（附件 10）

國立和美實驗學校資訊安全管理作業要點

102 年 10 月 8 日第 5 次擴大行政會議通過

壹、依據

「行政院及所屬各機關資訊安全管理要點」貳－五之規定訂定。

貳、目的

為強化本校資訊安全管理，確保電腦資料、系統、設備及網路安全，避免因人為疏失、蓄意破壞、資通危機事件或自然災害等風險，遭致資訊資產不當使用、洩漏、竄改、破壞等情事，而影響電腦作業系統正常運轉，建立安全及可信賴之電子化系統，積極落實資訊安全危機事件通報及相關應變作業之執行，特訂定資訊安全管理作業要點(以下簡稱本要點)。

參、適用範圍

本要點適用之管理範圍為本校教職員與學生個人資料處理及其相關資訊服務。

肆、組織架構及任期

為有效統籌、協調、研議本校各項資訊安全之政策、計畫及資源調度，特成立「國立和美實驗學校資訊安全管理小組」(以下簡稱本小組)。

本小組設置資訊安全長（召集人）1人由校長兼任之，資訊安全副組長由教務主任兼任之；執行秘書為設備組長兼任之；設置委員10至15人並由秘書、各處室主任、資訊專長人員共同組成；各處室主任、秘書及設備組長為各單位稽核人員，任期為1年。

伍、任務及權責分工

一、本小組職責如下：

(一)訂定資訊安全政策及管控機制。

(二)督導資訊安全政策之實施。

(三)稽核全校資訊安全。

(四)資訊安全事件通報、緊急應變及危機處理。

(五)規劃全校資訊安全教育訓練。

(六)其他資訊安全事項。

二、本小組各成員之任務／權責如下:

(一)資訊安全長：

由校長擔任本小組之召集人，綜理全校資訊安全管理作業協調與督導工作。

(二)資訊安全副組長：

1.協辦統籌資訊安全政策、計畫及技術規範之研議，及擬定或修正本校資訊安全管理政策。

2.督導及考核各單位資訊安全政策執行狀況及成效。

(三)執行秘書：

1.協助制定、執行及修正資訊安全政策。

2.決定單位內資安事件通報及應變處理事宜。

3.監督通報作業、應變計畫及資安演練之實施。

4.依據資安事件等級，授權系統復原作業之實施。

5.負責對校內外之資訊安全聯繫事宜。

6.負責鑑定資安事件並依程序進行通報作業。

7.隨時掌握國家資通安全會報或相關單位提供之資通安全危害通告資訊(如最新電腦病毒疫情、漏洞及駭客攻擊資訊等之預警訊息)。

8.發布資安訊息給校內所有人員，與系統管理人員保持連繫，並負責通告及監督系統漏洞修補與更新。

(四)稽核人員：

1.訂定稽核計畫，協助單位每年實施內部稽核 1 次。

2.依據資安檢核表評估單位整體資安風險，提出改善建議事項。

3.協助資安事件之偵防演練作業。

三、全體人員（含委外廠商）：配合及遵守資訊安全各項要求及規定。

四、本校每年進行一次資訊安全稽核。由各處室主任先做內部資安稽核(電腦安全自我檢查表)，發現問題記錄並反應至本小組協助處理。

陸、相關文件

一、教育體系資通安全管理規範

二、資訊安全政策

三、保密切結書

四、外部連絡清單

五、資訊服務申請表

六、委外廠商保密切結書

七、資訊安全事件報告單

八、人員資訊安全守則

柒、 本要點之實施範圍如說明：

一、資訊安全組織

(一)資訊安全長須每年至少召開一次資訊安全管理審查會議，討論內容包括如下：

1.資訊安全稽核與審查之結果。

2.來自利害相關者之回饋。

3.可用於組織以改進資訊安全績效與有效性之技術、產品或程序。

4.預防與矯正措施之執行狀況。

5.資安政策目標達成性衡量結果。

6.前次相關會議結論之跟催結果。

7.可能影響資訊安全管理作業之任何變更。

8.加強或改進資訊安全的其他各項建議。

(二)管理審查會議討論結果應包含：

1.資安政策目標之改進。

2.因為下列項目之變更，所進行之因應措施。

(1)各項營運要求。

(2)各項安全要求。

(3)影響既有各項營運要求之營運過程。

(4)法律或法規各項要求。

(5)契約的各項義務。

3.資源需求。

(三)管理審查會議應留存相關會議紀錄備查。

(四)資訊處理設備之使用，應具授權程序。

(五)本校教職員、代理代課教師、約聘（僱）人員、實習教師、替代役及工讀生等於到職時應簽署「保密切結書」（詳附件 10-1），課予機密維護責任。

(六)為確保資訊安全作業的順利運行，應建立能與相關外部團體（警消單位、主管機關、廠商等）即時連繫之「外部連絡清單」（詳附件 10-2）。

(七)任何資訊委外業務，皆應考量與包含資訊安全需求，且明訂廠商之資訊安全責任及保密規定，並列入契約。

二、資訊資產分類與管制

(一)為確實掌控資訊資產現況，各單位須編製資訊資產清冊（詳附件10-3），並定期更新。

(二)資訊資產應進行分類及分級，區分硬體類、軟體類、環境類、人員類、文件類及資料類，各類資訊資產依據機密等級分為 4 級：一般、限閱、敏感、機密。各級之評估標準如下：

1.一般：無特殊之機密性要求，可對外公開之資訊。

2.限閱：僅供組織內部人員或被授權之單位及人員使用。

3.敏感：僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用。

4.機密：為組織、主管機關或法律所規範之機密資訊。

5.資訊資產可依其機密等級進行標示，標示方式如下：

(1)實體設備之機密等級標示應以不同顏色標籤區分，一般等級者為藍色標籤；限閱等級者為綠色標籤；敏感等級者為黃色標籤；機密等級者為紅色標籤。

(2)文件類別之機密等級應於文件封面做明確的標示。

(三)考量重要資訊資產的需求，於必要時制定保護措施及處理流程。

三、人員管理及資訊安全教育訓練

(一)各單位對資訊相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要之考核；各單位對可存取機密性或敏感性資訊或系統之人員，及因工作需要須配賦系統存取特別權限之人員，應加強評估及考核。

(二)各單位負責重要資訊系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，實施人員輪調，建立人力備援制度。

(三)資訊作業相關人員離職時，應取消其個人帳號和使用權限，並確實做好資訊資產及相關文件之移交工作。

(四)各單位業務主管應負責督導所屬員工之資訊作業安全，防範不法及不當行為。

(五)資訊安全教育訓練及宣導事宜由本小組負責辦理，必要時，應請委外廠商人員一同參與資訊安全教育訓練。

(六)各單位若有資訊服務需求（如：帳號申請、電腦維修、系統開發或程式修改等），應填寫「資訊服務申請表」（詳附件 10-4），經權責主管核准後，交由資訊單位依需求處理。

四、電腦系統安全管理

(一)各單位辦理資訊業務委外作業時，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約中，要求廠商遵守及定期考核，並派員監督。

(二)電腦系統作業變更時，應詳實建立紀錄，以備查考。

(三)各單位應依相關法規或契約規定，複製及使用軟體；嚴禁使用非法軟體。

(四)電腦系統中應裝置防毒軟體並定期更新，磁片或隨身碟使用前應事先做掃毒檢查，以防止感染電腦病毒。

(五)應遵守智慧財產權相關規定，使用者應遵守軟體授權規定，禁止使用未取得授權的軟體。

(六)應依據電腦處理個人資料保護法等相關規定，審慎處理個人資訊。

五、網路安全管理

(一)各單位利用網路公佈及流通資訊時，應評估資料安全等級，機密、敏感性或未經當事人同意之個人隱私資料及文件，不得上網公佈。

(二)本校非屬機密性或敏感性之資料及文件得以電子郵件或其他電子方式傳送。機密性或敏感性之資料及文件，欲利用電子郵件或其他電子方式傳送時，須以適當的加密或電子簽章等安全技術處理。

六、系統存取控制

(一)各單位對電腦資料庫及檔案應建立分級(機密及安全等級)管理制度。

(二)各項正式作業之電腦系統操作及資料處理，由各權責單位指定專人負責建檔、核對、更新、審查及維護電腦資料之正確性。資訊系統發展人員非經核准不得操作使用或更改已正式作業之系統檔案。

(三)電腦資料庫及檔案，應按不同業務範圍及使用權限，分別設定目錄、識別保護碼；重要或具機密性資料在建檔或提供使用時，應加設通行

密碼、使用權限碼，以確保資料安全，且通行密碼應經常更新，並能三個月修改一次密碼。

(四)各單位離職、休職、調職人員，應立即取消使用單位內各項資源之所有權限和個人帳號並應通知資訊單位，並列入人員離職、休職、調職之必要手續；人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

(五)各電腦系統應建立系統使用者註冊管理制度，建立使用人員名冊。

(六)各單位之重要資料及系統委外廠商處理者，不論在機關內外執行，均應採取適當及足夠之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

(七)各項設備與系統相關之使用權限（例如使用者帳戶與作業權限）宜有授權紀錄，以備查核。

(八)系統管理人員結束系統操作應登出系統，並鎖定主控台螢幕。

(九)學校應建立校園網路拓樸圖，宜依業務性質之不同，區分不同內部網路網段，例如：教學、行政、宿網等，以降低未經授權存取之風險。

(十)網路管理人員應定期監控網路使用狀況，例如：網路流量、封包等，以及早發現異常狀況。

(十一)對於開放提供外部使用者或廠商存取之服務，必須限制使用者之網路功能以確保網路安全。

(十二)避免委外廠商使用系統管理者帳號（例如：Root、Adminstrator）或共用帳號，以釐清責任。

七、系統發展及維護安全管理

(一)各單位自行開發或委外發展之系統，應在系統之初始階段即將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動等作業，應予安全管制，避免不當軟體及電腦病毒危害系統安全。

(二)對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼；基於實際作業需要，得核發短期性及臨時性之系統辨識與通行密碼供廠商使用，但使用完畢後應立即取消其使用權限。

(三)委託廠商建置及維護重要軟硬體設施時，應在本校相關人員監督及陪同下始得為之，確認服務內容滿足合約之要求。

(四)本校委外廠商所執行之業務，若涉及個人隱私資料，承辦人員應要求其簽訂「委外廠商保密切結書」（詳附件 10-5）。並於服務契約中訂定委外廠商的安全處理責任。

(五)委外廠商（人員）異動、合約到期或其他因素服務終止時，承辦人員須確認其歸還各項設備、軟體、文件或鑰匙等，並取消或調整存取權限。

八、資訊資產安全管理

(一)各單位對於儲存各項機密資料或程式軟體之磁片、磁碟、磁帶、光碟片及報表等媒體，應設專人管理並定期備份，防止資料洩漏或損毀。

(二)對於需要長期保留或重要檔案之備份資料，應存放在防火、防潮、防磁的設備中。

九、通訊與作業安全管理

(一)資訊單位應建立資訊系統之安全控管機制，保護資料、系統及網路作業，防止未經授權之存取。

(二)伺服主機及網路設備應指定負責人，確保設備正常運作。

(三)新資訊系統、系統升級，正式上線前應適當的測試，並依驗收規定完成驗收。

(四)學校內電腦（伺服主機、個人電腦、筆記型電腦等）應安裝防毒軟體，定期更新病毒碼；伺服主機應定期掃描。

(五)各項系統資料（如：設定檔、網頁資料、伺服器日誌、資料庫等）應由系統負責人執行定期備份，並能定期進行回復測試演練。

(六)系統資料以可攜式儲存媒體保存時，應將該儲存媒體存放於上鎖儲櫃或安全處所。重要系統檔案或文件只有授權人員方能存取。

(七)可攜式儲存媒體若存有個人隱私資料，應加密儲存或實施安全控管措施。可攜式儲存媒體的遞送，應妥善包裝保護，做好安全保護措施。

(八)學校重要的資料檔案需訂有保存期限，並於超過保存期限時依相關規定刪除或銷毀。

(九)系統負責人變更系統作業程序時，應適時修改維護相關文件（如：系統文件、操作手冊等）。

(十)對外開放之資訊系統，其帳號密碼、個人資料等機密性資料傳輸過程應以加密方式處理，並妥善保管該資料，防止遭竊取或擅自挪作他途之用。

(十一)以電子郵件傳送含有個人隱私之資料時，宜以加密機制保護。

(十二)學校網頁資訊之公布，應經權責管理人員審查，確認內容未含個人隱私之資料及無違反學校規定與法令、法規之要求。

(十三)重要系統應留存電腦稽核紀錄，並妥善保護與保存至少三個月以上，以作為日後調查及監督之用。

(十四)系統管理人員發現資訊系統異常、駭客入侵等異狀時，應進行緊急應變處置並通報權責主管，並填寫「異常事件紀錄表」(詳附件 10-6)，留存系統異常處理紀錄備查。

(十五)系統管理人員應至少每季執行一次系統校時。

十、實體及環境安全管理

(一)各單位對於電腦設備之裝置地點，應考量使用及管理上之安全，並應指定專人負責管理，非經奉准之人員，不得隨意操作設備。管理或使用人員應詳細記載電腦設備故障、異常及維護等情形，以作為設備更新及作業安全之依據。

(二)電腦設備機房或電腦教室應設置適當之滅火設備。管理人員下班後應關閉門窗及不必要之電源，以確保安全。

(三)機房內應保持整齊清潔，並嚴禁飲食或堆置易燃物。

(四)機房宜設置足量之不斷電系統（UPS），確保重要資訊設備在非預期斷電情況下能具足夠電源完成緊急處置。

(五)冷氣機、不斷電系統（UPS）等機電設備及資訊處理設備之使用，應依照設備說明書指示操作，並施行檢查作業。

(六)資訊設備如送至校外維修時，應將內部敏感性的資料先備份後將資料刪除；資訊設備報廢與再使用時，應將含有個人隱私資料及有版權的軟體移除。

(七)禁止資訊設備在未經授權之情況下攜離所屬區域，若需將設備攜出，應填寫「設備進出紀錄表」（詳附件 10-7）。

十一、資訊安全事件之反應及處理

(一)資訊安全事件依影響等級區分為4個級別，由重至輕分別為「4級」、「3級」、「2級」及「1級」。

1.「4」級事件，符合下列任一情形者：

(1)法令、法規所規範應保護之資料外洩（例如：個人隱私資料）。

(2)重要系統或資料遭竄改、破壞或嚴重毀損。

2.「3」級事件，符合下列任一情形者：

(1)敏感資料外洩（如：財會資料、系統文件）。

(2)重要系統運作停頓，影響業務正常運作。

3.「2」級事件，符合下列任一情形者：

(1)內部行政資料外洩（如：校內行政資料）。

(2)非重要系統運作遭影響或系統停頓，已影響業務正常運作。

4.「1」級事件，符合下列情形者：

系統運作遭影響或系統停頓，不致影響業務正常運作。

(二)人員發現資訊安全事件，應即時通報，並記錄於「資訊安全事件報告單」（詳附件 10-8），並適當保護及留存相關證據資料。

(三)資訊安全事件確認處理完成後，相關單位應檢討現行管理措施之完整性，必要時進行檢討會議，討論改善之事宜。

十二、相關法規與施行單位政策之符合性

(一)學校應蒐集相關法律條文（如：智慧財產權、資料隱私保護及其他相關法規）、管理規定及合約要求，以確保相關作業符合要求。

(二)學校應定期進行弱點掃描或滲透測試，確保資訊系統之運行符合既定之安全實施標準，執行結果應留存紀錄。

(三)學校軟體的取得及個人資料之蒐集和處理，皆應符合各項法規規範。

(四)系統稽核工具之使用應審慎進行，避免造成系統中斷；系統稽核工具應妥善保管，避免遭誤用。

十三、業務永續運作之規劃

若發生資訊安全事件，應立即向相關人員通報，以採取適當反應措施。若有情節嚴重者，則聯繫檢警調單位協助偵查。

捌、違反規定之處理

本校全體人員未遵循上述規定者，視情節重大，提報本校相關考績（核）會議處。

玖、本要點經行政會議通過，陳　校長核准後公布實施，修正時亦同。