壹、 組織全景與宗旨

國立中正大學（以下簡稱本校）以「積極創新，修德澤人」為校訓，積極是一種理念，一種心態，也是一種實際作為。凡事從正面想，從光明面立志向，再遵循適當途徑鍥而不捨的完成理想，便是積極的表現。創新是大學研究應該發揮的功能。追求真理，發現或發明新事物，都是創新的表現。修德包括接受傳統美德，遵守現代文化規範，並具備前瞻價值觀念。

積極導致奮發有成，創新導致動態進步，修德導致品德高尚—而這一切不全為個人，而是為了人類社會的和諧、幸福與進步。本校校訓最後的澤人即寓有此意。

貳、 關注方的期望與需求

學生、民眾、政府機關、高階主管、本校同仁、產學合作對象、委外廠商，均期望本校提供完整持續的資通服務，並依循法令法規妥善保護各項資通資料，以提供更安全效率的資通服務內容。

參、 實施範圍

一、 本校資通安全管理系統（ISMS）實施範圍為全校；驗證範圍如下：

單位名稱	管理系統建置範圍
教務處教學組 資訊處管理資訊組	學籍系統
資訊處技術發展組	單一登入系統
資訊處資源管理組	大量寄送電子郵件個資稽核系統 校園網路服務及綠色機房維運

二、 本校建置實施範圍相關邊界：主要為實施範圍之系統所在機房的實體邊界，僅包含建置單位所管轄之設備及系統，或其相關之系統流程。相關之傳輸方式均採 SSL、VPN 及各項資通安全防護機制，以確保本校各級單位資通作業適用國際標準之規範。

適用性聲明書					
文件編號	ISMS-215-02	機密等級	內部	版次	4.0

ISO/CNS 27001:2013 要求	適用性	對應文件	理由及補充說明（註）
本文			
4.組織全景			
4.1.瞭解組織與其全景	適用	ISMS-215	1、3資通安全管理法施行細則
4.2.瞭解事件相關團體之需求與期望	適用	ISMS-215	1、3資通安全管理法施行細則
4.3.決定資訊安全管理系統之範圍	適用	ISMS-215	1、3資通安全管理法施行細則
4.4. 資訊安全管理系統	適用	ISMS-215	1、3資通安全管理法施行細則
5.統御力			
5.1.領導與承諾	適用	ISMS-101	1、3資通安全管理法施行細則
5.2.政策	適用	ISMS-101	1、3資通安全管理法施行細則
5.3.組織角色、職責與授權	適用	ISMS-201	1、3資通安全管理法施行細則
6.規劃			
6.1.闡明風險與機會之行動	適用	ISMS-204	1、3資通安全管理法施行細則
6.2.資訊安全目標及其達成計畫	適用	ISMS-215	1、3資通安全管理法施行細則
7.支援			
7.1.資源	適用	ISMS-215	1、3資通安全管理法施行細則
7.2.資格	適用	ISMS-215	1、3資通安全管理法施行細則
7.3.認知	適用	ISMS-215	1、3資通安全管理法施行細則
7.4.溝通	適用	ISMS-215	1、3資通安全管理法施行細則
7.5.文件化資訊	適用	ISMS-202	1
8.運作			
8.1.運作之規劃與控制	適用	ISMS-204	1
8.2.資訊安全風險評鑑	適用	ISMS-204	1、3資通安全管理法施行細則

ISO/CNS 27001:2013 要求	適用性	對應文件	理由及補充說明（註）
8.3.資訊安全風險處理	適用	ISMS-204	1、3資通安全管理法施行細則
9.績效評估			
9.1.監督、測量、分析與評估	適用	ISMS-215	1、3資通安全管理法施行細則
9.2.內部稽核	適用	ISMS-213	1、3資通安全管理法施行細則
9.3.管理審查	適用	ISMS-201	1、3資通安全管理法施行細則
10.改善			
10.1不適用項目與矯正措施	適用	ISMS-214	1、3資通安全管理法施行細則
10.2持續改進	適用	ISMS-214	1、3資通安全管理法施行細則
Annex A. Control objectives and controls			
A.5 Information security policies			
A.5.1 Management direction for information security			
A.5.1.1 資訊安全政策	適用	ISMS-101	1,5
A.5.1.2 資訊安全政策之審查	適用	ISMS-101	1,5管理審查
A.6 Organization of information security			
A.6.1 Internal organization			
A.6.1.1 資訊安全之角色及責任	適用	ISMS-201	1,3資通安全管理法施行細則、資通安全責任等級分級辦法
A.6.1.2 職務區隔	適用	ISMS-201	1,5
A.6.1.3 與權責機關之聯繫	適用	ISMS-201	1,3資通安全事件通報及應變辦法、5 ISMS-212-02_資通安全緊急聯絡人清冊
A.6.1.4 與特殊關注方之聯繫	適用	ISMS-201	1,3資通安全事件通報及應變辦法、5 ISMS-212-02_資通安全緊急聯絡人清冊
A.6.1.5 專案管理的資訊安全	適用	ISMS-209、ISMS-110	1,5
A.6.2 Mobile devices and teleworking			

ISO/CNS 27001:2013 要求	適用性	對應文件	理由及補充說明（註）
A.6.2.1 行動裝置政策	適用	ISMS-207	1,5
A.6.2.2 遠距工作	適用	ISMS-207	1,3資通安全責任等級分級辦法附表十
A.7 Human resource security			
A.7.1 Prior to employment			
A.7.1.1 篩選	適用	ISMS-205	1,5
A.7.1.2 聘僱條款與條件	適用	ISMS-205	1,3資通安全責任等級分級辦法附表六
A.7.2 During employment			
A.7.2.1 管理階層責任	適用	ISMS-101、ISMS-205	1、3資通安全管理法施行細則
A.7.2.2 資訊安全認知、教育及訓練	適用	ISMS-205	1、3資通安全責任等級分級辦法附表六
A.7.2.3 懲處過程	適用	ISMS-205	1、3公務機關所屬人員資通安全事項獎懲辦法
A.7.3 Termination and change of employment			
A.7.3.1 終止或變更聘僱責任	適用	ISMS-205	1、3教師法、公務員服務法、勞動基準法、國立大學校務基金進用教學人員研究人員及工作人員實施原則、5離職程序
A.8 Asset management			
A.8.1 Responsibility for assets			
A.8.1.1 資產清冊	適用	ISMS-203	1、5資產清冊
A.8.1.2 資產的擁有權	適用	ISMS-203	1、5資產清冊
A.8.1.3 資產之可被接受的使用	適用	ISMS-203	1、3擴大盤點所使用或採購之大陸廠牌資通訊產品原則
A.8.1.4 資產的歸還	適用	ISMS-203	1、5
A.8.2 Information classification			
A.8.2.1 資訊分類	適用	ISMS-203	1、5
A.8.2.2 資訊標示	適用	ISMS-203	1、5
A.8.2.3 資產處置	適用	ISMS-203	1、5
A.8.3 Media handling			

ISO/CNS 27001:2013 要求	適用性	對應文件	理由及補充說明（註）
A.8.3.1 可移除式媒體的管理	適用	ISMS-203	1、5
A.8.3.2 媒體的汰除	適用	ISMS-203	1、5
A.8.3.3 實體媒體傳輸	適用	ISMS-203	1、5專人遞送
A.9 Access control			
A.9.1 Business requirements of access control			
A.9.1.1 存取控制政策	適用	ISMS-208	1、5
A.9.1.2 存取網路與網路服務	適用	ISMS-208	1、3資通安全責任等級分級辦法附表十
A.9.2 User access management			
A.9.2.1 使用者的註冊與註銷	適用	ISMS-208	1、3資通安全責任等級分級辦法附表十
A.9.2.2 使用者存取配置	適用	ISMS-208	1、3資通安全責任等級分級辦法附表十
A.9.2.3 特許權限的管理	適用	ISMS-208	1、3資通安全責任等級分級辦法附表十
A.9.2.4 使用者私密認證資訊的管理	適用	ISMS-208	1、5
A.9.2.5 使用者存取權限的審查	適用	ISMS-208	1、3資通安全責任等級分級辦法附表十
A.9.2.6 存取權限的移除或調整	適用	ISMS-208	1、3資通安全責任等級分級辦法附表十
A.9.3 User responsibilities			
A.9.3.1 私密認證資訊的使用	適用	ISMS-208	1、5
A.9.4 System and application access control			
A.9.4.1 資訊存取限制	適用	ISMS-208	1、5
A.9.4.2 保全登入程序	適用	ISMS-208	1、3資通安全責任等級分級辦法附表十
A.9.4.3 通行碼管理系統	適用	ISMS-208	1、3資通安全責任等級分級辦法附表十
A.9.4.4 特權工具程式的使用	適用	ISMS-208	1、5
A.9.4.5 程式源碼的存取控制	適用	ISMS-208	1、3資通安全責任等級分級辦法附表十
A.10 Cryptography			
A.10.1 Cryptographic controls			
A.10.1.1 使用密碼控制措施的政策	適用	ISMS-208	1、5帳號密碼驗證
A.10.1.2 金鑰管理	適用	ISMS-208	1、5
A.11 Physical and environmental security			

ISO/CNS 27001:2013 要求	適用性	對應文件	理由及補充說明（註）
A.11.1 Secure areas			
A.11.1.1 實體安全周界	適用	ISMS-206	1、5機房
A.11.1.2 實體進入控制措施	適用	ISMS-206	1、5
A.11.1.3 保全辦公室、房間及設施	適用	ISMS-206	1、5
A.11.1.4 對外部與環境威脅的保護	適用	ISMS-206	1、5UPS、發電機、空調、消防及機房門禁
A.11.1.5 在安全區域內工作	適用	ISMS-206	1、5
A.11.1.6 收發及裝卸區	適用	ISMS-206	1、5物品出入管制
A.11.2 Equipment			
A.11.2.1 設備安置與保護	適用	ISMS-206	1、5機房
A.11.2.2 支援的公用設施	適用	ISMS-206	1、5機房
A.11.2.3 佈纜的安全	適用	ISMS-206	1、5機房
A.11.2.4 設備維護	適用	ISMS-206	1、5維護契(合)約
A.11.2.5 資產的攜出	適用	ISMS-206	1、5機房
A.11.2.6 場所外設備及資產的安全	適用	ISMS-206	1、5
A.11.2.7 設備的安全汰除或再使用	適用	ISMS-206	1、5
A.11.2.8 無人看管的使用者設備	適用	ISMS-206	1、5適用範圍內之設備均已指定保管人員
A.11.2.9 桌面淨空與螢幕淨空政策	適用	ISMS-206	1、5
A.12 Operations security			
A.12.1 Operational procedures and responsibilities			
A.12.1.1 文件化作業程序	適用	ISMS-202	1、5內部網站公告、相關操作文件
A.12.1.2 變更管理	適用	ISMS-207	1、5
A.12.1.3 容量管理	適用	ISMS-207	1、5執行紀錄(如日常檢查)
A.12.1.4 開發、測試及運作環境的分隔	適用	ISMS-209	1、3資通安全責任等級分級辦法附表十
A.12.2 Protection from malware			
A.12.2.1 對抗惡意程式的控制措施	適用	ISMS-207	1、3資通安全責任等級分級辦法附表十
A.12.3 Backup			
A.12.3.1 資訊備份	適用	ISMS-207	1、5
A.12.4 Logging and monitoring			
A.12.4.1 事件存錄	適用	ISMS-207	1、3資通安全責任等級分級辦法附表十

ISO/CNS 27001:2013 要求	適用性	對應文件	理由及補充說明（註）
A.12.4.2 日誌資訊的保護	適用	ISMS-207	1、5稽核監控系統與事件紀錄管理
A.12.4.3 管理者與操作者日誌	適用	ISMS-207	1、3資通安全責任等級分級辦法附表十
A.12.4.4 鐘訊同步	適用	ISMS-207	1、5
A.12.5 Control of operational software			
A.12.5.1 作業中系統的軟體安裝	適用	ISMS-207	1、5作業系統及套裝軟體變更規定
A.12.6 Technical vulnerability management			
A.12.6.1 技術脆弱性的管理	適用	ISMS-207	1、3資通安全責任等級分級辦法附表六
A.12.6.2 軟體安裝的限制	適用	ISMS-207	1、5
A.12.7 Information systems audit considerations			
A.12.7.1 資訊系統稽核控制	適用	ISMS-207	1、3資通安全責任等級分級辦法附表十
A.13 Communications security			
A.13.1 Network security management			
A.13.1.1 網路控制措施	適用	ISMS-207	1、3資通安全責任等級分級辦法附表十
A.13.1.2 網路服務的安全	適用	ISMS-207	1、5
A.13.1.3 網路區隔	適用	ISMS-207	1、3資通安全責任等級分級辦法附表十
A.13.2 Information transfer			
A.13.2.1 資訊傳輸政策與程序	適用	ISMS-207	1、5
A.13.2.2 資訊傳輸協議	適用	ISMS-207	1、5
A.13.2.3 電子傳訊	適用	ISMS-207	1、3資通安全責任等級分級辦法附表十
A.13.2.4 機密性或不可揭露的協議	適用	ISMS-210	1、5保密切結書
A.14 System acquisition, development and maintenance			
A.14.1 Security requirements of information systems			
A.14.1.1 資訊安全要求分析與規格	適用	ISMS-209	1、3資通安全責任等級分級辦法附表六
A.14.1.2 公眾網路的應用服務安全	適用	ISMS-209	1、5
A.14.1.3 保護應用服務交易	適用	ISMS-209	1、5
A.14.2 Security in development and support processes			
A.14.2.1 安全發展政策	適用	ISMS-209	1、5

ISO/CNS 27001:2013 要求	適用性	對應文件	理由及補充說明（註）
A.14.2.2 系統變更控制程序	適用	ISMS-209	1、5
A.14.2.3 作業平台變更後的應用系統技術審查	適用	ISMS-209	1、3資通安全管理法施行細則
A.14.2.4 套裝軟體變更的限制	適用	ISMS-207	1、5
A.14.2.5 安全系統工程原則	適用	ISMS-209	1、3資通安全責任等級分級辦法附表十
A.14.2.6 安全開發環境	適用	ISMS-209	1、3資通安全責任等級分級辦法附表十
A.14.2.7 委外開發	適用	ISMS-210	1、5
A.14.2.8 系統安全測試	適用	ISMS-209	1、3資通安全責任等級分級辦法附表十
A.14.2.9 系統驗收測試	適用	ISMS-209	1、3資通安全責任等級分級辦法附表十
A.14.3 Test data			
A.14.3.1 測試資料的保護	適用	ISMS-209	1、5
A.15 Supplier relationships			
A.15.1 Information security in supplier relationships			
A.15.1.1 供應商關係的資訊安全政策	適用	ISMS-210	1、5
A.15.1.2 供應商協議中之安全說明	適用	ISMS-210	1、3資通安全責任等級分級辦法
A.15.1.3 資訊與通信技術的供應鏈	適用	ISMS-210	1、5
A.15.2 Supplier service delivery management			
A.15.2.1 供應商服務的監視與審查	適用	ISMS-210	1、3資通安全責任等級分級辦法
A.15.2.2 供應商服務變更的管理	適用	ISMS-210	1、5維護契(合)約
A.16 Information security incident management			
A.16.1 Management of information security incidents and improvements			
A.16.1.1 責任與程序	適用	ISMS-211	1、3資通安全事件通報及應變辦法
A.16.1.2 通報資訊安全事件	適用	ISMS-211	1、3資通安全事件通報及應變辦法
A.16.1.3 通報資訊安全弱點	適用	ISMS-211	1、3資通安全情資分享辦法
A.16.1.4 資訊安全事件的評估與決策	適用	ISMS-211	1、3資通安全事件通報及應變辦法

ISO/CNS 27001:2013 要求	適用性	對應文件	理由及補充說明（註）
A.16.1.5 資訊安全事故的因應	適用	ISMS-211	1、3資通安全事件通報及應變辦法
A.16.1.6 從資訊安全事故中學習	適用	ISMS-211	1、3資通安全情資分享辦法
A.16.1.7 證據的收集	適用	ISMS-211	1、3資通安全事件通報及應變辦法
A.17 Information security aspects of business continuity management			
A.17.1 Information security continuity			
A.17.1.1 規劃資訊安全持續	適用	ISMS-212	1、3資通安全責任等級分級辦法附表六
A.17.1.2 實作資訊安全持續	適用	ISMS-212	1、3資通安全責任等級分級辦法附表六
A.17.1.3 驗證，審查和評估資訊安全持續	適用	ISMS-212	1、5
A.17.2 Redundancies			
A.17.2.1 資訊處理設施的可用性	適用	ISMS-207	1、5
A.18 Compliance			
A.18.1 Compliance with legal and contractual requirements			
A.18.1.1 識別適用之法條與契約要求	適用	ISMS-215	1、5文件依據、外來文件管制表
A.18.1.2 智慧財產權	適用	ISMS-215	1、3如著作權法
A.18.1.3 紀錄的保護	適用	ISMS-207	1、3資通安全責任等級分級辦法附表十
A.18.1.4 隱私及個人身分訊息的保護	適用	ISMS-207	1、3個人資料保護法
A.18.1.5 密碼控制措施的規定	適用	ISMS-208	1、3
A.18.2 Information security reviews			
A.18.2.1 資訊安全的獨立審查	適用	ISMS-201	1、5管理審查
A.18.2.2 安全政策與標準的遵循性	適用	ISMS-101	1、5管理審查、定期管理審查、查核評量資訊安全管理系統目標達成性及風險管理控制措施的有效性
A.18.2.3 技術遵循性審查	適用	ISMS-207	1、3資通安全責任等級分級辦法附表六

備註：

編號	適用理由說明	不適用理由說明
1	標準要求	驗證範圍內不提供此服務，不使用此資源、方法、作法
2	客戶或合約要求	驗證範圍內沒有與客戶或合約相關之使用協議
3	法令法規要求	國內法令法規無相關使用限制
4	風險評鑑結果	風險評鑑結果
5	管理階層之營運要求	

肆、 其他

本聲明書如有未盡事宜，得隨時補充或修改之。