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") has formulated this Policy to improve its information security management system, standardize life-cycle management of information assets, strengthen its ability to prevent and control information security risks, enhance information security awareness across the workforce, and ensure the secure and stable operation of its 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。为保障合作业务的安全、稳定与合规，公司与第三方（包括供应商及合作伙伴）的合作，应建立在共同遵守信息安全基本原则的基础上。在信息安全方面，第三方应遵守其业务所适用的的国家法律法规及监管规定，并采取与所处理公司信息的重要性、敏感度相适应的管理措施和技术手段，以保障信息安全，达到基本的合规要求。公司将通过包括但不限于《可持续发展（ESG）承诺书》在内的文件予以明确约定。

This Policy applies to all employees, shareholders, customers, suppliers, business partners, and other relevant parties of the Company and covers all business activities and physical environments. To ensure the security, stability, and compliance of collaborative business activities, cooperation between the Company and third parties, including suppliers and business partners, shall be based on shared compliance with fundamental information security principles. With respect to information security, third parties shall comply with the national laws, regulations, and regulatory requirements applicable to their businesses and adopt management measures and technical controls commensurate with the importance and sensitivity of the Company information they process to protect information security and meet basic compliance requirements. The Company specifies these requirements in documents including, but not limited to, the Sustainable Development (ESG) Commitment Letter.

二、指导监督机构

II. Governance and Oversight

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 structure. The Board of Directors is responsible for establishing and improving the overall information security risk management and monitoring systems and overseeing their implementation, and for integrating information security into corporate governance, corporate culture, and business development strategy. Senior management leads the day-to-day operation of information security risk management and internal controls and directs the Company's information security management. The Company has also established a Big Data Center, which implements information security policies and procedures, monitors information security and privacy management, and supports compliance in data processing, information sharing, and

privacy protection.

三、系统预防

III. System Protection and 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。公司采取加密传输、访问控制及备份恢复等技术措施，确保数据的完整性、可用性与保密性。

To ensure the security and stability of its information systems, the Company regularly conducts internal security inspections of information management systems. The Network Operations and Maintenance Office of the Big Data Center performs a comprehensive virus scan of the Company's network at least once each month and conducts a cybersecurity attack-and-defense exercise annually to assess the effectiveness of the information security management system. The Company uses technical measures including encrypted transmission, access controls, backup, and recovery to ensure the integrity, availability, and confidentiality of data.

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 Working Group monitors developments in incidents in real time. When an incident reaches the escalation threshold, it is immediately reported to the head of the Big Data Center for decision-making, the incident escalation process is initiated, and emergency response measures are implemented. Engineers in the Network Operations and Maintenance Office provide 24-hour monitoring and track system recovery. Information security engineers investigate and confirm the incident level and cause, prepare a summary report, and recommend improvements.

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 provides annual information security management training covering all employees and ensures that the Information Security Policy is communicated throughout the workforce. Training covers information security knowledge and skills relating to cybersecurity, data security, secure development, and other relevant areas to strengthen information security awareness across the Company.

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。同时，公司每年根据安全检查、攻防演练及风险评估结果，对信息安全管理措施进行评审和持续改进。

The Company reviews this Policy annually and revises it when necessary. It also reviews and continuously improves information security management measures each year based on the results of security inspections, attack-and-defense exercises, and risk assessments.