蒙牛信息安全政策

蒙牛将信息安全管理视为重要工作，围绕“让数据使用更安全”的核心目标，建立并实施高标准信息安全管理方针，持续改进并推进信息保护和数据安全的系统化建设，提升对信息安全威胁的响应能力，落实信息安全保护工作。

编制依据

本政策严格遵守《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、GB/T22239-2019:《信息安全技术 网络安全等级保护基本要求》、ISO/IEC 27001:2022 《信息安全、网络安全和隐私保护 信息安全管理体系要求》、ISO/IEC 27002:2022《信息安全、网络安全和隐私保护 信息安全控制》等有关法律法规制定《蒙牛信息安全政策》（以下称“本《政策》”）。如本《政策》与任何适用的法律及规例有冲突之处，应以适用的法律及规例为准。

范围

本《政策》适用于蒙牛集团及分子公司的所有部门与员工。

内容

1. 信息安全治理

蒙牛设立“决策层-管理层-执行层-支持层”四层级信息安全管理组织架构。其中，决策层为集团信息安全领导小组，蒙牛集团总裁为组长、蒙牛首席数智官为副组长，领导集团信息安全总体工作。信息安全组和数据安全组负责信息与数据安全治理体系的规划与建设，事业部安全组、职能安全组、控股单位安全组及全体员工负责落实各项安全工作，并配合外部专家、风险审计和监管机构的监督和检查。

2. 信息安全管理

蒙牛在如下方面要求集团及分子公司开展信息安全管理工作：

- 采用先进的信息安全技术，坚持持续改进原则，及时检查、修改和调整现有的安全策略和保护措施，以提升安全管理水平，持续维护信息安全管理体系的有效性；
- 定期开展内外部信息安全审计工作，积极获取权威信息安全认证，确保蒙牛的信息安全体系受到监督；
- 开展数据全生命周期安全控制措施，建立防范数据泄漏机制，确保数据始终准确、一致，并防止未经授权的访问、篡改或破坏；
- 主动监测网络安全风险，及时响应安全事件并实施缓解策略。当发生数据泄露或安全威胁时，保持对受影响方的透明度，积极采取补救措施，并制定未来风险预防方案；
- 坚持全员参与原则，开展全员信息安全培训，提高安全意识；为全体员工明确信息安全职责及对信息安全事件的上

报流程，要求员工在工作中如遇疑似信息安全事件，应立即向信息安全主管部门报告；

- 第三方合作伙伴需遵守蒙牛集团《商业伙伴合规行为准则》中列示的隐私与数据保护相关要求。

利益相关方沟通

蒙牛持续增强信息安全工作的透明度，定期公开披露工作进展。

蒙牛积极参与外部利益相关方的沟通，保持信息安全工作持续处于行业领先地位，并及时对本《政策》进行审阅和更新。

政策监督及汇报

本《政策》所载各项内容由蒙牛可持续发展执行委员会监督，主要工作及目标达成进展均向可持续发展委员会进行汇报。