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 Information Security Governance

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。由流程与信息中心及数字能源软件中心副总裁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 coordinated and led the creation of the company's IT security management system and oversaw numerous IT projects. The VP of the Process and IT Center and Digital Software 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.

■ 管理体系机制 Management System Mechanism

随着业务数字化程度不断加深，公司逐步建立起一套适应自身发展节奏的信息安全管理体系，贯穿系统运行、数据处理、员工行为及外部合作等多个环节，为业务稳定运行提供保障。
As the company continues to advance its digital transformation, we have progressively established an information security management system aligned with our own pace of development. This system spans system operations, data processing, employee conduct, and external collaboration, and serves as a foundation for maintaining stable business operations. A key principle of this system is continuously improving information security systems to stay ahead of emerging risks and ensure long-term resilience.

我们持续完善信息安全系统，以应对不断变化的外部风险环境。IT 团队定期开展系统排查与优化，及时修复潜在漏洞，确保关键业务系统运行稳定、安全可靠。
We continuously enhance our information security systems to monitor and response to information security threats, adapting an evolving external risk landscape. The IT team conducts regular system assessments and optimizations, promptly addressing potential vulnerabilities to ensure the stable and secure operation of key business systems. These efforts reflect our firm commitment to continuously improving information security systems and ensuring the integrity and protection of data across all platforms.

在数据保护方面，公司已形成以数据完整性与访问控制为核心的操作规范，明确数据分级分类要求，重要信息须由授权人员管理，防止数据被篡改、泄露或误用。
In terms of data protection, the company has established operational protocols

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

centered on data integrity and access control. These include clear requirements for data classification and hierarchical management, ensuring that critical information is handled only by authorized personnel to prevent tampering, leakage, or misuse. These practices ensure the integrity and protection of data throughout its lifecycle.

信息安全管理不仅是 IT 部门的职责，也需要全体员工共同参与。公司将安全意识纳入员工入职培训和日常宣导体系，明确“发现异常、及时报告”的基本行为要求，通过持续强化员工认知，构建风险共识。
Information security management is not solely the responsibility of the IT department—it requires the active participation of the entire workforce. The company integrates security awareness into onboarding programs and ongoing internal communication. Employees are expected to follow basic behavioral guidelines, such as reporting anomalies promptly. These actions support our approach to establishing individual responsibilities for information security across the organization.

对于涉及系统接口或数据传输的合作伙伴，我们会在合作初期明确提出基本的信息安全要求，包括数据保密责任、访问权限边界等，并视具体情况通过技术手段加以控制，力求在合作过程中不留安全盲区。
For third parties involved in system integration or data exchange, we define baseline information security requirements at the start of collaboration. These requirements cover data confidentiality obligations, access control boundaries, and expected security practices. Depending on the nature of the engagement, we also implement technical controls as needed to reduce risk exposure. This approach reflects our commitment to establishing clear information security requirements for third parties and maintaining a secure ecosystem throughout our business network.

■ **信息安全管理计划 Information Security Management Programs**

业务连续性管理 Business	针对核心系统，公司已制定业务连续性管理方案，包括数据备份、异地容灾、网络攻击应急响应等措施，确保在突发情况下可快速恢复关键业

东方日升信息安全政策

Information Security Policy

continuity plan	务。 For core systems, Risen has developed a business continuity plan, including data backups, offsite disaster recovery, and cyberattack response measures, to ensure rapid recovery of critical operations in emergencies.
信息系统漏洞分析 System vulnerability analysis	IT 部门定期开展漏洞分析（SVA）、权限梳理与系统风险评估，结合外部顾问建议，持续推进安全加固。分析结果为系统优化、技术整改及后续审计提供决策依据。 The IT department regularly conducts vulnerability analysis (SVA), access reviews, and system risk evaluations. Based on internal findings and external consultancy input, security enhancements are continuously implemented. Results inform system optimization, technical remediation, and future audits.
员工上报流程与内部升级机制 Escalation process for employees	公司已设立信息安全事件的报告路径，员工在遇到系统异常、钓鱼邮件、潜在漏洞等情况时，可通过内网工单系统、IT 服务热线或安全邮箱提交报告，相关信息将由 IT 或法务合规团队负责分级处理并视情况启动升级处置流程。 A reporting mechanism for information security incidents has established. Employees can report system anomalies, phishing emails, or potential vulnerabilities via the intranet ticketing system, IT hotlines, ore security email. Reports are classified and handled by the IT or Legal & Compliance team, with escalation procedures activated as needed.
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

东方日升信息安全政策

Information Security Policy

	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 training	✓ 员工入职时必须完成基础的信息安全培训，内容涵盖账号管理、邮件防护、敏感信息处理等，同时定期通过内部公告、月度提示、钓鱼邮件演练等方式加强安全意识。 All employees must complete basic information security training upon onboarding, covering account management, email protection, and handling of sensitive information. Regular awareness is reinforced through internal post、monthly reminders, and phishing simulations. ✓ 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

东方日升信息安全政策

Information Security Policy

	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.
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.
年度信息安全事件披露 Disclosure of total breaches in last	在上一个财年内，公司未发生重大数据泄露事件。一般性系统异常或轻微事件已按内部流程及时响应并处理，未对客户或合作伙伴数据造成实质性影响。 During the previous fiscal year, Risen did not experience any

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

FY	major data breaches. Routine system anomalies or minor incidents were promptly addressed in according with internal procedures and did not result in any material impact on customer or partner data.

■ **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 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。
  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.

■ **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.