資訊安全風險管理架構及年度具體管理方案

本公司資通安全風險管理架構、資通安全政策、具體管理方案及投入資通安全管理之資源如下：

1.資訊安全風險管理架構

為強化資訊安全之風險管理，成立資訊安全執行小組，建置資訊安全風險管理架構、訂定資訊安全政策及具體管理方案，並定期檢討資訊安全政策，以確保資訊安全。

2.資訊安全政策

資訊安全之目標

為促使本公司各項資訊安全管理制度能貫徹執行、永續運作及監督管理，維護重要資訊系統的機密性、完整性與可用性，特制定此一資訊安全政策，來強化資訊安全管理，提供安全、有效之資訊服務，建立安全可信賴之資訊作業環境，確保資料、系統、設備及網路之持續運作之目標。

3.資訊安全之範圍

(1)人員定期執行資訊安全宣導作業，強化同仁資安認知及法令觀念。

(2)電腦系統安全管理。

(3)網路安全管理。

(4)系統存取管制。

(5)系統發展及維護安全管理。

(6)資訊資產安全管理。

(7)實體及環境安全管理。

(8)資訊系統永續運作計畫管理。

(9)資訊安全稽核

4.具體之管理方案及措施

項目	具體管理措施
防毒軟體	使用防毒軟體，並自動更新病毒碼，減少病毒感染的機會。
社交工程演練服務	每年進行兩次進行員工社交工程警覺性測試，提升員工對資安的意識。
建置資通安全威脅偵測管理(SOC)監控服務	委託中華資安公司提供事前威脅的預警情報、事中威脅的即時告警以及事後威脅的分析建議，有效管理各種資安警訊，讓資安人員可以專注於處理重要的資安風險，共同防堵資安威脅。
對外網站執行弱點掃描或滲透測試	以駭客思維嘗試入侵公司網站、資訊系統、資訊設備等軟硬體，找出潛在的漏洞，驗證企業的資料與設備是否可被竊取或破壞，評估資訊系統與硬體安全性是否有待加強，提早進行修補。
通過ISO 27001資安認證作業(112/05)	112年05月由第三方單位BIS執行實地稽核且通過認證，並且每年進行複測。
導入網頁程式防火牆(WAF)	保護網站應用程式，透過監控及過濾網站傳輸的HTTP/HTTPS請求，WAF可比對病毒與惡意程式等網路攻擊，並拒絕可疑、惡意流量進入網站，只讓安全且正常的流量通過，避免遭受惡意攻擊、資料外洩，保障公司網站安全。
防火牆防護	防火牆設定連線規則。

項目	具體管理措施
	如有特殊連線需求需額外申請開放。
使用者上網控管機制	使用者需經申請核准後才可上網，系統自動過濾封鎖使用者上網可能連結到有木馬病毒、勒索病毒或惡意程式的網站。
作業系統安全性更新	透過WSUS伺服器自動派送更新檔到使用者電腦更新。
資料備份機制	資料庫資料及應用程式定期備份。 公用硬碟建立備援機制，每周將重要資料複寫到備援公用硬碟，避免硬碟損壞或中毒時，不會遭受資料遺失。
災難復原	每季執行資訊系統災難復原計劃演練，自備份的檔案資料轉到測試的資料庫，檢查某一系統的資料是否正常。
郵件安全管控	有郵件掃描防護，在使用者接收郵件之前，事先防範不安全的附件檔案、釣魚郵件、垃圾郵件。 個人電腦接收郵件後，防毒軟體也會掃描是否包含不安全的附件檔案。
權限管理	人員帳號權限管理及審核。 人員帳號權限定期盤點。
存取控制	密碼三個月強制更換，且最小長度6碼。 網路硬碟存取依照各單位權限控管。 根據使用者提出隨身碟申請單經主管同意，開放隨身碟使用權限。
系統維運管理	重要系統資源與廠商簽訂維護合約，以維持系統正常運作。
人員教育訓練	一年舉辦兩次員工資安教育訓練。 不定期於公司EIP網站宣導資安事件。 不定期派人參加國內研討會。
資訊安全稽核	每年定期接受內稽、內控文件稽核，外稽(會計師)及中鋼資安稽核。

5.緊急通報程序

(1)資安事件等級說明：

『1』級：屬個別事件受損輕微，作業短暫停頓可立即修復。

『2』級：屬區域性事件造成部分業務中斷，影響整體系統效率。

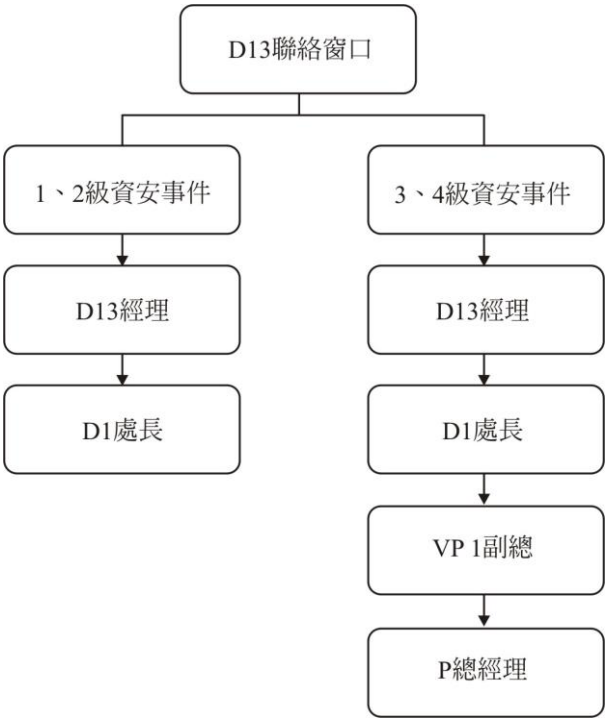
『3』級：屬公司全面性事件，業務全面停頓，影響公司營運。

『4』級：屬重大事故，足以影響公司聲譽及永續經營。

(2)當發生資訊安全事件時，發生單位通報資訊安全窗口，判斷事件等級並找出問題點，即時處理並留下紀錄，程序如下：

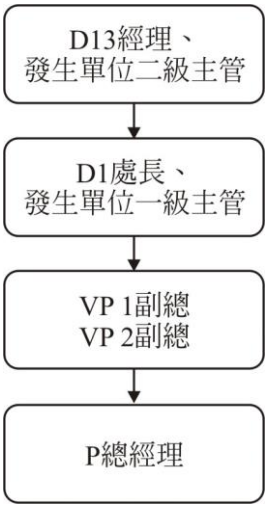
①D13 聯絡窗口應視事件類型採取相對應應變程序因應，以進行異常事件排除，另應將處理狀況持續向相關權責主管報告，並完成通報作業。

②本公司資安事件(IT)等級通報流程圖：



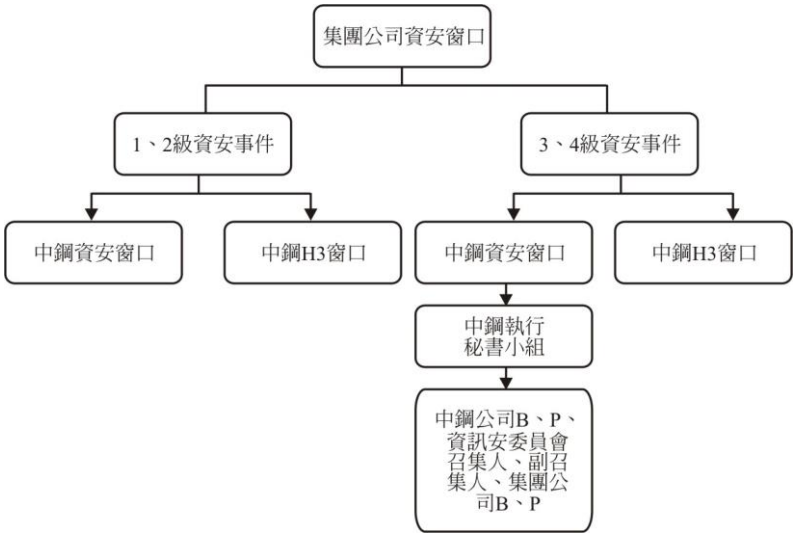
③本公司資安事件(OT)通報流程圖：

以3、4級資安事件通報。



④集團資安事件通報：

集團公司資安通報窗口為D13。資安事件等級及通報流程如下圖所示。



6.資安風險引起生產中斷，造成各單位的影響及因應措施：

檢查網路及系統設備狀況，根據資訊系統運行情況進行判定是否要阻斷對外網路連線，阻擋駭客的入侵及破壞(修復期間電子作業得改為紙本流程，不得影響出貨期程)。

針對網路安全，由資管課排定定期測試計畫，測試內容應包含網路攻擊模擬、特定威脅的定期監控、依賴關係的識別和漏洞的優先等級排序，測試為適用於相關客戶中斷的風險。訓練計畫與執行記錄由資管課留存備查。

(1)緊急處理計畫

步驟	時程	應變處理的步驟	對策內容	預計完成時間	責任者
1	T	啟動會議	查網路及系統設備狀況，探討影響層面。(含出貨予客戶之影響評估)	1HR	D3S/D8S/D13
2	T+1	確認中斷嚴重性	確認中斷時間，根據資訊系統運行情況進行判定是否要阻斷對外網路連線，阻擋駭客的入侵及破壞，將傷害降低。 依影響出貨之評估結果，確認是否立即將出貨作業由ERP系統作業改為人工手動作業。	1HR	廠長
3	T+1	確認系統狀況	根據以上狀態了解各單位系統使用的需求、資源需求(人力、時間)。	1HR	各單位
4	T+2	確認供應	IT系統確認復原前，為使仍能如期供貨，採用紙本作業並以人工複查方式，確保品質狀況無虞。 (1)電腦訂單(D5)、出貨內聯單(D5)、發貨通知單(D24)改採傳真後電話通知，傳遞至權責單位。 (2)產品以人工手動記錄及清點方式，管理入出庫數量。(D81/D31、D823/D323)(若僅有網路癱瘓，電腦仍可使用，可以excel等軟體輔助登記，若無電腦可使用，則以手寫紙本登錄) (3)產品品質狀況由品質保證室出具word檔品質分析報表(或人工填具數據)，並判定合格等級，交予倉儲組，作為產品檢驗與合格狀況之判定。(D83/D33、D823/D323)	1天	D13 D3S/D8S D5/D2 D24 D81/D31 D823/D323 D83/D33

步驟	時程	應變處理的步驟	對策內容	預計完成時間	責任者
			(4)批號挑選採人工依庫存報表與品質分析報表挑選方式進行。(D3S/D81/D323/D823) (5)出貨之品質證明書或品質分析報告若僅有網路癱瘓，電腦仍可使用，使用word軟體出具品質證明書，經簽核後，以傳真或直接交付方式，交予相關需求人員。若電腦均無法使用，則影印程序書紙本，人工手寫相關出貨資訊與數據，經簽核後，以傳真或直接交付方式，交予相關需求人員。(DD83/D33) (6)收到品質證明書或品質分析報告之單位(D823/D323、D24)依出貨需求，隨貨附上或傳真方式交予客戶，並辦理相關出貨所需事宜。		
5	T+2	通知客戶	向客戶報告中斷事件與因應計畫。	1HR	D2/D5
6	T+3	系統復原	(1)D13進行IT系統的修復。 (2)判定IT系統已無威脅。	1天(依實際狀況)	D13
7	T+4	恢復原作業模式決策	依據D13陳報判定IT系統資訊，判定可恢復原作業模式。	1HR	廠長
8	T+4	恢復原作業模式之通知	資管課通知各單位恢復正常作業模式。 業務通知客戶狀況已排除。	0.5HR	D13 業務

註1：若實際狀況無法與程序內排定時程相符，則依實際狀況調整。

註2：1.DCS軟體：無外網連接，亦無法使用USB做相關更新，故無網路攻擊威脅之風險。

2.製程設備僅PLC(Programmable Logic Controller，可程式化邏輯控制器)盤體之操作軟體：

(1)更新會由中碳儀電工程師(D822/D322)，透過公司電腦連線進行更新。D822/D322人員於個人電腦下載PLC盤更新軟體時，檔案會經過公司USB防毒隨身碟之防毒軟體進行相關病毒掃描與攔截。

(2)PLC盤操作軟體由D822/D322進行備份，若更新PLC盤時發生問題，可重新將備份之舊軟體程式重新載入，不致造成影響客戶之生產中斷。各PLC盤間無相連網路系統，亦不會相互影響。

(2)權責

危機處理小組組成	擔當工作角色	職責
廠長	工廠狀況監督。	工廠狀況確認、報告、恢復原作業模式之決策。
D13主管	確定網路資訊系統狀況、判定系統復原狀況。	系統復原、復原狀況通報。
作業規劃主管	掌握系統維修狀況。	確認成品出貨需求量排程與擬定成品交貨排程計畫。
業務	客戶溝通。	向客戶報告因應計畫。
營業管理課(D24) 生產操作室(D81/D31) 倉儲組(D823/D323) 品質保證室(D83/D33)	緊急應變過程執行之其他單位。	IT系統回復前，依應變方式執行作業，確保出貨順利。

(3)利害關係者溝通流程

優先次序	利害關係者	溝通方式	溝通項目	負責人
1	客戶	電話、E-MAIL	確認可容忍時間	業務
2	工廠	電話、E-MAIL	相關應變過程衍生資訊	D13 D3S/D8S D5/D2 D24 D81/D31 D823/D323 D83/D33