



# 中华人民共和国公共安全行业标准

GA/T 1390.7—2025

## 信息安全技术 网络安全等级保护 基本要求 第7部分：大数据系统安全 扩展要求

Information security technology—Baseline for classified protection of  
cybersecurity—Part 7: Extended requirements for big data system security

2025-10-13 发布

2026-02-01 实施

中华人民共和国公安部 发布

目 次

前言 ..... III

引言 ..... IV

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 大数据系统保护对象 ..... 2

5 第一级安全扩展要求 ..... 3

6 第二级安全扩展要求 ..... 3

    6.1 安全物理环境 ..... 3

    6.2 安全通信网络 ..... 3

    6.3 安全计算环境 ..... 3

    6.4 安全管理中心 ..... 4

    6.5 安全管理制度 ..... 4

    6.6 安全管理机构 ..... 4

    6.7 安全建设管理 ..... 5

    6.8 安全运维管理 ..... 5

7 第三级安全扩展要求 ..... 5

    7.1 安全物理环境 ..... 5

    7.2 安全通信网络 ..... 5

    7.3 安全计算环境 ..... 5

    7.4 安全管理中心 ..... 7

    7.5 安全管理制度 ..... 8

    7.6 安全管理机构 ..... 8

    7.7 安全建设管理 ..... 8

    7.8 安全运维管理 ..... 8

8 第四级安全扩展要求 ..... 9

    8.1 安全物理环境 ..... 9

    8.2 安全通信网络 ..... 9

    8.3 安全计算环境 ..... 9

    8.4 安全管理中心 ..... 11

    8.5 安全管理制度 ..... 12

    8.6 安全管理机构 ..... 12

8.7 安全管理 .....12

8.8 安全运维管理 .....12

9 第五级安全扩展要求 .....13

附录 A(资料性) 大数据系统保护对象与安全要求对应 .....14

参考文献 .....17

## 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。

本文件是 GA/T 1390《信息安全技术 网络安全等级保护基本要求》的第 7 部分。GA/T 1390 已经发布了以下部分：

- 第 2 部分：云计算安全扩展要求；
- 第 3 部分：移动互联安全扩展要求；
- 第 5 部分：工业控制系统安全扩展要求；
- 第 6 部分：边缘计算安全扩展要求；
- 第 7 部分：大数据系统安全扩展要求；
- 第 8 部分：IPv6 网络安全扩展要求；
- 第 9 部分：区块链安全扩展要求。

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。

本文件由公安部网络安全保卫局提出。

本文件由公安部信息系统安全标准化技术委员会归口。

本文件起草单位：公安部第三研究所、公安部网络安全保卫局、公安部第一研究所、深圳市腾讯计算机系统有限公司、国家信息中心、华为云计算技术有限公司、北京天融信网络安全技术有限公司。

本文件主要起草人：袁静、苏艳芳、江雷、任娟娟、康磊、刘卜瑜、李克鹏、章恒、耿涛、王龔、陈文生、王永霞、陈永刚、何应钦、梁亚楠。

# 引 言

GA/T 1390《信息安全技术 网络安全等级保护基本要求》旨在提出不同网络安全保护等级的基线安全要求,指导等级保护对象的安全建设和监督管理。GA/T 1390 拟由以下部分组成。

- 第 1 部分:安全通用要求。旨在提出适用于所有网络安全等级保护对象的安全基线要求。
- 第 2 部分:云计算安全扩展要求。旨在提出适用于云计算平台/系统的安全扩展要求。
- 第 3 部分:移动互联安全扩展要求。旨在提出适用于采用移动互联技术的等级保护对象的安全扩展要求。
- 第 4 部分:物联网安全扩展要求。旨在提出适用于物联网的安全扩展要求。
- 第 5 部分:工业控制系统安全扩展要求。旨在提出适用于工业控制系统的安全扩展要求。
- 第 6 部分:边缘计算安全扩展要求。旨在提出适用于采用边缘计算技术的等级保护对象的安全扩展要求。
- 第 7 部分:大数据系统安全扩展要求。旨在提出适用于采用大数据技术的等级保护对象的安全扩展要求。
- 第 8 部分:IPv6 网络安全扩展要求。旨在提出适用于 IPv6 等级保护对象的安全扩展要求。
- 第 9 部分:区块链安全扩展要求。旨在提出适用于区块链等级保护对象的安全扩展要求。
- 第 10 部分:生成式人工智能安全扩展要求。旨在提出适用于生成式人工智能等级保护对象的安全扩展要求。
- 第 11 部分:低空智联网安全扩展要求。旨在提出适用于低空智联网等级保护对象的安全扩展要求。
- 第 12 部分:智能车联网安全扩展要求。旨在提出适用于智能车联网等级保护对象的安全扩展要求。

信息安全技术 网络安全等级保护  
基本要求 第7部分：大数据系统安全  
扩展要求

1 范围

本文件规定了大数据系统等级保护对象的网络安全等级保护第一级到第四级的安全扩展要求。  
本文件适用于大数据系统等级保护对象的安全建设和监督管理。  
注：第五级大数据系统等级保护对象不在本文件中进行描述。

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—2019 信息安全技术 网络安全等级保护基本要求

3 术语和定义

GB/T 22239—2019 界定的以及下列术语和定义适用于本文件。

3.1

**大数据 big data**

具有体量巨大、来源多样、生成极快且多变等特征并且难以用传统数据体系结构有效处理的包含大量数据集的数据。

[来源：GB/T 35295—2017, 2.1.1, 有修改]

3.2

**数据生存周期 data lifecycle**

将原始数据转化为可用于行动的知识的一组过程。

注：数据生存周期一般包括收集、数据传输、数据存储、数据使用、数据加工（如计算、分析、可视化等）、数据提供、数据公开等，直至数据销毁。

[来源：GB/T 35295—2017, 2.1.2, 有修改]

3.3

**大数据系统 big data system**

实现大数据参考体系结构的全部或部分功能的系统。

[来源：GB/T 35295—2017, 2.1.14]

3.4

**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]

3.5

**数据资源 data resource**

存储大数据的软硬件集合。

3.6

**大数据处理节点 big data processing node**

在大数据处理架构中负责接收、存储、处理和分析数据的计算单元或服务器。

注：这些节点通常组成一个集群,通过分布式计算和存储技术协同工作,以处理海量数据。

3.7

**客户 customer**

为使用大数据系统服务与大数据系统服务商建立业务关系的参与方。

3.8

**去标识化 de-identification**

通过对个人信息的技术处理,使其在不借助额外信息的情况下,无法识别或者关联个人信息主体的过程。

注：去标识化建立在个体基础之上,保留了个体颗粒度,采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

[来源:GB/T 35273—2020,3.15]

4 大数据系统保护对象

大数据系统等级保护对象由数据资源、大数据平台、大数据应用构成,如图 1 所示。

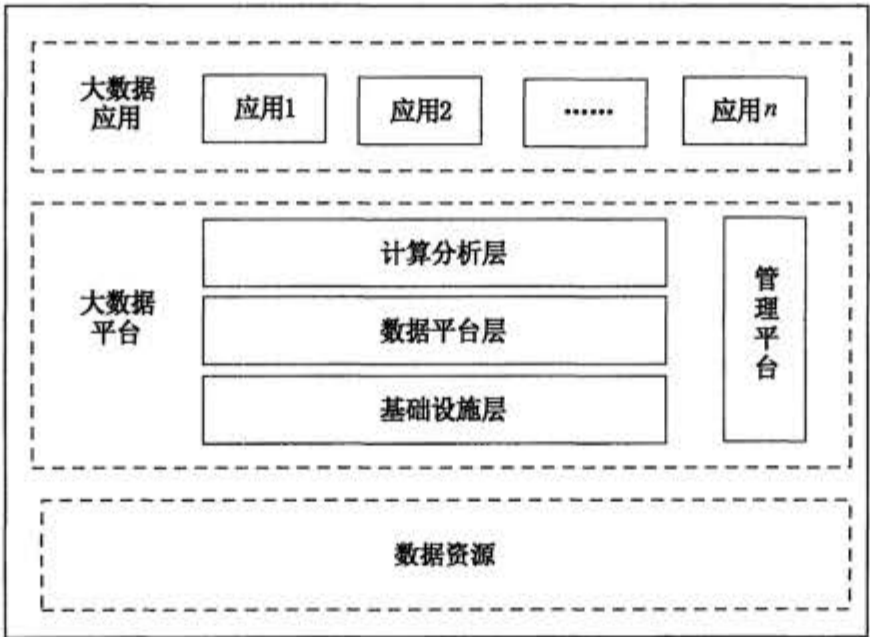


图 1 大数据系统等级保护对象的构成

- a) 数据资源一般存储在大数据平台,由大数据应用调用。
- b) 大数据应用是指基于大数据平台,采用大数据分析和挖掘技术对数据执行处理过程的业务应用系统。
- c) 大数据平台为大数据应用和数据资源提供资源和服务的支撑集成环境,包括基础设施层、数据平台层和计算分析层以及管理平台等部分或者全部的功能。基础设施层提供物理或虚拟的计

算、网络和存储能力；数据平台层提供结构化和非结构化数据的逻辑存储能力；计算分析层提供大量、高速、多样和多变数据的分析计算能力；管理平台提供大数据平台的辅助服务能力。大数据平台可以为多个大数据应用及数据资源提供服务。

数据资源、大数据应用、大数据平台可能由不同运营者承担安全责任，从定级对象的责任主体角度出发，三者可独立或组合作为定级对象，例如大数据平台、大数据应用、数据资源、数据资源与大数据应用、数据资源与大数据平台或大数据平台与大数据应用等均可作为定级对象。不同类型大数据系统保护对象与要求项的对应关系见附录 A。

## 5 第一级安全扩展要求

无。

## 6 第二级安全扩展要求

### 6.1 安全物理环境

承载大数据存储、处理和分析的设备机房应位于中国境内。

### 6.2 安全通信网络

大数据平台不应承载高于其安全保护等级的大数据应用和数据资源。

### 6.3 安全计算环境

#### 6.3.1 身份鉴别

身份鉴别应满足以下要求：

- a) 大数据系统提供的外部调用接口对调用主体进行身份鉴别；
- b) 建立分布式计算节点间安全连接策略和互操作规范，采用节点认证等技术机制对大数据处理节点接入身份的真实性进行确认。

#### 6.3.2 访问控制

访问控制应满足以下要求：

- a) 大数据平台或第三方在客户授权下才能对其数据资源进行访问、使用和管理；
- b) 采取技术手段对数据收集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用进行限制；
- c) 识别重要接口，采用最小权限原则分配重要接口的操作权限；
- d) 最小化数据使用、加工、导出、共享、交换的数据集。

#### 6.3.3 安全审计

安全审计应满足以下要求：

- a) 大数据系统对其提供的重要接口的调用情况以及各类重要账号的操作情况进行审计；
- b) 大数据系统服务商对客户数据的操作能被客户审计。

#### 6.3.4 数据完整性

数据在存储过程中的完整性保护应满足数据提供方对数据的安全保护要求。

### 6.3.5 数据保密性

数据保密性应满足以下要求：

- a) 大数据平台提供数据脱敏和个人信息去标识化的工具或服务组件技术；
- b) 依据安全策略对数据进行脱敏和个人信息去标识化处理；
- c) 数据在存储过程中的保密性保护满足数据提供方对数据的安全保护要求。

### 6.3.6 数据备份

备份数据应依据数据安全保护策略,采取与其数据类别和级别相匹配的安全防护措施。

### 6.3.7 剩余信息保护

剩余信息保护应满足以下要求：

- a) 大数据平台提供主动迁移功能,数据整体迁移的过程中杜绝数据残留；
- b) 存有敏感个人信息的存储空间被释放或重新分配前得到完全清除；
- c) 大数据平台能够根据与客户约定的数据销毁要求和方式实施数据销毁。

### 6.3.8 个人信息保护

个人信息保护应满足以下要求：

- a) 收集、存储、使用、加工、提供、公开个人信息获取个人信息主体授权同意,并保留授权审计记录；
- b) 对个人信息的重要操作设置内部审批流程,审批通过后才能对个人信息进行相应的操作,并保留操作审计记录。

## 6.4 安全管理中心

系统管理应满足以下要求：

- a) 大数据平台为客户提供管理其计算和存储资源使用状况的能力；
- b) 大数据平台对其提供的辅助工具或服务组件实施有效管理,包括但不限于安装、部署、监控、优化、升级、卸载、身份鉴别、访问控制等,相关操作日志保存至少6个月；
- c) 大数据平台发生计算、内存、存储资源等故障时,不能影响到业务正常运行；
- d) 大数据平台在系统维护、在线扩容等情况下,不影响大数据应用和数据资源的正常业务处理能力。

## 6.5 安全管理制度

安全管理制度应满足以下要求：

- a) 制定大数据安全工作的总体方针和安全策略,阐明本机构大数据安全工作的目标、范围、原则和安全框架等内容；
- b) 大数据安全策略覆盖数据生存周期相关的数据安全,内容至少包括目的、范围、岗位、责任、管理层承诺、内外部协调及合规性要求等。

## 6.6 安全管理机构

### 6.6.1 授权和审批

数据的收集应获得数据源所有者的授权,并遵循最小化数据收集的原则。

### 6.6.2 审核和检查

应定期审核数据的使用与相关安全管理制度要求的符合情况。

## 6.7 安全建设管理

供应链管理应满足以下要求：

- a) 选择安全合规的大数据平台,其所提供的大数据平台服务为其所承载的大数据应用和数据资源提供相应等级的安全保护能力;
- b) 以书面方式约定大数据平台提供者和大数据平台使用者的权限与责任、各项服务内容和具体技术指标等,尤其是安全服务内容。

## 6.8 安全运维管理

### 6.8.1 资产管理

资产管理应满足以下要求：

- a) 制定并执行数据分类分级保护策略;
- b) 对数据资产进行梳理,建立数据资产清单。

### 6.8.2 网络和系统安全管理

应建立对外数据接口安全管理机制,所有的接口调用均应获得授权和批准。

## 7 第三级安全扩展要求

### 7.1 安全物理环境

承载大数据存储、处理和分析的设备机房应位于中国境内。

### 7.2 安全通信网络

安全通信网络应满足以下要求：

- a) 大数据平台不承载高于其安全保护等级的大数据应用和数据资源;
- b) 大数据平台的管理流量与业务流量分离;
- c) 提供开放接口或开放性安全服务,允许客户接入第三方安全产品或在大数据平台选择第三方安全服务。

### 7.3 安全计算环境

#### 7.3.1 身份鉴别

身份鉴别应满足以下要求：

- a) 大数据系统提供的各类外部调用接口依据调用主体的操作权限实施相应强度的身份鉴别;
- b) 建立分布式计算节点间安全连接策略和互操作规范,采用节点认证等技术机制对大数据处理节点接入身份的真实性进行确认;
- c) 大数据平台提供双向身份鉴别机制,能对不同客户的大数据应用、数据资源进行双向身份鉴别;
- d) 采用两种或两种以上组合的鉴别技术对使用数据收集终端、数据导入服务组件、数据导出终端、数据导出服务组件的用户实施身份鉴别,且其中一种鉴别技术至少使用密码技术来实现;

- e) 采用密码技术对使用数据收集终端、数据导入服务组件、数据导出终端、数据导出服务组件的设备或组件实施身份鉴别；
- f) 对向大数据系统提供数据的外部数据源实施身份鉴别。

### 7.3.2 访问控制

访问控制应满足以下要求：

- a) 大数据平台或第三方在客户授权下才能对其数据资源进行访问、使用和管理；
- b) 采取技术手段对数据收集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用进行限制；
- c) 识别重要接口，采用最小权限原则分配重要接口的操作权限；
- d) 最小化数据使用、加工、导出、共享、交换的数据集；
- e) 大数据系统提供数据分类分级标识功能；
- f) 大数据系统具备设置数据安全标记功能，并基于安全标记进行访问控制；
- g) 在数据收集、传输、存储、使用、加工、提供、公开及销毁等各个环节，根据数据分类分级标识对数据进行不同处置，最高等级数据的相关保护措施不低于 GB/T 22239—2019 的第三级安全要求及本文件的第三级安全扩展要求，安全保护策略在各环节保持一致；
- h) 大数据系统对其提供的重要数据接口、重要服务接口的调用实施访问控制，包括但不限于数据收集、使用、加工、导出、共享、交换等操作；
- i) 大数据系统提供隔离不同客户应用数据资源的能力；
- j) 对数据共享过程进行监控，防止共享的数据超出授权范围。

### 7.3.3 安全审计

安全审计应满足以下要求：

- a) 大数据系统对其提供的各类接口的调用情况、接口权限变更情况以及各类账号的操作情况进行审计；
- b) 大数据系统服务商对客户数据的操作能被客户审计；
- c) 大数据系统将不同客户的审计数据隔离存放，并提供不同客户审计数据收集汇总和集中分析的能力。

### 7.3.4 入侵防范

入侵防范应满足以下要求：

- a) 对所有进入系统的数据进行安全检测；
- b) 对大量数据导出操作以及重要数据的数据流转、泄露和滥用情况进行监控，及时对异常数据操作行为进行告警，并能够对突发的严重异常操作及时定位和阻断；
- c) 能够发现各类接口可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；
- d) 能够对各类接口的状态进行实时监控，并在发生入侵事件时提供告警。

### 7.3.5 数据完整性

数据完整性应满足以下要求：

- a) 数据在存储过程中的完整性保护满足数据提供方对数据的安全保护要求；
- b) 采取技术手段保护源数据的完整性；
- c) 采用校验技术或密码技术保护重要的数据在数据迁移过程中的完整性，包括但不限于重要业务

数据、融合数据、溯源数据等,并在检测到完整性受到破坏时提供恢复措施。

### 7.3.6 数据保密性

数据保密性应满足以下要求:

- a) 大数据平台提供数据脱敏和个人信息去标识化的工具或服务组件技术;
- b) 依据安全策略和数据分类分级标识对数据进行脱敏和个人信息去标识化处理;
- c) 数据在存储过程中的保密性保护满足数据提供方对数据的安全保护要求;
- d) 采取技术措施避免汇聚大量数据时暴露敏感数据,包括但不限于核心数据、重要数据、敏感个人信息、商业秘密信息等;
- e) 对经过脱敏处理的数据进行评估,避免从中能恢复敏感数据。

### 7.3.7 数据备份

数据备份应满足以下要求:

- a) 备份数据依据数据安全保护策略,采取与其数据类别和级别相匹配的安全防护措施;
- b) 大数据平台提供若干个可用的用户数据副本,各副本之间的内容保持一致;
- c) 提供对关键溯源数据的异地备份。

### 7.3.8 剩余信息保护

剩余信息保护应满足以下要求:

- a) 大数据平台提供主动迁移功能,数据整体迁移的过程中杜绝数据残留;
- b) 存有重要的数据和敏感个人信息的存储空间被释放或重新分配前得到完全清除;
- c) 大数据平台能够根据数据分类分级策略以及与客户约定的数据销毁要求和方式实施数据销毁。

### 7.3.9 个人信息保护

个人信息保护应满足以下要求:

- a) 制定覆盖全流程个人信息处理活动的安全管理制度;
- b) 收集、存储、使用、加工、提供、公开个人信息获取个人信息主体授权同意,并保留操作审计记录;
- c) 对个人信息的重要操作设置内部审批流程,审批通过后才能对个人信息进行相应的操作。

### 7.3.10 数据溯源

数据溯源应满足以下要求:

- a) 跟踪和记录数据收集、使用、加工等过程;
- b) 实现数据副本和备份数据管理过程可溯源;
- c) 溯源数据满足数据业务要求和合规审计要求;
- d) 支持从海量数据中自动发现并定位敏感数据的位置、安全等级、数据类型、数据量、归属等;
- e) 采取技术手段保护溯源数据的完整性。

## 7.4 安全管理中心

### 7.4.1 系统管理

系统管理应满足以下要求:

- a) 大数据平台为客户提供管理其计算和存储资源使用状况的能力;
- b) 大数据平台对其提供的辅助工具或服务组件实施有效管理,包括但不限于安装、部署、监控、优

化、升级、卸载、身份鉴别、访问控制等,相关操作日志保存至少6个月;

- c) 大数据平台发生计算、内存、存储资源等故障时,不能影响到业务正常运行;
- d) 大数据平台在系统维护、在线扩容等情况下,不影响大数据应用和数据资源的正常业务处理能力。

#### 7.4.2 集中管控

应对大数据系统提供的各类接口和服务的使用情况进行集中审计和监测,并在发生问题时提供报警。

### 7.5 安全管理制度

安全管理制度应满足以下要求:

- a) 制定大数据安全工作的总体方针和安全策略,阐明本机构大数据安全工作的目标、范围、原则和安全框架等内容;
- b) 大数据安全策略覆盖数据生存周期相关的数据安全,内容至少包括目的、范围、岗位、责任、管理层承诺、内外部协调及合规性要求等。

### 7.6 安全管理机构

#### 7.6.1 授权和审批

授权和审批应满足以下要求:

- a) 数据的收集获得数据源所有者的授权,并遵循最小化数据收集的原则;
- b) 建立数据导入、导出、集成、分析、交换、交易、共享及公开的授权审批控制流程,赋予数据活动主体的最小操作权限、最小数据集和权限有效时长,依据流程实施控制并记录过程,及时回收过期的数据访问权限。

#### 7.6.2 审核和检查

应定期审核数据的使用与相关安全管理制度要求的符合情况。

### 7.7 安全建设管理

供应链管理应满足以下要求:

- a) 选择安全合规的大数据平台,其所提供的大数据平台服务为其所承载的大数据应用和数据资源提供相应等级的安全保护能力;
- b) 以书面方式约定大数据平台提供者和大数据平台使用者的权限与责任、各项服务内容和具体技术指标等,尤其是安全服务内容;
- c) 以书面方式约定数据交换、共享的接收方对数据的保护责任,并明确数据安全保护要求;
- d) 将供应链安全事件信息或安全威胁信息及时传达到数据交换、共享的接收方;
- e) 控制开源、共享软件的使用,并对其代码进行安全审计,针对发现的安全问题进行整改。

### 7.8 安全运维管理

#### 7.8.1 资产管理

资产管理应满足以下要求:

- a) 制定数据资产安全管理策略,对数据资产生存周期的操作规范、保护措施、管理人员职责等进行规定;

- b) 制定并执行数据分类分级保护策略,针对不同类别级别的数据制定相应强度的安全保护要求;
- c) 对数据资产和对外数据接口进行梳理,建立相应的资产清单,并实行统一管理;
- d) 定期评审数据的类别和级别,如需要变更数据所属类别或级别,依据变更审批流程执行变更。

### 7.8.2 介质管理

介质管理应满足以下要求:

- a) 在中国境内对存储敏感数据的介质进行清除或销毁,包括但不限于核心数据、重要数据、敏感个人信息、商业秘密信息等;
- b) 对存储敏感数据的存储介质或物理设备进行销毁时采取难以恢复的技术手段,如物理粉碎、消磁、多次擦写等。

### 7.8.3 网络和系统安全管理

应建立对外数据接口安全管理机制,所有的接口调用均应获得授权和批准。

## 8 第四级安全扩展要求

### 8.1 安全物理环境

承载大数据存储、处理和分析的设备机房应位于中国境内。

### 8.2 安全通信网络

安全通信网应满足以下要求:

- a) 大数据平台不承载高于其安全保护等级的大数据应用和数据资源;
- b) 大数据平台的管理流量与业务流量分离;
- c) 提供开放接口或开放性安全服务,允许客户接入第三方安全产品或在大数据平台选择第三方安全服务。

### 8.3 安全计算环境

#### 8.3.1 身份鉴别

身份鉴别应满足以下要求:

- a) 大数据系统提供的各类外部调用接口依据调用主体的操作权限实施相应强度的身份鉴别;
- b) 建立分布式计算节点间安全连接策略和互操作规范,采用节点认证等技术机制对大数据处理节点接入身份的真实性进行确认;
- c) 大数据平台提供双向身份鉴别机制,能对不同客户的大数据应用、数据资源进行双向身份鉴别;
- d) 采用两种或两种以上组合的鉴别技术对使用数据收集终端、数据导入服务组件、数据导出终端、数据导出服务组件的用户实施身份鉴别,且其中一种鉴别技术至少使用密码技术来实现;
- e) 采用密码技术对使用数据收集终端、数据导入服务组件、数据导出终端、数据导出服务组件的设备或组件实施身份鉴别;
- f) 对向大数据系统提供数据的外部数据源实施身份鉴别。

#### 8.3.2 访问控制

访问控制应满足以下要求:

- a) 大数据平台或第三方在客户授权下才可以对其数据资源进行访问、使用和管理;

- b) 采取技术手段对数据收集终端、数据导入服务组件、数据导出终端、数据导出服务组件的使用进行限制；
- c) 识别重要接口,采用最小权限原则分配接口的操作权限；
- d) 最小化数据使用、加工、导出、共享、交换的数据集；
- e) 大数据系统提供数据分类分级标识功能；
- f) 大数据系统具备设置数据安全标记功能,并基于安全标记进行访问控制；
- g) 在数据收集、传输、存储、使用、加工、提供、公开及销毁等各个环节,支持对数据进行分类分级处置,最高等级数据的相关保护措施不低于GB/T 22239—2019的第四级安全要求及本文件的第四级安全扩展要求,安全保护策略在各环节保持一致；
- h) 大数据系统对其提供的各类接口的调用实施访问控制,包括但不限于数据收集、使用、加工、导出、共享、交换等操作；
- i) 大数据系统提供隔离不同客户应用数据资源的能力；
- j) 对数据共享过程进行监控,防止共享的数据超出授权范围。

### 8.3.3 安全审计

安全审计应满足以下要求：

- a) 大数据系统对其提供的各类接口的调用情况、接口权限变更情况以及各类账号的操作情况进行审计；
- b) 大数据系统服务商对客户数据的操作可被客户审计；
- c) 大数据系统将不同客户的审计数据隔离存放,并提供不同客户审计数据收集汇总和集中分析的能力；
- d) 宜支持按多种维度进行审计规则设置,实现精细化安全审计监控。

### 8.3.4 入侵防范

入侵防范应满足以下要求：

- a) 对所有进入系统的数据进行安全检测；
- b) 对大量数据导出操作以及重要数据的数据流转、泄露和滥用情况进行监控,及时对异常数据操作行为进行告警,并能够对突发的严重异常操作及时定位和阻断；
- c) 能够发现各类接口可能存在的已知漏洞,并在经过充分测试评估后,及时修补漏洞；
- d) 能够对各类接口的状态进行实时监控,并在发生入侵事件时提供告警；
- e) 宜支持通过人工智能等技术,对各类变体攻击以及非常见威胁操作实现监控,以应对变化多端的攻击场景；
- f) 宜支持根据流量特征进行网络攻击行为告警。

### 8.3.5 数据完整性

数据完整性应满足以下要求：

- a) 数据在存储过程中的完整性保护满足数据提供方对数据的安全保护要求；
- b) 采取技术手段保护数据源到大数据系统之间的数据传输完整性；
- c) 采用校验技术或密码技术保护数据在数据迁移过程中的完整性,包括但不限于业务数据、融合数据、溯源数据等,并在检测到完整性受到破坏时提供恢复措施。

### 8.3.6 数据保密性

数据保密性应满足以下要求：

- a) 大数据平台提供数据脱敏和个人信息去标识化的工具或服务组件技术；
- b) 依据安全策略和数据分类分级标识对数据进行脱敏和个人信息去标识化处理；
- c) 数据在存储过程中的保密性保护满足数据提供方对数据的安全保护要求；
- d) 采取技术措施避免汇聚大量数据时暴露敏感数据,包括但不限于核心数据、重要数据、敏感个人信息、商业秘密信息等；
- e) 对经过脱敏处理的数据进行评估,避免从中可恢复敏感数据。

### 8.3.7 数据备份

数据备份应满足以下要求：

- a) 备份数据依据数据安全保护策略,采取与其数据类别和级别相匹配的安全防护措施；
- b) 大数据平台提供若干个可用的用户数据副本,各副本之间的内容保持一致；
- c) 提供对关键溯源数据的异地备份。

### 8.3.8 剩余信息保护

剩余信息保护应满足以下要求：

- a) 大数据平台提供主动迁移功能,数据整体迁移的过程中杜绝数据残留；
- b) 存有重要的数据和敏感个人信息的存储空间被释放或重新分配前得到完全清除；
- c) 大数据平台能够根据数据分类分级策略以及与客户约定的数据销毁要求和方式实施数据销毁。

### 8.3.9 个人信息保护

个人信息保护应满足以下要求：

- a) 制定覆盖全流程个人信息处理活动的安全管理制度；
- b) 收集、存储、使用、加工、提供、公开个人信息获取个人信息主体授权同意,并保留操作审计记录；
- c) 对个人信息的重要操作设置内部审批流程,审批通过后才能对个人信息进行相应的操作。

### 8.3.10 数据溯源

数据溯源应满足以下要求：

- a) 跟踪和记录数据收集、使用、加工等过程；
- b) 实现数据副本和备份数据管理过程可溯源；
- c) 溯源数据满足数据业务要求和合规审计要求；
- d) 支持从海量数据中自动发现并定位敏感数据的位置、安全等级、数据类型、数据量、归属等；
- e) 对重要数据的生命周期实施数据审计,以便能够对所有数据活动操作进行追溯；
- f) 采取技术手段保护溯源数据真实性、完整性和保密性。

## 8.4 安全管理中心

### 8.4.1 系统管理

系统管理应满足以下要求：

- a) 大数据平台为客户提供管理其计算和存储资源使用状况的能力；
- b) 大数据平台对其提供的辅助工具或服务组件实施有效管理,包括但不限于安装、部署、监控、优化、升级、卸载、身份鉴别、访问控制等,相关操作日志保存至少6个月；
- c) 大数据平台发生计算、内存、存储资源等故障时,不能影响到业务正常运行；
- d) 大数据平台在系统维护、在线扩容等情况下,不影响大数据应用和数据资源的正常业务处理能力。

#### 8.4.2 集中管控

集中管控应满足以下要求：

- a) 对大数据系统提供的各类接口和服务的使用情况进行集中审计和监测,并在发生问题时提供告警;
- b) 对数据安全产品进行集中管理,汇总相关监测数据,对数据安全事件进行关联分析和批量处置。

#### 8.5 安全管理制度

安全管理制度应满足以下要求：

- a) 制定大数据安全工作的总体方针和安全策略,阐明本机构大数据安全工作的目标、范围、原则和安全框架等内容;
- b) 大数据安全策略覆盖数据生存周期相关的数据安全,内容至少包括目的、范围、岗位、责任、管理层承诺、内外部协调及合规性要求等。

#### 8.6 安全管理机构

##### 8.6.1 授权和审批

授权和审批应满足以下要求：

- a) 数据的收集获得数据源所有者的授权,并遵循最小化数据收集的原则;
- b) 建立数据导入、导出、集成、分析、交换、交易、共享及公开的授权审批控制流程,赋予数据活动主体的最小操作权限、最小数据集和权限有效时长,依据流程实施控制并记录过程,及时回收过期的数据访问权限。

##### 8.6.2 审核和检查

应定期审核数据的使用与相关安全管理制度要求的符合情况。

#### 8.7 安全建设管理

##### 8.7.1 供应链管理

供应链管理应满足以下要求：

- a) 选择安全合规的大数据平台,其所提供的大数据平台服务为其所承载的大数据应用和数据资源提供相应等级的安全保护能力;
- b) 以书面方式约定大数据平台提供者和大数据平台使用者的权限与责任、各项服务内容和具体技术指标等,尤其是安全服务内容;
- c) 以书面方式约定数据交换、共享的接收方对数据的保护责任,并明确数据安全保护要求;
- d) 将供应链安全事件信息或安全威胁信息及时传达到数据交换、共享的接收方;
- e) 控制开源、共享软件的使用,并对其代码进行安全审计,针对发现的安全问题进行整改。

##### 8.7.2 数据源管理

应对数据源的数据质量进行评估。

#### 8.8 安全运维管理

##### 8.8.1 资产管理

资产管理应满足以下要求：

- a) 制定数据资产安全管理策略,对数据资产生存周期的操作规范、保护措施、管理人员职责等进行规定;
- b) 制定并执行数据分类分级保护策略,针对不同类别级别的数据制定相应强度的安全保护要求;
- c) 对数据资产和对外数据接口进行梳理,建立相应的资产清单,并实行统一管理,资产清单宜实时动态更新;
- d) 定期评审数据的类别和级别,如需要变更数据所属类别或级别,依据变更审批流程执行变更。

### 8.8.2 介质管理

介质管理应满足以下要求:

- a) 在中国境内对存储敏感数据的介质进行清除或销毁,包括但不限于核心数据、重要数据、敏感个人信息、商业秘密信息等;
- b) 对存储敏感数据的存储介质或物理设备进行销毁时采取难以恢复的技术手段,如物理粉碎、消磁、多次擦写等。

### 8.8.3 网络和系统安全管理

应建立对外数据接口安全管理机制,所有的接口调用均应获得授权和批准。

## 9 第五级安全扩展要求

略。

附 录 A

(资料性)

大数据系统保护对象与安全要求对应

不同类型大数据系统保护对象与安全要求的对应关系见表 A.1。

表 A.1 大数据系统保护对象类型与要求项对应表

标准条款	适用保护对象类型
6.1、7.1、8.1	包含大数据平台、大数据应用或数据资源的定级对象
6.2、7.2a)、8.2a)	包含大数据平台、大数据应用或数据资源的定级对象
7.2b)、8.2b)	包含大数据平台的定级对象
7.2c)、8.2c)	包含大数据平台的定级对象
6.3.1a)	包含大数据平台或大数据应用的定级对象
7.3.1a)、8.3.1a)	包含大数据平台、大数据应用或数据资源的定级对象
6.3.1b)、7.3.1b)、8.3.1b)	包含大数据平台的定级对象
7.3.1c)、8.3.1c)	包含大数据平台的定级对象
7.3.1d)、8.3.1d)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.1e)、8.3.1e)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.1f)、8.3.1f)	包含大数据平台的定级对象
6.3.2a)、7.3.2a)、8.3.2a)	包含大数据平台或大数据应用的定级对象
6.3.2b)、7.3.2b)、8.3.2b)	包含大数据平台、大数据应用或数据资源的定级对象
6.3.2c)、7.3.2c)	包含大数据平台、大数据应用或数据资源的定级对象
8.3.2c)	包含大数据平台、大数据应用或数据资源的定级对象
6.3.2d)、7.3.2d)、8.3.2d)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.2e)、8.3.2e)	包含大数据平台或数据资源的定级对象
7.3.2f)、8.3.2f)	包含大数据平台或数据资源的定级对象
7.3.2g)	包含大数据平台、大数据应用或数据资源的定级对象
8.3.2g)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.2h)	包含大数据平台、大数据应用或数据资源的定级对象
8.3.2h)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.2i)、8.3.2i)	包含大数据平台的定级对象
7.3.2j)、8.3.2j)	包含大数据平台、大数据应用或数据资源的定级对象
6.3.3a)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.3a)、8.3.3a)	包含大数据平台、大数据应用或数据资源的定级对象
6.3.3b)、7.3.3b)、8.3.3b)	包含大数据平台或大数据应用的定级对象
7.3.3c)、8.3.3c)	包含大数据平台、大数据应用或数据资源的定级对象

表 A.1 大数据系统保护对象类型与要求项对应表（续）

标准条款	适用保护对象类型
8.3.3d)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.4a)、8.3.4a)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.4b)、8.3.4b)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.4c)、8.3.4c)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.4d)、8.3.4d)	包含大数据平台、大数据应用或数据资源的定级对象
8.3.4e)	包含大数据平台的定级对象
8.3.4f)	包含大数据平台的定级对象
6.3.4、7.3.5a)、8.3.5a)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.5b)、8.3.5b)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.5c)、8.3.5c)	包含大数据平台或数据资源的定级对象
6.3.5a)、7.3.6a)、8.3.6a)	包含大数据平台的定级对象
6.3.5b)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.6b)、8.3.6b)	包含大数据平台、大数据应用或数据资源的定级对象
6.3.5c)、7.3.6c)、8.3.6c)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.6d)、8.3.6d)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.6e)、8.3.6e)	包含大数据应用的定级对象
6.3.6、7.3.7a)、8.3.7a)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.7b)、8.3.7b)	包含大数据平台的定级对象
7.3.7c)、8.3.7c)	包含大数据平台、大数据应用或数据资源的定级对象
6.3.7a)、7.3.8a)、8.3.8a)	包含大数据平台的定级对象
6.3.7b)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.8b)、8.3.8b)	包含大数据平台、大数据应用或数据资源的定级对象
6.3.7c)	包含大数据平台的定级对象
7.3.8c)、8.3.8c)	包含大数据平台的定级对象
7.3.9a)、8.3.9a)	包含大数据平台、大数据应用或数据资源的定级对象
6.3.8a)、7.3.9b)、8.3.9b)	包含大数据平台、大数据应用或数据资源的定级对象
6.3.8b)、7.3.9c)、8.3.9c)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.10a)、8.3.10a)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.10b)、8.3.10b)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.10c)、8.3.10c)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.10d)、8.3.10d)	包含大数据平台、大数据应用或数据资源的定级对象
7.3.10e)	包含大数据平台、大数据应用或数据资源的定级对象
8.3.10e)	包含大数据平台、大数据应用或数据资源的定级对象

表 A.1 大数据系统保护对象类型与要求项对应表（续）

标准条款	适用保护对象类型
8.3.10f)	包含大数据平台、大数据应用或数据资源的定级对象
6.4a)、7.4.1a)、8.4.1a)	包含大数据平台的定级对象
6.4b)、7.4.1b)、8.4.1b)	包含大数据平台的定级对象
6.4c)、7.4.1c)、8.4.1c)	包含大数据平台的定级对象
6.4d)、7.4.1d)、8.4.1d)	包含大数据平台的定级对象
7.4.2、8.4.2a)	包含大数据平台或大数据应用的定级对象
8.4.2b)	包含大数据平台、大数据应用或数据资源的定级对象
6.5a)、7.5a)、8.5a)	包含大数据平台、大数据应用或数据资源的定级对象
6.5b)、7.5b)、8.5b)	包含大数据平台、大数据应用或数据资源的定级对象
6.6.1、7.6.1a)、8.6.1a)	包含大数据平台、大数据应用或数据资源的定级对象
7.6.1b)、8.6.1b)	包含大数据平台、大数据应用或数据资源的定级对象
6.6.2、7.6.2、8.6.2	包含大数据平台、大数据应用或数据资源的定级对象
6.7a)、7.7a)、8.7.1a)	包含大数据平台、大数据应用或数据资源的定级对象
6.7b)、7.7b)、8.7.1b)	包含大数据平台、大数据应用或数据资源的定级对象
7.7c)、8.7.1c)	包含大数据平台、大数据应用或数据资源的定级对象
7.7d)、8.7.1d)	包含大数据平台、大数据应用或数据资源的定级对象
7.7e)、8.7.1e)	包含大数据平台、大数据应用或数据资源的定级对象
8.7.2	包含大数据平台、大数据应用或数据资源的定级对象
6.8.1a)	包含大数据平台、大数据应用或数据资源的定级对象
6.8.1b)	包含大数据平台、大数据应用或数据资源的定级对象
7.8.1a)、8.8.1a)	包含大数据平台、大数据应用或数据资源的定级对象
7.8.1b)、8.8.1b)	包含大数据平台、大数据应用或数据资源的定级对象
7.8.1c)	包含大数据平台、大数据应用或数据资源的定级对象
8.8.1c)	包含大数据平台、大数据应用或数据资源的定级对象
7.8.1d)、8.8.1d)	包含大数据平台、大数据应用或数据资源的定级对象
7.8.2a)、8.8.2a)	包含大数据平台、大数据应用或数据资源的定级对象
7.8.2b)、8.8.2b)	包含大数据平台、大数据应用或数据资源的定级对象
6.8.2、7.8.3、8.8.3	包含大数据平台、大数据应用或数据资源的定级对象

## 参 考 文 献

- [1] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
  - [2] GB/T 35273—2020 信息安全技术 个人信息安全规范
  - [3] GB/T 35274—2023 数据安全技术 大数据服务安全能力要求
  - [4] GB/T 35295—2017 信息技术 大数据 术语
  - [5] GB/T 35589—2017 信息技术 大数据 技术参考模型
  - [6] GB/T 37973—2019 信息安全技术 大数据安全管理指南
  - [7] T/ISEEE 002—2021 信息安全技术 网络安全等级保护大数据基本要求
  - [8] 大数据标准化白皮书-中电研究院
  - [9] 大数据安全管理自评估指南
  - [10] T-REC-Y.3600-201511 Big data-Cloud computing based requirements and capabilities
  - [11] NIST Special Publication 800-53 联邦信息系统推荐性安全控制措施
  - [12] NIST Special Publication 1500-4 DRAFT NIST Big Data Interoperability Framework: Volume 4, Security and Privacy
  - [13] Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability
  - [14] ENISA Big Data Security: Good Practices and Recommendations on the Security and Resilience of Big Data Services
  - [15] CSA Big Data Working Group: Expanded Top Ten Big Data Security and Privacy Challenges
  - [16] CSA Big Data Security and Privacy Handbook: 100 Best Practices in Big Data Security and Privacy
-

中华人民共和国公共安全  
行业标准  
信息安全技术 网络安全等级保护  
基本要求 第7部分:大数据系统安全  
扩展要求

GA/T 1390.7—2025

\*

中国标准出版社出版发行  
北京市朝阳区和平里西街甲2号(100029)

网址 [www.spc.net.cn](http://www.spc.net.cn)

总编室:(010)68533533 发行中心:(010)51780238

读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷

各地新华书店经销

\*

开本 880×1230 1/16 印张 1.5 字数 34 千字  
2025 年 12 月第 1 版 2025 年 12 月第 1 次印刷

\*

书号: 155066·2-39569 定价 43.00 元

如有印装差错 由本社发行中心调换

版权专有 侵权必究

举报电话:(010)68510107



GA/T 1390.7-2025