东方日升信息安全政策

Information Security Policy

东方日升深知，保护敏感信息和落实信息安全管理，是维护企业竞争力及应对网络威胁的关键。我们严格遵循《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》等相关法律法规，制定了《集团信息安全应急响应制度》《数据安全管理制度》等信息安全管理程序，全力保障内部制度及流程的合法合规和有效落实，保护信息资产的安全性和完整性。

At Risen Energy, we recognize the importance of protecting sensitive information and implementing IT security management. We strictly adhere to relevant laws and regulations, including the Cybersecurity Law of the People's Republic of China and the Personal Information Protection Law of the People’ s Republic of China. Our policies, such as the Group IT Security Emergency Response System and the Data Security Management Policy, are designed to ensure legal compliance, effective internal processes, and the security of our information assets.

- **组织架构与职责**
- **Governance and Responsibility**

集团高层组成信息安全委员会，负责制定集团与信息安全相关的战略；由董事会成员、集团总裁担任公司首席信息官（CIO），同时兼任首席信息安全官（CISO），统筹领导公司信息安全管理体系建设，于任内领导多项信息技术项目，有丰富的 IT 管理经验。由流程与信息中心总监负责公司信息安全管理体系的监督落实工作。

We have established an IT Security Committee composed of senior management to develop our company's IT security strategies. The President, who is also a Board member, serves as both the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO). Drawing on his extensive experience, he coordinates and leads the creation of the company's IT security management system and oversees numerous IT projects. The Director of the Process and IT Center is responsible for implementing the IT security management system.

我们成立了由业务部门、信息中心、风控中心等多个部门组成的数据安全管理小组，统筹协调数据安全管理的各项工作，确保各环节的高效运作。相关负责人包括管理小组成员、各层级信息安全员必须对信息安全负责。

To ensure effective information security management, we have established a data

东方日升信息安全政策

Information Security Policy

security management team consisting of representatives from the IT Center, Risk Control Center, and other relevant departments. The responsible individuals, including members of the management team and IT security officers at all levels, are accountable for IT security.

- **信息安全管理具体措施**
- **Measures for Information Security Management**

防止数据泄露 Data leakage prevention	敏感邮件开启机密模式 Confidential mode is set for sensitive emails
	亚信 OSCE、DS、TDA 实时检测内部安全风险，及时发现失陷主机以防数据泄漏 OSCE, DS and TDA are deployed for real-time detection of internal security risks to identify faulty hosts in time and prevent data leakage
	联软桌管和 DLP 管理敏感数据外发情况 UniAccess and DLP are deployed to manage outgoing sensitive data
定期系统维护 Regular system maintenance	根据业务更新周期维护系统、软件、硬件并及时更新厂商提供的安全补丁 Systems, software, and hardware are maintained according to the business update cycle and vendor-provided security patches are timely updated as well
	业务上线前会进行漏洞扫描，将高危漏洞反馈给业务人员修复 Vulnerability scan is conducted before business go-live and high-risk vulnerabilities are reported to relevant personnel for timely resolution
安全意识培训 Security awareness	员工必须经过安全信息培训并签署保密协议 Employees must participate in security IT training and sign off confidentiality agreements

东方日升信息安全政策

Information Security Policy

training	针对 IT 人员至少一年二次安全培训，内容涉及集团信息安全应急响应制度培训、信息安全框架解析培训、信息安全意识、钓鱼演练等。 Security training sessions are arranged for IT staff at least twice a year, covering information security emergency response policy training, information security framework analysis training, information security awareness, phishing drills and more.
应急事件响应测试 Emergency response testing	已实施如灾难恢复计划（DRP）、渗透测试和漏洞评估（VA）等网络安全测试，至少每半年进行一次测试，以确保其网络安全管理保持有效。 We have implemented cybersecurity tests such as Disaster Recovery Plan (DRP), Penetration Testing and Vulnerability Assessment (VA) at least semi-annually to ensure the effectiveness of our cybersecurity management.
外部认证及基础设施审计 External certification and infrastructure audits	✓ 公司的信息安全管理体系 100%通过了公安部的等保认证。 Our IT security system has 100% gained the certificates of Classified Protection of Cybersecurity by the Ministry of Public Security. ✓ 有外部安服团队出具的漏扫报告。 We have gained a vulnerability scan report issued by external security service team.

■ **数字化转型**

■ **Digital Transformation**

公司坚信数字化转型是组织谋求可持续发展和成功的关键路径。通过持续完善数字化基础设施建设、优化业务流程、推广数字化技术、推动创新发展来保持企业的竞争力和活力，以适应市场变化和科技进步的要求，实现可持续发展

We strongly believe that digital transformation is essential to our long-term

东方日升信息安全政策
Information Security Policy

sustainability, success, and competitiveness. We are dedicated to achieving sustainable growth through enhancing digital infrastructure, optimizing business processes, promoting innovation in digital technologies, and adapting to market changes and technological advancements.

■ **员工信息安全职责**

■ **The Information Security Responsibilities of Employees**

保障公司资产及数据的安全是每一位员工的责任，公司要求每位员工：

Safeguarding the company's assets and data is the responsibility of every employee, and we require every employee to:

- 确保所有设备（包括笔记本电脑、手机、U 盘、移动硬盘等）安全存放；
- Ensure that all equipment (including laptops, cell phones, USB flash drives, mobile hard drives, etc.) are stored safely

- 不得将办公设备用于非工作需求；
- Not to use the office devices for non-work purposes;

- 按公司要求使用复杂密码并且定期修改，避免启用“自动保存密码”或“自动登录”功能，以防潜在安全风险；
- Set complex passwords and change them regularly according to the company's requirements, and avoid enabling the "auto-save password" or "auto-login" function to prevent potential security risks.

- 严格遵守公司信息安全相关规定，积极参加信息安全培训并阅读信息安全宣导资料；
- Strictly comply with the company's information security regulations, participate in information security training and review information security documents.
- 一旦发现设备遗失或数据泄露迹象，立即向直属领导、IT 运维共享部及信息安全组报备，提供详细情况，包括设备型号、遗失/泄露时间地点原因等，并配合公司进行后续的风险评估和应对措施。

东方日升信息安全政策
Information Security Policy

- Immediately report any data leakage or device loss to direct supervisors, the IT Department and the information security team. Provide detailed information including the device model, reason, time, and location of the loss or leakage. Cooperate with the company to conduct risk assessment and implement mitigation measures.

■ **安全事件处理**

■ **Information Security Incident Management**

公司要求各个信息管理系统使用者，在使用过程中如果发现软硬件故障、事件，要向该系统归口管理部门和流程与信息中心报告:如故障、事件会影响或已经影响业务运行，必须立即报告相关部门，采取必要措施，保证对业务的影响降至最低。

We require all users of our information management systems to report any hardware and software malfunctions and incidents promptly to the responsible management department and the Process and Information Center. If these malfunctions and incidents affect or have affected business operations, users must immediately notify the relevant departments to take necessary measures to minimize the impact on the business.

信息安全弱点汇报处理流程：

发现弱点➡信息上报➡判断分析➡弱点处理和关闭

Escalation Process of Information Security Incident:

Discovery of vulnerability ➡ Information reporting ➡ Analysis ➡ Vulnerability addressing and closure.

■ **信息安全绩效考核**

■ **Information Security Performance Appraisal**

信息安全/网络安全作为其绩效评估的一部分，根据其信息安全方面的工作表现机遇相应的激励和惩罚。集团流程与信息中心负责在每季度中旬统计信息安全管理人员所在部门信息安全考核基本数据，通过《信息安全绩效考核》为其打分，由集团人力资源中心按照《信息安

东方日升信息安全政策
Information Security Policy

全目标与责任制管理制度》落实考核结果。
Information security/ cybersecurity is a component of our performance appraisal process. We have established incentives and penalties for information security performance. The Process and Information Center conducts quarterly assessments of IT security management personnel, scoring them based on the "Information Security Performance Assessment". The Human Resource Center implements the assessment results in accordance with the "Information Security Objectives and Accountability Management System.

- **人员培训与意识提升**
- **Training and Awareness Promotion**

持续加强信息安全培训，提高员工的信息安全意识和技能。培训内容包括信息安全政策、安全操作规范、应急处置等。同时，定期开展信息安全宣传活动，提升全员信息安全意识。
We continuously enhance information security training to improve employees' awareness and skills. Training covers information security policies, operational standards, and emergency response protocols. Additionally, we regularly organize information security awareness campaigns to educate all employees about the importance of information security.