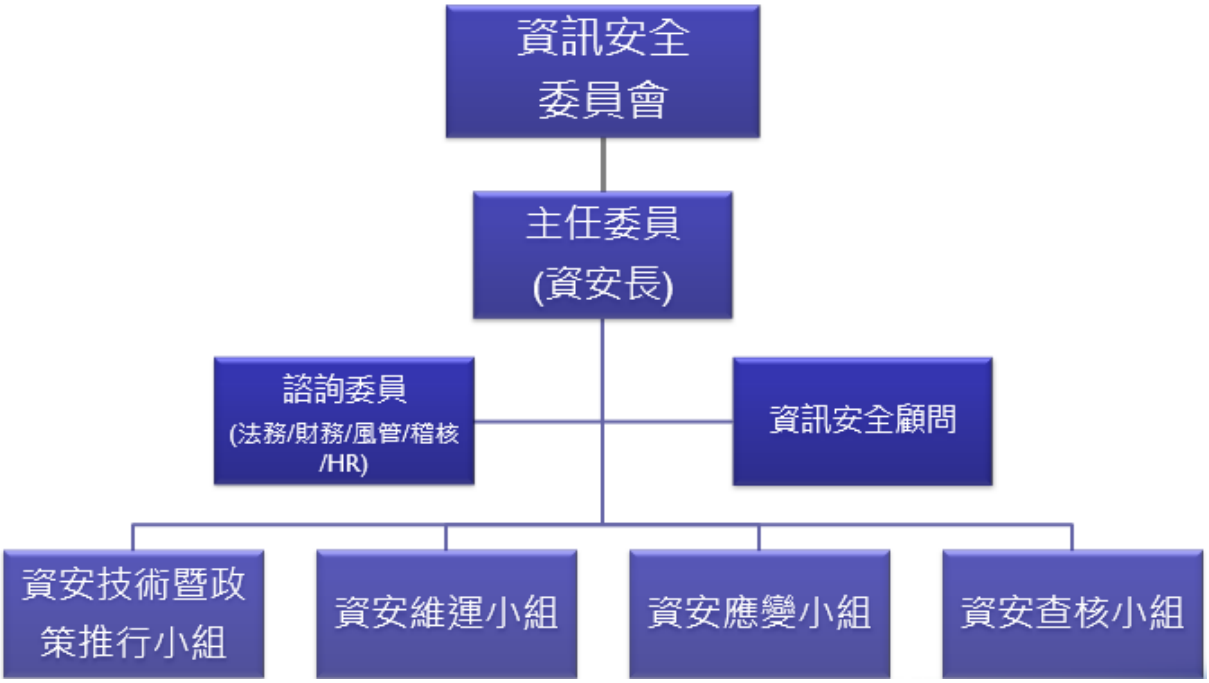
資通安全風險管理

- **資訊安全風險管理架構**

為確保資訊安全管理制度之執行，落實資訊安全政策，本公司已於 2022 年成立資訊安全組織，資訊安全組織架構如下圖所示：



為更完善資訊安全管理及因應主管機關要求，本公司已於 2022 年設立資安長，下轄資訊安全部，設置資安主管及資安人員，其掌理資訊安全治理之推動、建立一致性之資訊安全政策、制定資訊安全管理標準、整合及督導本公司及各子公司資安管理機制之執行、運作、協調等事項。並於 2023 年正式成立資訊安全委員會與資訊安全執行小組。

- 資訊安全委員會：由總經理擔任召集人，資安長擔任主任委員，各事業群一級主管與資訊長擔任委員，負責審查資訊安全政策、檢視公司整體資安管理機制之發展及執行。
- 資訊安全執行小組：包含資安技術暨政策推行小組、資安維運小組、資安應變小組、資安查核小組。由資訊安全委員會之主任委員資安長，負責督導並確保各資訊安全任務正常運作。

- **資訊安全管理委員會審議內容如：**

1. 審查資訊安全政策、檢視公司整體資安管理機制之發展及執行。
2. 重大資安事件之檢討及因應措施。
3. 重大資訊安全維護事項之核定。
4. 跨部門資訊安全事項權責分工之協調。
5. 審查主管機關、董事會及各項資安政策中另有規範或要求需呈報董事會者。

- **資訊安全具體管理方案及投入資通安全管理之資源**

為妥善保護本公司資訊安全管理體系內之資訊資產，對於資訊資產訂定及落實相關規範並執行風險評鑑程序，以確認資訊資產的風險水準，透過風險評鑑結果以及內部會議決定風險事項之處理措施，以達到風險能有效降低、移轉、消除甚至接受該風險。

本公司有建置一套內部掃瞄及監控系統，以確保系統運作有最新的作業更新，以降低被攻擊的風險。採購第三方資訊安全監控系統，分別針對各風險類別的層面、包含網路安全、網路名稱系統健康度、漏洞修補、端點安全、IP 信譽評等、應用程式安全等等進行監控，持續進行資安系統風險分析，並保持在 95 分(滿分 100 分，業界平均 85 分)。

資訊安全策略採用美國國家標準與技術研究所（NIST）提出的網路安全框架 Cybersecurity Framework（CSF），從識別、保護、偵測、回應與復原五大面向，進行資安管理與強化作業。每年會檢視各項法規及評估公司內部的資訊安全規章以確保符合法規及有效性, 並定期宣導相關資安規章，避免同仁違反內部規範造成公司損害。並計畫於 2025 年起，調整採用 CSF 2.0 新的框架。

在供應鏈環境，要求與第三方服務廠商簽訂合約，有要求其遵守保密及網路安全規定。另新人入職時進行基本資訊安全相關訓練外，本公司亦定期舉辦電子郵件社交工程演練，對員工進行電子郵件收發等相關資訊安全知識之教育訓練，以降低員工誤點擊惡意郵件之風險。透過各類課程的進行，除提升同仁資訊安全意識，亦確保資訊安全觀念能融入日常作業中。

2023 年導入 SOC(資訊安全監控中心)：整合並管理各種情況下的資安訊息，對資安事件依管控機制緊急應變，並整合及分析安全事件，以確保資訊安全及防範。同年亦導入 PAM(特權帳號存取管理)：針對特權帳號的存取安全策略，用以控制、監管、保護及稽核企業 IT 環境下的特權身份及活動。

2023 及 2024 皆執行資安紅隊演練：協助公司發現資安缺口、並驗證偵測與應變能力，藉以持續強化改善自身的資安防護能力。同時亦針對紅隊演練發現之問題進行調整及改善，並於覆測後確認問題已獲解決。

- **資訊安全管理制度認證**

本公司為因應現行之資訊安全技術風險，特別導入資訊安全管理制度，全面提升資訊安全防護，並已於 2020 年 8 月取得 ISO 27001 資訊安全國際標準認證，2021 年 8 月通過 ISO 27001 複驗。之後於 2023 年 8 月取得 ISO27001-2013 版續證，並於 2024 年 7 月取得 ISO27001-2022 轉版與續證，**目前證書之有效為 2023/8/16~2026/8/15**。

除了投入對資訊安全防護的軟硬體投資外，本公司同時也極力推動資訊安全管理系統與國際標準接軌，期能進一步提升資訊安全防護機制。並導入多因子認證、移動儲存裝置管制、執行紅隊演練、成立資安監控中心、建置資安情資平台、每年定期執行營運持續管理(BCP)演練及資安事件應變演練，2024 年已執行二次資安事件應變演練(分別於 5 月及 11 月)、及持續改善各項資訊安全管理維運作業，以達成符合「機密性」、「完整性」、「可用性」之資訊安全管理目標，並期有效降低可能之資訊安全事件衝擊，提升企業形象與競爭力。

- **2024 年度執行情形：**

1. 資訊安全管理委員會（每半年一次）召開，於 2024 年度分別已於 3 月、6 月、9 月、12 月召開 4 次會議，並定期（每季一次）向董事長及總經理（或召集人）彙報管理成效。
2. 本公司一年至少一次向董事會/審計委員會彙報資安管理成效、資安相關議題及方向，已於 2024 年 11 月執行報告。
3. 本公司內部每年定期推行「資通安全教育訓練」線上課程，課程內容包括：近期重大的資訊安全事件、資訊安全認知宣導、社交工程安全、勒索病毒、2024 年資訊安全趨勢，並以課後測驗檢視同仁之學習成本，2024 年度相關教育訓練課程計 2022 人次，合計 2022 人時。