dyaco

岱宇國際股份有限公司

Dyaco International Inc.

岱宇國際股份有限公司
ISO 27001 資安事件處理流程
（一般員工版）

保護公司資訊・守護研發創新・確保生產營運・維護客戶信任



流程步驟	作業內容與流程	主要責任角色

1 發現異常（疑似資安事件）



可能的異常情境（岱宇國際情境範例）

- 收到可疑郵件（如假冒客戶、供應商、銀行或物流）
- 帳號異常（無法登入、收到異地登入通知）
- 研發圖面、產品設計或技術文件疑似外洩
- 客戶 / 供應商資料異常存取或外洩風險
- 辦公電腦、伺服器、工廠或產線資訊設備異常
- 公司網站、網路服務或雲端系統異常
- 智慧健身或復健設備（連網設備、APP、雲端平台）異常
- 其他可能影響公司資訊安全的情況



一般員工

- 日常工作中保持警覺
- 發現異常立即通報
- 不自行處理或隱瞞
- 配合後續調查

2 立即通報（快速回報）



通報方式（依公司既定管道）

- 透過公司既定的資安通報窗口 / MIS / 部門主管進行通報
- 提供事件發生時間、現象、影響範圍與相關資訊
- 如為緊急重大事件，依公司緊急通報機制立即回報
- 保留現場狀態，避免進一步操作，等待指示



部門主管

- 協助確認事件資訊
- 立即向 MIS / 資安窗口通報
- 必要時協助隔離設備或停止使用
- 配合後續調查與處理

3 事件分級（初步判斷）



事件分級（由 MIS / 資安單位初步判斷）

等級	說明（範例）	可能影響
重大 (Critical)	大量客戶資料外洩、核心系統癱瘓、生產停擺、品牌重大影響	營運中斷、法規罰則、重大財務與聲譽損失
高 (High)	研發圖面外洩、關鍵系統受駭、製造 / 品保系統嚴重異常	研發競爭力受損、生產延誤、客戶信任下降
中 (Medium)	部分系統異常、可疑郵件攻擊、特定帳號異常	有限影響、需密切監控
低 (Low)	一般設備異常、單一帳號事件、非敏感資料外洩風險	影響較小、可控制



MIS / 資訊單位（資安窗口）

- 接收通報與初步判斷
- 評估事件等級
- 啟動資安事件應變機制（ISIRT）
- 通知相關單位

4 事件處理（調查與因應）



事件調查與處理措施（依事件類型採取適當措施）

- 蒐集與保全相關證據（Log、系統紀錄、郵件等）
- 進行事件影響範圍與原因調查
- 採取控制措施（如隔離設備、封鎖帳號、阻擋連線等）
- 通知相關業務單位（研發、製造、品質、業務 / 客服等）
- 必要時與外部專業單位合作（如原廠、資安廠商、法務）
- 持續追蹤事件處理進度



資安事件應變小組（ISIRT）

- 統籌指揮與協調處理
- 跨部門調查與因應
- 評估對營運、客戶、供應鏈與品牌的影響
- 必要時對外聯繫（客戶、供應商、主管機關等，依公司規定）

5 系統復原（恢復正常）



系統復原與驗證

- 清除惡意程式或修補弱點
- 恢復系統、資料或服務（含辦公、研發、生產、ERP 等）
- 驗證系統功能與資料完整性
- 確認智慧健身 / 復健設備、APP 及雲端平台正常運作（如有受影響）
- 監控是否再次發生異常
- 確認風險已降低並恢復正常營運



MIS / 相關業務單位

- 執行系統復原與修補
- 驗證各系統與設備正常運作
- 提供業務面測試與確認（研發、製造、品質、業務 / 客服等）
- 持續監控與追蹤

6 結案與持續改善（經驗回饋）



結案與持續改善

- 彙整事件處理紀錄與報告
- 進行原因分析（Root Cause Analysis）
- 提出改善措施（技術、流程、人員教育訓練等）
- 完成結案審核與存檔
- 必要時更新相關政策、程序、系統設定
- 納入教育訓練宣導，降低再次發生的風險



管理階層

- 審核結案報告
- 檢討與持續改善
- 提供必要資源
- 推動資安意識與教育訓練

一般員工重要提醒

- 發現異常立即通報
- 不自行刪除或修改證據
- 不任意對外說明或公開討論
- 依指示隔離設備或停止使用
- 配合調查提供資訊
- 事件後配合改善與教育訓練



岱宇國際股份有限公司

Dyaco International Inc.

以運動與健康，創造更美好的生活

Better Health Brighter Lives

