|  |  |
| --- | --- |
| ICS |  |
| CCS | 点击此处添加CCS号 |

|  |
| --- |
| 43 |

湖南省地方标准

DB 43/T XXXX—XXXX

能源工业互联网平台数据安全技术要求

Technical requirements for data security of energy industry internet platform

（本征求意见稿完成时间：2025年2月17日）

XXXX - XX - XX发布

XXXX - XX - XX实施

湖南省市场监督管理局  发布

目次

[前言 III](#_Toc25413)

[1 范围 1](#_Toc18057)

[2 规范性引用文件 1](#_Toc4310)

[3 术语和定义 1](#_Toc9747)

[4 缩略语 1](#_Toc22688)

[5 能源工业互联网平台平台数据安全框架 2](#_Toc15899)

[6 数据分类分级要求 2](#_Toc23153)

[6.1 数据分类 2](#_Toc4750)

[6.2 数据分级 2](#_Toc10381)

[7 数据采集技术要求 3](#_Toc14971)

[7.1 生产经营数据采集 3](#_Toc7200)

[7.2 个人信息采集 3](#_Toc14164)

[7.3 第三方数据获取 3](#_Toc20989)

[8 数据传输技术要求 3](#_Toc30499)

[8.1 内部数据传输 3](#_Toc14980)

[8.2 终端数据传输 3](#_Toc24917)

[8.3 第三方数据传输 3](#_Toc15795)

[9 数据存储技术要求 4](#_Toc2838)

[9.1 一般数据存储要求 4](#_Toc15522)

[9.2 重要数据存储要求 4](#_Toc22353)

[9.3 核心数据存储要求 4](#_Toc17404)

[10 数据应用技术要求 4](#_Toc10183)

[10.1 数据交互安全技术要求 4](#_Toc7991)

[10.1.1 用户访问页面交互安全要求 4](#_Toc12258)

[10.1.2 线上接口交互安全要求 4](#_Toc15002)

[10.1.3 线下导出共享安全要求 5](#_Toc16182)

[10.1.4 数据协同应用安全要求 5](#_Toc29259)

[10.2 数据分析安全技术要求 5](#_Toc18621)

[10.2.1 数据中台分析场景 5](#_Toc7937)

[10.2.2 其他数据分析场景 5](#_Toc21852)

[10.3 数据运维安全技术要求 5](#_Toc29961)

[10.3.1 数据运维事前授权 5](#_Toc17205)

[10.3.2 数据运维事中操作 5](#_Toc12486)

[10.3.3 数据运维事后审计 5](#_Toc201)

[10.4 数据测试安全技术要求 5](#_Toc9166)

[10.5 数据销毁技术要求 6](#_Toc10753)

[10.5.1 数据擦除 6](#_Toc4180)

[10.5.2 物理销毁 6](#_Toc24204)

[10.5.3 个人信息销毁 6](#_Toc27776)

[附录A（资料性） 能源工业互联网平台数据分级分类规则与示范 7](#_Toc9278)

[附录B（资料性） 典型场景数据安全防护 10](#_Toc13793)

[B.1 数据交互场景 10](#_Toc32083)

[B.2 数据分析场景 10](#_Toc32033)

[B.3 数据运维场景 11](#_Toc22968)

[B.4 研发测试场景 11](#_Toc21664)

1. 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：

本文件主要起草人：

能源工业互联网平台数据安全技术要求

* 1. 范围

本文件规定了能源工业互联网平台数据安全框架、数据分类分级要求、数据采集技术要求、数据传输技术要求、数据存储技术要求、数据应用技术要求。

本文件适用于能源企业、能源设备制造企业工业互联网平台数据安全保障工作。

* 1. 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 数据安全技术 数据分类分级规则

* 1. 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。

能源工业互联网平台 energy industry internet platform

针对能源行业设计的工业互联网平台，聚焦能源数据的收集与管理，实现数据的感知、认知、可视化与控制，实时安全感知、协同交互、平台运营、数据共享及生态链协作，简称平台。

核心能源数据 core energy data

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、一定深度的重要能源数据，一旦被非法使用或共享，可能直接影响政治安全。如关联1亿人以上公民个人信息的能源消费原始数据。

重要能源数据 key energy data

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数据。如特级电力用户的电力及其他能源消费原始数据；及关联100万人以上公民个人信息的能源消费原始数据。

一般能源数据 general energy data

核心能源数据、重要能源数据之外的其他数据。

* 1. 缩略语

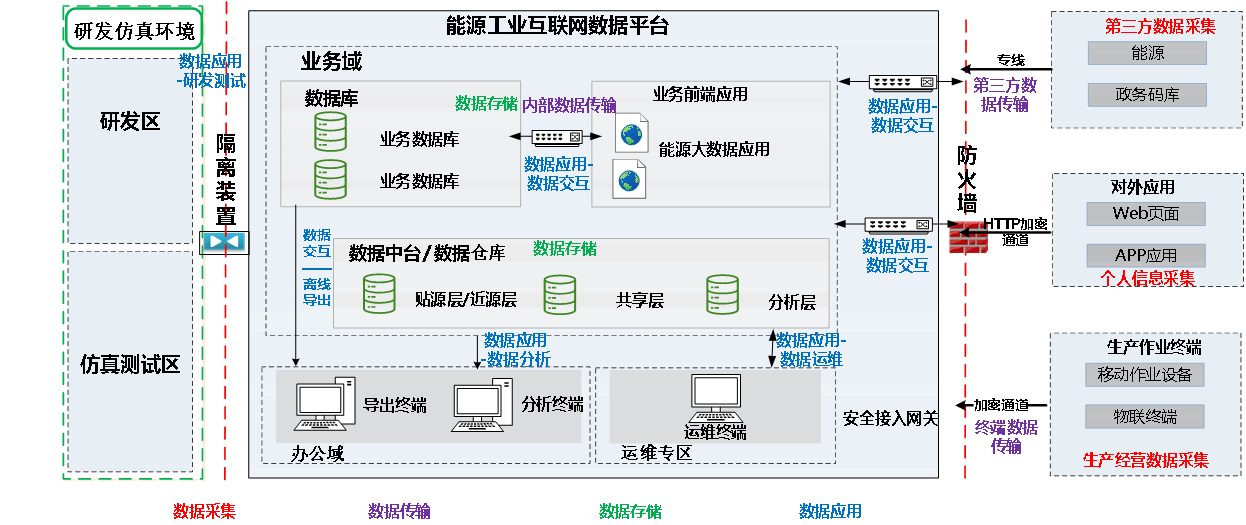
下列缩略语适用于本文件。

HTTPS：超文本传输安全协议(Hypertext Transfer Protocol Secure)

APP:应用程序(Application)

* 1. 能源工业互联网平台平台数据安全框架

平台数据安全围绕能源数据分类分级与数据采集、传输、存储、应用全环节，数据安全框架见图1。其中数据采集包括生产经营数据采集、个人信息采集、第三方数据获取。数据传输包括内部数据传输、终端数据传输、第三方数据传输等。数据应用包括数据交互、数据分析、数据运维、数据测试等。



1. 平台数据安全架构
   1. 数据分类分级要求
      1. 数据分类

6.1.1 平台数据分类应满足GB/T 43697中的要求。

6.1.2 平台数据分类应参考数据资源产生来源方、权利所有方等要素，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。

6.1.3 宜参考A.1按照三个层级进行分类，其中个人信息和公共数据可按照自身特征调整所涉及的分类层级。

6.1.4 分类层级宜参考A.2，按照业务特征分类，划分为专业领域、业务主题和业务对象，并依据数据规模划分为数据集和数据项。

* + 1. 数据分级

6.2.1 平台数据分级应符合GB/T 43697中的数据分级要求。

6.2.2 平台数据应总体分为核心数据、重要数据、一般数据三大级，并从高到低分为6级，其中核心数据为6级，重要数据为5级，一般数据根据影响程度分为1~4级。

6.2.3 应结合业务实际，采用自顶向下和自底而上相结合的方法进行数据分级。

6.2.4 数据分级应包括对数据集进行分级、对数据项进行分级，其中数据项分级最高级别为4级数据，数据集级别在数据项级别的基础上，综合考虑该数据集的数据规模、影响对象、影响程度，可上升为重要数据（5级）或核心数据（6级）。

6.2.5 数据分级判定宜参考A.3,数据分级中影响程度要素判断宜参考A.4。

* 1. 数据采集技术要求
     1. 生产经营数据采集

7.1.1 物联终端采集生产经营数据时,应遵循GB/T 3704 、GB/T 37093中物联终端安全防护要求，加强终端准入管控和安全监测；

7.1.2 通过无线网络采集物联终端的生产经营数据时应采取加密、认证及访问控制等安全措施。

* + 1. 个人信息采集

平台采集个人信息应遵循GB/T 35273相关要求，并满足如下安全要求：

1. 通过APP等应用采集用户个人信息时，应通过弹窗等明显方式向用户明示采集方主体名称和联系方式、个人信息处理目的、处理方式、处理的个人信息种类、保存期限、个人行使权利的方式和程序以及法律、行政法规规定应当告知的其他事项，并征得用户同意；
2. 采集用户个人信息时，应限于实现处理个人信息目的的最小范围，不应过度收集个人信息，不应以欺诈、诱骗、误导的方式收集个人信息，不应隐瞒产品或服务所收集个人信息的用途。
   * 1. 第三方数据获取

平台获取第三方数据的安全要求如下：

1. 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；
2. 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；
3. 从第三方获取个人信息时，应确认个人信息提供方已向个人告知接收方的名称和联系方式、处理目的、处理方式和个人信息种类，并取得本人的同意。
   1. 数据传输技术要求
      1. 内部数据传输

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。

* + 1. 终端数据传输

从终端采集的生产经营数据、个人信息数据传输安全要求如下：

1. 物联终端采集的生产经营数据，应对核心数据、重要数据进行加密；
2. 互联网移动APP采集的个人信息等敏感数据传输时，应采取接入认证、数据加密传输等措施，加强数据保护；
3. 业务系统采集的互联网个人信息，应优先采用HTTPS协议传输。
   * 1. 第三方数据传输

第三方获取的数据传输安全要求如下：

1. 与政府、银行等第三方单位进行能源数据传输时，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。
   1. 数据存储技术要求
      1. 一般数据存储要求

一般数据存储安全要求如下：

1. 可存储于专用网络，可采取通用安全保护措施进行适度防护；
2. 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；
3. 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。
   * 1. 重要数据存储要求

重要数据存储安全要求如下：

1. 原则上应存储于专用网络；
2. 应具有针对能源数据的完整性检测、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；
3. 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；
4. 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。
   * 1. 核心数据存储要求

核心数据存储安全要求如下：

1. 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；
2. 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；
3. 应建立异地灾难备份机制，建立数据容灾备份及恢复机制，保障业务的连续运行。
   1. 数据应用技术要求
      1. 数据交互安全技术要求
         1. 用户访问页面交互安全要求

用户访问页面交互的安全要求如下：

1. 应结合数据级别、用户角色设置数据访问权限，按需对数据进行脱敏处理；
2. 涉及重要数据、核心数据时，对浏览页面添加页面水印，确保因拍照、截屏造成数据泄露后能够定位溯源。
   * + 1. 线上接口交互安全要求

线上接口交互按数据共享对象分为对内共享、对外共享，安全要求如下：

1. 应严格执行数据共享审批流程，按需对数据进行脱敏、水印处理后再共享；
2. 应具备数据防泄露能力，对异常交互行为进行识别和阻断；
3. 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。
   * + 1. 线下导出共享安全要求

线下导出共享安全要求如下：

1. 应严格执行数据共享审批流程，按需对数据进行脱敏、水印处理后再共享；
2. 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。
   * + 1. 数据协同应用安全要求

宜采取隐私计算等技术对数据协同应用进行防护，实现各参与方数据可用不可见。

* + 1. 数据分析安全技术要求
       1. 数据中台分析场景

采用数据中台进行数据分析时安全要求如下：

1. 应对数据中台违规流转、数据高危操作、数据异常访问等行为进行安全风险监测；
2. 应加强数据中台数据使用权限以及账号权限的管控，规范数据分析权限申请、审批和授权流程；
3. 在数据分析终端上，应具备终端敏感数据发现、截屏管控、外发管控等数据安全防护措施；
4. 数据分析结果应进行安全评估，涉及重要数据、核心数据时应按需进行数据脱敏等处理。
   * + 1. 其他数据分析场景

未采用数据中台进行数据分析，在满足 10.2.1 中 c)、d)的前提下，还应采用敏感数据识别、数据脱敏、水印溯源、终端敏感数据保护、数据库安全审计等数据防护措施，开展防护工作。

* + 1. 数据运维安全技术要求
       1. 数据运维事前授权

10.3.1.1 应执行数据运维申请授权审批流程，按照权限最小化和权限分离原则进行账号授权。

10.3.1.2 应对运维人员批量修改数据、导出数据、删除数据、查看核心数据及重要数据等需求严格审核。

* + - 1. 数据运维事中操作

数据运维事中操作安全要求如下：

1. 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；
2. 应对运维过程中涉及的核心数据、重要数据进行脱敏处理；
3. 应采用终端敏感数据发现、截屏管控、外发管控等措施，加强运维终端的数据保护。
   * + 1. 数据运维事后审计

10.3.3.1 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。

10.3.3.2 应定期清理未实名账号、建设期临时账号，回收高风险权限。

* + 1. 数据测试安全技术要求

研发仿真环境对数据进行测试安全要求如下：

1. 研发环境禁止使用真实生产数据和脱敏数据,仅允许使用样例仿真数据；
2. 测试环境禁止直接使用真实生产数据，确需使用的，按照最小化原则申请数据接入，并进行脱敏处理；
3. 应加强测试人员账号权限管控和违规操作监测，对测试人员私自下载、拷贝数据等风险行为进行监测；
4. 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，防范研发人员违规操作造成数据泄露；
5. 应采用数据脱敏、水印溯源、敏感数据识别等措施，对测试环境不同区域进行差异化防护；
6. 应采用终端敏感数据发现、截屏管控、外发管控等措施，加强测试终端的数据保护。
   * 1. 数据销毁技术要求
        1. 数据擦除

10.5.1.1 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。

10.5.1.2 涉及核心数据、重要数据的应重点进行销毁结果验证。

* + - 1. 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。

* + - 1. 个人信息销毁

10.5.3.1 个人信息销毁应符合GB/T 35273相关要求。

10.5.3.2 信息系统、网站、APP等通过注册账号提供服务的，应设置便捷明显的注销功能界面，在用户注销账号后应及时对个人信息进行删除或匿名化处理。

10.5.3.3 因监管要求或个人信息主体权利要求对采集的个人信息进行删除、注销时，应及时响应，需要人工处理的，应在承诺时限内完成核查和处理。

2. （资料性）  
   能源工业互联网平台数据分级分类规则与示范

能源工业互联网平台数据分级分类规则与示范，如表A.1、表A.2、表A.3、表A.4所示。

* 1. 平台数据分类判定规则

| 数据分类 | 判断标准 |
| --- | --- |
| 平台数据 | 是指平台在业务运行、客户服务等活动中收集、产生的原始数据和衍生数据。平台数据涵盖平台中包含的全量数据，按照业务条线进行分类和定级，包括个人信息和公共数据。平台数据与个人信息、公共数据中相同数据项的定级应保持一致。 |
| 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。 |
| 公共数据 | 是指按照国家法律法规要求披露，或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。公共数据需按照国家和地方有关要求汇集或共享开放。 |

* 1. 平台数据分类参考示范

| 一层子类 | 三层子类 | 四层子类 | 五层子类 | 建议级别 |
| --- | --- | --- | --- | --- |
| 能源发展数据 | 发展战略 | 发展规划 | 电网、产业、金融、国际化等业务中长期发展规划等； | 4级数据 |
| 发展实施 | 发展实施意见、批复意见、发布单位（部门）等； | 4级数据 |
| 发展计划 | 发展计划 | 公司发展计划、批复意见、发布单位（部门）等； | 4级数据 |
| 发展方案 | 党建、建设、调控运行、检修、营销、人力资源、财务、物资、科技、信息化、后勤、法治、企业文化等专业发展方案； | 4级数据 |
| 电力设备数据 | 变电运维 | 变电运维信息 | 变压器、变压器绕组、并联电抗器、并联电容器、串联电抗器、串联电容器、调相机、断路器、发电机组、隔离开关交流滤波器、接地刀闸、母线等等运维； | 3级数据 |
| 变电检修 | 变电检修信息 | 变电检修工单、变电检修设备名称、检修单位、设备厂商、检修内容、检修问题及检修结果等； | 3级数据 |
| 变电检测 | 变电检测信息 | 变电检测工单、资产ID、所属变压器、所属厂站、所属换流站、许可机构、中性点接地方式等； | 3级数据 |
| 变电验收 | 变电验收信息 | 变电验收电压等级、电源类型、调度机构、额定功率、额定功率因数、发电机型号、分接头额定档位、生效时间、失效时间等； | 3级数据 |
| 变电评价 | 变电评价信息 | 变电评价设备名称、设备状态、设备缺陷、设备使用寿命等； | 2级数据 |
| 变电可靠性管理 | 变电可靠性信息 | 全额运行状态、降额运行状态、输送电量、可用小时、运行小时、不可用小时、计划停用小时及非计划停用小时等； | 3级数据 |
| 电力用户数据 | 客户管理 | 用电户  档案管理 | 客户名称、客户编号、客户类型、重要性等级、台区名称、线路名称、负荷特性，立户日期、费控标识、电价类别、行业类别、电压等级、账户状态、用电地址、额定容量、运行容量，证件号码、增值税号、联系号码等； | 3级数据 |
| 发电户  档案管理 | 发电户编号、发电户名称、客户编号、客户地址、银行账户、合同账户编号、证件号码、并网电压等级、介入方式、消纳方式、发电户状态、供电单位、合同容量、台区名称、并网日期、立户日期、电能资产编号等 | 3级数据 |
| 资产管理 | 用电客户  资产管理 | 资产编号、管理单位、设备码、设备明策划才能够、组箱码、合同编号、设备状态、逻辑地址码、生产厂家、建档日期、型号、出厂日期等； | 3级数据 |
| 计费结算管理 | 量费核算管理 | 用户编号、用户名称、用电地址、合同容量、电费年月、本月电量、同期电量、本月电量同比增减、本月电量同比增长率、累计电量、同期累计电量，累计电量同比增减，累计电量同比增长率，本月平均电价、同期平均电价、累计平均电价等 | 3级数据 |
| 支付结算管理 | 供电单位、用户编号、用户名称、用电地址、行业分类、用电类别、发型日期、总电量（千瓦时）、总电费（元）、欠费金额（元），本年累计电量、电费年月 | 3级数据 |

* 1. 平台数据分级

| 平台数据级别划分 | | 影响对象 | | | | 数据范围 |
| --- | --- | --- | --- | --- | --- | --- |
| 国家安全 | 公共利益 | 个人合法权益 | 组织合法权益 |
| 核心数据（6级） | | 严重危害  一般危害 | 严重危害 | - | - | 数据集 |
| 重要数据（5级） | | 轻微危害 | 一般危害  轻微危害 | - | - | 数据集 |
| 一般数据 | 4级数据 | 无危害 | 无危害 | 严重危害 | 严重危害 | 数据项、数据集 |
| 3级数据 | 无危害 | 无危害 | 一般危害 | 一般危害 | 数据项、数据集 |
| 2级数据 | 无危害 | 无危害 | 轻微危害 | 轻微危害 | 数据项、数据集 |
| 1级数据 | 无危害 | 无危害 | 无危害 | 无危害 | 数据项、数据集 |

* 1. 平台数据分级影响程度说明

| 影响程度 | 参考说明 |
| --- | --- |
| 严重危害 | 1.可能导致危及国家安全的重大事件，发生危害国家利益或造成重大损失的情况。  2.可能导致严重危害社会秩序和公共利益，引发公众广泛诉讼等事件，或者导致购售电市场秩序遭到严重破坏等情况。  3.可能遭到监管部门严重处罚，或者影响重要/关键业务无法正常开展的情况。  4.可能导致重大个人信息安全风险、侵犯个人隐私等严重危害个人权益的事件。 |
| 一般危害 | 1.可能导致危害社会秩序和公共利益的事件，引发区域性集体诉讼事件，或者导致购售电市场秩序遭到破坏等情况。  2.可能遭到监管部门处罚，或者影响部分业务无法正常开展的情况。  3.可能导致一定规模的个人信息泄漏、滥用等安全风险，或对个人权益可能造成一定影响的事件。 |
| 轻微危害 | 1.可能导致个别诉讼事件，使企业经济利益、声誉等轻微受损。  2.可能导致部分业务临时性中断等情况。  3.可能导致超出个人客户授权加工、处理、使用数据等情况，对个人权益造成部分或潜在影响。 |
| 无危害 | 对国家安全、公共利益、个人合法权益、组织合法权益不造成影响。 |

1. （资料性）  
   典型场景数据安全防护
   1. 数据交互场景

数据交互是指数据在企业内外部进行数据共享和访问等行为，包括用户访问页面、线上接口交互、线下导出共享、数据协同应用等方式。应采用敏感数据识别、数据脱敏、水印溯源、数据库安全审计、终端敏感数据保护、数据防泄露、隐私计算等数据安全防护能力，加强对数据交互场景的防护，见图B.1。



* 1. 数据交互场景安全防护示意图
  2. 数据分析场景

数据分析是指数据分析人员基于数据仓库、中台或其他环境开展数据分析、数据产品设计等行为。开展数据分析时，应采用敏感数据识别、数据脱敏、水印溯源、终端敏感数据保护等数据安全防护能力，防范人员违规查看、导出明细数据等导致数据泄露。在其他环境开展数据分析业务时，应参照数据安全防护措施，采用敏感数据识别、数据脱敏、水印溯源、终端敏感数据保护、数据库安全审计等数据安全防护能力，开展防护工作，见图B.2。



* 1. 数据分析场景安全防护示意图
  2. 数据运维场景

数据运维是指对信息系统中涉及的数据进行运营和维护等行为。应严格按照企业信息系统运维相关要求开展数据相关运维工作。开展数据运维工作时，应采用数据库安全审计、运维安全审计、终端敏感数据保护等数据安全防护能力，加强数据运维过程管控和审计，防止运维人员越权查看、批量导出、恶意修改数据，见图B.3。



* 1. 数据运维场景安全防护示意图
  2. 研发测试场景

研发测试是指研发人员在研发测试环境中开展数字化系统或应用等研发测试行为。应遵循企业数字化项目研发安全防护要求开展研发测试工作。开展研发测试工作时，应采用数据脱敏、水印溯源、敏感数据识别、终端敏感数据保护等数据安全防护能力，加强研发测试环境数据安全防护，见图B.4。



* 1. 数据研发测试场景安全防护示意图