甘李药业股份有限公司

IT 安全/网络安全措施、政策

一、政策目的

本 IT 安全/网络安全政策旨在系统化地保障公司网络与信息系统的安全性、稳定性和可靠性，全面应对信息技术快速发展带来的各类网络安全风险。政策通过建立全面的控制措施和管理框架，确保公司数字资产得到充分保护，防范未经授权的访问、攻击和滥用行为，维护信息的机密性、完整性与可用性。同时，政策致力于提升全体员工的网络安全意识和应急处理能力，形成主动预防与及时响应相结合的安全文化，为公司的可持续发展提供坚实的安全保障。

政策严格遵循《中华人民共和国网络安全法》、《数据安全法》、《个人信息保护法》等国家相关法律法规及行业标准要求，确保公司各项运营活动符合法律合规性标准。通过定期开展网络安全演练、风险评估与制度审核，不断优化和完善安全防护体系，降低网络安全事件发生的概率，最大限度减少安全事件可能造成的损失和影响。

二、适用范围

本政策适用于公司所有员工和用户，包括正式员工、实习生、访客以及任何获得授权使用公司网络与信息系统的个体。无论其职位级别或工作性质，只要接触或使用公司网络资源、信息系统和数据资产，都必须严格遵守本政策规定的内容和要求。

政策涵盖公司所有的网络基础设施、信息系统和数据资产，包括但不限于：

1、公司内部的局域网、无线网络、VPN 远程接入等网络环境。

2、服务器、终端设备（台式机、笔记本电脑）、移动设备（手机、平板）等硬件设施。

3、业务应用系统、数据库、办公软件、云服务等软件平台。

4、公司产生、收集、存储、处理和传输的任何形式的数据与信息。

本政策适用于公司所有办公场所和业务运营区域，包括总部、分支机构、远程办公场所以及任何使用公司网络资源的场景。对于关键信息基础设施的运营者，还将遵循《关键信息基础设施安全保护条例》等法规的特殊要求，实行重点保护。

三、核心承诺

3.1 网络安全保护承诺

公司承诺建立全面的网络安全防护体系，部署防火墙、入侵检测与防御系统等先进安全技术手段，实时监控网络流量，及时发现和阻断恶意攻击行为。所有网络设备和服务器的安全配置必须符合最低权限原则，关闭非必要的系统服务与端口，定期进行漏洞扫描与修复，确保网络基础设施的健壮性和安全性。

公司承诺实施严格的访问控制机制，确保员工仅能通过公司授权的设备和账户访问内部网络，严禁私接设备或未经授权访问。对于关键系统和敏感数据，实行双因素认证强化认证强度，并要求密码定期更换且符合复杂度要求。所有网络日志将记录并保存至少 180 天，定期进行审计分析，以便追溯安全事件和异常行为。

公司将严格遵守《数据安全法》和《个人信息保护法》的规定，建立数据安全管理体系，完善数据安全治理和个人信息保护机制。通过数据分类分级保护、风险监测预警和应急处置、数据安全审查、数据跨境流动安全管理等基本制度，持续提升数据安全治理和个人信息保护能力，严防数据泄露、毁损和丢失风险。

3.2 系统与终端安全承诺

公司承诺对所有终端设备实施统一安全管理，要求所有终端安装防病毒软件，定期更新病毒库及系统补丁，防止恶意软件感染和传播。对服务器、网络设备进行安全加固，及时更新补丁，消除已知安全漏洞。定期开展安全检查检测，及时发现并整改安全隐患，完善安全措施。

3.3 安全事件管理承诺

公司承诺建立完善的安全事件监测与报告机制，任何员工发现安全事件（如病毒入侵、黑客攻击、数据泄露）须立即向信息安全员报告。安全员须及时响应，初步分析后上报领导小组，并视情况向公安机关报告。公司制定详细的安全事件应急预案，明确处理流程与责任人，确保安全事件得到及时有效处置。

公司承诺每年至少组织一次应急演练，持续优化响应机制。按照国家网络安全事件应急预案的要求，建立健全网络安全事件应急工作机制，提高应对网络安全事件能力。建立健全网络安全应急协调和通报工作机制，及时汇集信息、监测预警、通报风险、响应处置，构建起“全国一盘棋”的工作体系。

3.4 员工行为规范与培训承诺

公司承诺建立明确的员工网络行为规范，要求员工不得利用公司网络制作、复制、传播违反法律法规及公司规定的信息。禁止私自安装软件、拆卸设备、更改网络设置及泄露账户密码。所有员工都有责任和义务保护公司网络与信息系统的安全，发现安全风险应及时报告。

公司承诺定期开展网络安全培训与意识教育活动，新员工须接受信息安全入职培训，全员需定期参加安全意识教育活动。通过案例分享、专题讲座等形式增强员工对最新安全威胁的识别与防范能力，全面提升员工的网络安全意识和防护技能，形成“网络安全为人民、网络安全靠人民”的良好氛围。