附件六、資通系統防護基準檢核表

# 資通系統防護基準檢核表(普級系統適用)

|  |  |
| --- | --- |
| 資通系統名稱 |  |
| 機關單位名稱 |  |
| 填寫人員 |  |
| 填寫日期 |  |
| 審核人員 |  |

| 構面 | 類別 | 項次編號  (原始) | 最低系統等級要求 | 安全控制措施 | 是否符合 | 現況說明 | 佐證 | 矯正作為 | 目標日期 | 備註說明 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 存取控制 | 帳號管理 | 1 | 普 | 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。 |  |  |  |  |  |  |
| 2 | 中 | 已逾期之臨時或緊急帳號應刪除或禁用。 |  |  |  |  |  |  |
| 3 | 中 | 資通系統閒置帳號應禁用。 |  |  |  |  |  |  |
| 4 | 中 | 定期審核資通系統帳號之申請、建立、修改、啟用、停用及刪除。 |  |  |  |  |  |  |
| 最小權限 | 9 | 中 | 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。 |  |  |  |  |  |  |
| 遠端存取 | 10 | 普 | 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 |  |  |  |  |  |  |
| 11 | 普 | 化。  使用者之權限檢查作業應於伺服器端完成。 |  |  |  |  |  |  |
| 12 | 普 | 應監控遠端存取機關內部網段或資通系統後臺之連線。 |  |  |  |  |  |  |
| 13 | 普 | 應採用加密機制。 |  |  |  |  |  |  |
| 14 | 中 | 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。 |  |  |  |  |  |  |
| 事件日誌與可歸責性 | 記錄事件 | 15 | 普 | 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。 |  |  |  |  |  |  |
| 16 | 普 | 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。 |  |  |  |  |  |  |
| 17 | 普 | 應記錄資通系統管理者帳號所執行之各項功能。 |  |  |  |  |  |  |
| 18 | 中 | 應定期審查機關所保留資通系統產生之日誌。 |  |  |  |  |  |  |
| 日誌紀錄內容 | 19 | 普 | 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。 |  |  |  |  |  |  |
| 日誌儲存容量 | 20 | 普 | 依據日誌儲存需求，配置所需之儲存容量。 |  |  |  |  |  |  |
| 日誌處理失效之回應 | 21 | 普 | 資通系統於日誌處理失效時，應採取適當之行動。 |  |  |  |  |  |  |
| 時戳及校時 | 23 | 普 | 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)。 |  |  |  |  |  |  |
| 24 | 中 | 系統內部時鐘應定期與基準時間源進行同步。 |  |  |  |  |  |  |
| 日誌資訊之保護 | 25 | 普 | 對日誌之存取管理，僅限於有權限之使用者。 |  |  |  |  |  |  |
| 26 | 中 | 應運用雜湊或其他適當方式之完整性確保機制。 |  |  |  |  |  |  |
| 營運持續計畫 | 系統備份 | 28 | 普 | 訂定系統可容忍資料損失之時間要求。 |  |  |  |  |  |  |
| 29 | 普 | 執行系統源碼與資料備份。 |  |  |  |  |  |  |
| 30 | 中 | 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。 |  |  |  |  |  |  |
| 系統備援 | 33 | 中 | 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。 |  |  |  |  |  |  |
| 34 | 中 | 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。 |  |  |  |  |  |  |
| 識別與鑑別 | 內部使用者之識別與鑑別 | 35 | 普 | 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。 |  |  |  |  |  |  |
| 身分驗證管理 | 37 | 普 | 使用預設密碼登入系統時，應於登入後要求立即變更。 |  |  |  |  |  |  |
| 38 | 普 | 身分驗證相關資訊不以明文傳輸。 |  |  |  |  |  |  |
| 39 | 普 | 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。 |  |  |  |  |  |  |
| 40 | 普 | 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) |  |  |  |  |  |  |
| 41 | 普 | 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) |  |  |  |  |  |  |
| 42 | 普 | 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。 |  |  |  |  |  |  |
| 43 | 中 | 身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 |  |  |  |  |  |  |
| 44 | 中 | 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。 |  |  |  |  |  |  |
| 鑑別資訊回饋 | 45 | 普 | 資通系統應遮蔽鑑別過程中之資訊。 |  |  |  |  |  |  |
| 加密模組鑑別 | 46 | 中 | 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。 |  |  |  |  |  |  |
| 非內部使用者之識別與鑑別 | 47 | 普 | 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 )。 |  |  |  |  |  |  |
| 系統與服務獲得 | 系統發展生命週期需求階段 | 48 | 普 | 針對系統安全需求(含機密性、可用性、完整性)  ，進行確認。 |  |  |  |  |  |  |
| 系統發展生命週期設計階段 | 49 | 中 | 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。 |  |  |  |  |  |  |
| 50 | 中 | 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。 |  |  |  |  |  |  |
| 系統發展生命週期開發階段 | 51 | 普 | 應針對安全需求實作必要控制措施。 |  |  |  |  |  |  |
| 52 | 普 | 應注意避免軟體常見漏洞及實作必要控制措施。 |  |  |  |  |  |  |
| 53 | 普 | 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。 |  |  |  |  |  |  |
| 系統發展生命週期測試階段 | 56 | 普 | 執行「弱點掃描」安全檢測。 |  |  |  |  |  |  |
| 系統發展生命週期部署與維運階段 | 58 | 普 | 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。 |  |  |  |  |  |  |
| 59 | 普 | 資通系統不使用預設密碼。 |  |  |  |  |  |  |
| 60 | 中 | 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。 |  |  |  |  |  |  |
| 系統發展生命週期委外階段 | 61 | 普 | 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。 |  |  |  |  |  |  |
| 獲得程序 | 62 | 中 | 開發、測試以及正式作業環境應為區隔。 |  |  |  |  |  |  |
| 系統文件 | 63 | 普 | 應儲存與管理系統發展生命週期之相關文件。 |  |  |  |  |  |  |
| 系統與資訊完整性 | 漏洞修復 | 70 | 普 | 系統之漏洞修復應測試有效性及潛在影響，並定期更新。 |  |  |  |  |  |  |
| 71 | 中 | 定期確認資通系統相關漏洞修復之狀態。 |  |  |  |  |  |  |
| 資訊系統監控 | 72 | 普 | 發現資通系統有被入侵跡象時，應通報機關特定人員。 |  |  |  |  |  |  |
| 73 | 中 | 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。 |  |  |  |  |  |  |
| 軟體及資訊完整性 | 75 | 中 | 使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 |  |  |  |  |  |  |
| 76 | 中 | 使用者輸入資料合法性檢查應置放於應用系統伺服器端。 |  |  |  |  |  |  |
| 77 | 中 | 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。 |  |  |  |  |  |  |