ICS 29.240
CCS P 62

DB43

湖　南　省　地　方　标　准

DB43/T 3366—2025

电力工业互联网数据安全技术要求

Technical requirements for data security of Electric Power Industrial Internet

2025－09－30 发布　　2025－12－30 实施

湖南省市场监督管理局　　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专利的责任。

本文件由中共湖南省委网络安全和信息化委员会办公室提出。

本文件由湖南省网络安全标准化技术委员会归口。

本文件起草单位：国网湖南省电力有限公司、湖南能源大数据中心有限公司、湖南省能源局、绿盟（湖南）网络安全技术有限公司、湖南郴电国际发展股份有限公司。

本文件主要起草人：孙毅臻、田建伟、周鹏、田峥、罗豪凯、吴雨希、刘晓盼、蒋毅舟、马骏、许路、张俊、过耀东、曾旻睿、余琦、毛鑫、兰润芬、尹钢、刘俊均、徐旸。

电力工业互联网数据安全技术要求

1 范围

本文件规定了数据分类分级要求、数据采集安全技术要求、数据传输安全技术要求、数据存储安全技术要求、数据处理安全技术要求、数据交换安全技术要求、数据销毁安全技术要求。

本文件适用于电力企业、电力设备制造企业电力工业互联网数据安全保障工作。

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 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 35295 信息技术 大数据 术语

GB/T 37044 信息安全技术 物联网安全参考模型及通用要求

GB/T 37093 信息安全技术 物联网感知层接入通信网的安全要求

GB/T 43697-2024 数据安全技术 数据分类分级规则

3 术语和定义

GB/T 25069、GB/T 35295界定的以及下列术语和定义适用于本文件。

3.1

电力工业互联网 electric power industrial internet

以工业互联网五大功能体系（网络、标识、平台、数据、安全）为技术底座，实现电力系统全链条数字化连接与智能协同的新型基础设施。

4 数据分类分级要求

4.1 数据分类

数据分类要求主要包括：

a） 数据分类应符合GB/T 43697-2024中第5章要求；

b） 应参考数据资源产生来源方、权利所有方等要素进行分类，在产生来源方、权利所有方存在冲突时，优先参考数据资源产权所有方进行数据分类；

c） 宜按平台数据、个人信息、公共数据进行分类，判定规则可参考A.1。

4.2 数据分级

数据分级要求主要包括：

a） 数据分级应符合GB/T 43697-2024中第6章要求；
b） 应总体划分为核心电力数据、重要电力数据、一般电力数据三个级别，分级规则可参考A.2。

5 数据采集安全技术要求

5.1 生产经营数据采集

通过电力物联终端采集生产经营数据的安全防护,应遵循GB/T 37044、GB/T 37093要求。

5.2 个人信息采集

通过业务系统采集个人信息的安全防护，应遵循GB/T 35273要求。

5.3 第三方数据获取

第三方数据获取要求主要包括：
a） 应通过合法、正当方式从政府、企业等第三方单位获取数据，不应窃取或者以其他非法方式获取，不应将数据进行二次传播；
b） 应建立获取数据的合规管控流程，确认数据来源、安全要求、授权时限范围及各方安全责任等，通过签订合同、协议等方式明确数据用途和双方权益。

6 数据传输安全技术要求

数据传输安全要求主要包括：
a） 应加强数据传输过程的安全监测，及时发现和预警核心数据、重要数据违规传输等行为；
b） 核心电力数据、重要电力数据的传输应进行加密；
c） 通过互联网APP等传输核心电力数据、重要电力数据时，应采取接入认证措施；
d） 与第三方单位传输电力数据时，宜采用专用光纤、第三方专线等方式建立安全通道，应采取校验技术、密码技术、安全传输通道或者安全传输协议等措施保障数据安全。

7 数据存储安全技术要求

7.1 一般电力数据存储

一般电力数据存储要求主要包括：
a） 可存储于专用网络区域；
b） 应根据数据安全级别和敏感程度建立数据访问授权机制，制定数据访问控制策略；
c） 应定期执行数据复制、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。

7.2 重要电力数据存储

重要电力数据存储要求主要包括：
a） 应满足7.1条相关要求；
b） 可存储于专用网络区域；
c） 应具有针对电力数据的完整性检测、告警和恢复机制，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；

d） 应提供异地备份功能，利用通信网络将数据备份至备份场地；
e） 应采用国家密码主管部门认可的密码技术保证数据存储的完整性和保密性。

7.3 核心电力数据存储

核心电力数据存储要求主要包括：
a） 应满足7.2条相关要求；
b） 应采用国家密码主管部门认可的密码技术加密存储于专用网络区域；
c） 应提供有效的磁盘保护方法或数据碎片化存储等措施，保证即使磁盘被窃取，非法用户也无法从磁盘中获取有效的数据；
d） 应建立数据异地灾难备份机制，保障业务的连续运行。

8 数据处理安全技术要求

8.1 数据分析

数据分析要求主要包括：
a） 应加强数据使用权限以及账号权限的管控；
b） 应采用终端敏感数据发现、水印、外发管控等措施，加强分析终端的数据保护；
c） 数据分析结果应进行安全评估，涉及重要电力数据、核心电力数据时应按需进行数据脱敏等处理；
d） 宜对数据违规流转、数据高危操作、数据异常访问等行为进行安全风险监测。

8.2 数据运维

8.2.1 事前授权

事前授权要求主要包括：
a） 应按照权限最小化和权限分离原则进行账号授权；
b） 应对运维人员批量修改数据、导出数据、删除数据、查看核心电力数据及重要电力数据等需求严格审核。

8.2.2 事中操作

事中操作要求主要包括：
a） 应采取技术措施加强对运维人员批量修改、导出、删除数据等高危操作的管控，采取访问权限认证、高危操作告警阻断等措施；
b） 应对运维过程中涉及的核心电力数据、重要电力数据进行脱敏处理；
c） 应采用终端敏感数据发现、水印、外发管控等措施，加强运维终端的数据保护。

8.2.3 事后审计

事后审计要求主要包括：
a） 应加强运维安全审计，及时发现和追溯非法访问、违规导出等行为。
b） 应定期清理未实名认证账号、建设期临时账号，回收高风险权限。

8.3 数据测试

数据测试要求主要包括：

a） 测试环境应禁止直接使用真实生产数据，确需使用的，按照最小化原则，并进行脱敏处理；
b） 应加强测试人员账号权限管控和违规操作监测；
c） 应将测试终端与测试人员角色强制绑定，并采取敏感数据识别、导出管控等措施，防范人员违规操作造成数据泄露；
d） 应采用终端敏感数据发现、水印、外发管控等措施，加强测试终端的数据保护。

9 数据交换安全技术要求

9.1 线上接口交互

线上接口交互按数据共享对象分为对内共享、对外共享，要求主要包括：
a） 应按需对数据进行脱敏、水印处理后再共享；
b） 应具备数据防泄露能力，对异常交互行为进行识别和阻断；
c） 对外共享时需对数据接收方数据安全防护能力进行评估确认。

9.2 线下导出共享

线下导出共享安全要求主要包括：
a） 应按需对数据进行脱敏、水印处理后再共享；
b） 数据导出目的终端应具备数据保护能力，实现终端外发管控、外发审计等。

9.3 数据协同应用

宜采取隐私计算等技术开展数据协同应用，实现各参与方数据可用不可见。

10 数据销毁安全技术要求

10.1 数据擦除

10.1.1 数据不再继续使用时，应采取覆写等逻辑销毁方式及时销毁，防范数据泄露。
10.1.2 涉及核心电力数据、重要电力数据的应重点进行销毁结果验证。

10.2 物理销毁

需要彻底销毁存储介质以及相关数据时，应采用物理摧毁、消磁等存储介质销毁手段，将存储介质中电子数据予以彻底删除，并确保存储介质不可以再次使用。

附 录 A
（资料性）
电力工业互联网数据分级分类参考规则与示范

电力工业互联网数据分级分类参考规则与示范，如表A.1、表A.2所示。

表A.1 电力工业互联网数据分类参考规则

数据分类	判断标准	示例
平台数据	是指在电力工业互联网业务运行、客户服务等活动中收集、产生的原始数据和衍生数据。	发电、送电调度计划、运行数据、设备安全分析等调度运行信息；购电管理、电量平衡、市场成员注册、电力电量等市场成员信息等。
个人信息	是指以电子或者其他方式记录的、与已识别或者可识别的自然人有关的个人信息，不包括匿名化处理后的信息。	身份证、户口本、军官证、护照、台胞证、驾驶证等个人信息数据；银行账号、公积金账号、存款信息等个人财产信息等。
公共数据	是指按照国家法律法规要求披露，或电力公司在提供公共服务中收集、产生，被纳入国家及地方公共数据范畴的数据，但不包含依照国家法律法规禁止披露或共享开放的数据，且不涉及个人信息。	用煤消费，耗煤量，库存总量，库存可用天数等能源消耗数据、年度交易品种、交易主体、交易规模、交易准入条件等市场结算数据等。

表A.2 电力工业互联网数据分级参考规则

数据分级	判断标准
核心数据	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，一旦被非法使用或共享，可能直接影响政治安全的数据。
重要数据	特定领域、特定群体、特定区域或达到一定精度和规模的，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、公共健康和安全的数据。
一般数据	核心数据、重要数据之外的其他数据。