ICS 35.040
L 80

ISEAA

团　　体　　标　　准

T/ISEAA 002—2021

信息安全技术
网络安全等级保护大数据基本要求

Information security technology—Big data baseline for classified protection of cybersecurity

2021-04-29 发布　　2021-05-30 实施

中关村信息安全测评联盟　　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。

本文件由中关村信息安全测评联盟提出并归口。

本文件起草单位：公安部第三研究所、杭州华三通信技术有限公司、国家信息中心、华为技术有限公司、杭州安信检测技术有限公司、北京奇虎科技有限公司、腾讯云计算（北京）有限责任公司、阿里巴巴（北京）软件服务有限公司、深圳市网安计算机安全检测技术有限公司、中国移动通信集团有限公司、北京江南天安科技有限公司。

本文件主要起草人：袁静、任卫红、江雷、赵泰、刘静、吴晓艳、孙晓军、章恒、高亚楠、舒俊浩、张丽佳、曾令桐、张睿、王艳辉、郭东东、郭涛、龙军、何冠辉、王永霞、李克鹏、杜文琦、倪祥焕、江为强、陈冠直。

引　言

为了更好地适应国家大数据战略要求，满足大数据技术发展带来的安全防护诉求，提升大数据安全保护的能力，增强大数据安全管理力度，本文件将 GB/T 22239—2019 的通用安全保护要求进行细化和扩展，提出网络运营者整体应实现的大数据安全保护技术和管理要求。

本文件是网络安全等级保护相关系列标准之一。

与本文件相关的标准包括：

——GB/T 22240　信息安全技术　网络安全等级保护定级指南；

——GB/T 22239　信息安全技术　网络安全等级保护基本要求。

在本文件中，**加黑部分**表示较高等级中增加或增强的要求。

信息安全技术
网络安全等级保护大数据基本要求

1 范围

本文件规定了网络安全等级保护第二级到第四级大数据等级保护对象的安全要求，对第五级大数据等级保护对象的安全要求不在本文件中描述。

本文件适用于指导分等级的非涉密大数据等级保护对象的安全建设和监督管理。

注：第五级大数据等级保护对象是非常重要的监督管理对象，对其有特殊的管理模式和安全要求，所以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

GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南

GB/T 35274—2017 信息安全技术 大数据服务安全能力要求

GB/T 35295—2017 信息技术 大数据 术语

GB/T 35589—2017 信息技术 大数据 技术参考模型

3 术语和定义

GB/T 22239—2019、GB/T 35274—2017、GB/T 35295—2017 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]

3.2

数据生命周期 data lifecycle

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

[来源：GB/T 35274—2017，3.2]

4 概述

大数据受到破坏、泄露或篡改会对国家安全、社会秩序或公共利益造成影响，大数据安全保护以数据为核心，以平台为支撑，以应用为导向，关注数据生命周期各环节的安全。

根据 GB/T 22240—2020 给出的定级对象基本特征和 GB/T 35589—2017 给出的大数据参考架构，大数据相关等级保护对象可抽象为大数据资源、大数据应用、大数据平台 3 类组件，如图 1 所示。

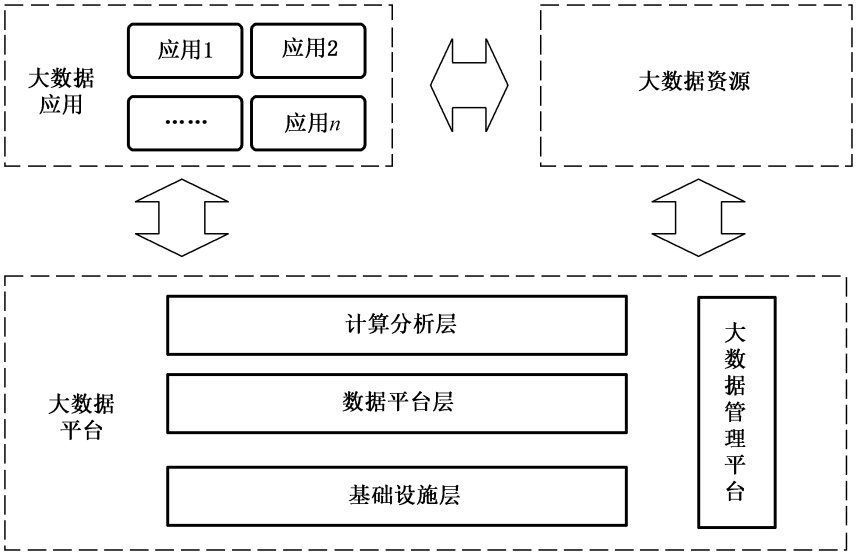

图 1　大数据相关等级保护对象的构成组件

大数据资源：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。

大数据应用：基于大数据平台对数据执行处理过程，通常包括数据采集、数据传输、数据存储、数据处理、数据交换和数据销毁等环节。

大数据平台：为大数据应用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大数据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物理存储、逻辑存储能力；计算分析层提供处理大量、高速、多样和多变数据的分析计算能力；大数据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大数据资源提供服务。

上述组件可能由不同运营者单独承担安全责任，从定级对象的责任主体角度出发，这些组件可独立或组合作为定级对象，例如大数据平台、大数据应用、大数据资源、大数据资源与大数据应用、大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。上述定级对象均可称为“大数据系统”。

5　第二级安全要求

5.1　安全物理环境

5.1.1　物理位置选择

见 GB/T 22239—2019 中 7.1.1.1。

5.1.2　物理访问控制

见 GB/T 22239—2019 中 7.1.1.2。

5.1.3　防盗窃和防破坏

见 GB/T 22239—2019 中 7.1.1.3。

5.1.4　防雷击

见 GB/T 22239—2019 中 7.1.1.4。

5.1.5 防火

见 GB/T 22239—2019 中 7.1.1.5。

5.1.6 防水和防潮

见 GB/T 22239—2019 中 7.1.1.6。

5.1.7 防静电

见 GB/T 22239—2019 中 7.1.1.7。

5.1.8 温湿度控制

见 GB/T 22239—2019 中 7.1.1.8。

5.1.9 电力供应

见 GB/T 22239—2019 中 7.1.1.9。

5.1.10 电磁防护

见 GB/T 22239—2019 中 7.1.1.10。

5.1.11 基础设施位置

应保证承载大数据存储、处理和分析的设备机房位于中国境内。

5.2 安全通信网络

5.2.1 网络架构

本项要求包括：

a) 见 GB/T 22239—2019 中 7.1.2.1；

b) 应保证大数据平台不承载高于其安全保护等级的大数据应用和大数据资源。

5.2.2 通信传输

见 GB/T 22239—2019 中 7.1.2.2。

5.2.3 可信验证

见 GB/T 22239—2019 中 7.1.2.3。

5.3 安全区域边界

见 GB/T 22239—2019 中 7.1.3。

5.4 安全计算环境

5.4.1 身份鉴别

本项要求包括：

a) 见 GB/T 22239—2019 中 7.1.4.1；

b) **大数据系统提供的重要外部调用接口应进行身份鉴别。**

5.4.2 访问控制

本项要求包括：

a) 见 GB/T 22239—2019 中 7.1.4.2；
b) 对外提供服务的大数据平台，平台或第三方应在服务客户授权下才可以对其数据资源进行访问、使用和管理；
c) 应对数据进行分类分级管理；
d) 应采取技术手段对数据采集终端、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；
e) 应最小化各类接口操作权限；
f) 应最小化数据使用、分析、导出、共享、交换的数据集。

5.4.3 安全审计

本项要求包括：
a) 见 GB/T 22239—2019 中 7.1.4.3；
b) 大数据系统应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；
c) 应保证大数据系统服务商对服务客户数据的操作可被服务客户审计。

5.4.4 入侵防范

见 GB/T 22239—2019 中 7.1.4.4。

5.4.5 恶意代码防范

见 GB/T 22239—2019 中 7.1.4.5。

5.4.6 可信验证

见 GB/T 22239—2019 中 7.1.4.6。

5.4.7 数据完整性

本项要求包括：
a) 见 GB/T 22239—2019 中 7.1.4.7；
b) 应采用技术手段对数据交换过程进行数据完整性检测；
c) 数据在存储过程中的完整性保护应满足数据提供方系统的安全保护要求。

5.4.8 数据保密性

本项要求包括：
a) 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；
b) 应依据相关安全策略对数据进行静态脱敏和去标识化处理；
c) 数据在存储过程中的保密性保护应满足数据提供方系统的安全保护要求。

5.4.9 数据备份恢复

本项要求包括：
a) 见 GB/T 22239—2019 中 7.1.4.8；
b) 备份数据应采取与原数据一致的安全保护措施。

5.4.10 剩余信息保护

本项要求包括：
a) 见 GB/T 22239—2019 中 7.1.4.9；
b) 大数据平台应提供主动迁移功能，数据整体迁移的过程中应杜绝数据残留；
c) 大数据平台应能够根据服务客户提出的数据销毁要求和方式实施数据销毁。

5.4.11 个人信息保护

本项要求包括：

a) 见 GB/T 22239—2019 中 7.1.4.10；

b) **采集、处理、使用、转让、共享、披露个人信息应在个人信息处理的授权同意范围内，并保留操作审计记录；**

c) **应采取措施防止在数据处理、使用、分析、导出、共享、交换等过程中识别出个人身份信息；**

d) **对个人信息的重要操作应设置内部审批流程，审批通过后才能对个人信息进行相应的操作。**

5.5 安全管理中心

5.5.1 系统管理

本项要求包括：

a) 见 GB/T 22239—2019 中 7.1.5.1；

b) **大数据平台应为服务客户提供管理其计算和存储资源使用状况的能力；**

c) **大数据平台应对其提供的辅助工具或服务组件实施有效管理；**

d) **大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行；**

e) **大数据平台在系统维护、在线扩容等情况下，应保证大数据应用和大数据资源的正常业务处理能力。**

5.5.2 审计管理

见 GB/T 22239—2019 中 7.1.5.2。

5.6 安全管理制度

5.6.1 安全策略

本项要求包括：

a) 见 GB/T 22239—2019 中 7.1.6.1；

b) 应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、原则和安全框架等相关内容；

c) 大数据安全策略应覆盖数据生命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。

5.6.2 管理制度

见 GB/T 22239—2019 中 7.1.6.2。

5.6.3 制定和发布

见 GB/T 22239—2019 中 7.1.6.3。

5.6.4 评审和修订

见 GB/T 22239—2019 中 7.1.6.4。

5.7 安全管理机构

5.7.1 岗位设置

见 GB/T 22239—2019 中 7.1.7.1。

5.7.2 人员配备

见 GB/T 22239—2019 中 7.1.7.2。

5.7.3 授权和审批

本项要求包括：

a) 见 GB/T 22239—2019 中 7.1.7.3；

b) 数据的采集应获得数据源管理者的授权，确保符合数据收集最小化原则。

5.7.4 沟通和合作

见 GB/T 22239—2019 中 7.1.7.4。

5.7.5 审核和检查

本项要求包括：

a) 见 GB/T 22239—2019 中 7.1.7.5；

b) **应定期对个人信息安全保护措施的有效性进行常规安全检查。**

5.8 安全管理人员

见 GB/T 22239—2019 中 7.1.8。

5.9 安全建设管理

5.9.1 定级和备案

见 GB/T 22239—2019 中 7.1.9.1。

5.9.2 安全方案设计

见 GB/T 22239—2019 中 7.1.9.2。

5.9.3 产品采购和使用

见 GB/T 22239—2019 中 7.1.9.3。

5.9.4 自行软件开发

见 GB/T 22239—2019 中 7.1.9.4。

5.9.5 外包软件开发

见 GB/T 22239—2019 中 7.1.9.5。

5.9.6 工程实施

见 GB/T 22239—2019 中 7.1.9.6。

5.9.7 测试验收

见 GB/T 22239—2019 中 7.1.9.7。

5.9.8 系统交付

见 GB/T 22239—2019 中 7.1.9.8。

5.9.9 等级测评

见 GB/T 22239—2019 中 7.1.9.9。

5.9.10 服务供应商选择

本项要求包括：

a) 见 GB/T 22239—2019 中 7.1.9.10；

b) 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用和大数据资源提供相应等级的安全保护能力；

c) 应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。

5.9.11 供应链管理

应确保供应商的选择符合国家有关规定。

5.9.12 数据源管理

应通过合法正当的渠道获取各类数据。

5.10 安全运维管理

5.10.1 环境管理

见 GB/T 22239—2019 中 7.1.10.1。

5.10.2 资产管理

本项要求包括：

a) 见 GB/T 22239—2019 中 7.1.10.2；

b) **应建立数据资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括但不限于数据采集、传输、存储、处理、交换、销毁等过程；**

c) 应对数据资产进行登记，建立数据资产清单。

5.10.3 介质管理

本项要求包括：

a) 见 GB/T 22239—2019 中 7.1.10.3；

b) **应在中国境内对数据进行清除或销毁。**

5.10.4 设备维护管理

见 GB/T 22239—2019 中 7.1.10.4。

5.10.5 漏洞和风险管理

见 GB/T 22239—2019 中 7.1.10.5。

5.10.6 网络和系统安全管理

本项要求包括：

a) 见 GB/T 22239—2019 中 7.1.10.6；

b) **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。**

5.10.7 恶意代码防范管理

见 GB/T 22239—2019 中 7.1.10.7。

5.10.8 配置管理

见 GB/T 22239—2019 中 7.1.10.8。

5.10.9 密码管理

见 GB/T 22239—2019 中 7.1.10.9。

5.10.10 变更管理

见 GB/T 22239—2019 中 7.1.10.10。

5.10.11 备份与恢复管理

见 GB/T 22239—2019 中 7.1.10.11。

5.10.12 安全事件处置

见 GB/T 22239—2019 中 7.1.10.12。

5.10.13 应急预案管理

见 GB/T 22239—2019 中 7.1.10.13。

5.10.14 外包运维管理

见 GB/T 22239—2019 中 7.1.10.14。

6 第三级安全要求

6.1 安全物理环境

6.1.1 物理位置选择

见 GB/T 22239—2019 中 8.1.1.1。

6.1.2 物理访问控制

见 GB/T 22239—2019 中 8.1.1.2。

6.1.3 防盗窃和防破坏

见 GB/T 22239—2019 中 8.1.1.3。

6.1.4 防雷击

见 GB/T 22239—2019 中 8.1.1.4。

6.1.5 防火

见 GB/T 22239—2019 中 8.1.1.5。

6.1.6 防水和防潮

见 GB/T 22239—2019 中 8.1.1.6。

6.1.7 防静电

见 GB/T 22239—2019 中 8.1.1.7。

6.1.8 温湿度控制

见 GB/T 22239—2019 中 8.1.1.8。

6.1.9 电力供应

见 GB/T 22239—2019 中 8.1.1.9。

6.1.10 电磁防护

见 GB/T 22239—2019 中 8.1.1.10。

6.1.11 基础设施位置

应保证承载大数据存储、处理和分析的设备机房位于中国境内。

6.2 安全通信网络

6.2.1 网络架构

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.2.1；
b) 应保证大数据平台不承载高于其安全保护等级的大数据应用和大数据资源；
c) **应保证大数据平台的管理流量与系统业务流量分离；**
d) **应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。**

6.2.2 通信传输

见 GB/T 22239—2019 中 8.1.2.2。

6.2.3 可信验证

见 GB/T 22239—2019 中 8.1.2.3。

6.3 安全区域边界

见 GB/T 22239—2019 中 8.1.3。

6.4 安全计算环境

6.4.1 身份鉴别

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.4.1；
b) **大数据平台应提供双向认证功能，能对不同客户的大数据应用、大数据资源进行双向身份鉴别；**
c) **应采用口令和密码技术组合的鉴别技术对使用数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的主体实施身份鉴别；**
d) **应对向大数据系统提供数据的外部实体实施身份鉴别；**
e) **大数据系统提供的各类外部调用接口应依据调用主体的操作权限实施相应强度的身份鉴别。**

6.4.2 访问控制

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.4.2；

b) 对外提供服务的大数据平台，平台或第三方应在服务客户授权下才可以对其数据资源进行访问、使用和管理；

c) **大数据系统应提供数据分类分级标识功能；**

d) **应在数据采集、传输、存储、处理、交换及销毁等各个环节，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第三级安全要求，安全保护策略在各环节保持一致；**

e) **大数据系统应对其提供的各类接口的调用实施访问控制，包括但不限于数据采集、处理、使用、分析、导出、共享、交换等相关操作；**

f) 应最小化各类接口操作权限；

g) 应最小化数据使用、分析、导出、共享、交换的数据集；

h) **大数据系统应提供隔离不同客户应用数据资源的能力；**

i) 应对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预警，**并能够对突发的严重异常操作及时定位和阻断。**

6.4.3 安全审计

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.4.3；

b) **大数据系统应保证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；**

c) **大数据系统应对其提供的各类接口的调用情况以及各类账号的操作情况进行审计；**

d) 应保证大数据系统服务商对服务客户数据的操作可被服务客户审计。

6.4.4 入侵防范

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.4.4；

b) **应对所有进入系统的数据进行检测，避免出现恶意数据输入。**

6.4.5 恶意代码防范

见 GB/T 22239—2019 中 8.1.4.5。

6.4.6 可信验证

见 GB/T 22239—2019 中 8.1.4.6。

6.4.7 数据完整性

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.4.7；

b) 应采用技术手段对数据交换过程进行数据完整性检测；

c) 数据在存储过程中的完整性保护应满足数据提供方系统的安全保护要求。

6.4.8 数据保密性

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.4.8；

b) 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；
c) 应依据相关安全策略和**数据分类分级标识**对数据进行静态脱敏和去标识化处理；
d) 数据在存储过程中的保密性保护应满足数据提供方系统的安全保护要求；
e) **应采取技术措施保证汇聚大量数据时不暴露敏感信息；**
f) **可采用多方计算、同态加密等数据隐私计算技术实现数据共享的安全性。**

6.4.9 数据备份恢复

本项要求包括：
a) 见 GB/T 22239—2019 中 8.1.4.9；
b) 备份数据应采取与原数据一致的安全保护措施；
c) **大数据平台应保证用户数据存在若干个可用的副本，各副本之间的内容应保持一致；**
d) **应提供对关键溯源数据的异地备份。**

6.4.10 剩余信息保护

本项要求包括：
a) 见 GB/T 22239—2019 中 8.1.4.10；
b) 大数据平台应提供主动迁移功能，数据整体迁移的过程中应杜绝数据残留；
c) **应基于数据分类分级保护策略，明确数据销毁要求和方式；**
d) 大数据平台应能够根据服务客户提出的数据销毁要求和方式实施数据销毁。

6.4.11 个人信息保护

本项要求包括：
a) 见 GB/T 22239—2019 中 8.1.4.11；
b) 采集、处理、使用、转让、共享、披露个人信息应在个人信息处理的授权同意范围内，并保留操作审计记录；
c) 应采取措施防止在数据处理、使用、分析、导出、共享、交换等过程中识别出个人身份信息；
d) 对个人信息的重要操作应设置内部审批流程，审批通过后才能对个人信息进行相应的操作；
e) **保存个人信息的时间应满足最小化要求，并能够对超出保存期限的个人信息进行删除或匿名化处理。**

6.4.12 数据溯源

本项要求包括：
a) **应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程；**
b) **溯源数据应满足数据业务要求和合规审计要求；**
c) **应采取技术手段保证数据源的真实可信。**

6.5 安全管理中心

6.5.1 系统管理

本项要求包括：
a) 见 GB/T 22239—2019 中 8.1.5.1；
b) 大数据平台应为服务客户提供管理其计算和存储资源使用状况的能力；
c) 大数据平台应对其提供的辅助工具或服务组件实施有效管理；
d) 大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行；
e) 大数据平台在系统维护、在线扩容等情况下，应保证大数据应用和大数据资源的正常业务处理能力。

6.5.2 审计管理

见 GB/T 22239—2019 中 8.1.5.2。

6.5.3 安全管理

见 GB/T 22239—2019 中 8.1.5.3。

6.5.4 集中管控

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.5.4；

b) **应对大数据系统提供的各类接口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。**

6.6 安全管理制度

6.6.1 安全策略

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.6.1。

b) 应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、原则和安全框架等相关内容；

c) 大数据安全策略应覆盖数据生命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。

6.6.2 管理制度

见 GB/T 22239—2019 中 8.1.6.2。

6.6.3 制定和发布

见 GB/T 22239—2019 中 8.1.6.3。

6.6.4 评审和修订

见 GB/T 22239—2019 中 8.1.6.4。

6.7 安全管理机构

6.7.1 岗位设置

见 GB/T 22239—2019 中 8.1.7.1。

6.7.2 人员配备

见 GB/T 22239—2019 中 8.1.7.2。

6.7.3 授权和审批

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.7.3；

b) 数据的采集应获得数据源管理者的授权，确保符合数据收集最小化原则；

c) **应建立数据导入、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，依据流程实施相关控制并记录过程，及时回收过期的数据访问权限；**

d) **应建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程。**

6.7.4 沟通和合作

见 GB/T 22239—2019 中 8.1.7.4。

6.7.5 审核和检查

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.7.5；

b) 应定期对个人信息安全保护措施的有效性进行常规安全检查。

6.8 安全管理人员

见 GB/T 22239—2019 中 8.1.8。

6.9 安全建设管理

6.9.1 定级和备案

见 GB/T 22239—2019 中 8.1.9.1。

6.9.2 安全方案设计

见 GB/T 22239—2019 中 8.1.9.2。

6.9.3 产品采购和使用

见 GB/T 22239—2019 中 8.1.9.3。

6.9.4 自行软件开发

见 GB/T 22239—2019 中 8.1.9.4。

6.9.5 外包软件开发

见 GB/T 22239—2019 中 8.1.9.5。

6.9.6 工程实施

见 GB/T 22239—2019 中 8.1.9.6。

6.9.7 测试验收

见 GB/T 22239—2019 中 8.1.9.7。

6.9.8 系统交付

见 GB/T 22239—2019 中 8.1.9.8。

6.9.9 等级测评

见 GB/T 22239—2019 中 8.1.9.9。

6.9.10 服务供应商选择

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.9.10；

b) 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用和大数据资源提供相应等级的安全保护能力；

c) 应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。

6.9.11 供应链管理

本项要求包括：

a) 应确保供应商的选择符合国家有关规定；

b) **应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；**

c) **应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。**

6.9.12 数据源管理

应通过合法正当的渠道获取各类数据。

6.10 安全运维管理

6.10.1 环境管理

见 GB/T 22239—2019 中 8.1.10.1。

6.10.2 资产管理

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.10.2；

b) 应建立数据资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括但不限于数据采集、传输、存储、处理、交换、销毁等过程；

c) **应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；**

d) **应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，应依据变更审批流程执行变更；**

e) 应对数据资产和**对外数据接口**进行登记管理，建立相应的资产清单。

6.10.3 介质管理

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.10.3；

b) 应在中国境内对数据进行清除或销毁；

c) **对存储重要数据的存储介质或物理设备应采取难恢复的技术手段，如物理粉碎、消磁、多次擦写等。**

6.10.4 设备维护管理

见 GB/T 22239—2019 中 8.1.10.4。

6.10.5 漏洞和风险管理

见 GB/T 22239—2019 中 8.1.10.5。

6.10.6 网络和系统安全管理

本项要求包括：

a) 见 GB/T 22239—2019 中 8.1.10.6；

b) 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。

6.10.7 恶意代码防范管理

见 GB/T 22239—2019 中 8.1.10.7。

6.10.8 配置管理

见 GB/T 22239—2019 中 8.1.10.8。

6.10.9 密码管理

见 GB/T 22239—2019 中 8.1.10.9。

6.10.10 变更管理

见 GB/T 22239—2019 中 8.1.10.10。

6.10.11 备份与恢复管理

见 GB/T 22239—2019 中 8.1.10.11。

6.10.12 安全事件处置

见 GB/T 22239—2019 中 8.1.10.12。

6.10.13 应急预案管理

见 GB/T 22239—2019 中 8.1.10.13。

6.10.14 外包运维管理

见 GB/T 22239—2019 中 8.1.10.14。

7 第四级安全要求

7.1 安全物理环境

7.1.1 物理位置选择

见 GB/T 22239—2019 中 9.1.1.1。

7.1.2 物理访问控制

见 GB/T 22239—2019 中 9.1.1.2。

7.1.3 防盗窃和防破坏

见 GB/T 22239—2019 中 9.1.1.3。

7.1.4 防雷击

见 GB/T 22239—2019 中 9.1.1.4。

7.1.5 防火

见 GB/T 22239—2019 中 9.1.1.5。

7.1.6 防水和防潮

见 GB/T 22239—2019 中 9.1.1.6。

7.1.7 防静电

见 GB/T 22239—2019 中 9.1.1.7。

7.1.8 温湿度控制

见 GB/T 22239—2019 中 9.1.1.8。

7.1.9 电力供应

见 GB/T 22239—2019 中 9.1.1.9。

7.1.10 电磁防护

见 GB/T 22239—2019 中 9.1.1.10。

7.1.11 基础设施位置

应保证承载大数据存储、处理和分析的设备机房位于中国境内。

7.2 安全通信网络

7.2.1 网络架构

本项要求包括：

a) 见 GB/T 22239—2019 中 9.1.2.1；
b) 应保证大数据平台不承载高于其安全保护等级的大数据应用和大数据资源；
c) 应保证大数据平台的管理流量与系统业务流量分离；
d) 应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。

7.2.2 通信传输

见 GB/T 22239—2019 中 9.1.2.2。

7.2.3 可信验证

见 GB/T 22239—2019 中 9.1.2.3。

7.3 安全区域边界

见 GB/T 22239—2019 中 9.1.3。

7.4 安全计算环境

7.4.1 身份鉴别

本项要求包括：

a) 见 GB/T 22239—2019 中 9.1.4.1；
b) 大数据平台应提供双向认证功能，能对不同客户的大数据应用、大数据资源进行双向身份鉴别；
c) 应采用口令和密码技术组合的鉴别技术对使用数据采集终端、数据导入服务组件、数据导出终端、数据导出服务组件的主体实施身份鉴别；
d) 应对向大数据系统提供数据的外部实体实施身份鉴别；
e) 大数据系统提供的各类外部调用接口应依据调用主体的操作权限实施相应强度的身份鉴别。

7.4.2 访问控制

本项要求包括：

a) 见 GB/T 22239—2019 中 9.1.4.2；
b) 对外提供服务的大数据平台，平台或第三方应在服务客户授权下才可以对其数据资源进行访问、使用和管理；
c) 大数据系统应提供数据分类分级标识功能；
d) 应在数据采集、传输、存储、处理、交换及销毁等各个环节，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**第四级**安全要求，安全保护策略在各环节保持一致；
e) **大数据系统应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；**
f) 大数据系统应对其提供的各类接口的调用实施访问控制，包括但不限于数据采集、处理、使用、分析、导出、共享、交换等相关操作；
g) 应最小化各类接口操作权限；
h) 应最小化数据使用、分析、导出、共享、交换的数据集；
i) 大数据系统应提供隔离不同客户应用数据资源的能力；
j) **应采用技术手段限制在终端输出重要数据；**
k) 应对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预警，并能够对突发的严重异常操作及时定位和阻断。

7.4.3 安全审计

本项要求包括：

a) 见 GB/T 22239—2019 中 9.1.4.3；
b) 大数据系统应保证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；
c) 大数据系统应对其提供的各类接口的调用情况以及各类账号的操作情况进行审计；
d) 应保证大数据系统服务商对服务客户数据的操作可被服务客户审计。

7.4.4 入侵防范

本项要求包括：

a) 见 GB/T 22239—2019 中 9.1.4.4；
b) 应对所有进入系统的数据进行检测，避免出现恶意数据输入。

7.4.5 恶意代码防范

见 GB/T 22239—2019 中 9.1.4.5。

7.4.6 可信验证

见 GB/T 22239—2019 中 9.1.4.6。

7.4.7 数据完整性

本项要求包括：

a) 见 GB/T 22239—2019 中 9.1.4.7；
b) 应采用技术手段对数据交换过程进行数据完整性检测；
c) 数据在存储过程中的完整性保护应满足数据提供方系统的安全保护要求。

7.4.8 数据保密性

本项要求包括：

a) 见 GB/T 22239—2019 中 9.1.4.8；
b) 大数据平台应提供静态脱敏和去标识化的工具或服务组件技术；
c) 应依据相关安全策略和数据分类分级标识对数据进行静态脱敏和去标识化处理；
d) 数据在存储过程中的保密性保护应满足数据提供方系统的安全保护要求；
e) 应采取技术措施保证汇聚大量数据时不暴露敏感信息；
f) 可采用多方计算、同态加密等数据隐私计算技术实现数据共享的安全性。

7.4.9 数据备份恢复

本项要求包括：
a) 见 GB/T 22239—2019 中 9.1.4.9；
b) 备份数据应采取与原数据一致的安全保护措施；
c) 大数据平台应保证用户数据存在若干个可用的副本，各副本之间的内容应保持一致；
d) 应提供对关键溯源数据的异地备份。

7.4.10 剩余信息保护

本项要求包括：
a) 见 GB/T 22239—2019 中 9.1.4.10；
b) 大数据平台应提供主动迁移功能，数据整体迁移的过程中应杜绝数据残留；
c) 应基于数据分类分级保护策略，明确数据销毁要求和方式；
d) 大数据平台应能够根据服务客户提出的数据销毁要求和方式实施数据销毁。

7.4.11 个人信息保护

本项要求包括：
a) 见 GB/T 22239—2019 中 9.1.4.11；
b) 采集、处理、使用、转让、共享、披露个人信息应在个人信息处理的授权同意范围内，并保留操作审计记录；
c) 应采取措施防止在数据处理、使用、分析、导出、共享、交换等过程中识别出个人身份信息；
d) 对个人信息的重要操作应设置内部审批流程，审批通过后才能对个人信息进行相应的操作；
e) 保存个人信息的时间应满足最小化要求，并能够对超出保存期限的个人信息进行删除或匿名化处理。

7.4.12 数据溯源

本项要求包括：
a) 应跟踪和记录数据采集、处理、分析和挖掘等过程，保证溯源数据能重现相应过程；
b) **应对重要数据的全生命周期实现数据审计，保证数据活动的所有操作可追溯；**
c) 溯源数据应满足数据业务要求和合规审计要求；
d) **应采取技术手段保证溯源数据真实性和保密性；**
e) 应采取技术手段保证数据源的真实可信。

7.5 安全管理中心

7.5.1 系统管理

本项要求包括：
a) 见 GB/T 22239—2019 中 9.1.5.1；
b) 大数据平台应为服务客户提供管理其计算和存储资源使用状况的能力；
c) 大数据平台应对其提供的辅助工具或服务组件实施有效管理；
d) 大数据平台应屏蔽计算、内存、存储资源故障，保障业务正常运行；

e) 大数据平台在系统维护、在线扩容等情况下，应保证大数据应用和大数据资源的正常业务处理能力。

7.5.2 审计管理

见 GB/T 22239—2019 中 9.1.5.2。

7.5.3 安全管理

见 GB/T 22239—2019 中 9.1.5.3。

7.5.4 集中管控

本项要求包括：

a) 见 GB/T 22239—2019 中 9.1.5.4。

b) 应对大数据系统提供的各类接口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。

7.6 安全管理制度

7.6.1 安全策略

本项要求包括：

a) 见 GB/T 22239—2019 中 9.1.6.1；

b) 应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、原则和安全框架等相关内容；

c) 大数据安全策略应覆盖数据生命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。

7.6.2 管理制度

见 GB/T 22239—2019 中 9.1.6.2。

7.6.3 制定和发布

见 GB/T 22239—2019 中 9.1.6.3。

7.6.4 评审和修订

见 GB/T 22239—2019 中 9.1.6.4。

7.7 安全管理机构

7.7.1 岗位设置

见 GB/T 22239—2019 中 9.1.7.1。

7.7.2 人员配备

见 GB/T 22239—2019 中 9.1.7.2。

7.7.3 授权和审批

本项要求包括：

a) 见 GB/T 22239—2019 中 9.1.7.3；

b) 数据的采集应获得数据源管理者的授权，确保符合数据收集最小化原则；

c) 应建立数据导入、导出、集成、分析、交换、交易、共享及公开的授权审批控制流程，赋予数据活动主体最小的操作权限、最小数据集和权限有效时长，依据流程实施相关控制并记录过程，及

时回收过期的数据访问权限；

d） 应建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程。

7.7.4 沟通和合作

见 GB/T 22239—2019 中 9.1.7.4。

7.7.5 审核和检查

本项要求包括：

a） 见 GB/T 22239—2019 中 9.1.7.5；

b） 应定期对个人信息安全保护措施的有效性进行常规安全检查。

7.8 安全管理人员

见 GB/T 22239—2019 中 9.1.8。

7.9 安全建设管理

7.9.1 定级和备案

见 GB/T 22239—2019 中 9.1.9.1。

7.9.2 安全方案设计

见 GB/T 22239—2019 中 9.1.9.2。

7.9.3 产品采购和使用

见 GB/T 22239—2019 中 9.1.9.3。

7.9.4 自行软件开发

见 GB/T 22239—2019 中 9.1.9.4。

7.9.5 外包软件开发

见 GB/T 22239—2019 中 9.1.9.5。

7.9.6 工程实施

见 GB/T 22239—2019 中 9.1.9.6。

7.9.7 测试验收

见 GB/T 22239—2019 中 9.1.9.7。

7.9.8 系统交付

见 GB/T 22239—2019 中 9.1.9.8。

7.9.9 等级测评

见 GB/T 22239—2019 中 9.1.9.9。

7.9.10 服务供应商选择

本项要求包括：

a） 见 GB/T 22239—2019 中 9.1.9.10；

b) 应选择安全合规的大数据平台，其所提供的大数据平台服务应为其所承载的大数据应用和大数据资源提供相应等级的安全保护能力；
c) 应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。

7.9.11 供应链管理

本项要求包括：
a) 应确保供应商的选择符合国家有关规定；
b) 应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；
c) 应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。

7.9.12 数据源管理

应通过合法正当的渠道获取各类数据。

7.10 安全运维管理

7.10.1 环境管理

见 GB/T 22239—2019 中 9.1.10.1。

7.10.2 资产管理

本项要求包括：
a) 见 GB/T 22239—2019 中 9.1.10.2；
b) 应建立数据资产安全管理策略，对数据全生命周期的操作规范、保护措施、管理人员职责等进行规定，包括但不限于数据采集、传输、存储、处理、交换、销毁等过程；
c) 应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；
d) 应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，应依据变更审批流程执行变更；
e) 应对数据资产和对外数据接口进行登记管理，建立相应的资产清单。

7.10.3 介质管理

本项要求包括：
a) 见 GB/T 22239—2019 中 9.1.10.3；
b) 应在中国境内对数据进行清除或销毁；
c) 对存储重要数据的存储介质或物理设备应采取难恢复的技术手段，如物理粉碎、消磁、多次擦写等。

7.10.4 设备维护管理

见 GB/T 22239—2019 中 9.1.10.4。

7.10.5 漏洞和风险管理

见 GB/T 22239—2019 中 9.1.10.5。

7.10.6 网络和系统安全管理

本项要求包括：
a) 见 GB/T 22239—2019 中 9.1.10.6；
b) 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。

7.10.7 恶意代码防范管理

见 GB/T 22239—2019 中 9.1.10.7。

7.10.8 配置管理

见 GB/T 22239—2019 中 9.1.10.8。

7.10.9 密码管理

见 GB/T 22239—2019 中 9.1.10.9。

7.10.10 变更管理

见 GB/T 22239—2019 中 9.1.10.10。

7.10.11 备份与恢复管理

见 GB/T 22239—2019 中 9.1.10.11。

7.10.12 安全事件处置

见 GB/T 22239—2019 中 9.1.10.12。

7.10.13 应急预案管理

见 GB/T 22239—2019 中 9.1.10.13。

7.10.14 外包运维管理

见 GB/T 22239—2019 中 9.1.10.14。

8 第五级安全要求

略。

参 考 文 献

[1] NIST Special Publication 800-53 Security and Pricacy Controls for Federal Information Systems and Organizations

[2] NIST Special Publication 1500-4 DRAFT NIST Big Data Interoperability Framework: Volume 4, Security and Privacy

[3] ENISA Big Data Security:Good Practices and Recommendations on the Security and Resilience of Big Data Services

[4] CSA Big Data Working Group:Expanded Top Ten Big Data Security and Privacy Challenges

[5] CSA Big Data Security and Privacy Handbook: 100 Best Practices in Big Data Security and Privacy

[6] T-REC-Y.3600—2015:Big data—Cloud computing based requirements and capabilities

[7] Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability