中国圣牧信息安全政策

一、目的

为保障中国圣牧及其利益相关者的合法权益，确保公司信息资产的安全性、完整性和可用性，防范信息安全风险，特制定本信息安全政策。本政策旨在明确公司在信息安全方面的管理要求和行为准则，为全体员工、合作伙伴及相关方提供指导，共同构建安全可靠的信息环境。

二、适用范围

本政策适用于中国圣牧及其所有分支机构、附属公司。全体员工（包括全职、兼职和临时员工）、管理层、董事以及代表公司从事相关活动的其他人员（如承包商、供应商、合作伙伴等）均需严格遵守本政策。

三、信息安全原则

（一）合法性原则严格遵守国家相关法律法规，包括但不限于《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》等，确保信息安全管理工作合法合规。

（二）责任原则明确信息安全责任，全体员工对自身的信息安全行为负责，管理层对信息安全管理工作负领导责任，信息安全管理部门负责制定和执行信息安全策略，监督信息安全工作的落实情况。

（三）预防原则采取积极主动的措施，预防信息安全事件的发生，包括但不限于风险评估、安全防护、应急响应等，将信息安全风险降至最低。

（四）最小化原则在处理个人信息和敏感数据时，遵循最小化原则，仅收集、使用和存储为实现业务目的所必需的最少信息，并严格限制信息的访问权限，确保

信息安全。

四、信息安全责任与义务

（一）全体员工

1. 遵守信息安全政策和相关法律法规，保护公司信息资产的安全。

2. 不得未经授权访问、使用、泄露或破坏公司信息资产。

3. 发现信息安全漏洞或异常情况时，应及时向信息安全管理部门报告；员工可通过邮箱或直接向信息部门相关负责人反馈。

4. 积极参加信息安全培训，提高自身信息安全意识和技能水平。

（二）信息部门

信息部门将定期或在必要时开展信息安全漏洞分析，以识别系统、网络、应用程序或数据处理流程中存在的潜在安全风险。包括漏洞分析、验证、记录、修复。最后对修复结果进行验证。

五、信息安全监督与审计

（一）内部审计定期开展信息安全内部审计，检查信息安全政策和制度的执行情况，发现信息安全管理工作中的问题和不足，及时提出整改建议，并跟踪整改落实情况。

（二）外部审计根据需要，委托专业的信息安全审计机构开展信息安全外部审计，对公司的信息安全管理工作进行全面、客观的评估，及时发现和解决信息安全管理工作中的问题。

六、信息安全合作与沟通

建立健全信息安全内部沟通机制，确保各部门之间信息畅通，及时传递信息安全相关信息。