委外資訊系統簽約注意事項參考

經 99 年 8 月計網中心資訊安全月會提出，99 學年度第 1 學期第 5 次行政會議報告。有鑑於本校各單位所委外開發之資訊系統，可能因廠商程式撰寫瑕疵或架構考慮不周，可能引發駭客入侵或植入病毒，導致系統出現資訊安全漏洞。計網中心特擬定「委外資訊系統簽約注意事項」，期望本校各單位在進行委外資訊系統簽約或採購時，均能注意並符合資訊安全原則。

以下條款內容分為一般、資安檢測、保固維護及罰則四大項，可於委外資訊系統簽約或採購時，依系統特性及需求參酌加入及修改，其中甲方代表本校（國立臺北科技大學），乙方代表委外廠商，紅色字體可視情況填入日期或數字。

一、一般條款（建議將此項條款內容都加入合約中）

項次	條款內容
（1）	乙方必需落實落實本校資訊帳號管理原則，且必需配合甲方資訊安全管理制度，並遵守甲方之「資訊安全管理系統（ISMS）」等相關資訊安全管理及保密規定，甲方得不定期查核乙方是否確實執行。
（2）	乙方所有參與本案人員均應據實簽署本契約附件「國立臺北科技大學計算機與網路中心保密承諾書」，乙方並應對本案人員保密義務負連帶保證責任，甲方得於契約期間對得標廠商實施之保密作業進行稽核。
（3）	乙方須確實交付測試與驗收報告，應至少包含下列項目： 1. 系統功能需求規格及資安需求文件。 2. 相關系統文件之提供。 3. 智慧財產權之歸屬。 4. 相關保密契約與處罰條款。 5. 系統後續保固責任與方式。
（4）	甲方所提供之一切機密資料、文件，均屬甲方所有之資產。於約定期間內或雙方無法成立合作事宜或技術移轉時，乙方應依甲方要求，立即無條件將其所持有（及員工所持有）之原本交還予甲方或其指定人，其他複製或記錄有該等機密資料之文件、媒體則應予銷毀。

二、資安檢測（包括弱點掃描及滲透測試，檢測項目可依系統實際情形作刪減）

項次	條款內容
（1）	基於資訊安全，本案所有系統及應用軟體於驗收時須檢附資訊安全檢測報告，內容需含弱點掃瞄、滲透測試、系統安全弱點分析、WEB AP 安全弱點分析、網站效能壓力測試、防止 DDOS 等封包攻擊等相關措施報告，並於保固期間內每半年至少提供乙次弱點掃瞄、滲透測試及修補等相關報告。
（2）	乙方檢驗本案系統安全檢測服務工具，至少需包含下列各種「安全弱點掃瞄項目(類別)」之弱點檢測功能： 1. File inclusion 攻擊、Directory traversal 攻擊、Code execution 攻擊、CRLF injection 攻擊與 Input validation 攻擊之網站(Web)弱點偵測。 2. 提供自動檢查資料隱碼弱點攻擊(SQL injection)與跨網站指令碼弱點(Cross site scripting vulnerabilities)功能。 3. 提供 Http 編輯器與監聽器(sniffer)功能。 4. 具有搜尋目錄權限弱點之功能(directories with weak

	permissions)。 5. 可以利用弱點編輯器(Vulnerability editor)檢查或修改參數設定。 6. 支援如 PHP、ASP、ASP.NET、JavaScript 與 CGI 等常見網頁技術。 7. 偵測網站中是否存有搜尋引擎攻擊(Google hacking)弱點功能。 8. 可以自動偵測有錯誤之網頁(error page detection)。
(3)	乙方交付之軟硬體及文件，應先行檢查是否內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)，並於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。

三、保固維護

(委外廠商於保固期間內需配合的資安事宜，條款內容可參酌加入合約書中)

項次	條款內容
(1)	乙方應定期更新伺服器主機系統資訊安全修正程式,並依甲方資訊安全規定每月提供資安報告。
(2)	乙方可採電話、傳真、電子郵件等方式，適時提供資訊安全警訊通報服務，通報內容以中文為主，包括：資訊安全威脅類型、說明、可能造成之影響。 1. 各大原廠發布的最新修正檔。 2. 新發現資訊安全漏洞與補救措施。 3. 資訊安全事故記錄與報導。 4. 漏洞分析、修補建議或對策。
(3)	甲方舉辦災害復原演練時，乙方須配合執行演練計畫。
(4)	如甲方發生資安事故時，乙方須配合甲方辦理災害復原程序。
	如甲方資安事故發生時，甲方除依乙方通報內容之應變措施處置外，得要求乙方派員至甲方協助事故處理,乙方應於接到通知後 0 小時內派員到場協助，乙方不得拒絕。

四、罰則(委外廠商因故產生資安事件的罰則，條款內容可參酌加入合約書中)

項次	條款內容
(1)	乙方辦理本採購案如有洩密、疏失、管理不善等情事,致甲方遭致損失,乙方應負全責並賠償甲方之損失。
(2)	乙方因故意或過失，致機關資訊資產遭不當取得、刪除或變更等情事，按次以契約價款之 00%計算違約金。
(3)	乙方需遵守甲方資安管制措施之相關規定,如有違反一經發現追溯自行為日起按日以契約價款 00‰計罰。
(4)	乙方如引起甲方發生資訊安全事件時應即通報甲方，並按甲方之「業務持續運作管理程序」處理，所造成的損失由乙方賠償，並依本契約書第 00 條第 00 項規定計算違約金。
(5)	本契約有效期間,若甲方遭受外來駭客攻擊入侵事故或政府機關攻防演練被入侵之事故或發生之資安事故已見諸於媒體影響機關名譽,經確定屬實且可歸責乙方者，甲方按次以契約價款之 00%計算違約金。
(6)	若有違反上述規定之情事發生，甲方得隨時以書面終止或解除契約，且乙方應就甲方所受損害負賠償之責，如致他人權利受有損害時，乙方亦應負責。