**資通系統防護基準查檢表-普級**

**一、資通系統基本資料**

|  |  |  |
| --- | --- | --- |
| 系統名稱 | 石油與天然氣輸儲設備查核及檢測雲端平台 | |
| 系統網址 | www.gasoilsystem.tw | |
| 主機所在位置 | ■工研院資訊處itriCloud[[1]](#footnote-1)  □工研院資訊處webhosting  □其他通過ISO 27001驗證之機房\_\_\_\_\_\_\_\_\_\_\_\_\_\_  註：煩請檢附該機房通過ISO 27001驗證之證書。(資訊處機房不需提供) | |
| 主機作業系統及版本 | ■Windows，版本:\_\_\_\_Server 2019\_\_\_\_\_\_  □Mac OS，版本:\_\_\_\_\_\_\_\_\_\_  □Unix / Linux，版本: \_\_\_\_\_\_\_\_\_\_  □FreeBSD，版本: \_\_\_\_\_\_\_\_\_\_  □其他，作業系統名稱\_\_\_\_\_\_\_\_\_\_\_\_\_\_，版本:\_\_\_\_\_\_\_\_\_  註：煩請寫出「種類」和「版本號碼」，如 Linux請寫CentOS 6.8、RHEL 6.8、Oracle Linux 6.8或其他，而非只寫Linux 6.8，以利查出明確漏洞資訊。 | |
| 開發語言及版本 | □C/C++，版本:\_\_\_\_\_\_\_\_\_\_  ■C#，版本:\_\_\_C#5.0\_\_\_\_\_\_\_  □Java，版本:\_\_\_\_\_\_\_\_\_\_  □JavaScript，版本:\_\_\_\_\_\_\_\_\_\_  □Python，版本:\_\_\_\_\_\_\_\_\_\_  □PHP，版本:\_\_\_\_\_\_\_\_\_\_  ■Visual Basic .NET，版本: \_\_\_\_4.5\_\_\_\_\_\_  □其他，語言名稱\_\_\_\_\_\_\_\_\_\_\_\_，版本:\_\_\_\_\_\_\_\_\_\_  註：煩請填寫詳細版本，如PHP請寫7.3.17或其他，而非PHP 7.0。 | |
| Web伺服器 | □無  □有，  □Apache HTTP Server，版本:\_\_\_\_\_\_\_\_\_\_  □Apache Tomcat Server，版本:\_\_\_\_\_\_\_\_\_\_  ■Microsoft IIS，版本：\_\_\_\_10\_\_\_\_  □Nginx，版本:\_\_\_\_\_\_\_\_\_\_  □其他，伺服器名稱\_\_\_\_\_\_\_\_\_\_\_\_\_\_，版本:\_\_\_\_\_\_\_\_\_  註：煩請填寫詳細版本，如Tomcat請寫7.0.65或其他，而非Tomcat 7.0。 | |
| 資料庫 | □無  ■有，  □DB2，版本:\_\_\_\_\_\_\_\_\_\_\_\_\_  □Sqlite，版本:\_\_\_\_\_\_\_\_\_\_\_\_\_  □Oracle，版本:\_\_\_\_\_\_\_\_\_\_  □MySQL，版本:\_\_\_\_\_\_\_\_\_\_\_\_\_  □PostgreSQL，版本:\_\_\_\_\_\_\_\_\_\_\_\_\_  □Microsoft Access，版本:\_\_\_\_\_\_\_\_\_\_\_\_\_  ■Microsoft SQL Server，版本: \_\_\_\_\_\_2019\_\_\_\_\_\_\_  □其他，資料庫名稱\_\_\_\_\_\_\_\_\_\_\_\_\_，版本:\_\_\_\_\_\_\_\_\_  註：煩請填寫詳細版本，如Oracle Database請寫12.1.0.1，而非僅寫12。 | |
| 網站框架 | □無  ■有，  □Struts，版本:\_\_\_\_\_\_\_\_\_\_\_\_\_  □Spring，版本:\_\_\_\_\_\_\_\_\_\_\_\_\_  □ZK，版本:\_\_\_\_\_\_\_\_\_\_\_\_\_  □django，版本:\_\_\_\_\_\_\_\_\_\_\_\_\_  ■.Net Framework，版本: \_\_\_\_4.5\_\_\_\_\_\_\_\_\_  □其他，網站框架名稱\_\_\_\_\_\_\_\_\_\_\_\_，版本:\_\_\_\_\_\_\_\_  註：煩請填寫詳細版本。 | |
| 軟體元件清單 | 元件名稱（以下可自行新增表格） | 版本（煩請填寫詳細版本） |
| jQuery | 3.3.7 |
| (範例) Bootstrap | (範例) 3.1 |
| (範例) jQuery | (範例) 3.3.7 |
| (範例) Ckeditor | (範例) 3.6.4 |
| (範例) ClosedXML | (範例) 0.94.2 |
| 首次上線日期 | 108　　年　　4　月　1　 日 | |
| 最近改版日期 | 113　　年　　7　月　22　 日 | |
| 資通系統防護需求分級 | ¢普 □中 □高 | |

**二、資通系統防護基準查檢表(法規版本：110/08/23)**

若對以下內容需要進一步瞭解，請至行政院國家資通安全會報技術服務中心網站>共通規範>下載「資通系統防護基準驗證實務」。

網址：https://www.nccst.nat.gov.tw/CommonSpecification

| No. | 構面 | 措施 | 控制措施 | 自評結果 | 稽核發現 | 稽核發現說明 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | 存取控制 | 帳號管理 | 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。 | ■是，請勾選已具備之程序： 　■帳號申請 email提交申請需求 　■帳號建立 網頁管理者進後台新增人員 　■帳號修改 網頁管理者進後台修改人員資料 　■帳號啟用 網頁管理者進後台做人員啟用動作 　■帳號停用 網頁管理者進後台做人員停用動作 　□帳號刪除 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 | OBS 1：網站停用帳號未盤點及帳號留存過久未實際刪除。 |
| 2 | 存取控制 | 遠端存取 | 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。 | □是，已有遠端存取的文件化資訊。 □否 ■不適用，請說明：\_\_\_不允許遠端登入\_\_\_\_ | ¢符合  £不符合  £不適用 | 未限制來源IP |
| 3 | 存取控制 | 遠端存取 | 使用者之權限檢查作業應於伺服器端完成。 | □是，請勾選實作方式： 　□於伺服器端進行權限檢查 　□其他 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □否 ■不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 | 於伺服器端檢查 |
| 4 | 存取控制 | 遠端存取 | 應監控遠端存取機關內部網段或資通系統後臺之連線。 | ■是，已有監控機制 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 5 | 存取控制 | 遠端存取 | 應採用加密機制。 | ■是，請勾選實作方式： 　¢HTTPS加密 　□SSH加密 　□VPN加密 　□遠端桌面通訊協定(RDP)啟用加密 　□其他 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 | 一般名稱 (CN) Go Daddy Secure Certificate Authority - G2  組織 (O) GoDaddy.com, Inc.  組織單位 (OU) http://certs.godaddy.com/repository/  發行日期 2024年4月10日 星期三 晚上11:05:14  到期日 2025年5月12日 星期一 晚上11:05:14 |
| 6 | 事件日誌與可歸責性 | 記錄事件 | 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。 | ■是，已保留6個月事件日誌 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 | Log:2023／12／1～2024/8/6 |
| 7 | 事件日誌與可歸責性 | 記錄事件 | 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。 | ■是，請勾選實作方式： 　■記錄身分驗證事件 　■記錄資料存取事件 　■記錄系統功能錯誤事件 　□其他 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □否，無事件記錄功能 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | £符合  ¢不符合  £不適用 | 帳號、姓名、帳號類別、登入時間、登入結果  OBS 2：人員登入歷史紀錄中8／2起多次登入失敗。帳號OOOO147oooo258@ |
| 8 | 事件日誌與可歸責性 | 記錄事件 | 應記錄資通系統管理者帳號所執行之各項功能。 | ■是 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 | 只紀錄帳號新、增、修、刪。 |
| 9 | 事件日誌與可歸責性 | 日誌紀錄內容 | 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，並採用單一日誌紀錄機制，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。 | □是，請勾選實作方式： 　□事件類型 　□發生時間 　□發生位置 　■使用者身分識別 　□採用單一的日誌紀錄機制 　□其他 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 | 帳號、姓名、帳號類別、登入時間、登入結果 |
| 10 | 事件日誌與可歸責性 | 日誌儲存容量 | 依據日誌儲存需求，配置日誌紀錄所需之儲存容量。 | ■是 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 11 | 事件日誌與可歸責性 | 日誌處理失效之回應 | 資通系統於日誌處理失效時，應採取適當之行動。 | □是，請勾選實作方式： 　□關閉資訊系統 　□覆寫最舊的日誌紀錄 　■停止產生日誌紀錄 　□通知管理者進行故障排除 　□其他 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 12 | 事件日誌與可歸責性 | 時戳及校時 | 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)。 | □是 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 13 | 事件日誌與可歸責性 | 日誌資訊之保護 | 對日誌之存取管理，僅限於有權限之使用者。 | ■是 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 | 限管理者群組權限 |
| 14 | 營運持續計畫 | 系統備份 | 訂定系統可容忍資料損失之時間要求。 | ■是，時間為\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 15 | 營運持續計畫 | 系統備份 | 執行系統源碼與資料備份。 | ■是 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 | 每天完整備份(am 12：00)，保留1個月。 |
| 16 | 識別與鑑別 | 內部使用者之識別與鑑別 | 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。 | ■是 □否，無法識別機關使用者，或允許共用帳號 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | £符合  ¢不符合  £不適用 | OBS 3：元弘廠商於8／6稽核時，使用賴斐瓔帳號進行網站操作，故有帳號共用議題。 |
| 17 | 識別與鑑別 | 身分驗證管理 | 使用預設密碼登入系統時，應於登入後要求立即變更。 | ■是，要求立即變更預設密碼 □否，未要求變更預設密碼 □不適用(如未使用預設密碼)， 請說明：\_\_\_\_\_\_\_\_\_\_\_\_ | £符合  ¢不符合  £不適用 | OBS 4：網站人員管理介面直接明碼呈現密碼。 |
| 18 | 識別與鑑別 | 身分驗證管理 | 身分驗證相關資訊不以明文傳輸。 | ■是，請勾選實作方式： 　□使用HTTPS或SSH加密 　□將身分驗證資訊加密或編碼後傳輸 　□其他 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 19 | 識別與鑑別 | 身分驗證管理 | 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。 | ■是，具備帳戶鎖定機制 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 | 身分驗證失敗達3次後，至少15分鐘內不允許該帳號繼續嘗試登入 |
| 20 | 識別與鑑別 | 身分驗證管理 | 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） | ■是，請勾選實作方式： 　■強制密碼複雜度 　■強制密碼最短效期 　■強制密碼最長效期 　□其他 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 | 8碼，大、小寫，數字，特殊符號 |
| 21 | 識別與鑑別 | 身分驗證管理 | 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 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 22 | 識別與鑑別 | 鑑別資訊回饋 | 資通系統應遮蔽鑑別過程中之資訊。 | ■是，請勾選實作方式： 　□輸入密碼時顯示\*或空白 　□其他 \_\_\_\_\_\_\_\_\_\_\_\_\_ □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 23 | 識別與鑑別 | 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) 。 | ■是，具備身分驗證機制 □否，未具備身分驗證機制 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 24 | 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)進行確認。 | ■是，以本表單進行確認 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 25 | 系統與服務獲得 | 系統發展生命週期開發階段 | 應針對安全需求實作必要控制措施。 | ■是 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 26 | 系統與服務獲得 | 系統發展生命週期開發階段 | 應注意避免軟體常見漏洞及實作必要控制措施。 | ■是 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 | HCL ApppScan Standard  2023／6／17，預計2024／8產出新報告  無中、高以上風險。 |
| 27 | 系統與服務獲得 | 系統發展生命週期開發階段 | 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。 | ■是 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 28 | 系統與服務獲得 | 系統發展生命週期測試階段 | 執行「弱點掃描」安全檢測。 | ■是 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 | HCL ApppScan Standard  2023／6／17，預計2024／8產出新報告  無中、高以上風險。 |
| 29 | 系統與服務獲得 | 系統發展生命週期部屬與維運階段 | 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。 | ■是 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 | HCL ApppScan Standard  2023／6／17，預計2024／8產出新報告  無中、高以上風險。 |
| 30 | 系統與服務獲得 | 系統發展生命週期部屬與維運階段 | 資通系統不使用預設密碼。 | ■是，本系統、資料庫或Web伺服器等軟體元件未使用預設密碼 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 31 | 系統與服務獲得 | 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。 | ■是 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 32 | 系統與服務獲得 | 系統文件 | 應儲存與管理系統發展生命週期之相關文件。 | ■是 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 | 20230816系統介面規格書.pdf  更新日期是2023/8/16 |
| 33 | 系統與資訊完整性 | 漏洞修復 | 系統之漏洞修復應測試有效性及潛在影響，並定期更新。 | ■是 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |
| 34 | 系統與資訊完整性 | 資通系統監控 | 發現資通系統有被入侵跡象時，應通報機關特定人員。 | ■是 □否 □不適用，請說明：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | ¢符合  £不符合  £不適用 |  |

1. [↑](#footnote-ref-1)