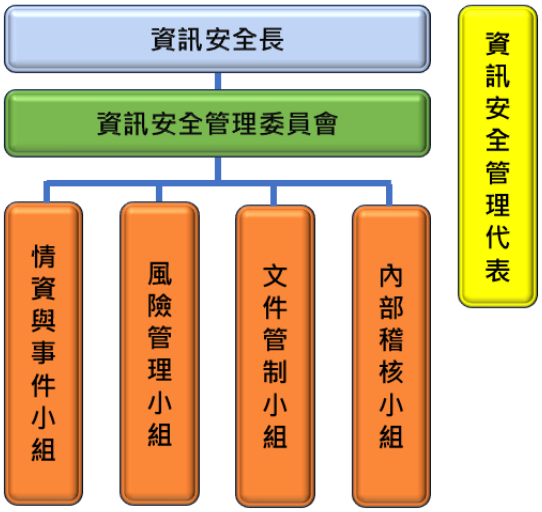
高力熱處理工業股份有限公司

114 年資通安全管理執行情形報告

一、 資訊安全管理架構

本公司於 113 年通過 ISO 27001:2022 資通安全管理系統，目前證書有效期為 113 年 3 月 1 日至 116 年 2 月 28 日。
依照 ISO27001 資通安全管理系統標準之步驟建立資訊安全管理制度，制訂資訊安全政策作為整體資訊安全管理制度之建置開發、實施操作、監控審查及持續維持改進之規範，並依據本公司業務活動與風險，以建立資訊安全管理政策及目標。

資訊安全組織架構:
本公司於 112 年建置資訊安全組織架構，由資訊處同仁擔任各小組成員



二、 資訊安全目標與政策

本公司資訊安全目標為確保重要及核心系統之機密性（Confidentiality）、完整性（Integrity）、可用性（Availability）及遵循性(Compliance)。並依各階層與職能定義及量測資訊安全績效之量化指標，以確認資訊安全管理系統實施狀況及是否達成資訊安全目標。

- 機密性:應避免本公司任何敏感資訊洩露於網際網路。
- 完整性:應確保本公司敏感資料（如:財務資訊、人事資料、系統資訊）之正確性。

- 可用性:應確保本公司所持有的重要資料確實備份。
- 遵循性:應確保本公司避免違反法律、法令、法規或契約義務對資訊安全之要求，

為達成本公司之任務目標及最高管理階層對資訊安全之期許與要求，確保本公司資訊資產之安全，資訊安全政策訂為：

1.確保本公司相關業務資訊之機密性， 防止本公司機密資訊及個人資料外洩與遺失。

2.確保本公司相關業務資訊之完整性與可用性，以正確執行本公司作業與各項業務。

3.確保本公司相關業務資訊之遵循性，防止本公司違反法律法規與合約。

三、 資通安全管理方案

管理事項	作業說明
1.資訊安全管理	● 每年定期施做資訊資產盤點 ● 重要資產簽訂維護保固合約 ● 重要系統及資料進行本地備份、異地備份或雲端備份機制。
2.人員管理及教育訓練	● 新進同仁資訊安全宣導訓練。 ● 不定期針對各類資訊安全事件進行宣導。
3.實體及環境安全管理	● 資訊機房設有門禁控制，確保人員進出均有授權及記錄。 ● 資訊機房設有環控系統，破窗感應及溫溼度監控。 ● 資訊機房設有監視器系統保護
4. 電腦系統及網路安全管理	● 管控外部及個人設備不得私自連接公司網路。 ● 每日檢視防毒及端點防護軟體，並確保更新之即時性。 ● 設置新世代網路防火牆，設定連線規則，確保使用安全。 ● 每日檢視系統狀態及備份環境 ● 建置特權帳號系統管理 ● 郵件系統防護，建置垃圾郵件過濾主機、病毒威脅防護
5.系統存取控制安全	● 每半年進行系統帳號權限盤點 ● 系統帳號權限，皆須進行申請才可開放使用
6.威脅與漏洞管理	● 2023/06 加入 TWCERT/CC 收集各項威脅情資，並進行內部查核及修正。 ● 每半年進行主機弱點掃描及重大漏洞修補更新。
7.營運持續運作	● 每年至少進行一次營運持續運作計畫之測試及檢核

四、 資通安全認證 ISO27001

為維護公司資通之機密性、完整性、可用性與適法性，以及強化資通安全事件之應變處理能力，確保公司與客戶之資訊資產安全，本公司已於 112 年底通過 ISO 27001:2022 資通安全管理系統認證，證書有效期限為 116 年 2 月 28 日。

五、 董事會資通安全管理報告

本公司於基於資訊安全風險管理重要性，每年就資訊安全管理執行情況定期向董事會報告。2025 年向董事會報告日期分別為 114 年 8 月 7 日與 114 年 12 月 18 日。

六、 資通安全管理執行情形

事項	2025 實績	執行項目
重大系統妥善率>= 95%	99.84%	重大系統包含 ERP/MES/資訊網路 之無法提供服務時間<=5%
資訊安全事件數≤ 2 件	0 件	TWCERT/CC (台灣電腦網路危機處理暨協調中心)威脅情資定期查檢，本年度資訊安全通報事件 <=0 件.
營運持續演練計畫:	1 次	依 ISO27001:2022 規範,每年執行至少 1 次，且符合 BIA 營運衝擊分析指標。
資安宣導覆蓋率≥ 90%	100%	定期進行資安宣導

七、 資安事件

事件類型	同仁通報事件	查核後資安事件
統計	4 件	0 件 (通報 4 件皆為誤判之虛驚事件)

八、 資通安全管理資源投入

2025 年本公司投入於維護資通安全管理系統，年度費用為 378 萬元。

資訊安全範疇	技術控制	效益
Identify (識別)	1.Radius Server (MAC 驗證) 2. 資產管理系統	1.管制未知設備接入公司環境 2.管理已知資產設備及端點安全控制

Protect (保護)	1.卡巴斯基防毒軟體 2.Coretex XDR 端點防護 3.CyberAKR 特權帳號系統 4.對外 次世代防火牆 5.Server Farm 次世代防火牆 6.SPAM 郵件防禦系統	1.保護端點-防範已知病毒碼威脅 2.保護端點-異常行為偵測/調查/阻斷攻擊 3.避免同仁電腦被駭進而擴散感染 Server 4.保護內、外部入侵防護 5.保護內、外部入侵與橫向擴散防護 6.過濾垃圾信件
Detect (偵測)	1.N-Reporter 日誌智慧防護 2.外部 次世代防火牆 3.ServerFarm 次世代防火牆	1.核心設備行為分析、異常警示 2.偵測內、外部入侵防護 (Client 環境) 3.偵測內、外部入侵防護 (Server 環境)
Respond (應變)	1.N-Reporter 日誌智慧防護	1.日誌關聯，資安事件回溯/應對/取證
Recover (復原)	1.VeeamBackup 2.VirtasBackupez 3.雲端備份空間 4.MAE 系統	1.災難還原-虛擬化主機環境 2.災難還原-MES 系統 3.異地備份空間 4.郵件備份系統