大 仁 科 技 大 學
Tajen University

管 制 文 件 訂 修 廢 履 歷 表

文件編號	資訊-手冊-02	文件名稱	適用性聲明書	
使用部門	圖書資訊館		機密等級	普通

版次	頁數	文件修訂摘要	實施日期
A.0	21	初版	99/05/24

訂修廢者	單位主管	資訊安全長

※管制文件不得擅自塗改及做記號並禁止影印。

1.資訊安全管理制度範圍：**本校圖書資訊館數位學習中心及校務資訊組辦公環境之安全管理。資訊機房及校務資訊系統運作及維護之安全管理。**

2.適用性聲明

條文編號	ISO27001 控制要項	是否適用	參考文件	適用與非適用之說明
A.5 **安全政策**				
A.5.1 **資訊安全政策** **控制目標：依照營運要求及相關法律與法規，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	資訊安全政策	資訊安全政策為本校資訊安全最高指導原則，為確保資訊安全各項作業能順利運作，須制訂資訊安全政策並公告週知。
A.5.1.2	資訊安全政策之審查	Y	資訊安全政策	為維持「資訊安全政策」適用性及正確性，須定期於「資訊安全執行小組審查會議」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：於組織內管理資訊安全**				
A.6.1.1	管理階層對資訊安全的承諾	Y	資訊安全政策	為清楚顯示管理階層對資訊安全之責任，特成立資訊安全執行小組並制定相關程序以利執行。

A.6.1.2	資訊安全協調工作	Y	資安組織與權責管理程序書	為維持資訊安全管理系統跨單位運作正常，須成立資訊安全執行小組推行相關管理活動。
A.6.1.3	資訊安全責任的配置	Y	資安組織與權責管理程序書	為有效落實資訊安全政策及相關管理規範，須明確定義資訊安全相關責任。
A.6.1.4	資訊處理設施的授權過程	Y	資訊資產管理程序書	為確保各資訊系統或相關設備之新增、異動或使用均經過授權程序，須制定相關規定以維護其安全。
A.6.1.5	機密性協議	Y	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.6.1.6	與權責機關的聯繫	Y	資安組織與權責管理程序書	為確保資訊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.6.1.7	與特殊利害相關團體的聯繫	Y	資安組織與權責管理程序書	為取得新技術或相關資訊安全知識，應與資訊安全專家提供資訊安全相關建議。
A.6.1.8	資訊安全的獨立審查	Y	資安組織與權責管理程序書 資訊安全稽核管理程序書	為確保資訊安全管理系統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.6.2 **外部團體** **控制目標：維持外部團體所存取、處理、管理或與其通訊之組織資訊與資訊處理設施的安全**				
A.6.2.1	與外部團體相關的風險之識別	Y	資訊資產管理程序書 資訊安全風險管理程序書	為確保廠商所提供維護服務部份所涉及之設備、軟體無資訊安全之虞，故需評估資

				訊系統開放給第三方存取之風險。
A.6.2.2	處理客戶事務的安全說明	Y	外單位資訊存取管理程序書	為確保外部人員存取本校資訊或資訊設備時之安全。
A.6.2.3	第三方協議中之安全說明	Y	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.7 **資產管理**				
A.7.1 **資產責任** **控制目標：達成及維持組織資產的適切保護**				
A.7.1.1	資產清冊	Y	資訊資產管理程序書	為確認所需保護之標的，應清查將所有資產清查並適當的分類後列冊。
A.7.1.2	資產的擁有權	Y	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.7.1.3	資產之可被接受的使用	Y	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.7.2 **資訊分類** **控制目標：確保資產受到適切等級的保護**				
A.7.2.1	分類的指導綱要	Y	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.7.2.2	資訊標示與處置	Y	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 **人力資源安全**				
A.8.1 **聘僱之前** **控制目標：確保員工、承包商及第三方使用者了解其責任，並勝任其所被認定的角色，以降低竊盜、詐欺或設施誤用的風險**				
A.8.1.1	角色與責任	Y	人力資源安全管理程序書	為使相關人員包含第三方使用者了解其所應負之資訊安全職責，工作執掌中應定義其所負之資訊安全責任。
A.8.1.2	篩選	Y	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.8.1.3	聘僱條款與條件	Y	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.8.2 **聘僱期間** **控制目標：確保所有員工、承包商及第三方使用者認知資訊安全的威脅與關切事項、其基本責任與強制責任，並有能力在日常工作中支持組織安全政策與降低人為錯誤的風險**				
A.8.2.1	管理階層責任	Y	人力資源安全管理程序書	為落實資訊安全相關規定，員工或外包廠商於工作執掌中應包含明確之資訊安全管理責任。

A.8.2.2	資訊安全認知、教育及訓練	Y	人力資源安全管理程序書 人員教育訓練管理程序書	為加強相關作業人員資訊安全認知以及相關技能，需進行相關教育訓練。
A.8.2.3	懲罰過程	Y	人力資源安全管理程序書	為使違反資訊安全規定情節者有警惕,應建立相關懲處規定。
A.8.3 **聘僱終止或變更** **控制目標：確保員工、承包商及第三方使用者以有條理的方式脫離組織或變更聘僱**				
A.8.3.1	終止責任	Y	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.8.3.2	資產的歸還	Y	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圖書資訊館資訊資產，應制定清楚之規範以進行管理。
A.8.3.3	存取權限的移除	Y	人力資源安全管理程序書 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安全，應同步完成其對資訊或設備的存取權限。
A.9 **實體與環境安全**				
A.9.1 **安全區域** **控制目標：防止組織場所與資訊遭未經授權的實體存取、損害及干擾**				
A.9.1.1	實體安全周界	Y	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.9.1.2	實體進入控制措施	Y	辦公區域管理程序書 資訊機房管理程序書	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.9.1.3	保全辦公室、房間及設施	Y	辦公區域管理程序書	為確保辦公區域設施之安全，應有適當之管控措施。
A.9.1.4	對外部與環境威脅的保護	Y	辦公區域管理程序書 資訊機房管理程序書	為確保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.9.1.5	在安全區域內工作	Y	辦公區域管理程序書 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.9.1.6	公共進出、收發、及裝卸區	Y	資訊機房管理程序書 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.9.2 **設備安全** **控制目標：防止資產的遺失、損害、竊盜或破解，並防止組織活動的中斷**				
A.9.2.1	設備安置與保護	Y	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.9.2.2	支援的公用設施	Y	資訊機房管理程序書	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.9.2.3	佈纜的安全	Y	網路安全管理程序書 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。

A.9.2.4	設備維護	Y	資訊機房管理程序書 資訊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.9.2.5	場外設備的安全	Y	資訊設備維護與管理程序書	為防止資訊設備攜出本校圖書資訊館以外地點可能遭受之損害，應制定管理規定。
A.9.2.6	設備的安全汰除或再使用	Y	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.9.2.7	財產的攜出	Y	資訊資產管理程序書 資訊設備維護與管理程序書	為確保資產不被任意攜出本校圖書資訊館，應訂定相關管控措施。
A.10 **通訊與作業管理**				
A.10.1 **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.10.1.1	文件化作業程序	Y	各項程序書(二階)、標準書(三階)文件	為確保資訊處理及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.10.1.2	變更管理	Y	系統發展與維護管理程序書	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.10.1.3	職務的區隔	Y	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成之風險，應將人員分工並作職責區隔。

A.10.1.4	開發、測試及運作設施的分隔	Y	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.10.2 **第三方服務交付管理** **控制目標：實作與維持適切等級之資訊安全及服務交付，並能與第三方服務交付協議一致**				
A.10.2.1	服務交付	Y	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，應制定可行之服務水準及處理計畫。
A.10.2.2	第三方服務的監視與審查	Y	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.10.2.3	第三方服務變更的管理	Y	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.10.3 **系統規劃與驗收** **控制目標：使系統失效的風險最小化**				
A.10.3.1	容量管理	Y	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.10.3.2	系統驗收	Y	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或測試，應建立適當之驗收準則。
A.10.4 **防範惡意碼與行動碼** **控制目標：保護軟體與資訊的完整性**				

A.10.4.1	對抗惡意碼的控制措施	Y	電腦病毒防範管理程序書	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。
A.10.4.2	對抗行動碼的控制措施	Y	網路安全管理程序書	為避免行動碼對應用系統或網路造成危害，應有適當之管制措施。
A.10.5 **備份** **控制目標：維持資訊及資訊處理設施的完整性與可用性**				
A.10.5.1	資訊備份	Y	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.10.6 **網路安全管理** **控制目標：確保對網路內資訊與支援性基礎建設的保護**				
A.10.6.1	網路控制措施	Y	網路安全管理程序書	為確保透過網路傳送資料之機密及完整性，應加入登入管制或監控機制。
A.10.6.2	網路服務的安全	Y	網路安全管理程序書 無線網路安全管理作業說明書 防火牆管理程序書 電子郵件管理程序書 弱點管理程序書	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.10.7 **媒體的處置** **控制目標：防止資產被未經授權的揭露、修改、移動或破壞，以及營運活動的中斷**				

A.10.7.1	可移除式媒體的管理	Y	可攜式設備及儲存媒體管理程序書	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.10.7.2	媒體的汰除	Y	資訊資產管理程序書 資訊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。
A.10.7.3	資訊處置程序	Y	資訊資產管理程序書 資訊設備維護與管理程序書	為確保資訊處理及各項作業均有書面程序供遵循，應製作相關之程序並使需要之使用者皆可取得。
A.10.7.4	系統文件的安全	Y	資訊資產管理程序書 文件與資料管理程序書	為確保重要系統文件之安全，應妥善存放。
A.10.8 資訊交換 控制目標：維護組織內及與任何外部個體所交換資訊與軟體的安全				
A.10.8.1	資訊交換政策與程序	Y	外單位資訊存取管理程序書	為確保與外部機關之資料交換之安全，應制定管控程序。
A.10.8.2	交換協議	Y	外單位資訊存取管理程序書	為確保與外機關之資料交換應有適當之協議，應有明確的管控。
A.10.8.3	輸送中的實體媒體	Y	資訊資產管理程序書 外單位資訊存取管理程序書 資訊備份管理程序書	為確保與外機關之資料交換之媒體安全，應有明確的管控。
A.10.8.4	電子傳訊	Y	外單位資訊存取管理程序書 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。

A.10.8.5	營運資訊系統	Y	應用系統管理程序書 系統發展與維護管理程序書 網路安全管理程序書 帳號密碼及存取控制管理程序書	為確保本校圖書資訊館營運相關之資訊系統資料安全，應有明確的管控措施。
A.10.9 **電子商務服務** **控制目標：確保電子商務服務的安全性及其安全的使用**				
A.10.9.1	電子商務	N	未提供電子商務服務，不適用。	目前本校圖書資訊館未提供電子商務服務。
A.10.9.2	線上交易	N	未提供線上交易，不適用。	目前本校圖書資訊館未提供線上交易。
A.10.9.3	公眾可用的資訊	Y	系統發展與維護管理程序書	為確保公開於網路上之資訊不受未經授權之修改，應保護資料之完整性。
A.10.10 **監視** **控制目標：偵測未經授權的資訊處理活動**				
A.10.10.1	稽核存錄	Y	系統發展與維護管理程序書	為確保使用者存取或異常紀錄於安全事件發生時可做為調查依據，相關系統之活動均需留下稽核紀錄。
A.10.10.2	監控系統的使用	Y	帳號密碼及存取控制管理程序書	為確保相關資訊設備維運品質，應加以監控。
A.10.10.3	日誌資訊的保護	Y	帳號密碼及存取控制管理程序書	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.10.10.4	管理者與操作者日誌	Y	網路安全管理程序書 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。
A.10.10.5	失誤存錄	Y	帳號密碼及存取控制管理程序書	為確保資訊處理或通訊系統的錯誤問題皆由留下記錄，錯誤通報之流程應有明確的規定。
A.10.10.6	鐘訊同步	Y	資訊設備維護與管理程序書	為確保資訊系統的時間一致性各系統，應定期進行時間校正。
A.11 **存取控制**				
A.11.1 **存取控制的營運要求** **控制目標：控制資訊的存取**				
A.11.1.1	存取控制政策	Y	帳號密碼及存取控制管理程序書	為確保資訊系統存取時安全，應制定一套符合需求之存取控制政策。
A.11.2 **使用者存取管理** **控制目標：確保經授權使用者對資訊系統的存取與防止未經授權的存取**				
A.11.2.1	使用者註冊	Y	應用系統管理程序書	為確保使用者帳號之安全，應有正式授權程序。
A.11.2.2	特權管理	Y	應用系統管理程序書	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.11.2.3	使用者通行碼管理	Y	應用系統管理程序書 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.11.2.4	使用者存取權限的審查	Y	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.11.3 **使用者責任** **控制目標：防止資訊與資訊處理設施被未經授權的使用者存取、洩露或竊盜**				
A.11.3.1	通行碼的使用	Y	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.11.3.2	無人看管的使用者設備	Y	資訊設備維護與管理程序書	為確保無人看管資訊設備之安全，如公用之電腦應於使用後立即登出。
A.11.3.3	桌面淨空與螢幕淨空政策	Y	辦公區域管理程序書	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.11.4 **網路存取控制** **控制目標：防止網路服務遭未經授權的存取**				
A.11.4.1	網路服務的使用政策	Y	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.11.4.2	外部連線的使用者鑑別	Y	外單位資訊存取管理程序書	為確保外部連線使用者皆經適當之授權，應實施相關規範。
A.11.4.3	網路設備識別	Y	網路安全管理程序書	為確保人員由特定地點或設備連結網路時之安全，應實施認證機制。
A.11.4.4	遠端診斷埠與組態埠保護	Y	外單位資訊存取管理程序書	為確保遠端診斷埠使用之安全，應對其存取安全地控管。

A.11.4.5	網路區隔	Y	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.11.4.6	網路連線控制	Y	網路安全管理程序書	為確保網路服務之安全性，應對連線進行限制。
A.11.4.7	網路選路控制	Y	網路安全管理程序書	為確保電腦連線之安全，應透過路由設備進行管制。
A.11.5 **作業系統存取控制** **控制目標：防止作業系統遭未經授權的存取**				
A.11.5.1	保全登入程序	Y	應用系統管理程序書	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.11.5.2	使用者識別與鑑別	Y	應用系統管理程序書 帳號密碼及存取控制管理程序書	為確保登入作業系統存取之安全，須使用帳號密碼進行使用者身份識別。
A.11.5.3	通行碼管理系統	Y	應用系統管理程序書 帳號密碼及存取控制管理程序書	為確保資訊系統均符合密碼管理要求，應建立密碼管理機制。
A.11.5.4	系統公用程式的使用	Y	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.11.5.5	會談期逾時	Y	帳號密碼及存取控制管理程序書	為確保與系統連線時之安全應於一段時間無作業回應後採取連線中止限制。
A.11.5.6	連線時間的限制	Y	帳號密碼及存取控制管理程序書	為確保與系統連線時之安全，應採取連線時間限制。

A.11.6 **應用系統與資訊存取控制** **控制目標：防止應用系統中的資訊遭未經授權的存取**				
A.11.6.1	資訊存取限制	Y	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.11.6.2	敏感性系統的隔離	Y	網路安全管理程序書	為確保各項業務系統運作之安全，應規定僅在特定的電腦上執行。
A.11.7 **行動計算與遠距工作** **控制目標：確保使用行動計算與遠距工作設施時之資訊安全**				
A.11.7.1	行動計算與通信	Y	可攜式設備及儲存媒體管理程序書	為確保系統使用行動電腦作業之安全，應加以控管。
A.11.7.2	遠距工作	Y	外單位資訊存取管理程序書	為確保本校圖書資訊館委外廠商以遠端方式存取本校資訊設備之安全性，應予以控管。
A.12 **資訊系統獲取、開發及維護**				
A.12.1 **資訊系統的安全要求** **控制目標：確保安全是整體資訊系統的一部份**				
A.12.1.1	安全要求分析與規格	Y	系統發展與維護管理程序書	為降低資訊系統之風險，應在資訊系統開發階段確認安全的要求。

A.12.2 **應用系統的正確處理** **控制目標：防止應用系統中資訊的錯誤、遺失、未經授權的修改或誤用**				
A.12.2.1	輸入資料確認	Y	系統發展與維護管理程序書	為確保各系統之資料輸入正確，輸入應用系統的資料應予確認。
A.12.2.2	內部處理的控制措施	Y	系統發展與維護管理程序書	為確保資料不會因處理錯誤而遭到破壞，應有確認檢查機制。
A.12.2.3	訊息完整性	Y	系統發展與維護管理程序書	為確保傳送訊息內容不受未經授權而揭露，應實行資料完整性之控制。
A.12.2.4	輸出資料確認	Y	系統發展與維護管理程序書	為確保所儲存資訊處理作業正確，應用系統的資料輸出經過確認。
A.12.3 **密碼控制措施** **控制目標：藉由密碼方式以保護資訊的機密性、鑑別性或完整性**				
A.12.3.1	使用密碼控制措施的政策	Y	系統發展與維護管理程序書	為確保加密技術之使用符合安全要求，應制定使用規範。
A.12.3.2	金鑰管理	N	未使用金鑰，不適用	資料交換未有使用金鑰之需求。
A.12.4 **系統檔案的安全** **控制目標：確保系統檔案的安全**				
A.12.4.1	作業軟體的控制	Y	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.12.4.2	系統測試資料的保護	Y	系統發展與維護管理程序書	為確保系統使用之測試資料安全，應對測試資料使用實施適切的管控。
A.12.4.3	程式源碼的存取控制	Y	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.12.5 **開發與支援過程的安全** **控制目標：維持應用系統軟體與資訊的安全**				
A.12.5.1	變更控制程序	Y	系統發展與維護管理程序書	為降低不當變更造成資訊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.12.5.2	作業系統變更後的應用系統技術審查	Y	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.12.5.3	套裝軟體變更的限制	Y	系統發展與維護管理程序書 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.12.5.4	資訊洩漏	Y	系統發展與維護管理程序書	為避免資訊因隱密通道而外流，應採取適當之控制措施。
A.12.5.5	委外的軟體開發	Y	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.12.6 **技術脆弱性管理** **控制目標：降低因利用已公佈的技術脆弱性所導致的風險**				
A.12.6.1	技術脆弱性控制	Y	弱點管理程序書	為確保資訊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.13 **資訊安全事故管理**				
A.13.1 **通報資訊安全事件與弱點** **控制目標：確保與資訊系統相關的資訊安全事件與弱點，被以能採取及時矯正措施的方式傳達**				
A.13.1.1	通報資訊安全事件	Y	資訊安全事件管理程序書 資訊安全事件通報及危機處理管理程序書	為確保資訊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.13.1.2	通報安全弱點	Y	資訊安全事件管理程序書 資訊安全事件通報及危機處理管理程序書	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.13.2 **資訊安全事故與改進的管理** **控制目標：確保實施一致與有效的方法管理資訊安全事故**				
A.13.2.1	責任與程序	Y	資訊安全事件管理程序書 資訊安全事件通報及危機處理管理程序書	為降低影響資訊安全的事件造成之影響，應建立適當途徑通報。
A.13.2.2	從資訊安全事故中學習	Y	資訊安全事件管理程序書 資訊安全事件通報及危機處理管理程序書	為降低資訊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.13.2.3	證據的收集	Y	資訊安全事件管理程序書 資訊安全事件通報及危機處理管理程序書	為確保事件發生時能有時有足夠之證據提起訴訟，應制定證據保存之規定。
A.14				

營運持續管理				
A.14.1 **營運持續管理的資訊安全層面** **控制目標：為對抗營運活動中斷，保護重要營運過程不受重大資訊系統失效或災害的影響，並確保及時再續（resumption）**				
A.14.1.1	資訊安全納入營運持續管理過程	Y	業務持續管理程序書	為確保各資訊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。
A.14.1.2	營運持續與風險評鑑	Y	業務持續管理程序書	為能識別營運過程可能發生之事件及將資源有效分配，應進行風險評鑑。
A.14.1.3	發展與實作包括資訊安全的持續計畫	Y	業務持續管理程序書 資訊安全風險管理程序書	為確保重要系統營運中斷能在一定時間內恢復營運，應發展營運持續計畫。
A.14.1.4	營運持續計劃框架	Y	業務持續管理程序書	為確保建立有效之營運持續計畫，應清楚說明起動的條件以及人員權責，並適當修正。
A.14.1.5	營運持續計畫的測試、維護及重新評鑑	Y	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.15 **遵循性**				
A.15.1 **遵循適法性要求** **控制目標：避免違反任何法律、法令、法規或契約義務，以及任何安全要求**				
A.15.1.1	識別適用之法條	Y	人力資源安全管理程序書	為避免違反相關法令法規，應鑑別出法令法規。

A.15.1.2	智慧財產權	Y	軟體使用管理程序書	為確保人員遵守智慧財產法令法規之要求，應制定適當之管制程序。
A.15.1.3	組織紀錄的保護	Y	文件與資料管理程序書	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.15.1.4	個人資訊的資料保護與隱私	Y	系統發展與維護管理程序書	為確保個人資料收集、處理皆依相關法令規定執行，應制定相關規範。
A.15.1.5	防止資訊處理設施的誤用	Y	資訊設備維護與管理程序書 應用系統管理程序書	為確保本校圖書資訊館資訊處理設施的行為皆經授權許可，對各系統之使用及運作應制定相關監控及授權規定。
A.15.1.6	密碼控制措施的法規	N	無此法令、法規要求，故不適用。	加密控制措施的存取或使用行為應遵守相關協議、法律或法規。
A.15.2 **安全政策與標準的遵循性以及技術遵循性** **控制目標：確保系統遵循遵循組織的安全政策與標準**				
A.15.2.1	安全政策與標準的遵循性	Y	人力資源安全管理程序書	為避免違反相關法令法規，應鑑別出法令法規。
A.15.2.2	技術遵循性查核	Y	軟體使用管理程序書	為確保人員遵守智慧財產法令法規之要求，應制定適當之管制程序。
A.15.3 **資訊系統稽核考量** **控制目標：使資訊系統稽核過程的有效性最大化，並使其產生或受到之干擾降至最低**				

A.15.3.1	資訊系統稽核控制	Y	資訊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.15.3.2	資訊系統稽核工具的保護	Y	資訊安全稽核管理程序書	為避免系統稽核工具遭誤用，稽核工具之使用及存取應有相關規範。