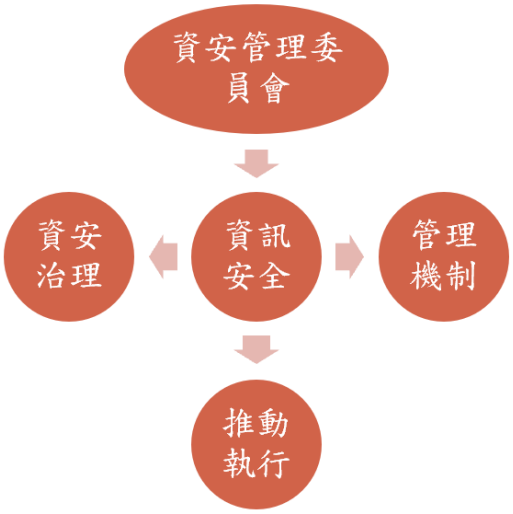
資通安全管理政策

（一）資通安全管理策略與架構

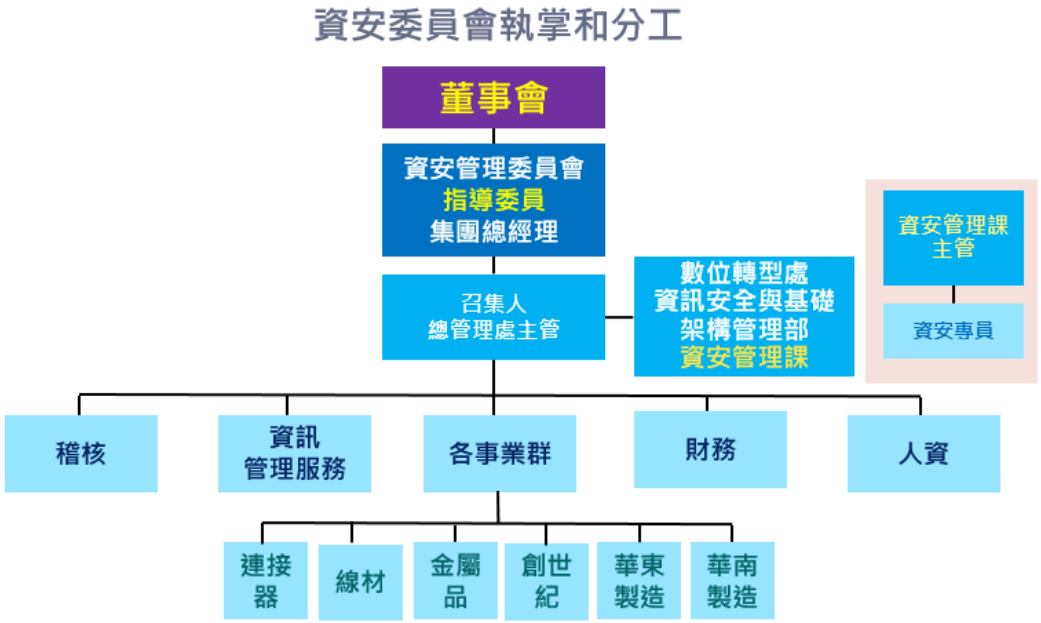
1. 宏致資訊安全管理委員會

因應強化公司資訊安全管理，於民國 109 年 10 月成立「宏致資訊安全管理委員會」，由集團總經理擔任指導委員，總管理處最高長官擔任召集人，公司內各單位最高領導階層為委員會成員，資安管理課主管負責審視各子公司資安治理政策，監督資安治理運作情形，並定期向董事會報告資安治理概況。



2. 宏致資訊安全管理委員會組織架構

成立資安管理課並編制資安專責主管及專責人員，召開資安服務管理會議每季至少一次、集團資安管理委員會會議每年至少兩次、向董事會報告治理概況每年至少一次。



3. 資通安全政策

(1) 宏致集團全球員工及約聘僱人員皆須遵循下述宏致資訊安全政策:

(2) 具體管理方案：

(a) 網路使用政策：導入次世代防火牆、控管上網行為與啟動先進網路防護機制、管控跨廠傳輸避免病毒擴散。

(b) 電子郵件使用政策：嚴謹管控垃圾郵件、導入 APT 防護機制、加強宣導、實施社交安全演練、更新郵件系統提升自身防護力。

(c) 電腦使用政策：控管使用端電腦權限、禁用不合規軟體、汰換老舊不安全作業系統、落實漏洞修補、管制卸除式儲存媒體。

(d) 防毒防護佈屬政策：導入伺服器防毒系統、落實防毒軟體佈署、病毒碼與防毒版本即時更新。

(e) 密碼原則：實施密碼複雜性原則、強制定期變更密碼、啟動異常使

用鎖定機制。

(f) 資訊備份/還原政策:除了基礎系統備份機制,導入高可靠性備份系統避免資料被篡改,且規劃異地及雲端加密備份方案;實施重要服務定期災難還原演練。

(g) 系統事件管理政策:建置自動告警機制,降低災難擴散與縮短服務中斷時間。

(h) 遠端存取政策:控管內部遠端存取權限、管制內外資訊傳輸、禁用 P2P 遠端控制軟體。

(i) 特權帳號管理政策:將特權帳號集中管理,使用電子保險箱保管密碼,定期自動更換密碼,使用帳號需申請,並透過系統待登入且全程紀錄使用內容。

(j) 端點安全防護政策:導入 EDR,實施全面條件式應用程式管控,透過政策稽核提高可視性,遏止攻擊橫向移動。

(k) 零信任網路政策:阻攔未經許可設備連接公司網路,要使用公司網路需經過申請及審核。

(3) 檢討與持續改善:

(a) 加強員工對社交工程攻擊的警覺性、定期不定時進行資訊安全演練、舉辦資訊安全課程。

(b) 強化公司資料保護避免公司重要資料外洩。

(c) 評估導入更進階備份機制,避免備份資料遭受破壞。

(d) 持續加強防毒防駭能力。

(e) 持續將實體主機虛擬化,縮短災難復原時間、符合永續經營。

(f) 每年請第三方公司實施系統弱點掃描,並限期修復重大弱點。

(g) 每年請第三方公司實施滲透攻擊演練,以提升資安防禦能力。

(h) 評估導入 ISO27001,提高公司資安等級。

(i) 評估導入多因子認證,降低資安風險,讓攻擊者無機可乘。

(j) 評估導入 SOC 機制,24 小時監控,資安保護滴水不漏

(4) 依資訊安全管制程序(TN-QP-0002)執行:

以維持資訊系統持續運作、防止駭客、病毒等入侵及破壞、避免人為疏失意外、防止人為意圖不當及不法使用、維護實體環境安全。

4. 資通安全目標

(二)資通安全風險與因應措施

公司已建立全面的網路與電腦相關資安防護措施，並導入高可靠性備份系統，然無法保證能完全避免網路攻擊、惡意程式…等迫害，因為這些攻擊以時時更新的非法方式想辦法入侵企業的內部網路系統，進行破壞企業之營運及損及企業商譽等活動為其主要目的，而在遭受嚴重網路攻擊的情況下，公司的系統可能會失去公司重要的資料，生產線也可能因此停擺。儘管如此，公司持續透過評估既有資訊安全規章及檢視程序，以確保時時維持適當性和有效性，以降低被瞬息萬變的資訊安全威脅及推陳出新的風險和攻擊所影響。

(三) 投入資通安全管理之資源

(1) 專責人力：設有專職之企業組織「資安管理課」，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；全體員工皆完成三小時線上資訊安全教育訓練及考核；每年執行至少二次社交工程釣魚郵件測試。

(3) 資安宣導：每年至少四次資安公告，傳達資安防護重要規定與注意事項。

(4) 投入費用：每年持續投入數百萬元在資安相關維護與建置，以強化集團資訊安全。