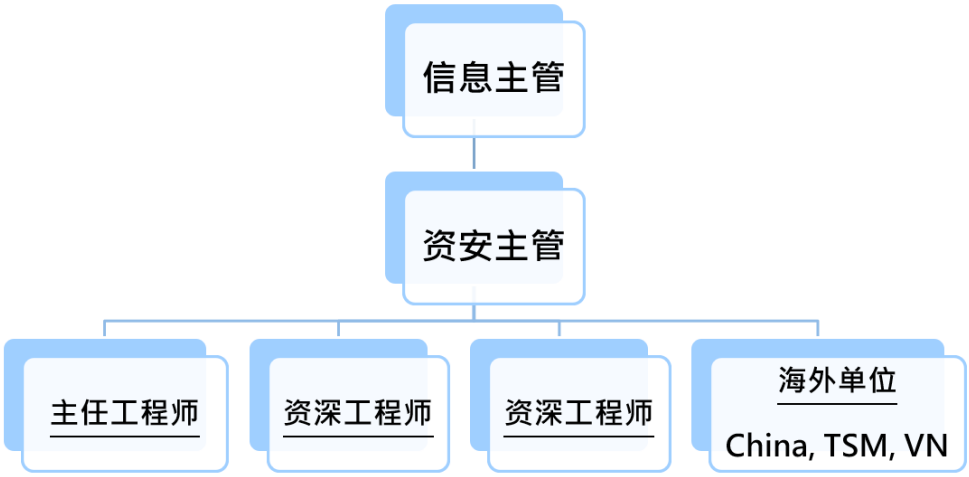
台橡股份有限公司
TSRC CORPORATION

信息安全政策与管理

1 信息安全组织架构

本公司信息安全之权责单位为信息安全组并隶属于信息部，该组织设置信息主管乙名，资安主管乙名与专业信息人员数名，负责规划内部信息安全政策、规划暨执行信息安全作业与资安政策推动与落实，并每年定期向董事会报告公司资安治理概况。



2 信息安全政策

本公司及子公司（以下个别或统称「公司」）内部人员不法、不诚信或不道德行为之检举与处理，适用本办法。

2.1 目的

信息安全政策制定的目的为防御一切有计划的、意外的、来自内部的或外部的威胁，以保护公司重要信息资产之安全。

2.2 范围

信息服务的所有用户都有义务保护公司的技术和信息资产，以防止未经授权的访问、盗窃和破坏。公司的技术和信息资产包含以下：

2.2.1 个人计算机之软硬件及应用
2.2.2 通信网路硬件和软件
2.2.3 系统软件
2.2.4 应用软件
2.2.5 资料：由公司内部各部门使用，包括员工数据、供货商数据、客户数据、物料主文件数据、库存数据、销售数据、财务数据、制造数据及各应用程序计算后产生的数据

2.3 使用者的责任

规范公司所属的个人计算机系统，网络和信息系统等资源的使用政策。

2.3.1 合适的使用权

(1) 公司信息系统上的用户账号仅用于公司业务，不得用于个人活动

(2) 使用者有责任保护其账号所使用和存储的所有机密信息

(3) 使用者不得故意从事以下活动：骚扰其他用户、降低系统的性能、访问他们没有授权的公司信息系统

(4) 用户不得在其个人计算机上附加或使用未经授权的软硬件，除非提出申请且获得主管同意，始得授权使用

(5) 用户必须向公司直接主管报告其个人计算机中可疑的资安状况

2.3.2 网络使用规范

(1) 公司的计算机及网络设备，是公司提供员工执行公司业务之工具，公司因促进资源合理使用、保护公司营业秘密、维护公司权益等目的，得对于员工的计算机及网络设备，进行必要的监督或管理

(2) 员工应于合理的限度内，合法使用计算机及网络设备，不得用以处理个人事务、妨害工作效率、干扰网络流通、占用过多网络带宽或浏览内容不当的网站，亦不得下载、上传、发送或重制有害、非法或任何足以损害公司信誉、权益或致公司应对第三人负法律责任之任何软件、数据或档案

(3) 不得流通含有猥亵、诽谤、计算机病毒、歧视、骚扰等性质之不当或有害信息

(4) 员工之间，非经他人明示同意，不得窥伺、读取或篡改他人计算机内部数据

(5) 研发相关部门的员工，和承包商/外部厂商/顾问必须获得其主管的许可，并向信息单位信息安全管理员提出请求因特网使用权

2.3.3 授权的登入控制

公司信息安全政策的控制，主要须防止未经授权的披露或修改关键信息系统的登入控制，登入控制的基本含义是将权限分配给有权访问特定资源的个人或系统。登入控制主要由登入的账号和密码实现。在重要的信息系统，可以实现进一步的登入限制(例如：双重认证)。

2.3.4 公司网络远程登录

远程连接到内部网络的唯一可接受的方法是使用 VPN 联机。登入 VPN 必须使用账号、密码并搭配多因子认证。

2.4 资安威胁预防措施

2.4.1 员工

员工须对信息安全威胁进行下列必要措施以降低威胁机率：

(1) 若于非企业网络，必需透过 VPN 连入公司网络
(2) 不要使用共享账户。切勿与同事分享登录信息员工应保护个人计算机资产的安全，离开座位时，将计算机系统锁上或关机

2.4.2 信息部

信息部须对信息安全威胁进行下列必要措施以降低威胁机率并缓解资安危害的程度

(1) 终端使用者安全管理措施
(2) 当员工离职或受到纪律处分时，应于规定时间内删除或限制对系统的登入及使用
(3) 定期针对重要系统执行弱点扫瞄。
(4) 监控信息系统的日志并针对可疑事件进行判断及处理
(5) 定期评估最新资安解决方案，以提升公司资安防护能力

2.5 外部厂商信息安全管理规范

办理信息作业委外前，依据公司信息安全政策，检视各类委外作业型态，于信息委外各阶段(事前规划、事中招标、事后维运)，订定相关的信息安全需求，以监督各项信息作业委外安全之进行，预防信息安全事件发生。

2.5.1 事前规划

(1) 需求评估阶段- 信息解决方案需将信息安全纳入考虑
(2) 决定解决方案- 委外建置的信息安全管理措施

2.5.2 事中招标

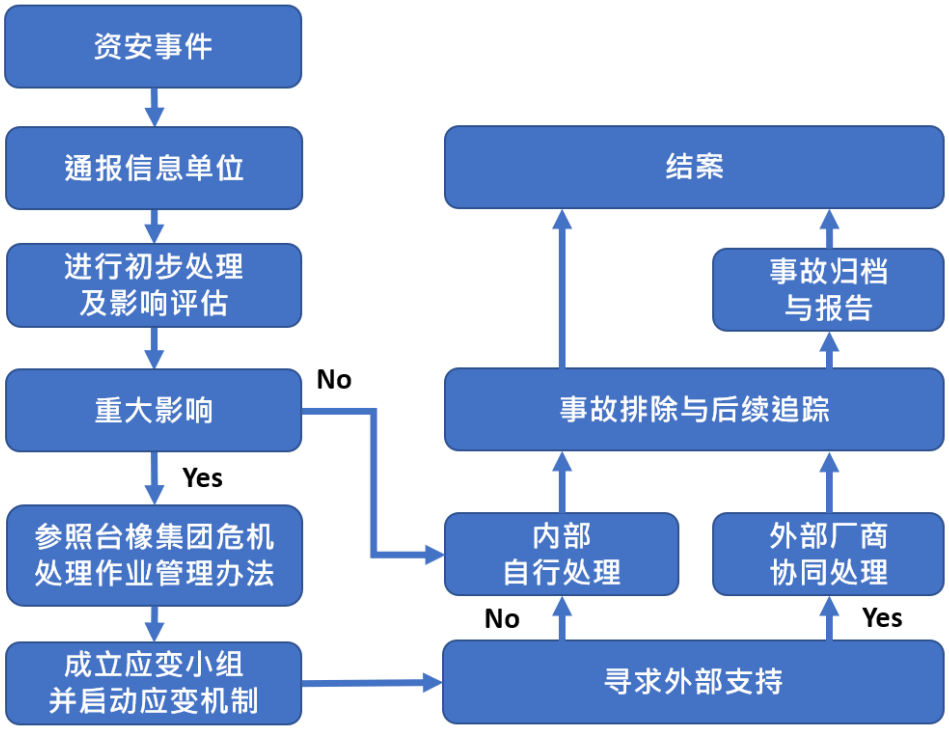
(1) 采购阶段 - 保密合约与服务水平协议
(2) 履行阶段 - 进行信息安全相关验证

2.5.3 事后维运

(1) 信息安全测试
(2) 系统维护
(3) 安全控制与存取管理
(4) 异常事件处理

2.6 资安事件应变

本公司资安事故之通报及处理，皆遵守下列资安事件应变程序进行



2.7 计算机系统复原及作业办法

为确保公司之计算机系统在发生损毁后，能迅速复原维持数据的完整性

2.7.1 服务器及主机将区分为三等级，实施不同等级的备份机制

(1) 第一级服务器为:对公司业务有重大影响，若损坏将影响公司业务

(2) 第二级服务器为:对公司业务无直接影响，但对公司内部流程有明显影响

(3) 第三级服务器为:对公司业务无影响，只影响少部分公司内部流程且对于公司同仁日常作业无明显影响

2.7.2 每年依据主机等级进行系统复原验证测试

2.8 人员训练

2.8.1 新进员工教育训练 - 加强信息安全政策倡导，以确保新进员工了解并遵守公司一切资安相关规定

2.8.2 资安教育训练 - 针对所有员工每年定期举办信息安全教育训练课程并于每季以邮件发送信息安全倡导，以提升同仁资安防护意识