-密等: □機密 □限閱 ■普通-

臺灣中華化學工業股份有限公司
CHUNG HWA CHEMICAL INDUSTRIAL WORKS, LTD.

114年資訊安全管理及執行情形報告

資訊室

2026/01/14

資訊安全政策

因應外部資安威脅升高與配合 ISO 27001:2022 導入需求，發行ISM-IT-01資訊安全政策以升級資訊安全治理架構

強化資訊資產之 機密性、完整性與可用性，確保營運持續與法規遵循

【全員責任與落實】

- 落實日常資訊安全作業與內控機制
- 即時通報資安事件與弱點
- 確保資訊資產存取與使用符合規範
- 配合教育訓練、稽核與管理審查

政策適用於全體單位及內外部相關人員，持續透過公告、會議與教育訓練完成宣導，確保落實執行

資訊安全風險管理程序-體系核心與權責分工

- **管理目標：**
  建立 ISO 27001:2022 合規之 ISMS 風險評鑑規範，預防資安事件

- **風險擁有者（單位主管）：**
  負責核定風險評鑑結果、可接受風險值及處理計畫

- **資訊安全執行小組：**負責複核風險值、產出風險處理與機會實作計畫

- **權責單位：**執行資訊資產之威脅與弱點評估及風險值計算

資訊安全風險管理程序-作業流程

識別風險：
資產鑑別、
威脅識別、
找出弱點

評估風險：
計算風險值、
判定層級、
產出報告

監督風險：
追蹤改善、
量測分析、
定期覆核

處置風險：
選擇措施、
執行計畫、
核定與實作

資訊安全風險管理程序-風險評鑑作業流程

- **資產鑑別**：依「資訊資產管理程序(ISP-IT-04)」進行分類

- **強制評估觸發**：(風險評估)
  資產價值 ≥ 7 或機密性、完整性、可用性任一項值為 4 時必評

- **六大威脅類別**：涵蓋人為、文件/資料、軟體、硬體、通訊、環境

- **量化評估標準**：
  發生可能性（1-4分）：依發生頻率（如三年 1 次至每月 1 次以上）判定
  衝擊程度（1-4分）：依業務停頓時間（如立即復原至超過三天）判定

資訊安全風險管理程序

- 風險計算與管理決策
  資訊資產風險值=資訊資產價值x事件發生可能性x事件衝擊性
- **風險處理**：
  超出「可接受風險值」之項目，須擬定 **風險處理計畫** 並追蹤改善

- 持續改善機制
  定期複核：每年至少執行 1 次 風險與機會評鑑
  動態調整：遇新增資產（價值 ≥ 7）或作業環境改變時應不定期複核
  機會評鑑：除管理風險外，亦須評估能增進資安之「機會」並納入實作計畫
  核心表單：威脅弱點評估表、風險評鑑彙整表、風險處理與機會實作計畫表

資訊安全風險管理-案例演示
(ERP 核心資料庫損毀硬體/軟體失效)

此案例模擬企業核心系統因硬體故障或勒索軟體導致資料庫無法存取

資產價值評分：9（屬於本公司重要基礎設施與流程，價值 > 7 必須評鑑 ）

風險評估細節：

- **威脅類別**：硬體失效或軟體操作不當
- **發生可能性：2（低）**
  評估標準：因目前有執行控制措施，威脅發生可能性極低，約一年發生 1 次
- **衝擊程度：4（高）**
  評估標準：導致多項業務營運停頓，復原需專業人員且無法在三天內完成
- **風險計算結果：**
  9(價值)x2(可能性)x4(衝擊)=72

管理決策：
此數值超出公司制定的「可接受風險值」，必須產出「風險處理與機會實作計畫表(ISP-IT-05-03)」，並列入追蹤管理

資訊安全管理方案

人員安全管理及教育訓練

- 定期更換密碼維持密碼的強度、機密性，並進行資訊安全教育訓練
- 人員職掌明確分工，重要或限閱等級以上的資訊不可由單獨一人知悉或運作，需有監督機制（透過ISMS表單）

電腦主機安全管理

- 個人電腦與伺服器之存取、密碼、螢幕保護與閒置鎖定機制，確保帳號與設備使用安全
- 落實防毒軟體、系統修補更新及軟體白名單管理，防止未授權程式與資安風險

網路安全管理

- 所有與外界連接均透過防火牆控管，每半年檢視一次防火牆規則與物件
- 關鍵業務系統及核心網路設備日誌至少保存3個月，一般伺服器日誌保存1個月
- 非經授權禁止遠端存取；廠商維護需申請「外對內連線服務」，並透過VPN或SSH等加密通道進行

機房安全管理

- 機房被定義為「安全區域」，實施嚴格的實體與環境控制

資訊安全管理執行情形-管理指標

設定四大目標，並設定具體年度待辦事項與量測指標，以評估達成狀況	
目標一： 人員知能與意識	指標內容：全體員工每年至少參加 2次 資安宣導訓練，並通過評量（分數需 >=70分） 目的：推廣員工資安意識並強化責任認知。
目標二： 避免資料外洩與未經授權存取	指標內容：系統遭入侵、資料外洩或未經授權的存取事件，件數每年 = 0 件 目的：保護業務資訊，確保其正確完整。
目標三： 落實日常維運與稽核	指標內容：年度內外部稽核開立之矯正處理單，未於「預訂完成日期」後二週內完成追蹤的件數 < 3 件 目的：確保相關作業確實落實並持續改善。
目標四： 確保服務可用性	指標內容：監控關鍵核心系統服務（含網路及核心資訊系統），非預期中斷時間年度超過 4 小時的件數 ≦ 2 件 目的：維持關鍵核心系統的穩定運作。

資訊安全管理執行情形-資通安全管理之資源

項目	說明
組織與人力資源	最高管理階層承諾確保ISMS所需之資源可取得 資訊安全執行小組：規劃及執行資安作業、推動活動及辦理教育訓練(資訊室) 緊急處理小組：由執行小組成員組成，負責重大資安事件的應變、通報與復原 資訊安全稽核小組：負責評估制度執行情形(稽核室) 執行秘書：負責協調上述小組之運作
技術與工具資源	使用NESSUS 軟體進行系統或設備的弱點檢測，每年至少執行一次 使用FortiGate 100F 防火牆，具備 IPS（入侵防禦）、應用程式控制及 AMP 功能 使用 NAS 系統中的 Log Server 來保存與審查系統日誌 部署防毒軟體並設定自動更新與即時掃描；內部威脅情資來源亦包含 EDR/XDR 等平台 系統效能監控使用 VMware tools 軟體監控 CPU、RAM、剩餘容量及頻寬使用率
組態與資產管理	建立「組態安全管理表」，詳細記錄伺服器硬體（如 CPU 核心數、RAM 大小）、作業系統版本（如 VMware ESXi、Windows Server）及網路設定

資訊安全管理執行情形

全景分析	於 11 月 6 日召開會議，識別出極端氣候、軟體停止支援（EOS）及資料外洩等外部議題，並決議納入風險評鑑
風險評鑑與管理	**評鑑執行：** 於 11 月 21 日完成風險評鑑，核定可接受風險值為 100 **評估結果：** 識別出 2 項超出可接受風險值的資產項目；另有 3 項軟體因 EOS（停止支援）被列入潛在風險，納入計畫加強管控
技術檢測	核心服務（HCI 伺服器）檢測出 4 項 High 風險，因原廠尚未釋出更新版本，決議採存取控制與實體隔離方式暫時因應
資安事件與威脅情資管理	**資安事件：** 12 月 5 日發生一起員工誤點釣魚郵件導致帳密外洩的事件。攻擊者利用外洩帳密發送釣魚信件。 **處置：** 強制更換相關人員密碼、刪除惡意郵件，並進行後台監控 **矯正措施：** 短期進行全公司密碼變更與宣導；長期對策將於 2026 年 1 月前針對雲端服務導入多重驗證（MFA）

資訊安全管理執行情形

威脅情資	定期追蹤弱點資訊（如 Fortinet 產品、MS SQL Server、一等一科技系統漏洞），並安排廠商進行韌體更新或系統修補
營運持續管理（BCP）	• **演練執行：** 於 12 月 2 日執行年度營運持續演練，情境模擬「伺服器硬體故障與資料庫損毀」。 • **演練結果：** 實際復原時間為 7 小時，符合復原時間目標（RTO）8 小時之要求，確認備份與還原程序有效
稽核與績效評估	• **內部稽核：** 於 12 月 26 日由外部顧問進行 114 年度資訊安全內部稽核，涵蓋管理面與技術面，無重大缺失 • **教育訓練：** 本年度已完成 2 次資安教育訓練，測驗成績皆達標（>=70分） • **日常維運：** 定期執行防火牆政策檢視、日誌審查及設備巡檢，結果均無異常

ISMS ISO27001:2022 取證時程(3月完成取證)

外部稽核執行： 由第三方驗證機構（BSI）派員進行稽核

第一階段稽核（115/1/26）： 文件審查，確認制度設計符合標準

第二階段稽核（115/2/9）： 實地查核，驗證制度落實情形

115/2/E：完成缺失改善(若有)、115/3：**預計取得證書**

因應 ISO 27001 要求，資訊室已完成並發行：

23 份程序書與管理說明書、43 份衍生表單

這些文件將成為公司資安管理的基礎，可帶來以下效益：

- 流程標準化：降低人為操作差異與資安風險
- 提升可追溯與稽核效率
- 強化事件應變能力與營運韌性
- 降低資安事件的後端成本與衝擊
- 全面提升公司資安成熟度與可靠度

報告完畢，感謝聆聽

臺灣中華化學工業股份有限公司
CHUNG HWA CHEMICAL INDUSTRIAL WORKS, LTD.

基礎化學品 Basic Chemicals
特用化學品 Specialty Chemicals
電子化學品 Electronic Chemicals