一、資安管理架構與權責

本公司依照內部資通安全事故管理辦法設置資安小組共計 7 人，負責執行資通安全事件之預防、通報與應變處理等相關作業。

成員與權責如下：

職務	成員	人數	權責
召集人	法務長或副總級主管	1	督導應變計畫執行成效、核定資安事件應變處理事宜
資安主管	資訊部門主管	1	資安政策制定、推動與執行
資安處理人	資訊部門成員	4	維護及執行資安防禦、判斷與緊急應變資安事件
內部稽核人	稽核部門成員	1	實施資通安全稽核、評估資安風險、提出改善建議

二、資通安全政策

為使本公司業務順利運作，防止資訊或資通系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，並確保其機密性（Confidentiality）、完整性（Integrity）及可用性（Availability），特制訂本政策，以供全體同仁共同遵循，本公司的資通安全目標如下：

1. 應建立資通安全風險管理機制，定期因應內外在資通安全情勢變化，檢討資通安全風險管理之有效性。
2. 應保護本公司所提供軟硬體系統機敏資訊及資通系統之機密性與完整性，避免未經授權之存取與竄改。
3. 應經常性告知（以書面電郵、現場培訓或其他形式）定期或不定期對各部門主管、董事會所有會員及獨立董事、暨各部門高階主管關於資訊安全系統之重要性；並不定期向彼等人員宣導關於本公司核心資訊安全系統韌性之重要性，暨各該部門或單位人員應配合管控及執行本公司資訊安全系統之各項程序與辦法，確保本公司業務持續營運，以達成永續發展目標。
4. 因應資通安全威脅情勢變化，辦理資通安全教育訓練，以提高同仁之資通安全意識，同仁亦應確實參與訓練。
5. 為因應緊急狀況之情事發生，本公司應訂定核心資通系統復原計畫，以確保各種不可抗力事由發生時，核心業務仍可持續運作。

三、資通安全管理實施狀況

為確保本公司資訊安全管理的有效性，以下為實際執行狀況。

■ 投保資安險，責任限額 200 萬美金。

■ 近期於 2024-11-01 召開資訊安全管理審查會議，並依據【ISMS-2-02 資訊安全實施程序】每年 10-11 月定期召開，亦可納入現行 IS9000/IATF16949 管審會一併召開，獨立資安相關報告。

■ 公司每位同仁每年都需要完成一次資安教育訓練，資訊部門資安小組(含主管)每年需接受一次(含以上)外部教育訓練

- 執行績效
  - 內部稽核之不符合事項與矯正措施（不符合事項:4 ,已改善:4)
  - 資安事件通報統計 2024/01~2024/10 發生資安事件總計 0 件
  - MDR 系統 10 月份紀錄 除一筆 MIS 測試用資料外，其餘均已正常結案
- 目標執行 ：
  - 降低資安事件發生機率，避免機密資料外洩。
  - 減少任何中斷營運的情況發生
  - 即便營運中段也能在最短時間內恢復

■ 於 2025-02-13 取得 ISO/IEC 27001:2022 證書。

	目標	監測資料收集清單	本次監測發現異常項目	備註
1	發生個資外洩資安事件 ≦1件/年	1. 依據內部系統監控通報 2. 依據是否遭受外部威脅	至目前無發現異常	
2	全公司年度資安教育訓練 1次/年	教育訓練執行記錄	2024年9/30~10/15已完成全公司之年度資安教育訓練	
3	主機弱點掃描主機弱點掃描 一次/年	弱點掃描報告	2024年共執行三次 ，雖有發現部分Critical 與High 風險問題，但已經依情節輕重處理。	
4	符合公司之威脅情資及處理記錄 >5筆/年	檢視資訊申請單等威脅情資記錄。	2024年9月份至今開立7張單據已處理完成7張。	

四、資安事件通報與因應流程

發生資安事件時，各單位應依循下列步驟進行處置，並保留系統異常、入侵、破壞之軌跡證據，供後續還原現場與蒐證使用。

- ■ 發現與通報：由資訊部門成員主動發現或由使用者通報資訊部門成員系統運作異常。
- ■ 確認與分類：資訊部門成員應立即確認其受影響範圍以及資安事件類別。
  可分為：資料外洩(破壞與刪除)、病毒(木馬、勒索軟體)感染、駭客入侵、網路骨幹與系統服務中斷、天然災害或火災、斷電、硬體故障等。
- ■ 控制與處理程序

資安事件類別	因應流程
資料外洩(破壞與刪除)	現資料遭人蓄意或因作業不慎導至毀損、刪除之事件時，應迅速查明資料受損程度，啟用備份資料並即刻依照還原計畫執行資料還原，恢復資料存取。
病毒(木馬、勒索軟體)感染	應立即中斷受感染設備之網路連線，達到實體隔離，避免感染程度擴大。同時應儘速取得清除程式、或系統漏洞修補程式，完成病毒清除與漏洞修補。
駭客入侵	應立即中斷實體網路連線，拒絕入侵者任何存取行為、避免機敏資料外洩，或 成為中繼跳板站台。同時查詢被入侵之設備與系統，是否因安全性漏洞尚未修 補，或防火牆規則設定不當而產生入侵之行為。修補前應儘量保留相關入侵軌跡與記錄供日後調查，保存記錄後隨即進行修補或調整等措施。
網路、主機及系統服務中斷	應立即查明損壞點，與影響範圍。並切換備援機制，縮小受影響範圍與時程。 如有簽訂維護合約者，應立即通知維護廠商進行除錯或重建，無簽訂維護合約者，應立即緊急採購備品進行汰換。
天然災害或火災、斷電等突發事件	應以人員安全為第一優先考量，待事件排除後，評估受損程度，確認是否啟動備援或還原機制。

- ■ 外援：如超出廠內資訊能力可復原、軌跡保存、蒐證、等作業時，應儘速委託外部技術之專業廠商進行處理。
- ■ 應變測試：針對相關事故與處置，每年至少需要一次演練測試，並將過程與結果紀錄，並針對找到的問題做適當的改進與修正。

五、持續改善

- 資訊安全要求事項納入新進員工資安宣導。
- 逐年納入其他分公司導入 ISMS
- 於新的委外維護合約納入 ISMS 的要求(從委外契約書、測試、維運各階段的 ISMS 要求事項)。
- 資訊安全一般人員通識課程(提升資安意識)納入每年教育訓練，並擴及全聚鼎集團