委外管理程序書

Outsource operations management procedure

(Contractor Management Procedures)

機密等級	Level of confidentiality	: 1 一般
文件編號	Document Number	: ISPI-B-011
版　　本	Version	: 1.0
發行日期	Release Date	: 113.06.12

修訂紀錄 Revision History

版本 Version	修訂日期 Revision Date	修訂頁次 Revised Page	修訂者 Redactor	修訂內容摘要 Summary
1.0	113.06.12	初版	曾郁凱	初版

目錄 / MENU

1. 目的

確保亞洲大學資通訊系統、設備及個人資料處理委外作業之安全，並對委託業務推行適當之管理及監督作業，以降低個人資料與資通安全風險。

2. 適用範圍

2-1 亞洲大學**各項委外**之資通訊設備、系統與個人資料處理之作業、流程與活動等相關事宜者，包括：

2-1-1 勞務委外

2-1-1-1 一般勞務。

2-1-1-2 涉及資通訊系統及個人資料處理的勞務，含資料處理及資料銷毀。

2-1-1-3 專業顧問服務

2-1-2 資通訊設備、軟體、硬體採購與維運服務(含資通訊設備設備租賃)

2-1-3 應用系統委外開發

2-1-4 應用系統套裝軟體客制化服務 (含網站架設)

2-1-5 租賃服務 (場地租賃)

3. 角色與權責

3-1 委外權責業務單位、委託者 (採購單位)

3-1-1 提供委外作業規格書或徵求建議書等說明文件，包含資通訊安全與個人資料管理需求。

3-1-2 評估委外廠商之資格。

3-1-3 要求委外廠商簽訂並遵循保密切結書。

3-1-4 監督委外作業合約履行情形及執行績效。

3-1-5 必要時應稽核委外廠商安全控管措施。

3-2 委外廠商、受託者

3-2-1 提供完整的工作說明書或專案管理計畫書。

3-2-2 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。

3-2-3 涉及個資及資通訊安全十，應簽訂保密切結書並執行保密作業。

3-2-4 須遵守本校其他相關安全規定並配合本校資通訊安全或個人資料管理稽核。

3-3 **資安暨個資保護推廣小組**：監督各委託業務權責單位，是否符合合約要求善盡委託監督之責，依本程序書遵循之法規要求，必要時得進行受委託方實地稽查以驗證符合法規及合約要求。

4. 名詞定義

遵循「個人資料保護法」及「資通安全管理法」已定義之相關名詞不再重複列出，其它定義用詞如下：

4-1 **業務流程**：業務識別「資源」、「處理及控制要求」及「目標」，達到所需的目標執行的過程。

4-2 **委託業務**：本程序書所指委託業務包含 2-1 所述業務。

5. 法規遵循

5-1 個人資料保護法

5-2 個人資料保護法施行細則

5-3 資通安全管理法

5-4 資通安全管理發施行細則

5-5 教育體系資通安全暨個人資料管理規範

5-6 高等教育深耕計畫-主冊專章(資安強化)

5-7 臺灣學術網路管理規範

5-8 亞洲大學採購辦法

5-9 亞洲大學校園網路管理辦法

本校委外作業管理，應依循「個人資料保護法施行細則」第 8 條各項，及「資通安全管理法施行細則」第 4 條各項辦理。委外權責業務單位有採購或委外服務需求時，應識別評估與其相關之業務流程符合個人資料安全及資通訊安全相關法規。

6. 作業說明

6-1委外安全規劃與採購

6-1-1 本校進行委外規劃時，須遵循本管理程序提出適當之安全需求。

6-1-2 採購流程須依據政府機關與本校相關採購規範辦理。採購需求文件應含資訊安全與個人資料管理相關需求規定，以符合本校資訊安全與個人資料管理作業之要求。

6-1-3 委外廠商簽訂資訊委外作業服務合約或合約時，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。

6-1-4 為確保安全性與可靠性，應於合約中明訂下列事項：

6-1-4-1 作業時如發生錯誤或資料漏失，經確認屬得標廠商責任者，應由得標廠商負責更正；另損及他人權利義務，得標廠商亦須負責。

6-1-4-2 得標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，得標廠商及人員均應依本校規定填具「保密切結書」，任何因得標廠商人員洩密所致之賠償及刑事責任，概由得標廠商負責。

6-2委外廠商作業之安全要求

6-2-1 委外廠商應提供負責設備、系統、維護等服務之聯絡窗口及電話詢答服務，應負責解決承包項目範圍內各項相關事宜，並配合本校相關程序辦理異常排除及通報，如必要應考慮提供駐點服務。

6-2-2 委外廠商處理各項服務應遵守本程序書章節 5 所列之相關法規、管理政策與規定。

6-2-3 依「個人資料保護法施行細則」第 8 條及「資通安全管理法施行細則」第 4 條辦理，委外廠商應依法接受本校及相關上層指導單位進行個資及資安措施監督查核作業，必要時委託者得進行實地訪查。

6-2-4 委外廠商履行合約，應提供使用合法授權軟體 (如必要，須提供可重複驗證之授權證明)，並不得違反智慧財產權之規定，如有違反事情發生，委外廠商須承擔所有法律責任。

6-2-5 委外廠商使用之工具軟體及處理作業之執行紀錄，依 6-2-3 項辦理，本校有權對其進行稽核。

6-2-6 委外廠商應留存異常處理紀錄，本校得視需要查核。

6-2-7 委外廠商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。

6-2-8 委外廠商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，委外廠商需負損害賠償責任，並依相關法規、法定、合約之規定辦理。

6-2-9 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，不得任意更換。

6-2-10 承辦關鍵服務之系統開發、服務、負責人員：

6-2-10-1 任用：依據委外廠商之相關規定完成聘用。

6-2-10-2 派任：針對本校各項專案應派任具備足夠能力之人員執行。

6-2-10-3 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。

6-2-11 委外廠商於提供本校服務時，應簽署「保密切結書」，並要求所屬與本案有關之人員應遵守相關保密規範，委外廠商負責人或專案負責人應善盡督導之責。 若該次於支援業務時獲知「敏感」等級以上資訊或個人資料時，相關作業人員亦應簽署「保密切結書」。 若符合以下情形之一者，可不另簽署「保密切結書」。

6-2-11-1 若委外廠商及其人員已簽署過「保密切結書」，且本校未更動「保密切結書」，委外維護服務重新簽訂服務合約，得標廠商仍為原委外服務廠商時，委外廠商及其人員得免重新簽署相關文件。

6-2-11-2 勞務、商品、套裝軟體、硬體設備採購服務之委外廠商，如該次服務僅為提供物件交付與基本安裝設定，且未接觸「敏感」等級以上之資料時，亦可不簽屬相關切結文件。

6-2-11-3 若委外服務廠商所提供之服務或處理本校相關資料所執行之業務受其他法令、法規規定約束者(如醫療法、醫事人員法、保險法等)，亦可不簽屬相關切結文件。

6-2-12 委外廠商人員之教育訓練，委外廠商於本校執行服務前須完成本校相關安全規定之認知訓練；而委外廠商應針對提供服務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。

6-2-13 是否允許分包作業 (複委託)；如允許分包，分包機構應至少執行與委託協議同等的安全控制措施。

6-3資訊系統委外服務

6-3-1 委外權責業務單位因業務需求提出資訊委外服務時，應適當評估資訊委外之必要性。

6-3-2 若為主機系統之委外採購，委外權責業務單應對系統需求做適當規劃，以確保足夠的處理效能及儲存容量。

6-4 硬體採購與維護

廠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。

6-5 系統開發及維護

6-5-1 資訊系統若委由外部廠商開發，廠商應提供完整之系統架構說明、系統分析設計、資料庫欄位設計等相關文件，經由本校相關人員確認後方能執行。 應提供文件，應載明於合約中。

6-5-2 委外廠商應確實控管程式與文件版本之一致性。

6-5-3 委外廠商進行系統開發與維護時，不得任意複製或攜出本校限閱等級以上之業務資料。

6-5-4 委外廠商需針對交付之系統，應保證系統內不含後門程式、隱密通道及特洛伊木馬程式。關鍵服務應於合約中載明廠商須提供具公信力之系統、組織或團體所產出之源碼掃描報告。

6-5-5 若系統、軟體由委外廠商開發者，應由委外權責單位測試及驗收上線之程式，確定符合相關需求後，方得依照「系統開發與維護程序書」之程序進行上線。

6-5-6 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。

6-6系統帳號管理

6-6-1 委外系統資料、軟體或作業系統最高權限帳號、資料庫最高權限帳號，除合約已另訂管理措施外，應由本校委外權責業務單位系統管理人員保管，不得直接授與委外廠商使用。

6-6-2 委外廠商之人員如因作業需求，需對本校系統進行存取，應參考「存取控制管理程序書」之相關管理規範，並由委外權責業務單位人員填寫相關表單代為提出申請。

6-6-2-1 申請表中應載明作業需求內容、所需權限、帳號有效時間，經由資訊單位主管人員核准後，由系統管理者依照所需權限及帳號有效時間，建立獨立之帳號供委外廠商人員使用。

6-6-3 委外廠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。

6-6-4 委外廠商人員對於系統之操作，本校各系統管理者應盡監督之責，委外廠商人員不得從事非工作範圍內之操作。各系統管理者並應於委外廠商人員完成工作後檢視系統紀錄。

6-7委外服務內容會涉及個人資料處理時，應於作業執行前進行委外廠商評估作業(可由廠商自評)，並陳權責主管簽核後備查。當學年度已進行評估之廠商，於第二次承接同類型作業，或延續承接相同作業(續約)時，可免評估。

6-8委外廠商處理個人資料時，其合約內容宜包含以下項目：

6-8-1 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。

6-8-2 受委託機關的保密及安全管理責任，及安全事故責任歸屬。

6-8-3 委託機構得對其作業流程及安全控制措施進行稽核。

6-8-4 是否被允許分包個人資料處理作業 (複委託)；如允許分包，分包機構應至少執行與委託協議同等的安全控制措施。

6-8-5　受託機構或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機構通知之事項及採行之補救措施。

6-8-6　委託機構如對受託者有保留指示者，其保留指示之事項。

6-8-7　委託關係終止或解除時，個人資料載體之返還，及受委託機構履行委託合約以儲存方式而持有之個人資料之刪除。

6-8-8　其他我國個人資料保護法律要求的要項。

6-9 緊急應變計畫

6-9-1 委託業務若涉及本校核心業務時，應要求委外廠商配合定期進行業務永續計畫，針對委託標的建立緊急應變計畫，並定期進行測試演練，委外廠商應協助演練計畫執行與修正；若該委外案件屬於整體委外者，委外廠商應兩年辦理一次演練。

6-9-2 備援需求：依據不同資訊資產價值及可用性等級，考量其備援需求，必要時，得建立異地備援機制。

6-10 可攜式電腦及儲存媒體管理

6-10-1 進出本校機房安全區域，應由安全區域管理人員陪同或監督，攜入之設備應註記於「人員進出機房登記表」。

6-10-2 本校機房安全區域，禁止使用自行攜帶之可寫入儲存媒體 (如、記憶卡、隨身碟、外接式硬碟)，委外廠商可借用入本校機房安全區域準備之可寫入儲存媒體，用畢會以格式化清除資料，借用及資料刪除確認應進行記錄。

6-11 例外作業

委託業務權責單位應遵循本程序書之規範，提出適當安全需求項目。但若因成本、時效、委外服務之特性、委外廠商之局限性等相關因素之考量，而致本程序書所規範之安全需求無法完全適用時，主辦單位得以簽呈或會議決議方式，提出其他適切之安全需求與規劃，提報權責主管簽核。

6-12 服務變更管理

委外廠商所提供之相關服務內容如有變更，需經由委託業務權責單位承辦人員以簽呈方式通報權責主管，並視需求附上相關風險評鑑之佐證資料，經主辦單位主管核可後，方能進行變更，其服務變更內容如下：

6-12-1 業務流程變更

6-12-2 處理所使用個人資料項目變更

6-12-3 遵循法規修正及變更

6-12-4 系統或網路架構改變

6-12-5 使用新的技術

6-12-6 產品轉換至新版本

6-12-7 新的開發工具及環境

6-12-8 服務設備之搬遷

6-12-9 更換服務提供廠商或服務人員。

6-13　亞洲大學受外部委託之業務、產品與維運標的，應遵循委託者個資與資安要求，擬定相關保護措施，並應配合接受委託者監督及稽核。

7. 個資與資安合約要求

本校委外業務或採購，若涉及個人資料保護或資通安全保護，應進行適法性及安全性評估後，載明於合約或協議中。

7-1 各類別合約應包含要求及範例載於本程序書附錄 A，依案件需求列入維護合約中或為合約附件，依採購類型分類如下：

7-1-1 **委外勞務業務及專業顧問服務。**

7-1-2 **設備、軟體採購或租賃 (不含第三方維運，純軟硬體保固及使用授權)。**

7-1-3 **設備、軟體採購或租賃** (**含委託第三方維運、操作及使用**)。

7-1-4 **維運服務 (維護合約)** 。

7-1-5 **應用系統委外開發服務**。

7-1-6 **應用系統套裝軟體客制化服務**。

7-1-7 **資料委外服務**。

7-2租賃服務

7-2-1 設備、軟體之租賃授權：應同 7-1-3 項，為採購租賃期間使用之設備。

7-2-2 租賃服務(場地租賃) ：如附錄 B。

8. 相關文件

8-1 個人資料保護法

8-2 個人資料保護法施行細則

8-3 資通安全管理法

8-4 資通安全管理發施行細則

8-5 教育體系資通安全暨個人資料管理規範

8-6 高等教育深耕計畫-主冊專章(資安強化)

8-7 臺灣學術網路管理規範

8-8 亞洲大學採購辦法

8-9 亞洲大學校園網路管理辦法

8-10 資安暨個資保護管理政策

8-11 資訊資產管理程序書

8-12 風險評鑑與管理程序書

8-13 系統開發與維護程序書

8-14 存取控制管理程序書

8-15 ISPI-D-013 保密切結書

8-16 ISPI-D-065 委外廠商查核項目表

8-17 ISPI-D-015 人員進出機房登記表

附錄 A 合約個資暨資安要求項目

紅色字部分，採購單位可依「委外廠商查核項目表」進行評核，並請依實際需求修訂合約項目。

甲方：財團法人亞洲大學

乙方：[得標廠商/受委託廠商]

合約名稱：○○○○○○○○○○○○○

合約名稱：○○○○○○○○○○○○○

採購類別：

□本案為「勞務業務」或「專業顧問服務」

□本案為「設備、軟體採購或租賃」，不含維運服務。

□本案屬「設備、軟體採購或租賃(含維運服務)」、「維運服務」、「委外開發系統」、「應用系統套裝軟體客制化服務」、「資料委外服務」其中一項，且涉及甲方網路及資訊安全管理範疇。

個資保護暨資訊安全控制協議：

1　乙方應與甲方共同遵守相關法規、管理政策與規定以履行本合約，詳列如下：

1.1　「個人資料保護法」

1.2　「個人資料保護法施行細則」

1.3　「資通安全管理法」

1.4　「資通安全管理發施行細則」

1.5　「教育體系資通安全暨個人資料管理規範」

1.6　「高等教育深耕計畫-主冊專章(資安強化)」

1.7　「臺灣學術網路管理規範」

1.8　「亞洲大學採購辦法」

1.9　「亞洲大學校園網路管理辦法」

1.10 亞洲大學個資暨資安管理措施「委外管理程序書」

1.11 (其他適用本案之法規，可往前排)

2　乙方應如合約所載明之標的物及要求，於合約期間內提供負責設備、系統、維護等服務之聯絡窗口及電話詢答服務，並解決安全性相關事宜，且應配合甲方相關程序辦理異常排除及通報事宜。(如、系統版本更新、遠端連線管制、網路 IP 管理措施....等)

(合約若包含提供駐點服務，駐點服務人員即可視為該連絡窗口。)

3　合約載明之保固或維運標的，若與業務單位個資或資安保護業務相關時，乙方同意盡相關保密義務，執行業務之人員 (每一人)皆應簽署「保密切結書」，有效期間依適用法規辦理或本合約另定之。

若符合以下情形之一者，可不另簽署「保密切結書」。

(1.　若乙方及其人員已簽署過「保密切結書」，且甲方未更動「保密切結書」內容，委外維護服務重新簽訂服務合約，得標廠商仍為原委外服務廠商時，乙方及其人員得免重新簽署相關文件，既有保密切結書有效期依新合約有效期間延長。

(2.　勞務、商品、套裝軟體、硬體設備採購服務之乙方，如該次服務僅為提供物件交付與基本安裝設定，且未接觸「敏感」等級以上之資料時。

(3.　若委外服務廠商所提供之服務或處理甲方相關資料所執行之業務受其他法令、法規規定約束者(如醫療法、醫事人員法、保險法等)。

4　**甲方之委託業務權責單位**應進行適法性及安全性評估

(合約若須依法進行個資及資安查驗，以甲方「委外廠商查核項目表」評估查核項目為主)

4.1　**委託業務權責單位**已針對本案進行個人資料清查與安全性評估 (請洽貴單位個資窗口)

☐ 本案業務未涉及個人資料項目

(如、純勞務工程與不含維運的「設備、軟體採購或租賃」，建議載明於合約中)

☐ 本案所接觸之個人資料項及適法性如下：

(建議有接觸到就列出在合約中，只要有接觸到可識別人員的資料就要列出。

如、學籍卡務服務：學號、班級、姓名....)

4.2　**委託業務權責單位**已針對本案進行乙方資訊安全管理措施與安全性評估。

(採購的項目需要連接使用校園網路<含校園無線網路>就涉及甲方的資訊安全管理)

☐ 本案業務不需連網，亦無需使用系統或應用程式，未涉及網路資訊安全範疇。

☐ 本案為採購獨立硬體設備或套裝軟體，操作使用及管理人員均為甲方人員。

□ 本案涉及網路及資訊安全範疇，且乙方具備下列資格之一：

(若屬於甲方核心服務，僅接受乙方具有效期內之 ISO 27001 或同等級證書。)

-□ 由驗證機構所發證之資訊安全管理制度有效證書。(如、ISO 27001)

-□ 於政府單位或教育機構，已佈建過相同採購項目，

並可提供已完成具公信力機構廠商之資安風險掃描或驗證報告之附件。

-□ 已完成「委外廠商查核項目表」評估。

(其他應註明事項請列出在合約中)

5 乙方處理業務涉及甲方資通訊系統時，應依循「個人資料保護法施行細則」第 8 條及「資通安全管理法施行細則」第 4 條辦理，進行個資及資通安全管理識別，乙方**應依法接受甲方及相關上層指導單位，進行個資及資安措施監督查核作業**，必要時委託者得進行實地訪查。甲方對乙方的資安與個資要求查核項目，以「委外廠商查核項目表」為主。

6 乙方履行合約，應提供使用合法授權軟體 (如必要，須提供可重複驗證之授權證明)，並不得違反智慧財產權之規定，如有違反事情發生，乙方須承擔所有法律責任。

7 乙方應留存異常處理紀錄，甲方得視需要查核。

8 複委託者，其約定之受託者，亦應具有相同責任要求之合約關係並可驗證。

(如、受託者再委託第三方執行業務時，相關的個資與資安保護責任及權利義務應與受託者相同，並應有合約可驗證。)

(乙方為經銷商時，代理商及原廠，若有直接或間接接觸本案業務，應具相同責任，並有文件或合約證明相對應關係。)

9 經甲方或上層指導單位進行之資通安全監管措施、弱點掃描、web 應用程式弱點掃描、滲透測試及資安健檢等產出之報告、內外部通報之資訊安全事件及嚴重之 CVE 弱點，乙方於合約期限內應協助進行修補或加強管控措施。

10 乙方所交付之標的物如侵害第三人合法權益時，應由乙方負責處理並承擔一切法律責任。

11 乙方之員工因執行業務之過失或違反甲方相關安全規定，造成甲方損失或傷害，乙方需負損害賠償責任，並依相關法規、法定、合約之規定辦理。

12 乙方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）非經甲方同意，不得任意更換。

13 乙方應針對提供服務之人員提供必要之專業訓練，必要時甲方得要求提供相關證明文件。(如、消防、工安、資安、個資...等。)

14 甲方對外部網路有進行遠端連線(SSH 及 RDP)管控，乙方若有遠端維運需求，遠端連線應有適宜管理措施，並應配合甲方之資通安全管理措施申請遠端連線，或於校內在委託者監督下進行維運。

15 執行本案業務不得於校園網路使用疑似危害國家資通安全之設備與系統。甲方依「高等教育深耕計畫-本冊專章(資安強化)」控制項辦理，甲方網路禁用疑似危害國家資通安全產品，乙方應協助業務權責單位識別並更換。若接續之網路來源為自行申辦之 ISP 網路服務則依「亞洲大學採購辦法」辦理。(禁止使用大陸品牌設備，使用甲方校園網路，非經亞洲大學資訊安全暨個人資料保護委員會個案審核同意，執行業務不應使用大陸品牌設備及系統。)

16 於合約外之特殊情況，由委託業務權責單位主管評估個資及資訊安全風險，並取得同意後方得執行。

17 受委託業務相關資料的傳輸應保持機密性與完整性。(如、加密傳輸)

18 委外系統資料、軟體或作業系統最高權限帳號、資料庫最高權限帳號，除合約已另訂管理措施外，應由甲方委外權責業務單位系統管理人員保管，特殊情況下未經授權不得授與乙方使用。(如、系統為廠商專屬系統，且因保密及維運所需無法交付最高權限帳號時，應載明於合約中)

19 乙方之人員如因作業需求，需對系統進行存取，業務權責單位負責人員應進行記錄與管理。

20 執行業務所需之帳號或權限，應於業務截止時停用或刪除，並留存紀錄。

21 乙方所提供之相關服務內容如有變更，需經由委託業務權責單位承辦人員以簽呈方式通報權責主管，並視需求附上相關風險評鑑之佐證資料，經主辦單位主管核可後，方能進行變更，其服務變更內容如下：

21.1 業務流程變更

21.2 處理所使用個人資料項目變更

21.3 遵循法規修正及變更

21.4 系統或網路架構改變

21.5 使用新的技術

21.6 產品轉換至新版本

21.7 新的開發工具及環境

21.8 服務設備之搬遷

21.9 更換服務提供廠商或服務人員。

22 維運或保固期終止後維運服務之延續，若因本校相關採購流程原因，致續期合約無法銜接，於續期合約簽訂完成前，仍由原受委託維運廠商協助維運，期間之異常損害得由乙方另行報價執行。

23 本案包含維運服務時，增列下述安全控制事項

23.1 設備或軟體與既有設備或系統做連結時，宜載明維運標的詳細資訊，包含直接或間接處理之個資項目、權限管理、系統軟硬體規格、複數標的間的關係圖、加密措施、網路區隔措施等資安相關維運管理項目。

23.2 乙方應提供與設備或軟體之架構、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。

23.3 乙方應提供予業務權責管理單位人員，對於標的設備或軟體適宜的資通安全保護措施。(如、更新修補服務、加密傳輸服務、權限管理...等)

23.4 本案應包含安裝使用之作業系統其資通安全保護維運管理。若因資訊技術及安全性問題，需進行平台轉移等相關作業，乙方應協助業務權責單位規劃執行。
(本項請依實際情況調整，作業系統若為業務權責單位人員自行管理亦應載明於合約)
(因資訊技術及安全性問題的變更轉移，如 WINDOWS SERVER 2012 EOL 須更新為更新版本時的資料及應用程式轉移，委外廠商應協助規劃升級，所需相關經費及資源，可不包含在本合約範圍內辦理。)

23.5 若涉及甲方之核心業務時，乙方應配合甲方定期進行業務永續運作演練，並針對委外標的建立緊急應變計畫，定期進行測試；若該委外案件屬於整體委外者，應以委外系統及資料兩者中最高資訊資產價值衡量演練週期。

24 本案為「委外開發系統」時，增列下列安全控制事項

24.1 系統若委由乙方開發，乙方應提供完整之系統架構說明、系統分析設計、資料庫欄位設計、安全風險評估等相關文件，經由委託業務權責單位確認後方能執行。

24.2 系統應評估會直接、間接進行蒐集、處理或利用之個人資料項目，並由委託業務權責單位確認後執行，並應協助進行系統所應提供之個人資料保護相關事宜。(如、個資宣告)

24.3 程式修改與開發應落實安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)，系統發展過程的需求、設計、開發、測試、部署維運等每個階段都應該納入必要的安全項目考量。

24.4 乙方應注意版本控制與變更管理，確實控管程式與文件版本之一致性。

24.5 乙方進行系統開發與維護時，不得任意複製或攜出未經同意之業務資料。

24.6 乙方需針對交付之系統，應保證系統內不含後門程式、隱密通道及特洛伊木馬程式。

24.7 若系統、軟體由委外廠商開發者，應由甲方之委託業務權責單位人員測試及驗收上線之程式，確定符合相關需求後，由委託業務權責單位依合約或本校資安要求之程序進行上線作業。

24.8 乙方於功能或系統結案時的各項資料轉移、留存、汰除相關程序與結案後維運規劃，應載明於合約

24.9 乙方於功能或系統結案時，應提供源碼掃描及應用程式弱點掃描報告。

25 本案為「應用系統套裝軟體客制化服務」時，增列下列安全控制事項

25.1 系統若為套裝軟體客制化構建，乙方應提供完整之架構、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。

25.2 客制化功能應評估會直接、間接進行蒐集、處理或利用之個人資料項目，並由甲方之委託業務權責單位確認後執行，並應協助進行系統所應提供之個人資料保護相關事宜。

25.3 乙方應注意版本控制與變更管理，確實控管程式與文件版本之一致性。

25.4 乙方需針對交付之系統，應保證系統內不含後門程式、隱密通道及特洛伊木馬程式，必要時應提供相關稽核證明。

25.5 若系統軟體應由甲方之委託業務權責單位人員測試及驗收上線之程式，確定符合相關需求後，由委託業務權責單位依合約或本校資安要求之程序進行上線結案作業。

25.6 乙方於系統結案時的各項資料轉移、留存、汰除相關程序與結案後維運規劃，應載明

於合約。

25.7 委外廠商於系統結案時，應提供客制化部分安全掃描相關報告。

26 若本案屬資料處理服務時，乙方應依合約進行資料處理服務，合約未指示之資料範圍，應由甲方之委託業務權責單位審核授權。

27 本合約應提供證明文件 (應可重複驗證)，如下列表

□本案為「勞務業務」或「專業顧問服務」
● 若為專業顧問服務，應檢附由驗證機構所發證之有效證書或相關業務導入證明。
□本案為「設備、軟體採購或租賃」，不含維運服務。
● 原廠證明(產地證明) ● 代理經銷證明 ● 經銷出貨證明 ● 如有必要應提供非大陸品牌證明
□本案屬「設備、軟體採購或租賃(含維運服務)」、「維運服務」、「委外開發系統」、「應用系統套裝軟體客制化服務」、「資料委外服務」其中一項，且涉及甲方網路及資訊安全管理範疇。
● 受託者資通安全管理措施證明 (詳 4.2」)，或通過第三方驗證之證明。 ● 受託者資通安全專業人員相關教育訓練證明。 ● 如有必要應提供非大陸品牌證明

立合約書人

甲　　方：**財團法人亞洲大學**
代 表 人：**蔡 進 發**
地　　址：**台中市霧峰區柳豐路 500 號**
電　　話：**04-23323456**
統一編號：**17713214**

乙　　方：○○○○○○○○
負 責 人：○○○○○○○○
地　　址：○○○○○○○○
電　　話：○○○○○○○○
統一編號：○○○○○○○○

中　華　民　國　○　○　○　年　○　○　月　○　○　日

附錄 B 租賃服務(場地租賃) 合約個資暨資安項目

紅色字為說明，請依實際需求修訂合約項目。

甲方：亞洲大學

乙方：[承租方]

合約名稱：〇〇〇〇〇〇〇〇〇〇〇〇〇

1 乙方應與甲方共同遵守相關法規、管理政策與規定以履行本合約，詳列如下：

1.1 「個人資料保護法」

1.2 「個人資料保護法施行細則」

1.3 「資通安全管理法」

1.4 「資通安全管理發施行細則」

1.5 「教育體系資通安全暨個人資料管理規範」

1.6 「高等教育深耕計畫-主冊專章(資安強化)」

1.7 「臺灣學術網路管理規範」

1.8 「亞洲大學採購辦法」

1.9 「亞洲大學校園網路管理辦法」

1.10 本校個資暨資安管理措施「委外管理程序書」

1.11 (其他適用本案之法規，可往前排)

2 乙方若與甲方有其他合作業務事宜，應另行訂定合約。

3 乙方若因承租項目範圍，涉及甲方個人資訊安全保護業務，應與接觸之業務權責單位釐清對應資料項，並載明於合約。

4 乙方若因承租項目範圍，涉及甲方資安保護業務，應配合相關法規使用。
(只要需要連接校園網路就算涉及)

5 乙方因承租項目範圍，與甲方個資或資安保護業務相關時，應擔負保密義務，接觸者應協助簽署「保密切結書」。

6 經甲方或上層指導單位進行之資通安全監管措施、弱點掃描、web 應用程式弱點掃描、滲透測試及資安健檢等產出之報告、內外部通報之資訊安全事件及嚴重之 CVE 弱點，乙方應協

助進行修補或加強管控措施。

7 甲方對外部網路有進行遠端連線(SSH 及 RDP)管控，承租方若有使用校園網路，有遠端維運需求時，除應有之適宜管理措施，並應配合甲方資通安全管理措施申請遠端連線，或於校內進行維運。

8 執行本案業務不得於校園網路使用疑似危害國家資通安全之設備與系統。甲方依「高等教育深耕計畫-本冊專章(資安強化)」控制項辦理，甲方網路禁用疑似危害國家資通安全產品，乙方應協助業務權責單位識別並更換。若接續之網路來源為自行申辦之 ISP 網路服務則依「亞洲大學採購辦法」辦理。(禁止使用大陸品牌設備，使用甲方校園網路，非經亞洲大學資訊安全暨個人資料保護委員會個案審核同意，執行業務不應使用大陸品牌設備及系統。)

立合約書人

甲　　方：**財團法人亞洲大學**
代 表 人：**蔡 進 發**
地　　址：**台中市霧峰區柳豐路 500 號**
電　　話：**04-23323456**
統一編號：**17713214**

乙　　方：○○○○○○○○
負 責 人：○○○○○○○○
地　　址：○○○○○○○○
電　　話：○○○○○○○○
統一編號：○○○○○○○○

中　華　民　國　○　○　○　年　○　○　月　○　○　日