甘李药业股份有限公司

IT 安全/网络安全管理计划

为保障公司信息系统及网络环境的稳定性、机密性和可用性，有效识别、评估和控制网络与信息安全管理中的各类风险与威胁，全面落实网络安全法律法规及国际标准要求，结合公司实际运营情况，特制定本 IT 安全/网络安全管理计划。本计划旨在通过系统化、规范化的管理措施，预防和减少网络安全事件、数据泄露及系统故障的发生，确保业务连续性和信息资产安全。

一、安全风险评估与更新

公司定期开展 IT 安全风险评价，覆盖所有网络基础设施、信息系统、数据中心、云平台及终端设备，全面评估硬件、软件、数据及人员操作行为中的安全威胁；每年更新网络安全风险评估表，每三年委托第三方专业机构进行渗透测试或安全审计。

二、风险分级与控制体系

公司建立四级网络安全风险管控体系（紧急、高、中、低），基于风险评估结果按等级制定管控清单，明确责任部门、整改措施及完成时限，并通过安全运营中心（SOC）动态监控执行情况。

三、应急预案与响应机制

公司建立覆盖网络攻击（如勒索软件、DDoS 攻击）、数据泄露、系统瘫痪等多种突发安全事件的应急预案，明确应急响应流程、通信机制和恢复策略；每三年全面更新预案并通过第三方专家评审。

四、应急资源保障

公司每年开展应急资源调查（包括硬件备份、云容灾资源、安全工具等），每月对应急物资（如防火墙备用设备、加密密钥、备份介质）进行点检与测试，确保可用性。

五、应急演练与持续改进

公司每年制定网络安全应急演练计划，经 IT 安全管理委员会审批后，按月开展模拟攻击、数据恢复等实战演练，并基于演练结果优化应急流程。

六、安全目标管理与考核

公司每年设定核心网络安全目标（如漏洞修复率、事件响应时间、安全培训覆盖率），并分解至各部门执行；每季度向 IT 安全管理委员会汇报进展，动态调整资源投入。

七、安全检查与隐患治理

公司每年制定网络安全检查计划，明确公司级、部门级、系统级三级检查职责，严格执行漏洞管理“五定”原则（定风险等级、定整改责任人、定整改措施、定完成时间、定验证人），实现闭环管理。

八、体系认证与合规性

依托国际标准的 ISO/IEC 27001 信息安全管理体系，公司建立了完善的信息安全治理结构。我们通过年度第三方审核这一常态化机制，持续驱动自身安全管理水平提升，以确保全面契合《网络安全法》、GDPR 等法律法规的合规性要求，有效降低运营风险，增强客户信任，赋能全球业务发展。

九、安全事件调查与改进

公司制定网络安全事件调查处理程序，确保事件及时响应、根因分析、纠正措施落地，并纳入知识库避免重复发生。

十、培训与相关方管理

公司每年制定网络安全培训计划，组织管理人员参加 CISP、CISSP 等外部认证；对入职员工、承包商、供应商及相关第三方实施安全准入教育和技术交底。