國立交通大學資通系統資訊安全管理規範

109 年 4 月 15 日資訊技術服務中心訂定

壹、 目的

因應資安法，資訊技術服務中心(以下簡稱資訊中心)特訂定「國立交通大學資通系統資訊安全管理規範」（以下稱本管理規範），以落實本校資安治理政策與提升資通系統開發案的執行績效及品質。

貳、 適用範圍

不論自行開發或委外開發及維護之資通系統，凡使用交通大學之網址(Domain name)、採用交通大學之 IP 以及網站標題包含「國立交通大學」之系統均適用。

參、 規範項目

一、自行開發系統

(一)資通系統上線須填寫「資訊服務申請單」向資訊中心提出申請，並提供系統開發安全之文件與弱點掃描報告，交付資訊中心審查。

1.系統開發安全之文件：視服務性質與用途斟酌內容要求，內容應包含項目舉例，如: 密碼以 hash 儲存、帳號管理措施、資料庫與服務後台存取控制措施、資料庫包含機敏資料用應採用 DMZ 架構、風險準備分析與應變計畫、程式碼安全性評估與系統備份及還原計畫等。

2.弱點掃描檢測應採用具公信力之軟體，如:Nessus、OWASP-ZAP、OpenVAS、Acunetix 等。

(二)資訊中心審查確認無高、中風險者，該資通系統即可上線；若審查不合格，資訊中心將提供弱點驗證結果，通知系統管理單位限期改善。

1. 弱點驗證結果為高風險者，請限期 1 週回覆並改善。
2. 弱點驗證結果為中、低風險者，請限期 2 週回覆並改善。

（三）資通系統服務期間配合事宜與資安事件處置

1. 資通系統上線後，仍須配合資訊中心每年定期抽測，若有資安風險疑慮，且未限期回覆與配合改善者，資訊中心有權要求下架(停止網路服務)或封鎖資通系統使用之 IP。
2. 當資通系統發生個資外洩與涉及毀損校譽之情況，資訊中心將立即要求下架並封鎖。
3. 當資通系統判定發生資安事件(如:服務遭破壞、內容操竄改、被入侵引發其他攻擊行為等情形)，系統管理單位須提出緊急應變處置，並配合資訊中心資安事件處理。資訊中心將會對資通系統進行弱點掃描，提供弱點驗證結果，並要求管理單位修補、改善與確認無中、高風險才得以上線。

二、委外開發系統

承商應確實遵守本校對資訊相關服務之要求及應負的責任，相關內容請參照「委外服務資訊安全責任契約附加條款」(附件一)，如有違反規定情事，須承擔相關法律及責任。

肆、 本管理規範經資訊中心主管業務會議通過後實施，修正時亦同。

附件一、委外服務資訊安全責任契約附加條款

第一條 承商交付國立交通大學(以下稱本校)之網站、資訊服務、系統維護(以下稱資訊相關服務)等，需確實遵守本校及本校主管機關要求之各項資訊安全相關規定，本校於必要時得對承商執行稽核之權利。

第二條 本校對承商資訊安全之要求

（一）承商應於驗收前交付弱點掃描報告與資訊安全開發安全之文件予以審查，且國立交通大學資訊技術服務中心(以下稱資訊中心)將保留「弱點掃描檢測」抽驗之權利，經確認無高、中風險存在作為審查合格之標準。建議承商採用弱點掃描檢測採用具公信力之軟體，如:Nessus, OWASP-ZAP, OpenVAS, Acunetix 等軟體。

(二) 承商應交付相關之文件，包含弱點掃描報告與系統開發安全文件，其中系統開發安全文件，內容應包含資訊安全控管功能，如: 密碼以 hash 儲存、帳號管理、存取控制措施、網頁與資料庫架構分離、風險準備分析與應變計畫、程式碼安全性評估、系統備份及還原計畫等。

(三) 承商交付之軟硬體及數位文件(包含隨身碟、光碟等電子文件)，應負資訊安全之完全責任，承商於交付前應先行檢查是否內藏惡意程式(如病毒、蠕蟲、木馬、間諜軟體等)及隱密通道(covert channel)，若資訊相關服務則需於正式環境上線前清除測試相關資料。

(四) 承商應確實遵守「委外服務資訊安全責任契約附加條款」之要求並限期改善不合規定事項，否則本校將正式通知要求下架或封鎖，相關違規事項與懲處措施依合約處理。

(五) 維護期間承商需配合資訊中心每年定期「弱點掃描檢測」以確保無中、高風險存在。網頁服務須使用安全加密機制並經本校資訊中心測試合格後，始得使用本校相關網域名稱。

(六) 承商交付本校資訊相關服務於保固及服務期間內定期稽核、弱點掃描、滲透測試...等，若有疑義，資訊中心得視需要進行稽核、弱點掃描、滲透測試等資訊安全因應措施，相關費用則由承商全額支付。

(七) 承商若須由外部進行主機維運管理，應依據「通信與作業管理程序書」填寫「資訊服務申請表」，經權責主管評估並核准後得以開放。

（八）契約履約或終止後，承商應刪除或銷毀執行服務所持有本校之相關資料，或依本校之指示返還之，並保留執行紀錄。

（九）承商所提供之資訊相關服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。

（十）承商應留存異常處理紀錄，資訊技術服務中心得視需要查核。

（十一）承商相關系統之開發或負責人員異動，應主動告知本校聯絡窗口，並繳回其所借用之設備、軟體及作業權限。

第三條 承商應負資訊安全責任

（一）承商於接觸或處理資訊相關服務時，承商應簽訂「保密協定」或「保密切結書」，並應負完全保密之責任。

（二）承商應遵守中華民國「個人資料保護法」及本校有相關個人資料保護之規定，保障本校各項資料及個人隱私資料(如姓名、出生年月日、身分證統一編號、特徵、指紋、婚姻、家庭、教育、職業、健康、病歷、財務情形、社會活動、電話、住家住址)之安全性；應修正系統，承商如因其員工執行業務之過失，造成本校損失或傷害，承商需負損害賠償責任(包括委由承商代為管理之網站資料外洩)。

（三）承商所提供之服務，如發生資安事件時，必須立即通報資訊技術服務中心或承辦單位，提出緊急應變處置，並配合後續處理。

（四）承商履行合約應提供其使用之軟體，須為合法軟體，並不得違反智慧財產權之規定，如有違反事情發生，承商須承擔所有法律責任。

（五）承商人員於支援業務時所獲知敏感等級(含)以上資訊，不得對外透露。

（六）承商所交付之標的物如侵害第三人合法權益時，應由承包承商負責處理並承擔一切法律責任。

第四條 其他注意事項

（一）如承商需將服務或產品給其他承商支援時，承商須於合約中註明相關下包承商之間的權責關係(可於契約本文描述或作為契約附件)，用以確保承商之整體服務交付品質，並應要求其下包承商遵守本校「國立交通大學資訊系統開發安全規範」。

（二）承商如需攜帶可攜式電腦或儲存媒體如磁片、光碟、隨身碟、外接式硬碟等進入資訊技術服務中心機房使用，需經陪同之單位承辦人員同意並註記於人員進出機房登記表，人員進出機房登記表應定期由權責主管審閱。