ICS 35.020
CCS L 70

# DB61

# 陕　西　省　地　方　标　准

DB 61/T 2036—2025

# 大数据平台安全保障规范

Big Data Platform Security Guarantee Specification

2025－04－18 发布　　2025－05－17 实施

陕西省市场监督管理局　　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。

本文件由陕西省工业和信息化厅提出并归口。

本文件起草单位：陕西省网络与信息安全测评中心、陕西正观政务信息技术研究院有限公司、陕西中认信安技术服务有限公司。

本文件主要起草人：杨向东、李严、马卓元、靳倩、赵首花、闫育芸、杨睿超、姚雨秋、张赏雪、亓泽瑜、孙蕊刚、冯燕飞、胡吉祥、牛创军、王玉婷。

本文件首次发布。

本文件由陕西省网络与信息安全测评中心负责解释。

联系信息如下：

单位：陕西省网络与信息安全测评中心

电话：029-88319550

地址：陕西省西安市高新区茶张路1号省信息化中心19层

邮编：710065

# 大数据平台安全保障规范

## 1 范围

本文件描述了大数据平台安全保障框架，规定了大数据平台安全管理、安全技术、安全运行和有效性评价的要求。

本文件适用于大数据平台安全保障。

## 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 35274 信息安全技术 大数据服务安全能力要求

GB/T 35295 信息技术 大数据 术语

## 3 术语和定义

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

3.1

**大数据平台 Big Data Platform**

采用分布式存储和计算技术，提供大数据处理功能，支持大数据应用安全高效运行的软硬件集合，包括监视数据输入/输出、控制数据处理活动等软硬件基础设施及其所控制的数据资产。

注：平台指由一组子系统和技术形成的软硬件设施组成，通过一些接口和使用工具提供一组一致的功能，任何由它所支持的应用都可以使用平台的功能而不必关心其实现细节。

［来源：GB/T 35274-2023，3.11］

## 4 安全保障框架

安全保障框架由安全管理、安全技术、安全运行组成，如图1所示：

——安全管理包括机构、人员、安全策略、资产管理、风险管理、业务连续性管理。

——安全技术包括通用要求、数据处理要求。

——安全运行包括安全监测、风险识别、应急处置。

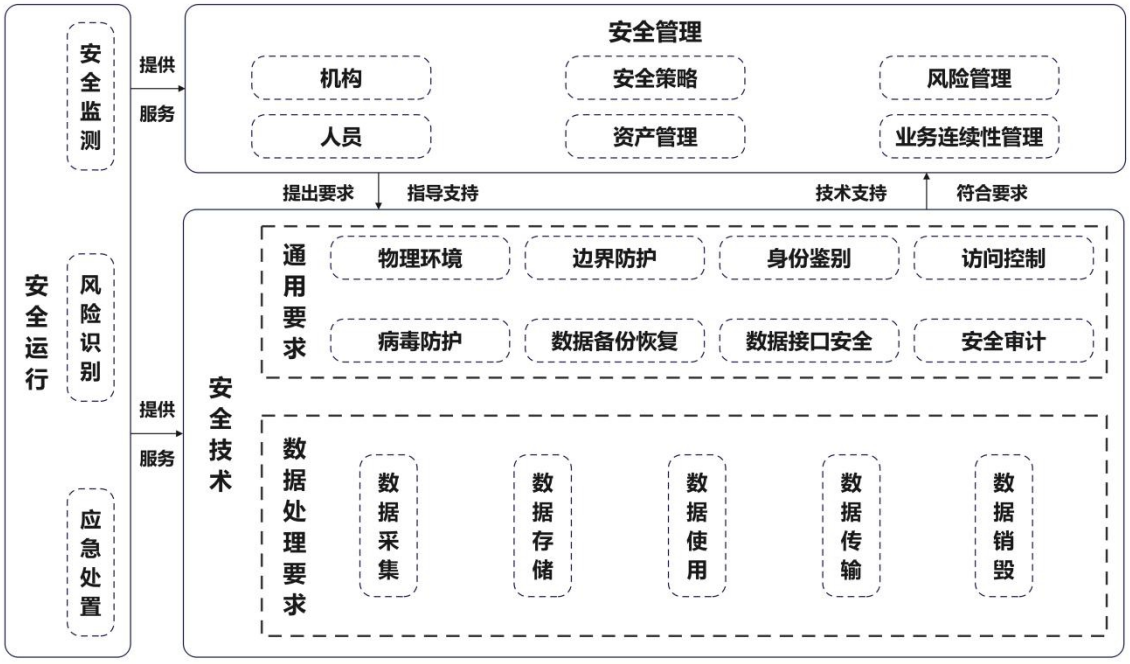


图 1　大数据平台安全保障框架

## 5　安全管理

### 5.1　机构

5.1.1　应建立大数据平台安全保障领导机构，明确决策层、管理层、执行层的职责划分。

5.1.2　应明确大数据平台安全责任与任务分配，由管理层制定，决策层批准，发布、传达至内部、外部相关方。

5.1.3　应明确大数据平台安全责任人，并将责任人的信息报备至行业主管部门，落实安全管理责任。

### 5.2　人员

5.2.1　平台管理岗位人员应熟悉相关法律法规、政策文件及平台基本架构和运行方式，通过专业培训或考核，签署安全责任协议和保密协议。

5.2.2　人员离职后应及时撤销访问权限，包括但不限于大数据平台管理账户、身份认证信息、设备访问权限。

### 5.3　安全策略

5.3.1　安全策略应由管理层负责制定，内容应覆盖对大数据平台的管理、技术和运行层面的要求。

5.3.2　应建立重要数据监测、自动化监控和应急处置机制，配备数据防泄漏和监测工具。

5.3.3　安全策略的制定应符合法律法规和标准要求。

### 5.4　资产管理

5.4.1 应根据重要程度对资产实施分类管理，并进行标识，编制资产清单，明确其归属、责任、分类和位置。
5.4.2 应对重要介质进行分类标识和管理，对查阅、拷贝、传输等操作进行审批。
5.4.3 应建立设备管理制度，对设备的选型、采购、领用、维护、报废等流程进行审批，并明确责任人。

### 5.5 风险管理

5.5.1 应建立大数据平台的核心资产分类评估制度，识别系统威胁和脆弱性，分析不可接受风险类别，提出风险防控措施。
5.5.2 应建立完整的大数据平台应急预案，包括应急组织、职责分工、安全事件分类、监测预警、处置流程和保障措施。
5.5.3 应结合风险评估结果和平台安全需求，整合控制措施，形成系统化的风险防控体系。
5.5.4 应建立自动化监控和应急处置机制，监测数据处理活动及操作接口，及时发现异常并进行响应。
5.5.5 应针对重要数据和个人信息建立监测机制，部署数据防泄漏工具，监控异常的数据交换和共享行为。
5.5.6 委托第三方开展风险评估，应对委托对象的资质进行审核，并签署委托协议和保密协议。

### 5.6 业务连续性管理

5.6.1 应建立应急响应机制，定期进行服务中断应急演练。
5.6.2 应建立数据备份机制，定期进行恢复性测试。
5.6.3 应设计冗余存储与计算架构。

## 6 安全技术

### 6.1 通用要求

#### 6.1.1 物理环境

6.1.1.1 大数据平台应设置在具有防震、防风和防雨等能力的建筑内，并符合机房场地安全选址要求。
6.1.1.2 出入口应配备具有电子门禁管理与记录功能的设备。
6.1.1.3 应具备关键设备的物理安全保护功能，支持对关键设备进行固定，标明不可移除的标识，并确保设备及机柜安全接地。
6.1.1.4 应具备电力冗余与过压保护功能，支持提供冗余电力线路、备用电力和过压保护装置。
6.1.1.5 应具备火灾报警与温湿度调节功能，支持配备火灾自动报警和灭火系统，并安装温湿度调节设施。
6.1.1.6 应具备环境安全防护功能，支持采取防水、防潮及防静电措施，包括防静电地板、湿度控制以及水敏感报警设备等。
6.1.1.7 大数据平台机房应具有异地灾备功能，灾备中心与主数据中心不小于300公里。

#### 6.1.2 边界防护

6.1.2.1 应具备网络攻击检测与防护功能，支持在大数据平台与外网边界部署网络攻击检测与防护设备。

6.1.2.2 应具备边界访问与数据流控制功能，支持跨越边界的访问和数据流必须通过受控接口进行通信。
6.1.2.3 应具备非授权设备连接检测与限制功能，支持对非授权设备连接内部网络的行为进行实时检测并限制。

#### 6.1.3 身份鉴别

6.1.3.1 应具备用户身份标识与鉴别功能，支持对登录用户进行唯一性身份标识和鉴别，确保鉴别信息复杂度并定期更换。
6.1.3.2 应具备登录失败处理功能，支持配置并启用结束会话、限制非法登录次数和登录连接超时自动退出等措施。
6.1.3.3 应具备远程管理安全防护功能，支持采取措施防止鉴别信息在网络传输过程中被窃听。
6.1.3.4 应具备多因素身份鉴别功能，支持采用口令、密码技术、生物技术等两种及以上组合的鉴别技术，且其中一种鉴别技术应使用密码技术实现。

#### 6.1.4 访问控制

6.1.4.1 应具备访问控制策略配置功能，支持由授权主体规定主体对客体的访问规则。
6.1.4.2 应具备用户标识与权限管理功能，支持对不同用户实施标识和鉴别，分配账户和权限，确保最小权限和权限分离。
6.1.4.3 应具备访问控制规则优化功能，支持删除无效或冗余的规则，优化访问控制列表。
6.1.4.4 应具备账户安全管理功能，支持重命名或删除默认账户，修改默认密码，删除或停用无效账户。

#### 6.1.5 病毒防护

6.1.5.1 应具备攻击检测与防护功能，支持在大数据平台的关键网络节点实施网络攻击检测与防护措施。
6.1.5.2 应具备安全防护及漏洞管理功能，支持在服务器、终端部署病毒防护软件，及时检测并修补已知漏洞。

#### 6.1.6 数据备份恢复

6.1.6.1 应具备数据备份与恢复功能，支持手动和自动执行。
6.1.6.2 应具备数据本地和异地实时备份功能，保证重要数据的机密性、完整性和可用性。

#### 6.1.7 数据接口安全

6.1.7.1 应具备数据接口访问控制功能，支持对数据处理、使用、分析、导出、共享、交换等操作进行控制。
6.1.7.2 应具备数据安全接口安全保障功能，支持对不可控网络中数据接口采用安全通道、加密传输等安全措施。
6.1.7.3 应具备数据接口访问审计功能，支持对数据接口访问进行审计。

#### 6.1.8 安全审计

6.1.8.1 应具备安全审计与事件记录功能，支持启用安全审计功能，跟踪和记录数据采集、处理、分析等过程和安全事件。
6.1.8.2 应具备审计记录备份功能，支持定期备份审计记录。

6.1.8.3 应具备审计记录保护功能，支持防止未授权的查阅、修改或删除审计记录。

## 6.2 数据处理要求

### 6.2.1 数据采集

6.2.1.1 应具备数据采集策略管理功能，配置采集原则、流程、方法和外部数据源合法性验证机制。
6.2.1.2 应具备采集范围动态管控功能，支持采集频度阈值设置与采集风险评估能力。
6.2.1.3 应具备敏感数据识别与访问控制功能，支持对数据的实时标记与权限管控。
6.2.1.4 应具备自动化采集范围管理功能，支持智能判定自动化采集的适用场景与边界控制。

### 6.2.2 数据存储

6.2.2.1 应具备存储资产标识管理功能，支持数据标注与存储内容可视化呈现。
6.2.2.2 应具备数据存储加密功能，支持国密算法套件与完整性、保密性校验机制。
6.2.2.3 应具备数据存储逻辑隔离功能，支持多租户架构的数据分区存储与访问控制策略管理。
6.2.2.4 应具备存储访问审计功能，支持访问日志记录、异常行为检测与审计报告生成。
6.2.2.5 应具备存储合规检查功能，支持随机抽样检测与存储策略匹配度验证。

### 6.2.3 数据使用

6.2.3.1 应具备数据使用评估与审计功能，支持对敏感数据操作的实时风险评估与预警。
6.2.3.2 应具备动态访问控制功能，支持基于数据分类分级的权限动态调整与越权操作阻断。
6.2.3.3 应具备完整的数据操作审计功能，支持操作日志采集、行为画像生成与责任定位。

### 6.2.4 数据传输

6.2.4.1 应具备传输策略动态管理功能，支持安全策略配置与变更。
6.2.4.2 应具备端到端加密传输功能，支持国密算法套件与完整性校验机制。
6.2.4.3 应具备传输安全审计功能，支持通道安全检测、密钥生命周期管理与密码配置合规审查。

### 6.2.5 数据销毁

6.2.5.1 应具备数据销毁策略配置功能，支持基于数据分类分级的自动化销毁方案。
6.2.5.2 应具备销毁流程管控功能，支持多级审批与销毁过程审计。
6.2.5.3 应具备销毁不可逆验证功能，支持敏感数据清除证明与检测。
6.2.5.4 应具备多数据副本销毁功能，支持全副本追踪与批量清除。

# 7 安全运行

## 7.1 安全监测

7.1.1 应依据数据安全基线或阈值制定监测规则，实时告警数据处理活动中的异常行为，并展示相关风险和威胁信息。
7.1.2 应对数据处理过程和存储数据的使用与访问进行审计，审计记录留存应大于6个月。
7.1.3 监测异常的数据交换、数据共享、数据处理和对接口的操作，并即时响应。

## 7.2 风险识别

7.2.1　应构建数据资产识别能力，分类和标记数据源信息，更新数据资产目录。
7.2.2　应对大数据平台进行威胁与脆弱性分析，评估服务的安全影响，形成风险分析报告，并进行整改。
7.2.3　应建立数据处理活动安全风险库，分析大数据平台运营日志，定期开展安全隐患排查。
7.2.4　应定期开展大数据平台风险识别、分析，保存分析报告及应对情况记录。

### 7.3　应急处置

7.3.1　应按照应急演练计划，定期开展演练，保存记录和总结报告。在大数据平台或外部环境发生重大变化时，应及时更新应急预案并保留审核发布记录。
7.3.2　应与主管部门、第三方安全机构和相关职能部门建立有效的应急处理、协调和沟通渠道。
7.3.3　根据安全事件处置操作规程，发生数据泄露、篡改、破坏、勒索等安全事件时，应按照规程明确的事件分类、启动条件、资源需求及响应措施进行处置。
7.3.4　应明确大数据平台故障恢复目标，包括关键服务和全部服务的恢复时间。应急处置完成后，应及时调查原因，评估影响，整理处置报告，总结经验并提出改进措施。

## 8　有效性评价

8.1　有效性评价应基于安全管理、安全技术及安全运行三个维度开展系统性评估，由平台责任主体、第三方合规审查机构及行业监管部门共同作为评价主体，通过定期自查、技术检测、文档审核、现场检查及应急演练等方法，综合验证安全保障措施的符合性与运行效能。
8.2　评价内容应涵盖安全策略执行、技术防护能力、风险监测与应急处置等关键环节，重点分析安全管理制度的完备性、技术措施的可靠性以及运行机制的持续优化能力，确保评价过程覆盖全生命周期管理。
8.3　评价结果应形成书面报告并提交至相关责任方，作为改进保障规范、优化资源配置及提升应急响应能力的重要依据，同时应将整改措施纳入后续监督计划，推动安全保障规范动态完善与合规性提升。

# 参 考 文 献

[1]《中华人民共和国网络安全法》中华人民共和国主席令第五十三号

[2]《中华人民共和国数据安全法》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

[3] GB/T 20269—2006 信息安全技术 信息系统安全管理要求

[4] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系要求

[5] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

[6] GB/T 35274—2023 数据安全技术 大数据服务安全能力要求

[7] GB/T 35589—2017 信息技术 大数据 技术参考模型

[8] GB/T 37973—2019 信息安全技术 大数据安全管理指南

[9] GB/T 37988—2019 数据安全能力 成熟度模型信息安全技术

[10]GB/T 35274—2023 数据安全技术 大数据服务安全能力要求