國立新營高級工業職業學校

委外管理程序書

機密等級：一般
文件編號：
HYIVS-ISMS-B－010
版　　次：1.0
發行日期：115年9月18日

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	115.09.18		資媒組	初版

委外管理程序書					
文件編號	HYIVS-ISMS-B-010	機密等級	一般	版次	1.0

目錄

1 目的 1

2 適用範圍 1

3 權責 1

4 名詞定義 1

5 作業說明 2

5.1 一般條款 2

5.2 資訊系統委外服務提出 2

5.3 資產辨識與風險評鑑作業 3

5.4 選擇或新增安全需求 3

5.5 硬體採購與維護 3

5.6 系統開發及維護 3

5.7 系統帳號管理 4

5.8 緊急應變計畫 4

5.9 可攜式電腦及儲存媒體管理 4

5.10 例外作業 5

5.11 服務變更管理 5

6 相關文件 5

委外管理程序書					
文件編號	HYIVS-ISMS-B-010	機密等級	一般	版次	1.0

1 目的

本程序書制訂之目的在於確保國立新營高級工業職業學校（以下簡稱「本校」）資訊委外作業之安全。

2 適用範圍

2.1 適用於本校資訊委外作業項目，包括：

2.1.1 主機系統委外採購與維護。

2.1.2 網路相關硬體設備委外採購與維護。

2.1.3 應用系統委外開發及維護。

2.1.4 應用系統套裝軟體客製化及維護。

2.1.5 資料服務委外。

2.1.6 設備租用服務委外。

2.1.7 專業顧問服務委外。

3 權責

3.1 主辦單位：負責依據本程序書之規定，提出適當之安全需求及擬定與廠商服務相關合約內容，並確實在合約中訂定保密條款。

3.2 業務權責單位：

3.2.1 負責審查主辦單位所擬定之合約，確認合約內容無違反本校應遵循之相關規定或傷害本校之權益。

3.2.2 對於服務提供廠商之遴選，應符合主辦單位所提出之安全需求及採購辦法之規範。

4 名詞定義

4.1 隱密通道：由惡意程式所建立，會將系統資訊暴露給未授權使用者之管道。

4.2 特洛伊木馬程式：藉由偽裝成其它種類應用程式來獲取未授權資訊之惡意程式。

5 作業說明

5.1 一般條款

5.1.1 委外廠商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，如必要應提供駐點服務。

5.1.2 委外廠商處理個人資料應遵守「個人資料保護法」及本校之相關規定，並簽訂「委外廠商保密切結書」。

5.1.3 委外廠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，委外廠商須承擔所有法律責任。

5.1.4 委外廠商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。

5.1.5 委外廠商應留存異常處理紀錄，本校得視需要查核。

5.1.6 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。

5.1.7 委外廠商如因其員工執行業務之過失，造成本校損失或傷害，委外廠商需負損害賠償責任。

5.1.8 委外廠商相關系統之開發或負責人員離職時，應繳回其所借用之設備、軟體及作業權限。

5.1.9 委外廠商人員，於支援業務時所獲知敏感等級（含）以上資訊，不得對外透露，為確保前述事項之落實，將要求廠商簽署「委外廠商保密切結書」。

5.2 資訊系統委外服務提出

5.2.1 主辦單位因業務需求提出資訊委外服務，應適當評估資訊委外之必要性。

5.2.2 若為主機系統之委外採購，主辦單位應對系統需求做適當規劃，以確保足夠的電腦處理及儲存容量。

5.3 資產辨識與風險評鑑作業

5.3.1 主辦單位應依據「資訊資產管理程序書」、「風險評鑑與管理程序書」，依照委外標的之資訊資產價值、機密性、完整性及可用性等級，適當評估其可能之威脅及弱點。

5.4 選擇或新增安全需求

5.4.1 主辦單位依據上述風險評鑑結果，進行風險管理作業，選擇適用之安全需求項目，明訂於合約之中。

5.5 硬體採購與維護

5.5.1 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。

5.6 系統開發及維護

5.6.1 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。

5.6.2 委外廠商應確實控管程式與文件版本之一致性。

5.6.3 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（含）以上之業務資料。

5.6.4 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。

5.6.5 若系統、軟體由委外廠商開發者，應由本校人員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。

5.6.6 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。

5.7 系統帳號管理

5.7.1 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，應由本校處理資訊單位人員保管，不得直接授與委外廠商使用。

5.7.2 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，並由本校人員代為填寫「資訊服務申請表」提出申請。

5.7.3 「資訊服務申請表」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，開放必要之帳號供委外廠商人員使用。

5.7.4 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。

5.7.5 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。

5.8 緊急應變計畫

5.8.1 資訊作業委外若涉及本校之關鍵業務時，應要求委外廠商配合本校定期進行業務永續計畫針對委外標的建立緊急應變計畫，並定期進行測試；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。

5.8.2 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。

5.9 可攜式電腦及儲存媒體管理

5.9.1 委外廠商如需攜帶可攜式電腦或儲存媒體如磁片、光碟、隨身碟、外接式硬碟等進入本校機房使用，需經陪同之資訊單位承辦人員同

意，並註記於「人員進出機房登記表」，「人員進出機房登記表」應定期由權責主管審核。

5.9.2 廠商維修人員，當進入機房重地並使用可攜式電腦或儲存媒體時，須有本校人員全程陪同或監控。

5.10 例外作業

資訊委外服務之主辦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，主辦單位得以簽呈方式，提出其他適切之安全需求與規劃，提報權責主管簽核。

5.11 服務變更管理

委外廠商所提供之相關服務內容如有重大變更，需經由業務承辦人員以簽呈方式通報主辦單位主管，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：

5.11.1 系統網路架構改變。

5.11.2 使用新的技術。

5.11.3 產品轉換至新版本。

5.11.4 新的開發工具及環境。

5.11.5 服務設備之搬遷。

5.11.6 更換服務提供廠商或服務人員。

6 相關文件

6.1 個人資料保護法

6.2 資訊安全政策

6.3 資訊資產管理程序書

6.4 風險評鑑與管理程序書

6.5 系統獲取、開發及維護程序書

6.6 存取控制管理程序書

6.7 資訊服務申請表

6.8 委外廠商保密切結書

6.9 人員進出機房登記表