聯新國際醫院

AI 醫材軟體試用評估申請單

|  |  |  |  |
| --- | --- | --- | --- |
| **基本資料** | | | |
| **申請單位** |  | **申請者** |  |
| **試用期間** |  | **連絡方式** |  |
|  |
| **中文名稱** |  | | |
| **英文名稱** |  | | |
| **通過許可證情**  **況** | 通過 TFDA 通過本院 IRB 核可 其他： | | |
| **請上傳通過許可證(TFDA/IRB 等)(電子表單系統介面-上傳附件)** | | |
| **自評風險分級** | **風險分級說明(提供給填表者參考)**    **說明：**   1. **治療或診斷：軟體輸出直接作為醫師診斷依據** 2. **驅動臨床管理：材軟體輸出啟動醫護人員對病人進行二次評估或介入** 3. **告知臨床管理資訊：醫材軟體輸出僅供參考，診斷、決策由醫護執行** | | |
| **請申請者勾選：**  第 I 級 第 II 級 第 III 級 第 IV 級 | | |
| **自評風險分級**  **理由說明** |  | | |
| **醫療器材軟體來源( 相關文件請於電子表單系統介面-上傳附件)** | * 申請單位自購**(請上傳廠商授權使用文件)** * 醫療器材軟體製造商捐贈**(請上傳廠商捐贈之無償授權使用文件)**。製造商名稱： * 醫療器材軟體製造商試用**(請上傳廠商該物件之產權文件或是已簽署之合約)**。製造商名稱：宏碁智醫Acer Medical * 學術研究單位研發： * 其他，說明**： (請註明單位，若有相關物件產權文件或使用授權文件或合約請提供)** | | |
| **申請者請勾選同意條款**  申請者、協同申請者以及單位主管皆保證此所提之醫療器材軟體內容敘述屬實。申請者願意負擔一切責任。  於本醫院試用之醫療醫材軟體，不代表可作為商業使用之憑證。 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **醫療資訊安全評估** | | | |
| **主要運算硬體**  **配置地點** | 本院機房 臨床端設備  其他 | | |
| **運算硬體設備**  **提供方式** | 廠商自備 使用單位自備  其他 | | |
| **主要運算軟體配置- 作業系**  **統類型與版本** |  | | |
| **是 否 需 安 裝 client 軟體於院內電腦，請**  **說明** |  | | |
| **資安維護檢查項目** | 請參考「資通系統防護需求分級原則」  請填寫「安全等級評估表」  請填寫「負責任AI執行申請產品及軟體資訊安全自評表」(附表2~4一自評安全等級擇一填寫) | | |
| **介接醫院資訊**  **系統** | 是 否 | | |
| HIS NIS ●PACS 儀器設備 | | |
| **主要固定 IP**  **需求組數** |  | **是否對外連線** | 是 否 |
| **資料傳輸採用之加密機制及**  **版本** |  | **是否適用於緊急醫療處置情**  **境** | 是  否 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **資料評估** | | | | | | |
| **資料來源** |  | | | | | |
| **輸入資料篩選** |  | | | | | |
| **資料大小、數**  **量評估** |  | | | | | |
| **輸入欄位說明** |  | | | | | |
| **是否回傳** | 是 | 否 |  |  |  |  |
| **輸出欄位說明** |  | | | | | |
| **輸出地點** |  | | | | | |
| **資料保留機制** | | | | | | |
|  | **自醫院端輸入資料** | | **運算過程資料** | | **運算結果資料** | |
| **是否保留** | * 保留 | * 不保留 | * 保留 | * 不保留 | * 保留 | * 不保留 |
| **是否去識別** | * 是 | 否 | * 是 | 否 | * 是 | 否 |
| **保留位置** | * 回傳院內系統 * 上傳院外系統 * 其他，請說明： | | * 回傳院內系統 * 上傳院外系統 * 其他，請說明： | | 回傳院內系統   * 上傳院外系統 * 其他，請說明： | |
| **保留期間** |  | |  | |  | |
| **資料接解人員**  **權限管控機制** |  | |  | |  | |
| **試用結束後資料處理機制** | * 交由數位發展部處理 * 交由主持人處理 * 刪除傳統磁碟與SSD   內容   * 其他 | | * 交由數位發展部處理 * 交由主持人處理 * 刪除傳統磁碟與SSD   內容   * 其他 | | * 交由數位發展部處理 * 交由主持人處理 * 刪除傳統磁碟與SSD   內容   * 其他 | |
| **銷毀機制** |  | |  | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| **確效評估** | | | |
| **器材使用資料**  **類別** |  | | |
| **輸出目的** | 輔助診斷 治療輔助 醫療風險預測  其他： | | |
| **輸出格式** |  | | |
| **確效評估方式** | 於試用期收集資料 收集歷史資料測試  於試用其收集資料，平行與醫護評估標準比較  其他(請說明)： | | |
| **確效評估所需**  **個案數** |  | | |
| **評估標準定義** | 由三位專科醫師共同裁判  其他(請說明)： | | |
| **評估結果指標** |  | | |
| **定期驗證週期** |  | | |
| **適用領域( 醫**  **療領域)** |  | | |
| **定期持續維護**  **計畫** |  | | |
| **本院為衛生福利部指定負責任 AI 中心，本院官網將公告各項 AI 醫材軟體試**  **用評估相關的九大透明性原則資訊查詢服務，以下資料請確實填寫。** | | | |
| **介入詳情及輸出** | | **介入目的** | **介入的警告範圍外使用** |
|  | |  |  |
| **介入開發詳情及輸入特徵** | | **確保介入開發公平性的過程** | **外部驗證過程** |
|  | |  |  |
| **模型表現量化指標** | | **介入實施和使用的持續維護** | **更新和持續驗證或公平性評**  **估計畫** |
|  | |  |  |

\*備註：橘底建議由提供軟體開發單位(軟體供應商)填寫

附表1：安全等級評估表

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **「OOO系統」安全等級評估表** | | | | | | | | | | | |
| **功能說明：** | | | | | | | | | | | |
| **業務屬性：　□行政類 □醫療類** | | | | | | | **日期：\_\_\_年\_\_\_月\_\_\_日** | | | | |
| **影響構面** | | | | | | | | | | | **資訊系統安全等級** |
| **1.機密性** | | **2.完整性** | | | **3.可用性** | | | | **4.法律遵循性** | |
|  | |  | | |  | | | |  | |  |
| 步驟1：設定影響構面等級 | | | | | | | | | | | |
| 影響構面 | | |  | 安全等級 | | 原因說明 | | | | | |
| **1.機密性** | | | 初估 |  | |  | | | | | |
| **2.完整性** | | | 初估 |  | |  | | | | | |
| **3.可用性** | | | 初估 |  | |  | | | | | |
| **4.法律遵循性** | | | 初估 |  | |  | | | | | |
|  | | | |  | |  | |  | |  |  |  |
| 步驟2：識別業務屬性(行政類/醫療類) | | | | | | | | | | | |  |
| 項目 | | |  | 業務屬性 | | 原因說明 | | | | | |
| 識別業務屬性 | | | 初估 |  | |  | | | | | |  |
|  |  | |  |  | |  | |  | |  |  |  |
| 備註 | | |  | | | | | | | | |
| \*請參考「資通系統防護需求分級原則」填寫。 | | | | | | | | | | | |
|  |  | |  |  | |  | |  | |  |  |  |

負責任AI執行申請產品及軟體資訊安全自評表(含表2至表4)

附表2、資通系統防護基準檢核表(普級系統適用)

附表3、資通系統防護基準檢核表(中級系統適用)

附表4、資通系統防護基準檢核表(高級系統適用)

**附表2、資通系統防護基準檢核表(普級系統適用)**

| 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。 |  |  |  |  |  |  |
| 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、連線需求及文件化。 |  |  |  |  |  |  |
| 11 | 普 | 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。 |  |  |  |  |  |  |
| 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6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。 |  |  |  |  |  |  |
| 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)。 |  |  |  |  |  |  |
| 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。 |  |  |  |  |  |  |
| 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。 |  |  |  |  |  |  |
| 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。 |  |  |  |  |  |  |
| 鑑別資訊回饋 | 45 | 普 | 資通系統應遮蔽鑑別過程中之資訊。 |  |  |  |  |  |  |
| 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。 |  |  |  |  |  |  |
| 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。 |  |  |  |  |  |  |
| 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。 |  |  |  |  |  |  |
|  | 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。 |  |  |  |  |  |  |

**附表3、資通系統防護基準檢核表(中級系統適用)**

| 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。 |  |  |  |  |  |  |

**附表4、資通系統防護基準檢核表(高級系統適用)**

| 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。 |  |  |  |  |  |  |
| 5 | 高 | 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。 |  |  |  |  |  |  |
| 6 | 高 | 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。 |  |  |  |  |  |  |
| 7 | 高 | 應依機關規定之情況及條件，使用資通系統。 |  |  |  |  |  |  |
| 8 | 高 | 監控資通系統帳號，如發現帳號違常使用時回報管理者。 |  |  |  |  |  |  |
| 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。 |  |  |  |  |  |  |
| 22 | 高 | 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。 |  |  |  |  |  |  |
| 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。 |  |  |  |  |  |  |
| 27 | 高 | 定期備份日誌至原系統外之其他實體系統。 |  |  |  |  |  |  |
| 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。 |  |  |  |  |  |  |
| 31 | 高 | 應將備份還原，作為營運持續計畫測試之一部分。 |  |  |  |  |  |  |
| 32 | 高 | 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。 |  |  |  |  |  |  |
| 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。 |  |  |  |  |  |  |
| 36 | 高 | 對資通系統之存取採取多重認證技術。 |  |  |  |  |  |  |
| 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。 |  |  |  |  |  |  |
| 54 | 高 | 執行「源碼掃描」安全檢測。 |  |  |  |  |  |  |
| 55 | 高 | 系統應具備發生嚴重錯誤時之通知機制。 |  |  |  |  |  |  |
| 系統發展生命週期測試階段 | 56 | 普 | 執行「弱點掃描」安全檢測。 |  |  |  |  |  |  |
| 57 | 高 | 執行「滲透測試」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。 |  |  |  |  |  |  |  |
| 系統與通訊保護 | 傳輸之機密性與完整性 | 64 | 高 | 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。 |  |  |  |  |  |  |  |
| 65 | 高 | 使用公開、國際機構驗證且未遭破解的演算法。 |  |  |  |  |  |  |  |
| 66 | 高 | 支援演算法的最大長度金鑰。 |  |  |  |  |  |  |  |
| 67 | 高 | 加密金鑰或憑證週期性更換。 |  |  |  |  |  |  |  |
| 68 | 高 | 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。 |  |  |  |  |  |  |  |
| 資料儲存之安全 | 69 | 高 | 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。 |  |  |  |  |  |  |  |
| 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。 |  |  |  |  |  |  |  |
| 74 | 高 | 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。 |  |  |  |  |  |  |  |
| 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。 |  |  |  |  |  |  |
| 78 | 高 | 應定期執行軟體和資訊完整性檢查。 |  |  |  |  |  |  |

**廠商：**

|  |  |  |  |
| --- | --- | --- | --- |
| **廠商填表人姓名** | **廠商填表人簽章** | **填表廠商名稱** | **填表廠商簽章** |
|  |  |  |  |