德明財經科技大學

資訊作業委外安全管理規定

機密等級：一般

文件編號：Takming-ISMS-B-007

版　次：V 2.0

初版日期：107.12.25

修 訂 紀 錄

版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	107.12.25	N/A	執行小組	初版
2.0	114.1.27	N/A	推動小組	修改各委外應注意資通安全事項，並將資訊安全改資通安全

1. 目的

為建立德明財經科技大學(以下簡稱本校)所需之資訊業務，於委外執行前或委外契約履行時，提供訂定委外管理相關資通安全管理制度或條款之依循標準。

2. 適用範圍

本辦法適用於本校資訊軟硬體服務、業務資訊與個人資料蒐集處理利用及專業服務等委外作業均適用之。

3. 名詞定義

無。

4. 權責

4.1. 委外權責業務單位

4.1.1.提供委外作業規格書或徵求建議書說明文件，包含資通安全管理需求。

4.1.2.評估委外廠商之資格。

4.1.3.要求委外廠商簽訂並遵循保密切結書。

4.1.4.監督委外作業契約履行情形及執行績效。

4.1.5.必要時應稽核委外廠商資通安全與其他安全相關控管措施。

4.2. 委外廠商

4.2.1.提供完整的工作說明書或專案管理計畫書。

4.2.2.委外廠商須依合約執行相關工作，並提交工作報告或維護紀錄。

4.2.3.簽訂保密切結書並執行保密作業。

4.2.4.須遵守本校其他相關安全規定並配合本校資通安全或個人資料管理稽核。

5. 要求事項

5.1. 委外安全規劃與採購

5.1.1.本校進行委外規劃時，須遵循本管理規定提出適當之安全需求。但若因成本、時效、委外服務之特性或委外廠商之局限性等相關因素之考量，而致所規範之安全需求或新增之安全需求無法完全適用時，應於建立委外安全需求作業時以簽呈方式，說明不適用之項目，提報權責主管核准。

5.1.2.委外廠商應具備完善之資通安全管理措施或通過第三方資通安全驗證。

5.1.3.採購流程須依據政府機關相關採購規範辦理。徵求建議書說明文件(RFP)應含資通安全與個人資料管理相關需求規定，以符合本校資通安全與個人資料管理作業之要求。

5.1.4.委外廠商簽訂資訊委外作業服務契約或合約時，應明訂委外作業服務需求、服務水準、服務提供方式、品質保證、變更管理、安全保密、稽核作業、智慧財產權與個人資料保護等法規遵循、驗

收程序方法、爭議與違約處理及其他雙方權利義務等主要項目。

5.1.5.為確保安全性與可靠性，應於合約中明訂下列事項：

5.1.5.1.作業時如發生錯誤或資料漏失，經確認屬委外廠商責任者，應由委外廠商負責更正；另損及他人權利義務，委外廠商亦須負責。

5.1.5.2.委外廠商對業務上所接觸之資料，應視同機密文件採必要之保密措施，委外廠商及人員均應依本校規定填具「委外廠商保密切結書」，任何因委外廠商人員洩密所致之賠償及刑事責任，概由委外廠商負責，並列入本校拒絕往來戶。

5.2. 委外廠商作業資通安全要求

5.2.1.委外人員執行業務時，應遵守政府及本校資通安全與個人資料保護相關法令規定，若違反時(如電腦洩密、盜取個人資料...等)，依契約及相關法令辦理。

5.2.2.委外廠商需提供完整之工作說明書或專案管理計畫書，內容包含專案目標、範圍、時程、組織、管理機制、服務水準、變更要求等。

5.2.3.委外廠商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)非經本校同意，不得更換。

5.2.4.重要系統之委外廠商應訂定緊急應變與回復標準程序，以確保本校資訊業務之持續運作。

5.2.5.委外廠商於本校執行業務時，應於本校所指定之作業地點執行。

5.2.6.委外廠商之合作或協力廠商皆應併同遵循法律要求及本校資通安全與個人資料管理規定。

5.2.7.委外廠商須配合本校進行資通安全與個人資料管理稽核。

5.3. 委外服務交付管理

5.3.1.委外人員於本校執行業務時，應由業務負責同仁陪同處理。

5.3.2.委外人員因公務所需存取學校系統，需建置特定帳號，開放所需最小權限，並記錄於「系統授權清單」及「帳號使用登記表」。

5.3.3.委外人員進出本校辦公區域或電腦機房區域，應填寫「電腦機房廠商進出管制登記表」並依據「實體環境安全管理規定」辦理。

5.3.4.委外人員需於辦公區域及電腦機房攜出入資訊設備時，依據「實體環境安全管理規定」辦理，填寫「設備進出登記表」。

5.3.5.委外廠商於外部對本校進行遠端存取維護時，依據「資訊安全存取管理規定」及「網路安全管理規定」辦理。遠端連線管制採「原則禁止，例外允許」方式，委外廠商需自校外進行遠端連線時，應由校方委外承辦人填寫「網路服務連線申請表」提出申請，連線設定須限制 IP 位址並管制連線時間，時間到立即斷線，並須監視連線行為，發現異常立即採取應變措施。

5.3.6.委外專案人員有異動，經本校同意後，需記錄於「系統授權清單」及「帳號使用登記表」。

5.3.7.委外專案執行過程發現專案執行效益不彰、政令變更或是委外廠商無法履行合約等不利專案繼續執行之因素時，如專案需暫停或取消，系統承辦人須以行政程序辦理專案暫停或取消，並以公文會辦相關單位辦理。

5.4. 委外服務變更管理

5.4.1.若第三方服務有變更(包含人員變更或工作內容異動)，須於委外廠商合約中說明雙方責任。

6. 參考文件

6.1. 資訊資產管理規定。

6.2. 實體環境安全管理規定。

6.3. 資訊安全存取管理規定。

6.4. 網路安全管理規定。

6.5. 委外廠商保密切結書。

6.6. 系統授權清單。

6.7. 帳號使用申請表。

6.8. 電腦機房廠商進出管制登記表。

6.9. 設備進出登記表。

6.10. 網路服務連線申請表。