國立嘉義高級家事職業學校資訊安全管理要點

101.03.05行政會議訂定

壹、資訊安全管理要點訂定

一、依據：行政院核定之「行政院及所屬各機關資訊安全管理要點」。

二、目的：為強化本校資訊安全管理，確保資料、系統、設備及網路安全，特訂定本資訊安全管理要點。

三、實施：本資訊安全管理要點以書面及電子方式公告本校教職員工及學生，並請提供資訊服務之廠商共同遵行。

四、評估：本資訊安全管理要點實施後，需每年評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

貳、資訊安全權責分工

一、本校設置資訊管理人員，由設備組長負責資訊安全管理事項之協調及推動。

二、本校設置資訊技術小組，由資訊專長人員組成，負責辦理資訊安全相關事宜。

三、本校設置資訊小組，由校長、各處室主任、各學科召集人、資訊技術小組成員組成，統籌資訊安全政策、計畫、資源調度等事項之協調研議。

四、資料及資訊系統之安全需求研議、使用管理及保護等事項，由各業務單位負責辦理，必要時由資訊技術小組協助。

五、資訊機密維護及使用管理事項，由資訊技術小組會同各處室主管負責辦理。

參、人員管理及資訊安全教育訓練

一、本校依實際需要，辦理資訊安全教育訓練及宣導，建立員工資訊安全認知，提升學校資訊安全水準。

二、加強資訊安全管理人力之培訓，提升資訊安全管理能力。

三、對於負責重要資訊系統之管理、維護、設計及操作之人員，需妥適分工，分散權責，並視需要建立人力備援制度。

四、各處室主任需負責督導所屬員工之資訊作業安全，防範不法及不當行為。

肆、電腦系統安全管理

一、本校辦理資訊業務委外作業，需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，要求廠商遵守並定期考核。

二、對於系統變更作業，由資訊管理人員建立紀錄，以備查考。

三、依照相關法規或契約規定，合法複製及使用軟體，並建立軟體使用管理制度。

四、本校設置防火牆及防毒軟體，以偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

伍、網路安全管理

一、本校設立防火牆，以控管外界與學校內部網路之資料傳輸與資源存取。

二、利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。

陸、系統存取控制管理

一、本校依資訊安全政策，賦予各級人員必要的系統存取權限。

二、離職及退休人員，立即取消使用機關內各項資訊資源之所有權限，並列入機關人員離職及退休之必要手續。

三、對學校內外擁有系統存取特別權限之人員建立使用人員名冊，加強安全控管。

四、各業務單位對系統服務廠商以遠端登入方式進行系統維修者，需加強安全控管，並建立人員名冊，課其相關安全保密責任。

五、各業務單位之重要資料委外建檔，需與廠商簽訂適當之安全管制合約，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

柒、系統發展及維護安全管理

一、各業務單位自行開發或委外發展系統，需在系統生命週期之初始階段，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作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。

二、各業務單位委託廠商建置及維護重要之軟硬體設施，需由各系統管理人員及本校資訊管理人員監督及陪同下始得為之。

捌、資訊資產安全管理

各業務單位需對使用之資訊資產進立安全管理，發現異常時應迅速通知服務商或本校資訊人員處理。

玖、實體及環境安全管理

一、全校性伺服器主機應置於主機房，並由資訊管理人員管理，管制非相關人員進出。

二、各業務單位之伺服器主機由各單位指派專人管理。

拾、業務永續運作計畫管理

一、為因應各種人為及天然災害造成業務運作受影響，各業務單位需建立緊急應變及回復作業機制，並定期備份重要資料。

二、各處室於發生資訊安全事件時，應立即向權責主管單位或資訊管理人員通報。

拾壹、本要點經行政會議通過，陳 校長核可後實施，修正時亦同。