國立陽明交通大學資通系統安全管理規範

110 年 6 月 2 日本校 109 學年度第 5 次行政會議通過
111 年 9 月 14 日本校 111 學年度第 1 次行政會議修正通過
112 年 11 月 29 日本校 112 學年度第 3 次行政會議修正通過
114 年12 月 24 日本校 114 學年度第 4 次行政會議修正通過
115 年 4 月 29 日本校 114 學年度第 7 次行政會議修正通過

一、 國立陽明交通大學（以下簡稱本校）為維護校內資通系統之機密性、完整性及可用性，防止本校資通系統遭惡意入侵，特訂定本校資通系統安全管理規範（以下簡稱本規範）。

二、 各單位自行開發公務資通系統須提供系統開發安全之文件與弱點掃描報告，交付本校資訊技術服務中心（以下簡稱資訊中心）。經確認無高、中風險者始可正式啟用；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。

三、 各單位委外開發資通系統時，應依「資通安全管理法施行細則」第七條第一項第一款 :要求廠商應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。

四、 各單位委外開發資通系統時，應於事前審慎評估可能的潛在安全風險，並與廠商簽訂適當的資訊安全協定，確實遵守本校對資訊相關服務之安全要求及應負的責任，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)。

五、 委外期間應適當控管委外人員之資通系統使用權限；委外結束後，應立即收回該項權限。

六、 各單位應定期盤點自行或委外開發之資通系統，依據資通安全管理法之資通安全責任等級分級辦法的分級原則與防護基準確實落實執行。

七、 各單位管理之重要資通系統，須以防火牆或其他安全設施防護，控管外界與內部網路之資料傳輸及存取，防止被侵入破壞、竄改、刪除及未經授權之存取，並應定期確認防火牆管控政策之適用性。

八、 本管理規範經行政會議通過後實施，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 承商交付國立陽明交通大學(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。

第二條 本校對承商資訊安全之要求

(一) 承商交付本校資通系統應於驗收前提供弱點掃描報告與系統開發安全文件予以審查，且本校資訊技術服務中心(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) 承商交付本校資通訊系統應附資訊安全相關之文件，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。如屬本校核心資通系統，則弱點掃描、滲透測試及源碼檢測等安全性檢測報告，均應於驗收時一併交付，並完成中、高級以上之風險修補。

(三) 承商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)，提出安全性檢測證明，涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。廠商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。

(四) 承商應確實遵守中華民國「資通安全管理法」及本條款之要求，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契約處理。

(五) 保固和維護服務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和維護服務期間，應依資通安全責任等級分級辦法之要求每年執行弱點掃描，並依需求執行滲透測試或源碼檢測等安全性檢測，並完成中、高級以上之風險修補；如屬本校核心資通系統，則上述三項安全性檢測項目均應納入。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，如發現瑕疵，應由承商於機關單位指定之期限內負責免費無條件改正。屆期不為改正者，機關單位得逕為處理，所需費用由承商負擔，或動用保固保證金逕為處理，不足時向廠商追償。如該瑕疵非歸責於承商，其改正所需之費用，由雙方另行議定之。

(七) 承商若需進行資訊系統主機及設備遠端維運管理時，如該資訊系統主機及設備建立於本校資訊技術服務中心資訊機房，應遵循「國立陽明交通大學虛擬遠端應用存取服務管理規範」之要求；非「國立陽明交通大學虛擬遠端應用存取服務管理規範」適用範圍者，請依相關權責單位要求執行遠端維運作業。

(八) 契約履約終止或解約時，承商應刪除或銷毀執行服務所持有本校之相關資料，簽具「個人資料歸還與銷毀切結書」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「保密同意書」或「保密切結書」，校內單位及承商雙方並互負相關之保密義務。

(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；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，如違反資通安全相關法令、知悉機關或廠商發生資安事件時，均必須於 1 小時內通報機關，提出緊急應變處置，並配合機關做後續處理；必要時，得由資通安全管理法主管機關於適當時機公告與事件相關之必要內容及因應措施，並提供相關協助。

(四) 承商所交付之標的物，涉及利用非承商自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明，若侵害第三人合法權益時(如智財權)，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交由其他承商支援時，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「國立陽明交通大學資通系統安全管理規範」。

(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、外接式硬碟等進入本校資訊中心機房使用，須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。