耕莘健康管理專科學校資訊安全管理辦法

中華民國 103 年 04 月 27 日行政會議通過

中華民國 107 年 05 月 28 日行政會議通過

第一條　為強化資訊安全管理，建立安全及可信賴之電子化系統，確保資料、系統、設備與網路之安全，特依「行政院及所屬各機關資訊安全管理要點」、「政府機關（構）資通安全責任等級分級作業規定」、「教育部與所屬機關(構)及學校資通安全責任等級分級作業規定」及「教育體系資通安全暨個人資料管理規範」，訂定「耕莘健康管理專科學校資訊安全管理辦法」（以下簡稱本辦法）。

第二條　有關資訊安全管理事務，依下列原則分工：

一、 資訊暨圖書中心負責研擬、建置及評估資訊安全政策、規範及相關實施計畫等事項。

二、 學校各業務單位依據資訊安全政策、規範及相關實施計畫，負責資料之使用管理及維護等事項。

第三條　資訊安全管理原則如下：

一、 各單位對可存取機密性或敏感性資訊或系統之人員，及因工作需要須配賦系統存取特別權限之人員，應簽署保密協議。

二、 負責重要資訊系統之管理、維護及操作之人員，應妥適依權責分工，並建立代理人制度。

三、 業務主管應負責督導所屬之資訊或資料作業安全，防範不法或不當行為。

四、 利用公眾網路或電子郵件等網路工具傳送資訊或進行交易處理，應注意可能發生之風險。

五、 利用網際網路與全球資訊網公布及流通資訊，應注意資料之安全性、機密性及敏感性，未經當事人同意之個人隱私資料及文件，不得上網公布。單位網站存有個人資料及檔案者，應加強安全保護措施，防止個人隱私資料遭違法竊取或不當使用。

六、 離職、留職停薪與休職人員，應依不同業務性質於期限內取消使用校內各項資訊資源之所有權限，並列入人員離職、留職停薪與休職必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

七、 辦理資訊業務委外作業時，應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，並列入契約中。廠商以遠端登入方式進行系統維護者，應加強安全控管。廠商建置及維護重要軟硬體設施時，應在本校相關人員監督及陪同下始得為之。

八、 各單位對於儲存各項機密資料或程式軟體之磁碟及光碟片等媒體，應設專人管理並定期備份，防止資料洩漏或損毀。並依資料之儲存方式不同，避免因環境因素造成對儲存媒體之損害。

九、 對於電腦設備之裝置地點，應考量使用及管理上之安全，並應指定專人負責，非經允許，不得進入及隨意操作設備，並採行必要之事前預防及保護措施，偵測及防制電腦病毒與其他惡意軟體，以確保系統正常運作。

十、　應擬定「資訊安全政策」與「資訊安全暨緊急應變管理規範」，評估資安相關法令與各種資安事件對單位正常業務運作之影響，審查政策的可行性與有效性，並訂定相關緊急應變與回復作業程序及相關人員之權責，定期演練與調整更新計畫，以維業務永續運作。資訊安全政策應參考資安相關法令及施行單位業務上的需求，並經由資訊安全推動小組及行政會議審議通過後，以適當方式向所有員工公布與宣導，在必要時告知相關單位及合作廠商，以利共同遵守。

第四條　若發生資訊安全事件，應立即向資訊組人員通報，以利資訊組採取適當反應措施。若確定為資安事件，發生事件之單位應填寫資安事件通報表至資訊組。

第五條　應成立本校「資訊安全推動小組」，以統籌本校資訊安全政策擬定、推行及稽核、管理事宜。資訊安全推動小組設置要點另訂之。

第六條　本辦法修正應經資訊安全推動小組通過，提請行政會議審議，陳請校長核定後，公布實施，修正時亦同。