# 國立臺東大學附屬體育高級中學資訊安全管理要點

100年10月05日校務會議通過

壹、依據

本規範依據行政院88年09月15日台88經字第34735號函訂頒「行政院及所屬各機關資訊安全管理要點」訂定。

貳、實施目的

為強化本校資訊安全管理，建立安全及可信賴之電子化服務，並確保相關資料、系統、設備及網路安全，保障教職員工生權益，特訂定本要點。

參、通則

本規範中所稱各單位，指本校所屬各處、室、中心及圖書館。

肆、電腦系統安全管理

一、辦理資訊業務委外作業，須明定廠商之資訊安全責任及保密規定，並列入契約，要求廠商遵守並由校方作定期考核。

二、各系統伺服器所存放之機房須由電腦中心、網路中心及行政電腦化專人專責管理，嚴禁非相關人員進出，並請總務處協助控管有關鑰匙的使用。

三、建立系統備援設施，當遇到災害或系統當掉時，可迅速回復正常作業。

四、建立電腦病毒防制機制並由管理人員定期檢查更新。對外使用防火牆以隔絕駭客非法入侵。

五、系統發生各種作業錯誤時，應詳細紀錄事件過程，報告管理人員，並採取必要之更正行動。

六、主機系統應做好既有的安全設定並強化辨識登入者身份之能力，以防冒用、偷竊、破壞情事。

七、電腦作業環境如溫度、溼度及電源供應之品質等，應隨時監測，並採取必要的補救措施。

八、電腦設備之設置，應予保護，以防止斷電或其他電力不正常導致的傷害；電源供應依據製造廠商提供的規格設置，安置預備電源，並使用不斷電系統。

九、應謹慎使用電源延長線，以免電力過載導致火災，危害校園安全。

十、學校負責管理人員卸職或離職後，應即更改相關資訊系統識別代碼。

十一、校內電腦之網路IP設定應遵守主管單位之規定，違反規定擅自盜用他人IP者，將鎖定網路卡，禁止上網2星期。

伍、資訊資產安全管理

一、為防突發斷電造成系統毀損或資料流失，主機房須配置不斷電系統以因應斷電時有足夠時間作存檔與正常關機之程序。

二、可重複使用之資料儲存媒體與設備，不再繼續使用時，應將儲存之內容消除。

三、攜離辦公場所的儲存媒體與設備，應建立書面的授權規定，並建立使用紀錄。

四、儲存媒體應依製造廠商提供的保存規格，存放於乾燥恆溫箱等安全的環境。

五、系統文件應鎖在安全的儲櫃或其他安全場所。

六、委外處理的電腦文具、設備、媒體蒐集及委外處理資料，應慎選有足夠安全管理能力及經驗的機構作為委辦對象。

七、不使用來源不明之磁片。

八、不安裝、下載及使用非經許可之軟體程式。

九、電腦設備需裝置防毒軟體，並開啟於即時掃描狀態。對所收電子郵件之附加檔案更須先經過掃描確定安全後始得開啟。

十、遵守智慧財產權相關規定及網路倫理道德的規範。

十一、各單位欲公佈於本校全球資訊網上之電子檔案須實施機密安全等級評估，並經主管核可後始可發布。

陸、其他

一、周邊環境之安全

（一）實體及環境的安全保護，應以事前規劃的各項周邊設施為基礎，並設置必要的安全控管，如：使用身分識別卡之安全門或監視設備。

（二）實體及環境的安全保護原則：

1、明確界定那些週邊設施須列為安全管制的對象。

2、不應對非相關人員提供過多有關管制區內的作業細節。

3、為防止可能的不當行動，未經授權之人員禁止單獨於管制區內作業。

4、資訊管理人員或委外維護服務人員，只有在被要求或是被授權的情形下，才能進入管制區域，需要有人員陪同並監督其活動。

二、人員進出管制

（一）管制區內應有適當的進出管制保護措施，以確保只有被授權人員始得進入，並備置工作日誌，紀錄每次進入人員與工作相關資料等。

（二）進出管制應考量的事項：

1、來訪人員進入管制區應予適當的管制，並記錄進出時間；來訪人員只有在特定的目的或是被授權情形下，才能進入管制區。

2、委外維修的人員應配載學校管制通行身分識別證，並隨時注意其活動地點。

3、學校負責管理人員卸職或離職後，未經允許不可再進入管制機房。

柒、附則

本要點經校務會議通過，陳請校長核定後公告實施，修正時亦同。