ICS
点击此处添加中国标准文献分类号

团　　体　　标　　准

T/××× ××××—××××

能源大数据 数据生存周期安全技术规范

Data standard of energy big data:data life cycle security protection technical specifications

××××－××－××发布　　××××－××－××实施

中国能源研究会　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》给出的规则编制。

本文件由中国能源研究会提出。

本文件由电力行业信息标准化技术委员会（DL/TC27）归口。

本文件起草单位：国网山东省电力公司电力科学研究院、国网山东省电力公司、国家电网有限公司大数据中心、湖南能源大数据中心有限责任公司、国网泰安供电公司、国网山东省电力公司经济技术研究院、国网宁夏省电力公司、国网甘肃省电力公司、国网辽宁省电力公司、国网河南省电力公司、国网信息通信产业集团有限公司、石化盈科信息技术有限责任公司、安徽南瑞继远电网技术有限公司、山东省委网信办、国家计算机网络与信息安全管理中心、山东能源集团有限公司。

本文件主要起草人：

本文件首次发布。

本文件在执行过程中的意见或建议反馈至中国电力企业联合会标准化管理中心（北京市白广路二条1号，100761）。

能源大数据　数据生存周期安全防护技术规范

1　范围

本标准规定了能源行业数据从数据采集、传输、存储、处理、交换、销毁等全生命周期各环节安全防护技术及管理要求。

本标准适用于指导能源大数据全生命周期安全防护工作。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 24874-2010　草地资源空间信息共享数据规范

GB/T 25069-2022　信息安全技术　术语

GB/T 35295-2017 信息技术 大数据 术语

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 39477-2020 信息安全技术 政务信息共享 数据安全技术要求

DL/T 1757　电子数据恢复和销毁技术要求规定

Q/GDW 1937　国家电网公司非国家秘密电子数据销毁、清除和恢复技术要求

3　学术和定义

GB/T 25069-2022、GB/T 35295-2017、GB/T 37988-2019、GB/T 39477-2020界定的以及下列术语和定义适用于本文件。

3.1

数据全生命周期 data life cycle

数据从产生，经过数据采集、数据传输、数据存储、数据处理（包括加工、分析、使用），数据交换，直至数据销毁等各种生存形态的演变过程。

3.2

能源大数据 energy big data

水、电、煤、天然气、油等行业在生产、经营、消费和管理过程中产生的数据，以及宏观经济运行、生态环境、气象等能源行业密切相关的数据。

3.3

企业重要能源大数据 important enterprise energy big data

在公司经营管理过程中产生与公司利益密切相关的且存在一定的社会影响的能源大数据数据。

3.4

一般能源大数据 general energy big data

涉及电力、新能源、煤炭、石油、热力、自来水、天然气等能源领域的可在互联网上直接获取的公开能源大数据。

3.5

政务数据 government data

各级政务部门及其技术支撑单位在履行职责过程中依法采集、生成、存储、管理的各类数据资源。例如气象数据、管廊数据等。

注：根据可传播范围，政务数据一般包括可共享政务数据、可开放公共数据及不宜开放共享政务数据。

[GB/T 38664.1-2020,定义3.1]

3.6

个人敏感信息 personal sensitive information

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

[GB/T 35273-2020,定义 3.2]

3.7

数据脱敏 data desensitization

通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。

3.8

数据共享 data sharing

不同用户或不同系统按照一定的规则共同使用根据协议形成的数据。用户可以通过多种程序设计语言成查询语言去使用这些数据。

[GB/T 24874-2010,定义3.3]

3.9

数据清洗 data cleansing

从记录集、表或数据库中检测并纠正(或删除)损坏或不准确的记录的过程，指识别数据的不完整、不正确、不准确或无关的部分，然后替换、修改或删除脏数据或粗糙数据。

3.10

数据集成 data integration

数据集成是将电子文本、相关数据的内容信息、结构信息、背景信息采用标准和规范手段，进行编码、聚合、重组，使其成为一个有机整体，以便集中、交汇和共享。

3.11

数据擦除 data erasure

数据擦除是针对数据恢复行为而产生的逆向操作，用以保证数据无法被恢复。

3.12

数据销毁 data destruction

数据销毁是指采用各种技术手段将计算机存储设备中的数据予以彻底删除，避免非授权用户利用残留数据恢复原始数据信息，以达到保护关键数据的目的。

3.13

能源大数据负面清单 energy big data negative list

能源大数据负面清单是能源行业中依据法律法规与公司数据管理要求有条件公开或不予公开的能源大数据清单。

3.14

能源大数据应用 energy big data application

通过对能源大数据统一管理、加工和应用对内、对外提供不同数据服务的过程。

3.15

能源大数据服务 energy big data service

业务流程的接口，通常通过web应用程序接收或交付数据属性。

3.16

数据服务提供方 data provider

决定数据信息处理的目的和方式，实际控制数据信息，处理数据信息的组织或个人。

3.17

数数据服务需求方 date demander

从数据服务者中获取数据信息并加以利用的组织或个人。

3.18

数据分析 data analysis

数据分析是对组织各项经营管理活动提供数据决策支持而进行的组织内外部数据分析或挖掘建模,以及对应成果的交付运营、评估推广等活动。

3.19

能源大数据中心 energy big data center

以电力数据为基础，汇集全能源、各环节数据，以数据价值应用和能效分析服务为核心的功能完善、资源共享、服务多元、供需对接的能源大数据平台。

4 能源大数据分级分类模型

4.1 能源行业数据安全级别划分

能源行业数据依据数据重要性、敏感性进行安全分级，并实行差异化防护，主要划分为商密数据、企业重要数据、一般数据；推荐在数据共享等环节，结合各单位自身数据共享负面清单开展。数据安全分级如表1所示。

表 1 数据安全分级示例表

数据安全分级	说明
商密数据	为公司所有、且不为公众所知悉，具有实际或潜在的商业价值的技术信息和经营信息。
企业重要数据	在公司经营管理过程中产生的不涉及商业秘密，但与公司利益密切相关的

	且存在一定的社会影响的数据。
一般数据	除商密数据和企业重要数据之外，公司在生产经营管理过程中产生的数据。

[Q/DGW 12111-2021,定义5.2]

4.2 能源大数据安全级别变更

数据安全级别变更应遵循以下原则：

a) 一般数据经过整合、关联之后，可转化为企业重要数据；

b) 单次请求处理的一般数据规模超过一定的数量，其数据安全管控等级可上升一级；

c) 企业重要数据可经过数据脱敏处理后转换为一般数据；

d) 随着时间、空间的变化，数据安全级别可能会发生变化，宜定期进行再评估。

[Q/DGW 12111-2021,定义5.3]

5 能源大数据参与者分类要求

5.1 能源大数据参与者分类

依据能源行业数据产生、加工及使用角色的不同，能源行业数据参与者划分应参考 GB/T 35589-2017 要求，宜包含数据提供者、数据对外服务提供者、数据消费者。

a) 数据提供者：负责将新的行业数据或信息引入大数据系统的实体或其他系统；

b) 数据对外服务提供者：负责执行行业数据对外服务操作的实体及系统，以满足系统调用者定义的需求以及安全和隐私保护需求；

c) 数据消费者：使用行业数据对外服务提供者提供的服务的末端用户或其他系统。

5.2 能源大数据参与者职责要求

数据参与者是数据对外共享的参与主体，参与者应遵守相关职责，明确其相关权力及义务。

a) 数据提供者应明确数据消费者的数据共享和交换需求，数据分发范围，对数据分类分级为商密数据、企业数据和一般数据，是否需要脱敏处理，并如实提供数据给数据对外服务提供者；

b) 数据对外服务提供者应保障数据提供者所提供数据的全生命周期安全性，加工数据，并对数据消费者提供对外数据服务；

c) 数据消费者应遵守数据对外服务的服务规范，保障数据安全，不得损害数据提供者公司、数据对外服务提供者等相关方利益。

6 数据采集安全技术要求

6.1 基本要求

基本要求包括：

a) 应设置采集访问控制及可信认证技术防护手段；

b) 数据源服务器应设置漏洞更新、主机加固和病毒防护等安全技术防护手段。

6.2 增强要求

增强要求应符合下述要求：

a) 宜采取必要的安全技术手段，对采集到数据进行完整性、真实性和一致性校验；
b) 宜采取数据跟踪技术跟踪记录数据收集获取过程，确保数据收集过程的可追溯性；
c) 宜采取动态建模等技术手段，明确数据的获取源、收集范围、方式和频度，确保数据采集和获取仅为业务所需的数据最小集；
d) 宜对数据采集过程进行审计及异常事件告警，内置审计规则宜适用多种数据来源，如OSS、RDS、MaxCompute、PolarDB等，并按照访问内容敏感类型、访问内容敏感程度、库、表、字段、访问源、数据库实例等多种维度进行审计规则设置，审计规则宜涵盖范围详见表1。

表 3 审计规则涵盖范围

审计规则涵盖类别	子项
异常操作	应用账号风险操作
	运维人员风险操作
	数据库探测
数据泄露	拖库攻击
	数据库外联
	大流量返回
漏洞攻击	缓冲区溢出
	存储过程滥用
	拒绝服务漏洞
	隐通道攻击
SQL 注入	SQL 注入尝试利用
	疑似 SQL 注入
	基于报错的 SQL 注入
	基于时间的 SQL 注入

7 数据传输安全技术要求

7.1 传输保密性

7.1.1 基本要求

基本要求包括：

a) 应结合数据传输场景，选用满足数据安全传输需求的传输通道类型接入公司网络；

b) 建立数据传输通道前，应对数据传输终端进行身份鉴别和认证；
c) 建立数据传输通道时，应采用加密算法、数据脱敏或其他措施对数据进行保护，采用国家密码主管部门认可的密码技术确保数据传输通道安全；

7.1.2 增强要求

增强要求包括：
a) 建立数据传输通道前，宜对传输两端的身份进行双向鉴别和认证；
b) 必要时可采用加密算法、数据脱敏等技术对数据传输双方身份进行隐私保护；
c) 宜采用国家密码主管部门认可的密码技术保证传输过程中的数据保密性和抗抵赖性；
d) 必要时可采用专用传输协议或安全传输协议服务，避免来自基于协议的攻击破坏保密性。

7.2 传输完整性

7.2.1 基本要求

基本要求应符合下述要求：
a) 应采用数据完整性校验技术，对数据进行传输完整性保护。

7.2.2 增强要求

增强要求包括：
a) 宜采用通信延时和中断处理等技术对数据进行传输完整性保护；
b) 在检测到完整性遭到破坏时，宜采取相关技术措施来恢复或重新获取数据。

7.3 传输可用性

7.3.1 基本要求

基本要求包括：
a) 传输数据中应包含时间标识等时间信息，以识别历史数据或超出时限的数据；
b) 数据传输时应采用容错技术，当数据存在可接受的误差时，保障系统正常运行；
c) 在检测到传输数据不可用时，应采用重载技术保证数据的正常获取。

7.3.2 增强要求

增强要求包括：
a) 数据中应包含时间标识，可采用加密技术保护时间标识字段；
b) 可采用数据传输链路冗余技术，保证数据传输可靠性和网络传输服务可用性；
c) 可充分利用传输通道的容错和服务质量等能力，保证实时性要求高的数据优先传输。

8 数据存储安全技术要求

8.1 基本要求

基本要求包括：
a) 一般能源大数据可存储于互联网大区和管理信息大区，经过数据脱敏处理后，可长期存储于互联网大区；
b) 应根据数据的敏感程度采用数据访问授权、用户身份标识、数据访问控制、权限分配及相关技术，规避对存储数据的未授权访问风险；

c) 能源大数据中心每半年应开展一次数据复制、备份和恢复，实现对存储数据的冗余性管理，保护数据的可用性；
d) 针对数据存储服务器，应每年进行一次漏洞更新、主机加固和病毒防护；
e) 应对移动存储介质的接入行为等数据存储过程进行审计，审计规则涵盖范围详见表1，并对异常事件告警。

8.2 增强要求

增强要求包括：
a) 企业重要能源大数据存储时，宜采用国家密码主管部门认可的密码技术保证存储过程中的完整性和保密性；
b) 对企业重要能源大数据，宜采用数据完整性检测和恢复技术，保证在检测到数据完整性受到破坏时采取必要的恢复措施；
c) 数据存储终端宜保留最少的个人敏感数据，并限制数据存储量和保留时间，禁止本地明文存储支付密码等客户信息数据；
d) 宜将个人敏感信息脱敏数据与可用于恢复、识别个人敏感信息的数据分开存储。
e) 应定期将重要外部数据更新备份至灾备机房。

9 数据处理安全技术要求

9.1 基本要求

基本要求应符合下述要求：
a) 应采用身份鉴别和认证技术，限定用户可访问数据范围；
b) 应采用数据防泄露技术，防止数据处理过程中的调试信息、日志记录、不受控制输出等受保护的敏感信息泄露；
c) 应采用加密算法、数据脱敏等技术手段保证数据分析结果不泄露敏感数据信息。

9.2 增强要求

增强要求包括：
a) 宜采用相关技术加强对企业重要能源大数据处理、分析、使用异常行为的识别、监控和预警；
b) 个人敏感信息的分析、使用宜采用加密算法、数据脱敏等技术手段避免精确定位到特定个人，避免信用、资产和健康等敏感数据；
c) 宜对企业重要能源大数据处理、分析、使用过程中的数据操作进行记录，通过日志审计进行分析溯源及追责，并对审计记录进行保护和备份，避免受到未预期的删除、修改或覆盖等；
d) 宜将数据脱敏技术运用于企业重要能源大数据处理、分析、使用过程；
e) 企业重要能源大数据在预处理、清洗、转换和加载过程中，宜采用数据完整性检测和恢复技术，保证产生问题时能有效恢复。

10 数据交换安全技术要求

10.1 数据导入导出

10.1.1 基本要求

基本要求包括：

a) 应对导入导出用户或终端进行身份鉴别、权限控制，保证身份可信及操作可审计；
b) 在导入导出完成后应及时对操作过程中产生的缓存或者临时数据进行擦除或销毁，且保证不可被恢复。

10.1.2 增强要求

增强要求包括：
a) 宜采取多因素身份鉴别技术对数据导入导出操作人员进行身份鉴别；
b) 宜采取服务监测技术对数据服务接口进行监测，确保数据导入导出过程安全可控；
c) 当数据脱离公司网络环境对外提供时，宜结合业务需求实施数据脱敏并添加数字水印；
d) 导出数据较多应选择文本文档，导出数据较少应选择SQL文档。

10.2 数据获取

10.2.1 基本要求

基本要求包括：
a) 数据获取应选用安全数据服务接口，强化接口间认证授权管控；
b) 应对数据获取过程进行监控和记录，确保数据获取过程可溯源、可审计。

10.2.2 增强要求

增强要求包括：
a) 宜采取多因素身份鉴别技术，加强对获取数据的人员或终端的身份鉴别、权限控制，确保获取操作安全可控。

10.3 数据共享

10.3.1 基本要求

基本要求包括：
a) 能源大数据中心应优先采用数据服务接口形式外发数据，加强接口间身份认证，安全检查以及植入数据脱敏、溯源等其他安全保护措施

10.3.2 增强要求

增强要求包括：
a) 宜提供统一途径（统一平台、统一出口、统一模型等）对企业重要能源大数据进行共享；
b) 宜采用标准化数据共享格式，确保高效获取共享数据；
c) 应定期评估数据共享机制、服务组件和共享通道的安全性；
d) 应采用数据加密、脱敏、溯源、安全通道等措施防止数据共享过程中企业重要能源大数据泄露；
e) 对于各级政务数据共享要求，应按照DB52/T 1540.5-2021。

10.4 数据发布

10.4.1 基本要求

基本要求应符合下述要求：
a) 应建立数据发布接口及发布格式规范，如提供机器可读的可扩展标记语言格式；

10.4.2 增强要求

增强要求包括：

a) 可建立数据公开数据库，根据数据级别和用户级别开放相应权限。

11 数据销毁安全技术要求

基本要求包括：

a) 应遵照Q/GDW 1937的要求进行数据和文件的归档和销毁；

b) 应确保存储过企业重要能源大数据的各类存储介质在报废、返厂维修、内部再利用等转作他用之前，依据 Q/GDW 1937与DL/T 1757规定，采用符合标准的设备及方法对存储介质进行有效处理，并做记录；

c) 数据擦除与销毁工具或设备应具有国家权威认证机构的认证；

d) 在使用数据擦除与销毁工具或设备过程中应严格遵守操作规范，并由专人操作并监督；

e) 对于本单位无法通过常规技术手段进行电子数据恢复、擦除与销毁的情况，可委托公司信息安全实验室或具有相关类别国家权威机构认证的机构处理。

12 数据安全防护管理

12.1 边界管控

边界管控安全要求如下：

a) 应在内网边界按照“最小权限”原则严格控制外部机构的访问权限，管控措施包括但不限于：防火墙、入侵防御、应用安全防护、API 网关、数据安全防护等；

b) 互联网区和外联接入区为不可控区域，应在内部可控区域与不可控区域之间进行隔离，并根据应用需求和数据传输需要逐一开通访问关系，默认为禁止访问；

c） 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间应采取技术手段进行隔离；

d) 应明确生产网络接入和数据传输接口开通相关审批流程；

12.2 访问控制

访问控制管理要求如下：

a) 依据数据的不同类型与安全级别设计不同的访问控制策略：

b） 应建立面向数据应用的安全控制机制，包括访问控制时效的管理和验证，以及应用接入数据存储的合法性和安全性取证机制，宜建立基于用户行为或设备行为的数据存储安全监测与控制机制。

12.3 安全监测

安全监测管理要求如下：

a) 对数据生命周期过程中数据的采集、查询、修改、删除、共享等相关操作进行跟踪，通过留存数据流动记录等方式，确保数据相关操作行为可追。

b) 应建立日常数据泄露、数据改、数据取、数据非法使用的风险监控机制，主动预防、发现和终止数据泄露异常行为，有效防范和化解风险。

c) 宜在内部各个关键节点，通过安全设备、探针等检测相关信息，包括但不限于设备指纹、上网行为口志、管理平台的审批口志、业务操作口志、数据库口志、流量口志；

12.4 安全审计

审计管理安全要求如下：

a) 应制定日志数据管理与安全审计规范，明确日志的存储、分析、检查等要求；

b) 安全审计范围应覆盖至每个有权使用数据的用户，包括但不限于数据库管理员、数据库用户、操作系统管理员、操作系统用户、存储介质管理员、业务管理员、业务使用者、存储介质用户等；

c) 宜搭建数据安全审计系统，对日志进行统一管理和处理，建立并执行审计策略，提供对审计记录进行统计、查询、分析及生成审计报表的功能，形成审计报告反馈相关部门；

d) 应具备审计记录分权管理能力，可针对不同的角色和组设置审计范围，各组无法看到自己管理的审计范围以外的数据，保证审计数据的安全；

12.5 检查评估

定期或不定期开展数据安全相关检查和评估，管理安全要求如下：

a) 应建立数据安全检查评估机制，定期制定数据安全检查评估计划；

b) 在产品或服务发布前，或业务功能发生重大变化时，应及时做好数据安全评估；

c) 在国家及行业主管部门的相关要求发生变化时，或在业务模式、信息系统、运行环境发生重大变更时，或发生重大数据安全事件时，应进行数据安全评估；

d) 针对检查评估过程中发现的问题，应指定责任部门，制定适宜的整改计划，并跟踪落实；

e) 应妥善留存有关安全评估报告，确保可供相关方查阅，并以适宜的形式对外公开；

12.6 应急响应与事件处置

制定应急响应预案，及时处置数据安全事件告警，并在重大事件发生时立即启动应急响应，安全要求如下：

a) 制定应急响应与事件处置规范，建立完善的应急响应与事件处置和问责机制，做好应急预案，组织应急演练，确保在紧急情况下重要信息资源的可用性；

b) 应依据国家及行业主管部门规定、事件性质、影响范围等，对安全事件进行分级管理；

c) 应制定安全策略，对不同级别的安全事件进行相应处置，重大事件发生后应及时启动应急响应机制；

d) 应按照主管部门有关规定，向主管部门上报数据安全事件及其处置情况；

e) 事件处置结束后，应分析和总结原因和存在的问题，形成调查记录和事件清单，调整数据安全策略，避免事件再次发生，并形成总结报告。