大林慈濟醫院-高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	3	4
最低系統等級要求	普	中	中	中
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。	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				

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

	(1)帳號管理			
項次編號（原始）	5	6	7	8
最低系統等級要求	高	高	高	高
安全控制措施	機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。	逾越機關所許可之閒置時間或可使用期限時，系統應自動將使用者登出。	應依機關規定之情況及條件，使用資通系統。	監控資通系統帳號，如發現帳號違常使用時回報管理者。
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:2025 年 11 月 28 日

	(2)最小權限	(3)遠端存取	
項次編號（原始）	9	10	11
最低系統等級要求	中	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:2025 年 11 月 28 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	中
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			

事件日誌與可歸責性				
	(1)記錄事件			
項次編號(原始)	15	16	17	18
最低系統等級要求	普	普	普	中
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 6 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。	應定期審查機關所保留資通系統產生之日誌。
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:2025 年 11 月 28 日

	(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	22
最低系統 等級要求	普	普	普	高
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。	機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。
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:2025 年 11 月 28 日

	(5) 時戳及校時	
項次編號(原始)	23	24
最低系統等級要求	普	中
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。
是否符合		
現況說明		
佐證		
矯正作為		
目標日期		
備註說明		

	(6)日誌資訊之保護		
項次編號（原始）	25	26	27
最低系統等級要求	普	中	高
安全控制措施	對日誌之存取管理，僅限於有權限之使用者。	應運用雜湊或其他適當方式之完整性確保機制。	定期備份日誌至原系統外之其他實體系統。
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)系統備份		
項次編號（原始）	28	29	30
最低系統等級要求	普	普	中
安全控制措施	訂定系統可容忍資料損失之時間要求。	執行系統源碼與資料備份。	應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。
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:2025 年 11 月 28 日

	(1)系統備份	
項次編號（原始）	31	32
最低系統等級要求	高	高
安全控制措施	應將備份還原，作為營運持續計畫測試之一部分。	應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。
是否符合		
現況說明		
佐證		
矯正作為		
目標日期		
備註說明		

	(2)系統備援	
項次編號（原始）	33	34
最低系統等級要求	中	中
安全控制措施	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。	原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。
是否符合		
現況說明		
佐證		
矯正作為		
目標日期		
備註說明		

識別與鑑別				
	(1)內部使用者之 識別與鑑別		(2)身分驗證管理	
項次編號 (原始)	35	36	37	38
最低系統 等級要求	普	高	普	普
安全控制 措施	資通系統應具備唯一 識別及鑑別機關使用 者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	對資通系統之存取採取多重認證技術。	使用預設密碼登入系統時，應於登入後要求立即變更。	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				

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

	(2)身分驗證管理		
項次編號（原始）	39	40	41
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。(對非內部使用者，可依機關自行規範辦理)	密碼變更時，至少不可以與前 3 次使用過之密碼相同。(對非內部使用者，可依機關自行規範辦理)
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:2025 年 11 月 28 日

	(2)身分驗證管理		
項次編號（原始）	42	43	44
最低系統等級要求	普	中	中
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。	身分驗證機制應防範自動化程式之登入或密碼更換嘗試。	密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。
是否符合			
現況說明			
佐證			
矯正作為			
目標日期			
備註說明			

	(3)鑑別資訊回饋	(4)加密模組鑑別	(5)非內部使用者之識別與鑑別
項次編號（原始）	45	46	47
最低系統等級要求	普	中	普
安全控制措施	資通系統應遮蔽鑑別過程中之資訊。	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	資通系統應識別及鑑非機關使用者（或代表機關使用者行為之程序)。
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:2025 年 11 月 28 日

系統與服務獲得			
	(1)系統發展生命週期需求階段	(2)系統發展生命週期設計階段	
項次編號（原始）	48	49	50
最低系統等級要求	普	中	中
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。	根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。	將風險評估結果回饋需求階段的檢核項目，並提出安全需求修正。
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:2025 年 11 月 28 日

	(3)系統發展生命週期開發階段		
項次編號(原始)	51	52	53
最低系統等級要求	普	普	普
安全控制措施	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。	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。
是否符合			
現況說明			
佐證			
矯正作為			
目標日期			
備註說明			

	(3)系統發展生命週期開發階段	
項次編號（原始）	54	55
最低系統等級要求	高	高
安全控制措施	執行「源碼掃描」安全檢測。	系統應具備發生嚴重 錯誤時之通知機制。
是否符合		
現況說明		
佐證		
矯正作為		
目標日期		
備註說明		

	(4)系統發展生命週期測試階段	
項次編號（原始）	56	57
最低系統等級要求	普	高
安全控制措施	執行「弱點掃描」安全檢測。	執行「滲透測試」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		

	(5)系統發展生命週期部署與維運階段		
項次編號（原始）	58	59	60
最低系統等級要求	普	普	中
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，並關閉不必要服務及埠口。	資通系統不使用預設密碼。	於系統發展生命週期之維運階段，應執行版本控制與變更管理。
是否符合			
現況說明			
佐證			
矯正作為			
目標日期			
備註說明			

	(6)系統發展生命週期委外階段	(7)獲得程序	(8)系統文件
項次編號（原始）	61	62	63
最低系統等級要求	普	中	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。	開發、測試以及正式作業環境應為區隔。	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			

	系統與通訊保護		
	(1)傳輸之機密性與完整性		
項次編號（原始）	64	65	66
最低系統等級要求	高	高	高
安全控制措施	資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。	使用公開、國際機構驗證且未遭破解的演算法。	支援演算法的最大長度金鑰。
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:2025 年 11 月 28 日

	(1)傳輸之機密性與完整性		(2)資料儲存之安全
項次編號（原始）	67	68	69
最低系統等級要求	高	高	高
安全控制措施	加密金鑰或憑證週期性更換。	伺服器端之金鑰保管應製定管理規則及實施應有之安全防護措施。	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。
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	
項次編號（原始）	70	71
最低系統等級要求	普	中
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。	定期確認資通系統相關 漏洞修復之狀態。
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		
	(2)資訊系統監控		
項次編號（原始）	72	73	74
最低系統等級要求	普	中	高
安全控制措施	發現資通系統有被入侵跡象時，應通報機關特定人員。	監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。	資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。
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:2025 年 11 月 28 日

	(3)軟體及資訊完整性			
項次編號（原始）	75	76	77	78
最低系統等級要求	中	中	中	高
安全控制措施	使用完整性驗證工具，以偵測未授權變更特定 軟體及資訊。	使用者輸入資料合法性檢查應置放於應用系統伺服器端。	發現違反完整性時，資通系統應實施機關指定之安全保護措施。	應定期執行軟體和資訊完整性檢查。
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:2025 年 11 月 28 日