明新學校財團法人明新科技大學資訊委外作業之資訊安全注意事項

一、 權責

本校主辦單位應與供應商簽訂之文件如下：

(一)組織對組織：

保密協議書（各簽署一式兩份，由雙方分別留存）

(二)個人（含業務窗口、技術窗口及專案執行工程師／技師）：

供應商保密切結書（人員異動應即更新，效期三年）

(三)供應商作業涉及資通安全暨個人資料安全維護檢核表

(四)供應商應提供系統維護服務，並設置聯絡窗口及電話支援服務，負責處理系統相關問題;另應配合本校相關程序辦理異常排除及通報作業，必要時應依《MUST-ISMS-B-010 供應商管理程序書》提供駐點服務。

二、 配合項目

依據教育部相關規範與要求，敬請配合下述作業：

(一)定期弱點掃描（須提供掃描報告並進行弱點修補）。

(二)委外開發系統、服務應提供相應的服務安全檢測報告。

(三) 委外開發系統、服務上線前應有主辦單位通過之測試報告並有上線復原計畫。

(四) 供應商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，供應商須承擔所有法律責任。

(五) 本校保有稽查權利，依資訊安全檢查目的為由可實地稽查供應商之開發環境、工具、與開發維護紀錄等或委由第三方稽核單位進行稽核查檢作業。若有不符，可限期要求改善。

(六) 供應商人員異動應即時更新或繳回其所借用之設備、軟體及作業權限。

(七) 供應商應提供與設備主機之架構、操作、管理、維護等相關之操作手冊、文件與技術支援，如必要亦應提供教育訓練課程。

(八) 合約內相關供應商人員應符合資安規範要求提供每年教育訓練證明或佐證資料。

三、 系統開發與維護

(一)供應商應確實控管程式版本。

(二)程式修改與開發需遵守本校「系統開發與維護程序書」之規定，若有例外，須經資訊單位主管人員同意以後，方可實施。

(三) 供應商之人員如因作業需求，需對本校系統進行存取或是遠端連線，應提出相應申請通過後執行。

(四) 供應商人員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。

(五) 供應商維修人員，當進入機房重地並使用可攜式電腦或儲存媒體時，須有本校權責或是授權人員全程陪同。

四、 優先選擇通過 ISO27017 或 ISO27018 等相關雲服務標準驗證之提供者。

五、 委外開發系統或委外服務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與損失賠償。

其內容包含：

(一)因供應商或其員工執行業務之過失。

(二)因委外開發系統或服務因安全漏洞產生資安危害。

(三)其他可歸責供應商之責任。

本注意事項依據本校 ISMS文件《MUST-ISMS-B-010 供應書管理程序書》內容節錄編列。