甘李药业股份有限公司

IT 安全/网络安全治理

一、宗旨

为构建世界一流的 IT 安全与网络风险防控体系，确保公司数字资产、信息系统及数据资源的机密性、完整性与可用性，履行企业数字化可持续发展之责，特制定本政策。我们矢志不渝地通过系统性技术防护、全员安全意识提升和持续治理优化，实现网络安全零重大事件、数据零泄露的核心目标，为全球业务运营奠定坚实可靠的数字基础。

二、适用范围

本政策适用于全体员工、承包商、供应商及第三方合作方，涵盖公司全部信息系统（包括工控网络、云平台、移动应用）、数据资产及网络基础设施。网络安全是公司数字化转型的核心保障，保护每一比特数据的安全是企业义不容辞的责任。

三、核心承诺

（一）合规为先，严守标准

严格执行《中华人民共和国网络安全法》《数据安全法》《个人信息保护法》及等级保护 2.0 标准。

全面对接国际安全框架（如 ISO 27001、NIST CSF），建立覆盖网络安全、数据安全、应用安全及终端安全的标准化治理体系。

（二）技术防护，纵深防御

公司构建多层协同的技术防护体系：

1. 网络边界防护：部署下一代防火墙（NGFW）、入侵检测/防御系统（IDS/IPS）及抗 DDoS 服务，实现网络分区隔离与访问控制。

2. 数据安全保护：实施数据分类分级与加密，强化数据库审计与防泄漏（DLP）能力。

3. 应用与系统安全：推行安全开发生命周期（SDL），落实代码审计、渗透测试及漏洞扫描；系统实施安全加固、补丁管理与最小权限原则。

4. 终端安全管控：部署统一终端安全与准入网络终端，实现终端准入控制、行为审计及恶意代码防护。

（三）全员参与，共筑防线

全员信息安全意识培训：

1. 形式：基础培训（专家讲座）、实战演练（钓鱼模拟）、在线平台（自主学课程库）等。

2. 内容：全员信息安全意识培训，高管层专题课程，包括最新威胁与法规。

3. 效果：测试考核 + 绩效挂钩，优秀者奖励，配宣传周强化意识。

多渠道反馈机制：

1. 渠道：线上（OA / 企业微信匿名入口、邮件 / 热线）+ 线下（意见箱），加月度问卷主动征集。

2. 响应：24 小时确认反馈，5 个工作日分级处理，员工可查进度，解决后闭环沟通。

3. 激励：设“信息安全突出表现奖”，公示反馈数据与改进措施。

实施保障

信息安全纳入全员绩效考评，每季度评估优化。

持续改进，体系优化

公司承诺通过以下机制推动治理体系持续升级：

1. 威胁情报监测：实时了解全球安全威胁情报，按月更新攻击特征库与防护策略。

2. 红蓝对抗演练：每年开展攻防演练与渗透测试，检验防御体系有效性。

3. 年度内部审计：由 IT 安全部门主导，对全部系统进行合规自评与风险复盘。

（四）目标管理，精准治理

公司基于年度安全态势设定可量化的核心目标（经总裁审批），并分解至各部门执行。关键绩效指标（KPI）包括：

1. 重大安全事件数量

2. 漏洞平均修复时间（MTTR）

3. 数据泄露事件数

4. 安全培训覆盖率与通过率

5. 安全策略合规率

四、责任与问责

管理层：负责审批安全目标、分配资源并主导安全文化建设。

IT 安全部门：落实防护措施、监控安全态势、应急响应及审计调查。

全体员工：遵循安全策略、参与培训演练、及时报告安全事件。