大林慈濟醫院-普級資通系統防護基準評估表

評估日期:　　/　　/

申請人資料	姓名		單位		連絡電話	
	員工編號		職稱		Email	
軟體資訊	中文名稱					
	英文名稱					

★ 檢核項目

存取控制		
	(1)帳號管理	
項次編號(原始)	1	2
最低系統等級要求	普	普
安全控制措施	建立帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。	已逾期之臨時或緊急帳號應刪除或禁用。
是否符合		
現況說明		
佐證		
矯正作為		
目標日期		
備註說明		

制定日期:2025 年 11 月 28 日
最後修訂日期:2026 年 06 月 15 日

存取控制		
	(1)帳號管理	
項次編號（原始）	3	4
最低系統等級要求	普	普
安全控制措施	資通系統閒置帳號應禁用。	定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。
是否符合		
現況說明		
佐證		
矯正作為		
目標日期		
備註說明		

	(1)最小權限	(2)遠端存取	
項次編號（原始）	9	10	11
最低系統等級要求	普	普	普
安全控制措施	採最小權限原則，僅允 許使用者（或代表使用 者行為之程序）依機關 任務及業務功能，完成 指派任務所需之授權存取。	對於每一種允許之遠端存取類型，均應先取得授權，建立使用限制、組態需求、連線需求及文件化。	使用者之權限檢查作業應於伺服器端完成。
是否符合			
現況說明			
佐證			
矯正作為			
目標日期			
備註說明			

制定日期:2025 年 11 月 28 日
最後修訂日期:2026 年 06 月 15 日

	(3)遠端存取		
項次編號（原始）	12	13	14
最低系統等級要求	普	普	普
安全控制措施	應監控遠端存取機關內部網段或資通系統後臺之連線。	應採用加密機制。	遠端存取之來源應為機關已預先定義及管理之存取控制點。
是否符合			
現況說明			
佐證			
矯正作為			
目標日期			
備註說明			

制定日期:2025 年 11 月 28 日
最後修訂日期:2026 年 06 月 15 日

事件日誌與可歸責性			
	(1)記錄事件		
項次編號（原始）	15	16	17
最低系統等級要求	普	普	普
安全控制措施	訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。	確保資通系統有記錄 特定事件之功能，並決定應記錄之特定資通系統事件。	應記錄資通系統管理者帳號所執行之各項功能。
是否符合			
現況說明			
佐證			
矯正作為			
目標日期			
備註說明			

	(2)日誌紀錄內容	(3)日誌儲存容量	(4)日誌處理失效之回應
項次編號（原始）	19	20	21
最低系統等級要求	普	普	普
安全控制措施	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	依據日誌儲存需求，配置所需之儲存容量。	資通系統於日誌處理失效時，應採取適當之行動。
是否符合			
現況說明			
佐證			
矯正作為			
目標日期			
備註說明			

	(5) 時戳及校時		(6)日誌資訊之保護
項次編號(原始)	23	24	25
最低系統等級要求	普	普	普
安全控制措施	資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間 (GMT)。	系統內部時鐘應定期與基準時間源進行同步。	對日誌之存取管理，僅限於有權限之使用者。
是否符合			
現況說明			
佐證			
矯正作為			
目標日期			
備註說明			

營運持續計畫			
	(1)資料備份		(2)系統備援
項次編號（原始）	28	29	33
最低系統等級要求	普	普	普
安全控制措施	訂定資料可容忍損失之時間要求。	執行資料備份。	訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。
是否符合			
現況說明			
佐證			
矯正作為			
目標日期			
備註說明			

制定日期:2025 年 11 月 28 日
最後修訂日期:2026 年 06 月 15 日

識別與鑑別			
	(1)使用者之 識別與鑑別	(2)身分驗證管理	
項次編號 (原始)	36	38	39
最低系統 等級要求	普	普	普
安全控制 措施	資通系統應識別及鑑別使用者，並禁止使用者使用共用帳號。	使用預設密碼初次登入系統時，應於登入後立即變更。	身分驗證相關資訊不以明文傳輸。
是否符合			
現況說明			
佐證			
矯正作為			
目標日期			
備註說明			

	(2)身分驗證管理		
項次編號（原始）	40	41	42
最低系統等級要求	普	普	普
安全控制措施	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達 5 次後，至少 15 分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。	使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。	密碼變更時，至少不可以與前三次使用過之密碼相同。
是否符合			
現況說明			
佐證			
矯正作為			
目標日期			
備註說明			

	(2)身分驗證管理	(3)鑑別資訊回饋
項次編號（原始）	43	46
最低系統等級要求	普	普
安全控制措施	上述兩點所定措施， 對非內部使用者，可依機關自行規範辦理。	資通系統應遮蔽鑑別過程中之資訊。
是否符合		
現況說明		
佐證		
矯正作為		
目標日期		
備註說明		

系統與服務獲得			
	(1)系統發展生命週期需求階段	(2)系統發展生命週期開發階段	
項次編號（原始）	48	51	52
最低系統等級要求	普	普	普
安全控制措施	針對系統安全需求（含機密性、可用性、完整性），進行確認。	應針對安全需求實作必要控制措施。	應注意避免軟體常見漏洞及實作必要控制措施。
是否符合			
現況說明			
佐證			
矯正作為			
目標日期			
備註說明			

	(2)系統發展生命週期開發階段	(3)系統發展生命週期測試階段
項次編號(原始)	53	56
最低系統等級要求	普	普
安全控制措施	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息。	執行「弱點掃描」安全檢測。
是否符合		
現況說明		
佐證		
矯正作為		
目標日期		
備註說明		

	(4)系統發展生命週期 部署與維運階段	
項次編號 (原始)	58	59
最低系統 等級要求	普	普
安全控制 措施	於部署環境中應針對相關資通安全威脅，進行更新與修補。	識別並關閉不必要服務及埠口。
是否符合		
現況說明		
佐證		
矯正作為		
目標日期		
備註說明		

	(4)系統發展生命週期 部署與維運階段	
項次編號 (原始)	60	61
最低系統 等級要求	普	普
安全控制 措施	資通系統不使用預設密碼。	執行系統源碼備份。
是否符合		
現況說明		
佐證		
矯正作為		
目標日期		
備註說明		

	(5)系統發展生命週期委外階段	(6)獲得程序	(7)系統文件
項次編號（原始）	63	64	66
最低系統等級要求	普	普	普
安全控制措施	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。	識別資通系統使用之第三方軟體、服務、函式庫或其他元件。	應儲存與管理系統發展生命週期之相關文件。
是否符合			
現況說明			
佐證			
矯正作為			
目標日期			
備註說明			

	系統與資訊完整性		
	(1)漏洞修復	(2)資訊系統監控	(3)軟體及資訊完整性
項次編號（原始）	72	74	77
最低系統等級要求	普	普	普
安全控制措施	系統之漏洞修復應測試有效性及潛在影響，並定期更新。	發現資通系統有被入侵跡象時，應通報機關特定人員。	使用者輸入資料合法性檢查應置放於應用系統伺服器端。
是否符合			
現況說明			
佐證			
矯正作為			
目標日期			
備註說明			

核章欄			
申請人	承辦單位	資訊室	資通安全長

制定日期:2025 年 11 月 28 日

最後修訂日期:2026 年 06 月 15 日