1 目的

為確保○○高級中學（以下簡稱「本校）資訊安全管理作業推行，符合資訊安全政策之目標，特訂定本作業要點。

2 適用範圍

本作業要點適用之管理範圍為本校○○所提供的各項資訊相關服務與個人資料為實施範圍。

3 權責

3.1 資訊安全長：由○○擔任，負責綜理資訊安全管理作業協調與督導工作。

3.2 資訊安全執行秘書：由○○擔任，負責規劃及管理資訊安全管理作業相關事宜。

3.3 執行小組：由○○擔任，負責執行資訊安全管理作業相關事宜。

3.4 稽核小組：由○○擔任，負責規劃及執行資訊安全管理作業稽核工作。

3.5 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。

4 相關文件

4.1 教育體系資通安全管理規範

4.2 資訊安全政策

4.3 保密切結書

4.4 外部連絡清單

4.5 資訊服務申請表

4.6 委外廠商保密切結書

4.7 資訊安全事件報告單

4.8 人員安全守則

5 作業說明

5.1 資訊安全組織

5.1.1 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：

5.1.1.1 資訊安全稽核與審查之結果。

5.1.1.2 來自利害相關者之回饋。

5.1.1.3 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。

5.1.1.4 預防與矯正措施之執行狀況。

5.1.1.5 資安政策目標達成性衡量結果。

5.1.1.6 前次相關會議結論之跟催結果。

5.1.1.7 可能影響資訊安全管理作業之任何變更。

5.1.1.8 加強或改進資訊安全的其他各項建議。

5.1.2管理審查會議討論結果應包含：

5.1.2.1 資安政策目標之改進。

5.1.2.2 因為下列項目之變更，所進行之因應措施。

5.1.2.2.1 各項營運要求。

5.1.2.2.2 各項安全要求。

5.1.2.2.3 影響既有各項營運要求之營運過程。

5.1.2.2.4 法律或法規各項要求。

5.1.2.2.5 契約的各項義務。

5.1.2.3　資源需求。

5.1.3管理審查會議應留存相關會議紀錄備查。

5.1.4 資訊處理設備之使用，應具授權程序。

5.1.5 本校教職員應簽署「保密切結書」(如附件一)，課予機密維護責任。

5.1.6 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」(如附件二)。

5.1.7 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。

5.2 資訊資產分類與管制

5.2.1 為確實掌控資訊資產現況，各單位須編製資訊資產清冊並定期更新(附件：資訊資產清冊)。

5.2.2 書面報告、磁性媒體、電子訊息及檔案資料等，宜標示適當的安全等級以利使用者遵循。

5.3 人員安全管理與教育訓練

5.3.1 ○○應依主管機關要求，辦理資訊安全教育訓練及宣導，強化教職員資訊安全認知，必要時，應請委外廠商人員一同參與資訊安全教育訓練。

5.3.2 人員離職，須依流程辦理資訊資產移交，並即時移除相關存取權限。

5.3.3 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」(附件三)，經權責主管核准後，交由資訊單位依需求處理。

5.3.4 本校教職員工之資訊安全管理相關規定，須遵守「人員資訊安全守則」。

5.3.5 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」(附件四)。

5.3.6 對於委外廠商提供之服務，承辦人員應監視和審查，確認服務內容滿足合約之要求。

5.3.7 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。

5.4 實體與環境安全

5.4.1 學校應採取適當防護措施以保障人員辦公處所安全。

5.4.2 重要資訊設施應設置於機房，並確保經授權人員方可進出。

5.4.3 機房應採取適當的控制措施與指引，確保其安全性。

5.4.4 機房內應保持整齊清潔，並嚴禁飲食或堆置易燃物。

5.4.5 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。

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

5.4.7 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。

5.4.8 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」(附件五)。

5.5 通訊與作業安全管理

5.5.1 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。

5.5.2 伺服主機及網路設備應指定負責人，確保設備正常運作。

5.5.3 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。

5.5.4 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；防毒伺服主機應設定定期掃描機制。

5.5.5 各項系統資料（如：設定檔、網頁資料、資料庫等）應由系統負責人執行定期備份。

5.5.6 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。

5.5.7 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。

5.5.8 可攜式儲存媒體的遞送，應妥善包裝保護。

5.5.9 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）。

5.5.10 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。

5.5.11 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。

5.5.12 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。

5.5.13 重要系統應留存電腦稽核紀錄，並妥善保護與保存，以作為日後調查及監督之用。

5.5.14 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」（附件六），留存系統異常處理紀錄備查。

5.5.15系統管理人員應每○執行一次系統校時。

5.6 存取控制安全

5.6.1 資訊系統使用權限之申請、異動應依「資訊服務申請表」流程辦理；使用權限之終止，應依離職程序辦理。

5.6.2 使用者職務異動或離職時，使用單位應通知資訊單位，調整或終止使用者之存取權限。

5.6.3 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。

5.6.4 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。

5.6.5 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。

5.6.6 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。

5.6.7 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。

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

5.7 系統開發與維護之安全

5.7.1 系統開發應包含安全性功能之規劃。

5.7.2 應用系統之資料輸入，應檢核、過濾主要欄位之資料輸入或資料內容，以確保資料的有效性及真確性。

5.7.3 輸出之資料，應確認其正確性；對於系統內之資料處理，則須保護其完整性。

5.7.4 作業系統變更，應審查與測試，以確保現行資訊系統與服務正常運作。

5.7.5 系統軟體應由系統負責人進行安裝，安裝時應視狀況通知相關技術人員支援或通知使用者，以避免資訊服務中斷或影響業務。

5.8 資訊安全事件之反應及處理

5.8.1 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」。

5.8.1.1 「4」級事件，符合下列任一情形者：

5.8.1.1.1 法令、法規所規範應保護之資料外洩（例如：個人隱私資料）。

5.8.1.1.2 重要系統或資料遭竄改、破壞或嚴重毀損。

5.8.1.2 「3」級事件，符合下列任一情形者：

5.8.1.2.1 敏感資料外洩（如：財會資料、系統文件）。

5.8.1.2.2 重要系統運作停頓，影響業務正常運作。

5.8.1.3 「2」級事件，符合下列任一情形者：

5.8.1.3.1 內部行政資料外洩（如：校內行政資料）。

5.8.1.3.2 非重要系統運作遭影響或系統停頓，已影響業務正常運作。

5.8.1.4 「1」級事件，符合下列情形者：

5.8.1.4.1 系統運作遭影響或系統停頓，不致影響業務正常運作。

5.8.2 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」(附件七)。

5.8.3 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。

5.9 相關法規與施行單位政策之符合性

5.9.1 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。

5.9.2 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。

5.9.3 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。

6 違反規定之處理

6.1 人員未遵循上述規定者，視情節重大，提報○○會議議處。

本作業要點由○○核准後公告實施，修訂時亦同。

附件一

保密切結書

本人 _____ 將嚴守工作保密規定與國家相關法令對業務機密負完全保密之責，並尊重智慧財產權。絕不擅自洩漏、傳播職務上任何業務相關資料及任職期間經辦、保管或接觸之所有須保密訊息資料；絕不擅自複製、傳播任何侵害智慧財產權之任何程式、軟體，違者願負法律責任。

此致

○○高級中學

立 同 意 書 人：_____

身 分 證 字 號：_____

電　　話：_____

住　　址：_____

中　華　民　國　　年　　月　　日

附件二

外部連絡清單

單位	聯絡人					備註
	職稱	姓名	電話	手機	電子郵件/地址	
XX 分局 XX 派出所 （警政單位）					XX 縣 XX 市 XX 路 XX 號	
XX 縣市消防局 XX 分隊 （消防單位）					XX 縣 XX 市 XX 路 XX 號	
法務部調查局 XX 縣市調查處 （檢調單位）					XX 縣 XX 市 XX 路 XX 號	
XX 縣市 地方法院 （檢調單位）					XX 縣 XX 市 XX 路 XX 號	
教育部電算中心 （主管單位）						
區域網路中心 （連線單位）						
中華電信 XX 營運處 （服務廠商）						
XXXX 空調設備行 （設備廠商）						
XXXX 股份有限公司 （軟/硬體採購、維修廠商）						

附件三

資訊服務申請表

申請人		部門主管		申請日期	年　月　日
事　由					
申請項目： □帳號/權限/密碼　□軟體安裝　□電腦維修 □資料需求　□其它資訊服務支援					
說　明： （以上由申請人填寫）					
審核結果：□同意　□不同意					
審核意見說明：					
承辦人簽章：			主管簽章：		
預定完成日期：					

附件四

委外廠商保密切結書

具保密切結廠商（人員）＿＿＿＿＿＿＿＿於民國＿＿年＿＿月＿＿日起於○○高級中學執行「＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿」業務（或專案），因而知悉　貴校機密或任何不公開之文書、電子資料、圖畫、消息、物品或其他資訊，將恪遵保密規定，未經　貴校書面授權，不得以任何形式利用或洩漏、告知、交付、移轉予任何第三人，如有違誤願負法律上之責任。

此致

○○高級中學

具切結書委外廠商（人員）：＿＿＿＿＿＿＿＿

身分證字號/護照號碼（人員）：＿＿＿＿＿＿＿＿

代　表　人（委外廠商）：＿＿＿＿＿＿＿＿

統 一 編 號：＿＿＿＿＿＿＿＿＿＿＿＿

地　　址：＿＿＿＿＿＿＿＿＿＿＿＿

中　華　民　國　年　月　日

附件五

填表日期：　　年　　月　　日

設備進出紀錄表

□攜入 □攜出	日期 時間	年　月　日 時　分	攜入/出人員 單　位	
設備名稱			設備序號	
設備 品牌/規格				
攜入/出方式	□自行攜入/出 □貨運代送(公司名稱/電話：_____ 貨運編號：_____) □其他(請說明：_____)			
攜入/出原因	□備份媒體異地儲存 □異地儲存之備份媒體送回 □新增設備 □設備送修(預計修復完成日期：　/　/　) □調 / □借 / □還 其他單位：_____ 聯 絡 人：_____ 聯絡電話：_____ (預計歸還日期：　/　/　) □其他(請說明：_____)			
覆核單位				
承辦人		權責主管		

附件六

填表日期：　　年　　月　　日

異常事件紀錄表

異常原因	異常項目：資產名稱：_____ 異常發現時間：　　年　　月　　日　　時　　分
處理說明	異常排除時間：　　年　　月　　日　　時　　分

承辦人	權責主管

附件七

資訊安全事件報告單

通報單位聯絡資料			
單位名稱		通 報 人	
電　　話		電子郵件	

資訊安全事件通報事項	
發生時間	____年____月____日____時____分
設備資料	IP 位址（無；可免填）： Web 位址（無；可免填）： 設備廠牌、機型： 作業系統名稱、版本： 已裝置之安全機制：

資訊安全事件資料				
事件影響等級	□4 級	□3 級	□2 級	□1 級
事件分類	□非法入侵	□感染病毒	□阻斷服務	□其他
破壞程度	□系統當機	□資料庫毀損	□網頁遭篡改	□其他
事件說明				
可能影響範圍及損失評估				
應變措施				

期望支援項目

解決辦法	
解決時間	____年____月____日____時____分

權責單位	會辦單位	資訊安全執行秘書