國立臺灣大學採購資訊應用系統網站資訊安全管理辦法

105.6.28 本校第 2911 次行政會議修正通過

第一條 總則

一、國立臺灣大學為落實資訊安全管理及個人資料保護，特訂定本辦法。

二、本校之採購單位(以下簡稱甲方)以委外方式辦理資訊應用系統網站採購，承包廠商(以下簡稱乙方)負責應用系統網站開發或維護。甲方應以書面、電子傳輸或其他方式告知本辦法所定義務，並規範其所屬員工及相關人員(包含分包或臨時人員)，依本辦法辦理。

三、甲方資訊應用系統委外開發或維護時，應於事前審慎評估可能之潛在安全風險(如資料或使用者通行碼被破解、系統被破壞或資料損失等風險)，並與乙方簽訂適當之資訊安全協定，課予相關之安全管理責任，並納入契約條款。

四、乙方為甲方開發或維護之資訊應用系統網站其營運涉及個人資料蒐集、處理、利用等事項者，乙方應依個人資料保護法相關法規辦理。

第二條 綜合管理

一、乙方應填寫資訊安全保密合約書。相關人員執行委託業務前，應填寫保密承諾書。保密合約書及相關人員之保密承諾書應簽署一式兩份，由甲方及乙方留存。

二、資安事件發生時，乙方應配合甲方資安事件通報應變流程，協助於時限內完成事件排除。

前項之處理時限，依行政院「國家資通安全通報應變、作業要綱」規定之時限。

三、甲方資訊應用系統網站委外開發時，應通過安全性檢測(如弱點掃描及滲透測試)並持續維護，降低遭受入侵、竄改或刪除之風險。

甲方應將安全性要求，或個人資料蒐集與利用之相關資料(如資料類別、目的及法規依據)納入專案契約。

四、資訊應用系統網站開發，應預作下線或停止服務等退場機制，及保留所有原始契約和原始碼(SOURCE CODE)，並於契約中詳述甲方及乙方個別之權利與義務。

第三條 資訊應用系統網站管理

一、資訊應用系統網站於上線前應完成弱點及漏洞檢測並完成修補，甲方應於合約中明訂相關執行事宜，以利乙方執行。

二、資訊應用系統網站資安管理之執行作業，得參考下列規定：

(一)上線前：

1.資訊應用系統網站應進行原始碼檢測，資料庫系統弱點掃描，作業系統更新與弱點掃描及滲透測試，並提供檢測報告詳述修復建議及檢測日期，上線前須完成所有弱點及漏洞修補工作。

2.資訊應用系統網站如有個人資料及機敏性資料需填報或資料上載，須提供加密機制，如 SSH, SSL(Https), SFTP 等。

3.確認資訊應用系統網站之程式碼及資料具備定期備份機制。

(二)上線後：

1.資訊應用系統網站應定期進行相關程式、資料庫系統等軟體弱點掃描，作業系統應定期更新、弱點掃描及滲透測試，並依掃描報告修補弱點及漏洞。資訊應用系統網站如修改程式，應再次進行原始碼檢測，並完成弱點修復才得以更新上線。

2.訊應用系統網站之程式碼及資料應定期備份。

3.如因維護不當造成個人資料及機敏性資料外洩者，依個人資料保護法負法律責任。

第四條 本辦法經本校行政會議通過後，自發布日施行。