名稱	**適用性聲明書**	安全等級	一般
編號	ISMS-1-002	版次	3.0

1 驗證範圍

文藻外語大學(高雄市三民區民族一路 900 號)之學籍系統開發、操作與維護與電子郵件系統維護，以及相關之資教中心機房、網路基礎設施管理作業。

2 適用聲明

條文編號	ISO27001 控制要項	是否適用	對應文件	適用與不適用之說明
A.5 組織控制措施				
A.5.1	資訊安全政策 Policies for information security	Y	資訊安全管理政策 管理審查程序	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。 並維持「資訊安全政策」適用性及正確性，須定期於「管理審查會議」中進行檢討修訂。
A.5.2	資訊安全角色和責任 Information security roles and responsibilities	Y	資訊安全管理程序	為清楚顯示管理階層對資訊安全之責任，特成立資訊安全工作小組並制定相關程序以利執行。
A.5.3	職務區隔 Segregation of duties	Y	人員安全管理程序 業務持續運作管理程序	為維持資訊安全管理系統於本單位與跨單位運作正常，相互衝突的職務與責任領域加以區隔，以降低組織資產遭未經授權或非故意的修改或誤用之機會。
A.5.4	管理階層責任 Management responsibilities	Y	資訊安全管理程序 管理審查程序	為確保管理階層要求員工及供應商，依照組織既定政策與程序實施資訊安全事宜。

條文編號	ISO27001 控制要項	是否適用	對應文件	適用與不適用之說明
A.5.5	與權責機關聯繫 Contact with authorities	Y	資訊安全管理程序 業務持續運作管理程序	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.5.6	與特殊利害關係者的聯繫 Contact with special interestgroups	Y	網路管理程序 資訊系統管理程序 接收資安組織如 CERT-CC、ICST 之資安訊息 與負責資安之政府機關如研考會保持合作 與資安廠商如 Avira(小紅傘)等保持合作	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.5.7	威脅情資 Threat intelligence	Y	資訊安全管理程序	為蒐集和分析與資訊安全威脅有關的資訊，以產出威脅情資。
A.5.8	專案管理中的資訊安全 Information security in project management	Y	資訊系統管理程序 專案執行計畫書大綱規範	為確保委外大型軟硬體專案管理都應依循有效且資訊安全的管理機制，可以如期如質的完成專案。 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.5.9	資訊和其他相關資產的清冊 Inventory of information and other associated assets	Y	資訊資產及風險管理程序 軟硬體資產管理程序	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，並為確保所有資訊資產皆有適當之維護，指派專人負責管理。
A.5.10	資訊和其他相關資產的可被接受使用 Acceptable use of information and other associated assets	Y	資訊資產及風險管理程序 軟硬體資產管理程序 個人終端設備管理辦法	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，並為確保各資訊資產皆有分級原則以區別資訊之

條文編號	ISO27001 控制要項	是否適用	對應文件	適用與不適用之說明
				機密等級 。
A.5.11	資產返還 Return of assets	Y	資訊資產及風險管理程序 軟硬體資產管理程序	為確保所有的員工與外部團體使用者，在其聘僱、契約或協定終止後應立即歸還全部的組織資產。
A.5.12	資訊分類 Classification of information	Y	資料處理管理程序 資訊資產及風險管理程序 軟硬體資產管理程序	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.5.13	資訊標示 Labelling of information	Y		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。
A.5.14	資訊傳輸 Information transfer	Y		為確保與外部機關之資料交換之安全，應制定管控程序，確保與外部機關之資料交換應有適當之協議與管控，以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.5.15	存取控制 Access control	Y	資料處理管理程序 人員安全管理程序	僅提供使用者經特定授權可存取使用的網路與網路服務，確保營運與資訊安全要求，建立、文件化及審查存取控制政策。
A.5.16	身份管理 Identity management	Y	資料處理管理程序 人員安全管理程序	為確保使用者帳號之安全使用與管理，應有正式授權程序。
A.5.17	驗證資訊 Authentication information	Y	資料處理管理程序 人員安全管理程序	建立密碼管理機制，以確保通行碼使用符合要求，使用者應確實遵守

條文編號	ISO27001 控制要項	是否適用	對應文件	適用與不適用之說明
				密碼使用原則，確保在機密授權資訊的使用，使用者必須遵循組織的安全作法。
A.5.18	存取權限 Access rights	Y	資料處理管理程序 人員安全管理程序	為實施一個正式的使用者存取權限配置程序，以對所有系統與服務的全部使用者類型(含人員離調職或專案結束)分配和、調整與撤銷移除存取權限，並定期執行存取權限審查。
A.5.19	供應商關係的資訊安全 Information security in supplier relationships	Y	供應商管理程序 合約	為確保與供應商協議資訊安全要求，以減少供應商對組織資產存取的風險並加以文件化。
A.5.20	在供應商協議中的資訊安全要求 Addressing information security within supplier agreements	Y	供應商管理程序	為確保建立所有相關的資訊安全要求，並與每個可存取、處理、儲存、傳組織資訊或提供 IT 基礎設施組件的供應商達成協議。
A.5.21	管理資通技術(ICT)供應鏈的資訊安全 Managing information security in the information and communication technology (ICT) supply chain	Y	供應商管理程序 合約	為確保與供應商的協議，包含因應有關資訊與通訊技術服務及產品供應鏈之資訊安全風險的要求。
A.5.22	供應商服務的監控、審查和變更管理 Monitoring, review	Y	供應商管理程序	為確保本校定期監視、審查及稽核供應商提供之服務，並於委外供應

條文編號	ISO27001 控制要項	是否適用	對應文件	適用與不適用之說明
	and change management of supplier services			商所提供服務變更時，包含維持與改進現有的資訊安全政策、程序及控制措施均加以管理，並考量所涉及之營運系統與過程的重要性及風險重新評鑑。
A.5.23	使用雲端服務之資訊安全 Information security for use of cloud services	Y	使用雲端服務之安全管理辦法	為確保本校的資訊安全要求，建立獲取、使用、管理和退出雲端服務的流程。
A.5.24	資訊安全事故管理規劃和準備 Information security incident management planning and preparation	Y	資安事件管理程序 矯正與預防管理程序 業務持續運作管理程序書	為降低影響資訊安全的事件造成之影響，建立適當途徑通報。
A.5.25	資訊安全事件的評估和決策 information security events	Y	資安事件管理程序 資訊資產及風險管理程序	為評鑑資訊安全事件，並決定是否歸類為資訊安全事故。
A.5.26	對資訊安全事故的回應 Response to information security incidents	Y	矯正與預防管理程序 業務持續運作管理程序	為確保依據文件化程序對資訊安全事故作回應。
A.5.27	從資訊安全事故中學習 Learning from information security incidents	Y	資安事件管理程序 矯正與預防管理程序 業務持續運作管理程序	為降低資訊安全事件發生之機率及損失，將事件和失敗的類型、數量進行量化與監控。
A.5.28	證據的蒐集 Collection of evidence	Y	資安事件管理程序 矯正與預防管理程序 業務持續運作管理程序 資訊系統管理程序	為確保事件發生時能有時有足夠之證據提起訴訟，制定證據保存之規定。

條文編號	ISO27001 控制要項	是否適用	對應文件	適用與不適用之說明
A.5.29	中斷期間的資訊安全 Information security during disruption	Y	資安事件管理程序 業務持續運作管理程序	為確保各資訊系統安全使其能穩定的運作，達到預期資訊安全績效目標，應對重要系統進行營運持續運作規劃，定期驗證已建立及實施的資訊安全持續之控制措施，以確保在中斷期間，可適切且有效的維持適當的水準，並保留個過程中之文件紀錄。
A.5.30	ICT 為營運持續性做好資通技術(ICT)的準備 ICT readiness for business continuity	Y	供應商管理程序 合約 業務持續運作管理程序	為符合營運持續目標和 ICT 持續性要求來規劃、實施、維護並測試 ICT 準備情形。
A.5.31	法律、法令、法規及契約要求 Legal, statutory, regulatory and contractual requirements	Y	內部稽核管理程序 管理審查程序	為確保對每一個資訊系統與組織，所有相關法律法規、規章與契約要求及組織用以符合此等要求之方法，宜加以明確界定、文件化及維持最新，並使用密碼控制措施，以遵循所有相關的協議、法律及法規。
A.5.32	智慧財產權 Intellectual property rights	Y	資訊系統管理程序 人員安全管理程序 個人終端設備管理辦法	為確保實施適當程序，以確保有關智慧財產權與所使用的專屬軟體產品，可遵循法律、法規及契約的要求。
A.5.33	紀錄之保護 Protection of records	Y	文件及紀錄管理程序 資訊系統管理程序	為確保依據法律、法規、契約及營運要求，保護紀錄免於遺失、毀損、偽造、未授權的存取與發佈。

條文編號	ISO27001 控制要項	是否適用	對應文件	適用與不適用之說明
A.5.34	隱私與個人可識別資訊(PII)的保護 Privacy and protection of personal identifiable information (PII)	Y	資安相關法令規章 資料處理管理程序	為確保遵循相關的適用法令與法規所要求，確保隱私權及個人識別資訊的保護。
A.5.35	資訊安全的獨立審查 Independent review of information security	Y	內部稽核管理程序 管理審查程序	為確保在計畫的間隔內或當發生重大變更時，獨立審查組織資訊安全的管理與實施作法(例如資訊安全的控制措施、政策、過程及程序)
A.5.36	資訊安全政策、規則與標準之遵循性 Compliance with policies, rules and standards for information security	Y	內部稽核管理程序 管理審查程序	遵循組織的資訊安全政策與標準，管理人員採取適當的安全政策、標準及任何其他安全要求，定期審查資訊處理的遵循性與其責任範圍內的程序。
A.5.37	文件化的作業程序 Documented operating procedures	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，製作相關之程序讓需要之使用者皆可取得。
A.6 **人員**控制措施				
A.6.1	篩選 Screening	Y	人員安全管理程序	依照相關法律、法規及倫理，並兼顧營運要求的相稱性、所存取資訊的保密類別及所察覺的風險，對所有聘僱之應徵者的背景予以查核。
A.6.2	僱傭條款與條件 Terms and conditions of employment	Y	人員安全管理程序	為確保與員工和委外供應商的契約協議應明確敘述與組織對資訊安全的責任。

條文編號	ISO27001 控制要項	是否適用	對應文件	適用與不適用之說明
A.6.3	資訊安全認知、教育和培訓 Information security awareness,education and training	Y	人員安全管理程序	為確保組織所有員工和相關的委外供應商，均接受與其工作職務相關，以及定期更新適切的認知教育及訓練。
A.6.4	懲處程序 Disciplinary process	Y	人員安全管理程序	為確保對違反資訊安全的員工所採取的措施，有一個正式且經過溝通之懲處過程。
A.6.5	聘僱終止或變更後的責任 Responsibilities after termination or change of employment	Y	人員安全管理程序	為確保在聘僱的終止或變更生效、傳達予員工或委外供應商，並強制執行之後資訊安全的責任與義務仍然有效。
A.6.6	機密性或保密協議 Confidentiality or non-disclosure agreements	Y	資料處理管理程序 資訊系統管理程序	為確保組織於資訊保護需要之機密性或不揭露協議要求，應加以識別、定期審查並予文件化。
A.6.7	遠距工作 Remote working	Y	網路管理程序 資訊系統管理程序	為確保本校委外廠商以遠端方式存取本校資訊設備與資料之安全性，予以控管。
A.6.8	資訊安全事件通報 Information security event reporting	Y	資安事件管理程序	為確保本校可提供一種機制，供人原可透過適當管道即時通報觀察到或可疑的資訊安全事件。
A.7 **實體**控制措施				
A.7.1	實體安全邊界 Physical security perimeters	Y	實體安全環境管理程序	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。

名稱	**適用性聲明書**	安全等級	一般
編號	ISMS-1-002	版次	3.0

條文編號	ISO27001 控制要項	是否適用	對應文件	適用與不適用之說明
A.7.2	實體進出管制 Physical entry	Y	實體安全環境管理程序	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，並區分收發區及裝卸區。
A.7.3	辦公室、空間與設施的保護 Securing offices, rooms and facilities	Y	實體安全環境管理程序	為確保辦公區域設施之安全，應有適當之管控措施。
A.7.4	實體安全監控 Physical security monitoring	Y	實體安全環境管理程序	為確保持續監視場域，以避免未經授權的實體進出。
A.7.5	對抗實體和環境威脅的保護 Protecting against physical and environmental threats	Y	實體安全環境管理程序	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.7.6	在安全區域內工作 Working in secure areas	Y	實體安全環境管理程序	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.7.7	桌面淨空與螢幕淨空 Clear desk and clear screen	Y	實體安全環境管理程序	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.7.8	設備安置與保護 Equipment siting and protection	Y	實體安全環境管理程序	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.7.9	場域外資產的安全 Security of assets off-premises	Y	實體安全環境管理程序	為防止資訊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.7.10	儲存媒體 Storage mediaon	Y	軟硬體資產管理程序	為確保儲存媒體按本校分類方案與處理要求，於其獲取、使用、運送和處置的整個生命週期中受到管理。

條文編號	ISO27001 控制要項	是否適用	對應文件	適用與不適用之說明
A.7.11	支援的公用設施 Supporting utilities	Y	實體安全環境管理程序	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.7.12	佈纜安全 Cabling security	Y	實體安全環境管理程序	為避免線路遭受破壞或拔除，線路應標示及保護。
A.7.13	設備維護 Equipment maintenance	Y	實體安全環境管理程序 資訊系統管理程序 網路管理程序	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.7.14	設備的汰除或再使用之安全 Secure disposal or reuse of equipment	Y	實體安全環境管理程序 資料處理管理程序 網路管理程序 資訊系統管理程序 個人終端設備管理辦法	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.8 **技術**控制措施				
A.8.1	使用者終端裝置 User end point devices	Y	個人終端設備管理辦法	為保護透過使用者終端裝置儲存、處理或可存取的資訊。
A.8.2	特權存取權限 Privileged access rights	Y	資料處理管理程序 人員安全管理程序	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.8.3	資訊存取限制 Information access restriction	Y	資料處理管理程序 人員安全管理程序	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.8.4	程式源碼的存取 Access to source code	Y	資訊系統管理程序	為確保程式源碼的安全管理，而限制對程式源碼的存取。
A.8.5	安全驗證 Secure authentication	Y	網路管理程序 資訊系統管理程序	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。

條文編號	ISO27001 控制要項	是否適用	對應文件	適用與不適用之說明
A.8.6	容量管理 Capacity management	Y	資訊系統管理程序 網路管理程序	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.8.7	防範惡意程式 Protection against malware	Y	個人終端設備管理辦法	為避免資料或軟體遭受惡意程式之攻擊，加以警示防範或制定必要之回復措施。
A.8.8	技術漏洞管理 Management of technical vulnerabilities	Y	資訊系統管理程序	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，並定期審查資訊系統是否遵循組織的資訊安全政策與標準。
A.8.9	組態管理 Configuration management	Y	資訊安全管理程序 資訊資產及風險管理程序	為確保建立、文件化、實施、監控和審查硬體、軟體、服務和網路的組態，包括安全組態。
A.8.10	資訊刪除 Information deletion	Y	文件及紀錄管理程序 資料處理管理程序	為確保當不再需要時，應刪除儲存於資訊系統、裝置或任何其他儲存媒體中的資訊。
A.8.11	資料遮罩 Data masking	Y	資料處理管理程序	為確保本校的存取控制特定主題政策和其他相關業務要求，同時考慮適用的法律要求使用資料遮罩。
A.8.12	預防資料洩露 Data leakage prevention	Y	資訊系統管理程序 網路管理程序 資料處理管理程序	為確保對系統、網路等處理、儲存、傳輸敏感資訊的設備，應當採取資料洩露防護措施。
A.8.13	資訊備份 Information backup	Y	資訊系統管理程序 網路管理程序 資料處理管理程序	為確保所有重要的資訊或軟體在災難發生時能立即復原，定期執行備份與測試。

條文編號	ISO27001 控制要項	是否適用	對應文件	適用與不適用之說明
A.8.14	資訊處理設施的備援 (複式配置) Redundancy of information pro-cessing facilities	Y	軟硬體資產管理程序 資訊系統管理程序	為確保資訊處理設施應有足夠的複式配置，以符合可用性要求。
A.8.15	日誌存錄 Logging	Y	資訊系統管理程序 網路管理程序 資安事件管理程序	為確保紀錄活動、異常、錯誤和其他相關事件的日誌，應被產生、儲存、保護和分析。
A.8.16	活動監測 Monitoring activities	Y	資訊系統管理程序 網路管理程序 實體安全環境管理程序	為確保監測網路、系統和應用程式的異常行為，並採取適當行動以評估潛在的資訊安全事故。
A.8.17	鐘訊同步 Clock synchronization	Y	實體安全環境管理程序 資訊系統管理程序 網路管理程序	為確保本校或安全網域內所有相關資訊處理系統的時脈，應與單一的參考時間來源同步。
A.8.18	使用特權公用程式 Use of privileged utility programs	Y	資訊系統管理程序	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.8.19	在作業系統上安裝軟體 Installation of software on operational systems	Y	資訊系統管理程序	為確保建立與實施管理使用者之軟體安裝的規則，相關軟體之安裝、設定及維護由系統負責人進行。
A.8.20	網路安全 Networks security	Y	網路管理程序	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.8.21	網路服務安全 Security of network services	Y	網路管理程序	為確保網路服務之安全，應制定網路服務水準及管理要求。

條文編號	ISO27001 控制要項	是否適用	對應文件	適用與不適用之說明
A.8.22	網路區隔 Segregation of networks	Y	網路管理程序	為確保網路之安全性，應採取實體區隔或以防火牆區隔。
A.8.23	網頁過濾 Web filtering	Y	資訊安全管理程序 網路管理程序	為管理對外部網站的存取，以減少接觸惡意內容。
A.8.24	密碼學的使用 Use of cryptography	Y	資訊系統管理程序 網路管理程序 人員安全管理程序	為確保定義並有效使用密碼學的規則，包括密碼學的金鑰管理。
A.8.25	安全之開發生命週期 Secure development life cycle	Y	資訊系統管理程序	為確保建立軟體與系統的開發規則，並適用於組織內的開發。
A.8.26	應用程式安全要求 Application security requirements	Y	資訊安全管理程序 資訊系統管理程序	為確保在開發或獲取應用程式時，應識別、明訂並核准資訊安全要求。
A.8.27	安全系統架構與工程原則 (設計原理) Secure system architecture and engineering principles	Y	資訊系統管理程序	為確保建立安全系統工程的原則並予維護及文件化，且適用資訊系統規劃建置之生命周期中各作業。
A.8.28	安全編碼 Secure coding	Y	資訊系統管理程序 應用系統安全編碼管理辦法	為確保軟體開發採用安全編碼原則。
A.8.29	開發與驗收的安全測試 Security testing in development and acceptance	Y	資訊系統管理程序	為確保於開發生命週期中定義並實施安全測試流程。
A.8.30	委外開發 Outsourced development	Y	資訊系統管理程序	為確保軟體委外開發之安全，制定相關管理及監視與監督機制。

條文編號	ISO27001 控制要項	是否適用	對應文件	適用與不適用之說明
A.8.31	開發、測試和正式環境區隔 Separation of development, test and production environments	Y	資訊系統管理程序	為確保軟體開發時能區隔並保護開發、測試和正式環境。
A,8.32	變更管理 Change management	Y	資訊系統管理程序 網路管理程序	為確保資訊處理設施和資訊系統的變更應遵循變更管理程序，降低不當變更造成資訊系統毀損的情形降到最低，對變更的執行採取適當的控制措施。
A.8.33	測試資訊 Test information	Y	資訊系統管理程序 資料處理管理程序	為確保慎選、保護及管制測試資料。
A.8.34	於稽核測試期間對資訊系統保護 Protection of information systems during audit testing	Y	內部稽核管理程序	為確保稽核測試與其他涉及評鑑運作中系統的保證活動，應對測試人員和適當的管理人員之間進行規劃並同意。