通系統之管理 9
二、存取控制與加密機制管理 11
三、作業與通訊安全管理 13
四、資通安全防護設備 18
壹拾、資通安全事件通報、應變及演練相關機制 19
壹拾壹、資通安全情資之評估及因應 19

一、資通安全情資之分類評估 19
二、資通安全情資之因應措施 20
壹拾貳、資通系統或服務委外辦理之管理 21
一、選任受託者應注意事項 21
二、監督受託者資通安全維護情形應注意事項 21
壹拾參、資通安全教育訓練 21
一、資通安全教育訓練要求 21
二、資通安全教育訓練辦理方式 22
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 22
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 23
一、資通安全維護計畫之實施 23
二、資通安全維護計畫實施情形之稽核機制 23
三、資通安全維護計畫之持續精進及績效管理 24
壹拾陸、資通安全維護計畫實施情形之提出 25
壹拾柒、相關法規、程序及表單 25
一、相關法規及參考文件 25
二、附件表單 26

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

本計畫適用範圍涵蓋彰化縣新庄國民小學全機關。(以下簡稱本校)。

參、核心業務及重要性

一、核心業務及重要性

本校配合資通安全責任等級 D 級政策，配合向上集中無自行維運核心資通系統。

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
學校官方網站	為本校依組織法執掌，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
網域名稱服務	為本校依組織法執掌，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
彰化縣國中小學生學籍與教師差假系統	為本校依組織法執掌，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
電子郵件系統(教育部校園雲端電子郵件)	為本校依組織法執掌，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

二、非核心業務及說明

本校之非核心業務及說明如下表：

非核心業務系統	業務失效影響說明	最大可容忍中斷時間
公文管理系統	電子公文無法即時送達機關，影響機關行政效率。	由上級管理單位訂之
教育處新雲端網站	可能使本校部分業務中斷	由上級管理單位訂之
學校基本資料平台	可能使本校部分業務中斷	由上級管理單位訂之
Gsuite 入口網	可能使本校部分業務中斷	由上級管理單位訂之
OPENID 單一帳號認證平台	可能使本校部分業務中斷	由上級管理單位訂之
網路防火牆系統	可能使本校部分業務中斷	由上級管理單位訂之
教育部學生健康資訊系統	可能使本校部分業務中斷	由上級管理單位訂之
教育部校園安全暨災害防救通報處理中心	可能使本校部分業務中斷	由上級管理單位訂之
行政院管考系統	可能使本校部分業務中斷	由上級管理單位訂之
教育機構資安通報平台	可能使本校部分業務中斷	由上級管理單位訂之
地方教育發展基金會計資訊系統	可能使本校部分業務中斷	由上級管理單位訂之
校園食材登錄平台	可能使本校部分業務中斷	由上級管理單位訂之
智慧網路管理平台	可能使本校部分業務中斷	由上級管理單位訂之
人事服務網	可能使本校部分業務中斷	由上級管理單位訂之
財產/會計/出納/薪資等套裝軟體或上級機關提供之管理系統	可能使本校部分業務中斷	4 小時
防毒軟體服務 保全/監視/電子圍籬等系統 NAS 系統(儲存媒體裝置設備) IOT 物聯網裝置等系統	可能使本校部分業務中斷	1 小時

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. 機密資料檔案的讀取及複製，須符合本校各業務單位的規定，並經該單位主管或其授權人員核可。
8. 本政策每年應至少評估檢討一次，以反映本校資訊安全需求、政府法令法規、外在網路環境變化及資訊安全技術等最新發展現況，以確保其對於維持營運和提供適當服務的能力。
9. 本政策如遇重大改變時應立即審查，以確保其適當性與有效性。必要時應告知相關單位及委外廠商，以利共同遵守。

本政策經資通安全長核准，於公告日施行，並以書面、電子或其他方式通知員工及與本校連線作業之有關機關（構）、委外廠商，修正時亦同。

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. 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%。(請機關自行設定指標)
3. 資安事件通報時間(含演練)超過一小時次數≤0 次。
4. 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。

5. 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. 提升本校人員資安防護意識，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簽陳資通安全長核定。

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，向機關內所有人員進行宣導，並檢視執行成效。
2. 本校應每年向利害關係人(例如 IT 服務供應商、與機關連線作業有關單位）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「資通安全管理法」第 11 條之規定，本校訂吳文輝校長為資通安全長，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，由資通安全長召集各業務部門(處事)主管/副主管以上之人員代表成立資通安全推動小組，其任務宜包括：

1. 跨部門(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. 傳達機關資通安全政策與目標。
6. 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：(請參考範例自行分組)

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. 資訊及資通系統之盤點及風險評估。
6. 資通安全相關規章與程序、制度之執行。
7. 資料及資通系統之安全防護事項之執行。
8. 資通安全事件之通報及應變機制之執行。
9. 其他資通安全事項之辦理與推動。
10. 每年定期召開資通安全管理審查會議，提報資通安全事項執行情形。

陸、 人力及經費配置

一、專職(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，無須設置資通安全專職（責）人員，目前機關透過「資通安全推動小組」兼辦資通安全業務負責本校之法遵義務暨現有資通安全推動小組分組人員名單及職掌應列冊，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，負責本校對所屬公務機關或所管特定非公務機關之法遵義務執行事宜。
2. 本校之承辦單位於辦理資通安全業務時，應加強資通安全人力之培訓，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，得洽請相關學者專家或專業機關(構)，提供顧問諮詢服務。
3. 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. 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. 資通安全處理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. 本校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通安全推動小組提出，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、人員資產、資料資產、支援服務資產等，各分類說明如下：

(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) 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。

(5) 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。

(6) 支援服務資產：相關基礎設施及其他機關內部之支援服務，如電力系統、消防系統、環控系統、保全系統、監視系統等。

2. 本校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。
3. 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。
4. 各單位管理之資訊或資通系統如有異動，應即時通知資通安全推動小組更新資通系統資產清冊。

二、機關資通安全責任等級分級

本校依據教育部臺教資(四)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

1. 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，核心資訊系統由上級或監督機關兼辦或代管則不需進行，校內尚有其他資通系統，故需針對資訊及資通系統資產進行盤點與風險評估，將評估結果紀錄於「資通系統資產清冊與風險評鑑彙整表」。
2. 本校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之資通系統防護需求分級，每年並最少檢視 1 次資通系統分級妥適性。

3. 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。

二、資通安全風險之因應

1. 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。
2. 非核心資通系統及最大可容忍中斷時間。

非核心資通系統	資訊資產	最大可容忍中斷時間	非核心資通系統主要功能
財產/會計/出納/薪資/等管理系統或套裝軟體	財產管理系統：彰化縣政府財產管理資訊系統 會計管理系統：地方教育發展基金會計資訊系統	4 小時	行政事務使用
防毒軟體服務	ESET ENDPOINT SECURITY	4 小時	資通安全防護
保全/監視/電子圍籬等系統	FIME	1 小時	強化校園周界安全管理
IOT 物聯網裝置	影印事務機：Konica Minolta bizhub C364E；Konica Minolta bizhub C363 傳真機：EPSON AL-MX300 智慧電視： ViewBoard IFP7552-IC75 吋 13 台 富動科技 Aero Touch 75 吋 21 台	24 小時	行政事務使用 教學使用

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:

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. 本校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. 非本校同仁使用本校之資訊及資通系統，應確實遵守本校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. 本校之網路區域劃分如下：
   (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。(原則禁止例外允許)
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. 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。
5. 本校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。
6. 對網路系統管理人員或資通安全主管人員的操作，均應建立詳細的紀錄。並應定期檢視網路安全相關設備設定規則與其日誌紀錄，並檢討執行情形。
7. 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。
8. 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) 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 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。(請勿使用弱密碼或帳號與密碼相同)

(3) 使用者每 90 天應更換一次通行碼，應對個人所持有通行碼盡保密責任。

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. 本校之機密資訊於儲存或傳輸時應進行加密。

2. 本校之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) 應避免留存解密資訊。

(3) 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) 遠距工作之安全措施

1. 本校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。
3. 針對遠距工作之連線應採適當之防護措施（並包含伺服器端之集中過濾機制檢查使用者之授權），並且記錄其登入情形。
   (1) 提供適當通訊設備，並指定遠端存取之方式。
   (2) 提供虛擬桌面存取，以防止於私有設備上處理及儲存資訊。
   (3) 進行遠距工作時之安全監視。
   (4) 遠距工作終止時之存取權限撤銷，並應返還相關設備。

(三) 電子郵件安全管理

1. 本校配合向上集中計畫，校內無電子郵件伺服器，校內同仁均申請教育部校園雲端電子郵件為公務信箱。
2. 遵循教育部校園雲端電子郵件使用管理要點。
3. 本校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。
4. 電子郵件系統管理人應定期進行電子郵件帳號清查。
5. 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。
6. 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。
7. 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。
8. 使用者應確保電子郵件傳送時之傳遞正確性。
9. 使用者使用電子郵件時，應注意電子簽章之要求事項。
10. 本校應定期舉辦(或配合上級機關舉辦)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. 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之文件或可移除式媒體在不使用或下班時，應存放在櫃子內上鎖。

(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。

(五) 資料備份

1. 重要資料及資通系統應進行資料備份，其備份之頻率應滿足復原時間點目標之要求，並執行異地存放。

2. 敏感或機密性資訊之備份應加密保護。

3. 本校應定期確認其資料備份之有效性。且測試該等資料備份時，宜於專屬之測試系統上執行，而非直接於覆寫回原資通系統。

(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. 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。

3. 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。
4. 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。

(七) 電腦使用之安全管理

1. 電腦、業務系統或自然人憑證，若超過三十分鐘不使用時，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事務機、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。
3. 本校人員一律禁用私人的可攜式設備及可攜式儲存媒體等設施，如公務上須使用則須提出申請經權責主管核准後方可使用。
4. 機關財產之可攜式設備及可攜式儲存媒體僅限於公務使用，禁止使用於私人用途，使用時應僅防資訊外洩或中毒。
5. 使用者如需使用外來的可攜式資訊設備或可攜式儲存媒體，必須先進行掃毒，確認其不含病毒與惡意程式，掃毒後方可進行資料

之上傳及寫入作業，以避免受到惡意程式的威脅。

6. 將機密資料存放於可攜式儲存媒體上時，得採取適當加密處理或設定密碼保護（如 Word、Excel 或壓縮軟體之密碼功能），避免可攜式儲存媒體遺失時造成資訊外洩。
7. 筆記型電腦(行動設備)應安裝防毒軟體，並定期檢查作業系統修正程式與更新病毒碼為最新版本。
8. 存有重要機密性資訊之可攜式資訊設備或儲存媒體攜出時，設備管理人員應負保護之責不得離身，且針對相關檔案資料須執行加密或先清除其機密資訊，以避免資料洩露，另作業完成後須徹底抹去媒體上相關資料。
9. 筆記型電腦(行動設備)、可攜式設備及儲存媒體等裝置，遺失時應立即通報單位主管，並評估資料遺失是否具有機密性，依情節之重大程度決定是否向上呈報。

(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。

(十) 禁止使用危害國家資通安全產品與大陸廠牌資通訊產品(含軟體、硬體及服務)

1. 使為避免公務及機敏資料遭不當竊取，導致機敏公務資訊外洩或

造成國家資通安全危害風險。

(1) 公務用之資通設備不得使用中國大陸廠牌，且不得安裝非公務用軟體。

(2) 本校應就已使用或採購之中國大陸廠牌資通訊設備列冊管理，如於汰換前須與公務環境介接者，須於行政院管考系統填報「汰換前配套措施或相關作為」等資訊。

2. 針對個人資通設備部分，本校應落實要求大陸廠牌資通訊產品一律禁止處理公務事務或介接公務環境；另，考量機關內部業務實務運作，目前多有透過個人資通訊產品處理公務事務之需求，如收發電子郵件或使用即時通訊軟體等，爰建議如下：

(1) 本校應掌握同仁使用情形並適度管控，如採報備制方式了解同仁使用狀況。

(2) 應強化設備安全性設定、落實定期更新及提升人員資安意識。

四、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。(網路防火牆、電子郵件伺服器為向上集中管理，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、設定異動應保留相關修改紀錄，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，本校依「資通安全事件通報及應變辦法」及「臺灣學術網路各級學校資通安全通報應變作業程序」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、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、國民身分證統一編號、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。

(四) 涉及核心業務、核心資通系統之情資

資通安全處理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. 受託者應採取之其他資通安全相關維護措施 。
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

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實施期程及內容，轉知有關行政院、教育部、TACERT(臺灣學術網路危機處理中心)、各大專院校、彰化縣政府、彰化縣教育網路中心等機關辦理之資通安全教育訓練或利用e等公務園學習平臺數位學習、磨課師+等方式，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上課紀錄。
2. 本校辦理資通安全認知宣導及教育訓練其內容得包含：

   (自行辦理教育訓練須呈報彰化縣政府教育處核備研習時數)

   (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。
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，彰化縣政府暨所屬機關公務人員平時獎懲標準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、資通安全維護計畫實施情形之稽核機制

(一)稽核機制之實施

1. 資通安全處理小組應定期12月前(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. 辦理稽核前資通安全推動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，資通安全推動小組應於執行稽核前7日，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、是否定期更改密碼等）。
7. 本校應配合上級或監督機關之規定辦理查核作業，以確認人員是否遵循本計畫與機關之管理程序要求，並有效實作及維持管理制度。

(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. 本校之資通安全處理小組應於每年 12 月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、資通安全處理小組決議事項等。

(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) 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

本校依據「資通安全管理法」第 12 條之規定，配合主管機關(行政院)規定應於次年向上級或監督機關，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

一、依據行政院 109 年 11 月 9 日院臺護字第 1090195231 號函辦理。

二、依據彰化縣政府 109 年 11 月 12 日府計資字第 1090408571 號函辦理。

主旨:行政院訂定「各機關資通安全事件通報及應變處理作業程序」，自即日生效，試行一年，請查照。

5. 資通安全情資分享辦法

一、依據行政院資通安全處 109 年 12 月 1 日院臺護字第 1090196975 號函辦理。

二、依據彰化縣政府 109 年 12 月 4 日府計資字第 1090440022 號函辦理。

主旨:檢送「資通安全情資分享說明」及「資通安全情資分享通報單」各 1 份，請查照。

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. 資訊作業委外安全參考指引
14. 彰化縣政府暨所屬機關公務人員平時獎懲標準
15. 資通安全責任等級 D 級之各機關應辦事項

二、附件表單

1. 資通安全管理代表及推動小組成員分工表
2. 員工保密切結書
3. 資通安全需求申請單
4. 資通系統資產清冊與風險評鑑彙整表

(4.1 資通系統資產清冊)

(4.2 風險評鑑彙整表)

5. 資通安全教育訓練計畫及教育訓練簽到表

6. 管制區域人員進出登記表

7. 委外廠商執行人員保密同意書

8. 委外廠商執行人員保密切結書

9. 內部稽核/委外廠商查核項目表

10. 資通安全維護計畫實施情形

11. 審查結果及改善報告

12. 改善績效追蹤報告

13. 經費配置表

14. 專(職)責人力

15. 大陸品牌資通訊設備清冊

一、依據行政院秘書長 109 年 12 月 31 日院臺護長字第 1090203566 號函辦理。

二、依據彰化縣政府 110 年 1 月 5 日府計資字第 1090486463 號函辦理。

主旨:中華民國 110 年 1 月 5 日-有關盤點大陸廠牌資通訊產品案(本府 109 年 12 月 23 日府計資字第 1090468346 號函諒達），請將涉及資通訊軟體、硬體或服務相關採購案之委外廠商 (含分包廠商)納入盤點對象，請查照並轉知所屬。

1. 資通安全管理代表及推動小組成員分工表

彰化縣新庄國民小學
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： 112 年 08 月 01 日

組別	單位-職稱	職掌分工業務事項	備註 （督導附件表單）
資安長	教務處-教務主任	-督導學校資通安全相關事項 -召開管理審查會議	督導本機關資安維護計畫 1. 本機關資通安全處理小組名冊及分工表
策略規劃組	教務處-資訊組長	-依據資通安全目標擬定年度工作計畫 -訂定本機關資通安全相關規章與程序、制度文件之執行 -資通安全事件之通報及應變機制之執行 -辦理本機關相關資通安全研習、教育訓練	5. 本機關資通安全教育訓練計畫及教育訓練簽到表 10. 本機關資通安全維護計畫實施情形 11. 本機關審查結果及改善報告 12. 本機關改善績效追蹤報告
資安防護組	學務處-學務主任 總務處-總務主任	-傳達資通安全政策與目標 -資料及資通系統之安全防護事項之執行 -資訊及資通系統之盤點及風險評估 -本機關內部稽核/委外廠商資安稽核 -資通安全事件演練	4. 本機關資通系統資產清冊與風險評鑑彙整表 15. 本機關大陸品牌資通訊設備清冊 6. 本機關管制區域人員進出登記表 7. 本機關委外廠商執行人員保密同意書(合約) 8. 本機關委外廠商執行人員保密切結書(個人) 9. 本機關內部稽核/委外廠商查核項目表

1. 資通安全管理代表及推動小組成員分工表

有效管理組	人事處-人事主任 會計處-會計主任	-其他資通安全事項之規劃、辦理與推動 -權限控管 -保密切結書保管 -資通安全獎懲考核 -控管資安經費預算	2. 本機關員工保密切結書 3. 本機關資通安全需求申請單 13. 本機關經費配置表 14. 本機關專職(責)人力

全處理小組承辦人員：教師兼資訊組長蘇志祥　　資安長：[illegible]校長吳文輝

2. 資通安全保密同意書本表單所蒐集之個人資料僅限於特定目的內之使用，非經當事人同意絕不轉做其他用途(特定目的外之利用)，亦不會公布任何資訊，並遵循本府資安及個資保護管理規範。

資 通 安 全 保 密 切 結 書

立切結書人_____(以下簡稱本人)在_彰化縣新庄國民小學_(以下簡稱本機關)服務期間，將落實本機關資安政策與目標，恪守本機關資通安全管理規範、法令法規要求以及下列事項：

1、本人無論在職或離職，對各項業務機密負完全保密之責。

2、本人所知悉或持有之資料或文件，包括但不限於口頭、書面或電磁紀錄等形式之資料，非經事前書面同意，在職期間或離職後皆不得以任何形式留存暨利用。

3、任職期間職務上任何經辦、保管或接觸須保密之訊息資料(包含個人資料)，除依法令應公開者外，本人保證僅限於本機關之營運及行政目的之使用，非經同意絕不擅自洩漏、複製、交付、竄改、竊取或以其他任何方式交予第三者。如有違反之情事，經查證屬實，除依本機關規章懲處外，並負一切相關民事、刑事責任。

4、本人於本機關使用之電腦軟體遵守智慧財產權之規定，絕不擅自複製、傳播任何侵害智慧財產權之任何程式、軟體，違者願負民事、刑事責任。

此　致

立切結書人：_____（簽章）

身分證後四碼：_____

聯絡電話：_____

通訊住址：_____

中　　華　　民　　國　　年　　月　　日

風險評鑑工作表

單位名稱:彰化縣和美鎮新庄國民小學

紀錄編號：

列印日期：1120308

資訊資產鑑別與評價								風險評鑑(評估與分析)				
No.	資產名稱	資產類別		資產價值評估				脆弱點評估		威脅評估		風險估計
		大類	小類	機密性(C)	完整性(I)	可用性(A)	合計	弱點名稱	脆弱度(V)	威脅名稱	威脅發生機率(T)	風險值小計
1	Ruckus L3-ICX-7250/網路交換器	硬體類	網路設備	1	1	1	3	不良的通行碼（password）管理	1	出非授權的人員使用軟體	1	3
2	全球資訊網管理人員	人員類	編制內人員	1	1	1	3	不足的維護或儲存媒體錯誤的安裝	1	使用人員的錯誤	1	3
3	學校校務系統管理人員	人員類	編制內人員	1	1	1	3	不足的安全訓練及認知	1	使用人員的錯誤	1	3
4	負責學務系統管理人員	人員類	編制內人員	1	1	1	3	不足的維護或儲存媒體錯誤的安裝	1	使用人員的錯誤	1	3
5	負責學術防火牆管理	人員類	編制內人員	1	1	1	3	不足的安全訓練及認知	1	使用人員的錯誤	1	3
承辦人員								權責主管				

5.資通安全教育訓練計畫及教育訓練簽到表

彰化縣新庄國民小學113年度資通安全教育訓練計畫

壹、依據

彰化縣新庄國民小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:

本機關所屬人員：

人員類別	人數
資訊人員（系統管理者）	1
一般人員	55
主管人員（校長及主任）	7
共計	63

肆、訓練項目

人員類別	訓練課程名稱	應取得時數
資訊人員（系統管理者）	用戶端資安與APT攻擊 校園常見資安事件與防毒軟體應用	3小時
一般人員	資訊安全基礎認知	3小時
主管人員（校長及主任）	資訊安全基礎認知	3小時

伍、訓練期程（113年12月16日前完成訓練）

由各機關自行排定教育訓練期程。

陸、訓練方式

一、本機關採行教育訓練方式為線上課程。

二、至數位學習資源整合平臺「磨課師+」(https://moocs.moe.edu.tw/moocs/#/home)線上修習包含資安管理制度、社交工程攻擊防護、個人資料保護、行動裝置使用安全、物聯網資安威脅等資安課程取得上述應取得之研習時數。

三、線上教育訓練後，將研習證明匯至指定雲端資料夾中。

5.資通安全教育訓練計畫及教育訓練簽到表

彰化縣○○國民○學　資通安全教育訓練

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：○○○年○○月○○日 8：00 — 9：00

地　　點：○○○會議室

單　位	職　稱	姓　名	簽　名
○○室	○○組長	○○○	

6.管制區域人員進出登記表

彰化縣新庄國民小學　管制區域人員進出登記表

編號：

製表日期：113 年 01 月 01 日

編號	姓名	單位	陪同人員	日期	進入時間	離開時間	事由	進出設備	攜帶物品
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									

註：陳核層級請學校依需求調整

承辦人員：　　單位主管：

7.委外廠商執行人員保密同意書

彰化縣新庄國民小學　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**彰化縣新庄國民小學**（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

8.委外廠商執行人員保密切結書

彰化縣新庄國民小學　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**彰化縣新庄國民小學**（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，並將其黏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

9.內部稽核/委外廠商查核項目表

彰化縣新庄國民小學 內部稽核查核項目表
委外廠商查核項目表

編號：

填表日期：113 年 01 月 03 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1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。
	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？	■	□	□	陪同進出人員監督其活動。

9.內部稽核/委外廠商查核項目表

	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？	□	■	□	主機房天花板漏水，已通知總務處修繕。
	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。
	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。

9.內部稽核/委外廠商查核項目表

	5.27 通行碼長度是否超過 8 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
	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 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 。
	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
	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。

註:陳核層級請學校依需求調整

資安推動小組承辦人員:教師兼資訊組長蘇志祥　　資安長:新庄國小校長吳文輝

11.審查結果及改善報告

彰化縣新庄國民小學　審查結果及改善報告

範圍	全機關
日期	113 年 ○○ 月○○ 日
審查日期	113 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				
資通安全推動小組 承辦人員			資安長	

彰化縣和美鎮新庄國民小學(2.16.886.111.90010.90003.100004) D級 112年實施情形-附表2-經費配置-檢視

被填寫機關：彰化縣和美鎮新庄國民小學(2.16.886.111.90010.90003.100004) D級

註：此畫面為2024年(113年)填寫2023年(112年)的實施情形、附表1~3、應辦事項。
註：預算單位為「元」(不是「千元」)，若填寫非整數，系統將強制當試轉換。
註：去年填寫資料：「機關年度實施情形提報(109年)」/「查詢、匯出填報資料」/「附表2-機關經費-查詢、匯出填報項目」
註：每一機關只有一筆，故不提供「新增」、「刪除」、「匯入填寫」功能。
註：「機關年度經費」應與各年度法定單位預算數相符；「年度資訊經費」原則應包含在「機關年度經費」之內；「年度資安經費」原則應包含在「年度資訊經費」之內。
註：此表係為了解機關之資訊、資安經費配置占比，若機關有其他基金、特別預算、預算外補助等，也可一併加總計算填入此表(若機關全數經費來源為基金也請一併填入)。
註：數值不得有負數、小數點

填表說明：
一、資訊經費係指各機關之業務費、設備及投資費。
(一)業務費(經常門)：
教育訓練費：凡各機關、學校處理經常一般公務或特定工作計畫所需之各項業務費用屬之。凡對現職員工實施教育訓練所需補貼(補助)有關學分費、雜費、教材、膳宿及交通費等費用屬之。

資訊服務費：凡公務所需使用資訊操作、維修、購買雲端等服務費用、金額未達1萬元之軟體購置或屬營業租賃性質之資訊設備租金屬之。

(二)設備及投資(資本門)：
(1)資訊軟硬體設備費：凡公務所需各項電腦設施、週邊設備、裝置（含一次購買時所配置 之套裝軟體，如作業系統軟體，以及後續2年以上效益之軟體改版、升級與應用系統開發規 劃設計）及雲端服務等購置（含資本租賃）費用屬之。

二、資安經費(經常門、資本門)：辦理資通安全管理法及其子法之法遵事項相關經費。

說明：

實施情形(112)-附表2-經費配置-檢視

流水編號	2560
被填機關OID	2.16.886.111.90010.90003.100004
被填機關名稱	彰化縣和美鎮新庄國民小學

核定機關資安等級	D

111年機關預算執行：

本機關未獨立編列預算(112年)	☐
1.機關年度預算執行情形-資本門(112年)	285000
2.機關年度預算執行情形-經常門(112年)	89909000
3.年度資訊預算執行情形-資本門(112年)	176477

4.年度資訊預算執行情形-經常門(112年)	143185
5.年度資安預算執行情形-資本門(112年)	0
6.年度資安預算執行情形-經常門(112年)	8000

112年機關預/概算配置(如已審議填預算)：

本機關未獨立編列預算(113年)	☐

7.機關年度預算-資本門(113年)	232000
8.機關年度預算-經常門(113年)	94352000
9.年度資訊預算-資本門(113年)	181000
10.年度資訊預算-經常門(113年)	20000
11.年度資安預算-資本門(113年)	0
12.年度資安預算-經常門(113年)	20000

112年資通安全自主產品經費調查

13. 機關年度資通安全硬體產品經費(112年)	0
14. 機關年度資通安全軟體產品經費(112年)	8000
15. 機關年度資通安全服務經費(112年)	0
最後填寫者-機關OID	2.16.886.111.90010.90003.100004
最後填寫者-機關名稱	彰化縣和美鎮新庄國民小學
最後填寫者-更新時間	2024/4/8 上午 08:11:20

本網站設計支援Windows 10或更新版平台，瀏覽器 Edge 或 Chrome 最新版，最佳瀏覽解析度為1366 x 768或以上

14.機關專職(責)人力

機關名稱	姓名	職稱	人員屬性(職聘僱或委外)	是否專職	持有之有效專業證照張數	持有之有效職能評量證書張數
彰化縣新庄國民小學	蘇志祥	資訊組長	兼辦	否	0	0

填表說明：

1、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，無須設置資通安全專職（責）人員，但目前機關透過「資通安全推動小組」兼辦資通安全相關業務。