致理科技大學應用軟體安全管理辦法

104.09.17　104 學年度第 1 次資訊發展暨安全委員會會議通過

第 1 條 目的

為確保本校應用軟體(網站)、資料庫、程式開發建置之使用安全，避免因人為疏忽、系統漏洞、蓄意破壞等風險，遭致資訊資產不當使用、洩漏、竄改、破壞等情事，而影響應用軟體系統之正常運作，特訂定本辦法。

第 2 條 適用範圍

一、人員：本校教職員工生及委外資訊服務廠商。

二、軟體設備：各網站系統、資料庫、應用軟體、程式開發。

第 3 條 共同規範

一、應用軟體(網站)進行遠端維護時，應於加密管道進行，並管制維護網路 IP 來源。

二、應用軟體(網站)存取時需建立檢核機制，並適當進行安全檢查。

三、應用程式對於所有輸入欄位應進行字元檢查，排除特殊字元，防止資料庫隱碼攻擊。

四、應描述在各文件中所使用的特殊名詞、縮寫符號與簡稱。

五、軟體專案之文件，須記載組織及作業手冊之編號、標題、改訂版、與日期，及其他相關的文件等。

第 4 條 軟體需求規格

軟體開發須交付軟體需求規格文件提供可茲參考依循之軟體需求分析作業程序，以利進行需求訂定作業並提昇分析品質。

第 5 條 軟體設計規格

軟體開發需交付軟體設計規格文件提供可茲參考依循之設計作業程序，以加速進行設計作業並提昇其品質，作為進行軟體設計工作相關人員之參考及執行軟體設計作業之依據，進而提昇設計技術及增進設計成果品質。

第 6 條 軟體程式設計

軟體開發需交付原始程式碼，應敘明該程式之程式碼，程式碼中應使用註解(Comment)說明程式功能，並將程式碼以光碟媒體儲存交付。

第 7 條 軟體維護使用手冊

軟體開發需交付軟體維護使用手冊，應包含項目如下：

一、系統建置目的及預期目標。

二、系統功能摘要。

三、軟硬體環境需求

描述此系統發展環境所需軟硬體需求及該設備之特性、處理速度、記憶體容量、系統軟體使用規則、備份與復原處理、系統安全管理及應注意事項。應包含內容

如下：

（一）硬體需求。

（二）作業系統及軟體需求。

（三）系統軟硬體架構圖。

（四）客戶端所需環境說明。

四、安裝指南需提供系統軟硬體建置應有詳細安裝步驟，詳細說明軟體安裝時之每一步驟、先後順序、以及安裝應注意事項。

五、操作手冊應提供各種使用者查閱本系統之各項功能。

第 8 條 系統上線導入

系統上線導入時須有完整測試及驗收作業，相關規範如下：

一、測試

（一）測試環境與線上環境應予區隔。

（二）完成程式變更設計或開發後，應進行安全測試(如弱點掃描)，並有效保留測試紀錄。

二、上線與驗收

（一）安全測試完成後，須與申請單位確認並進行相關驗收作業。

（二）系統上線後，應視個案特性及需求維護系統分析文件。

（三）系統若委由其他單位開發時，應請開發單位交付系統功能說明文件，由本處程式開發權責單位審閱，並留存備查。

第 9 條 系統組態管理

應建立系統組態管理文件提供負責人員執行組態管理可依循之作業依據，以降低資訊環境變更對於業務造成的影響，確保所有組態項目之間的整體一致性。

第 10 條 本辦法經資訊發展暨安全委員會通過，陳請校長核定後實施，修正時亦同。