侨威科技股份有限公司

信息安全管理计划

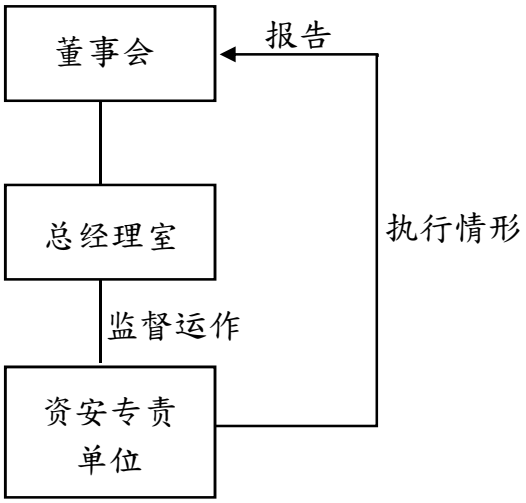
一. 资通安全管理策略与架构

（一） 资通安全风险管理架构

1. 信息安全治理组织:

本公司资安专责单位由信息部负责，目前设置资安主管(信息部主管兼任)，资安人员各一员，负责信息安全政策之制定，执行及风险管理，定期检讨及调整信息安全政策，并向董事会报告资通安全执行情形，确保运作之适切性及有效性。

2. 信息安全组织架构



（二） 资通安全政策

本公司已制订「计算机设备管理、公开信息申报办法、网络与信息管理程序」等作业办法。

1. 保护公司核心资通系统，确保公司的核心业务可以顺畅运作，不受外来干扰中断营运。
2. 员工之工作职掌应作适当区隔，并仅授予完成工作所需之必要权限与必要信息。
3. 定期办理资安倡导教育，以提高同仁之信息安全意识及个人防护能力。
4. 不论客户是在哪一个地区或国家，不论该地区有否立法，妥善保护客户信息及隐私。

5. 不外泄员工个资，落实个人资料保护法。
6. 本公司信息安全措施应符合法律之规范及本公司信息安全相关办法之要求。
7. 所有信息安全规范或程序之建置及修改，须符合并遵循信息安全管理制度之机制。

（三） 具体管理方案

1. 人员资安意识教育训练：定期实施信息安全教育训练及倡导，以提高公司同仁对信息安全之认知及风险意识。
2. 信息系统安全管理：
   2.1公司主机服务器、个人计算机及笔记本电脑统一安装防病毒软件，并自动更新病毒特征，并定期检视更新状况。
   2.2邮件系统建置垃圾邮件过滤功能，恶意邮件侦测功能等，提升整体邮件信息安全。
   2.3应用系统及数据库，每日进行数据备份，每年定期实施系统数据还原演练作业，并监控每日备份结果，以确保数据储存安全性。
   2.4管控各系统管理者权限，规范各系统只能使用公司授权之合法软件，并遵守相关法令规定，非经合法授权及与业务无关之软件，无法安装使用，以确保公司软件授权合规性，并降低使用非法软件感染病毒，后门程序之风险。
   2.5信息系统业务委外时，于事前审慎评估可能潜在安全风险，确保委外厂商执行委外作业时，具备完善之资通安全管理措施。
3. 网络安全管理：
   3.1公司对外服务应用系统以防火墙与外部因特网隔离。
   3.2公司内部办公区域针对无线网络设备进行管控，避免外部人员经由无线网络入侵公司系统。
4. 系统访问控制：
   4.1有新进员工时，人资单位需协助上系统提出申请，通知信息部执行用户之新增其权限，确保系统存取安全。
   4.2当员工调整职务及离职时，人员异动单据需会签信息部门调整或删除其权限，确保系统存取安全。
   4.3内部应用系统依照人员工作需求，由员工使用电子签核系统填写权限申请单会签稽核部门审查，核准后才交信息单位处理执行。

4.4信息系统必需设定账号密码，用户通行密码应符合安全原则，并要求用户定期更改系统密码。

5. 资通安全健诊:

公司每年应办理资通安全健诊，其至少应包含下列项目，并检讨执行情形：

5.1网络架构检视。

5.2网络恶意活动检视。

5.3用户端计算机恶意活动检视。

5.4服务器主机恶意活动检视。

5.5安全设定检视。

6. 资安永续管理与运作:

6.1成立资安专责单位，负责资安政策，管理办法之建立及推行，审议资安问题与因应对策，并要求全体员工确实遵守，维护公司信息安全。

6.2若发生信息安全事件，依资通安全事件等级，迅速通报总经理室、资安主管及资安人员，并进行适当处置及快速执行复原作业。

（四） **投入资通安全管理之资源**

1. 本公司定期检视整体资通安全计划，以应对现在快速发展的信息环境，并加强倡导同仁信息安全概念。

2. 本公司将计算机化信息系统相关控制作业列入年度稽核计划之稽核项目定期查核，以落实资安计划执行。

二. 资通安全风险与因应措施:

本公司已建立资安防护措施，虽无法保证能完全避免资安事件，但是可以最短时间回复信息系统运作使公司核心业务不受影响中断并与时俱进持续改善资安规范，减少公司核心业务受到干扰。

三. 提报董事会日期: 112 年 12 月 28 日