2.4.2 資訊安全管理與個資保密

▲ISO 27001
(效期2022~2025)

(1) 政策 / 承諾

- 為保護公司產品與服務，避免有未經授權之存取、修改、使用及揭露，以及天然災害所引起之損失，並適時提供完整與可用之資訊，可成致力於資訊安全管理，以確保公司重要資訊財產之機密性、完整性及可用性，並符合相關法令法規之要求，進而獲得客戶信賴、達到對股東的承諾，保證公司重要業務持續運作

資訊安全與個資保護政策		
全員參與、提升資安意識	積極預防、落實資安管理	客戶信賴、確保永續經營
透過全員認知，達成資訊安全人人有責的共識	建置各項資安技術，導入資訊安全管理制度，以PDCA手法持續改進	提供安全及受客戶信賴之生產環境，確保公司業務之永續營運

(2)目標：保障資訊機密性

✧ 資訊安全推動目標：

1.對於公司所儲存或傳遞之資訊採取適當之保護與防範措施

2.降低發生毀損、失竊、洩漏、竄改、濫用與侵權等資通安全事件時之衝擊

3.持續提升各資訊服務系統所有作業之機密性、完整性與可用性

✧ 個人資料保護推動目標：遵循個人資料保護法及位於其他營運地區所適用之個資保護相關法規，蒐集、處理及利用個資，並採取適當安全維護措施，確保合規作業並共同致力於維護個資安全，以保障個資所有人之權益

目標	2024	短期目標 (1~3年)	中期目標 (3~10年; 至2030年)	長期目標 (10年以上; 至2050年)
社交工程郵件年平均點擊率	集團平均點擊率 0.6%	年平均點擊率低於10%，中長期持續擴展核心產品與技術的應用市場，同時妥善保護公司關鍵資產及客戶機密資訊		
涉及個人資料保護相關之申訴件數	0件	無個人資料保護申訴案件發生		

(3) 權責

- 依據內部「資訊安全管理系統手冊」與「個資保護管理制度程序」，適用範圍涵蓋營運本 身、客戶、供應商與涉及個資保護制度相關所有人員等。由銷售市場行銷處負責新案開發、生產時程管控、交期、價格，品保處負責確保產品品質，資安室負責訂定推動機密資訊保護，資訊單位負責執行資訊安全管理制度之各項工作，全體員工遵循公司保密政策

(4) 投入資源

- 增設資安專責人員，統籌資安政策之督導查核、教育訓練及認知提升活動。資訊人員執行各項 資安制度及具體作為、軟硬體設備維運

(5)申訴機制

- 官網提供聯絡資訊、客訴處理流程

(6) 本年度具體行動

❖ 為展現貫徹資訊安全管理決心， 確保所有資訊與資訊系統獲得適當保護， 依照ISO/IEC 27001：2022外部驗證，依照標準之要求建立、記載、實施及維護資訊安全管理系統，並持續改進系統的有效性，效期至2025年10月18日。

隱私權保護

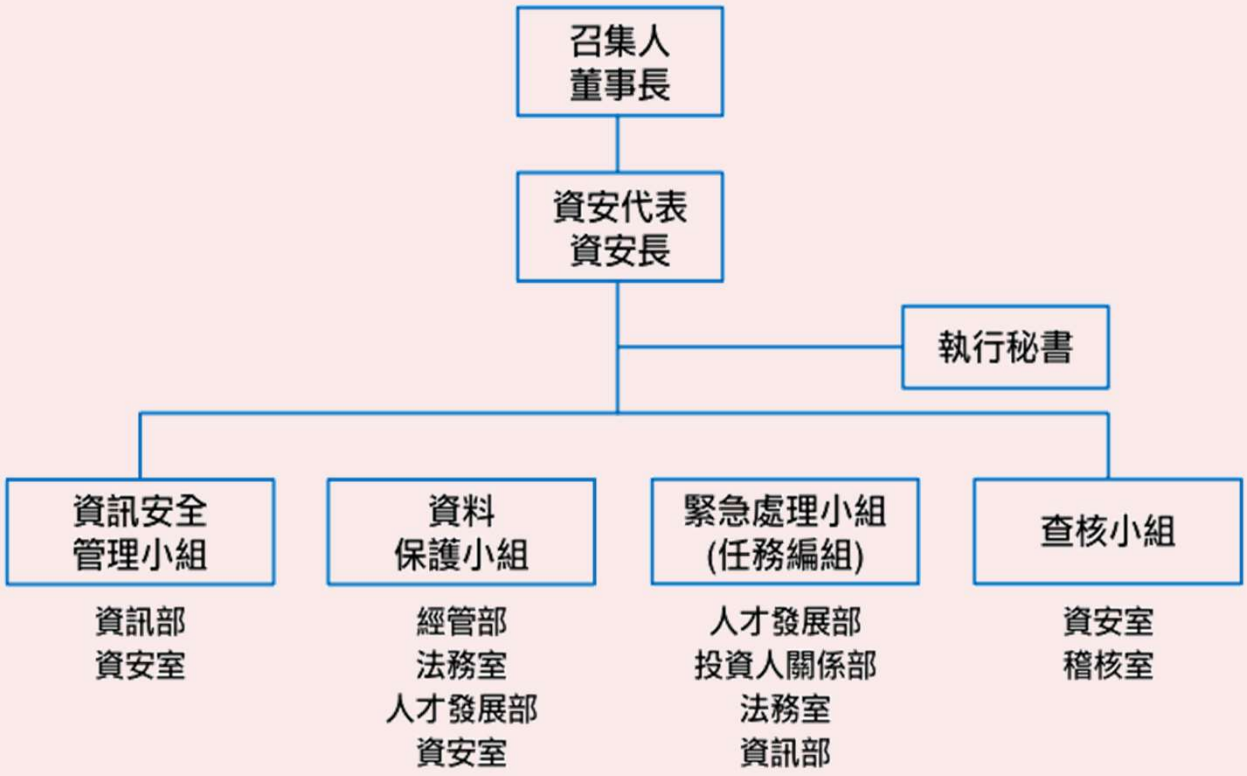
為落實個人資料保護及管理，參照ISO 27001及當地法規相關要求，訂定「個資蒐集、處理及利用管理辦法」，涵蓋對象包含可成集團所有員工、供應商、客戶與涉及個資保護制度相關所有人員等。該管理辦法對個人資料之蒐集、處理及利用等相關事項皆有明確之規範。公司亦安排內部教育訓練及宣導來強化員工對隱私權保護的理解與遵循，內部稽核人員透過定期查核，檢視個資蒐集及管理實際情形，以確保遵守當地法令及公司內部行為規範。

可成瞭解機密資訊對公司本身及客戶而言相當重要，攸關品牌聲譽與客戶信賴度，管理不當亦可能遭致處罰或罰款，因此，可成不遺餘力尊重、保護相關的隱私及機密。對外與客戶、供應商、承攬商、驗證公司等外部單位合作時，會簽訂雙方同意的保密協定，以防機密資訊外洩造成損失。經查本年度並無違反客戶隱私權或遺失、洩露客戶資料而損及客戶權益之投訴事件，及無涉及個人資料保護相關之申訴案件等，彰顯可成內部管理成效。

資訊安全風險管理架構

本公司成立資訊安全推動小組，成員包含召集人、管理代表、執行秘書、資訊安全管理小組、資料保護小組、緊急處理小組(任務型)以及稽核小組，擬訂各項資訊安全發展方向及策略，推動及辦理資訊安全管理之各項工作，以確保資訊安全管理制度持續穩健運作。

- **資訊安全推動小組**：本公司資訊安全之決策管理組織，綜理資訊安全之推動。
- **管理代表**：統籌資訊安全相關議題之制度規劃、資源協調以及專案推行。
- **執行秘書**：協助管理代表及召集人執行資訊安全管理業務。
- **資訊安全管理小組**：負責本公司資訊系統資訊安全管理制度之規劃、建立、實施、維護、審查以及持續改善；向資訊安全推動小組提報資訊安全相關議題，協調確立稽核時程，監督稽核執行以及預防矯正改善等措施。
- **資料保護小組**：負責公司資料及個資保護管理制度之推動。
- **緊急處理小組**：任務編組；監測追蹤重大資訊安全事件發展，維護、更新並執行各項災害復原程序。
- **稽核小組**：訂定資訊安全相關之稽核計畫、執行相關稽核作業、追蹤不符稽核準則事項之預防矯正措施



個資安全管理三大防護措施

針對個資檔案進行盤點及分類，在資料存取、系統存取、網路存取分別設定控管機制

針對涉及個資保護制度相關所有人員進行管理，得要求簽訂保密協定， 善盡保護個資之義務

個資檔案處理之相關設備及週邊環境應有控管保護機制，以確保檔案之安全性，並應用防護及監控軟體進行個資保護及記錄

資訊安全相應機制

可成為確保公司重要資訊財產之機密性、完整性及可用性，建立全面的網路與電腦相關資安防護措施，但無法保證其控管或維持公司製造營運及會計等重要企業功能之電腦系統，能完全避免來自任何第三方癱瘓系統的網路攻擊，為了預防及降低此類攻擊所造成的傷害，公司積極規劃、建置資訊安全措施，持續改善資訊安全環境，降低資訊安全風險，於各層面建置相應機制如下：

類型	說明	相關控制措施
管理管制度	建立資訊安全理制度	• 依照國際資訊安全管理標準ISO 27001:2022，建立資訊安全管理制度
網路與裝毒置安全	潛在弱點與防防駭的防護措施	• 建置次世代防火牆以防護內部網路環境 • 建置垃圾郵件過濾防堵系統 • 建置防毒措施及端點防護機制，定期執行病毒掃描與主動惡意程式偵測 • 定期執行軟硬體弱點掃描及修補更新 • 建置機台入廠掃毒、及應用程式白名單控管機制，防止內含惡意軟體的機台進入公司 • 導入DDoS防護網路流量清洗服務 • 持續強化實施網段隔離策略
應用系統	系統可用狀態與服務中斷時之處置	• 建置系統/網路狀態監控與通報機制 • 建置系統服務/資料之備份與異地備援機制 • 制訂服務中斷之應變措施 • 制訂營運持續計畫並定期演練
存取管控	人員存取內外部系統及資料傳輸管道之控制措施	• 制訂各項帳號權限管理審核機制並定期盤點 • 內/外部資料存取管控與操作軌跡記錄分析 • 建置零信任VPN通道，供員工外部辦公使用 • 建置行動裝置管理系統 • 導入多因子驗證機制
員工訓練	持續建立、宣導及推廣員工資訊安全認知， 以提升資訊安全水準	• 定期/不定期進行資訊安全宣導 • 新進員工資訊安全教育訓練 • 在職員工資訊安全通識課程 • 每季定期執行社交工程演練

資訊安全管理與個人資料保護本年度推動成果

完善資安管理制度

1. 本公司於2024年度完成 ISO/IEC 27001：2022轉版認證作業，證書有效日期至2025年10月18日。可成及海外子公司依照ISO/IEC 27001：2022標準，採用"Plan-Do-Check-Act" (PDCA)循環運作模式，建立與實施資訊安全管理系統，維繫ISO/IEC 27001證書有效性與持續改進
2. 本年度累計召開12場次資訊安全管理會議
3. 依據現行作業流程並考量資訊安全管理體系之運行，合計共修訂57份文件
4. 強化資料保護之各項管理面及技術面作為
5. 本年度導入個資保護專案，以因應個人資料保護法之法規遵循要求
6. 實施供應商資安查核，以降低風險

強化資安防護行為

1. 本年度共完成10次關鍵資訊系統營運演練，強化營運應變能力
2. 本年度共完成3次資訊安全事件通報演練，強化資安事件應變能力
3. 定期執行全廠域裝置弱點掃描及風險評鑑共6次，本年度針對高風險項目改善完成率達100%
4. 本年度執行外部網站滲透測試，降低漏洞風險，提升網站安全及防護能力
5. 持續接收資通安全情資分享平臺(TWCERT)所提供之最新情資，並運用於公司內相應的資安管理作為，並作為社群之一員，參與相關活動
6. 無涉及個人資料保護相關之申訴件數

提升員工資安素養

1. 依據風險和時事，製作30篇資訊安全宣導文件，持續傳遞資訊安全重要規定和事項。本年度向公司同仁發出資安宣導，累計逾6萬人次
2. 本年度所有員工均完成年度資訊安全及資料保護教育訓練，資安通識課程完訓率100%
3. 本年度集團共執行4次社交工程演練，年平均點擊率0.6%

集團資訊安全教育訓練成果

訓練總人次	訓練總時數
6,490 人次	4,451 小時