雲林縣麥寮鄉公所

資訊安全管理系統

適用性聲明

文件編號： YLML-01-003

版　　次： 1.0

文件日期： 110 年 09 月 15 日

機密等級： 普通

文件制/修訂履歷

制/修訂 版次	制/修訂 日期	制/修訂 說明	作 者	備 註
V1.0	110.09.15	初版發行	ISMS 執行小組	

適用範圍：

本所核心系統與資訊機房維運與管理活動所涉及辦公環境。

全景與宗旨：

確保資訊系統安全，建立安全及可信賴之資通環境，提升服務品質，保障民眾權益。

關注方需求：

實現本所政策方向、合宜制度、推動施政計畫、提升相關服務。

實施範圍：

本所實施 ISO 27001 / CNS 27001 資訊安全管理系統之範圍為本所網路服務、辦公室資訊環境及其電腦機房安全維護管理。

相關邊界：

本所範圍相關之邊界主要為民眾及本所其他辦公室之介面，機敏性資料的交換均須採取電子資料加密傳輸或實體資料由專人傳送管制之機制。

控制領域/目標/條款		適用性	對應之文件名稱	適用/不適用原因
A.5 資訊安全政策				
A.5.1 資訊安全之管理指導方				
A.5.1.1	資訊安全政策	適用	YLML-01-001 資訊安全政策	1、5
A.5.1.2	資訊安全政策之審查	適用	YLML-01-001 資訊安全政策 YLML-01-002 資訊安全手冊 YLML-01-004 資訊安全管理小組設置要點	1、5 管理審查
A.6 資訊安全之組織				
A.6.1 內部組織				
A.6.1.1	資訊安全之角色及責任	適用	YLML-02-006 資訊安全組織管理程序	1、5 資訊安全組織
A.6.1.2	職務區隔	適用	YLML-02-008 人員安全管理程序 YLML-02-010 通訊與操作管理程序 YLML-02-011 存取控制管理程序 YLML-02-012 資訊系統開發與維護管理程序 YLML-02-016 網路安全管理程序	1、5
A.6.1.3	與權責機關之連繫	適用	YLML-02-013 資通安全事件通報及應變管理程序	1、5 資訊安全緊急事件聯絡人員表
A.6.1.4	與特殊關注方之連繫	適用	YLML-02-013 資通安全事件通報及應變管理程序	1、5 國家資通安全會報(技服中心)
A.6.1.5	專案管理之資訊安全	適用	YLML-01-002 資訊安全手冊	1、5
A.6.2 行動裝置及遠距工作				
A.6.2.1	行動裝置政策	適用	YLML-01-002 資訊安全手冊 YLML-02-010 通訊與操作管理程序	1、5

控制領域/目標/條款		適用性	對應之文件名稱	適用/不適用原因
A.6.2.2	遠距工作	適用	YLML-02-010 通訊與操作管理程序 YLML-02-011 存取控制管理程序 YLML-02-012 資訊系統開發與維護管理程序 YLML-02-016 網路安全管理程序	1、5
A.7 人力資源安全				
A.7.1 聘用前				
A.7.1.1	篩選	適用	YLML-02-008 人員安全管理程序	1、5
A.7.1.2	聘用條款及條件	適用	YLML-02-008 人員安全管理程序	1、5
A.7.2 聘用期間				
A.7.2.1	管理階層責任	適用	YLML-02-008 人員安全管理程序	1、5
A.7.2.2	資訊安全認知、教育及訓練	適用	YLML-02-008 人員安全管理程序	1、5 教育訓練記錄
A.7.2.3	懲處過程	適用	YLML-02-008 人員安全管理程序	1、5
A.7.3 聘用之終止及變更				
A.7.3.1	聘用責任之終止或變更	適用	YLML-02-008 人員安全管理程序	1、5 離職程序
A.8 資產管理				
A.8.1 資產責任				
A.8.1.1	資產清冊	適用	YLML-02-007 資產分類與管理程序	1、5 資產清冊
A.8.1.2	資產擁有權	適用	YLML-02-007 資產分類與管理程序	1、5 資產清冊
A.8.1.3	資產之可被接受使用	適用	YLML-02-007 資產分類與管理程序 YLML-02-010 通訊與操作管理程序 YLML-02-011 存取控制管理程序 YLML-02-016 網路安全管理程序	1、5
A.8.1.4	資產之歸還	適用	YLML-02-007 資產分類與管理程序 YLML-02-008 人員安全管理程序	1、5
A .8.2 資訊分級				
A.8.2.1	資訊之分級	適用	YLML-02-007 資產分類與管理程序	1、5
A.8.2.2	資訊之標示	適用	YLML-02-007 資產分類與管理程序	1、5
A.8.2.3	資產之處置	適用	YLML-02-007 資產分類與管理程序	1、5
A.8.3 媒體處置				
A.8.3.1	可移除式媒體之管理	適用	YLML-02-007 資產分類與管理程	1、5

控制領域/目標/條款		適用性	對應之文件名稱	適用/不適用原因
			序 YLML-02-009 實體與環境安全管理程序 YLML-02-010 通訊與操作管理程序	
A.8.3.2	媒體之汰除	適用	YLML-02-007 資產分類與管理程序	1、5
A.8.3.3	實體媒體傳送	適用	YLML-02-007 資產分類與管理程序	1、5 專人遞送
A.9 存取控制				
A.9.1 存取控制之營運要求事項				
A.9.1.1	存取控制政策	適用	YLML-02-011 存取控制管理程序	1、5
A.9.1.2	對網路及網路服務之存取	適用	YLML-02-011 存取控制管理程序 YLML-02-016 網路安全管理程序	1、5
A .9.2 使用者存取管理				
A.9.2.1	使用者註冊及註銷	適用	YLML-02-008 人員安全管理程序 YLML-02-011 存取控制管理程序	1、5
A.9.2.2	使用者存取權限之配置	適用	YLML-02-011 存取控制管理程序	1、5
A.9.2.3	具特殊存取權限之管理	適用	YLML-02-010 通訊與操作管理程序 YLML-02-011 存取控制管理程序 YLML-02-016 網路安全管理程序 YLML-02-014 營運持續管理程序	1、5
A.9.2.4	使用者之秘密鑑別資訊的管理	適用	YLML-02-011 存取控制管理程序	1、5
A.9.2.5	使用者存取權限之審查	適用	YLML-02-008 人員安全管理程序 YLML-02-011 存取控制管理程序	1、5
A.9.2.6	存取權限之移除或調整	適用	YLML-02-008 人員安全管理程序 YLML-02-011 存取控制管理程序	1、5
A.9.3 使用者責任				
A.9.3.1	秘密鑑別資訊之使用	適用	YLML-02-008 人員安全管理程序 YLML-02-016 網路安全管理程序 YLML-02-011 存取控制管理程序	1、5
A.9 .4 系統及應用存取控制				
A.9.4.1	資訊存取限制	適用	YLML-02-016 網路安全管理程序 YLML-02-011 存取控制管理程序	1、5
A.9.4.2	保全登入程序	適用	YLML-02-016 網路安全管理程序 YLML-02-011 存取控制管理程序	1、5
A.9.4.3	通行碼管理系統	適用	YLML-02-016 網路安全管理程序 YLML-02-011 存取控制管理程序	1、5
A.9.4.4	具特殊權限公用程式之使用	適用	YLML-02-016 網路安全管理程序 YLML-02-011 存取控制管理程序	1、5

控制領域/目標/條款		適用性	對應之文件名稱	適用/不適用原因
A.9.4.5	對程式源碼之存取控制	適用	YLML-02-012 資訊系統開發與維護管理程序	1、5
A.10 密碼學				
A.10.l 密碼式控制措施				
A.10.1.1	使用密碼式控制措施之政策	適用	YLML-02-016 網路安全管理程序 YLML-02-011 存取控制管理程序 YLML-02-012 資訊系統開發與維護管理程序	1、5 帳號密碼驗證
A.10.1.2	金鑰管理	適用	YLML-02-010 通訊與操作管理程序	1
A.11 實體及環境安全				
A.11.1 保全區域				
A.11.1.1	實體安全周界	適用	YLML-01-002 資訊安全手冊 YLML-02-009 實體與環境安全管理程序 YLML-03-001 電腦機房管理作業	1、5 機房
A.11.1.2	實體進入控制措施	適用	YLML-02-009 實體與環境安全管理程序 YLML-03-001 電腦機房管理作業	1、5
A.11.1.3	保全之辦公室、房間及設施	適用	YLML-02-009 實體與環境安全管理程序 YLML-03-001 電腦機房管理作業	1、5
A.11.1.4	防範外部及環境威脅	適用	YLML-02-009 實體與環境安全管理程序 YLML-03-001 電腦機房管理作業	1、5 UPS、發電機、空調、消防及機房
A.11.1.5	於保全區域內工作	適用	YLML-02-009 實體與環境安全管理程序 YLML-03-001 電腦機房管理作業	1、5
A.11.1.6	交付及裝卸區	適用	YLML-03-001 電腦機房管理作業	1、5 物品出入管制
A.11. 2 設備				
A.11.2.1	設備安置及保護	適用	YLML-02-009 實體與環境安全管理程序 YLML-03-001 電腦機房管理作業	1、5 機房
A.11.2.2	支援之公用服務事業	適用	YLML-02-009 實體與環境安全管理程序 YLML-03-001 電腦機房管理作業	1、5 機房
A.11.2.3	佈纜安全	適用	YLML-02-009 實體與環境安全管理程序 YLML-03-001 電腦機房管理作業	1、5 機房
A.11.2.4	設備維護	適用	YLML-02-009 實體與環境安全管理程序	1、5 維護契(合)約

控制領域/目標/條款		適用性	對應之文件名稱	適用/不適用原因
			YLML-03-001 電腦機房管理作業	
A.11.2.5	資產之攜出	適用	YLML-02-009 實體與環境安全管理程序 YLML-03-001 電腦機房管理作業	1、5 機房
A.11.2.6	場所外設備及資產之安全	適用	YLML-02-007 資產分類與管理程序 YLML-02-009 實體與環境安全管理程序 YLML-03-001 電腦機房管理作業	1、5
A.11.2.7	設備汰除或再使用之保全	適用	YLML-02-007 資產分類與管理程序 YLML-02-009 實體與環境安全管理程序 YLML-03-001 電腦機房管理作業	1、5
A.11.2.8	無人看管之使用者設備	適用	YLML-02-007 資產分類與管理程序	1、5 適用範圍內之設備均已指定保管人員
A.11.2.9	桌面淨空及螢幕淨空政策	適用	YLML-01-002 資訊安全手冊 YLML-02-016 網路安全管理程序	1、5
A.12 運作安全				
A.12.1 運作程序及責任				
A.12.1.1	文件化運作程序	適用	YLML-01-002 資訊安全手冊 YLML-02-001 文件與紀錄管理程序	1、5 內部網站公告、相關操作文件
A.12.1.2	變更管理	適用	YLML-02-007 資產分類與管理程序 YLML-02-010 通訊與操作管理程序 YLML-02-011 存取控制管理程序 YLML-02-012 資訊系統開發與維護管理程序 YLML-02-016 網路安全管理程序	1、5
A.12.1.3	容量管理	適用	YLML-02-012 資訊系統開發與維護管理程序	1、5 執行紀錄(如日常檢查)
A.12.1.4	開發、測試及運作環境之區隔	適用	YLML-02-012 資訊系統開發與維護管理程序	1、5
A.12.2 防範惡意軟體				

控制領域/目標/條款		適用性	對應之文件名稱	適用/不適用原因
A.12.2.1	防範惡意軟體之控制措施	適用	YLML-02-010 通訊與操作管理程序 YLML-02-011 存取控制管理程序 YLML-02-012 資訊系統開發與維護管理程序 YLML-02-016 網路安全管理程序	1、5
A.12.3 備份				
A.12.3.1	資訊備份	適用	YLML-02-017 備份與回復管理程序	1、5
A.12.4 存錄及監視				
A.12.4.1	事件存錄	適用	YLML-02-007 資產分類與管理程序 YLML-02-011 存取控制管理程序 YLML-02-016 網路安全管理程序	1、5
A.12.4.2	日誌資訊之保護	適用	YLML-02-007 資產分類與管理程序 YLML-02-011 存取控制管理程序 YLML-02-016 網路安全管理程序	1、5 稽核監控系統與事件紀錄管理
A.12.4.3	管理者及操作者日誌	適用	YLML-02-007 資產分類與管理程序 YLML-02-011 存取控制管理程序 YLML-02-016 網路安全管理程序	1、5 安全性監控
A.12.4.4	鐘訊同步	適用	YLML-02-010 通訊與操作管理程序	1、5
A.12.5 運作中軟體之控制				
A.12.5.1	對運作中系統之軟體安裝	適用	YLML-02-010 通訊與操作管理程序 YLML-02-012 資訊系統開發與維護管理程序 YLML-02-016 網路安全管理程序	1、5 作業系統及套裝軟體變更規定
A.12.6 技術脆弱性管理				
A.12.6.1	技術脆弱性管理	適用	YLML-02-010 通訊與操作管理程序 YLML-02-012 資訊系統開發與維護管理程序	1、5 弱點掃描與修補
A.12.6.2	對軟體安裝之限制	適用	YLML-02-012 資訊系統開發與維護管理程序 YLML-02-016 網路安全管理程序	1、5
A.12.7 資訊系統稽核考量				
A.12.7.1	資訊系統稽核控制措施	適用	YLML-02-002 資訊安全稽核程序 YLML-02-010 通訊與操作管理程序 YLML-02-011 存取控制管理程序	1、5

控制領域/目標/條款		適用性	對應之文件名稱	適用/不適用原因
			YLML-02-016 網路安全管理程序	
A.13 通訊安全				
A.13.1 網路安全管理				
A.13.1.1	網路控制措施	適用	YLML-02-002 資訊安全稽核程序 YLML-02-016 網路安全管理程序	1、5
A.13.1.2	網路服務之安全	適用	YLML-02-002 資訊安全稽核程序 YLML-02-016 網路安全管理程序	1、5
A.13.1.3	網路之區隔	適用	YLML-02-002 資訊安全稽核程序 YLML-02-016 網路安全管理程序	1、5
A.13.2 資訊傳送				
A.13.2.1	資訊傳送政策及程序	適用	YLML-01-002 資訊安全手冊 YLML-02-010 通訊與操作管理程序 YLML-02-011 存取控制管理程序 YLML-02-016 網路安全管理程序	1、5
A.13.2.2	資訊傳送協議	適用	YLML-02-010 通訊與操作管理程序 YLML-02-011 存取控制管理程序 YLML-02-016 網路安全管理程序	1、5
A.13.2.3	電子傳訊	適用	YLML-01-002 資訊安全手冊 YLML-02-010 通訊與操作管理程序 YLML-02-011 存取控制管理程序 YLML-02-016 網路安全管理程序	1、5
A.13.2.4	機密性或保密協議	適用	YLML-02-008 人員安全管理程序 YLML-02-012 資訊系統開發與維護管理程序	1、5 保密切結書
A.14 系統獲取、開發及維護				
A.14.1 資訊系統之安全要求事項				
A.14.1.1	資訊安全要求事項分析及規格	適用	YLML-01-002 資訊安全手冊 YLML-02-012 資訊系統開發與維護管理程序	1、5
A.14.1.2	保全公共網路之應用服務	適用	YLML-01-002 資訊安全手冊 YLML-02-010 通訊與操作管理程序 YLML-02-012 資訊系統開發與維護管理程序 YLML-02-016 網路安全管理程序	1、5
A.14.1.3	保護應用服務交易	不適用		1 範圍內無應用服務交易行為
A.14.2 於開發及支援過程中之安全				
A.14.2.1	保全開發政策	適用	YLML-01-002 資訊安全手冊	1、5

控制領域/目標/條款		適用性	對應之文件名稱	適用/不適用原因
			YLML-02-012 資訊系統開發與維護管理程序	
A.14.2.2	系統變更控制程序	適用	YLML-02-010 通訊與操作管理程序 YLML-02-012 資訊系統開發與維護管理程序 YLML-02-016 網路安全管理程序	1、5
A.14.2.3	運作平台變更後，應用之技術審查	適用	YLML-02-010 通訊與操作管理程序 YLML-02-012 資訊系統開發與維護管理程序	1、5
A.14.2.4	軟體套件變更之限制	適用	YLML-01-002 資訊安全手冊 YLML-02-012 資訊系統開發與維護管理程序 YLML-02-016 網路安全管理程序	1、5
A.14.2.5	保全系統工程原則	適用	YLML-02-012 資訊系統開發與維護管理程序	1、5
A.14.2.6	保全開發環境	適用	YLML-02-012 資訊系統開發與維護管理程序	1、5
A.14.2.7	委外開發	適用	YLML-02-010 通訊與操作管理程序 YLML-02-011 存取控制管理程序 YLML-02-012 資訊系統開發與維護管理程序 YLML-02-016 網路安全管理程序	1、5
A.14.2.8	系統安全測試	適用	YLML-02-012 資訊系統開發與維護管理程序	1、5
A.14.2.9	系統驗收測試	適用	YLML-02-012 資訊系統開發與維護管理程序	1、5 維護契(合)約
A .14.3 測試資料				
A.14.3.1	測試資料之保護	適用	YLML-02-012 資訊系統開發與維護管理程序	1、5
A.15 供應者關係				
A.15.1 供應者關係中之資訊安全				
A.15.1.1	供應者關係之資訊安全政策	適用	YLML-02-008 人員安全管理程序 YLML-02-012 資訊系統開發與維護管理程序	1、5
A.15.1.2	於供應者協議中闡明安全性	適用	YLML-02-008 人員安全管理程序 YLML-02-012 資訊系統開發與維護管理程序	1、5

控制領域/目標/條款		適用性	對應之文件名稱	適用/不適用原因
			YLML-02-011 存取控制管理程序	
A.15.1.3	資訊及通訊技術供應鏈	適用	YLML-02-008 人員安全管理程序 YLML-02-012 資訊系統開發與維護管理程序	1、5
A.15.2 供應者服務交付管理				
A.15.2.1	供應者服務之監視及審查	適用	YLML-02-008 人員安全管理程序 YLML-02-012 資訊系統開發與維護管理程序 YLML-02-011 存取控制管理程序	1、5 維護契(合)約
A.15.2.2	管理供應者服務之變更	適用	YLML-02-008 人員安全管理程序 YLML-02-012 資訊系統開發與維護管理程序	1、5 維護契(合)約
A.16 資訊安全事故管理				
A.16.1 資訊安全事故及改善之管理				
A.16.1.1	責任及程序	適用	YLML-02-006 資訊安全組織管理程序 YLML-02-013 資通安全事件通報及應變管理程序	1、5 資安事件處理及紀錄
A.16.1.2	通報資訊安全事件	適用	YLML-02-013 資通安全事件通報及應變管理程序	1、5
A.16.1.3	通報資訊安全弱點	適用	YLML-02-013 資通安全事件通報及應變管理程序	1、5
A.16.1.4	對資訊安全事件之評鑑及決策	適用	YLML-02-013 資通安全事件通報及應變管理程序	1、5
A.16.1.5	對資訊安全事故之回應	適用	YLML-02-013 資通安全事件通報及應變管理程序	1、5
A.16.1.6	由資訊安全事故中學習	適用	YLML-02-003 矯正措施處理程序 YLML-02-013 資通安全事件通報及應變管理程序	1、5 異常狀況之應變處理紀錄
A.16.1.7	證據之收集	適用	YLML-02-010 通訊與操作管理程序 YLML-02-011 存取控制管理程序 YLML-02-016 網路安全管理程序 YLML-02-013 資通安全事件通報及應變管理程序	1、5 異常狀況之應變處理紀錄
A.17 營運持續管理之資訊安全層面				
A.17.1 資訊安全持續				
A.17.1.1	規劃資訊安全持續	適用	YLML-02-014 營運持續管理程序 YLML-03-002 營運持續計畫	1、5

控制領域/目標/條款		適用性	對應之文件名稱	適用/不適用原因
A.17.1.2	實作資訊安全持續	適用	YLML-02-014 營運持續管理程序 YLML-03-002 營運持續計畫	1、5
A.17.1.3	查證、審查並評估資訊安全持續	適用	YLML-02-014 營運持續管理程序 YLML-03-002 營運持續計畫	1、5
A . 17 . 2 多重備援				
A.17.2.1	資訊處理設施之可用性	適用	YLML-02-014 營運持續管理程序 YLML-03-002 營運持續計畫	1、5
A . 18 遵循性				
A .18.1 對法律及契約要求事項之遵循				
A.18.1.1	適用之法規及契約的要求事項之識別	適用	YLML-02-001 文件與紀錄管理程序 YLML-02-015 法規遵循性管理程序	1、5 文件依據、外來文件管制表
A.18.1.2	智慧財產權	適用	YLML-02-012 資訊系統開發與維護管理程序 YLML-02-015 法規遵循性管理程序	1、3 如著作權法
A.18.1.3	紀錄之保護	適用	YLML-02-001 文件與紀錄管理程序 YLML-02-011 存取控制管理程序 YLML-02-012 資訊系統開發與維護管理程序 YLML-02-016 網路安全管理程序 YLML-03-001 電腦機房管理作業	1、5
A.18.1.4	個人可識別資訊之隱私及保護	適用	YLML-02-001 文件與紀錄管理程序 YLML-02-008 人員安全管理程序 YLML-02-011 存取控制管理程序	1、3 個人資料保護法
A.18.1.5	密碼式控制措施之監管	適用	YLML-02-011 存取控制管理程序	1、3
A .18.2 資訊安全審查				
A.18.2.1	資訊安全之獨立審查	適用	YLML-02-002 資訊安全稽核程序 YLML-02-003 矯正措施處理程序 YLML-02-006 資訊安全組織管理程序	1、5 管理審查
A.18.2.2	安全政策及標準之遵循性	適用	YLML-01-001 資訊安全政策 YLML -01-002 資訊安全手冊 YLML -02-002 資訊安全稽核程序 YLML -02-003 矯正措施處理程序	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

控制領域/目標/條款		適用性	對應之文件名稱	適用/不適用原因
A.18.2.3	技術遵循性審查	適用	YLML -01-002 資訊安全手冊 YLML -02-002 資訊安全稽核程序 YLML -02-010 通訊與操作管理程序 YLML -02-011 存取控制管理程序 YLML -02-016 網路安全管理程序	1、5 如弱點掃描

註	**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	