资通安全管理

一、资通安全风险管理架构

由信息管理处负责统筹全公司信息安全及相关事宜，并定期进行内部信息安全检查。

管理架构:

（1） 信息安全之权责单位为信息管理处，本处设置信息主管乙名，与专业信息人员二名，负责订定内部信息安全政策、规划暨执行信息安全作业与资安政策推动与落实。

（2） 本公司稽核室为信息安全监理之督导单位，该室设置稽核主管乙名，负责督导内部资安执行状况，若有查核发现缺失，即要求受稽查单位提出相关改善计划与具体作为，且定期追踪改善成效，以降低内部资安风险。

二、资通安全政策

（1） 目的:

为有效管理公司内部计算机及网络运作环境, 提高软硬件使用效率及其档案文件之安全, 维持业务持续运作, 降低信息作业风险, 保障信息服务用户之权益，建立信息安全管理系统，规范本程序为最高指导方针，以达成信息安全管理的目标。

（2） 范围:

本公司信息安全管理范围，包括本公司所属各据点信息作业之相关人员、管理制度、应用程序、数据、文件、媒体储存、硬设备及网络设施。

（3） 目标:

避免信息系统遭受来自内、外部人员不当使用或蓄意破坏, 或当已遭受不当使用、蓄意破坏等紧急事故时, 公司能迅速应变处置, 并在最短时间内回复正常运作，降低该事故可能带来之经济损害及营运中断。

（4） 程序:

执行信息机房、网络安全、ERP 程序修改、数据安全、信息保密、知识产权、信息委外等管理。

（5） 资通安全稽核管理实施：

信息安全政策订定、信息安全组织与权责、人员安全与管理、资产分类与控管、实体及环境安全管理、通讯与操作管理、访问控制管理、系统开发与维护管理、永续运作管理、内部稽核及其他。

（6） 资通安全稽核依稽核项目：

资通安全稽核依稽核项目逐项检查，并得调阅有关资料、实地测试或检查信息软、硬设备使用情形，受稽核部门及人员应配合提供必要之说明及文件资料。稽核人员对稽核之文件应予保密。

三、具体管理方案及投入资通安全管理之资源

防火墙防护、防病毒软件、内外网管制、档案存取管制、邮件安全管控、网站防护机制、数据备份机制、异地备份存放、检修纪录、资通安全倡导、操作系统更新、定期实施信息安全稽核，落实信息安全管理政策，确保信息数据、系统、设备及网络安全。本公司信息及资安人员共五名，每周固定召开会议讨论管理资通安全，并且每年编列二佰多万用于设备更新、维护、弱扫等服务，降低资安风险。