資訊系統/個人資料委外維護與處理安全作業要求

1 一般要求

1.1 受託者必需配合執行本校資訊安全管理制度，遵守本校「資訊安全管理系統（ISMS）」規範及相關法令法規之要求及落實保密義務，本校得不定期查核是否確實執行。

1.2 受託者應提供負責系統維護、聯絡窗口及電話詢答服務，並解決系統相關事宜，並配合本校相關程序辦理異常排除及通報事宜。

1.3 受託者處理本校報修作業時應留存異常處理紀錄備查。

1.4 受託者之員工因執行業務之過失或違反本校相關安全規定，造成本校損失或傷害，受託者需負損害賠償責任，並依相關法規、法定、合約之規定辦理。

1.5 受託者負責本校之專案計畫主持人或重要成員（如專案經理、專案工程師、專案服務人員等）若需更換，應以書面或電子文件通知本校。

1.6 受託者相關系統之開發、服務、負責人員：

1.6.1 任用：依據受託者之相關規定完成聘用。

1.6.2 派任：針對本校各項專案應派任具備足夠能力之人員執行。

1.6.3 離職：應繳回其所借用之設備、軟體及作業權限，並遵守相關之保密協議。

1.7 受託者於本校執行服務前須接受本校相關安全規定之認知訓練或宣導作業；而受託者應針對執行本校專案之人員提供必要之專業訓練，必要時本校得要求提供相關證明文件。

1.8 受託者處理個人資料應遵守「個人資料保護法」及本校之相關管理政策與規定。

1.9 受託者及其人員，於支援業務時所獲知敏感(包含個人資料)等級以上資訊，不得對外透露，為確保前述事項之落實，將要求廠商及其人員簽署「合約商保密切結書」及「人員保密切結書」。

1.10本校所提供之一切資料、文件，均屬本校所有之資產。於約定期間內或雙方無法成立合作事宜或技術移轉時，受託者應依本校要求，立即無條件將其所持有（及員工所持有）之原本交還予本校或其指定人；其他複製或記錄有該等資料之文件、媒體則應予銷毀，並提供相關證明文件，必要時本校得進行相關之查核作業。

1.11智慧財產權：

1.11.1 受託者履行合約應提供其使用之軟體，且均需為合法軟體，並不得違反智慧財產權之規定，如有違反事情發生，受託者須承擔所有法律責任。

1.11.2 受託者使用之工具軟體及處理作業之執行紀錄，本校有權進行稽

核，廠商不得異議。

1.11.3 受託者所交付之標的物如侵害第三人合法權益時，應由承包廠商負責處理並承擔一切法律責任。

1.12本案之執行應避免採用「危害國家資通安全」之產品；若為維護案，應協助建立相關之安全管控機制，與協助進行系統安全建查，並提供設備、系統更新之規畫方案，提供本校作為後續更新作業之參考。

1.13與本案相關之系統、軟體如發生資安事件，應於知悉後 1 小時內通報本校。本校資通安全事件通報專線為 06-2671214#301；非上班時間請撥打校安中心 06-2903545。

以下要求事項請依據執行項目勾選：

□資訊設備採購/建置/硬體設備維護之作業要求：

1. 受託者依合約執行設備交付作業，並留存處理紀錄，本校得視需要進行查核。
2. 設定作業需由原廠工程師或代理商專業工程人員協助設定。
3. 於設備安裝前，若必要，須完成設備上線安全檢查與緊急復原計畫之擬訂並與建置單位完成確認。
4. 設備安裝若須中斷服務，宜於本校非上班時間執行或由雙方議定時間，並於中斷服務前一周通知管理單位，以利公告中斷服務時間。
5. 受託者可採電話、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。內容可包含：
   - 各大原廠發布的最新修正檔。
   - 新發現資訊安全漏洞與補救措施。
   - 資訊安全事故記錄與報導。
   - 漏洞分析、修補建議或對策。
6. 承前項之要求，若相關之威脅、漏洞對本校資訊系統具有影響，受託者應協助依本校資訊安全相關管理規範，經過確認後進行必要的修補作業。
7. 本校辦理業務營運持續演練時，如有需要受託者須配合執行演練計畫之執行。
8. 如本校發生資安事件或事故時，受託者須協助本校辦理災害復原程序。

□應用軟體/套裝軟體採購之作業要求：

1. 受託者依合約執行設備交付作業，並留存處理紀錄，本校得視需要進行查核。
2. 軟體之安裝、設定作業，若有需要宜由原廠工程師或代理商專業工程人員協助設定。
3. 受託者可採電話、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。內容可包含：
   - 原廠發布的最新修正檔。
   - 與本專案相關之新發現資訊安全漏洞與補救措施。
   - 與本專案相關之資訊安全事故記錄與報導。
   - 與本專案相關之漏洞分析、修補建議或對策。
4. 承前項之要求，若相關之威脅、漏洞對本校資訊系統具有影響，受託者應協助依本校資訊安全相關管理規範，經過確認後進行必要的修補作業。
5. 如本校發生資安事件或事故時，受託者須協助本校辦理災害復原程序。

□應用系統建置之作業要求：

1. 受託者依合約執行系統建置作業，並留存處理紀錄，本校得視需要進行查核。
2. 設定作業需由原廠工程師或代理商專業工程人員協助設定。
3. 於設備安裝前，若必要，須完成設備上線安全檢查與緊急復原計畫之擬訂並與建置單位完成確認。

4. 公開服務之應用系統，於系統上先前須完成弱點掃描、滲透測試，若有弱點、漏洞須完成系統的更新始得上線；或提供該系統之系統安全驗證證明文件。
5. 受託者可採電話、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。內容可包含：
6. 原廠發布的最新修正檔。
7. 與本專案相關之新發現資訊安全漏洞與補救措施。
8. 與本專案相關之資訊安全事故記錄與報導。
9. 與本專案相關之漏洞分析、修補建議或對策。
10. 承前項之要求，若相關之威脅、漏洞對本校資訊系統具有影響，受託者須協助依本校資訊安全相關管理規範，經過確認後進行必要的修補作業。
11. 本校辦理業務營運持續演練時，如有需要受託者須配合執行演練計畫之執行。
12. 如本校發生資安事件或事故時，受託者須協助本校辦理災害復原程序。

□應用系統維護之作業要求：

1. 受託者依合約執行維護作業，並留存處理紀錄，本校得視需要進行查核。
2. 公開服務之應用系統，本校會定期依據資通訊系統等級(依據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)執行弱點掃描、滲透測試，受託者須協助進行系統的弱點、漏洞修補作業，相關執行方式於服務合約中議定。
3. 公開服務之應用系統，於系統維護時若須中斷服務，宜於本校非上班時間執行或由雙方議定時間，並於中斷服務前一周通知管理單位，以利公告中斷服務時間。
4. 受託者可採電話、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。內容可包含：
   - 原廠發布的最新修正檔。
   - 與本專案相關之新發現資訊安全漏洞與補救措施。
   - 與本專案相關之資訊安全事故記錄與報導。
   - 與本專案相關之漏洞分析、修補建議或對策。
5. 承前項之要求，若相關之威脅、漏洞對本校資訊系統具有影響，受託者須助依本校資訊安全相關管理規範，經過確認後進行必要的修補作業。
6. 本校辦理業務營運持續演練時，如有需要受託者須配合執行演練計畫之執行。
7. 如本校發生資安事件或事故時，受託者須協助本校辦理災害復原程序。

□個人資料委外處理之作業(應用系統建置與維護中如含包含教職員生資料亦須勾選此項)

1. 受託者必需配合執行本校個人資料保護管理制度，並遵守本校「個人資料保護管理系統（PIMS）」規範及相關法令法規之要求及落實保密義務，本校得不定期查核是否確實執行。
2. 受託者依合約執行作業，並留存處理紀錄，本校得視需要進行查核。
3. 如本校發生資安事件或事故時導致個資外洩，受託者須協助本校辦理災害復原程序。

4. 如執行之作業包含個人資料處理、利用、揭露等，需遵循以下作業：

- 個人資料處理作業，如需複委託，應取得本校書面同意。複委託方之安全控制措施等同於原簽約之受託者，且原簽約之受託者對分包廠商須負全部之管理監督責任。
- 受託者及其所屬人員處理本校個人資料時，如發生安全事件，應立即通報本校，並依相關法令法規執行緊急應變與事件處理程序，並與本校協調相關之補救措施；衍生之各項費用由受託者負擔。
- 合約中宜載明蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。
- 受託者於完成處理事項後，應將委託處理之個人資料檔案返還本校，及刪除因執行合約而保存、儲存於受託者之本校個人資料檔案。
- 協助完成「委外處理個人資料保護管理制度檢核表」之填寫。