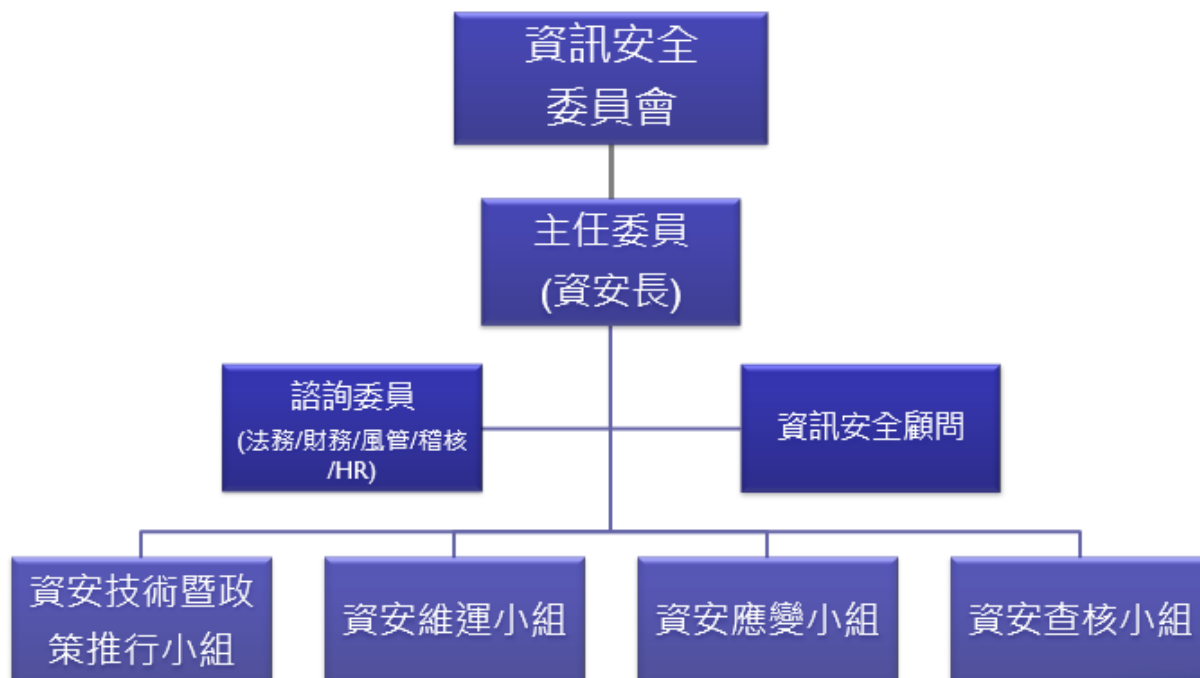


資通安全風險管理

● 資訊安全風險管理架構

為確保資訊安全管理制度的執行，落實資訊安全政策，本公司已于 2022 年成立了資訊安全組織。以下是資訊安全組織架構示意圖：



為更完善信息安全管理及因應主管機關要求，本公司已于 2022 年設立資安長，下轄信息安全部，設置資安主管及資安人員，其掌理信息安全治理之推動、建立一致性之信息安全政策、制定信息安全管理標準、整合及督導本公司及各子公司資安管理机制之執行、運作、協調等事項。并于 2023 年正式成立信息安全委員會與信息安全執行小組。

- 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机制之發展及執行。
- 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机制之發展及執行。
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。

- **资讯安全具体管理方案及投入资通安全管理之资源**

为妥善保护本公司资讯安全管理体系内之资讯资产，对于资讯资产订定及落实相关规范并执行风险评鉴程序，以确认资讯资产的风险水准，透过风险评鉴结果以及内部会议决定风险事项之处理措施，以达到风险能有效降低、移转、消除甚至接受该风险。

本公司有建置一套内部扫描及监控系统，以确保系统运作有最新的作业更新，以降低被攻击的风险。采购第三方资讯安全监控系统，分别针对各风险类别的层面、包含网路安全、网路名称系统健康度、漏洞修补、端点安全、IP 信誉评等、應用程式安全等等进行监控，持续进行资安系统风险分析，并保持在 95 分(满分 100 分，业界平均 85 分)。

资讯安全策略采用美国国家标准与技术研究所 (NIST) 提出的网路安全框架 Cybersecurity Framework (CSF)，从识别、保护、侦测、回应与复原五大面向，进行资安管理与强化作业。每年会检视各项法规及评估公司内部的资讯安全规章以确保符合法规及有效性，并定期宣导相关资安规章，避免同仁违反内部规范造成公司损害。并计划于 2025 年起，调整采用 CSF 2.0 新的框架。

在供应链环境，要求与第三方服务厂商签订合约，有要求其遵守保密及网路安全规定。另新人入职时进行基本资讯安全相关训练外，本公司亦定期举办电子邮件社交工程演练，对员工进行电子邮件收发等相关资讯安全知识之教育训练，以降低员工误点击恶意邮件之风险。透过各类课程的进行，除提升同仁资讯安全意识，亦确保资讯安全观念能融入日常作业中。

2023 年导入 SOC(资讯安全监控中心)：整合并管理各种情况下的资安讯息，对资安事件依管控机制紧急应变，并整合及分析安全事件，以确保资讯安全及防范。同年亦导入 PAM(特权帐号存取管理)：针对特权帐号的存取安全策略，用以控制、监管、保护及稽核企业 IT 环境下的特权身份及活动。

2023 及 2024 皆执行资安红队演练：协助公司发现资安缺口、并验证侦测与应变能力，借以持续强化改善自身的资安防护能力。同时亦针对红队演练发现之问题进行调整及改善，并于覆测后确认问题已获解决。

- **资讯安全管理制度认证**

本公司为因应现行之资讯安全技术风险，特别导入资讯安全管理制度，全面提升资讯安全防护，并已于 2020 年 8 月取得 ISO 27001 资讯安全国际标准认证，2021 年 8 月通过 ISO 27001 复验。之后于 2023 年 8 月取得 ISO27001-2013 版续证，并于 2024 年 7 月取得 ISO27001-2022 转版与续证，**目前证书之有效为 2023/8/16~2026/8/15。**

除了投入对资讯安全防护的软硬件投资外，本公司同时也极力推动资讯安全管理系统与国际标准接轨，期能进一步提升资讯安全防护机制。并导入多因子认证、移动储存装置管制、执行红队演练、成立资安监控中心、建置资安情资平台、每年定期执行营运持续管理(BCP)演练及资安事件应变演练，2024 年已执行二次资安事件应变演练(分别于 5 月及 11 月)、及持续改善各项资讯安全管理维运作业，以达成符合「机密性」、「完整性」、「可用性」之资讯安全管理目标，并期有效降低可能之资讯安全事件冲击，提升企业形象与竞争力。

● **2024 年度执行情形：**

1. 资讯安全管理委员会（每半年一次）召开，于 2024 年度分别已于 3 月、6 月、9 月、12 月召开 4 次会议，并定期（每季一次）向董事长及总经理（或召集人）汇报管理成效。
2. 本公司一年至少一次向董事会/审计委员会汇报资安管理成效、资安相关议题及方向，已于 2024 年 11 月执行报告。
3. 本公司内部每年定期推行「资通安全教育训练」线上课程，课程内容包括：近期重大的资讯安全事件、资讯安全认知宣导、社交工程安全、勒索病毒、2024 年资讯安全趋势，并以课后测验检视同仁之学习成本，2024 年度相关教育训练课程计 2022 人次，合计 2022 人时。