基隆市中正區正濱國民小學

資通安全維護計畫

版次：V2.0(第二版)

機密等級:一般

修訂人核章	
單位主管核章	
資安長核章	

中 華 民 國 1 0 9 年 0 7 月 0 8 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	修訂內容	修訂單位	修訂人	核定人 （資安長）
V1.0(初版)	107年12月25日	新擬訂文件	正濱國小	許慧文	王春奎
V2.0(第二版)	109年07月01日	更新內容 （資通系統清單、通訊軟體安全）	正濱國小	許慧文	王春奎

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。

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、基隆市政府資通安全政策。

貳、適用範圍

本計畫適用範圍涵蓋本全校。

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
教務業務	基隆市校務行政系統	為本校依組織法執掌，足認為重要者。	影響部分教學業務運作	由上級管理單位訂之
學生事務	基隆市校務行政系統含門禁系統	為本校依組織法執掌，足認為重要者。	影響部分教學業務運作	由上級管理單位訂之
總務業務	基隆市基層公文線上簽核系統	為本校依組織法執掌，足認為重要者。	影響部分業務運作	由上級管理單位訂之
輔導業務	基隆市校務行政系統	為本校依組織法執掌，足認為重要者。	影響部分業務運作	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	非核心資通業務	業務失效影響說明	最大可容忍中斷時間
教務業務	國民小學及國民中學學生學習扶助資源平臺	影響學校部分教學業務運作	3天
教務業務	教育部國民及學前教育署人力資源網	影響學校部分教學業務運作	3天

學務業務	教育部校園安全暨災害防救通報處理中心	影響學校部分業務運作	3天
學務業務	教育部特殊教育通報網	影響學校部分業務運作	3天
總務業務	財產管理系統	影響學校部分業務運作	3天
總務業務	綠色採購資訊網	影響學校部分業務運作	3天
總務業務	政府電子採購網	影響學校部分業務運作	3天
總務業務	台灣銀行網路銀行	影響學校部分業務運作	3天
總務業務	庫款支付管理系統	影響學校部分業務運作	3天
總務業務	勞健保E化服務系統	影響學校部分業務運作	3天
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天
會計業務	地方教育發展基金成立附屬單位會計執行系統	會計部份業務無法運作	3天
會計業務	支付管理系統	會計部份業務無法運作	3天
會計業務	EBAS全國主計網	會計部份業務無法運作	3天
出納業務	郵局傳輸系統	影響學校部分業務運作	3天
出納業務	薪資管理系統	影響學校部分業務運作	3天
午餐業務	教育部校園食材登陸平台	影響學校部分業務運作	3天
資訊業務	學校網站(向上管理)	影響學校部分業務運作	3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. 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業務之機密性與完整性，避免未經授權的存取與竄改。
3. 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業務帳號。
7. 落實資通安全通報機制。

二、資通安全目標

1. 提報教育機構資安通報平台之資通安全 3、4 級事件不得發生，1、2 級事件發生應為 5 件以下(含)。知悉資安事件發生，能於規定時間內完成通報、應變及復原。
2. 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。
3. 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。
4. 每人每年接受三小時以上之一般資通安全教育訓練。
5. 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(資通安全長)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，本校訂定校長為資通安全長，負責督導學校資通安全相關事項，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、專職人力及經費配置

一、專職人力及資源之配置

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，最低應設置資通安全兼辦人員 1 人，本校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，得洽請基隆市教育處資訊小組或相關專業機構，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. 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、服務資產等。
2. 資訊及資通系統資產項目如下：

資產類別	資產項目
資訊資產(未含有個資)	一、業務資料檔案，例如：XX業務檔案。 二、系統資料檔案，例如：資料庫檔案、應用程式檔案及備份檔案等。 三、電子化儲存之文件檔案，例如：系統或軟體使用手冊及教育訓練教材等。 四、書面管理文件，例如：系統文件、使用手冊、各種程序及指引辦法等。 五、書面紀錄，例如：申請表單等。
軟體資產	一、系統軟體，例如：業務資訊系統、公文系統等。 二、資料庫軟體，例如：ORACLE、SQL Server等。 三、套裝軟體，例如：Windows10、Office等。
硬體資產	一、電腦設備，例如：伺服器、工作站、個人主機、筆記型電腦及PDA等。 二、通訊設備，例如：路由器、網路交換器、數據機、傳真機、印表機及影印機等。 三、儲存媒體，例如：隨身碟、磁帶、磁帶機、磁帶櫃、光碟及光碟機等。 四、其他支援設備，例如：監視器、不斷電系統、空調系統、消防系統、環控系統及機房用發電機等。
服務資產	一、一般維運支援性服務，例如：中華電信網路專線、市電系統、供水服務等。 二、委外服務，例如：XX公司網路安全服務、XX公司設備主機維護服務等、XX中央共構系統等。
人員資產	一、內部同仁，例如：資訊科同仁、約聘人員及替代役人員等。 二、外部(常駐型)人員，例如：XX公司駐點人員等。
個資資產	一、紙本個資，例如：通訊錄、報名表、履歷表等。 二、檔案形式個資，例如：個人電腦中或主機內個人資料檔案等。 三、資料庫個資，例如：資訊系統含有個人資料資料庫等。

3. 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」。

4. 資訊及資通系統之硬體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。

5. 各單位管理之資訊或資通設備如有異動，應即時通知資通安全推動小組更新資產清冊。

二、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、資訊及資通設備之管理

(一) 資訊及資通系統之使用

1. 本校同仁使用資訊及資通系統須遵守系統管理機關相關規範。
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。

二、存取控制與加密機制管理

(一) 網路安全控管

1. 本校區域劃分如下：

(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) ：本校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**防火牆統一由基隆市教育網路中心管理**統一辦理更新與升級，並適時向基隆市教育網路中心提出防火牆進出規則申請。

4. 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。

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. 本校網域名稱系統(DNS)統一設定**指向本市教育網路中心DNS**，統一由中心更新防護。

7. 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. 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。

(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. 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) 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) 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) 電子郵件安全管理

1. 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。

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。

5. 使用者使用電子郵件時，應注意電子簽章之要求事項。

6. 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，不使用或下班時應該上鎖。

(五) 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。

(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。

(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，應主動循本校之通報程序通報。

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。

四、資通安全防護設備

1. 本校應建置防毒軟體，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、電子郵件伺服器由**本市教育網路中心**管理更新與升級。

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，詳本校**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。

1. 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. 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。

(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。

3. 持續改善機制之管理審查應做成改善績效追蹤報告[1]，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. 本校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