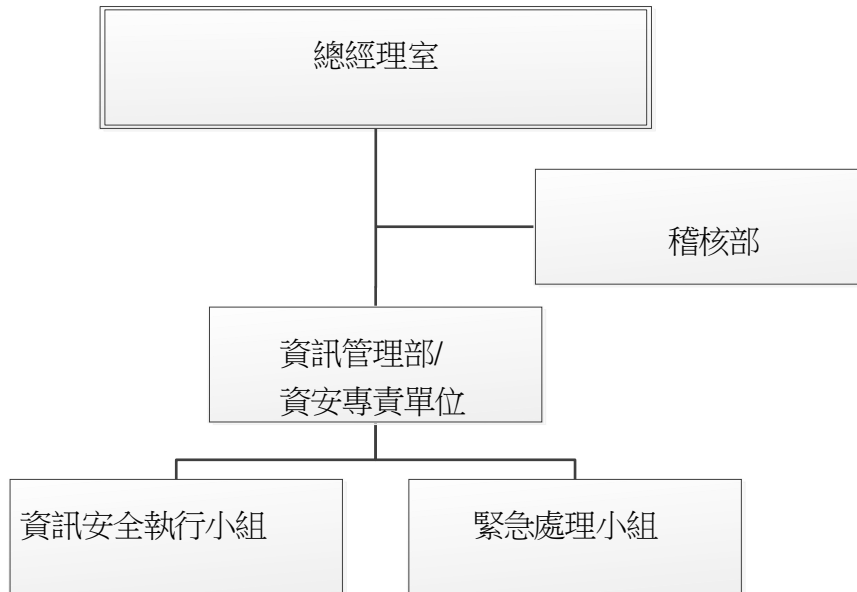


資通安全管理之資訊揭露

（一）資通安全風險管理架構

為積極推動鼎基先進材料股份有限公司(以下簡稱我司)資訊安全政策，並透過合理的責任分派、有效的資源管理提升資訊安全管理制度(以下簡稱 ISMS)之有效性，於民國 112 年特成立資訊安全專責單位，期使達成 ISMS 既定之目標，確保我司資訊業務正常運作。



資訊安全專責單位，主要負責資訊安全管理制度之維護與落實，權責範圍包括下列各項：

- 3.1.1 資訊安全政策修訂審查。
- 3.1.2 資訊安全管理制度之管理審查。
- 3.1.3 各單位資訊安全事項權責分工之協調。
- 3.1.4 資訊資產面臨威脅與風險之監督。
- 3.1.5 採用之資訊安全技術、方法及程序之協調研議。
- 3.1.6 資訊安全事件之監督及檢討。
- 3.1.7 矯正措施改善之監督。
- 3.1.8 其他重要資訊安全事項之協調研議。
- 3.1.9 每年定期召開管理審查會議。

資訊安全執行小組應藉由「ISMS 有效性量測表」之量測項目與目標水準建立 ISMS 績效指標，蒐集各項量測項目之相關資料，據以評估資訊安全目標之達成情形。

（二）資通安全政策

第一條 目的

「鼎基先進材料有限公司」為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本公司之資訊業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。

此政策規範由最高管理階層擬定，藉有效的系統運作，包含各流程持續改善，以預防不符合事項，以達到資訊安全之目的。

第二條 適用範圍

設定為資訊機房維運及系統維護之安全管理，已充份掌握資訊運作及管理過程並滿足各項安全要求與期盼。

本公司之內部人員、委外服務廠商與訪客皆應遵守本政策，以避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本公司帶來各種可能之風險及危害。

第三條 目標

維護本公司資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由全體同仁共同努力來達成下列目標：

- 一.保護本公司業務活動資訊，避免未經授權的存取。
- 二.保護本公司業務活動資訊，避免未經授權的修改，確保其正確完整。
- 三.宣導員工資訊安全之意識與強化其對相關責任之認知。
- 四.實施資訊安全內部稽核制度，確保資訊安全管理之落實執行。

第四條 責任

- 一.本公司的管理階層建立及審查此政策。
- 二.資訊安全管理者透過適當的標準和程序以實施此政策。
- 三.所有人員均須依照相關安全管理程序以維護資訊安全政策。
- 四.所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。
- 五.任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本公司之相關規定進行懲處。

（三）具體管理方案

1. 建立防火牆：提升公司在防禦外部攻擊以及確保內部機密資訊防護的能力。
2. 增進網路及應用安全：提升端點設備的異常偵測及防護能力，包含防毒軟體、資安更新修補(Patch)機制。
3. 教育訓練：進行全員資安教育訓練，以提升資安意識，使資安的運作在高階主管與各部門的支持下，落實到每一位員工身上。
4. 風險管理程序:我司依據歷史性資料、經驗、利害相關者回饋觀察、預測與判斷資訊來源，將各資訊系統可能之風險分類，並建立「資訊資產風險評鑑清冊」。資訊安全執行小組每年召開會議檢討可接受風險值，可接受風險值

得考量本所環境及作業之安全需求作適當調整。

5. 存取控制管理:公務於公司外部使用「安全連線」存取公司內部服務。需具完整連線存取活動記錄，連線之前必須取得授權和身份驗證。確保管理遠端存取會話的機密性和完整性。並可以隨時依資安要求立即停用遠端存取。我司採用 MFA 多因子認證機制建立安全存取連線，公司外對公司內需透過防火牆進行多因子認證取的授權方可連線公司內部服務。
6. 行動裝置管理(Mobile Device Management, MDM):智慧型手機都需安裝 MDM 納管，既遺失或失能時可遠端刪除其內資訊。保管人須負保管及狀況通報責任。

(四) 投入資通安全管理之資源

民國 112 年企業資訊安全措施推動執行成果

1. 專責人員：設有專職之資安專責人員、專責主管，負責公司資訊安全規劃、技術導入與相關的稽核事項，以維護及持續強化資訊安全。
2. 教育訓練：所有新進員工到職前皆完成資訊安全教育訓練課程；全體員工皆每年定期完成線上資訊安全教育訓練及考核。
3. 資安公告：定期宣傳資安防護重要規定與注意事項。
4. 多因子認證機制(Multi-factor authentication ,MFA)：MFA 多因子認證機制建立安全存取連線，公司外對公司內需透過防火牆進行多因子認證取的授權方可連線公司內部服務。
5. SSL 憑証：伺服器佈署憑証，有助於確保伺服器之間的所有通信都加密。
6. 防毒軟體：可偵測並調查主機和端點上的可疑活動，對收集的資料執行分析，加強公司的防護。
7. 行動裝置管理(Mobile Device Management, MDM)：如果智慧行手機遺失/被竊/受到損害，可以讓遠端抹除資料。

重大資通安全事件

無

資通安全風險與因應措施

鼎基先進材料股份有限公司於民國 112 年成立資安專責單位，主要管理公司內風險，並評估資安相關風險等級及威脅弱點，並訂定風險管理方案及定期檢討。

面對惡意駭客的勒索病毒、病毒感染，不僅可能使公司暴露於資料外洩及風險外，也可能造成系統中斷而造成嚴重營運損失。故建立了一套完整的防禦架構。其中包含防火牆、入侵偵測、防毒系統、修補程式管理及備份備援等，以確保持續提升資安防禦能力。