ICS 35.110
CCS F 10

DB 14

山　西　省　地　方　标　准

DB 14/T 3552—2025

能源企业数据安全保护管理规范

2025－08－26 发布　　2025－12－01 实施

山西省市场监督管理局mVmV发　布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由山西省能源局提出、组织实施和监督检查。

山西省市场监督管理局对本文件的组织实施情况进行监督检查。

本文件由山西省能源标准化技术委员会（SXS/TC42）归口。

本文件起草单位：太原清众鑫科技有限公司、山西省煤炭规划设计院（集团）有限公司、中国矿业大学（北京）、中煤科工开采研究院有限公司、山西省市场监督管理局企业档案数据中心、大唐山西发电有限公司、中煤平朔集团信息产业公司、国网山西建设分公司、太原科技大学。

本文件主要起草人：靳黎忠、宋雪娇、左明、张燕平、田子建、庞义辉、赵明、王瑞、赵士杰、任健铭、肖华、高改梅。

能源企业数据安全保护管理规范

1 范围

本文件规定了能源企业开展数据安全保护工作的管理框架及总体要求、数据运行安全以及数据处理活动的安全保护措施。

本文件适用于能源企业开展数据安全保护工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239 信息安全技术 网络安全等级保护基本要求
GB/T 35295 信息技术 大数据 术语
GB/T 39786 信息安全技术 信息系统密码应用基本要求
GB/T 41479 信息安全技术 网络数据处理安全要求
GB/T 45577 数据安全技术 数据安全风险评估方法
DB14/T 3551 能源数据安全保护分类分级指南

3 术语和定义

GB/T 22239、GB/T 35295、GB/T 39786 、GB/T 41479、GB/T 45577、DB14/T XXXX界定的以及下列术语和定义适用于本文件。

3.1
数据处理活动
数据的采集、传输、存储、使用加工、交换、销毁等过程。

3.2
数据载体
数据处理活动中使用的系统、平台、设备、媒介等。

4 管理框架

能源企业数据安全保护管理框架由总体要求、数据运行安全和数据处理活动安全三个部分组成,见图1。总体要求从组织保障、制度管理、数据分类分级等方面奠定数据安全保护基础；数据运行安全从数据载体安全、权限管理、接口管理、日志管理、数据安全审计、风险监测预警与应急处置、数据安全评估、数据维护安全等方面规范了数据运行条件的安全保护措施；数据处理活动安全是能源企业数据安全保护管理框架的核心，明确了数据的采集、传输、存储、使用加工、交换、销毁等数据处理活动各个环节的安全保护要求。

能源企业按照管理框架对一般数据、重要数据采取对应数据级别的安全保护措施，核心数据、个人信息等涉及法律法规有专门管理要求的数据类别，按照有关规定和标准进行安全保护；重要数据涉及委托他人处理的情形，还应要求被委托方具备相应的数据安全保护能力，双方明确各自的数据安全责任和义务。管理框架具体如下：

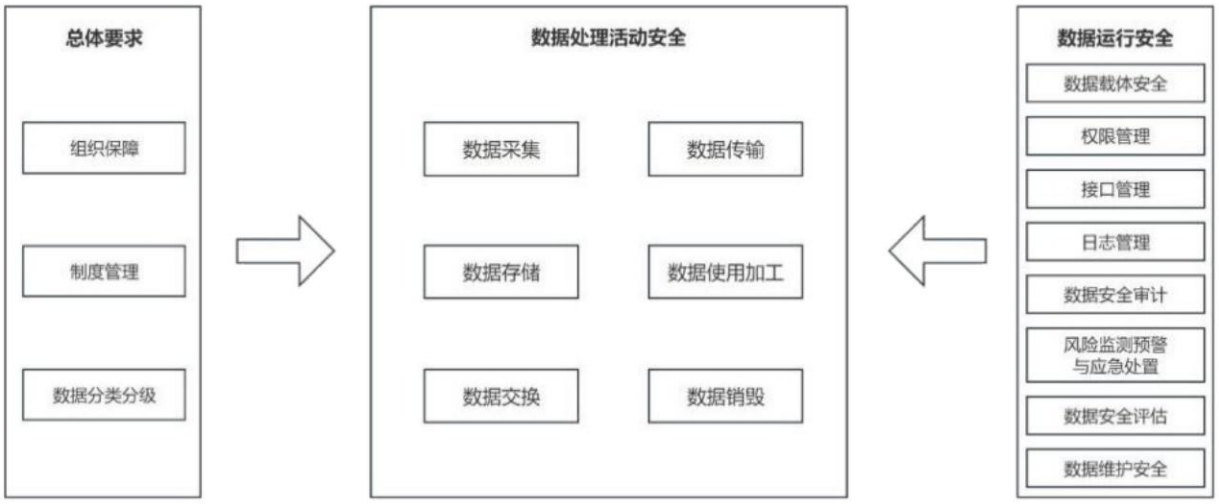

图 1　能源企业数据安全保护管理框架图

5　总体要求

5.1　组织保障

5.1.1　一般数据应符合以下要求：

a)　设立数据安全管理责任部门，明确数据安全责任人，统筹开展数据安全管理工作；

b)　数据安全管理机构设立数据安全管理员、数据安全审计员等岗位，定义各岗位职责，保障数据安全管理与审计工作开展；

c)　加强人员管理，明确人员录用、离岗、离职、安全教育培训、外部人员管理等方面的管理规定并严格落实；

d)　制定数据安全岗位人员教育和培训计划，对数据安全相关岗位人员定期开展教育培训。

5.1.2　重要数据除符合 5.1.1 的要求，还应符合以下要求：

a)　明确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，分管数据安全的负责人是直接责任人，每季度召开数据安全专项会议，协调其他相关部门与安全部门协同工作，并建立常态化沟通与协作机制；

b)　建立数据安全工作体系，覆盖数据安全责任部门以及研发设计、生产制造、经营管理、运行维护、外部服务、采购、审计、法务等相关部门；

c)　明确数据安全关键岗位，并与关键岗位人员签署保密协议；

d)　在数据安全培训过程中明确年度培训时长，并对参加培训的人员进行考核评定，考核不合格者暂停数据操作权限。

5.2　制度管理

5.2.1　一般数据应符合以下要求：

a) 建立数据安全管理制度体系，包括但不限于数据安全总体策略、组织机构与人员管理、数据分类分级、数据处理活动安全管理要求、数据访问控制、数据安全评估、数据安全审计、数据安全风险监测预警、数据安全应急与处置、数据安全教育培训、合作方管理、数据出境、投诉举报受理处置等制度；
b) 建立数据安全制度文件管理控制流程，规范制度文件的建立、审批、发布、修订和废止，实施文件版本控制，确保制度文件的及时更新和有效访问；
c) 定期对数据安全管理制度的合理性、充分性和适用性进行论证和评价，对存在不足或需要改进的数据安全管理制度进行修订。

5.2.2 重要数据除应符合 5.2.1 的要求外，宜建立监督评价机制，定期对数据安全管理制度落实情况进行评价。

5.3 数据分类分级

5.3.1 一般数据应符合以下要求：

a) 识别数据资源，形成数据资源清单；
b) 参照 DB14/T XXXX《能源数据安全保护分类分级指南》，建立能源企业自身数据分类分级规则，根据业务需求、数据来源和用途等因素，进行数据分类；根据数据重要程度和可能造成的影响程度，确定数据安全级别，形成数据分类分级清单；
c) 根据数据资源变动和分类分级要求变动等情况，及时更新数据分类分级清单。

5.3.2 重要数据除符合 5.3.1 的要求外，还应按照有关要求识别并形成重要数据目录，并按有关程序报送。

6 数据运行安全

6.1 数据载体安全

6.1.1 一般数据应符合以下要求：

a) 对处理一般数据的系统、平台等数据载体，采取不低于 GB/T 22239 第二级要求的安全防护措施；
b) 对数据库、研发终端、生产设备、开发代码库等数据载体进行安全配置，建立安全配置清单，定期进行配置审计；
c) 及时对数据载体的安全漏洞采取升级措施，短期内无法升级的，开展针对性安全加固；
d) 规范数据载体的登录账户及口令管理，避免使用默认口令或弱口令，并定期更换口令。

6.1.2 重要数据除符合 6.1.1 的要求，还应符合以下要求：

a) 对处理重要数据的系统、平台等数据载体采取不低于 GB/T 22239 第三级要求的安全防护措施；
b) 对涉及重要数据处理活动的数据载体的访问行为进行双因子身份鉴别；
c) 对处理重要数据的系统、平台、设备等数据载体采取 GB/T 39786 第三级密码应用保护措施。

6.2 权限管理

6.2.1 一般数据应符合以下要求：

a) 根据企业业务范围和岗位职责明确数据安全管理审批事项；
b) 遵循安全策略和最小授权原则，合理界定数据处理权限；
c) 对开展数据处理活动的平台系统操作使用权限，明确审批流程和操作要求，使用技术手段进行权限管理；

d) 在人员变更、调离或终止劳动合同时，及时变更或终止其权限。

6.2.2 重要数据除符合 6.2.1 的要求，还应符合以下要求：

a) 建立内部登记、审批机制，明确数据安全授权审批事项、审批部门和审批人等；
b) 定期对人员数据处理权限分配情况进行复核；
c) 对处理重要数据的系统、平台，具备基于 IP 地址、账号与口令和多因子认证等身份鉴别手段。

6.3 接口管理

6.3.1 一般数据应符合以下要求：

a) 明确数据接口的安全要求、管控措施和控制策略；
b) 规范数据接口调用的审批流程；
c) 定期梳理数据接口，形成接口清单，明确不同接口的类型、数据内容、频次、上下游信息系统等信息，并动态更新接口活动状态（如新增、活跃、失活、复活、下线等接口状态）；
d) 对数据接口定期开展安全检测，及时发现并处置数据安全风险隐患，不符合要求的接口及时整改或关停；
e) 在数据接口调用前进行身份鉴别，通过技术手段对接口输入参数进行限制或过滤；
f) 接口调用时，明确数据的使用目的、供应方式、保密约定及数据安全责任等情况；
g) 对相关接口调用行为和数据交互行为进行监测，留存相关日志记录。

6.3.2 重要数据除应符合 6.3.1 的要求外，宜实现对异常数据接口调用行为自动预警、拦截功能。

6.4 日志管理

6.4.1 一般数据应符合以下要求：

a) 对数据处理日志、权限管理日志、人员操作日志等进行记录；
b) 日志的留存时间不少于六个月。

6.4.2 重要数据除符合 6.4.1 的要求，还应符合以下要求：

a) 对高风险操作（如批量复制、批量传输、批量销毁等操作）日志进行备份；
b) 涉及重要数据安全事件处置、溯源的，相关日志留存时间不少于一年；
c) 涉及向他人提供、委托处理、共同处理重要数据的，相关日志留存时间不少于三年。

6.5 数据安全审计

6.5.1 一般数据应符合以下要求：

a) 制定数据安全审计制度，审计覆盖数据处理活动各环节，明确数据安全审计策略、审计对象等要求；
b) 定期对数据处理活动各环节的数据访问和操作进行安全审计，并形成数据安全审计情况总结。

6.5.2 重要数据除符合 6.5.1 的要求外，还应对数据访问、数据服务调用以及查询、修改、更新、删除、导出、共享、交换备份、恢复等关键操作进行安全审计，并采取技术措施保护审计记录的完整、准确、真实、有效。

6.6 风险监测预警与应急处置

6.6.1 一般数据应符合以下要求：

a) 开展数据安全风险监测，及时发现数据安全缺陷、漏洞等问题隐患，并立即采取补救措施；
b) 对发现的各类数据安全事件及风险进行分析研判、预警通报；
c) 建立数据安全应急处置机制，针对事件不同类别、级别、影响范围等因素，制定数据安全事件应急预案，明确应急处置的责任分工、工作流程和处置措施等；

d) 定期和在重大活动开始之前开展数据安全应急演练，并留存演练记录；
e) 如发生数据安全事件，立即启动应急预案，采取相应的应急处置措施，留存处置过程记录，编写事件报告并按规定上报。

6.6.2 重要数据除符合 6.6.1 的要求外，涉及重要数据的数据安全事件，还应按照有关规定进行上报，并开展事态跟踪分析，及时采取相关措施降低事件影响。

6.7 数据安全评估

6.7.1 一般数据和重要数据应符合以下要求：
a) 能源数据处理者依据 GB/T 45577 有关要求，自行或委托第三方评估机构开展数据安全风险评估；
b) 对需申报数据出境安全评估的情形按要求开展数据出境风险评估。

6.8 数据维护安全

6.8.1 一般数据应符合以下要求：
a) 建立数据安全运维管理制度，规范作业流程，指导数据维护人员开展数据安全监测、维护、风险处置、应急响应等工作；
b) 建立统一运维入口，运维人员仅可通过唯一入口进行运维管理；
c) 加强数据权限管控，严格限制运维人员对数据进行更新、删除、修改等，非必要不授权，严格落实数据权限变更审批。

6.8.2 重要数据除符合 6.8.1 的要求，还应符合以下要求：
a) 进行数据独立运维管理，仅必要环节允许被授权维护人员对数据开展维护；
b) 对维护人员的数据操作行为进行记录与审计。

7 数据处理活动安全

7.1 数据采集

7.1.1 一般数据应符合以下要求：
a) 明确数据采集的目的、范围、类型、渠道、频度、流程等，保证数据采集的合法性、正当性、必要性、一致性（如煤矿感知数据采集应符合《煤矿感知数据接入规范》中第 5 章采集要求；电力监控系统数据采集应符合《电力监控系统安全防护规定》，生产控制大区与管理信息大区间数据交互需通过横向隔离装置）；
b) 采用人工核查或技术措施对外部数据的真实性、有效性、安全性进行鉴别，避免采集不明来源的数据；
c) 根据 DB14/T XXXX《能源数据安全保护分类分级指南》，结合能源企业实际情况对生成或采集的数据进行分类分级标识；
d) 通过间接途径获取数据的，与数据提供方通过签署相关协议、承诺书等方式，明确双方法律责任。

7.1.2 重要数据除符合 7.1.1 的要求，还应符合以下要求：
a) 加强数据采集人员的管理，对数据采集的来源、时间、类型、数量、频度、流向等信息进行记录和审计，避免出现超范围数据采集活动；
b) 定期对数据采集的精度和完整性进行校验，确保采集数据的准确性；

c) 具备对数据采集行为进行监测的技术能力，确保数据采集的合规性和执行的一致性，并能够在发现异常时进行告警；
d) 对数据采集终端或系统进行接入授权，仅授权的设备 IP 和端口号可以通信，并为授权人员分配独立且唯一的账号，防止恶意工具非法采集数据。

7.2 数据传输

7.2.1 一般数据应符合以下要求：
a) 根据应用场景、数据类型、数据级别和安全域等因素，制定数据传输安全策略；
b) 对数据传输两端进行身份鉴别，确保数据传输双方可信任。

7.2.2 **重要数据除符合 7.2.1 的要求，还应符合以下要求：**

a) 数据跨不同网络区域或安全域传输时，采用技术手段进行安全隔离和访问控制；
b) 采用满足 GB/T 39786、GB/T 22239 要求的密码加密技术和校验技术，保证数据传输过程的保密性和完整性；
c) 针对受条件限制无法通过网络传输的工业现场数据，可采用受控加密的移动存储介质实现数据安全传输；
d) 宜采用数据传输异常检测技术，对陌生 IP 地址、数据库异常连接等进行实时告警，在检测到数据遭破坏时及时采取恢复措施。

7.3 数据存储

7.3.1 一般数据应符合以下要求：
a) 制定数据存储管理制度，对安全管控措施、数据访问流程、访问控制、介质管理、存储时限等作出规定；
b) 明确数据备份与恢复安全策略，建立数据备份恢复操作规程，说明数据备份周期、备份方式、备份地点、数据恢复性验证机制等；
c) 采取有效的技术和管理手段对数据存储介质进行安全保护。

7.3.2 重要数据除符合 7.3.1 的要求，还应符合以下要求：
a) 采用满足 GB/T 39786、GB/T 22239 要求的密码加密技术和校验技术，保证数据存储过程中的保密性和完整性；
b) 定期开展数据备份和恢复测试，对备份数据的有效性和可用性进行检查和恢复验证；
c) 数据存储备份有行业要求的，从其规定（如煤矿企业安全监控、人员位置监测、图纸、技术资料等数据的存储备份符合《煤矿安全规程》有关要求；重要电力监控系统的重要数据备份恢复符合《电力监控系统安全防护规定》有关要求）；
d) 在中国境内存储。

7.4 数据使用加工

7.4.1 一般数据应符合以下要求：
a) 明确数据使用业务场景的目的、范围、审批流程（含权限授予、变更、撤销等）、人员岗位职责等，在保障安全、数据合法正当使用的情况下开展数据使用加工；
b) 对测试过程中产生的过程性数据采取防护措施；
c) 对矿山大模型、智慧电厂等人工智能服务的训练数据处理活动进行安全管理，采取能够有效防范和处置数据安全风险的措施。

7.4.2 重要数据除符合 7.4.1 的要求外，还应使用去标识化、匿名化访问控制、数据脱敏等技术措施保

障重要数据使用加工过程的安全性。

7.5 数据交换

7.5.1 一般数据应符合以下要求：

a) 明确数据提供的范围、数量、条件、程序、时间等，建立跨网、跨安全域的数据提供安全操作规范；

b) 共享、转让、委托处理数据的，与数据接收方通过合同等方式，明确数据使用目的、供应方式、保密约定、范围、数据安全保护要求等内容，规定数据接收方的责任、义务并进行监督，留存共享、转让情况及安全管理记录。

7.5.2 重要数据除符合 7.5.1 的要求，还应符合以下要求：

a) 履行严格的审批流程，并与数据获取方签订数据安全协议，对数据获取方的数据安全保护能力进行核验；

b) 采取数据加密、数据脱敏、数据水印等必要的技术防护措施；

c) 在数据接入互联网等活动中，开展数据安全风险监测，对安全风险高的网络出口和资产，加强网络边界的身份认证和访问控制。

7.6 数据销毁

7.6.1 一般数据应符合以下要求：

a) 建立数据销毁制度，明确销毁数据对象、规则、流程、技术等要求；

b) 对数据销毁活动进行记录，记录数据销毁的审批、实施过程，以及被销毁数据的情况等。

7.6.2 重要数据除符合 7.6.1 的要求，还应符合以下要求：

a) 保证数据销毁后不被恢复；

b) 数据销毁后，及时更新数据清单和目录，并按有关要求报备。

参 考 文 献

[1] GB/T 37988 信息安全技术 数据安全能力成熟度模型

[2] YD/T 4982 工业企业数据安全防护要求

[3] 数据安全法（2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过）

[4] 个人信息保护法（2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过）

[5] 关键信息基础设施安全保护条例（中华人民共和国国务院令 第745号，2021年9月1日）

[6] 网络数据安全管理条例（中华人民共和国国务院令 第790号，2024年9月30日）

[7] 数据出境安全评估办法（国家互联网信息办公室令 第11号，2022年5月19日）

[8] 自然资源领域数据安全管理办法（自然资发〔2024〕57号，2024年3月22日）

[9] 煤矿安全规程（中华人民共和国应急管理部令 第17号，2025年8月4日）

[10] 电力监控系统安全防护规定（中华人民共和国国家发展和改革委员会令 第27号，2024年11月25日经国家发展改革委第18次委务会议审议通过）

[11] 煤矿感知数据接入规范（试行）（应急管理部科技和信息化工作领导小组办公室，2019年5月）