# 輔英科技大學資訊安全暨個人資料保護管理要點

104 年 12 月 30 日 104 學年度第 5 次擴大行政會議通過

一、本校為維護整體資訊安全暨個人資料保護(以下簡稱資安暨個資保護)，強化各項資訊資產之安全管理，確保其具機密性、完整性、可用性、鑑別性與不可否認性，以因應業務運作需要，支援教職員工生各應用系統之使用暨妥善保護其相關個人資料，特訂定本要點。

二、本要點及依本要點所訂定之各項附屬規定（以下簡稱資安暨個資保護管理制度)，係參考行政院所屬各機關資訊安全管理要點、教育體系資通安全管理規範、個人資料保護法、著作權法、國家機密保護法等法規及其他相關標準所訂定。

三、本要點名詞定義如下：

（一）資訊安全：指保護資訊資產避免遭受各種不當使用、洩漏、竄改、竊取、破壞等事故威脅，並降低可能影響及危害本校業務運作之損害程度。

（二）資訊資產：指本校所收集、產生、運用之資料與檔案，以及為完成以上工作所需使用之相關設備。

（三）個人資料：自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

（四）個人資料檔案：依系統建立而得以自動化機器或其他非自動化方式檢索、整理之個人資料之集合。

四、本要點適用於本校各項資訊資產及其資訊使用者，資訊使用者應確實遵守，如有違反者，依相關法令辦理。

五、本校為落實資安暨個資保護管理，成立跨單位「資訊安全暨個人資料保護委員會」，負責本校資安暨個資保護之政策、計畫、資源調度等統籌、協調與研議之整體資通安全維護任務，該會並設置資安暨個資保護執行小組及資安暨個資保護稽核小組以統籌各項作業原則及稽核事宜。

六、為保護本校資訊資產安全，各單位應建立資訊資產與個人資料清冊，並加以分類分級，訂定相對應之管制措施。

七、為提高人員對資安暨個資保護之認知，本校應視需要實施資安暨個資保護教育訓練及宣導；為提高委外作業之安全，本校應要求廠商簽署保密協議書，並管理相關委外專案人員及外部人員之各項資訊資產存取權限。

八、為確保電腦機房維運、網路服務使用及資訊資產使用區域之安全，應訂定安全管理規範；為確保主機作業平台及資料庫之安全，使操作程序標準化，應訂定安全技術規範；為確保應用系統開發、測試、上線及維護之安全，應訂定標準管制及驗收程序。

九、為避免資訊資產因未授權之存取而使機密性或敏感性資料遭不當使用，應考量人員職務授予相關權限，必要時得採行加解密及身分鑑別機制，以加強資料之安全，另為避免資訊資產遭受災害而影響業務永續運作，應訂定應變及復原計畫，並定期測試演練。

十、為降低資安暨個資保護事件造成之損害，各單位應建立資通安全通報及處理程序，並加以記錄。

十一、為落實資安暨個資保護管理制度，資安暨個資保護稽核小組應訂定稽核計畫，並定期執行。

十二、為有效管理本校各項資訊資產所面臨之威脅、弱點及其衝擊程度，本校應辦理風險評鑑並實行必要之風險管理。

十三、本要點應定期檢討，以反映最新標準規範、技術及業務現況。各項附屬規定由資安暨個資保護執行小組視需要修訂，若內容涉及跨單位權責變動，應向資訊安全暨個人資料保護委員會提出後辦理之。

十四、違反本要點者，教師應送教師評審委員會、職員工應送職員工評審委員會予以議處；其以資安暨個資保護為由，而消極不執行業務者，亦同。

十五、本要點經行政會議通過，陳校長核定後發布實施；修正時亦同。