一貫道崇德學院資訊安全管理辦法

中華民國106年2月24日行政會議通過

**壹、目的**

第一條   一貫道崇德學院（以下簡稱本校）為強化資訊安全管理，督促改善資訊安全防護，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，特訂定「一貫道崇德學院資訊安全管理辦法」（以下簡稱本辦法）。

**貳、適用範圍**

第二條   本校各項資訊資產使用者，含全校教職員生、合約廠商駐校人員及其它經授權使用之人員。

**參、組織與權責**

第三條   為強化本校資訊安全，健全資訊安全管理制度，特設立「一貫道崇德學院資訊安全委員會」(以下簡稱本委員會)，以推動本校資訊 安全管理業務之運作。

第四條   本委員會之成員為校長、教務長、學務長、總務長、圖資館館長為當然委員。本委員會委員為無給職，任期為二學年，連聘得連任。

第五條   本校資訊安全長由校長擔任，兼任本委員會召集人，圖資館館長為執行秘書，行政及技術相關事宜由資訊中心負責。本委員會視需要得聘請校內外具資訊安全專長人員為顧問。

第六條   本委員會權責如下:

一、訂定本校資訊安全政策及資訊安全管控機制。

二、督導資訊安全政策之實施。

三、資訊安全事件通報、緊急應變及危機處理。

四、規劃並督導資訊安全教育訓練、資訊安全演練及資訊安全稽核。

五、協助推動本校資訊安全管理系統之認證。

第七條   本委員會每年開會一次為原則，得視業務需要召開臨時會議。會議須有應出席委員半數(含)以上出席始得開會，並得邀請相關人員列席。

**肆、電腦系統安全防護**

第八條   所有電腦帳號須設定密碼，guest等公用帳號須停用，使用者須善盡帳號密碼保管之責。密碼至少每六個月更換一次，長度須為八位數（含）以上，且夾雜英數字或特殊符號。

第九條   各類作業系統若有螢幕保護功能，必須啟用。啟動螢幕保護時間設定應小於十分鐘，且須設定繼續後以密碼保護功能。

第十條   各類作業系統及應用軟體須開啟自動更新功能或留意其更新資訊，隨時確保軟體的漏洞為已修補狀態。電腦因故重灌後，應立即重新完成所有之漏洞修補作業。

第十一條 所有電腦必須安裝防毒軟體，不可任意關閉或移除，且防毒軟體病毒碼須定期更新。

第十二條 當電腦中毒，病毒無法移除、隔離或作業不正常時，為避免產生大規模電腦病毒感染及擴散情形，應將電腦關機、拔除網路連線，儘速通報資訊中心。

第十三條 來路不明的軟體或檔案常為散播病毒的來源，為確保電腦使用安全，不得安裝使用。

第十四條 電腦系統若具備防火牆功能，必須開啟，以提升電腦防護能力。

第十五條 各單位架設伺服器依照本校「校園伺服器管理辦法」，須有專人負責維護並進行相關資訊安全作業。

第十六條 各單位伺服器每年須執行一次弱點掃描程序，並即時修補缺失，資訊中心將不定期進行檢測。

第十七條 對於用戶端之連線，伺服器端必須設定閒置逾時期限，當閒置逾時發生時須自動切斷其連線。

第十八條 禁止與他人共用電腦系統帳號。

第十九條 採取權限區隔，非專責處理特定個人資料者，不得具有存取或查閱個人資料之權限。

第二十條 禁止人員使用即時通訊軟體傳輸個人資料檔案。

第二十一條 禁止人員使用校外網頁式電子郵件傳輸個人資料檔案。

第二十二條 禁止人員使用點對點（P2P）軟體及即時通訊軟體等相關工具下載或提供分享檔案。

第二十三條 禁止人員在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之個人資料。

**伍、存取控管**

第二十四條 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。

第二十五條 機密性或敏感性之資料及文件，欲利用電子郵件傳送時，須以適當的加密或電子簽章等安全技術處理。

第二十六條 電腦內的資料若須開啟網路分享，務必設定密碼及可存取之帳號，嚴禁未設權限控管開放電腦資料供人任意存取之行為，以防電腦病毒侵害及機密、敏感資料洩露或損毀，且重要資料務必定期備份。

第二十七條 各單位離職人員須立即取消使用單位內各項資源之所有權限，並列入人員離職之必要手續。

第二十八條 各單位主機須限制外部人員以管理者權限帳號登入使用，如有設備保管人以外人士使用或維護設備的須求時，須經主管同意後由系統管理人員陪同下進行。

第二十九條 應指定專人負責管理儲存個人資料檔案之資訊設備與其他相關設施，並檢視、處理其錯誤或異常事件等訊息。

第三十條   儲存個人資料之資訊設備應置放於實體安全區域（如：門禁控管之辦公區域、機房），避免有心人士或非授權人員存取。

第三十一條 儲存個人資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，應指定專人管理，並置於實體保護之環境（如：上鎖之防潮箱、書櫃），必要時應建立備援機制，以防止資料損壞、遺失或遭竊取。相關儲存媒體非經權責單位同意並留存紀錄，不得任意攜出或拷貝複製。

第三十二條 儲存個人資料檔案之電腦或相關設備如須報廢或移轉他用時，應確實刪除該設備所儲存之個人資料檔案。

第三十三條 對重要資訊服務之日誌與紀錄等加以適度存檔，以便日後查核使用。

**陸、可攜式儲存媒體**

第三十四條 使用可攜式設備，須先確認電腦已安裝啟用防毒軟體，避免電腦、系統與網路受到病毒威脅。

第三十五條 使用可攜式設備與媒體時，須謹慎防範資訊洩漏或妨害本校利益等情節發生，資料攜入或攜出，使用者單位主管或廠商接洽窗口人員須盡控管之責。

第三十六條 將機密資料存放於可攜式設備與媒體時，須採取適當加密處理或保護措施，避免遺失時洩漏資訊。

**柒、實體與安全環境管理**

第三十七條 外部人員及訪客須遵守各單位辦公區域安全管制相關規定，並於指定環境內執行作業，防止未經授權的存取、干擾及損害。

第三十八條 重要之出入口須有門禁管理機制，內部人員於進出時須隨時注意是否有非經授權人員跟隨進入，保持警覺，留意陌生人士。

第三十九條 辦公環境內須置放適當之消防設備（如：手提式滅火器、煙霧偵測器等），設備存放環境須保持淨空，以確保其可用性，並定期檢測與紀錄。

第四十條   使用影印機、印表機、傳真機或多功能事務機等資料複印設備後，須立即將相關資料取走，並清除可能暫存於該設備之資訊。

第四十一條 敏感文件（內含姓名、身分證、出生年月日、地址等個人資料）須放置於抽屜或儲櫃並上鎖。

第四十二條 下班時，必須實施桌面淨空，重要文件妥善保管，並關閉不須使用之電腦系統暨其週邊設備。

**捌、資安教育訓練與宣導**

第四十三條 本校人員須定期參與資訊中心主辦的資訊安全教育訓練及宣導，建立並加強資訊安全認知，提升資訊安全水準。

**玖、人員管理**

第四十四條 各單位對資訊相關職務及工作，須進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。

第四十五條 各單位對負責重要資訊系統管理、維護、設計及操作之人員，須妥適分工，分散權責，並視須要建立制衡機制，實施人員輪調，建立人力備援制度。

第四十六條 本校各級業務主管人員，須負責督導所屬員工之資訊作業安全，防範不法及不當行為。若有違反，由主管單位送請校方依本校相關法規懲處。

第四十七條 處理個人資料檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重置通行碼外，應視須要更換使用者識別帳號。

第四十八條 處理個人資料檔案之人員，應簽訂保密切結書，並確認於離職時或合約終止時取消或停用其使用者識別帳號，且收繳其通行證及相關證件。

**拾、資安事件通報**

第四十九條 學校內人員若發現有資訊安全可疑事件時，須儘速通報資訊中心。資訊中心做緊急必要之處理後會發出「資訊安全事件處理暨回覆單」給事件發生單位，事件發生單位須填寫後續處置情形，經主管核簽後回覆資訊中心存查。

第五十條   各單位須設資安聯絡人及其職務代理人，負責資安事件之通報及處理等業務，並將名單送資訊中心存查。

**拾壹、系統開發及委外管理**

第五十一條 自行開發或委外處理個人資料檔案之資訊系統，應在系統開發生命週期之初始階段，將個人資料檔案的安全須求納入考量（如：邏輯測試）；系統之維護、更新、上線及版本異動等作業，應予安全管制，避免危害個人資料安全。

第五十二條 維護人員或系統服務廠商避免以遠端登入方式進行牽涉個人資料的資訊系統維護或其他有關之運作；若因業務須要必須使用遠端登入方式進行維護時，應透過加密通道進行（如：HTTPS、SSH等）。

第五十三條 自行開發或委外處理個人資料檔案之資訊系統，應將個人資料（包含測試用個人資料）施予妥善之保護與控管。

第五十四條 個人資料檔案若委外建檔，應於委外合約中載明所處理之個人資料保密義務、資訊安全相關責任及違反之罰則。

第五十五條 透過網路存取之相關系統應於上線前，確認所開發的系統架構是否已排除系統安全弱點之漏洞。

**拾貳、附則**

第五十六條 本辦法經行政會議通過，呈校長核定後公告實施，修訂時亦同。