管理系統文件

文件類別	第一階文件	
文件編號	ISMS-M-002	
文件名稱	適用性聲明書	
發行單位	文件管制小組	
發行日期	111 年 02 月 17 日	
版　次	2.3	
訂修廢單位	審　查	核　准
資通安全處理小組		

（原版簽名頁保存於文件管制小組）

訂　　修　　廢　　記　　錄		
版次	發行日期	訂 修 廢 內 容 摘 要
2.0	104/04/30	2015 改版發行。
2.1	107/03/09	修改資訊安全管理制度範圍資訊科技中心單位名稱為圖書資訊處。
2.2	108/04/15	因應資通安全管理法修訂本文件
2.3	111/02/17	調整資訊安全管理制度範圍為「圖書資訊處辦公環境、電腦機房及校務行政系統運作及維護之安全管理。」 調整「A.10.1.2、A.12.4.2、A.14.1.3、A.18.1.5」控制要項。

文件編號	ISMS-M-002	文件名稱	適用性聲明書		
機密等級	內部使用	版　　次	2.3	頁　　次	3 / 25

1.資訊安全管理制度範圍：**圖書資訊處辦公環境、電腦機房及校務行政系統運作及維護之安全管理**

2.適用性聲明

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.5 資訊安全政策				
A.5.1 資訊安全的管理方向 **控制目標：依照營運需要及相關法律與法規，提供管理階層對資訊安全之指示與支持。**				
A.5.1.1	資訊安全政策文件	Y	ISMS-M-001 資通安全管理政策	資通安全管理政策為本校資通安全最高指導原則，為確保資通安全各項作業能順利運作，須制訂資通安全管理政策並公告週知。
A.5.1.2	資訊安全政策之審查	Y	ISMS-M-001 資通安全管理政策	為維持「資通安全管理政策」之適用性及正確性，須定期於「資通安全管理委員會」會議中進行檢討、修訂。
A.6 資訊安全的組織				
A.6.1 內部組織 **控制目標：建立一個管理框架，用以開創與管制組織內資訊安全的實施和操作。**				
A.6.1.1	資訊安全的角色與責任	Y	ISMS-P-002 資通安全組織與權責管理程序書	為有效落實資通安全管理政策及相關管理規範，須明確定義資通安全相關責任。

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.6.1.2	職務的區隔	Y	ISMS-P-010 人力資源安全管理程序書	為降低人員蓄意或誤用對資訊系統所造成之風險，應將人員分工並作職責區隔。
A.6.1.3	與權責機關的聯繫	Y	ISMS-P-002 資通安全組織與權責管理程序書	為確保資通安全相關事件發生時能立即得到相關之建議或緊急之處理，應與主管機關或消防單位維持適當之聯繫。
A.6.1.4	與特殊利害相關團體的聯繫	Y	ISMS-P-002 資通安全組織與權責管理程序書	為取得新技術或相關資通安全知識，應與資訊安全專家提供資通安全相關建議。
A.6.1.5	專案管理的資訊安全	Y	ISMS-P-018 委外作業管理程序書	已於內、外部專案管理的過程中，透過風險評鑑明訂及陳述與專案相關之各項資通安全要求。
A.6.2 行動設備與遠距工作 **控制目標：確保遠距工作與使用行動設備的安全。**				
A.6.2.1	行動設備的政策	Y	ISMS-P-016 資通設備維護與管理程序書	為確保系統使用行動電腦作業之安全，應加以控管。
A.6.2.2	遠距工作	Y	ISMS-P-018 委外作業管理程序書	為確保本校委外廠商以遠端方式存取本校資通設備之安全性，應予以控管。

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.7 人力資源安全				
A.7.1 聘僱之前 **控制目標：確保員工與承包商了解他們的責任，且適合他們被認定的角色。**				
A.7.1.1	篩選	Y	ISMS-P-010 人力資源安全管理程序書	為確保人員晉用時符合內部規定或資格之要求，應建立相關作業人員任用篩選標準。
A.7.1.2	聘僱條款與條件	Y	ISMS-P-010 人力資源安全管理程序書	為確保人員安全，人員任用時需描述其對本校相關安全要求。
A.7.2 聘僱期間 **控制目標：確保員工與承包商認知並履行其資訊安全的責任。**				
A.7.2.1	管理階層責任	Y	ISMS-P-002 資通安全組織與權責管理程序書 ISMS-P-010 人力資源安全管理程序書	為落實資通安全相關規定，員工或外包廠商於工作執掌中應包含明確之資通安全管理責任。
A.7.2.2	資訊安全認知、教育及訓練	Y	ISMS-P-010 人力資源安全管理程序書	為加強相關作業人員資通安全認知以及相關技能，需進行相關教育訓練。
A.7.2.3	懲處過程	Y	ISMS-P-010 人力資源安全管理程序書	為使違反資通安全規定情節者有警惕，應建立相關懲處規定。

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.7.3 聘僱的終止與變更 **控制目標：保護組織的利益，作為變更或終止聘僱的過程之一部分。**				
A.7.3.1	聘僱責任的終止與變更	Y	ISMS-P-010 人力資源安全管理程序書	為確保人員於聘僱終止後一段時間其保密協定及任用條件仍為有效，應於雙方協定或合約中清楚定義。
A.8 資產管理				
A.8.1 資產責任 **控制目標：鑑別組織的資產與明訂適當的保護責任。**				
A.8.1.1	資產清冊	Y	ISMS-P-003 資訊資產管理程序書	為確認所需保護之標的，應清查所有資產並適當的分類後列冊。
A.8.1.2	資產的擁有權	Y	ISMS-P-003 資訊資產管理程序書	為確保所有資訊資產皆有適當之維護，應指派專人負責管理。
A.8.1.3	資產之可被接受的使用	Y	ISMS-P-003 資訊資產管理程序書	為確保人員對資訊資產使用皆有一定認知，應制定相關管理規則。
A.8.1.4	資產歸還	Y	ISMS-P-010 人力資源安全管理程序書	為確保所有人員於終止聘僱或合約時，歸還其所使用之本校資訊資產，應制定清楚之規範以進行管理。
A.8.2 資訊分類 **控制目標：確保資訊受到適切等級的保護，依照其對組織的重要性。**				

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.8.2.1	資訊分類	Y	ISMS-P-003 資訊資產管理程序書	為確保相關資訊資產保護措施之實施，應制定資訊類資產的分級原則以區別資訊之機密等級。
A.8.2.2	資訊標示	Y	ISMS-P-003 資訊資產管理程序書	為確保各資訊資產皆有分級原則以區別資訊之機密等級，應制定資訊資產標示與處理程序。
A.8.2.3	資產處置	Y	ISMS-P-003 資訊資產管理程序書 ISMS-P-016 資通設備維護與管理程序書	須確保已制定相關書面程序供資訊資產各項處理作業遵循，且需要之使用者皆可取得相關程序文件。
A.8.3 媒體的處置 **控制目標：防止儲存在媒體的資訊被未經授權的揭露、修改、移除或破壞。**				
A.8.3.1	可攜式媒體的管理	Y	ISMS-P-016 資通設備維護與管理程序書	為確保可攜式及移動式電腦媒體之使用皆有適當管控，如授權或資料移除等控制，應制定相關管理規定。
A.8.3.2	媒體的汰除	Y	ISMS-P-003 資訊資產管理程序書 ISMS-P-016 資通設備維護與管理程序書	為避免媒體因報廢不當，而將敏感資料外洩，應制定標準作業程序。

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.8.3.3	實體媒體的傳送	Y	ISMS-P-003 資訊資產管理程序書 委外作業管理程序書 ISMS-P-018 委外作業管理程序書	為確保與外部機關之資料交換時的媒體安全，應有明確的管控。
A.9 存取控制				
A.9.1 存取控制的營運要求 **控制目標：限制資訊與資訊處理設施的存取。**				
A.9.1.1	存取控制政策	Y	ISMS-P-013 帳號密碼及存取控制管理程序書	為確保資通系統存取時的安全，應制定一套符合需求之存取控制政策。
A.9.1.2	網路與網路服務的存取	Y	ISMS-P-012 網路安全管理程序書	為確保網路使用之安全，應制定使用之相關規範。
A.9.2 使用者存取管理 **控制目標：確保經授權使用者對系統與服務的存取及防止未經授權的存取。**				
A.9.2.1	使用者登錄與註銷	Y	ISMS-P-013 帳號密碼及存取控制管理程序書	為確保使用者帳號之安全，應有正式授權程序。
A.9.2.2	使用者的存取配置	Y	ISMS-P-013 帳號密碼及存取控制管理程序書	為確保使用者帳號之安全，應有正式授權程序。

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.9.2.3	特權的管理	Y	ISMS-P-013 帳號密碼及存取控制管理程序書	為降低擁有特殊權限之管理者可能造成之非法存取，應透過正式授權管道授權。
A.9.2.4	使用者的機密授權資訊之管理	Y	ISMS-P-013 帳號密碼及存取控制管理程序書	為確保使用者通行碼之安全，應制定授權管理程序。
A.9.2.5	使用者存取權限的審查	Y	ISMS-P-013 帳號密碼及存取控制管理程序書	為確保使用者存取權限是否合宜，應定期執行存取權限審查。
A.9.2.6	存取權限的移除或調整	Y	ISMS-P-010 人力資源安全管理程序書 ISMS-P-013 帳號密碼及存取控制管理程序書	為確保人員或廠商在聘僱或合約終止或職務調整時的安全，應同步完成其對資訊或設備的存取權限。
A.9.3 使用者責任 **控制目標：讓使用者在維護他們的鑑別資訊上負責。**				
A.9.3.1	機密授權資訊的使用	Y	ISMS-P-013 帳號密碼及存取控制管理程序書	為確保通行碼使用符合要求，使用者應確實遵守密碼使用原則。
A.9.4 系統與應用系統的存取控制 **控制目標：防止對系統與應用系統的未授權存取。**				

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.9.4.1	資訊存取限制	Y	ISMS-P-013 帳號密碼及存取控制管理程序書	為確保資訊存取之安全，應依據既定的存取控制政策提供應用系統的使用者存取資訊和應用系統功能的權限。
A.9.4.2	安全之登入程序	Y	ISMS-P-014 系統發展與維護管理程序書	為降低不當存取之風險，應對登入作業系統嚴加限制與控制。
A.9.4.3	通行碼管理系統	Y	ISMS-P-013 帳號密碼及存取控制管理程序書 ISMS-P-014 系統發展與維護管理程序書	為確保資通系統均符合密碼管理要求，應建立密碼管理機制。
A.9.4.4	特權的公用程式之使用	Y	ISMS-P-013 帳號密碼及存取控制管理程序書	為確保應用程式之安全，應對其使用之公用程式嚴加限制與控制。
A.9.4.5	程式原始碼的存取控制	Y	ISMS-P-014 系統發展與維護管理程序書	為避免原始程式碼遭不當存取或修改，應對程式碼存取加以適切的管制。
A.10 密碼				
A.10.1 密碼控制措施 **控制目標：確保密碼的適當與有效使用，以保護資訊的機密性、鑑別性與/或完整性。**				

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.10.1.1	使用密碼控制措施的政策	Y	ISMS-P-013 帳號密碼及存取控制管理程序書	為確保系統之使用符合安全要求，已制定密碼使用規範。
A.10.1.2	金鑰管理	Y	ISMS-P-12 網路安全管理程序書 ISMS-P-13 帳號密碼及存取控制管理程序書	為確保金鑰及憑證的使用與保護，已制定金鑰管理規範，並加以實作與管理。
A.11 實體與環境安全				
A.11.1 安全區域 **控制目標：防止組織的資訊與資訊處理設施遭未經授權的存取、損害及干擾。**				
A.11.1.1	實體安全周界	Y	ISMS-P-011 實體與環境安全管理程序書	為確保相關實體安全控制符合安全上的需求，應明確定義實體安全範圍。
A.11.1.2	實體進入控制措施	Y	ISMS-P-011 實體與環境安全管理程序書	為確保只有授權人員方可進入實體安全區域，應制定人員進出管制規定。
A.11.1.3	保全辦公室、房間及設施	Y	ISMS-P-011 實體與環境安全管理程序書	為確保辦公區域設施之安全，應有適當之管控措施。

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.11.1.4	對外部與環境威脅的保護	Y	ISMS-P-011 實體與環境安全管理程序書	為避免安全工作區域遭受外在環境威脅，如火災、水災等重大災害之影響，應設置適當之保護措施。
A.11.1.5	在安全區域內工作	Y	ISMS-P-011 實體與環境安全管理程序書 資訊機房管理程序書	為確保在安全區域內工作之人員有適當之控制措施，以避免惡意行為之發生。
A.11.1.6	收發與裝卸區	Y	ISMS-P-011 實體與環境安全管理程序書	為防止未經授權之人員進入，應區分收發區及裝卸區。
A.11.2 設備 **控制目標：防止資產的遺失、損害、竊盜或破解，並防止組織運作的中斷。**				
A.11.2.1	設備安置與保護	Y	ISMS-P-011 實體與環境安全管理程序書 資訊機房管理程序書	為避免設備因環境影響而造成損害，應考量合適地點並加以保護。
A.11.2.2	支援的公用設施	Y	ISMS-P-011 實體與環境安全管理程序書	為確保設備不受電源或其它設施失效而中斷，應對支援設施（如空調、水電等）定期維護檢查。
A.11.2.3	佈纜的安全	Y	ISMS-P-012 網路安全管理程序書 ISMS-P-011 實體與環境安全管理程序書	為避免線路遭受破壞或拔除，線路應標示及保護。

文件編號	ISMS-M-002	文件名稱	適用性聲明書		
機密等級	內部使用	版　　次	2.3	頁　　次	13 / 25

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.11.2.4	設備維護	Y	ISMS-P-016 資通設備維護與管理程序書	為避免因設備損壞造成服務中斷，應對實體設備進行適當維護。
A.11.2.5	資產的攜出	Y	ISMS-P-003 資訊資產管理程序書 ISMS-P-016 資通設備維護與管理程序書 ISMS-P-011 實體與環境安全管理程序書	為確保資產不被任意攜出本校，應訂定相關管控措施。
A.11.2.6	場外設備的安全	Y	ISMS-P-016 資通設備維護與管理程序書	為防止資通設備攜出本校以外地點可能遭受之損害，應制定管理規定。
A.11.2.7	設備的汰除或再使用之安全	Y	ISMS-P-003 資訊資產管理程序書	為確保相關設備報廢或回收使用時不造成資料洩漏，應訂定相關管控措施。
A.11.2.8	無人看管的使用者設備	Y	ISMS-P-016 資通設備維護與管理程序書	為確保無人看管的資通設備之安全，如公用之電腦，應於使用後立即登出。
A.11.2.9	桌面淨空與螢幕淨空政策	Y	ISMS-P-011 實體與環境安全管理程序書	為降低機密資料遭不當存取，應制定電腦螢幕淨空及桌面淨空規範。
A.12 作業的安全				

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.12.1 作業之程序與責任 **控制目標：確保正確與安全地操作資訊處理設施。**				
A.12.1.1	文件化作業程序	Y	各項程序書(二階)、標準書(三階）文件	為確保資通各項作業均有書面程序供遵循，應製作相關之程序讓需要之使用者皆可取得。
A.12.1.2	變更管理	Y	ISMS-P-014 系統發展與維護管理程序書 ISMS-P-018 委外作業管理程序書	為確保作業系統及應用系統軟體不因變更不當所造成之風險，應制定相關變更管理規定。
A.12.1.3	容量管理	Y	ISMS-P-014 系統發展與維護管理程序書	為確保系統之執行效能，各系統應考量其設備及系統之容量規劃及資源管理。
A.12.1.4	開發、測試及運作環境的分隔	Y	ISMS-P-014 系統發展與維護管理程序書	為避免系統之開發、測試活動可能會影響正式營運，應將開發、測試作業與正式作業區隔。
A.12.2 防範惡意程式 **控制目標：確保資訊與資訊處理設施對惡意程式的防範。**				
A.12.2.1	對抗惡意程式的控制措施	Y	ISMS-W-002 一般資通設備安全管理作業標準書	為避免資料或軟體遭受惡意碼之攻擊，應加以警示或制定必要之回復措施。

文件編號	ISMS-M-002	文件名稱	適用性聲明書		
機密等級	內部使用	版　　次	2.3	頁　　次	15 / 25

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.12.3 備份 **控制目標：防範資料的損失。**				
A.12.3.1	資訊備份	Y	ISMS-P-015 資訊備份管理程序書	為確保所有重要的資訊或軟體在災難發生時能立即復原，應定期執行備份與測試。
A.12.4 存錄與監控 **控制目標：紀錄事件與生成證據。**				
A.12.4.1	事件存錄	Y	ISMS-P-014 系統發展與維護管理程序書	應產生、保留與定期審查記錄使用者活動、異常、失誤及資通安全事件之稽核日誌，以協助未來調查與存取控制監視，且錯誤通報之流程應有明確規範。
A.12.4.2	日誌資訊的保護	Y	ISMS-P-014 系統發展與維護管理程序書	為降低系統或稽核日誌遭修改或不當存取風險，應對系統或稽核日誌加以保護。
A.12.4.3	管理者與操作者日誌	Y	ISMS-P-012 網路安全管理程序書 ISMS-P-013 帳號密碼及存取控制管理程序書	為確保系統之管理能有效執行，系統管理者及操作活動應留下日誌。

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.12.4.4	時脈同步	Y	ISMS-P-016 資通設備維護與管理程序書	為確保資通系統的時間一致性，各系統應定期進行時間校正。
A.12.5 作業軟體的控制 **控制目標：確保作業系統的完整性。**				
A.12.5.1	作業系統上軟體的安裝	Y	ISMS-P-014 系統發展與維護管理程序書	相關軟體之安裝、設定及維護由系統負責人進行。
A.12.6 技術脆弱性管理 **控制目標：防範技術脆弱性的利用。**				
A.12.6.1	技術脆弱性的管理	Y	ISMS-P-012 網路安全管理程序書	為確保資通技術弱點能適當找出並改正，應制定相關修補及改正程序。
A.12.6.2	軟體安裝的限制	Y	ISMS-P-017 軟體使用管理程序書 ISMS-W-002 一般資通設備安全管理作業標準書	建立與實施本校各項電腦軟體之安裝與管控規定，以避免因軟體之漏洞造成軟體被誤用及入侵的風險。
A.12.7 資訊系統稽核考量 **控制目標：使作業系統上的稽核活動之衝擊降至最低。**				
A.12.7.1	資訊系統稽核控制	Y	ISMS-P-007 資通安全稽核管理程序書	為確保稽核時之安全，涉及作業系統檢查的活動應獲同意。
A.13 通訊安全				

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.13.1 網路安全管理 **控制目標：確保對網路內資訊與支援性資訊處理設施的保護。**				
A.13.1.1	網路控制措施	Y	ISMS-P-012 網路安全管理程序書	為確保透過網路傳送資料之機密性及完整性，應加入登入管制或監控機制。
A.13.1.2	網路服務的安全	Y	ISMS-P-012 網路安全管理程序書 ISMS-W-004 網路連線中斷緊急應變作業標準書	為確保網路服務之安全，應制定網路服務水準及管理要求。
A.13.1.3	網路區隔	Y	ISMS-P-012 網路安全管理程序書	為確保網路之安全性，應採取實體區隔或以防火牆區隔。
A.13.2 資訊轉換 **控制目標：維護組織內及與外部個體所轉換資訊的安全。**				
A.13.2.1	資訊交換政策與程序	Y	ISMS-P-018 委外作業管理程序書	為確保與外部機關之資料交換的安全，應制定管控程序。
A.13.2.2	資訊交換的協議	Y	ISMS-P-018 委外作業管理程序書	為確保與外部機關之資料交換應有適當之協議，應有明確的管控。
A.13.2.3	電子傳訊	Y	ISMS-P-018 委外作業管理程序書 ISMS-P-012 網路安全管理程序書	為避免資訊遭到未經授權之變更，應適當地保護其傳遞過程。

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.13.2.4	機密性或保密協議	Y	ISMS-P-010 人力資源安全管理程序書	為確保人員保守業務資訊，相關作業人員及委外廠商須簽署保密條款。
A.14 資訊系統獲取、開發及維護				
A.14.1 資訊系統的安全要求 **控制目標：確保跨越整個生命週期內，資訊安全是整體資訊系統的一部分。這也包含在提供有關公共網路服務之資訊系統的要求中。**				
A.14.1.1	資訊安全要求分析與規格	Y	ISMS-P-014 系統發展與維護管理程序書	為降低資通系統之風險，應在資通系統開發階段確認安全的要求。
A.14.1.2	公共網路應用系統之安全服務	Y	ISMS-P-012 網路安全管理程序書	將公眾網路上傳輸而涉及應用系統服務的資訊加以保護，免於詐欺行為、契約爭議及未經授權的揭露與修改，確保應用服務資訊之完整性及機密性。
A.14.1.3	保護應用系統服務之交易	Y	ISMS-P-12 網路安全管理程序書 ISMS-P-14 系統發展與維護管理程序書	為確保應用服務交易之安全，應採取適當的控制措施。
A.14.2 開發與支援過程的安全 **控制目標：確保資訊安全被整合至資訊系統開發生命週期之設計與實施之中。**				

文件編號	ISMS-M-002	文件名稱	適用性聲明書		
機密等級	內部使用	版　　次	2.3	頁　　次	19 / 25

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.14.2.1	安全開發政策	Y	ISMS-P-014 系統發展與維護管理程序書	為確保軟體與系統開發的規則已應用至本校，應建立軟體與系統開發管理程序以管控本校資通系統。
A.14.2.2	系統變更控制程序	Y	ISMS-P-014 系統發展與維護管理程序書	為將不當變更造成資通系統毀損的情形降到最低，應對變更的執行採取適當的控制措施。
A.14.2.3	作業系統變更後的應用系統技術審查	Y	ISMS-P-014 系統發展與維護管理程序書	為確保作業系統變更時不影響應用系統，應在實施完成後進行適切的檢查。
A.14.2.4	套裝軟體變更的限制	Y	ISMS-P-014 系統發展與維護管理程序書 ISMS-P-017 軟體使用管理程序書	為確保系統之安全，應防止修改套裝軟體的行為。
A.14.2.5	安全系統工程原則	Y	ISMS-P-014 系統發展與維護管理程序書	設計安全系統之原則應建立文件化的管理程序，並實作於本校所有資通系統。
A.14.2.6	安全開發環境	Y	ISMS-P-014 系統發展與維護管理程序書	為確保系統開發過程之安全性，應建立與適切地保護涵蓋整個系統開發生命週期中所有活動之安全開發環境。

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.14.2.7	委外開發	Y	ISMS-P-018 委外作業管理程序書	為確保軟體委外開發之安全，應制定相關管理及監督機制。
A.14.2.8	系統安全測試	Y	ISMS-P-014 系統發展與維護管理程序書	為確保系統之安全性，應於系統發展中執行安全性功能之測試。
A.14.2.9	系統驗收測試	Y	ISMS-P-014 系統發展與維護管理程序書	為確保新系統驗收和使用前均具有完整之文件及驗收測試，應建立適當之驗收準則。
A.14.3 測試資料 **控制目標：確保測試用途之資料的保護。**				
A.14.3.1	測試資料的保護	Y	ISMS-P-014 系統發展與維護管理程序書	為確保系統使用之測試資料的安全，應對測試資料實施適切的保護及管控措施。
A.15 供應商關係				
A.15.1 供應商關係的資訊安全 **控制目標：確保供應商可存取之組織資產的保護。**				
A.15.1.1	供應商關係的資訊安全政策	Y	ISMS-P-018 委外作業管理程序書	為降低供應商存取本校資訊資產相關風險，應與供應商協議資通安全要求事項並於合約中清楚敘明。

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.15.1.2	供應商協議內的安全處理	Y	ISMS-P-018 委外作業管理程序書	為確保與第三方之相關合約中，皆具備保密等安全要求，應制定可滿足安全要求之合約條款。
A.15.1.3	資訊與通信科技供應鏈	Y	ISMS-P-018 委外作業管理程序書	與供應商之協議應涵蓋處理資訊與通信科技之服務與產品供應鏈相關的資通安全風險。
A.15.2 供應商服務之交付管理 **控制目標：維持議定等級之資訊安全及服務交付，並能與供應商協議一致。**				
A.15.2.1	供應商服務的監控與審查	Y	ISMS-P-018 委外作業管理程序書	為確保第三方人員達成於合約預定之服務水準，應制定相關監控或安全管制措施。
A.15.2.2	供應商服務變更的管理	Y	ISMS-P-018 委外作業管理程序書	為因應第三方服務變更或調整時可能之風險，應制定相關管理程序。
A.16 資訊安全事故管理				
A.16.1 資訊安全事故與改進的管理 **控制目標：確保資訊安全事故管理之一致與有效的作法，包含安全事件與弱點的傳達。**				
A.16.1.1	責任與程序	Y	ISMS-P-009 資通安全事件通報及應變管理程序範本書	為降低影響資通安全的事件造成之影響，應建立適當途徑通報。

文件編號	ISMS-M-002	文件名稱	適用性聲明書		
機密等級	內部使用	版　　次	2.3	頁　　次	22 / 25

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.16.1.2	通報資訊安全事件	Y	ISMS-P-009 資通安全事件通報及應變管理程序範本書	為確保資通安全事件應循適當的管理途徑儘快通報，應建立正式的通報程序以及事件反應程序。
A.16.1.3	通報資訊安全弱點	Y	ISMS-P-009 資通安全事件通報及應變管理程序範本書	為降低可能發生資安事件的機率，應規範人員和廠商在發現、懷疑系統或服務出現安全弱點或受到威脅時，必須立即通報。
A.16.1.4	資訊安全事件的評鑑與決定	Y	ISMS-P-009 資通安全事件通報及應變管理程序範本書	資安事件發生時，應對資安事件進行評估與分析，以決定是否將其歸類於資通安全事故並進行後續適當之處置。
A.16.1.5	對資訊安全事故的回應	Y	ISMS-P-009 資通安全事件通報及應變管理程序範本書	應依據已建立之資安事件管理程序進行資安事故之通報、處置及預防作業。
A.16.1.6	從資訊安全事故中學習	Y	ISMS-P-009 資通安全事件通報及應變管理程序範本書	為降低資通安全事件發生之機率及損失，應將事件和失敗的類型、數量進行量化與監控。
A.16.1.7	證據的收集	Y	ISMS-P-009 資通安全事件通報及應變管理程序範本書	為確保事件發生時能有足夠之證據提起訴訟，應制定證據保存之規定。

文件編號	ISMS-M-002	文件名稱	適用性聲明書		
機密等級	內部使用	版　　次	2.3	頁　　次	23 / 25

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.17 營運持續管理的資訊安全層面				
A.17.1 資訊安全的持續性 **控制目標：資訊安全持續應嵌入於組織的營運持續管理系統。**				
A.17.1.1	規劃資訊安全的持續性	Y	ISMS-P-006 業務持續管理程序書 ISMS-P-004 資通安全風險管理程序書	為確保重要系統營運中斷時，能在一定時間內恢復營運，應發展營運持續計畫。
A.17.1.2	實施資訊安全持續	Y	ISMS-P-006 業務持續管理程序書 ISMS-P-004 資通安全風險管理程序書	為確保各資通系統安全使其能穩定的運作，應對重要系統進行營運持續運作規劃，並且建立有效之營運持續計畫以確保重要系統營運中斷時，能在一定時間內恢復營運。
A.17.1.3	驗證、審查及評估資訊安全持續	Y	ISMS-P-006 業務持續管理程序書	為確保營運持續計畫有效，應定期測試及更新。
A.17.2 複式配置 **控制目標：確保資訊處理設施的可用性。**				
A.17.2.1	資訊處理設施的可用性	Y	ISMS-P-016 資通設備維護與管理程序書	應對資通處理設施實作充分的複式措施以達到可用性要求。
A.18 遵循性				

文件編號	ISMS-M-002	文件名稱	適用性聲明書		
機密等級	內部使用	版　　次	2.3	頁　　次	24 / 25

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.18.1 遵循適法性與契約要求 **控制目標：避免違反有關資訊安全的法律、法令、法規或契約義務，以及任何安全要求。**				
A.18.1.1	識別適用之法規與契約要求	Y	ISMS-P-001 文件與紀錄管理程序書	為避免違反相關法令、法規，應鑑別出相關法令、法規。
A.18.1.2	智慧財產權	Y	ISMS-P-017 軟體使用管理程序書	為確保人員遵守智慧財產權相關法令、法規之要求，應制定適當之管制程序。
A.18.1.3	紀錄的保護	Y	ISMS-P-001 文件與紀錄管理程序書	為確保資安管理系統制度文件、日誌、稽核報告及管理審查紀錄之安全，均需加以控管。
A.18.1.4	隱私權與個人識別資訊的保護	Y	ISMS-P-014 系統發展與維護管理程序書 個人資料保護法、PIMS	為確保個人資料收集、處理皆依照相關法令規定執行，應制定相關規範。
A.18.1.5	加密控制措施的法規	Y	ISMS-P-13 帳號密碼及存取控制管理程序書 電子簽章法	為確保遵循加密控制相關協議、法律及法規，應訂定加密式控制相關規範。
A.18.2 資訊安全審查 **控制目標：確保資訊安全是依據組織政策與程序實施與操作。**				

文件編號	ISMS-M-002	文件名稱	適用性聲明書		
機密等級	內部使用	版　　次	2.3	頁　　次	25 / 25

條文編號	ISO 27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.18.2.1	資訊安全的獨立審查	Y	ISMS-P-002 資通安全組織與權責管理程序書 ISMS-P-007 資通安全稽核管理程序書	為確保資訊安全管理制度推行之符合性與有效性，應有管理階層進行獨立的管理審查。
A.18.2.2	安全政策與標準的遵循性	Y	ISMS-M-001 資通安全管理政策 ISMS-P-001 文件與紀錄管理程序書	管理階層應確保其責任範圍內所有安全程序皆正確執行，以達成各項安全政策與標準的遵循性。
A.18.2.3	技術遵循性審查	Y	ISMS-P-012 網路安全管理程序書	應定期查核各資通系統是否遵循所制定的各項資通安全政策與標準。