

系統開發與維護					
文件編號	HGSH-ISMS-B-007	機密等級	限閱	版次	1.1

1 目的

為確保國立新竹女子高級中學（以下簡稱本校）資通系統開發、測試與維護作業之安全管理。

2 適用範圍

資通系統之程式開發相關支援活動，如既有線上系統之測試、修改、維護、上線變更、原始碼之管控與儲存等作業。

3 權責

本校相關資通系統開發、維護人員與委外人員遵守相關規定，以確保本校相關軟體與資料等資通資產之安全。

4 名詞定義

無。

5 作業說明

5.1 一般控制措施

5.1.1 當發展新資通系統，或現有系統功能之強化，於系統規劃需求分析階段，即將安全需求要項納入系統功能。

5.1.2 除由系統自動執行之安全控管措施之外，亦可考量由人工執行相關控管措施。

5.1.3 在採購套裝軟體時，視其安全需求，進行分析。除事前經權責單位主管核准外，應避免修改套裝軟體，如需修改應依本程序書之變更作業控制措施加以控管。

5.1.4 系統之安全需求及控制程度，應與資通資產價值相稱，並考量安全措施不足，可能帶來之傷害程度。

5.1.5 資通系統應保護敏感等級（含）以上之資料，防止洩漏或被竄改，必要時應使用資料加密之相關機制保護。

5.1.6 在作業系統上執行應用軟體，應建立控制程序並嚴格執行，為減少可能危害作業系統之風險，應用程式之更新作業應限定只能由授權之管理人員才可執行，且應建立應用程式之更新稽核紀錄。

系統開發與維護					
文件編號	HGSH-ISMS-B-007	機密等級	一般	版次	1.1

5.1.7 真實資料被複製到測試系統時，應依複製作業之性質及內容，在取得授權後始能進行，敏感資料欄位應予模糊化。

5.1.8 系統若需委外建置或維護，請參考資通安全維護計畫壹拾貳、資通系統或服務委外辦理之管理、政府資訊服務採購作業指引、依「資通安全責任等級分級辦法」執行系統防護需求等級之相關防護控制措施（附表九、資通系統防護需求分級原則及附表十、資通系統防護基準），並符合資通安全管理法及子法、個人資料保護法及施行細則等法遵。

5.1.9 系統弱點管理，請參考「通信與作業管理」之相關管理規範。

5.1.10 各單位若有資料需求申請時，申請人視情況應依電子公文程序或填寫「資料需求申請表」經單位主管同意後，呈資通安全執行祕書核決，本校始得提供資料內容。

5.2 軟體控制措施

5.2.1 作業系統變更時，應審查與測試重要營運系統，以確保對組織作業或安全無不利之衝擊。

5.2.2 系統軟體安裝

5.2.2.1 系統軟體應由系統負責人進行安裝，安裝時應視狀況通知相關技術人員支援或通知使用者，以避免資訊服務中斷或影響業務。

5.2.3 系統軟體測試

5.2.3.1 軟體測試由系統負責人辦理，測試時應事先通知協調相關人員支援。

5.2.3.2 系統負責人應通知相關人員及使用者以避免資訊服務中斷或影響業務。

5.2.4 系統軟體更新

系統負責人需定期檢視更新系統安全修補、防毒軟體及防毒碼，以維持系統正常運作。

5.3 開發作業控制措施

5.3.1 提案與回覆

系統開發與維護					
文件編號	HGSH-ISMS-B-007	機密等級	一般	版次	1.1

5.3.1.1 申請單位提出「系統需求申請與回覆單」敘明需求理由。

5.3.1.2 承辦人員於完成與申請單位之訪談與系統分析後，於「系統需求申請與回覆單」中回覆評估結果，包含功能細項、預估人力與時程、建議方案等。

5.3.1.3 經評估系統修改幅度不大，且不涉及系統流程變更者，於「系統需求申請與回覆單」中回覆處理結果並結案。

5.3.2 分析規劃與程式撰寫

5.3.2.1 程式開發者應於程式開發前進行系統分析，系統分析時應將系統安全需求納入考量。如涉及重要資料之傳輸，應使用 SSL 加密金鑰，並依下列規定管理金鑰：

5.3.2.1.1 金鑰應有明確的啟動與止動日期，並於可用期間，保護其不被修改、遺失和破壞。

5.3.2.1.2 金鑰之使用與存取，應限於使用金鑰之系統管理者，不可由其他非系統管理者任意存取。

5.3.2.1.3 對於金鑰之使用、啟動、止動，皆應留存相關之紀錄。

5.3.2.2 輸入應用系統之資料，應檢查主要欄位或資料檔案的內容，以確保資料的有效性及真確性。

5.3.2.3 對高敏感性的輸入資料，必要時應採用資料保密機制，在傳輸或儲存過程中應採加密方法保護。

5.3.2.4 輸出之資料，應於輸出之前，確認其正確性；對於系統內之訊息，則需保護其完整性。

5.3.3 測試

5.3.3.1 測試環境與線上環境應予以分開。

5.3.3.2 程式設計初步完成後，準備「系統測試記錄表」通知申請單位進行聯合測試，並請申請單位於「系統測試記錄表」中填寫測試結果。

5.3.3.3 程式功能若無法達成申請單位預定需求，則請系統開發人員另行修改程式後，擇期再測試，直至符合預定需求為止。

5.3.4 上線與驗收

系統開發與維護					
文件編號	HGSH-ISMS-B-007	機密等級	一般	版次	1.1

- 5.3.4.1 聯合測試進行順利完成後，進行相關驗收作業，並請申請單位簽收「系統測試記錄表」。
- 5.3.4.2 若原系統已經存在，應於系統上線前訂定「系統上線及緊急復原計畫表」，內容包含系統轉換規劃，轉換備援處理等。
- 5.3.4.3 系統上線後，程式開發者應提出系統設計與功能規格書，內容包含系統作業流程圖、系統資料庫說明表、系統程式碼清冊。
- 5.3.4.4 系統若委由其他單位開發時，應請開發單位交付系統設計與功能規格書，由本校程式開發權責單位審閱，並留存備查。

5.3.5 後續系統增修維護

- 5.3.5.1 專案上線後功能如需修補，申請單位應填「系統需求申請與回覆單」，程式開發權責單位依需求規格進行訪談規劃設計。
- 5.3.5.2 程式開發權責單位完成系統增修作業後與申請單位進行測試驗收結案。

5.4 變更作業控制措施

5.4.1 變更作業應考量之事項：

- 5.4.1.1 在實際執行變更作業前，變更作業之細項建議，應取得權責主管人員之核准。
- 5.4.1.2 應確保系統變更作業不致影響或破壞系統原有的安全控制。
- 5.4.1.3 系統開發或變更，應更新系統文件。
- 5.4.1.4 程式維護時，應在程式內以註解說明異動部分。
- 5.4.1.5 所有系統變更作業請求，皆應建立紀錄供稽核運用。

5.4.2 變更作業之控制流程：

- 5.4.2.1 在實際執行變更作業前，申請者應先填具「系統需求申請與回覆單」提出變更需求，並經權責主管人員核准確認。
- 5.4.2.2 變更作業如有需要，應會辦相關人員配合。
- 5.4.2.3 上線前應先進行測試，必要時請相關人員配合建置測試環境。
- 5.4.2.4 除非事先經由權責主管人員核准外，測試不應在線上營運系統執行。

系統開發與維護					
文件編號	HGSH-ISMS-B-007	機密等級	一般	版次	1.1

5.4.2.5 測試完成後，程式開發權責單位應擬定「系統上線及緊急復原計畫表」，決定上線日期，經權責主管人員確認後始得上線。

5.4.2.6 上線後應立即於線上營運系統再行測試，以確認系統運作正常。測試人員不宜與程式開發者為同一人，以減少錯誤機會發生。

5.4.2.7 上線後測試如發現狀況，應嘗試可否立即排除，如無法立即排除，應依緊急復原計畫，回復上線前原狀。

5.4.2.8 變更作業完成後應修改相關系統設計與功能規格書。

6 相關文件

6.1 通信與作業管理

6.2 資料需求申請表

6.3 系統需求申請與回覆單

系統開發與維護					
文件編號	HGSH-ISMS-B-007	機密等級	一般	版次	1.1

資料需求申請表

填表日期： 年 月 日

系統別			
申請單位		連絡人及電話	
需求事申			
依據文件 請附文件影本			
需求範圍 (請詳列如學生科別、年級、學制、畢業年度)			
需求欄位 請詳列如學生學號、姓名、性別、戶籍地址、聯絡電話或提供範本格式			
申請單位 承辦人及主管簽章	資料權責單位 承辦人及主管簽章	資安單位 承辦人及主管簽章	申請單位簽收 承辦人及主管簽章

※資料僅供需求事由相關目的使用，不得任意提供他人或其他目的使用。

※需求資料內容如包含個人資料應遵守「個人資料保護法」指定專人依相關法令辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

系統開發與維護					
文件編號	HGSH-ISMS-B-007	機密等級	一般	版次	1.1

系統需求申請與回覆單

填表日期： 年 月 日

需求申請說明			
系統名稱		希望啟用日期	年 月 日
作業現況	☐ 未電腦化（ ☐ 新增作業 或 ☐ 舊有人工作業） ☐ 已電腦化（需要 ☐ 新增功能 ☐ 修改功能 ☐ 重新設計系統） ☐ 系統開發中需求變更		
預期成效	使用年限： ☐ 一年內 ☐ 一至三年 ☐ 三至五年 ☐ 五年以上 使用頻率（作業週期）：_____人次/ ☐ 日 ☐ 月 ☐ 季 ☐ 學期 或 ☐ 年 其他成效指標：		
功能/流程描述	☐ 詳細文案（共_____頁） ☐ 參考資料 附件資料共_____件		
申請人		單位主管	

需求申請回覆說明					
說明/可能影響範圍					
評估結果	☐ 自行開發，可於期望時限內完成 ☐ 自行開發，無法於期望時限內完成 ☐ 尋求委外廠商 ☐ 尋求_____協助 ☐ 不建議執行 補充說明：				
配合事項					
預計工時		預計交付 測試日		預計 上線日期	
系統上線及緊急復原計畫表紀錄編號： （若為系統變更請填上編號）					
承辦人		單位主管			