能源行业数据安全管理办法（试行）

第一章 总　则

第一条 为规范能源行业数据处理活动，加强数据安全管理，防范数据安全风险，促进数据开发利用，保护个人、组织的合法权益，维护国家安全和发展利益，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国能源法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规，制定本办法。

第二条 本办法适用于在中华人民共和国境内开展能源行业数据处理活动及其安全监督管理。

能源数据处理者开展涉及国家秘密或由其汇聚关联后属于国家秘密事项的能源行业数据处理活动时，应遵守《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

第三条 本办法所称数据，是指任何以电子或者其他方式对信息的记录。

本办法所称能源行业数据，是指在开展能源活动中收集和产生的数据。能源活动主要包括与能源相关的规划、设计、建设、生产、储运、消费、科研等。与城市燃气、供热、加油站等能源活动相关的数据应遵守有关主管部门规定。

本办法所称能源数据处理者，是指开展能源行业数据处理活动的能源行业各类单位。能源行业数据处理活动包括能源行业数据的

收集、存储、使用、加工、传输、提供、公开、删除等。

本办法所称数据安全，是指通过采取必要措施，确保能源行业数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

第四条 根据数据重要性、精度、规模、安全风险等，能源行业数据分为一般、重要、核心三级。

能源行业重要数据是指特定领域、特定群体、特定区域或达到一定精度和规模的能源行业数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。仅影响组织自身或公民个体的能源行业数据，一般不作为能源行业重要数据。

能源行业核心数据是指对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的能源行业重要数据，一旦被非法使用或共享，可能直接影响政治安全。主要包括：关系国家安全重点领域的数据，关系国民经济命脉、重要民生和重大公共利益的数据，经评估确定的其他能源行业数据。

能源行业一般数据是指能源行业重要数据、能源行业核心数据之外的其他能源行业数据。

第五条 鼓励能源数据处理者积极开展能源行业数据创新应用，在保障安全合规的情况下促进数据开发利用。

第二章 能源行业数据安全基本职责

第六条 在国家数据安全工作协调机制统筹协调下，国家能源局

负责能源行业数据安全监督管理，督促指导各省、自治区、直辖市和新疆生产建设兵团能源主管部门（以下简称省级能源主管部门）开展数据安全监督管理，督促指导国务院国资委管理的能源企业（以下简称能源央企）和国家能源局指导监管的全国性能源行业协会依法依规履行能源数据处理者责任义务，组织制定和发布能源行业数据分类分级标准规范，审核并确定能源行业重要数据目录，向有关部门提出核心数据目录建议并实行动态管理，加强能源行业数据安全监测预警和应急处置能力建设。

第七条 省级能源主管部门负责对本地区能源行业数据处理活动和安全保护进行监督管理，督促指导本地区能源数据处理者（含能源央企在本地区的各级子公司、控股企业）依法依规履行能源数据处理者责任义务，按照能源行业数据分类分级标准规范，编制并按年度更新报送本地区能源行业重要数据目录，开展本地区能源行业数据安全监测预警、信息报送、制定应急预案、开展应急处置等工作。

第八条 能源数据处理者应依法依规履行数据安全保护责任义务。能源行业重要数据和能源行业核心数据的处理者对自身的数据安全负主体责任，应明确数据安全负责人和管理机构，本单位法定代表人或者主要负责人是数据安全第一责任人，分管数据安全的领导是直接责任人。能源央企负责对其各级子公司、控股企业的数据处理活动和安全保护进行监督管理。

第九条 能源数据处理者应依照能源行业数据分类分级标准规

范，识别并编制本单位能源行业重要数据目录，按照数据载体所在地省级能源主管部门要求报送重要数据目录。能源央企各级子公司、控股企业编制的能源行业重要数据目录，应按照数据载体所在地省级能源主管部门和能源央企总部要求分别报送。

重要数据目录报送内容包括但不限于数据类别、级别、规模、精度、来源、载体、适用范围、对外共享、跨境传输、安全情况及责任单位等数据字段信息，不包括数据内容本身。

第十条 省级能源主管部门、能源央企分别负责汇总审核本地区、本企业的能源行业重要数据目录，并报送国家能源局。对按程序确认为能源行业重要数据和能源行业核心数据的，省级能源主管部门、能源央企应及时告知能源数据处理者。

第十一条 上一次报送重要数据目录后，能源行业重要数据、核心数据的级别、责任主体情况、数据处理情况、数据安全情况内容发生重大变化的，能源数据处理者应在三个月内重新按程序报送重要数据目录。

第三章 能源行业数据保护要求

第十二条 能源数据处理者开展数据处理活动，应建立健全数据安全管理制度，明确数据全生命周期各环节的管理要求；定期组织开展能源行业数据安全知识和技能教育培训。能源行业重要数据、能源行业核心数据的处理者应建立数据安全工作体系，加强人员和经费保障，并配合有关部门开展监督检查工作。

第十三条 利用互联网等信息网络开展能源行业数据处理活动

的，应落实网络安全等级保护、关键信息基础设施安全保护、密码保护和保密等制度要求。

存储处理能源行业重要数据的信息网络应落实三级及以上网络安全等级保护要求。

存储处理能源行业核心数据的信息网络，如涉及关键信息基础设施，应在网络安全等级保护制度的基础上，落实关键信息基础设施安全保护要求；不涉及关键信息基础设施的，应落实四级网络安全等级保护要求。

法律法规和国家有关规定要求使用商用密码进行保护的，还应遵守商用密码保护有关规定。

第十四条 能源行业重要数据的处理者应自行或者委托具有风险评估能力的第三方评估机构，对其数据处理活动每年至少开展一次风险评估，及时整改风险问题，并按省级能源主管部门要求报送风险评估报告。省级能源主管部门、能源央企应将本地区、本企业数据安全风险评估情况按年度报送至国家能源局。

风险评估报告应当准确、清晰地描述评估活动的主要内容，具体包括但不限于数据处理者基本信息，评估团队基本情况，开展数据处理活动的情况及其合规性评价，处理的能源行业重要数据的种类、数量，面临的数据安全风险及其应对措施，风险评估结论和整改建议等要素。

第十五条 能源行业数据安全风险评估重点评估以下内容：

（一）能源行业重要数据和核心数据识别认定的基本情况、所

处安全状态及风险分析；

（二）数据处理活动是否合法、正当、必要；

（三）数据安全负责人、管理机构、岗位配备和职责履行情况；

（四）全流程数据安全管理制度及保障机制的建立和落实情况；

（五）数据处理活动相关人员管理和教育培训情况；

（六）国家数据分类分级保护制度落实情况，以及对能源行业重要数据和核心数据保护要求落实情况；

（七）数据安全技术防护能力建设及应用情况；

（八）已发生的数据安全案事件和处置情况，以及数据安全风险监测预警工作落实情况；

（九）涉及数据提供、转移、委托处理、共同处理的，数据接收方的安全保障能力、责任义务约束和履行情况；

（十）其他涉及数据安全的有关情况。

第十六条 能源行业重要数据的处理者在重要数据的收集、存储、使用、加工、传输、提供、公开、删除等环节，应综合运用加密、鉴权、认证、脱敏、校验、审计等技术手段进行安全保护。

第十七条 能源行业重要数据的处理者，应按照业务需要和最小授权原则，依据岗位职责设定数据处理权限，控制重要数据的接触范围，发生人员变动时应及时调整权限。

第十八条 能源行业重要数据的处理者应加强对数据共享、调用的安全管控，采取技术措施定期监测数据共享、调用情况，并配备风险隔离、认证鉴权、威胁告警等安全保护措施。

第十九条 委托他人处理或者与他人共同处理能源行业重要数据的，委托人应当提前告知受托人数据等级，数据安全责任不因委托而改变。委托方应严格审批明确受托方的数据处理权限和保护责任，监督受托方履行数据安全保护义务。受托方应依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供能源行业重要数据。

涉及使用云计算服务处理能源行业重要数据的，可以选择通过云计算服务安全评估的云计算服务，并遵守本管理办法有关要求。

第二十条 未经委托方批准，涉及能源行业重要数据的信息系统建设、运维项目不得转包、分包。

未经委托方明确授权，涉及能源行业重要数据信息系统建设、运维人员不得处理委托方的重要数据。

对涉及能源行业重要数据的信息系统建设、运维过程中收集、产生的数据，不得用于其他用途，服务完成后按照与委托方约定处理或者及时删除。

第二十一条 能源行业重要数据处理活动应记录维护数据安全所需的日志，涉及安全事件处置、溯源的，相关日志留存时间不少于一年。涉及向他人提供、委托处理、共同处理能源行业重要数据的，相关日志留存时间不少于三年。

能源行业重要数据的处理者在组织数据安全风险评估时，应对其数据查询、下载、修改、删除等重点操作的日志开展审计分析，发现违规或者异常行为应采取相应处置措施。

第二十二条 能源行业重要数据的处理者因合并、分立、解散、被宣告破产等原因需要转移、销毁能源行业重要数据的，应采取必要的安全保护措施，并事前向省级能源主管部门报告数据处置方案。引起重要数据目录变化的，应及时向数据载体所在地省级能源主管部门报备。

第二十三条 在我国境内收集和产生的能源行业重要数据，确需向境外提供的，能源数据处理者应依法依规申报数据出境安全评估。

第二十四条 能源行业核心数据的处理者跨不同法人主体提供、转移、共享核心数据的，应采取必要的安全保护措施，并告知数据接收方按照对应级别进行分类分级保护。自当年度1月1日起可能累计达到上一年度末该项核心数据静态总量30%及以上的，应经国家能源局报有关部门组织风险评估；未达到30%的，由省级能源主管部门提出初步评估意见，报国家能源局开展评估。涉及国家机关依法履职、国家机关或企事业单位内部流动的能源行业核心数据除外。

第二十五条 能源行业核心数据的处理者在落实以上能源行业重要数据保护要求的基础上，可以采取以下措施加强对能源行业核心数据的保护：

（一）优先使用商用密码进行保护；

（二）优先使用安全可信的产品和服务；

（三）优先使用第三方评估机构开展风险评估；

（四）涉及核心数据安全事件处置、溯源的相关日志，留存时

间不少于三年；

（五）对相关关键岗位人员、涉及核心数据信息系统建设和运维单位等，依法依规提交公安机关、国家安全机关进行国家安全背景审查。

第二十六条 不同类别、级别数据同时被处理且难以分别采取保护措施的，应按照其中级别最高的要求实施保护，确保数据集整体持续处于有效保护和合法利用的状态。

第四章 能源行业数据安全监测预警和应急处置

第二十七条 省级能源主管部门、能源央企应分别加强本地区、本企业能源行业数据安全监测预警和应急处置能力建设，指导本地区数据处理者和能源央企各级子公司、控股企业做好风险监测、事件处置和报告等工作，强化对新技术新应用的能源行业数据安全风险研究和评估，强化对公开渠道数据汇聚、关联后可能引发能源行业数据安全风险的监测能力。

第二十八条 能源数据处理者发现数据安全缺陷、漏洞等风险时，应立即采取补救措施；发生数据安全事件时，应立即采取处置措施，按照规定及时告知相关用户并向省级能源主管部门报告，其中，能源央企各级子公司、控股企业应同步向能源央企总部报告。

风险监测预警的内容应包括：风险基本情况、可能产生的危害和程度、风险演化发展态势、可能影响的范围、处置风险的对策建议及其他应报告的情况。

事件情况报告的内容应包括：事件发生时间、事件简要经过、

造成的危害和影响、已采取的措施、下一步对策建议及其他应报告的情况。

第二十九条 本地区、本企业发生能源行业数据安全事件时，省级能源主管部门、能源央企应根据事件级别依法启动应急预案，采取相应应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

第三十条 省级能源主管部门、能源央企发现可能直接危害国家安全、经济运行、社会稳定、公共健康和安全，以及直接影响政治安全的重大或者特别重大的能源行业数据安全风险、事件，应于发现或者得知后1个工作日内将有关情况报送国家能源局，并按要求进行续报。紧急情况下可以通过电话联系方式及时报告，随后补报书面报告。国家能源局负责按规定向有关部门报告相关情况。

第三十一条 省级能源主管部门、能源央企完成重大或者特别重大能源行业数据安全应急处置工作后，应及时总结提炼经验，并于3个工作日内形成处置情况报告，于10个工作日内形成总结报告，分别报送国家能源局。国家能源局负责按规定向有关部门报送总结报告。

第五章 监督检查和法律责任

第三十二条 国家能源局和省级能源主管部门应当依照《网络数据安全管理条例》有关规定，对能源行业数据安全工作进行监督检查。

第三十三条 国家能源局和省级能源主管部门在履行数据安全

监督管理职责中，发现数据处理活动存在较大安全风险的，可以按照规定权限和程序约谈相关能源数据处理者，要求采取措施进行整改，消除隐患，并将问题线索及时移送有关主管部门。

第三十四条 对于违反本办法规定的行为，有关主管部门按照《中华人民共和国数据安全法》《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》《网络数据安全管理条例》等法律法规规定予以处理处罚；构成犯罪的，移送司法机关依法追究刑事责任。

第六章 附 则

第三十五条 开展涉及个人信息的数据处理活动，还应遵守有关法律法规的规定。

第三十六条 本办法由国家能源局负责解释。

第三十七条 本办法自2026年7月1日起施行，有效期5年。