耕莘健康管理專科學校
資通安全維護計畫

112.12.27

目錄

壹、 依據及目的

本計畫依據教育部要求及資通安全管理法第10條及施行細則第6條訂定，並參考引用本校現行之資通安全相關作業程序，以符合法令法規之要求。

貳、 適用範圍

本計畫適用範圍涵蓋耕莘健康管理專科學校全校(以下簡稱本校)。

參、 核心業務及重要性

一、核心業務及說明

本校之核心業務重要性及說明如下表：

項次	單位	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(小時)
1	教務處	依據「耕莘健康管理專科學校處務規程」教務處規章辦理	「整合式數位學習管理暨成效分析診斷系統」-漢龍-D教務系統	中	影響全校教務業務推行	4
2	學生事務處	依據「耕莘健康管理專科學校處務規程」學務處規章辦理	「整合式數位學習管理暨成效分析診斷系統」-漢龍-E學務系統	中	影響全校救貸、減免、獎助學金、生輔(獎懲、缺曠)、業務推行	24
3	總務處	依據「耕莘健康管理專科學校處務規程」總務處規章辦理	「整合式數位學習管理暨成效分析診斷系統」-漢龍-F學雜費註冊繳費系統	中	影響全校註冊繳費及銀行帳號相關業務推行	24

項次	單位	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（小時）
4	資訊暨圖書中心	依據「耕莘健康管理專科學校處務規程」資圖中心作業辦理	「耕莘健康管理專科學校」網站	中	影響全校官網及各系統入口可用性	24

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	業務失效影響說明	最大可容忍中斷時間
核心業務以外之業務及資通系統	對學校之營運、資產或信譽等方面將產生有限之影響	24小時

肆、　資通安全政策及目標

一、資通安全政策

本校制定「資通安全暨個資保護政策」，經校長核定，於公告日施行，並以書面、電子或其他方式通知教職員及與本校連線作業之有關機構、委外廠商及其他利害關係者，修正時亦同，詳細內容請詳參「資通安全暨個資保護政策」。

二、資通安全目標

為維護本校資訊資產之機密性、完整性、可用性與遵循性，期藉由本校全體同仁共同努力以達成下列目標：

1. 機密性：保護本校業務資訊之安全，確保敏感資訊以及個資需經授權才可存取。
2. 完整性：保護本校業務服務之的正確，避免未經授權之篡改。
3. 可用性：建立本校業務永續運作計畫，以確保本校業務服務之持續運作。
4. 遵循性：確保本校各項業務服務之執行須符合相關法令或法規之要求。

詳細內容請詳參「資通安全暨個資保護政策」及「資訊安全目

標管理作業程序」。

三、資通安全政策及目標之核定程序

資通安全政策經資訊安全推動小組通過，提請行政會議審議，陳校長核定後公布實施，修訂時亦同。

四、資通安全政策及目標之宣導

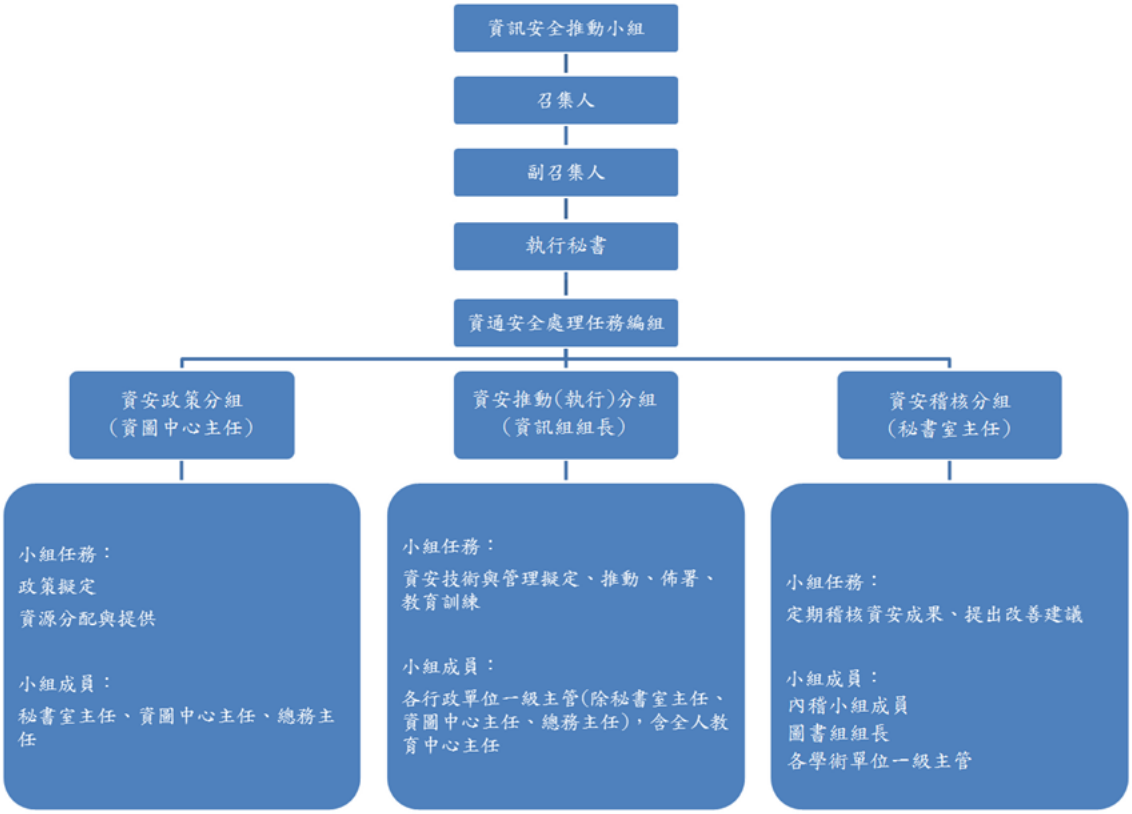
本校之資通安全政策及目標以內部公告及會議之方式，向學校內所有人員進行宣導；利害關係人(例如IT服務供應商、與學校連線作業有關單位)以本校全球資訊網進行傳達。

五、資通安全政策及目標定期檢討程序

本校資通安全政策及目標由資訊安全推動小組每年至少審查乙次，並視需要修訂，以反映政府法令、技術及業務等最新發展現況，並確保本校資安管理實務作業之有效性與合法性。

伍、 資通安全推動組織

為確保本校資訊安全管理制度之資訊安全責任，落實資訊安全政策之推行，成立「資訊安全推動小組」，負責監督與管理資訊安全制度。資訊安全推動小組設置召集人(資通安全長)一人，由副校長兼任；副召集人一人，由秘書室主任兼任，負責推動及協調本校個人資料保護管理業務；執行秘書一人，由資訊暨圖書中心主任兼任，負責綜理本小組相關業務。並設置本校資訊安全推動小組結構如下：



詳細內容請詳參「耕莘健康管理專科學校資訊安全推動小組設置要點」及「資訊安全組織作業程序」。

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及教育部與所屬機關(構)及學校資通安全責任等級分級作業之規定，為資通安全責任等級C級學校，應設置資通安全專責人員1人，其業務說明如下，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。

資通安全管理面業務(含系統安全管理業務)1 人，負責推動資通系統防護需求分級(含資通系統分級及防護基準、安全性檢測、業務持續運作演練等業務)、資通安全管理系統導入、內部資通安全稽核、教育訓練、資通安全防護設施建置、資通安全事件通報及應變等業務之推動。

（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，並提升學校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足，得洽請相關學者專家或專業學校（構）提供顧問諮詢服務。

(三)資通安全專責人員專業職能之培養(如證書、證照、培訓紀錄等)，應依據資通安全責任等級分級辦法之規定。資通安全專責人員應持有1張以上資通安全專業證照並持續維持其有效性。

(四)本校負責重要資通系統之管理、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，應簽署書面約定，並視需要實施人員輪調，建立人力備援制度。

(五)本校之校長、副校長及各單位主管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。

(六)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)資訊安全推動小組配置相關經費及資源時，應考量本學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。

(二)各單位於規劃建置資通系統建置時，應一併規劃資通系統之資安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。

(三)各單位如有資通安全資源之需求，應配合學校預算規劃期程編列，並視需要提報至資通安全管理審查會審查，由資通安全推動小組視整體資通安全資源，經召集人（資通安全長)核定後，進行相關之建置。

(四)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、 資通系統及資訊之盤點

一、資通系統及資訊盤點

(一)本校已制定「資訊資產管理作業程序」，並依程序規範辦理資通系統及資訊資產盤點及價值鑑別，同時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，分別為人員、文件、軟體、通訊、硬體、資料、環境等7大類，詳細內容請參閱「資訊資產管理作業程序」。

(二)資通系統及資訊資產項目請參閱「資訊資產管理作業程序」。

(三)本校每年度應依資訊及資通系統盤點結果 ，製作「資訊資產清冊」 ，欄位應包含：資通系統及資訊名稱、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。

(四)各成員管理之資訊或資通系統如有異動，依照「資訊資產異動程序」辦理。

(五)資通系統及資訊資產應之標示，依照「資訊資產管理作業程序」辦理。

二、資通安全責任等級分級

依據教育部與所屬機關(構)及學校資通安全責任等級分級作業規定及資通安全責任等級分級辦法規定，本校為私立專科校，資通安全等級為C級學校。

捌、 資通安全風險評估

一、資通安全風險評估

(一)本校為確保達成制度管理目標，並預防或減少非預期之影響，以達成持續改善，每年執行風險評鑑。

(二)執行風險評估時已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」，並依循「資通安全風險評鑑程序」進行風險評估之工作。詳細內容請參閱「資通安全風險評鑑程序」。

(三)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或委外開發之資通系統防護需求分級，並訂定「資訊資產盤點表」及「資通系統清冊」。

二、核心資通系統及最大可容忍中斷時間

請參閱本計畫參、一「核心業務及說明」。

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」所提出風險評估結果、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下：

一、資通系統及資訊之管理

(一)資通系統及資訊之保管

1. 資通系統及資訊管理人應確保資通系統及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. 資通系統及資訊管理人應確保資通系統及資訊被妥善的保存或備份。
3. 資通系統及資訊管理人應確保重要之資通系統及資訊已採取適當之存取控制政策。

詳細內容請參閱本校「資訊資產管理作業程序」及「存取控制管理作業程序」。

(二)資通系統及資訊之使用

1. 本校同仁使用資通系統及資訊前應經其管理人授權。
2. 本校同仁使用資通系統及資訊時，應留意其資通安全要求事項，並負對應之責任。
3. 本校同仁使用資通系統及資訊後，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通系統及資訊，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. 對於資通系統及資訊，宜識別並以文件記錄及實作可被接受使用之規則。

詳細內容請參閱本校「資訊資產管理作業程序」及「資訊資產異動作業程序」。

(三)資通系統及資訊之刪除或汰除

1. 資通系統及資訊之刪除或汰除前應評估學校是否已無需使用該等資通系統及資訊，或該等資通系統及資訊是否已妥善移轉或備份。
2. 資通系統及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。

詳細內容請參閱本校「資訊資產管理作業程序」及「資訊資產異動作業程序」。

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）：學校內部單位人員及內部伺服器使用之網路區段。
   (3)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。
2. 為確保網路服務及設備安全，本校之網路及網路安全相關設備（如：防火牆、DNS、網路交換器、無線網路等），皆進行相關安全設定與管理措施。

詳細內容請參閱本校「通信與作業管理作業程序」。

(二)資通系統權限及特權帳號之存取管理

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數字或特殊符號。
   (3)使用者每 6個月應更換一次通行碼。
2. 各項系統資源使用權限之申請、註冊及註銷作業管理，並維護相關之申請、註冊、註銷資料與紀錄，以備查核。
3. 特殊權限之授權管理，必須依執行業務系統別之需求，例如作業系統、資料庫管理系統、網路服務系統、監控管理系統等賦予系統存取特殊權限的授權，且以執行業務及職務所必要的最低資源存取授權為限。
4. 使用者職務異動或離職時，部門主管應即時填具「資訊系統帳號權限異動申請單」，通知相關單位調整或終止使用者之存取權限。

詳細內容請參閱本校「存取控制管理作業程序」。

(三)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)一旦加密資訊有遭破解跡象，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

本校之系統主機及個人電腦皆已安裝防毒軟體並定期更新病毒碼，並進行必要之軟硬體更新。詳細內容請參閱「通信與作業管理作業程序」。

(二)遠距工作之安全措施

1. 所有資訊資源使用者，非經主管授權或允許，禁止執行遠端存取之作業。
2. 遠端存取作業應填具「外部連線申請／異動申請書」，經單位主管簽准後，向資圖中心資訊組提出申請。

詳細內容請參閱本校「通信與作業管理作業程序」。

(三)電子郵件安全管理

為確保本校同仁使用電子郵件之使用安全，本校已制定相關規範本校同仁應遵守電子郵件使用規定，並配合教育部電子郵件社交工程演練作業，以提醒同仁提高警覺，詳細

內容請參閱本校「通信與作業管理作業程序」。

(四)確保實體與環境安全措施

為確保實體與環境安全管理,本校已制定相關規範以維護管制區域之關鍵設施與相關資訊資產之機密性、完整性及可用性，詳細內容請參閱本校「電腦機房管理作業程序」及「實體安全管理作業程序」。

(五)資料備份

為促使本校在進行各項資訊備份時有一明確之規範,以確保資料的完整性與可用性，本校已制定相關規範，詳細內容請參閱本校「通信與作業管理作業程序」及「日常操作管理作業程序」。

(六)媒體防護措施

為確保儲存媒體使用之安全,本校已制定相關規範以確保同仁於使用儲存媒體時，執行安全控制措施，並規範媒體報廢或再使用之規定，詳細內容請參閱本校「日常操作管理作業程序」、

「資訊資產管理作業程序」及「資訊資產異動作業程序」。

(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。

(八)行動裝置之安全管理

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，用戶端應有身分識別及認證機制。

四、系統獲取、開發及維護

本校之資通系統應依「資通安全責任等級分級辦法」附表九規定完成系統防護需求分級，並依分級之結果完成附表十中「資通系統防護基準」，另為確保應用系統之獲取、開發及維護符合資通安全要求，本校針對系統開發及維護流程已制定相關規範，以確保系統開發及維護過程與資料之機密性、完整性與可用性，詳細內容請參閱本校「系統開發與維護作業程序」。

五、業務持續運作演練

本校關鍵業務應擬定「業務永續運作計畫」且每年測試演練，本校針對業務持續運作流程已制定相關規範，以確保關鍵業務之可行性，詳細內容請參閱本校「業務永續運作管理作業程序」及「災難復原作業程序」。

六、執行安全性檢測

本校資訊組每2學年進行資訊安全檢測（至少包含弱點掃描、資通安全健診，若為高等級之資通系統則需執行源碼掃描與滲透測試等），並提供安全檢測結果給託管理單位，由資訊組協助託管理單位執行修補作業，且於修補完成後驗證完成改善，並將結果改善情形登載於「安全性檢測（弱掃、滲透、源碼）管考表」。

七、執行資通安全健診

本學校每2年應辦理資通安全健診，其至少應包含下列項目，並檢討執行情形：

(一)網路架構檢視。

(二)網路惡意活動檢視。

(三)使用者端電腦惡意活動檢視。

(四)伺服器主機惡意活動檢視。

(五)目錄伺服器設定及防火牆連線設定檢視。

八、資通安全防護設備

(一)本學校應建置防毒軟體、網路防火牆、電子郵件過濾裝置及資通安全弱點通報機制（VANS），持續使用並適時進行軟、硬體之必要更新或升級。

(二)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，本校已

訂定資通安全事件通報、應變及演練相關機制，詳細內容請參閱本校「資訊安全暨緊急應變管理規範」、「安全事件管理作業程序」及「緊急應變與處理作業程序」。

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

本校接獲資通安全情資後，應指定資通安全專責人員進行情資分析，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學校、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學校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

由資通安全專責人員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。

(四)涉及核心業務、核心資通系統之情資

資通安全專責人員應就涉及核心業務、核心資通系統之情資評估其是否對於學校之運作產生影響，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，詳細內容請參閱本校「委外管理作業程序」。

壹拾參、　資通安全教育訓練

為提升本校教職員資通安全意識與專業知識，本校每年應編列資通安全教育訓練經費，規劃相關資安教育訓練課程，或派員接受外單位辦理之專業資安課程，詳細內容請參閱本校「人員安全與教育訓練作業程序」。

一、資通安全教育訓練要求

(一)本校資通安全專責人員每年至少接受12小時以上之資安專業課程訓練或資通安全職能訓練。

(二)本校資訊人員每人每二年至少接受3小時以上之資通安全專業課程訓練或資通安全職能訓練，且每年接受3小時以

上之資通安全通識教育訓練。

(三)本校之一般使用者與主管，每人每年接受3小時以上之資通安全通識教育訓練。

二、資通安全教育訓練辦理方式

(一)本校應於每年年初，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，以建立同仁資通安全認知，提升本校資通安全水準，並保存相關之資通安全認知宣導及教育訓練紀錄。

(二)本校資訊安全教育及訓練的內容宜包括：本校資訊安全政策、資訊安全管理辦法、資訊安全暨緊急應變管理規範、安全責任、各資訊系統之安全防範或資料交換、機密性或敏感性資料之妥善收藏、如何正確使用資訊設備與資訊管理系統，以及作業相關處理程序之等資通安全通識教育訓練。

(三)新進人員正式執行操作前，應先安排作業及相關處理程序之教育訓練。

(四)資通安全教育及訓練之政策，除適用所屬教職員外，對學校外部的使用者，亦應一體適用。

詳細內容請參閱本校「人員安全與教育訓練作業程序」。

壹拾肆、　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，依據本校教職員工獎懲辦法、教職員工獎懲標準以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

為落實本校資通安全維護計畫，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，應與本學校之資通安全政策、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紀錄。

二、資通安全維護計畫實施情形之稽核機制

本校資通安全維護計畫實施情形稽核作業

本校應定期辦理資訊安全內部稽核作業以及視需要不定期執行專案稽核，　使本校資通安全管理能達到持續改善之目的，詳細內容請參閱本校「資訊安全稽核作業程序」。

三、本校稽核改善報告

本校應針對資通安全管理制度運作過程中發生之不符合事項及潛在之風險，採取相關的矯正及預防措施，以防止類似事

件發生，進而達成持續改善之目標，本校已訂有相關規範，詳細內容請參閱本校「矯正及預防管理作業程序」。

四、資通安全維護計畫之持續精進及績效管理

(一)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。

(二)管理審查議題應包含下列內容:

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：

(1) 資通安全政策及目標之實施情形。

(2)資通安全人力及資源之配置之實施情形。

(3)資通安全防護及控制措施之實施情形。

(4)內外部稽核結果。

(5)不符合項目及矯正措施。

5.利害關係人的回饋。

6.風險評鑑的結果與風險處理計畫執行進度。

7.持續改進的機會。

8.重大資通安全事件之處理及改善情形。

(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

本校依據資通安全管理法第12條之規定，應向上級或監督機關，提出資通安全維護畫實施情形，使其得瞭解本校資通安全維護計畫實施情形。

壹拾柒、 相關法規、程序及表單

一、相關法規及參考文件

(一)資通安全管理法

(二)資通安全管理法施行細則

(三)資通安全責任等級分級辦法

(四)資通安全事件通報及應變辦法

(五)資通安全情資分享辦法

(六)特定非公務機關資通安全維護計畫實行情形稽核辦法
(七)教育部與所屬機關(構)及學校資通安全責任等級分級作業
(八)資通安全暨個資保護政策
(九)伺服器管理作業程序
(十)系統開發與維護作業程序
(十一) 宿舍網路申請作業程序
(十二) 資訊專業教室借用作業程序
(十三) 電腦安裝及維修作業程序
(十四) 電腦機房管理作業程序
(十五) 日常操作管理作業程序
(十六) 資訊資產管理作業程序
(十七) 資訊資產異動作業程序
(十八) 人員安全與教育訓練作業程序
(十九) 委外管理作業程序
(二十) 緊急應變與處理作業程序
(二十一) 資訊安全暨緊急應變管理規範
(二十二) 災難復原作業程序
(二十三) 安全事件管理作業程
(二十四) 校園網路智慧財產權疑似侵權處理作業程序
(二十五) 矯正及預防管理作業程序
(二十六) 業務永續運作管理作業程序
(二十七) 關鍵業務障礙偵測與復原作業程序
(二十八) 實體安全管理作業程序
(二十九) 資訊安全組織作業程序
(三十) 文件管理作業程序
(三十一) 通信與作業管理作業程序
(三十二) 存取控制管理作業程序
(三十三) 資訊安全風險評鑑程序
(三十四) 資訊安全目標管理作業程序
(三十五) 資訊安全稽核作業程序

二、附件表單
(一)資訊資產清冊
(二)資通系統清冊
(三)資訊系統帳號權限異動申請單
(四)外部連線申請／異動申請書
(五)安全性檢測（弱掃、滲透、源碼）管考表

（六）業務永續運作計畫