江苏今世缘酒业股份有限公司
信息安全政策

Jiangsu King's Luck Brewery Joint-Stock Co., Ltd.

Information Security Policy

江苏今世缘酒业股份有限公司（以下简称"公司"）为完善公司信息安全管理体系，规范信息化资产全生命周期管理，强化信息安全风险防控能力，提升全员信息安全素养，保障公司信息系统安全稳定运行，特制定本政策。

Jiangsu King's Luck Brewery Joint-Stock Co., Ltd. (hereinafter referred to as "the Company") formulates this policy in order to improve the Company's information security management system, standardize the management of the entire life cycle of information assets, strengthen the ability to prevent and control information security risks, enhance the information security literacy of all employees, and ensure the safe and stable operation of the Company's information systems.

一、适用范围

I. Scope of Application

本政策适用于公司全体员工、股东、客户、供应商、合作伙伴等，覆盖所有业务活动及物理环境。

This policy applies to all employees, shareholders, customers, suppliers, partners, etc. of the Company, and covers all business activities and physical environments.

二、指导监督机构

II. Guiding and Supervising Institution

公司搭建自上而下的信息安全治理架构，董事会负责从整体上建立健全信息安全风险管理体系和监控体系落实，将信息安全相关内容纳入到公司治理、企业文化建设和经营发展战略之中。高级管理层负责领导公司信息安全风险管理与内部控制的日常运行，指导公司信息安全管理工作。同时公司设有大数据中心，负责执行公司的信息安全相关政策及制度，监控信息安全和隐私管理，确保公司在数据处理、信息共享及隐私保护等方面的合规性。

The Company has established a top-down information security governance framework. The Board of Directors is responsible for comprehensively establishing and improving the information security risk management system and monitoring system, and incorporating information security-related contents into the Company's governance, corporate culture construction, and business development strategies. The senior management is responsible for leading the daily operation of the Company's information security risk management and internal control, and guiding the Company's information security management work. In the meantime, the Company has set up a big data center, which is responsible for implementing the Company's information security-related policies and systems, monitoring information security and privacy

management, and ensuring the Company's compliance in aspects such as data processing, information sharing, and privacy protection.

三、系统预防

III. Systematic Prevention

为确保公司信息系统的安全稳定，公司定期对信息管理系统实施内部安全检查。大数据中心网络运维处每月对公司网络开展不少于一次的全面病毒扫描，并于每年进行一次网络安全攻防演练，确保公司信息安全管理体系的有效性。

To ensure the security and stability of the Company's information systems, the Company conducts regular internal security checks on its information management systems. The Network Operation and Maintenance Department of the Big Data Center conducts a comprehensive virus scan of the Company's network at least once a month and organizes a network security attack-defense drill once a year to ensure the effectiveness of the Company's information security management system.

四、风险应对

IV. Risk Response

信息安全小组实时监控事件动态变化，当事件级别达到升级标准时，立即上报大数据中心负责人决策，启动事件升级，并采取应急处置措施。网络运维处工程师执行 24 小时监测，关注恢复系统状态。信息安全工程师调查确认事件等级及原因，撰写总结报告并提出改进建议。

The Information Security Team monitors the dynamic changes

of incidents in real time. When an incident reaches the escalation criteria, it shall immediately report to the person in charge of the Big Data Center for decision-making, initiate the incident escalation, and take emergency response measures. The engineers of the Network Operation and Maintenance Department conduct 24-hour monitoring and pay attention to the recovery status of the system. Information security engineers investigate and confirm the level and cause of the incident, write a summary report, and put forward improvement suggestions.

五、信息安全培训

V. Information Security Training

公司每年开展覆盖全体员工的信息安全管理培训，并确保信息安全政策内容传达至全体员工。培训内容包括网络安全、数据安全、开发安全等信息安全知识和技能，提升全员信息安全意识。

The Company conducts information security management training covering all employees every year and ensures that the content of the information security policy is communicated to all employees. The training content includes information security knowledge and skills such as network security, data security, and development security to enhance the information security awareness of all employees.

六、修订与审阅

VI. Revision and Review

公司每年审阅本政策，并在必要时进行修订。

The Company will regularly review this policy annually and make revisions as necessary.