南京钢铁股份有限公司
信息安全政策

Nanjing Iron & Steel Co., Ltd.
Information Security Policy

第一条 总则

为保障公司信息资产的机密性、完整性和可用性，防范信息安全风险，提升全员信息安全意识与管理水平，南京钢铁股份有限公司（以下简称“公司”）依据国家相关法律法规及行业标准，结合企业实际运营需求，制定本信息安全政策。公司致力于构建安全、可靠、可控的信息化环境，支撑业务稳定运行与可持续发展。

I General Rules

To ensure the confidentiality, integrity, and availability of the Company's information assets, prevent information security risks, and enhance the information security awareness and management level of all employees, Nanjing Iron & Steel Co., Ltd. (hereinafter referred to as the "Company") has formulated this Information Security Policy in accordance with relevant national laws, regulations, and industry standards, combined with the actual operational needs of the Company. The Company is committed to building a secure, reliable, and controllable information environment to support stable business operations and sustainable development.

第二条 适用范围

本政策适用于公司及下属企业，以及供应商、承包商，以

及其他业务伙伴共同遵守本政策，共同维护信息环境的安全与合规。

II Coverage

This Policy applies to the Company and its subsidiaries, as well as suppliers, contractors, and other business partners who shall comply with this Policy to jointly maintain the security and compliance of the information environment.

第三条 管理政策

III Management Policy

（一） 信息安全管理架构

公司持续完善信息安全治理架构，明确董事会、管理层及相关部门在信息安全工作中的职责分工，建立由董事会战略与ESG委员会下属数字安全管理委员会统筹领导、数字应用研究院统筹协调、各业务单位协同配合的管理体系，数字应用研究院为公司信息安全工作的监督管理机构，向公司首席信息官（CIO）以及分管信息安全和数字化工作的高管汇报。系统识别网络攻击、数据泄露、内部违规、第三方风险等各类信息安全威胁，并通过定期风险评估、审计与改进机制，不断健全覆盖全生命周期的信息安全管理体系。

1. Information Security Management Structure

The Company continuously improves its information security governance structure, clearly defining the responsibilities of the Board of Directors, management, and relevant departments in information security work. It establishes a management system led by the Digital Security Management Committee under the Board's Strategy and ESG Committee, coordinated by the Digital

Application Research Institute, and cooperated by various business units. The Digital Application Research Institute serves as the supervisory and management body for the Company's information security work, reporting to the Company's Chief Information Officer (CIO) and senior executives in charge of information security and digitalization. It systematically identifies various information security threats such as cyber-attacks, data leaks, internal violations, and third-party risks, and continuously improves the information security management system covering the full lifecycle through regular risk assessments, audits, and improvement mechanisms.

（二） 数据收集与处理规范

公司坚持合法、正当、必要原则开展数据收集活动，严格遵守《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》等相关法律法规，规范数据采集流程，采用受控网络环境和安全传输通道，对数据实行分类分级管理，落实差异化存储策略。公司针对敏感数据实施加密存储，明确访问权限与使用边界，全面降低数据在采集、传输、存储、使用等环节的泄露与滥用风险。

2. Data Collection and Processing Standards

The Company adheres to the principles of legality, legitimacy, and necessity in data collection activities, strictly complies with relevant laws and regulations such as the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, and the Personal Information Protection Law of the People's Republic of China, standardizes data collection processes, adopts controlled network environments and secure

transmission channels, implements classified and graded management of data, and implements differentiated storage strategies. The Company implements encrypted storage for sensitive data, clearly defines access permissions and usage boundaries, and comprehensively reduces the risk of data leakage and misuse during collection, transmission, storage, and use.

（三） 访问控制与权限管理

公司严格执行“最小权限原则”（Least Privilege），根据岗位职责设定信息系统的访问权限，确保员工仅能接触其履行职责所必需的信息资源。公司通过统一身份认证、多因素验证、零信任访问控制、权限审批与定期复核等机制，严格控制信息的知悉范围，防止越权访问、非法拷贝或不当操作，保障核心数据资产的安全可控。

3. Access Control and Permission Management

The Company strictly implements the "Least Privilege" principle, setting access permissions for information systems based on job responsibilities, ensuring that employees can only access the information resources necessary to perform their duties. The Company strictly controls the scope of information knowledge through mechanisms such as unified identity authentication, multi-factor authentication, zero-trust access control, permission approval and periodic review, preventing unauthorized access, illegal copying, or improper operations, and ensuring the security and controllability of core data assets.

（四） 安全监测与预警机制

公司依据网络与数据安全防护等级，部署相应的技术监控手段，实现对关键信息系统和敏感数据的动态监测。公司重点

防范网络攻击、计算机病毒、数据泄露、篡改、毁损、丢失及未授权访问等异常行为，利用网络安全态势感知平台、终端安全管理系统、入侵防御系统、邮件安全网关等工具及时发现潜在风险，触发预警响应，做到早识别、早处置，提升整体安全态势感知能力。

4. Security Monitoring and Early Warning Mechanism

Based on the network and data security protection levels, the Company deploys corresponding technical monitoring measures to achieve dynamic monitoring of key information systems and sensitive data. The Company focuses on preventing abnormal behaviors such as cyber attacks, computer viruses, data leaks, tampering, destruction, loss, and unauthorized access. It uses tools such as network security situational awareness platforms, terminal security management systems, intrusion prevention systems, and email security gateways to promptly detect potential risks, trigger early warning responses, achieve early identification and early handling, and enhance overall security situational awareness capabilities.

（五） 安全事件应急响应

公司已建立完善的信息安全事件应急响应机制，明确组织架构、职责分工、报告路径与处置流程。一旦发生信息安全事件，公司立即启动应急预案，最大限度减少损失和影响。事件处理全过程记录存档，并开展事后复盘，持续优化防控措施。

5. Security Incident Emergency Response

The Company has established a comprehensive information security incident emergency response mechanism, clearly defining the organizational structure, division of responsibilities, reporting

paths, and handling procedures. Once an information security incident occurs, the Company immediately activates the emergency plan to minimize losses and impacts. The entire incident handling process is recorded and archived, and post-incident reviews are conducted to continuously optimize prevention and control measures.

（六） 员工行为规范

公司全体员工对信息安全负有责任，在使用公司网络和信息系统时，必须严格遵守国家法律法规及公司规章制度，严禁非法获取、窃取、泄露或篡改个人信息。公司禁止擅自下载、复制、转移重要企业数据和个人信息至个人设备（如 U 盘、手机、私人云盘等移动存储介质）。所有数据操作应基于工作需要并在受控环境下进行，杜绝私自留存或外传行为。

6. Employee Code of Conduct

All employees of the Company are responsible for information security. When using the Company's network and information systems, they must strictly comply with national laws and regulations and the Company's rules and regulations. It is strictly prohibited to illegally obtain, steal, leak, or tamper with personal information. The Company prohibits unauthorized downloading, copying, or transferring of important enterprise data and personal information to personal devices (such as USB drives, mobile phones, private cloud drives, and other mobile storage media). All data operations should be based on work needs and conducted in a controlled environment, eliminating any private retention or external transmission.

（七） 安全意识培训

公司将信息安全教育纳入全员培训体系，制定年度培训计划并分层组织实施。针对新员工、关键岗位人员及管理层开展信息安全培训，普及信息安全基础知识、典型风险案例与防护技能等。通过宣传、演练、测试等多种形式，持续提升全体员工的安全意识与责任认知，筑牢信息安全防线。

7. Security Awareness Training

The Company incorporates information security education into the full-staff training system, develops annual training plans and organizes implementation at different levels. It provides information security training for new employees, personnel in key positions, and management, popularizing basic information security knowledge, typical risk cases, and protection skills. Through various forms such as publicity, drills, and tests, it continuously enhances all employees' security awareness and responsibility recognition, strengthening the information security defense.

（八） 事故、漏洞与可疑活动的报告机制

公司鼓励全体员工积极履行信息安全责任，主动报告在工作中发现的信息安全事件、系统漏洞或可疑行为。公司建立便捷、多样化的上报渠道，确保员工可通过多种方式及时反映问题。

员工如发现数据泄露、网络攻击、设备失窃、账号异常、恶意软件感染或任何可能威胁信息安全的情况，应立即通过以下方式上报：

- 向直属主管或本单位信息安全管理负责人报告；
- 拨打公司统一 IT 服务热线；

- 发送邮件至信息安全事件专用邮箱；
- 通过企业网络安全工作群组反馈。

所有报告将被迅速响应和调查，相关部门将在 1 小时内启动初步处置流程，对积极报告并协助化解风险的员工给予表彰或奖励。

8. Reporting Mechanism for Incidents, Vulnerabilities, and Suspicious Activities

The Company encourages all employees to actively fulfill information security responsibilities and proactively report information security incidents, system vulnerabilities, or suspicious behaviors discovered during work. The Company establishes convenient and diverse reporting channels to ensure employees can promptly report issues through multiple methods.

If employees discover data breaches, cyber attacks, device theft, account anomalies, malware infections, or any situation that may threaten information security, they should immediately report through the following methods:

- Report to the direct supervisor or the information security management responsible person of the unit;
- Call the Company's unified IT service hotline;
- Send an email to the dedicated information security incident mailbox;
- Provide feedback through the corporate network security working group.

All reports will be responded to and investigated promptly. Relevant departments will initiate preliminary handling

procedures within 1 hour, and employees who actively report and assist in mitigating risks will be commended or rewarded.

（九） 第三方数据安全管理

公司原则上不向无关第三方提供企业信息与数据。对于因法律要求或业务确需委托外部机构处理数据的情形，公司优先采用脱敏、去标识化等技术手段降低风险，在合作前对其数据安全能力进行尽职调查，签订保密协议，明确数据保护责任，并监督其合规执行。所有外包活动均纳入统一安全管理范畴，确保第三方服务符合公司信息安全标准。

9. Third-Party Data Security Management

In principle, the Company does not provide corporate information and data to unrelated third parties. For situations where data must be entrusted to external organizations due to legal requirements or business needs, the Company prioritizes using technical measures such as desensitization and de-identification to reduce risks. Before cooperation, it conducts due diligence on the third party's data security capabilities, signs confidentiality agreements, clarifies data protection responsibilities, and supervises compliance. All outsourcing activities are included in the unified security management scope to ensure that third-party services meet the Company's information security standards.

第四条 附则

本政策经公司董事会战略与 ESG 委员会审议批准，自发布之日起生效。

IV Annex

This Policy has been reviewed and approved by the Strategy

and ESG Committee of the Board of Directors of the Company, which is effective as of the date of promulgation.