信息安全管理政策

信息安全政策

依「公开发行公司建立内部控制度处理准则」第九条「计算机化信息系统处理」之规定制定相关内部作业规定，以降低日新月异的信息科技应用及环境变异所带来未知的资安风险威胁，达方基础信息安全政策管控共有8项。

資訊安全說明：

1. 內外網路存取需通過防火牆 / 病毒牆 / 入侵防禦系統檢查。
2. 所有資訊設備一律安裝防毒 / 防後門軟體。
3. 每 3 個月定期更換使用者密碼，且須符合密碼複雜性原則。
4. 存取任何系統皆需申請帳號並有權限限制的開放存取，離職後帳號刪除。
5. 機密資料調閱，檔案全程加密處理。
6. 所有企業流程需經由電子簽核核准後方能生效。
7. 所有 End-point（用戶終端）資訊設備回收 Admin（管理員）權限，並安裝資產管理軟件和端點安全防護軟體。
8. 定期內外部資訊安全稽核。

信息安全风险管理架构

本公司于 110 年第四季成立信息安全委员会，并设立信息安全长，定期召开信息安全审查会议。除资安委员外，编列负责资通安全管理之同仁，与委员会共同管控信息安全风险并推动各项资安政策、制定及导入资安制度及信息安全风险稽核等工作。委员会组织相关管理架构划分如下：

(1)管理单位：信息安全委员会设定主任委员一名，并由总经理担任。委员若干名，主要由副总级担任。召集人由信息部主管担任，主要负责信息安全委员会组织管理、召集。下设常态编组有：

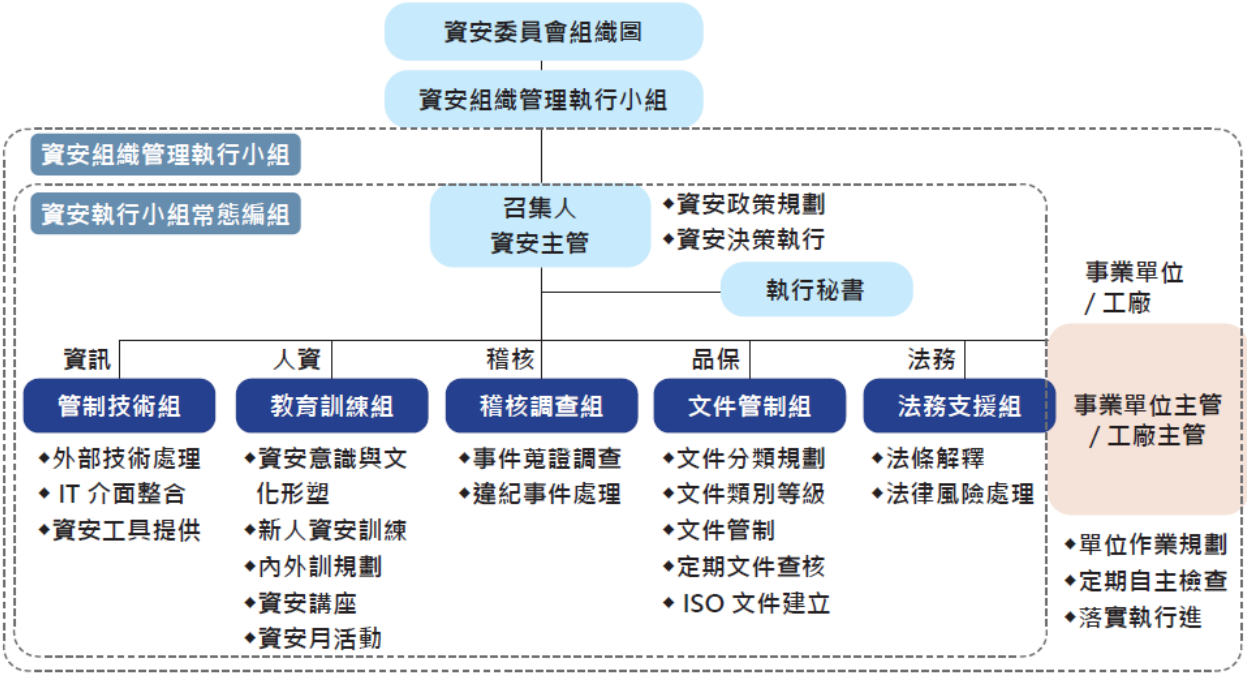
①管制技术组：由信息部担任，负责信息安全技术工作、接口整合及信息安全提供解决方案。

②教育训练组：由人事部担任，负责提升信息安全风险意识、信息安全风险训练及讲座举行。

③稽核调查组：由稽核部担任，负责信息安全风险稽核，异常搜证、调查及处理。

④文件管制组：由质量部担任，负责包含机密文件分类、等级定义、管制及查核。

(2)其它单位：涵盖公司所有事业单位及工厂，主要职责有与资安相关的日常作业规划、定期进行信息安全风险自我检查及落实资安风险改善项目执行。



信息安全具体管理方案及投入资通安全管理之资源

公司为强化整体信息安全，推动相关信息安全强化政策及投入之资源如下：

(1)重大基础信息安全系统建设(97 年~112 年)

- 机房环境安全

①机房自动环保气体消防设施建置。

②机房双回路UPS供电系统。

③机房备援空调系统建置。

④机房全景摄像监控系统建置。

⑤机房24小时环控监控(温度/电力/漏水/空调/门禁/消防等)和实时简讯发报系统建置。

- 系统信息安全

①垃圾邮件防护及邮件进出记录备份系统建置。

②ERP历史数据虚拟化导入，长期保存系统和数据安全。

③透过外部弱点扫描，补强系统漏洞。

④改善外部系统成为加密传输，降低信息安全风险。

- 网络信息安全

①防火墙升级功能IPS入侵检测系统防护。

②专线线路双备援自动切换机制系统导入。

③全公司网络导入禁止任意非法网络设备接入内网系统。

- 主机信息安全

①虚拟化传统架构升级为高容错多复本超融合架构，以强化软硬件的信息安全高可用性。

②服务器全面监控和实时简讯告警系统导入。

③服务器漏洞定期追踪处理。

④全公司信息设备导入端点防护禁止任意非授权软件安装和恶意木马程序植入。

(2)信息安全中长期发展规划(110 年~113 年)

- 信息安全制度

①导入ISO 27001信息安全管理系统。透过ISO 27001信息安全管理系统的定期验证，以落实信息安全政策、保护客户数据及公司智能产出、强化信息安全事件应变能力及达成信息安全政策衡量指针，并已于111年10月取得ISO 27001认证，证书效期至114年11月。

②定期进行社交工程演练，提升同仁信息安全意识。

- 信息安全预警

①导入相关资安预警设备和机制，将内部安全风险黑箱可视化。并结合外部资安情资和分析，针对外部黑客入侵行为能够提前感知，而能先进行相关反制作业。保护企业内部数据和系统的安全。

②定期进行内部弱点扫描，针对漏洞进行预防修补，以降低信息全安风险曝露。

③由外到内渗透测试演练，进行深入的漏洞测试与分析，找出设备及系统的潜在风险，提高安全性。

- 信息安全防护

①导入双因子验证，透过两次验证程序检视用户合法性，以杜绝未授权用户获取公司内部信息或进行破坏活动。

②导入日志管理，收集系统日志集中保存，利于未来信息安全事件追踪、厘清及预防。

③导入特权账号管理，避免内部特权用户滥用遭外部窃取，集中管理并定期稽核，降低入侵风险。

④导入营业秘密数据保护，避免机密资料及关键技术外泄，保障公司核心竞争力。

- 员工信息安全倡导及训练

①公司内部网站不定期倡导信息安全知识。
②不定期以E-Mail发送信息安全公告。
③对新进同仁做信息安全倡导。
④定期全公司资安教育训练
⑤资通安全人员积极参与外部研讨会及进修课程，以提升专业职能并掌握关注议题。

112年信息安全风险管理执行情形已于同年11月向董事会报告，执行情形报告内容如下：

一、管理面：

(1)每年遵循 ISO 27001-2013 资安体系之管理制度执行内稽、管审及验证工作。
(2)111/10 总部及台南厂取得 ISO 27001-2013 ISMS(信息安全管理系统)的认证，112/10 取得大陆 3 厂区 ISO 27001-2013 ISMS 认证。

二、技术面：

(1)111 年起总部、台南厂及大陆淮安厂执行资安监控，112 年推广至苏州厂及重庆厂。包括网络恶意软件检视、用户端计算机恶意活动检视、服务器端计算机恶意活动检视等内部网络的入侵检测资安活动监控。
(2)每月执行外部弱点扫描，每月对弱点进行改善；112/10 完成外部系统渗透测试检测针对弱点进行改善。
(3)公司已建置防病毒软件、网络防火墙、邮件过滤规则、入侵检测及防护等机制。

三、认知及训练面：

(1)资安专业人员在今年完成 80 小时资安专业练课程。
(2)基础架构及网络管理人员接受 ISO 27001 资安体系教育训练。
(3)112/3 及 112/10 执行全体员工的资安通识教育训练。
(4)112/6 完成全公司人员执行社交工程演练，对于上当同仁已执行调训，强化资安意识。

四、未来计划：

(1)遵循 ISO 27001-2022 资安体系的管理制度持续执行内稽、管审及验证工作。
(2)每年评鉴公司各项信息资产的风险值，针对高风险资产持续执行改善工作，降低资安风险。
(3)增加执行 Source code 资安扫描，以找出应用程序的弱点进行修补；强化资安健检工作。