附件8資通系統防護基準

|  |  |  |  |
| --- | --- | --- | --- |
| 系統防護需求分級 控制措施 | 高 | 中 | 普 |
| 構面 | 措施內容 |
| 存取控 制 | 帳號管 理 | 一、逾越機關所定預期閒置時間或可使用期限時，系統應自 動將使用者登出。二、應依機關規定之情況及條件，使用資 通系統。三、監控資通系統帳 號，如發現帳號違常使用時回報管理者。四、等級「中」之所有控制措施。 | 一、已逾期之臨時或緊急帳號應刪除或禁用。二、資通系統閒置帳號 應禁用。三、定期審核資通系統 帳號之建立、修改、啟用、禁用及刪除。四、等級「普」之所有控 制措施。 | 建立帳號管理機制，包含帳號之申請、開通、停用 及刪除之程序。 |
| 最小權 限 | 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。 | 無要求。 |
| 遠端存 取 | 一、應監控資通系統遠端連線。二、資通系統應採用加密機制。 三、資通系統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。 四、等級「普」之所有控制措施。 | 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。 |
| 稽核與可歸責 性 | 稽核事 件 | 一、應定期審查稽核事件。二、等級「普」之所有控制措施。 | 一、依規定時間週期及紀錄留存政策，保留 稽核紀錄。二、確保資通系統有稽 核特定事件之功能， 並決定應稽核之特 定資通系統事件。三、應稽核資通系統管理者帳號所執行之 各項功能。 |
| 稽核紀 錄內容 | 一、資通系統產生之稽核紀錄，應依需求納入其他相關資訊。 二、等級「普」之所有控制措施。 | 資通系統產生之稽核紀錄應包含事件類型、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，並採用單一日誌紀錄機制，確保輸出 格式之一致性。 |
| 稽核儲存容量 | 依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。 |
| 稽核處 理失效 之回應 | 一、機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人 員提出警告。二、等級「中」及「普」 之所有控制措施。 | 資通系統於稽核處理失效時，應採取適當之行動。 |
| 時戳及 校時 | 一、系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。 二、等級「普」之所有控制措施。 | 資通系統應使用系統內部時鐘產生稽核紀錄所 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)。 |
| 稽核資 訊之保 護 | 一、定期備份稽核紀錄至與原稽核系統不 同之實體系統。二、等級「中」之所有控 制措施。 | 一、應運用雜湊或其他適當方式之完整性 確保機制。二、等級「普」之所有 控制措施。 | 對稽核紀錄之存取管理，僅限於有權限之使用者。 |
| 營運持 續計畫 | 系統備 份 | 一、應將備份還原，作為營運持續計畫測試之一部分。二、應在與運作系統不同處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。三、等級「中」之所有控制措施。 | 一、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。二、等級「普」之所有 控制措施。 | 一、訂定系統可容忍資 料損失之時間要求。 二、執行系統源碼與資 料備份。 |
| 系統備 援 | 一、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。二、原服務中斷時，於可容忍時間內，由備援設 備取代提供服務。 | 無要求。 |
| 識別與 鑑別 | 內部使 用者之 識別與 鑑別 | 一、對帳號之網路或本機存取採取多重認 證技術。二、等級「中」及「普」 之所有控制措施。 | 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。 |

|  |  |  |  |
| --- | --- | --- | --- |
|  | 身分驗 證管理 | 一、身分驗證機制應防範自動化程式之登入或密碼更換嘗試。 二、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。 三、等級「普」之所有控制措施。 | 一、使用預設密碼登入系統時，應於登入後要求立即變更。二、身分驗證相關資訊不以明文傳輸。三、具備帳戶鎖定機制，帳號登入進行身分 驗證失敗達三次後，至少十五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。四、基於密碼之鑑別資通系統應強制最低密 碼複雜度；強制密碼最短及最長之效期 限制。五、使用者更換密碼時，至少不可以與前三 次使用過之密碼相 同。六、第四點及第五點所定 措施，對非內部使用 者，可依機關自行規範辦理。 |
| 鑑別資訊回饋 | 資通系統應遮蔽鑑別過程中之資訊。 |
| 加密模組鑑別 | 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。 | 無要求。 |
| 非內部使用者 之識別 與鑑別 | 資通系統應識別及鑑別非機關使用者(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 | 針對系統安全需求（含機密性、可用性、完整性），以檢核表方式進行確認。 |
| 系統發展生命 週期設 計階段 | 一、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。 二、將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。  | 無要求。 |

|  |  |  |  |
| --- | --- | --- | --- |
|  | 系統發 展生命 週期開 發階段 | 一、執行「源碼掃描」安全檢測。二、具備系統嚴重錯誤 之通知機制。 三、等級「中」及「普」之所有控制措施。 | 一、應針對安全需求實作必要控制措施。二、應注意避免軟體常見漏洞及實作必要控制措 施。三、發生錯誤時，使用者頁面僅顯示簡短錯誤訊息 及代碼，不包含詳細之錯誤訊息。 |
| 系統發展生命 週期測 試階段 | 一、執行「滲透測試」安全檢測。 二、等級「中」及「普」之所有控制措施。 | 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 | 一、於系統發展生命週期之維運階段，須注意版本控制與變更管理。 二、等級「普」之所有控制措施。 | 一、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。二、資通系統相關軟體， 不使用預設密碼。 |
| 系統發展生命 週期委 外階段 | 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 | 開發、測試及正式作業環境應為區隔。 | 無要求。 |
| 系統文件 | 應儲存與管理系統發展生命週期之相關文件。 |
| 系統與通訊保 護 | 傳輸之 機密性 與完整 性 | 一、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。二、使用公開、國際機構驗證且未遭破解之演算法。三、支援演算法最大長 度金鑰。四、加密金鑰或憑證週 期性更換。五、伺服器端之金鑰保管應訂定管理規範及實施應有之安全 防護措施。 | 無要求。 | 無要求。 |