國立宜蘭大學各式採購資通安全附加條款範本

一、資訊安全與個人資料保護要求

（一）廠商應遵守資通安全管理法、個人資料保護法及其相關子法要求及本校相關規定，採取適當之安全維護措施。

（二）廠商承作本案如需複委託，應評估複委託之資安風險並進行適當之監督與管理。複委託前需獲得本校同意，並對複委託廠商蒐集、處理或利用個人資料或檔案之行為負完全責任。

（三）廠商承作本案相關人員應簽署「委外廠商保密切結書」。

（四）廠商承作本案若需蒐集、處理或利用個人資料時應採資料蒐集最小化原則，且不得逾越個人資料使用之特定目的範圍。

（五）廠商承作本案時，若違反資安相關法令、知悉個人資料外洩或資通安全事件時，應立即通知校方及採行相關補救措施，並依據本校「資通安全事件通報及應變管理程序」，協助校方於時限內辦理事件通報、事件應變、後續事件調查、處理及改善作業。

（六）廠商承作本案相關人員如因其執行業務之過失，造成本校損失或傷害，廠商需負損害賠償責任。

（七）廠商所提供之相關服務內容如有變更，需經本校權責主管核可同意後，方能進行變更。

二、資通系統安全要求

（一）本案資通系統經本校依「資通安全責任等級分級辦法」附表九「資通系統防護需求分級原則」規定，完成資通系統分級鑑別屬[□普□中□高]之資通系統，最大可容忍中斷時間為　小時。廠商應依「資通安全責任等級分級辦法」附表十「資通系統防護基準」及「資通系統籌獲各階段資安強化措施」相關規定，配合校方要求採行適當防護措施，以確保資通系統達到應具備之安全水準。

（二）新建置資通系統上線前廠商應進行弱點掃描及交付弱點掃描報告。檢測結果若有中、高風險漏洞，廠商需進行系統修補作業並進行複測，直至無中、高風險漏洞或經校方同意後方可進行上線作業。

（三）資通系統應採傳輸加密機制，如 SSH、SSL(https)、SFTP 等。

（四）資通系統合約期間因弱點掃描發現資訊安全中高風險漏洞之情事，廠商需進行系統修補作業，並維持產品穩定性及安全性。

（五）廠商對於系統帳號應善盡保管之責，系統帳號不得任意交由非作業相關人員使用。

（六）資料之轉移、刪除應取得校方之同意，禁止自行移轉或刪除。

三、資訊安全稽核與結案資料處理方式

（一）本校得定期或不定期派員檢查或稽核廠商。

（二）合約終止或解除時，廠商應將承作本案所保有之個人資料刪除或銷毀，或依校方指示返還，並簽署相關資料銷毀返還紀錄後交校方收執，若無保有個人資料則免。