112 年度國立高級中等學校採購雲端版校務行政系統之資通安全及個人資料保護規範

一、廠商應遵守資通安全管理法、資通安全管理法 FAQ、國家機密保護法、資通安全管理法施行細則、資通安全責任等級分級辦法(包括資通安全責任等級 B 級之公務機關應辦事項及中級資通系統防護基準控制措施)、資通安全事件通報及應變辦法、資通安全情資分享辦法、個人資料保護法、臺灣學術網路各級學校資通安全通報應變作業程序、各機關對危害國家資通安全產品限制使用原則、受託者資通安全聯合查核指引、行政院及行政院國家資通安全會報技術服務中心頒訂之各項資通安全規範及標準、行政院及所屬各機關行動化服務發展作業原則、教育部、教育部國民及學前教育署(以下簡稱國教署)及學校所訂資通安全管理及個人資料保護相關規定。

二、廠商執行本案人員不得為陸籍人士，且應接受適任性查核；廠商不得提供及使用大陸廠牌或危害國家資通安全產品，並應符合「各機關對危害國家資通安全產品限制使用原則」規定。

三、廠商應將系統置於國教署指定之機房，並接受國教署之監督及管理。機房基礎設備及資源(例如：電力、網路、空調、消防、門禁、錄影監視、機櫃、虛擬主機、儲存空間、網路 IP、機房管理人力)、Windows Server 作業系統及 Microsoft SQL Server 資料庫系統，由國教署提供，廠商不得再向學校收取相關費用。

四、系統之資通系統防護需求分級為「中級」之「核心」資通系統(機密性、完整性、可用性及法律遵循性均列為中級)，最大可容忍中斷時間(MTPD)為 24 小時、系統復原時間目標(RTO)為 24 小時、可容忍資料損失時間(RPO)為 24 小時。廠商應依資通安全責任等級分級辦法執行中級資通系統防護基準控制措施；惟可歸責於學校、國教署或機房之事由，致相關控制措施無法執行者，不在此限。

五、系統應於 112 年 12 月 31 日前導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，並將導入佐證資料送國教署備查。

六、廠商應配合國教署辦理系統主機弱掃、網頁弱掃、滲透測試、源碼檢測、資安健診(包含網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定檢視)等安全性檢測，並提供檢測環境或原始碼；於收到檢測報告 2 週內，應完成 OWASP TOP 10 及中級以上之風險修補，或提交風險處理計畫送國教署備查。

七、廠商應配合國教署導入資通安全威脅偵測管理機制(SOC)、政府組態基準(GCB)、資通安全弱點通報機制(VANS)、端點偵測及應變機制(EDR)、應用程式防火牆(WAF)、伺服器負載平衡(SLB)、防毒軟體、網路防火牆、入侵偵測及防禦機制、電子郵件過濾機制等資通安全軟體、硬體及服務，並排除導入過程相關問題。

八、廠商應配合國教署辦理定期稽核與專案稽核，並提供系統相關佐證文件；廠商於收到稽核報告1個月內，應完成稽核發現缺失事項改善，或提交風險處理計畫送國教署備查。

九、廠商交付之軟硬體及文件，應先行檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)，提出安全性檢測證明，涉及利用非受託者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。廠商於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。

十、廠商所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。

十一、廠商應確實執行組態管理(Configuration Management)，以確保系統之完整性及一致性。

十二、廠商於知悉發生資通安全事件後，應於30分鐘內通報學校及國教署，通報內容包括發生或知悉時間、狀況之描述、等級之評估、因應事件所採取之措施、外部支援需求評估及其他相關事項。廠商應協助相關證據之保全(例如：維護現場完整，避免改變數位證據原始狀態，確保非相關人員進出資安事件現場)，並配合國教署於資通安全事件通報及應變辦法所訂時間內，完成資通安全事件之通報、應變、鑑識、調查、處理及改善，並繳交書面報告。

十三、廠商應配合國教署每年辦理1次業務持續運作演練及1次資通安全事件通報演練。

十四、廠商人員每年應參加國教署辦理之3小時以上資通安全通識教育訓練及3小時以上資通安全專業課程訓練或資通安全職能訓練。

十五、廠商應實施之資訊及資通系統之盤點及風險評估：

(一)建立資通系統及資通資產目錄，並隨時維護更新。

(二)各項資產應有明確之管理者及使用者。

(三)進行資訊、資通系統分級與處理之相關規範。

(四)進行資訊、資通系統之風險評估，並採取相應之控制措施。

十六、廠商每年至少應完成1次防火牆規則檢視作業(含內建防火牆)，移除不適當之防火牆規則(例如：對外國IP開放之防火牆、對特定IP開通所有的埠號)以確保：

(一)規則設定允許通過的範圍適當。

(二)關閉不提供服務之主機連線規則。

(三)避免重複設定的規則佔用系統資源。

十七、廠商應實施之系統日誌管理：

(一)系統應保存系統日誌或建置系統記錄伺服器，以保存軌跡及歷程紀錄，並具有不可否認性。

(二)廠商每3個月至少應執行1次主機紀錄檔及防火牆紀錄檔(log review)檢視作業。稽核系統主機及所連線之防火牆，針對所有管理者及使用者帳號執行之各項紀錄檔，以助於事前預防及發生資安事件之追查。

十八、廠商就其人員及系統，應實施帳號、密碼及權限管理：

(一)應符合最小權限管理原則，僅允許使用者(或代表使用者行為之程序)依學校任務及業務功能，完成指派任務所需之授權存取。進行授權決定時，應考量該使用者(或代表使用者行為之程序)之業務性質與範圍，限制其所能存取的系統功能及資料。

(二)廠商管理系統(包括應用系統、作業系統、資料庫、網路設備系統)之最高管理者權限帳號數量，至多以3個為限。

(三)廠商應符合以下身分驗證及帳號管理原則：

1.禁止使用身分證字號、學校代碼或其他公開資訊作為帳號及密碼。

2.系統之管理權限密碼設定：

(1)密碼以12碼以上組成，需包含英文大、小寫、數字、特殊符號以上4種字元之其中3種。

(2)帳號密碼不可相同。

(3)不可使用鍵盤順序鍵。

(4)不可使用身分證字號。

3.系統之非管理權限密碼設定：

(1)密碼以8碼以上組成，需包含英文大、小寫、數字、特殊符號以上4種字元之其中3種。

(2)帳號密碼不可相同。

(3)不可使用鍵盤順序鍵。

4.系統所在場域及廠商人員使用電腦之密碼設定：

(1)符合政府組態基準(GCB)之帳號密碼原則。

(2)密碼以8碼以上組成，需包含英文大、小寫、數字、特殊符號以上4種字元之其中3種。

(3)密碼最長使用期限為90天。

(4)修改密碼不得與前3次密碼相同。

(5)密碼最短使用期限為1天。

(6)帳號 3 次嘗試登入失敗鎖定帳號。

(7)帳號鎖定時間至少 15 分鐘。

(8)密碼不得與帳號相同。

(9)密碼不得使用鍵盤連續字元組成。

5.最高權限帳號控制情形：

(1)系統帳號應具惟一識別性與鑑別性，並禁止共用帳號。

(2)人員異動或離職應立即停用或刪除帳號。

6.依國教署提供之弱密碼字典檔，建立弱密碼檢核機制，並禁止所有人員使用弱密碼。

十九、廠商應實施作業系統管理：

(一)廠商不得將國教署提供之 Windows Server 作業系統、Microsoft SQL Server 授權軟體檔案及序號，進行散布、傳輸、公開顯示、啟用、移轉、出售等任何其他用途，亦不得於文心機房以外環境使用；如經查核有違反授權使用之行為，相關民事及刑事責任由廠商負責。

(二)伺服主機應安裝主機型防火牆，阻絕不使用之網路通訊埠，及定期檢視防火牆策略清單是否符合資安要求。

(三)伺服主機應安裝防毒軟體，並即時更新病毒碼及檢查運作是否正常。

(四)伺服主機應即時進行作業系統及相關應用軟體更新及修補，並定期或不定期進行主機弱點掃描。

(五)廠商如因緊急狀況等特殊原因，需遠端維護資通系統，應經國教署同意及授權。遠端存取開放期間以每次至多 7 天為原則，並應建立異常行為管理機制。廠商於結束遠端存取期間後，應確實關閉網路連線，並每次更新遠端存取通道登入密碼。主機、系統遠端維護時，應於加密通道進行及限制來源 IP，並建立監控機制。

(六)系統管理者不在場時，主控台(Console)應置於登出狀態，並設置密碼管理。

(七)伺服主機、資料庫系統、應用系統應定期依人事及業務異動情形進行使用權限之調整。

(八)系統管理者應隨時注意及觀察分析系統之作業容量，以避免容量不足而導致主機當機或資料毀損。

(九)系統管理者應進行系統作業容量之需求預測，以確保足夠之系統處理及儲存容量。

(十)系統管理者應隨時注意及觀察分析系統資源使用狀況，包括處理器、主儲存裝置、檔案儲存、印表機及其他輸出設備及通信系統之使用狀況。

(十一)系統管理者應隨時注意相關設備之使用趨勢，尤應注意系統於業務

處理及資訊管理上之應用情形。

(十二)系統管理者應隨時掌握與利用電腦及網路系統容量使用狀況之資訊，分析及找出可能危及系統安全之瓶頸，預作補救措施之規劃。

(十三)系統管理者應準備適當及足夠之備援設施，定期執行必要之資料與軟體備份及備援作業，以於災害發生或儲存媒體失效時，得迅速回復正常作業。

(十四)系統資料備份及備援作業，應符合國教署業務持續運作、系統或服務相關 RTO、RPO 及 MTPD 之需求。

(十五)電腦作業人員應忠實記錄系統啟動及結束作業時間、系統錯誤及更正作業等事項，並依實際需求保留所有紀錄檔。

(十六)電腦作業人員之系統作業紀錄，應定期交由客觀之第三者查驗並律訂保留期限，以確認其是否符合廠商規定之作業程序。

二十、廠商應實施資料管理：

(一)系統流程、作業流程、資料結構及授權程序等系統文件，廠商應予適當保護，以防止不當利用。

(二)廠商應保護重要之資料檔案，以防止遺失、毀壞、被偽造或竄改。重要之資料檔案應依相關規定，以安全之方式保存。

(三)儲存機密性及敏感性資料之電腦媒體，當不再繼續使用時，廠商應以安全之方式處理(如以用重物敲碎搗毀或以碎紙機處理，或將資料從媒體中完全清除)。

(四)廠商蒐集、處理及利用個人資料，應符合個人資料保護法規範，並應明確區分廠商人員及系統瀏覽個資之權限。

(五)廠商人員違反個人資料保護法及其他相關規定時，應負擔相關損害賠償責任，並應通知學校違法之事實及補救措施。

(六)廠商應指定專人辦理個人資料安全維護事項，且該人員應具有管理及維護個人資料檔案之能力或相關經驗，並足以擔任本專案個人資料檔案安全維護經常性工作。

二十一、廠商應實施應用系統(網站)管理：

(一)上線前：

1. 應用程式所有輸入及輸出欄位應完成過濾及編碼(encode)排除特殊字元(如’"!$%^&*_|-><;等)或跳脫字元，以避免被進行跨網站(XSS)及注入攻擊(Injection)，對於使用者輸入欄位資料，採用正規表示式(Regular Expression)進行檢查，僅允許輸入特定白名單內容，檢查其邏輯規則是否合法，並應於伺服器端進行檢查。
2. 應用系統應就涉及機敏資料部分建立稽核日誌，並確保資通系統有稽核特定事件(至少包括更改密碼、登入成功及失敗、資通系統存取成功

及失敗)之功能，採用單一日誌記錄機制，確保輸出格式之一致性，且僅限特定授權之使用者能存取稽核日誌。

3. 應用系統具備直接蒐集個人資料之功能時，應依個人資料保護法之規定，於蒐集前設計應告知事項之頁面，明確告知當事人應告知之事項。
4. 應用系統具備上傳計畫或成果報告等含個人資料檔案之功能時，應於蒐集前明確告知當事人。
5. 移除任何測試性服務、資料、功能、模組、埠口、帳號等影響正式上線安全性之項目，並關閉有關作業系統、應用程式、開發套件及軟硬體版本資訊等相關錯誤訊息頁面，並確保已更新至最新版本。

(二)上線後：

1. 相關個人資料及機敏性資料提供填報或資料傳輸應採用加密機制(如SSH、TLS、SFTP 等)。其因維護不當造成資料外洩者，應負相關法律責任。
2. 涉及個人資料及機敏性資料，於系統儲存時應加密。
3. 應用系統伺服器上之應用程式不得賦予資料庫及作業系統最高權限帳號，應給予最小使用權限，以免惡意人員透過資料庫管理系統破壞內部資訊作業。

二十二、廠商若執行系統修正時執行測試作業不得使用真實個人資料或正式營運之資料；經確認功能正常無誤後，得以更新至正式營運系統。

二十三、廠商執行資通安全及個人資料保護規範之相關資料、紀錄、佐證文件及統計數據，國教署得提供學校作為履約管理、統計廠商服務績效或判定違約之參考。

二十四、學校與廠商就本規範之問題及疑義，由國教署依公平、合理原則統一解釋之。