

大林慈濟醫院-中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				

	(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			

	(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				

	(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	26
最低系統 等級要求	普	中	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。	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。
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			

	(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	37	38
最低系統 等級要求	普	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。	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			

	(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			

	(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			

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			

	(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			

	(4)系統發展生命週期測試階段	(5)系統發展生命週期部署與維運階段		
項次編號 (原始)	56	58	59	60
最低系統 等級要求	普	普	普	中
安全控制 措施	執行「弱點掃描」安全檢測。	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			

	系統與資訊完整性			
	(1)漏洞修復		(2)資訊系統監控	
項次編號 (原始)	70	71	72	73
最低系統 等級要求	普	中	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。	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。
是否符合				
現況說明				
佐證				
矯正作為				
目標日期				
備註說明				

	(3)軟體及資訊完整性		
項次編號 (原始)	75	76	77
最低系統 等級要求	中	中	中
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。
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