|  |  |
| --- | --- |
| ICS  | 35.240  |
| CCS  | L70 |

|  |
| --- |
|  43 |

湖南省地方标准

DB 43/T XXXX—XXXX

政务数据分类分级规范

Classification and grading specifications for government affairs data

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](#_Toc181286217)

[1 范围 4](#_Toc181286218)

[2 规范性引用文件 4](#_Toc181286219)

[3 术语和定义 4](#_Toc181286220)

[4 分类分级原则 5](#_Toc181286221)

[5 数据分类 5](#_Toc181286222)

[5.1 方法 5](#_Toc181286223)

[5.1.1 分类框架 5](#_Toc181286224)

[5.1.2 数据用途维度 6](#_Toc181286225)

[5.1.3 数据主体维度 6](#_Toc181286226)

[5.1.4 数据共享维度 6](#_Toc181286227)

[5.1.5 数据来源维度 7](#_Toc181286228)

[5.2 流程 7](#_Toc181286229)

[5.2.1 概述 7](#_Toc181286230)

[5.2.2 分类准备 7](#_Toc181286231)

[5.2.3 分类实施 8](#_Toc181286232)

[5.2.4 维护改进 8](#_Toc181286233)

[6 数据分级 8](#_Toc181286234)

[6.1 方法 8](#_Toc181286235)

[6.1.1 分级对象 8](#_Toc181286236)

[6.1.2 分级框架 8](#_Toc181286237)

[6.1.3 数据影响分析 8](#_Toc181286238)

[6.1.4 分级规则 9](#_Toc181286239)

[6.2 流程 9](#_Toc181286240)

[6.2.1 概述 9](#_Toc181286241)

[6.2.2 数据梳理 10](#_Toc181286242)

[6.2.3 数据分级准备 10](#_Toc181286243)

[6.2.4 数据级别判定 10](#_Toc181286244)

[6.2.5 数据级别审核 10](#_Toc181286245)

[6.2.6 数据级别批准 11](#_Toc181286246)

[6.3 级别变更 11](#_Toc181286247)

[6.3.1 变更情形 11](#_Toc181286248)

[6.3.2 变更要求 11](#_Toc181286249)

[7 数据分类分级实施流程 11](#_Toc181286250)

[7.1 实施流程图 11](#_Toc181286251)

[7.2 主要步骤 12](#_Toc181286252)

[8 数据安全分级管控要求 12](#_Toc181286253)

[附录A（资料性） 数据分级与共享开放对应参考 13](#_Toc181286254)

[附录B（资料性） 数据安全分级管控要求 14](#_Toc181286255)

[附录C（资料性） 个人信息分类分级参考示例 20](#_Toc181286256)

[参考文献 23](#_Toc181286257)

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。

本文件由湖南省数据局提出并归口。

本文件起草单位：

本文件主要起草人：

政务数据分类分级规范

* 1. 范围

本文件规定了政务数据分类分级原则、数据分类方法与流程、数据分级方法与分级流程及级别变更情形要求、数据分级分类实施流程、数据安全分级管控要求等。

本文件适用于指导湖南省范围内政务数据的分类分级工作。

本文件不适用于涉及国家秘密的政务数据。

* 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 38664.1 信息技术 大数据 政务数据开放共享 第1部分：总则

GB/T 38667 信息技术 大数据 数据分类指南

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 38664.1、GB/T 38667、GB/T 43697界定的以及下列术语和定义适用于本文件。

政务数据 government affairs data

各级政务部门及其技术支撑单位在履行职责过程中依法采集、生成、存储、管理的各类数据资源。

[来源：GB/T 38664.1，3.1，有修改]

政务数据分类（以下简称“数据分类”） government affairs data categorization

根据数据的属性或特征，将其按一定的原则和方法进行区分和归类，并建立起一定的分类体系和排列顺序的过程。

[来源：GB/T 38667，3.3，有修改]

政务数据分级（以下简称“数据分级”） government affairs data classification

根据政务数据的敏感程度和遭到破坏、泄露、篡改、非法利用后对国家安全、经济运行、社会稳定、公共利益、组织权益、个人权益造成的影响程度，按照一定的原则和方法进行定级。

政务数据共享（以下简称“数据共享”） government affairs data sharing

各级政务部门因履行职责需要，使用其他政务部门的政务数据以及为其他政务部门提供政务数据的行为。

[来源：GB/T 38664.1，3.2]

政务数据开放 government affairs data opening

各级政务部门在安全保密、公共利益导向前提下，面向个人、法人和其他组织提供具有原始性、可机器读取、可供社会化利用的数据集的数据服务。

[来源：GB/T 38664.1，3.3，有修改]

重要数据 key data

特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

1. 仅影响组织自身或公民个体的数据一般不作为重要数据。

[来源：GB/T 43697，3.2，有修改]

核心数据 core 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，一旦被非法使用或共享，可能直接影响政治安全的重要数据。

1. 核心数据主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据。

[来源：GB/T 43697，3.3]

衍生数据 derived data

经过统计、关联、挖掘、聚合、去标识化等加工活动而产生的数据。

[来源：GB/T 43697，3.10]

个人信息 personal information

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各种信息，不包括匿名化处理后的信息。

[来源：GB/T 43697，3.5，有修改]

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。

1. 个人敏感数据：生物识别信息、宗教信仰信息、特定身份信息、医疗健康信息、金融账户信息、行踪轨迹信息、未成年人个人信息。

[来源：GB/T 43697，3.6，有修改]

* 1. 分类分级原则

政务数据分类分级原则按照GB/T 43697 中数据分类分级基本原则要求执行。

* 1. 数据分类
		1. 方法
			1. 分类框架

本文件采用多维度和线分类法相结合的方法，政务部门可选择数据用途、数据主体、数据共享、数据来源四个维度中一个或多个维度对数据进行分类，对于各级类别划分，可根据实际需要，采用线分类法（示意图参见图1）进行细分。

1. 线分类法主要是按照选定的若干属性（或特征），逐次地分为若干层级，每个层级又分为若干类目，同一分支的同层级类目之间构成并列关系，不同层级类目之间构成隶属关系。



1. 线分类法示意图
	* + 1. 数据用途维度

按照政务数据的管理属性进行细化分类，一级类别分为基础数据、主题数据、专题数据。

二级类别在一级类别基础上细化，参考如下：

1. 基础数据：国家人口基础数据、法人单位基础数据、自然资源和空间地理基础数据、社会信用基础数据、电子证照基础数据等类别；
2. 主题数据：公共服务、健康保障、社会保障、食品药品安全、安全生产、价格监管、能源安全、信用体系、城乡建设、社区治理、生态环保、应急维稳等类别；
3. 专题数据：社会服务、经济发展、公共安全、城市运行、社会稳定、舆情监测等类别。
4. 主题数据是围绕经济社会发展的同一主题领域，由多部门数据共同形成的政务数据目录。
	* + 1. 数据主体维度

按照政务数据所属主体或属性进行细化分类，一级类别分为组织数据、个人信息。其中：

1. 组织数据指政务部门在自身运营活动中收集、产生的不涉及个人信息和公共利益的数据；
2. 个人信息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各种信息。

二级类别在一级类别基础上细化，参考如下：

1. 组织数据：不涉及个人信息和公共利益的业务数据、经营管理数据、系统运维数据等类别；
2. 个人信息：个人身份信息、个人生物识别信息、个人财产信息、个人通信信息、个人位置信息、个人健康生理信息等类别。
	* + 1. 数据共享维度

按照湖南省政务信息资源共享属性及要求将政务数据分类为：

1. 无条件共享类：可提供给所有政务部门共享使用的政务信息资源；
2. 有条件共享类：可提供给相关政务部门或者仅能够部分提供给其他政务部门共享使用的政务信息资源；
3. 不予共享类：不宜提供给其他政务部门共享使用的政务信息资源。
	* + 1. 数据来源维度

按照政务数据来源属性，将政务数据分类为：

1. 政府部门数据，根据来源部门进行细化；
2. 法人及其他组织数据；
3. 公民个人数据。
	* 1. 流程
			1. 概述

数据分类根据数据管理和使用需求，可结合已有数据分类基础，灵活选择业务属性将数据细化分类，数据分类工作流程参见图2。



1. 数据分类工作流程
	* + 1. 分类准备

调研业务数据。对单位内数据的产生情况、存储现状、质量情况、业务类型、敏感程度、应用情况、时效性情况以及权属情况等进行调查研究。

确定数据范围。政务部门按照行业领域主管（监管）部门职责，结合数据调研情况，明确本单位数据分类范围和对象。

确定分类维度。选择数据分类维度，初步确定使用分类维度方法，可选择单个维度或多个维度组合进行分类。

* + - 1. 分类实施

制定分类计划。拟定数据分类工作具体的分类实施计划，包括但不限于明确实施步骤、确定实施人员、拟使用实施工具（含模板材料）、开展实施工作要求和检查实施成果要求等。

分类方法审批。政务部门可组织审核数据分类的对象、方法及分类表，并对数据分类对象、方法及分类表进行审议批准。

分类框架制定。对照分类框架结构，从对应的类别中选择适用的分类将数据逐层分类。一级类别应维持不变，二级类别和三级类别可根据实际需要进行扩展，也可继续划分四级子类，细化形成数据规则。

数据分类实施。结合政务数据的实际应用场景拟定具体的分类实施流程，并使用自动化开发工具或脚本，利用其分类算法对政务数据进行分类。同时记录分类实施过程中的各步骤及其分类结果。

分类结果审核。对最后分类完成结果，应形成相关清单内容，并对其内容进行核查，保障数据分类的准确性、一致性。

* + - 1. 维护改进

定期评估。定期评估数据分类维度和方法的合理性，检查其是否符合业务场景变化和数据管理需要，定期评估数据分类结果的有效性和应用情况，检查其是否满足业务应用需求的更新。

变更控制。数据资源分类进行变更时，分析数据资源所属分类变更的必要性和合理性，确定是否实施变更；应对新增的业务数据分类结果进行评估并发布新增的业务数据分类结果。

* 1. 数据分级
		1. 方法
			1. 分级对象

数据分级对象主要包括结构化数据、半结构化数据和非结构化数据，数据分级的最小单元为数据项，对数据项进行分级时，默认数据项集合的安全级别为其所包含数据项级别的最高级别。非结构化数据应按照其数据标签及标签聚合情况下的敏感程度进行分级。

* + - 1. 分级框架

根据数据在经济社会发展中的重要程度，以及一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益造成的危害程度，将数据从高到低分为核心数据、重要数据、一般数据三个级别；根据单位内部数据安全管控需求，将一般数据继续细分级别，由高到低分为二级、一级，总体包括四个安全等级。

* + - 1. 数据影响分析

影响对象指政务数据安全性遭受破坏后受到影响的对象，包括国家安全、经济运行、社会稳定、公共利益、组织权益、个人权益等，影响对象的判断与分析应按照GB/T 43697中6.4.1要求执行。

影响程度是指数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能造成的影响程度。影响程度从高到低可分为特别严重危害、严重危害、一般危害。影响程度的规则确定应按照GB/T 43697中6.4.2要求执行。

* + - 1. 分级规则

根据数据的安全属性被破坏后造成的影响对象、影响程度，将数据划分为四个级别，由高到低分别为四级、三级、二级、一级，触发其中一个即达到对应的最低安全等级，具体对应关系见表1。

1. 数据分级规则

|  |  |  |  |
| --- | --- | --- | --- |
| 数据等级 | 影响对象 | 影响程度 | 数据示例 |
| 四级 | 核心数据 | 国家安全 | 特别严重危害/严重危害 | 如：直接关系国民经济命脉的重要行业和关键领域的经济利益安全的数据。 |
| 经济运行 | 特别严重危害 |
| 社会秩序 | 特别严重危害 |
| 公共利益 | 特别严重危害 |
| 三级 | 重要数据 | 国家安全 | 一般危害 | 如：如未公开的领陆、领水、领空数据、满足一定精度指标的地理数据或与战略物资产能、储备量有关的数据、记录历史文化遗产的数据、描述重点安保单位、重要生产企业、国家重要资产（如铁路、输油管道）的施工图、内部结构、安防情况的数据。 |
| 经济运行 | 严重危害/一般危害 |
| 社会秩序 | 严重危害 |
| 公共利益 | 严重危害 |
| 二级 | 一般数据（极敏感） | 经济运行 | 一般危害 | 如：公共交通调度数据，敏感个人信息或组织商业秘密中的核心技术等秘密信息。 |
| 社会秩序 | 一般危害 |
| 公共利益 | 一般危害 |
| 组织权益 | 特别严重危害 |
| 个人权益 | 特别严重危害 |
| 一级 | 一般数据（一般/敏感） | 组织权益 | 一般危害/严重危害/无危害 | 如：已去标识化的个人信息或统计数据，组织商业秘密中的一般信息。 |
| 个人权益 | 一般危害/严重危害/无危害 |

* + 1. 流程
			1. 概述

数据分级根据数据内容和安全属性，结合国家及行业有关法律法规、部门规章要求与数据规模、数据时效性、数据形态进行数据分级，数据分级工作流程参见图3。



1. 数据分级工作流程
	* + 1. 数据梳理

对数据进行盘点后，按照本文件5.1.1进行梳理与分类，形成统一的数据清单，并按类别进行数据分级准备工作。

* + - 1. 数据分级准备

识别不同类别数据内容及其安全属性遭到破坏后可能影响的对象和范围。

* + - 1. 数据级别判定

在6.1.4基础上，结合国家及行业有关法律法规、部门规章要求，按照以。下规则对数据级别进行综合判定，形成数据级别评定结果及不同级别的数据清单：

1. 如数据涉及多个要素、多个影响对象或影响程度,应按照就高从严原则确定数据级别；
2. 数据项集合级别可在数据项级别的基础上,按照就高从严的原则,将数据项集合包含数据项的最高级别作为数据集默认级别,但同时也要考虑分级要素(如数据规模)变化可能需要调高级别；
3. 数据集中各数据项级别与数据集级别不一定相同,具体要根据该数据项的影响对象和影响程度进行判断。
4. 衍生数据级别可按照就高从严原则，在原始数据级别的基础上,综合考虑加工后的数据深度等分级要素对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益的影响进行确定；
5. 跨行业领域数据分级,原则上可按照数据来源的行业领域数据分级规则确定级别,如果存在跨行业领域数据融合加工,需考虑融合加工对数据分级要素的影响,按照衍生数据确定级别。
	* + 1. 数据级别审核

审核数据分级评定过程和结果，必要时重复本文件6.2.4及其后工作，直至级别的划定与数据安全保护目标一致。

* + - 1. 数据级别批准

应由数据安全管理决策组织对数据分级结果进行审议批准。

* + 1. 级别变更
			1. 变更情形

数据分级完成后，出现下列情形之一时，政务部门应对相关数据的级别进行变更，并按照数据分级流程实施：

1. 数据内容发生变化，导致原有数据的分级级别不适用变化后的数据；
2. 数据内容未发生变化，但因数据时效性、数据规模、数据使用场景、数据加工处理方式等发生变化，导致原定的数据级别不再适用；
3. 因数据汇聚融合，导致原有数据级别不再适用汇聚融合后的数据；
4. 因国家或行业主管部门要求变化，导致原定的数据级别不再适用；
5. 需要对数据级别进行变更的其他情形。
	* + 1. 变更要求

安全级别变更要求包括：

1. 从原始数据中直接部分复制出来的新数据级别不应高于原有数据级别；
2. 从多个原始数据直接合并的新数据不应低于原有数据级别；
3. 对不同数据选取部分数据进行合并形成的新数据，应根据新数据的关键要素进行重新判定；
4. 数据内容不发生变化时，级别变更需有明确的依据；
5. 安全级别变更时，应由数据管理部门的相关主要领导人进行审批同意；
6. 汇聚数据的安全级别须经数据使用方和数据所属方联合评估确认后进行判定。
	1. 数据分类分级实施流程
		1. 实施流程图

数据分类分级实施流程参见图4。



1. 数据分类分级实施流程图
	* 1. 主要步骤

数据资产识别。对数据资产进行全面梳理，包括以物理或电子形式记录的数据库表、数据项、数据文件等结构化和非结构化数据资产，明确数据资产基本信息和相关方，形成数据资产清单。

数据分类确定。依据本文件5.2数据分类流程，参考本文件5.1.1分类框架，建立数据分类规则及框架，对相关数据资产进行识别和分类。

数据级别判定。依据本文件6.2数据分级流程，结合本文件6.1.4分级规则，对数据分类框架判定级别，形成分类分级框架，统一分类分级标准，并实施数据分类分级。

审核标识管理。对数据分类分级结果进行审核和完善，最后批准发布实施，对数据进行分类分级标识，形成数据分类分级清单、政务数据目录清单和重要数据、核心数据目录。政务数据目录清单宜细化到表、文件级别，必要情况下需细化到字段级别，清单应至少包含数据基础信息、数据存储信息、分类分级信息。重要数据、核心数据目录形成后应按有关程序报送。

动态更新管理。根据数据重要程度和可能造成危害程度的变化，对数据分类分级规则、重要数据/核心数据目录、数据分类分级清单及标识等进行动态更新管理，动态更新场景及数据安全级别变化示例见表2。

1. 数据安全级别变化示例

|  |  |
| --- | --- |
| 数据级别变更 | 场景 |
| 升级 | 数据体量增加到特定规模导致产生社会重大影响 |
| 升级 | 达到国家有关部门规定精度的数据 |
| 升级 | 关联多个业务部门的数据 |
| 升级 | 大量多维数据进行关联 |
| 升级 | 发生特定事件导致数据敏感性增强 |
| 降级 | 数据已被公开或披露 |
| 降级 | 数据进行脱敏或删除关键字段 |
| 降级 | 数据进行去标识化、假名化、匿名化 |
| 降级 | 数据发生特定事件导致数据失去敏感性 |

* 1. 数据安全分级管控要求

数据安全分级管控应依据数据分类分级结果与共享开放属性进行对应，将业务属性与安全级别关联（参见附录A），按照数据处理活动制定数据分级安全管控要求（参见附录B），制定个人信息分类分级参考示例（参见附录C）。

政务部门在进行数据安全分级管控时，除满足国家信息安全相关规范之外，还应满足本文件要求。

1. （资料性）
数据分级与共享开放对应参考

数据分级及共享开放属性与数据分级的对应参考见表A.1。

* 1. 数据分级及共享开放对应参考

|  |  |  |
| --- | --- | --- |
| 数据分级 | 共享 | 开放 |
| 一级 | 无条件共享 | 有条件开放（审批/脱敏） |
| 二级 | 有条件共享 | 有条件开放/不予开放 |
| 三级 | 有条件共享 | 不予开放 |
| 四级 | 不予共享 | 不予开放 |

1.
2. （资料性）
数据安全分级管控要求

数据分级安全管控要求见表B.1。

* 1. 数据分级安全管控要求

| 政务数据管理活动 | 数据分级安全管控要求 |
| --- | --- |
| 通用要求 | 一级数据 | 二级数据 | 三级数据 | 四级数据 |
| 数据采集 | 1.明确数据采集目的、方式、数量、用途、获取源、接收方、范围、频率和周期等，规范数据采集的流程和方法；2.对数据采集行为进行监控与审计，一旦发现异常行为（如采集异常、传输量超过设定阀值）需及时告警。 | 在有可参照原始数据的情况下，采取双向认证及完整性校验，保障数据采集前后的完整性、一致性。 | 1.在有可参照原始数据的情况下，采取双向认证及完整性校验，保障数据采集前后的完整性、一致性；2.数据采集前应与数据拥有者进行协商，在获得数据拥有者的明确授权后方可进行数据采集；3.对数据采集的工具、系统、设备等进行安全检测，确保数据采集端安全；4.对数据采集的工具、系统、设备采用准入控制、身份认证和访问权限控制，避免非法访问；5.对采集的数据源的有效性、安全性进行鉴别，禁止采集来源不明的数据；6.对采集数据内容的完整性、可用性进行校验；7.在数据采集过程中采取管理和技术措施防止数据泄漏。 | 1.数据采集前应与数据拥有者进行协商，在获得数据拥有者的明确授权后方可进行数据采集；2.对数据采集的工具、系统、设备等进行安全检测，确保数据采集端安全；3.对数据采集的工具、系统、设备采用准入控制、身份认证和访问权限控制，避免非法访问；4.对采集的数据源的有效性、安全性进行鉴别，禁止采集来源不明的数据；5.在有可参照原始数据的情况下，采取双向认证及完整性校验，保障采集数据的完整性、一致性；6.对采集数据内容的可用性进行校验；7.在数据采集过程中采取管理和技术措施防止数据泄漏；8.对采集的数据进行加密保护；9.采集的数据禁止在终端留存。 | 1.在有可参照原始数据的情况下，采取双向认证及完整性校验，保障数据采集前后的完整性、一致性；2.数据采集前应与数据拥有者进行协商，在获得数据拥有者的明确授权后方可进行数据采集；3.对数据采集的工具、系统、设备等进行安全检测，确保数据采集端安全；4.对数据采集的工具、系统、设备采用准入控制、身份认证和访问权限控制，避免非法访问；5.对采集的数据源的有效性、安全性进行鉴别，禁止采集来源不明的数据；6.对采集数据内容的完整性、可用性进行校验；7.在数据采集过程中采取管理和技术措施防止数据泄漏；8.数据采集的工具、系统、设备账号应采用双因素认证；9.采取合理的加密方式对数据进行保护；10.采集的数据禁止在终端留存；11.使用溯源分析等技术手段，对数据泄露风险进行分析，对采集行为进行追踪溯源。 |
| 数据传输 | 1.对数据传输范围进行控制，仅发送给内部人员，外部人员需使用数据时**，**只能通过堡垒机、云桌面或大数据中心内部配发的终端；2.对数据传输过程和内容进行记录；3.对传输的数据内容进行敏感信息的监测与识别，对违规传输行为进行告警与处置。 | 建立数据传输接口安全管理规范，包括跨机构内部区域、跨机构和跨境数据传输接口等。 | 1.建立数据传输接口安全管理规范，包括跨机构内部区域、跨机构和跨境数据传输接口等；2.对数据传输范围进行控制，仅发送给相关人员；3.建立传输两端的身份认证机制，使用身份认证技术（如密码、证书等）；4.应采用加密通道进行数据传输，如SSL、TLS等安全协议进行数据传输，保证传输数据的保密性、完整性。 | 1.建立数据传输接口安全管理规范，包括跨机构内部区域、跨机构和跨境数据传输接口等；2.对数据传输范围进行控制，仅发送给相关人员；3.建立传输两端的身份认证机制，使用身份认证技术（如密码、证书等）；4.应采用加密通道进行数据传输，如SSL、TLS等安全协议进行数据传输，保证传输数据的保密性、完整性；5.采用加密技术，保证数据在传输过程中的完整性、保密性和可用性，加密算法和产品的选择应符合国家有关规定。 | 1.建立数据传输接口安全管理规范，包括跨机构内部区域、跨机构和跨境数据传输接口等；2.对数据传输范围进行控制，仅发送给相关人员；3.建立传输两端的身份认证机制，使用身份认证技术（如密码、证书等）；4.应采用加密通道进行数据传输，如SSL、TLS等安全协议进行数据传输，保证传输数据的保密性、完整性；5.采用加密技术，保证数据在传输过程中的完整性、保密性和可用性，加密算法和产品的选择应符合国家有关规定；6.应具备数据溯源能力，确保所有数据传输路径可恢复，数据传输行为可溯源；7.应具备数据传输实时监测处置能力，保证能够及时告警并阻断违规传输。 |
| 数据存储 | 1.建立数据存储管理规范和制度；2.对存储服务器、数据库服务器、文件系统等进行主机加固、漏洞扫描，确保数据存储环境安全，终端访问应符合大数据中心内部接入要求，数据库访问通过堡垒机、数据库运维工具进行，确保数据访问环境安全；3.定期对数据库进行漏洞扫描；4.对应用服务器、数据库服务器的访问开启身份认证和访问控制，防止非法访问；5.利用数据库审计、日志审计、主机审计等技术措施对数据存储情况进行记录；6.数据存储位置仅允许存放大数据中心内部电脑或服务器；7.定期对系统数据进行备份，如每月对数据库表进行全量备份，每周对数据库表进行数据增量备份，每天进行数据差量备份。 | 遵循通用要求 | 1.建立数据存储系统的账号权限管理制度；2.设置数据访问控制规则；3.应采取技术手段防止数据的泄漏、篡改。 | 1.建立数据存储系统的账号权限管理制度；2.设置数据访问控制规则；3.应采取技术手段防止数据的泄漏、篡改；4.应采取技术手段对存储数据的使用身份进行认证和鉴权；5.应提供对数据泄漏、篡改、破坏的监测和告警；6.应采用文件加密或数据加密方式存储，实现存储数据的保密性、完整性和可用性。 | 1.建立数据存储系统的账号权限管理制度；2.设置数据访问控制规则；3.应采取技术手段防止数据的泄漏、篡改；4.应采取技术手段对存储数据的使用身份进行认证和鉴权；5.应提供对数据泄漏、篡改、破坏的监测和告警；6.应采用文件加密或数据加密方式存储，实现存储数据的保密性、完整性和可用性；7.建立本地备份及异地备份保护和恢复措施，应设置合理的恢复点和恢复时间；8.应采取措施对数据实行区域隔离存储。 |
| 数据使用 | 1.建立数据使用管理流程，明确使用目的、范围及使用属性；2.应提供数据使用测试环境，在测试环境开展数据使用过程的设计和开发，验证通过后再置入生产环境运行；3.应采取措施确保数据在使用中的环境安全。 | 对数据使用系统的账户进行统一管理、统一认证、统一授权。 | 1.对数据使用系统的账户进行统一管理、统一认证、统一授权；2.建立访问权限管理及身份认证机制，对系统用户采用身份鉴别手段，**并**对数据的使用进行授权和验证；3.应在不影响数据使用的情况下，对数据脱敏后再进行处理；4.应对超出范围和超出规模的数据使用行为开展监测和告警。 | 1.对数据使用系统的账户进行统一管理、统一认证、统一授权；2.建立访问权限管理及身份认证机制，对系统用户采用身份鉴别手段，**并**对数据的使用进行授权和验证；3.应在不影响数据使用的情况下，对数据脱敏后再进行处理；4.应对超出范围和超出规模的数据使用行为开展监测和告警；5.对数据使用权限进行访问控制，仅允许授权人员访问；6.应周期性的检查数据使用系统用户操作数据的情况。 | 1.对数据使用系统的账户进行统一管理、统一认证、统一授权；2.建立访问权限管理及身份认证机制，对系统用户采用身份鉴别手段，**并**对数据的使用进行授权和验证；3.应在不影响数据使用的情况下，对数据脱敏后再进行处理；4.应对超出范围和超出规模的数据使用行为开展监测和告警；5.对数据使用权限进行访问控制，仅允许授权人员访问；6.应周期性的检查数据使用系统用户操作数据的情况；7.应具备数据使用行为实时监控能力，在发现异常时及时终止数据使用行为，并采用技术手段确保所有数据挖掘、使用、使用、分析等行为可溯源。 |
| 数据共享开放 | 1.应建立数据共享开放管理流程，明确数据共享开放的范围、数量、条件、程序等，并与数据获取方签订数据安全协议；2.应具备数据共享开放安全监控技术能力，确保提供的数据合理规范使用，未超出授权范围。 | 1.数据共享开放应由数据所有者进行审批，并对相关操作进行记录；2.数据共享开放应通过指定平台或方式进行，如共享交换平台、共享网站等。 | 1.数据共享开放应由数据所有者进行审批，并对相关操作进行记录；2.数据共享开放应通过指定平台或方式进行，如共享交换平台、共享网站等；3.建立数据共享开放的工具、系统，对提供过程进行审批授权，并采用不可篡改技术实现提供过程审批授权的记录；4.数据共享开放前应与数据拥有者进行协商，在获得数据拥有者的明确授权后方可提供相关数据。 | 1.数据共享开放应由数据所有者进行审批，并对相关操作进行记录；2.数据共享开放应通过指定平台或方式进行，如共享交换平台、共享网站等；3.建立数据共享开放的工具、系统，对提供过程进行审批授权，并采用不可篡改技术实现提供过程审批授权的记录；4.数据共享开放前应与数据拥有者进行协商，在获得数据拥有者的明确授权后方可提供相关数据；5.应采取技术措施对提供审批的业务过程和数据共享开放的技术过程开展风险监测和预警，对违规行为及时报警或阻断；6.应采取必要的保护措施，包括但不限于数据脱敏、数据水印等技术手段进行数据共享开放。 | 1.数据共享开放应由数据所有者进行审批，并对相关操作进行记录；2.数据共享开放应通过指定平台或方式进行，如共享交换平台、共享网站等；3.建立数据共享开放的工具、系统，对提供过程进行审批授权，并采用不可篡改技术实现提供过程审批授权的记录；4.数据共享开放前应与数据拥有者进行协商，在获得数据拥有者的明确授权后方可提供相关数据；5.应采取技术措施对提供审批的业务过程和数据共享开放的技术过程开展风险监测和预警，对违规行为及时报警或阻断；6.应采取必要的保护措施，包括但不限于数据脱敏、数据水印等技术手段进行数据共享开放；7.采用可用不可见的方式进行数据共享开放，如有特殊情况应采取“一事一议”进行审批。 |

1. （资料性）
个人信息分类分级参考示例

个人信息分类分级参考示例见表C.1。

表C.1 个人信息分类分级参考示例

| 一级类别 | 二级类别 | 典型示例和说明 | 级别 | 备注 |
| --- | --- | --- | --- | --- |
| 个人基本资料 | 个人基本资料 | 自然人基本情况信息，如个人姓名、生日、年龄、性别、民族、国籍、籍贯、婚姻状况、家庭关系、住址、个人电话号码、电子邮件地址、兴趣爱好等。 | 一级 | 100万条以上或覆盖范围超过1个地市为重要数据（三级） |
| 个人身份信息 | 个人身份信息 | 可直接标识自然人身份的信息，如身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证、港澳台通行证等证件号码、证件有效期、证件照片或影印件等。 | 二级 |
| 个人生物识别信息 | 个人生物识别信息 | 生物识别原始信息（如样本、图像等）和比对信息（如特征值、模板等），如人脸、指纹、步态、声纹、基因、虹膜、笔迹、掌纹、耳廓、眼纹等。 | 二级 |
| 网络身份标识信息 | 网络身份标识信息 | 可直接标识网络或通信用户身份的信息及账户相关资料信息（金融账户除外），如用户账号、用户ID、即时通信账号、网络社交用户账号、用户头像、昵称、个性签名、IP地址、账户开立时间等。 | 一级 |
| 个人健康生理信息 | 健康状况信息 | 与个人身体健康状况相关的一般信息，如体重、身高、体温、肺活量、血压、血型等。 | 一级 |
| 个人医疗信息 | 个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、体检报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、既往病史、诊治情况、家族病史、现病史、传染病史、吸烟史等。 | 二级 |
| 个人教育工作信息 | 个人教育信息 | 个人受教育和培训情况相关信息，如学历、学位、教育经历（入学日期、毕业日期、学校、院系、专业等）、成绩单、资质证书、培训记录、奖惩信息、受资助信息等。 | 一级 |
| 个人工作信息 | 个人求职和工作情况相关信息，如个人职业、职位、职称、工作单位、工作地点、工作经历、工资、工作表现、简历等。 | 一级 |
| 个人财产信息 | 金融账户信息 | 金融账户及账户相关信息，如银行卡号、支付账号、银行卡磁道数据（或芯片等效信息）、证券账户、基金账户、保险账户、公积金账户、公积金联名账号、账户余额、支付标记信息等。 | 二级 |
| 个人交易信息 | 交易过程中产生的交易信息和消费记录，如交易订单、交易金额、支付记录、透支记录、交易状态、交易日志、交易凭证、账单，证券委托、成交、持仓信息，保单信息、理赔信息等。 | 二级 |
| 个人资产信息 | 个人实体和虚拟财产信息，如个人收入状况、房产信息、存款信息、车辆信息、纳税额、公积金缴存明细（含余额、基数、缴纳公司、公积金中心、状态等）、银行流水、虚拟财产（含虚拟货币、虚拟交易、游戏类兑换码等）、个人社保与医保存缴金额等。 | 二级 |
| 个人借贷信息 | 个人在借贷过程中产生的信息，如个人借款信息、还款信息、欠款信息、信贷记录、征信信息、担保情况等。 | 二级 |
| 身份鉴别信息 | 身份鉴别信息 | 用于身份鉴别的数据，如账户登录密码、银行卡密码、支付密码、账户查询密码、交易密码、银行卡有效期、银行卡片验证码（CVN和CVN2）、USBKEY、动态口令、U盾（网银、手机银行密保工具信息）、短信验证码、密码提示问题答案、手机客服密码、个人数字证书、随机令牌等。 | 二级 |
| 个人通信信息 | 个人通信信息 | 通信记录，短信、彩信、话音、电子邮件、即时通信等通信内容（如文字、图片、音频、视频、文件等），及描述个人通信的元数据（如通话时长）等。 | 二级 |
| 联系人信息 | 联系人信息 | 描述个人与关联方关系的信息，如通讯录、好友列表、群列表、电子邮件地址列表、家庭关系、工作关系、社交关系等。 | 二级 |
| 个人上网记录 | 个人操作记录 | 个人在业务服务过程中的操作记录和行为数据，包括网页浏览记录、软件使用记录、点击记录、Cookie、发布的社交信息、收藏列表、搜索记录、服务使用时间、下载记录、访问时间（含登录时间、退出时间）等。 | 一级 |
| 业务行为数据 | 用户使用某业务的行为记录（如游戏业务：用户游戏登录时间、最近充值时间、累计充值额度、用户通关记录）等。 | 一级 |
| 个人设备信息 | 可变更的唯一设备识别码 | AndroidID、IDFA、IDFV、OAID等。 | 一级 |
| 不可变更的唯一设备识别码 | IMEI、IMSI、MEID、设备MAC地址、硬件序列号、ICCID等。 | 一级 |
| 应用软件列表 | 终端上安装的应用程序列表，如每款应用软件的名称、版本等。 | 一级 |
| 个人位置信息 | 粗略位置信息 | 仅能定位到行政区、县级等的位置信息，如地区代码、城市代码等。 | 一级 |
| 精确位置信息 | 能具体定位到个人的地理位置数据，包括经纬度、住宿信息、小区代码、基站号、基站经纬度坐标等。 | 二级 |
| 个人出行信息 | 乘坐飞机、火车、汽车、轮船等交通信息，行踪轨迹等。 | 二级 |
| 个人标签信息 | 个人标签信息 | 基于个人上网记录等各类个人信息加工产生的用于对个人用户分类分析的描述信息，如App偏好、关系标签、终端偏好、内容偏好等标签信息。 | 一级 |
| 个人运动信息 | 个人运动信息 | 步数、步频、运动时长、运动距离、运动方式、运动心率等。 | 一级 |
| 未成年信息 | 不满十四岁未成年个人信息 | 不满十四岁未成年个人信息。 | 二级 |
| 其他个人信息 | 其他个人信息 | 性取向、婚史、宗教信仰、未公开的违法犯罪记录等。 | 二级 |
| 1. 个人画像，是由多个用户个人标签组成的数据集。
 |

参考文献

[1] GB/T 35273-2020 信息安全技术个人信息安全规范

[2] GB/T 37964-2019 信息安全技术个人信息去标识化指南

[3] GB/T 37973-2019 信息安全技术大数据安全管理指南

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

[5] GB/T 43697-2024 数据安全技术数据分类分级规则

[6]《网络数据安全管理条例》（中华人民共和国国务院令 第790号）

[7]《湖南省政务信息资源共享管理办法》（湖南省人民政府令第301号）

