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。