文件編號	NCHU-ISMS-D-078	機密等級	限閱	版次	3.0

國立中興大學**XXXX**建置合約書(範本)

國立中興大學 (以下稱甲方) 委託XXXXXX有限公司 (以下稱乙方) 建置XXXXXX案。雙方議定條款如下:

一、建置標的

國立中興大學XXXXXXXX建置與開發。

(需說明本案是做什麼系統、功能說明或網站架構圖等。)

二、履約期限

乙方應依約定完成本專案各階段工作, 各階段完成期限如次:

(一)開發建置:應於 _ 年 _ 月 _日前完成。

(二)整合測試:應於 _ 年 _ 月 _日前完成。

(三)系統交付:應於 _ 年 _ 月 _日前完成。

三、價款總額

總計新台幣　　元整(含稅)。

四、付款方式

合約簽訂後, 依甲方會計流程兩次支付 (五月、十一月)。(得視情況調整)

五、系統資安防護需求分級界定(若非系統請填:▫無)

建置標的物之系統安全分級:▫普 ▫中 ▫高

建置標的物須符合「資通安全責任等級分級辦法」附表十「資通系統防護基準」對應系統分級之相關要求, 可利用資通系統防護需求分級評估表進行評估(附件一)。

六、交付與驗收

1. 交付標的物須檢附相關文件, 包含但不僅限於a.資訊作業委外安全管理辦法所規定之文件、b.圖片[1]、c.資料庫及主機權限、d.後臺操作手冊、e.教育訓練(得視情況要求)。
2. 依據資安責任等級分級辦法附表十規定, 資通系統需執行「弱點掃描」安全檢測, 乙方須依據資訊作業委外安全管理辦法檢附本校認可之弱點掃描報告, 且該報告不應有中高風險項目。若資安系統分級為高者, 須再檢附原碼檢測與滲透測試報告。
3. 乙方應於約定之期限屆滿前完成本專案, 並將建置標的物及相關文件交由甲方進行驗收; 但經甲方同意或因不可歸責於乙方之事由致本軟體之完成遲延時, 不在此限。
4. 甲方於驗收時若發現乙方交付之標的物不符合甲方要求或含有不符合實用之瑕疵時, 應通知乙方進行修正, 乙方應於接獲甲方通知後____天內將上述瑕疵修正完成, 並將修改完成後之標的物交付 甲方再依前述流程進行測試驗收, 至驗收合格為止。

七、保固與後續維運

1. 須提供原廠軟硬體保固、軟體升級授權及憑證的建立與置換。
   保固期間:___年___月___日~___年___月___日
2. 應就標的物提供顧問服務, 如提供電話、email、專案系統等諮詢管道。
3. 乙方提供 5*8 系統維護服務(每週五天, 每天八小時), 服務時間為星期一至星期五(不含國定假日) 08:30~17:30。
4. 須配合甲方的資安政策, 若弱點掃描出現風險或漏洞, 亦或是發生資安事件或有斷裂鏈結之情形, 應提供作業系統或應用程式相關套件之更新或修補:
   (1) 如遇高風險漏洞, 應於兩個工作日內修補。(得視情況調整)

[1] 含合法拿到授權之同意書或是說明著作權歸屬於學校

(2) 其他等級之漏洞，乙方應提出具體解決方案及預計完成日期，若無法如期完成應於七個工作日前提出後經甲方同意得展延之。(得視情況調整)
(3) 依據資訊作業委外安全管理辦法規定，針對無法修補之內容，乙方需提供具體說明。

5. 乙方建置與保固過程中必需與甲方確認時程與步驟，以免影響系統服務。現有設備如須停機配合，則必須於夜間或假日之非上班時段實施。

八、資通安全責任

1. 系統必須完全符合「資通安全責任等級分級辦法」附表十「資通系統防護基準」相關要求，且乙方應遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守機關資通安全管理及保密相關規定。
2. 乙方應就承作本專案而蒐集、處理、利用之個人資料建構完備之資料控管保護機制，並遵守個人資料保護相關法令規定及資訊保密附加條款。
3. 乙方必須完整符合資通安全管理法施行細則第四條之委外系統所需事項。
4. 乙方必須完全符合本校資訊作業委外安全管理辦法。
5. 廠商提供之作業服務項目，應落實資通安全管理機制及防護措施。含供應軟硬體標的，應檢視並評估相關產品供應程序有無潛在風險，進而採取必要之防護機制，以降低潛在的資安威脅及弱點。
6. 廠商將契約之部分交由其他廠商代為履行時，應與分包廠商書面約定，分包廠商應遵循政府採購法令及本契約關於分包與轉包之內容；並應約定分包廠商應遵循之事項，其至少包括廠商受稽核時，如稽核範圍涉及分包部分，分包廠商就該部分應配合受稽核。
7. 乙方所提供之勞務或服務之原產地不得為大陸地區，及本案涉及資通訊軟體、硬體或服務等相關事務，乙方執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。
8. 乙方受託業務如涉及國家機密者，應接受本校適任性查核，並依國家機密保護法之規定，管制其出境。
9. 乙方相關人員應據實簽署「委外廠商保密同意書」。若本契約所約定之部分服務，乙方將改由其他分包商提供時，乙方應以書面方式或mail告知並獲得甲方同意，後須補上分包商之「委外廠商保密同意書」，並且複委託之廠商亦須具備本專案所託廠商相同的資通安全維護措施，惟乙方對於外包廠商履約之部分，仍應負完全責任。
10. 乙方負責本校合約系統維護作業之人員變動時，應通知本校承辦人員。
11. 長期合約之系統維護人員(非專案合約)應每年參與至少一次資安通識教育訓練，教育時數必須有3小時以上。如不參與本校資安通識教育訓練，　必須提供其他資安教育訓練證明，該訓練須是一年內的證明。
12. 乙方交付之軟硬體及文件，應確保無內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert　channel)，提出安全性檢測證明。涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。乙方於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。
13. 乙方需落實學校資訊帳號管理原則，且必須配合學校之「資訊安全管理系統　ISMS)」制度以及資通安全管理法等最新相關資訊安全管理及保密規定。
14. 學校所提供之一切機敏性資料、文件等均屬本校之資產，約定期間或雙方無法合作、或技術移轉時，乙方應依本校要求，無條件將所持有之原本交還，複製之機敏文件、資料、媒體應予銷毀。乙方所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。
15. 乙方如有遠端連線進入本校系統進行維修之需求，須依照本校資訊作業委外安全管理辦法完成遠端連線申請程序，經甲方同意後方得進行遠端連線。
16. 乙方如欲進入機房進行作業時，需將可攜式設備或媒體放置管制區，由相關人員陪同。因業務需要進入電腦機房作業時，應由機房管理人員陪同進入並於「電腦機房進出管制登記

簿」上登記。委外人員應配帶原公司所製發之員工證或相關證明，並應於指定環境內執行作業。

17. 本校將定期進行資訊安全演練、入侵偵測、弱點掃瞄等資安相關措施，如發現需改善之系統漏洞，乙方應配合改正。
18. 本校認定之資通系統應配合本校指定流程進行業務持續運作演練，確保系統緊急中斷、災害發生時之應對處理，乙方應配合辦理。
19. 乙方提供之服務，如有違反資通安全相關法令或乙方發生資安事件時，均必須於 1 小時內通報機關，提出緊急應變處置，並配合機關做後續處理。
20. 當系統發生重大事故、中斷、錯誤無法運行，或系統無法復原之情境，乙方應協助將備援資料還原至設備並再度啟用系統，令該業務得持續進行。
21. 乙方如違反第八條規定，應適用第十二條之違約責任，並就機關所受損害負賠償之責；如致他人權利受有損害時，乙方亦應負責。
22. 乙方因執行本契約業務致個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。
23. 乙方維修人員不得輸入任何干擾程式或探取、損壞、消除、竊閱、洩漏本校輸入之電腦資料，如有上列情形，應負一切法律上之責任。
24. 乙方進入本校進行作業時其派遣人員如違反相關資安政策，依契約相關罰則進行處置，如情節造成重大資安事件達「資通安全事件通報及應變辦法」等級 3 以上，甲方將立即終止及解除契約，並自負違反法律之責。

九、蒐集生物特徵之要求

1. 本建置案若進行生物特徵蒐集，需遵守下列要求事項：
   (1) 本項所提「生物特徵」指具個人專屬性足以識別個別身分之個人生理特徵資料（如指紋、臉部特徵、虹膜、聲音、掌紋、靜脈等），需遵守「校園使用生物特徵辨識技術個人資料保護指引」之作業要求。
   (2) 蒐集前需進行特定目的及蒐集事項進行法定告知，且經當事人同意後始得蒐集；當事人若拒絕時本系統需提供其它替代方案供當事人使用，宜不得影響當事人之各項權益。
   (3) 系統需提供當事人具隨時取消使用/被蒐集之界面，並於當事人申請停止蒐集或取消使用時提出適當刪除資料之證明。
   (4) 未盡事項，請依「校園使用生物特徵辨識技術個人資料保護指引」辦理。
2. 得標簽約時需檢附上述要求事項之符合證明文件。（可依公司文件或格式提供，請完成合約章之用印）

十、採用雲端服務之要求

1. 本建置案若使用雲端服務時，為降低可能之風險，需遵守下列要求事項：
   (1) 應禁止使用大陸地區(含香港及澳門地區)廠商之雲端服務運算提供者。
   (2) 提供機關雲端服務所使用之資通訊產品(含軟硬體及服務)不得為大陸廠牌，執行委外案之境內團隊成員(含分包廠商)亦不得有陸籍人士參與，就境外雲端服務之執行團隊成員，至少應具備相關國際標準之人員安全管控機制，並通過驗證。另，雲端服務提供者自行設計之白牌設備暫不納入限制。
   本項所指白牌設備仍指因本案特殊需求而由不同**供應商提供的標準化零件組裝而成之產品**。
   (3) 機敏資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。
2. 得標簽約時需檢附上述要求事項之符合證明文件或**切結書**。（可依公司文件或格式提供，請完成合約章之用印）

十一、保密及安全需求

1. 乙方承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約或法令對第三人負有保密義務未標示得對外公開之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，乙方不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至機關或機關所指定處所以外之處所。
2. 乙方知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。乙方須同意本條所定公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之乙方團隊成員，並應要求該等人員簽署與本條款內容相同之保密同意書。
3. 乙方在下述情況下解除其依本條所應負之保密義務：
   (1) 乙方原負保密義務之資訊，由機關提供以前，已為乙方所合法持有或已知且無保密必要者。
   (2) 乙方原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所週知之資訊。
   (3) 乙方原負保密義務之資訊，係乙方自第三人處得知或取得，該第三人就該等資訊並無保密義務。
4. 乙方應保證其派至機關提供勞務之派駐勞工於機關工作期間以及本契約終止後，在未取得機關之書面同意前，不得向任何人、單位或團體透露任何業務上需保密之文件及資料。且乙方須保證所派駐人員於契約終止(或解除)時，應交還機關所屬財產，及在履約期間所持有之需保密之文件及資料。
5. 前款所稱保密之文件及資料，係指：
   (1) 機關在業務上認為不對外公開之一切文件及資料，包括與其業務或研究開發有關之內容。
   (2) 與乙方派至機關提供勞務之派駐勞工的工作有關，其成果尚不足以對外公布之資料、訊息及文件。
   (3) 依法令須保密或受保護之文件及資料，例如個人資料保護法所規定者。
6. 乙方同意其人員、代理人或使用人如有違反本條或其自行簽署之保密同意書者，視同乙方違反本條之保密義務。
7. 其餘涉及資通安全事項，由機關視個案實際需要，依國家資通安全研究院（網址：https://www.nics.nat.gov.tw/）共通規範辦理，例如「政府資訊作業委外資安參考指引」與資通安全有關事項。

十二、仲裁與訴訟

1. 若履約期間內乙方未達合約所定服務與落實資安危害相關處理，除有不可抗力或不可歸責於乙方事由外，依本款約定計算違約金得每次罰1%，可累計。
2. 本合約內容如發生疑慮，應以中華民國法律為準。雙方如有爭訟，同意以甲方所在地之地方法院，為訴訟第一審管轄法院。

十三、合約收執

本合約一式二份，雙方各執一份。

立合約人

甲 方:
負責人:
地 址:
電 話:

乙 方:
負責人:
地 址:
電 話:

中 華 民 國 _____ 年 ____ 月 ____ 日

附件一(不須影印)

安全等級	普	中	高
機密性	未經授權之資訊揭露，在機關營運、資產或信譽等方面，造成可預期之「有限」負面影響，如:一般性資料，資料外洩不致影響機關權益或僅導致機關權益輕微受損。	未經授權的資訊揭露，在機關營運、資產或信譽等方面，造成可預期之「嚴重」負面影響，如:限閱性資料，資料外洩將導致機關權益嚴重受損，像是涉及區域性或地區性個人資料，包含出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情形、社會活動及其他得以直接或接識別個人之資料。	系統運作、資料保護、資訊及資通系統資產使用等若未依循相關法律規範辦理，造成可預期之「非常嚴重」或「災難性」負面影響，如:機密性資料，依「國家機密保護法施行細則」第28條第4款規定，國家機密之保管方式直接儲存於資訊系統者，須將資料以政府權責主管機關認可之加密技術處理，該資訊系統並不得與外界連線。因此，機關若未依循規定儲存資料，將涉及從根本上違反法律之遵循性。又如:醫療機構醫囑暨電子病歷系統，依「醫療機構電子病歷製作及管理辦法」第3條、第4條規定，電子病歷資訊系統之建置、電子病歷之製作及儲存應符合相關規定。因此，機關若未依循相關規定進行系統建置維運及資料儲存，將涉及從根本上違反法律之遵循性。
完整性	未經授權之資訊修改或破壞，在機關營運、資產或信譽等方面，造成可預期之「有限」負面影響，如:資料遭竄改不致影響機關權益或僅導致機關權益輕微受損。	未經授權之資訊修改或破壞，在機關營運、資產或信譽等方面，造成可預期之「嚴重」負面影響，如:資料遭竄改將導致機關權益嚴重受損。	系統運作、資料保護、資訊及資通系統資產使用等若未依循相關法律規範辦理，造成可預期之「非常嚴重」或「災難性」負面影響，如:機密性資料，依「國家機密保護法施行細則」第28條第4款規定，國家機密之保管方式直接儲存於資訊系統者，須將資料以政府權責主管機關認可之加密技術處理，該資訊系統並不得與外界連線。因此，機關若未依循規定儲存資料，將涉及從根本上違反法律之遵循性。又如:醫療機構醫囑暨電子病歷系統，依「醫療機構電子病歷製作及管理辦法」第3條、第4條規定，電子病歷資訊系統之建置、電子病歷之製作及儲存應符合相關規定。因此，機關若未依循相關規定進行系統建置維運及資料儲存，將涉及從根本上違反法律之遵循性。

可用性	資訊、資通系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之「有限」負面影響，如： ▪ 系統容許中斷時間較長(如72小時)。 ▪ 系統故障對社會秩序、民生體系運作不致造成影響或僅有輕微影響。 ▪ 系統故障造成機關業務執行效能輕微降低。	資訊、資通系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之「嚴重」負面影響，如： ▪ 系統容許中斷時間短。 ▪ 系統故障對社會秩序、民生體系運作將造成嚴重影響。 ▪ 系統故障造成機關業務執行效能嚴重降低。	系統運作、資料保護、資訊及資通系統資產使用等若未依循相關法律規範辦理，造成可預期之「非常嚴重」或「災難性」負面影響，如：機密性資料，依「國家機密保護法施行細則」第28條第4款規定，國家機密之保管方式直接儲存於資訊系統者，須將資料以政府權責主管機關認可之加密技術處理，該資訊系統並不得與外界連線。因此，機關若未依循規定儲存資料，將涉及從根本上違反法律之遵循性。又如：醫療機構醫囑暨電子病歷系統，依「醫療機構電子病歷製作及管理辦法」第3條、第4條規定，電子病歷資訊系統之建置、電子病歷之製作及儲存應符合相關規定。因此，機關若未依循相關規定進行系統建置維運及資料儲存，將涉及從根本上違反法律之遵循性。
法律規章遵循性	系統運作、資料保護、資訊及資通系統資產使用等若未依循相關法律規範辦理，造成可預期之「有限」負面影響，如：全球資訊網，必須符合智慧財產權相關法令尊重他人智慧財產，並遵守兒童及少年福利與權益保障法進行資訊內容管理，否則將涉及違反法律之遵循性。	系統運作、資料保護、資訊及資通系統資產使用等若未依循相關法律規範辦理，造成可預期之「嚴重」負面影響，如：政府電子採購網，依「政府採購法」第27條規定，機關辦理公開招標或選擇性招標，應將招標公告或辦理資格審查之公告刊登於政府採購公報或公開於資訊網路。因此，若系統資料遭竄改導致公告資料錯誤，將影響採購作業透明化。	系統運作、資料保護、資訊及資通系統資產使用等若未依循相關法律規範辦理，造成可預期之「非常嚴重」或「災難性」負面影響，如：機密性資料，依「國家機密保護法施行細則」第28條第4款規定，國家機密之保管方式直接儲存於資訊系統者，須將資料以政府權責主管機關認可之加密技術處理，該資訊系統並不得與外界連線。因此，機關若未依循規定儲存資料，將涉及從根本上違反法律之遵循性。又如：醫療機構醫囑暨電子病歷系統，依「醫療機構電子病歷製作及管理辦法」第3條、第4條規定，電子病歷資訊系統之建置、電子病歷之製作及儲存應符合相關規定。因此，機關若未依循相關規定進行系統建置維運及資料儲存，將涉及從根本上違反法律之遵循性。

注：若有任一構面較其他構面為高者，則系統資安防護需求分級應以較高

文件編號	NCHU-ISMS-D-078	機密等級	限閱	版次	3.0

國立中興大學**XXXX**維護合約書(範本)

為確保 XXXXXX系統 的服務品質, 國立中興大學 (以下稱甲方) 委託XXXXXX有限公司(以下稱乙方) 維護該系統軟體的正常運作。
雙方議定條款如下:

一、維護標的
國立中興大學 XXXXXX維護

二、維護期間
民國XXX年XX 月XX日至民國XXX年XX月XX日止

三、維護費用
總計新台幣　　元整(含稅）。

四、付款方式

合約簽訂後, 依甲方會計流程兩次支付 (五月、十一月)。(得視情況調整)

五、維護項目及範圍

1. 維護範圍以本合約維護標的物在甲方正常使用下所致之損壞為限(軟體維護包括軟體正常功能之維持/硬體維護包含硬體正常功能之維持)。
2. 乙方於進行效能調校時及執行各類維護、維修及設定時, 應據實建立相關技術文件供甲方存查。
3. 應就標的物提供顧問服務, 如提供電話、email、專案系統等諮詢管道。
4. 乙方提供 5*8 系統維護服務 (每週五天, 每天八小時), 服務時間為星期一至星期五 (不含國定假日) 08:30~17:30。
5. 標的物運作異常時, 乙方應於接獲甲方書面、電話或電子郵件通知日起 1 工作日內回覆測試或問題排解方案。(得視情況調整)
6. 乙方之修護服務如超出維護範圍時, 由雙方另行議定維修費用。

□應用軟體系統維護如:

1. 系統版本更新。
2. 應用軟體系統瑕疵與錯誤之修正。
3. 因法令或作業方式修改之系統或程式功能之變更。
4. 因作業需要須新增之電腦報表/螢幕查詢功能。
5. 定期檢視系統之運作情形, 維持系統功能不中斷/中斷後之恢復/故障修復。
6. 強化系統功能。
7. 管理系統之執行及定義備份/復原策略。
8. 每年至少二次資料庫備份資料回復驗證。
9. 須配合甲方的資安政策, 若弱點掃描出現風險或漏洞, 應協助修補系統問題。
   (1) 如遇高風險漏洞, 應於兩個工作日內修補。(得視情況調整)
   (2) 其他等級之漏洞, 乙方應提出具體解決方案及預計完成日期, 若無法如期完成應於七個工作日前提出後經甲方同意得展延之。(得視情況調整)
   (3) 依據資訊作業委外安全管理辦法, 針對無法修補之內容, 乙方需提供具體說明。
10. 視需要協助定期更換SSL憑證。

□硬體設備維護如:

1. 乙方應提供必要之檢查、調整或更換零件等預防保養服務, 以維持標的物之正常運作功能。
2. 硬體設備遷移。
3. 乙方同意依本合約約定, 每個月對本合約維護標第物實施丨次定期保養, 保養工作包括清理、調整、檢視和測試等工作、以減少設備故障。(得視情況調整)

4. 雙方同意，維護範圍以本維護標的在甲方正常使用下所致之損害為限，若維護標的之損害係受天災(水災、火災、地震、雷擊等)，人為之故意破壞(如敲打、破、裂、重擊等)，電源失調，人為疏失或未經乙方人員同意，而由非乙方合格人員所為之維護、調整、移動、重新安裝或其他非正常使用所致者，不包括在內。
5. 若乙方為檢修之必要，應於___小時內修復完成，若無法則得暫以功能不低於故障標的物之機器設備提供甲方代用。於此情形，該標的物視為已回復正常運作。

六、資通安全責任

1. 系統必須完全符合「資通安全責任等級分級辦法」附表十「資通系統防護基準」相關要求，且乙方應遵守資通安全管理法、其相關子法及行政院所頒訂之各項資通安全規範及標準，並遵守機關資通安全管理及保密相關規定。
2. 乙方應就承作本專案而蒐集、處理、利用之個人資料建構完備之資料控管保護機制，並遵守個人資料保護相關法令規定及資訊保密附加條款。
3. 乙方必須完整符合資通安全管理法施行細則第四條之委外系統所需事項。
4. 乙方必須完全符合本校資訊作業委外安全管理辦法。
5. 廠商提供之作業服務項目，應落實資通安全管理機制及防護措施。含供應軟硬體標的，應檢視並評估相關產品供應程序有無潛在風險，進而採取必要之防護機制，以降低潛在的資安威脅及弱點。
6. 廠商將契約之部分交由其他廠商代為履行時，應與分包廠商書面約定，分包場商應遵循政府採購法令及本契約關於分包與轉包之內容;並應約定分包廠商應遵循之事項，其至少包括廠商受稽核時，如稽核範圍涉及分包部分，分包廠商就該部分應配合受稽核。
7. 乙方所提供之勞務或服務之原產地不得為大陸地區，及本案涉及資通訊軟體、硬體或服務等相關事務，乙方執行本案之團隊成員不得為陸籍人士，並不得提供及使用大陸廠牌資通訊產品。
8. 乙方受託業務如涉及國家機密者，應接受本校適任性查核，並依國家機密保護法之規定，管制其出境。
9. 乙方相關人員應據實簽署「委外廠商保密同意書」。若本契約所約定之部分服務，乙方將改由其他分包商提供時，乙方應以書面方式或mail告知並獲得甲方同意，後須補上分包商之「委外廠商保密同意書」，並且複委託之廠商亦須具備本專案所託廠商相同的資通安全維護措施，惟乙方對於外包廠商履約之部分，仍應負完全責任。
10. 乙方負責本校合約系統維護作業之人員變動時，應通知本校承辦人員。
11. 長期合約之系統維護人員(非專案合約)應每年參與至少一次資安通識教育訓練，教育時數必須有3小時以上。如不參與本校資安通識教育訓練，必須提供其他資安教育訓練證明，該訓練須是一年內的證明。
12. 乙方維護之軟硬體，應確保無內藏惡意程式(如病毒、蠕蟲、特洛伊木馬、間諜軟體等)及隱密通道(covert channel)。
13. 乙方需落實學校資訊帳號管理原則，且必須配合學校之「資訊安全管理系統 ISMS)」制度以及資通安全管理法等最新相關資訊安全管理及保密規定。
14. 學校所提供之一切機敏性資料、文件等均屬本校之資產，約定期間或雙方無法合作、或技術移轉時，乙方應依本校要求，無條件將所持有之原本交還，複製之機敏文件、資料、媒體應予銷毀。乙方所提供之服務，如為軟體或系統發展，須針對各版本進行版本管理，並依照資安管理相關規範提供權限控管與存取紀錄保存。
15. 乙方如有遠端連線進入本校系統進行維修之需求，須依照本校資訊作業委外安全管理辦法完成遠端連線申請程序，經甲方同意後方得進行遠端連線。
16. 乙方如欲進入機房進行作業時，需將可攜式設備或媒體放置管制區，由相關人員陪同。因業務需要進入電腦機房作業時，應由機房管理人員陪同進入並於「電腦機房進出管制登記簿」上登記。委外人員應配帶原公司所製發之員工證或相關證明，並應於指定環境內執行作

業。

17. 本校將定期進行資訊安全演練、入侵偵測、弱點掃瞄等資安相關措施，如發現需改善之系統漏洞，乙方應配合改正。
18. 本校認定之資通系統應配合本校指定流程進行業務持續運作演練，確保系統緊急中斷、災害發生時之應對處理，乙方應配合辦理。
19. 乙方提供之服務，如有違反資通安全相關法令或乙方發生資安事件時，均必須於 1 小時內通報機關，提出緊急應變處置，並配合機關做後續處理。
20. 當系統發生重大事故、中斷、錯誤無法運行，或系統無法復原之情境，乙方應協助將備援資料還原至設備並再度啟用系統，令該業務得持續進行。
21. 乙方如違反第六條規定，應適用第十條之違約責任，並就機關所受損害負賠償之責;如致他人權利受有損害時，乙方亦應負責。
22. 乙方因執行本契約業務致個人資料遭不法蒐集、處理、利用或其他侵害情事，應負損害賠償責任。
23. 乙方維修人員不得輸入任何干擾程式或探取、損壞、消除、竊閱、洩漏本校輸入之電腦資料，如有上列情形，應負一切法律上之責任。
24. 乙方進入本校進行作業時其派遣人員如違反相關資安政策，依契約相關罰則進行處置，如情節造成重大資安事件達「資通安全事件通報及應變辦法」等級 3 以上，甲方將立即終止及解除契約，並自負違反法律之責。

七、蒐集生物特徵之要求

1. 本建置案若進行生物特徵蒐集，需遵守下列要求事項:
   (1) 本項所提「生物特徵」指具個人專屬性足以識別個別身分之個人生理特徵資料(如指紋、臉部特徵、虹膜、聲音、掌紋、靜脈等)，需遵守「校園使用生物特徵辨識技術個人資料保護指引」之作業要求。
   (2) 蒐集前需進行特定目的及蒐集事項進行法定告知，且經當事人同意後始得蒐集;當事人若拒絕時本系統需提供其它替代方案供當事人使用，宜不得影響當事人之各項權益。
   (3) 系統需提供當事人具隨時取消使用/被蒐集之界面，並於當事人申請停止蒐集或取消使用時提出適當刪除資料之證明。
   (4) 未盡事項，請依「校園使用生物特徵辨識技術個人資料保護指引」辦理。
2. 得標簽約時需檢附上述要求事項之符合證明文件。(可依公司文件或格式提供，請完成合約章之用印)

八、採用雲端服務之要求

1. 本維護標的物若為雲端服務時，為降低可能之風險，需遵守下列要求事項:
   (1) 應禁止使用大陸地區(含香港及澳門地區)廠商之雲端服務運算提供者。
   (2) 提供機關雲端服務所使用之資通訊產品(含軟硬體及服務)不得為大陸廠牌，執行委外案之境內團隊成員(含分包廠商)亦不得有陸籍人士參與，就境外雲端服務之執行團隊成員，至少應具備相關國際標準之人員安全管控機制，並通過驗證。另，雲端服務提供者自行設計之白牌設備暫不納入限制。
   本項所指白牌設備仍指因本案特殊需求而由不同**供應商提供的標準化零件組裝而成之產品**。
   (3) 機敏資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。
2. 得標簽約時需檢附上述要求事項之符合證明文件或**切結書**。(可依公司文件或格式提供，請完成合約章之用印)

九、保密及安全需求

1. 乙方承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切機關未標示得對外公開之公務秘密，以及機關依契約或法令對第三人負有保密義務未標示得對外公開之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於機關指定之處所內使用之。非經機關事前書面同意，乙方不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至機關或機關所指定處所以外之處所。
2. 乙方知悉或取得機關公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。乙方須同意本條所定公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之乙方團隊成員，並應要求該等人員簽署與本條款內容相同之保密同意書。
3. 乙方在下述情況下解除其依本條所應負之保密義務：
   (1) 乙方原負保密義務之資訊，由機關提供以前，已為乙方所合法持有或已知且無保密必要者。
   (2) 乙方原負保密義務之資訊，依法令業已解密、依契約機關業已不負保密責任、或已為公眾所週知之資訊。
   (3) 乙方原負保密義務之資訊，係乙方自第三人處得知或取得，該第三人就該等資訊並無保密義務。
4. 乙方應保證其派至機關提供勞務之派駐勞工於機關工作期間以及本契約終止後，在未取得機關之書面同意前，不得向任何人、單位或團體透露任何業務上需保密之文件及資料。且乙方須保證所派駐人員於契約終止(或解除)時，應交還機關所屬財產，及在履約期間所持有之需保密之文件及資料。
5. 前款所稱保密之文件及資料，係指：
   (1) 機關在業務上認為不對外公開之一切文件及資料，包括與其業務或研究開發有關之內容。
   (2) 與乙方派至機關提供勞務之派駐勞工的工作有關，其成果尚不足以對外公布之資料、訊息及文件。
   (3) 依法令須保密或受保護之文件及資料，例如個人資料保護法所規定者。
6. 乙方同意其人員、代理人或使用人如有違反本條或其自行簽署之保密同意書者，視同乙方違反本條之保密義務。
7. 其餘涉及資通安全事項，由機關視個案實際需要，依國家資通安全研究院（網址：https://www.nics.nat.gov.tw/）共通規範辦理，例如「政府資訊作業委外資安參考指引」與資通安全有關事項。

十、仲裁與訴訟

1. 若履約期間內乙方未達合約所定服務與落實資安危害相關處理，除有不可抗力或不可歸責於乙方事由外，依本款約定計算違約金得每次罰1%，可累計。
2. 本合約內容如發生疑慮，應以中華民國法律為準。雙方如有爭訟，同意以甲方所在地之地方法院，為訴訟第一審管轄法院。

十一、合約收執

本合約一式二份，雙方各執一份。

立合約人

甲 方:
負責人:
地 址:
電 話:

乙 方:
負責人:
地 址:
電 話:

中 華 民 國 _____ 年 ____ 月 ____ 日