ICS
CCS

团　　体　　标　　准

T/XXXX XX—2024

信息安全管理 数据分类分级指南

Information security management- Guidelines for data classification and grading

（征求意见稿）

2024－XX－XX 发布　　2024－XX－XX 实施

山东数据交易流通协会　　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。

通过建立科学、有效、一致的数据分类标准，梳理数据资产目录，有利于数据管理运营人员掌握数据资产分布、状态、数据价值，有利于业务人员进行细粒度的数据查找、使用、加工和业务分析。基于数据分级形成数据安全管理准则，为数据全生命周期管理的安全策略制定提供支撑，指导构建分级数据安全防护体系。充分发挥数据作为新型生产要素的驱动作用，保障数据有序自由流动，促进数据开放共享，加强数据在国家治理、经济运行、社会生活等方面有效利用。

本文件由山东数据交易流通协会提出并归口。

本文件起草单位：

本文件主要起草人：

信息安全管理 数据分类分级指南

1 范围

本文件适用于企业数据的分类分级原则、方法，和数据分级保护工作，适用对象为有一定数据量、有数据分类分级要求的企业。

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。

《中华人民共和国个人信息保护法》
GB/T 4754-2017 国民经济行业分类
GB/T 10113-2003 分类与编码通用术语
GB/T 25069-2022 信息安全技术 术语
GB/T 35295-2017 信息技术 大数据 术语
GB/T 38667-2020 信息技术 大数据 数据分类指南
GB/T 35273-2020 信息安全技术 个人信息安全规范
JR/T 0197—2020 金融数据安全 数据安全分级指南

3 术语和定义

《中华人民共和国个人信息保护法》、GB/T 10113-2003、GB/T 25069-2022、GB/T 35295-2017、GB/T 35273-2020界定的以及下列术语和定义适用于本文件。

3.1

个人信息 personal information

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。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

[来源：《中华人民共和国个人信息保护法》]

3.2

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，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

[来源：《中华人民共和国个人信息保护法》]

3.3

组织数据 organizing data

组织在自身的业务生产、经营管理和信息系统运维过程中收集和产生的数据。

[来源：TC260-PG-20212A，2.8]

3.4

商业秘密 trade secret

不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。

[来源：TC260-PG-20212A，2.10]

3.5

核心数据 core data

即国家核心数据，是指关系国家安全、国民经济命脉、重要民生、重大公共利益等的数据。

[来源：TC260-PG-20212A，2.3]

3.6

重要数据 important data

一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。

[来源：TC260-PG-20212A，2.2]

3.7

一般数据 general data

一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人、组织合法权益造成危害，但不会危害国家安全、公共利益的数据。

[来源：TC260-PG-20212A，2.4]

3.8

衍生数据 derived data

原始数据经过统计、关联、挖掘或聚合等加工活动而产生的数据。

[来源：TC260-PG-20212A，2.9]

——衍生的数据有原始形态和非原始形态两种，原始形态是基于对源数据进行简单汇总或关联而展现的形态，非原始形态是基于对源数据进行计算、挖掘、聚合、分析、脱敏等方式而展现的形态。

3.9

类别 category

具有共同属性（或特征）的数据集合。

[来源：GB/T 38667-2020，3.9]

3.10

分类 classification

按照选定的属性（或特征）区分分类对象，将具有某种共同属性（或特征）的分类对象集合在一起的过程。

[来源：GB/T 10113-2003，2.1.2]

3.11

分类维度 categorical dimension

用于实现的分类数据所具有的某个或某些共同特征。

[来源：GB/T 38667-2020，3.6]

3.12

线分类法 method of linear classification

按选定的若干属性（或特征），逐次地分为若干层级，每个层级又分为若干类目。同一分支的同层及类目之间构成并列关系，不同层级类目之间构成隶属关系。

[来源：GB/T 10113-2003，2.1.5]

——线分类法适用于针对一个类别只选取单一分类维度进行分类的场景。

3.13

面分类法 method of area classification

选定的分类对象的若干属性（或特征），将分类对象按每一属性（或特征）划分成一组独立的类目，每一组类目构成一个“面”。再按照一定的顺序将各个“面”平行排列。使用时根据需要将有关“面”中的相应类目按“面”的指定排列顺序组配再一起，形成一个新的复合类目。

[来源：GB/T 10113-2003，2.1.6]

——面分类法是并行化分类方式，同一层级可有多个分类维度。面分类法适用于对一个类别同时选取多个分类维度进行分类的场景。

3.14

上位类 category in higher level

在线分类法体系中，一个类目相对于由它直接划分出来下一级类目而言，称为上位类。

[来源：GB/T 10113-2003，2.1.8]

3.15

下位类 category in lower level

在线分类法体系中，由上位类直接划分出来的下一级类目。

[来源：GB/T 10113-2003，2.1.9]

4 信息安全管理分类原则

4.1 稳定性原则

选择数据最稳定的本质特性作为分类的基础和依据，以保障分类设置在相当长一个时期内是稳定的。

4.2 可执行性原则

对数据进行简单清晰的分类规划，保障数据分类使用和执行的可行性。

4.3 分类多维原则

数据分类具有多种视角和维度。

4.4 动态调整原则

数据分类因时间变化、政策变化、安全事件发生、不同业务场景的敏感性变化或相关行业规则不同而发生改变，需对数据分类进行定期审核并及时调整。

5 信息安全管理分级原则

5.1 安全性原则

从利于数据安全管控的角度对数据进行分级。

5.2 时效性原则

数据分级随时间变化按照一些预定的安全策略发生改变，具有一定的有效期。

5.3 自主性原则

数据的分级根据自身的数据管理需要，按照数据分级方法自主确定更多的的数据层级。

5.4 合理性原则

数据级别要求具有合理性，合理分配数据到不同级别中。

5.5 客观性原则

数据的分级规则是客观并可以被校验的，已经分级的数据可以复核和检查。

5.6 就高不就低原则

不同级别的数据被同时处理、应用时，按照其中级别最高的要求来实施保护。

5.7 关联叠加效应原则

在非敏感数据关联后产生敏感数据的场景中，关联后的数据级别高于原始数据级别。

6 数据分类

6.1 分类维度

6.1.1　个人信息维度

基于数据识别自然人或与自然人关联划分类别，即数据可分为个人信息和非个人信息。

6.1.2　组织对象维度

基于数据资产描述对象划分类别，可划分为个人、组织、客体等资产对象数据。

——个人：指自然人个体，包括属性数据和行为数据；

——组织：指政府部门、企事业单位、其他正规团体，包括属性数据和业务数据；

——客体：指非个人或组织的客观实体，如道路、建筑、视频捕捉设备等，包括属性数据和感应数据。

——其他：指除个人、组织、客体外的其他数据对象，如视频数据、感知数据、审批事项、公共服务事项等。

6.1.3　组织经营维度

在遵循国家和行业数据分类分级要求的基础上，个人或组织用户的数据单独划分，其他数据基于业务生产和经营管理角度划分类别。

6.1.4　共享和开放维度

6.1.4.1　共享属性

基于数据共享属性进行划分类别，可划分为无条件共享、有条件共享和不予共享 3 个分类类别。

6.1.4.2　开放属性

基于数据开放属性进行划分类别，可划分为无条件开放、有条件开放和不予开放 3 个分类类别。

6.1.5　数据对象维度

除上述分类维度之外，还可基于数据产生频率、数据产生方式、数据结构化特征、数据存储方式、数据质量要求、数据使用频率划分类别。

6.2　分类方法

在上述维度的基础上，主要聚焦并采用线分类法，将数据从上到下按层次依序分类。

6.3　分类流程

6.3.1　分类准备

调研数据现状，对数据来源、存储位置、数据量大小、数据质量、数据类型、时效性以及数据权属等方面调查研究。

6.3.2　分类判定

数据分类按照实际业务情况，选择维度输出数据分类表。

6.3.3　分类审批

审核数据分类的对象、维度，检查数据分类表。

6.3.4　分类实施

结合数据的实际管理情况，按照数据分类表对数据进行分类。

6.3.5　结果核查

核查验证分类结果，包括但不限于分类方法、数据分类表、分类过程记录和分类实施结果。

6.3.6　分类成果应用

选取合适的业务场景，应用数据分类成果。

6.3.7　维护与改进

根据数据分类应用成效制定变更计划，评估变更对数据分类工作的影响。定期评估数据分类维度和方法的合理性、数据分类结果的有效性和应用情况。

7　数据分级

7.1　分级注意事项

a）基于数据完全泄露或损坏考虑数据泄露或损坏影响。

b）《中国人民共和国网络安全法》已明确要对个人信息保护，业务相关的个人信息要在数据分级中分配高等级。

c）安全属性（完整性、保密性、可用性）是信息安全风险评估中的重要参考属性，数据安全属性遭到破坏后可能造成的影响是确定数据级别的重要判断依据。

d）分级的数据对象只针对一般数据，国家法律法规定义的重要数据及核心数据均按照颁布的法律法规进行执行。

7.2 分级规则

7.2.1 级别定义

数据分级根据数据安全性遭受破坏后（如：篡改、损毁、泄露或者非法获取、非法利用等），其影响对象及影响程度，将数据从高到低分为核心（5级）、重要（4级）、敏感（3级）、一般（2级）和公开（1级）五个安全级别，各个级别数据特征如下：

a）核心数据（5 级）：数据安全性遭到破坏后，对国家安全、重要民生和重大公共利益造成影响，或对公众权益造成严重影响。5 级作为预备等级，暂不使用，未来将按照国家要求规划启用。

b）重要数据（4 级）：数据安全性遭到破坏后，对公众权益造成一般影响，或对个人隐私或企业合法权益造成严重影响，但对国家安全、重要民生和重大公共利益无影响，例如个人身份鉴别信息、核心业务数据等。

c）敏感数据（3 级）：数据的安全性遭到破坏后，对公众权益造成轻微影响，或对个人隐私或企业合法权益造成一般影响，对国家安全、重要民生和重大公共利益无影响，例如客户敏感数据、业务敏感数据等。

d）一般数据（2 级）：数据的安全性遭到破坏后，对个人隐私或企业合法权益造成轻微影响，对国家安全、重要民生和重大公共利益、公众权益无影响，例如客户一般数据、业务一般数据等。

e）公开数据（1 级）：数据的安全性遭到破坏后，可能对个人隐私或企业合法权益不构成影响或仅造成微弱影响，对国家安全、重要民生和重大公共利益、公众权益无影响，例如对外公开数据等。

7.2.2 多影响对象的数据级别定义

涉及国家安全、公众利益、组织、自然人中的两类及以上时，级别为其影响对象类别中的最高级。

7.2.3 数据的保护级别

本文件中核心数据的数据保护级别不低于四级，重要数据的数据保护级别不低于三级，一般数据的数据保护级别可为一级或二级。

特定类型一般数据的最低参考级别包括：

a）敏感个人信息不低于三级，一般个人信息不低于二级；

b）组织内部员工个人信息不低于二级；

c）有条件开放/共享的公共数据级别不低于二级，禁止开放/共享的公共数据不低于四级。

7.2.4 衍生数据的定级

按照数据加工程度的不同，数据通常可分为原始数据、脱敏数据、标签数据、统计数据，其中脱敏数据、标签数据、统计数据均属于衍生数据。

衍生数据定级遵从就高从严原则，对照原始数据级别进行定级，按照数据加工程度进行升级或降级调整，包括但不限于：

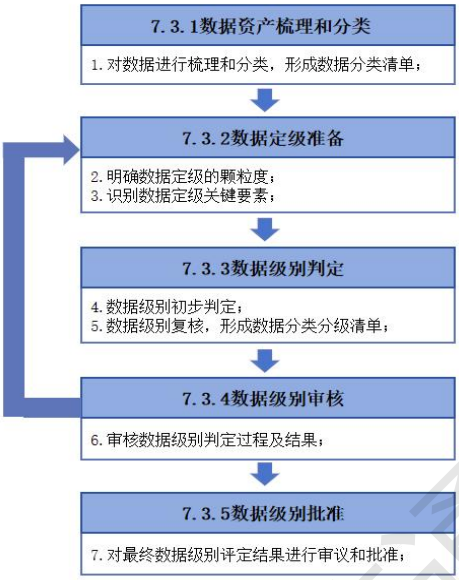
a）脱敏数据级别原则上比原始数据级别低，去标识化的个人信息不低于二级，匿名化的个人信息不低于一级。

b）标签数据级别原则上比原始数据集级别低，个人标签信息不低于二级。

c）统计数据如涉及大规模群体特征或行动轨迹，级别高于原始数据。

7.3 分级流程

数据分类分级过程包括数据资产梳理和分类、数据定级准备、数据级别判定、数据级别审核及数据级别批准。具体工作流程如下图所示。



7.3.1　数据资产梳理和分类

1.对数据进行盘点、梳理、分类，形成多层级的数据分类清单。

7.3.2　数据定级准备

2.明确数据定级的颗粒度。

3.识别数据定级关键要素。

7.3.3　数据级别判定

4.对最低层级子类的数据安全等级进行初步判定。

5.综合考虑数据规模、数据时效性、数据形态等因素，对数据安全级别进行复核，调整并形成数据安全级别评定结果及定级清单。

7.3.4　数据级别审核

6.审核数据安全级别评定过程和结果，必要时重复第二步及其后工作，直至安全级别的划定与数据安全保护目标一致。

7.3.5　数据级别批准

7.对数据安全分级结果进行审议批准。

8　数据分类分级变更

8.1　数据变更概述

数据分类分级变更场景包括但不限于：

a）数据时效性变更，如已明确公开时间或废止时间的数据。

b）数据原始用途或所在系统发生改变。

c）因业务调整获取的外部数据。

d）聚合后的数据较原始数据获得的更多的敏感信息。

e）法律法规对数据分类分级的要求发生变更。

f）其它可能影响数据分类分级结果的情况。

8.2　数据级别变更流程

数据发生变更时，由产生数据的业务部门重新进行分类分级，经业务开发小组及数据安全相关小组确认后生效。

8.3　数据聚合与数据分类分级的变更

数据在流转、传递、使用过程中，由于各类业务需要，会出现将相同或不同级别数据集成进行分析、处理的场景。在数据聚合时，需注意：

a）因业务需要，将来自不同途径或不同系统的数据集成，数据的原始用途或所在系统发生改变，需要对数据重新进行分类分级。

b）重新定级时，深入分析数据集成后较原始数据获得额外信息的程度，评估集成后的数据安全遭到破坏后的影响。

c）集成后的数据级别一般不低于原始数据的最高级别。

8.4 数据时效性与数据分类分级的变更

数据在流转、传递、使用过程中，为利于数据的公开、共享和应用，会出现在特定的时间对数据的级别调整的情况。针对数据时效性的处理，需注意：

a）数据时效性是最初数据分类分级判定因素之一。

c）同一类数据级别在某时间点前后发生变化，需说明时间点前后的级别及触发变化的条件。

d）准确标识发生变更后数据时效性要素和类别、级别，通知相关人员知悉。

8.5 数据的获取与提供

因业务需要，从外部机构获取数据或将企业内部数据提供给相关方，需注意：

a）数据提供方明确数据的级别和安全保护要求，并告知数据接收方。

b）数据提供方说明数据级别是否参照本文件确定，如未参照本文件的方法确定，说明数据分级的方法。

c）对于从外部获取的数据进行集成，按照 8.3 节列出的情形进行处理。

8.6 数据的逻辑加工

因业务需要进行逻辑加工产生的数据，需注意：

a）逻辑加工产生的数据要重新分级。

b）对于逻辑加工产生的数据，如已采用匿名化技术处理个人信息，处理后的数据可以等于或低于原始数据级别，如采用去标识化的手段处理数据，处理后的数据不能低于原始数据级别。

附录 A　数据分类参考示例

交通领域某公司数据的分类分级规则参考如表 A1 所示，实际应用过程中，按照数据的类型、 特性等因素，综合考虑该公司的数据安全管理的总体目标和安全策略要求，按照一定的颗 粒度对数据资产进行梳理、归类和细分，并最终确定数据分类分级清单。此外，重要数据的识别、认定及保护工作依据国家及行业主管部门有关规定和要求执行。

表 A1 交通领域某公司数据分类分级规则参考表

一层分类	二层分类	三层分类	四层分类	分类描述	最低安全级别参考
客户	个人	个人基本信息	个人自然信息	包括个人姓名、生日、性别、年龄、民族、国籍、身份证号等。	3
			个人附带信息	包括基于个人基本属性信息构建的用于 刻画个人的附带数据，如电话号码、银行卡号、邮箱地址、征信、房贷、学历、（APP用户名）、行驶证等。	3
			个人位置信息	包括住址、行踪轨迹、精准定位信息、 住宿信息、航班信息、经纬度、行政区划等。	3
		个人关系信息	关系信息	指用于描述个人与个人关联方关系的记录数据，如家庭关系、子女、父母、 兄弟姐妹、配偶、社交关系、（工作单位、工作单位信息）等。	2
		个人身份鉴别信息	身份鉴别信息	指用于身份鉴别的弱隐私个人生物特征 样本数据与特征值数据，如人脸、身份证照片、声纹、步态、耳纹、眼纹、笔迹等。	4
		个人行为信息	行为信息	指发生业务关系时的行为数据，如描述 客户通过网上营业厅、APP、邮件、短信、社交网络、辅助渠道等咨询、购买或使用产品或服务时产生的如拜访时间 （含登录时间、访问时间）、地点、网页浏览记录、APP浏览记录、个人驾驶习惯等。	2

	企业	企业基本信息	企业基本概况	指企业基础概况数据，如法定代表人姓名、法人身份证照片、企业名称、统一社会信用代码、经营许可证、经营范围、行业分类、经济类型、人员规模、 注册资本、企业地址等。	2
			企业股东信息	指主要出资人信息数据，如控股股东名称、持股比例、担保信息等。	2
			企业联系信息	指企业的联系方式信息数据，如联系电话、通信地址、行政区划等。	2
			企业财务信息	指企业财务信息数据，如营业收入、利润总额、资产状况、负债状况、（对公 账户）等。	2
		企业资讯信息	资讯信息	指企业在市场监管部门录入的可查询数据，如企业证照信息、注册日期、企业类型、股东及出资人信息、主要管理人员信息、企业对外投资等。	1
		企业行为信息	行为信息	指企业发生业务关系时的行为数据，如通过网上营业厅、APP、邮件、短信、社交网络、辅助渠道等咨询、购买或使用产品或服务时产生的如拜访时间（含登录时间、访问时间）、地点、网页浏 览记录、APP 浏览记录等。	2
	资产信息	车辆	车辆基本信息	指车辆的基本信息，如车辆品牌、车型、内外廓尺寸（长、宽、高）、车牌号、车辆识别代号、发动机号、车牌颜 色等。	3
ETC	业务	卡签（固定信息）	卡信息	指ETC卡的基本信息，如卡号、卡片类型、启用时间、到期时间等信息。	2
			OBU信息	指OBU设备的基本信息，如obu编号、 OBU 印刷号、OBU 品牌、启用时间、到期时间等信息。	2
			签约信息	指合同法规定的协议基本属性数据，如合同编号、合同名称、合同种类、合同状态、生效日期、到期日期、终止日期等信息。	2

		订单	**订单基本信息**	指ETC卡和OBU设备的订单信息，如、订单号、订单编号、订单时间、订单总金额、订单备注、失败订单等。	**2**
		状态	**卡状态**	指ETC卡的状态信息，如正常使用、待签约、待挂失等信息。	**2**
			OBU状态	指OBU设备的状态信息，如初始状态、已发行、已激活、已挂起、黑名单等信息。	**2**
			订单状态	指订单的状态信息，如提交成功、已取消、取消中、资料审核成功、审核失败、已激活等信息。	**2**
			签约状态	指签约的状态信息，如签约成功、待转黑名单、待解黑名单、待挂失、待解挂、解约中、已补换新卡等信息。	**2**
			车辆状态	指车辆的状态信息，如车辆拉黑、异常消费等数据。	**3**
		交易信息	**签约信息**	指动态签约动作信息，如签约四要素，姓名、手机号、银行卡号、子签约号、签约渠道等信息。	**3**
			交易基本信息	指交易基本数据，如交易流水号、交易日期、交易类型（含如储值、提现等， 以及账户查询、修改密码等）、交易渠道、交易来源、交易地点、请求日期、生效日期、终端号、代扣完成时间、扣款类型等。	**2**
			记账信息	指会计主体因交易发生的经济活动而进行事后核算记账的数据,如记账日期、 记账时间等。	**2**
			账单信息	指交易中产生的客户账单，如账单日、 账单金额、扣款金额、优惠金额、手续 费服务费、实际扣款金额、账单总金额、支付的车辆数量等数据。	**2**
		电子账户	**账户信息**	指账户的基本信息数据，如账户编号、 账户类型、账户状态、开户日期、销户日期、支付标记（作为支付账号等原始 交易要素的替代值，用于完成特定场景 支付交易）、代扣请求上送交易中心分 配的商户号ID、商户号、商户ID、用 户编号、客户编号等。	**2**
			属性信息	指账户上的金额信息、变更信息、储值信息等数据。	**2**
		贷款	**基本信息**	指贷款业务信息的基本属性信息数据，如贷款类型、贷款金额、放款金额等。	**3**

			逾期信息	指记账业务涉及逾期的相关数据信息，如逾期日期、逾期金额、逾期天数、欠账金额等。	**2**
			展期信息	指记账业务涉及展期的相关数据信息，如展期期限、展期金额、展期次数、展期原因等。	**2**
	经营	**产品**	**货车产品信息**	指用于货车产品管理的基础描述数据，如产品编号、产品类型、产品简介、适用客户类型、活动产品、产品码等。	**2**
			客车产品信息	指用于客车产品管理的基础描述数据，如产品编号、产品类型、产品简介、适用客户类型等。	**2**
		渠道	**客车代理**	指客车的代理渠道数据，如代理机构、联系方式等。	**3**
			货车代理	指货车的代理渠道数据，如代理机构、联系方式等。	**3**
			车险代理	指车险的代理渠道数据，如代理机构、联系方式等。	**3**
		推广	**行为数据**	指营销推广分析时的融合的行为数据，如个人行为数据和企业行为信息的分析数据等。	**2**
			标签数据	指营销推广分析时的融合的标签数据，如个人附带数据和企业咨询信息的分析数据等。	**2**
			客户端基础数据	指营销推广的基建数据，如APP、小程序、公众号、其他等信息。	**2**
	监管信息	**数据报送**	**监管指标上报信息**	指机构按要求上报的监管指标数据、业务统计指标等。	**1**
			监管明细数据上报信息	指机构按要求上报的各类监管明细 数据，如监管标准化数据、清单级 业务数据等。	**2**
			统计信息	指机构计算的宏观统计相关数据，如调查问卷及其他重要事项等。	**1**
综合	**综合管理**	**机构信息**	**基本信息【公开】**	指机构组织架构中，其内设部门、分支机构等已公开的基础概况记录 数据，如机构编号、机构名称、机 构地址、机构电话等。	**1**

			基本信息【非公开】	指机构组织架构中，其内设部门、 分支机构等未直接公开的基础概况 记录数据，如部门编号、部门名称、部门职责、上级账务机构编号、收费站等。	**2**
			内部层级信息	指机构组织架构中，其内设部门、分支机构等的层级划分标识数据，如总公司、分公司、子公司、所属大区等。	**2**
			分类信息	指机构组织架构中，其内设部门、分支机构等按不同管理要求维度进行分类的标识数据，如网点等。	**2**
		人员信息	**基本信息**	指机构内部的人员信息，如职称、花名、简介、联系方式等信息、操作员工号。	**3**
			权限信息	指机构内部人员的权限信息，如岗位、职责、分工、授权等信息。	**3**
技术管理	**项目**	**项目基本信息**	**基本信息**	指项目基本信息，如项目名称、项目编号、交易场景等。	**2**
		项目管理信息	**规划信息**	指信息化项目、信息系统的规划文档等数据。	**3**
			质量管理信息	指信息科技管理文档、制度文档、质量管控文档等数据。	**2**
			开发信息	指信息系统设计方案、源代码等数据。	**3**
			测试信息	指测试方案、测试计划、测试报告等数据。	**2**
	系统	**系统基本信息**	**基本信息**	指系统基本信息，如系统名称，规格配置，版本型号，最新更新日期等	**2**
		系统管理信息	**配置信息**	指与信息系统配置相关的数据，包括关键配置参数、存放路径、重要参数等。	**2**

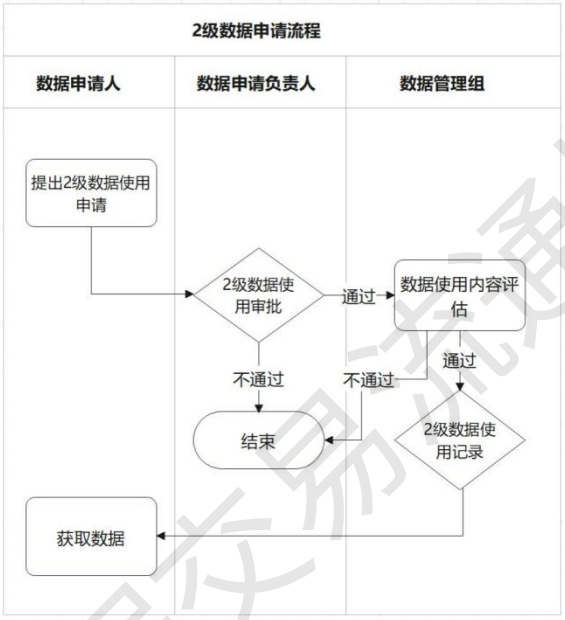
			信息资产管理信息	指与信息资产相关的数据，包括资产类型信息、资产价值信息、资产折旧信息、资产生命周期信息、拓扑关系信息、系统网络安全等级清单、（终端IP，调用支付API的机器IP）等。	**2**
			数据字典信息	指各个信息系统中的数据字典，如数据符号、数据示意、说明解释等。	**2**
			安全管理信息	指信息系统漏洞信息、安全防护配置与策略信息、自行识别的威胁数据、安全告警信息、安全事件信息等数据。	**2**
			运行日志信息	指各个系统、应用、网络、机房设施、监控平台中记录的日志数据，如记录时间、记录日期、记录内容、告警类型、告警等级、诊断信息、报文等数据。	**2**
			系统运维信息	指用于系统维护或统计数据产生的 shell 脚本、SQL 脚本等。	**3**
		系统资源信息	**IT系统资源**	指用于系统日常运行的系统资源、客户端IP地址等。	**2**
			云资源	指用于系统建设的云端资源信息等。	**2**

附录 B　数据分类分级结果应用参考示例

交通领域某公司数据分类分级结果应用参考如下所示，实际应用过程中，按照数据级别分别设置不同审批机制，明确各级数据的可公开对象，切实保障数据的安全。

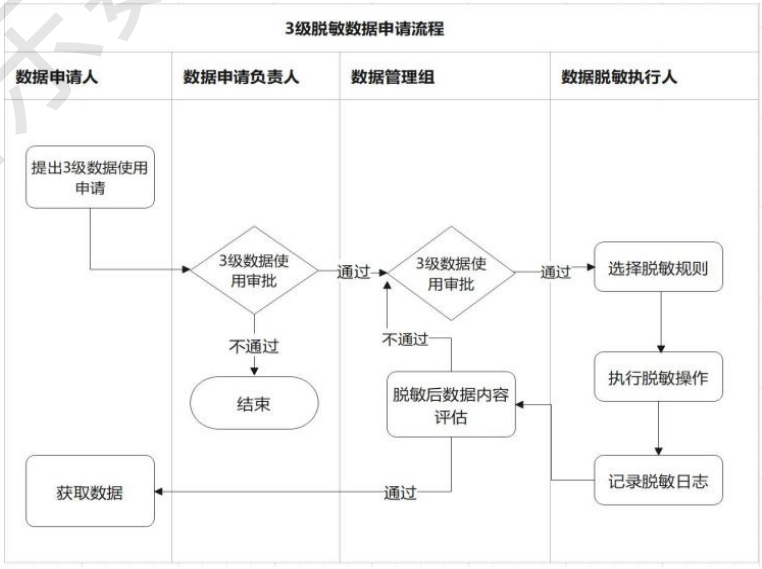
a）公开（1 级）数据可被公开或可被公众获知、使用。

b）一般（2 级）数据根据业务先行原则用于本单位一般业务使用，一般针对受限对象公开，通常作为内部管理，不进行广泛公开，审批过程见 2 级审批流程图。



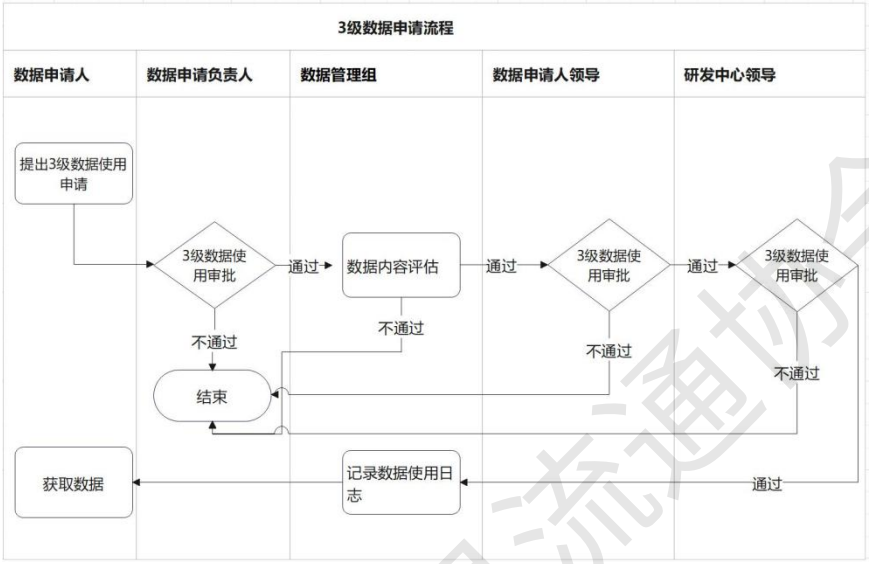
2 级审批流流程图

c）敏感（3 级）数据用于本单位关键或重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。敏感数据管理由数据管理部门确定，在数据访问、加工、下载等操作前应经审批后脱敏使用，审批过程见 3 级内部审批流程图。



3 级内部审批流流程图

d）敏感（3 级）数据发生共享时，严格执行数据脱敏。若因业务确需，无法对数据进行脱敏的，应对共享内容经过对应数据业务管理部门审批，选用安全可靠的传输协议或在安全可控的环境中进行共享，审批过程见 3 级共享审批流程图。



3 级共享审批流程图

e）重要（4 级）数据及核心（5 级）数据通常主要用于企业重要业务使用，仅针对必须知悉的特定人员公开，除此以外不得用于查询、引用、分析、共享及下载等操作。

参 考 文 献

[1] 《中华人民共和国数据安全法》
[2] 《中华人民共和国个人信息保护法》
[3] GB/T 4754—2017 国民经济行业分类
[4] GB/T 35273—2020 信息安全技术 个人信息安全规范
[5] GB/T 37973—2019 信息安全技术 大数据安全管理指南
[6] GB/T 38667—2020 信息技术 大数据 数据分类指南
[7] TC260-PG-20212A 网络安全标准实践指南 网络数据分类分级指引
[8] 信息安全技术 重要数据识别指南（征求意见稿）
[9] JR/T 0158—2018 证券期货业数据分类分级指引
[10] JR/T 0171—2020 个人金融信息保护技术规范
[11] JR/T 0197—2020 金融数据安全 数据安全分级指南
[12] YD/T 3813—2020 基础电信企业数据分类分级方法
[13] YD/T 3867—2021 基础电信企业重要数据识别指南
[14] 网络安全标准实践指南 网络数据分类分级指引

山东数据交易流通协会团体标准
《信息安全管理 数据分类分级指南》编制说明

一、背景说明

数据安全是信息安全的一部分。近几年国家逐步加强对信息安全建设的要求，从《中华人民共和国数据安全法》（以下简称《数据安全法》）的出台，再到《中华人民共和国个人信息保护法》的实施，无疑对数据信息化建设提出了更高标准的要求。其中《数据安全法》明确提出了各单位要对数据进行分类分级保护。同时作为数据处理者，《数据安全法》也明确指出要求各单位建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，加强风险监测，定期进行数据安全性评估，保障信息安全。

《个人信息保护法》也对个人信息处理者提出了信息保护的义务：制定内部管理制度和操作规程；对个人信息实行分类管理；采取相应的加密、去标识化等安全技术措施；合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；制定并组织实施个人信息安全事件应急预案；处理个人信息前要进行个人信息保护影响评估等等要求。

同时国家质量监督检验检疫总局、国家标准化管理委员会发布了我国首个数据管理领域国家标准《数据管理能力成熟度模型》（简称 DCMM），其中包含八大能力域（数据战略、数据治理、数据架构、数据标准、数据质量、数据安全、数据应用、数据生存周期），数

据分类分级在数据安全能力域中被明确提出。

随着国家越来越重视数据安全问题、在数据安全层面立法、立规的不断推进，亟需通过分类分级进行安全实施，分类分级作为数据安全建设的第一步也是重要组成部分，对于数据安全的实施起着重要作用。目前数据分类分级还处于快速发展阶段，如何进行安全相关的数据分类分级没有规范化的流程，且多种维度的分类定义并没有明确，同时也未出现以影响程度为基准的分级规则文件。

因此，研制一项通用性强、科学全面的数据安全管理数据分类分级指南变得尤为重要，《信息安全管理 数据分类分级指南》编写组根据政策文件及相关文献研究，经过多次研讨，主要从术语定义、分类分级原则、数据分类、数据分级、数据分类分级变更方面进行撰述，该指南适用于有一定数据量、有数据分类分级要求的企业，尤其对于存储个人敏感数据的企业和事业单位有着一定指导性作用，为今后数据分类分级体系的构建奠定基础。

在此背景下，山东高速信联科技股份有限公司和山东数据交易流通协会对《信息安全管理 数据分类分级指南》团体标准进行了立项。

二、标准编制过程

（一）成立工作组。2023 年 7 月-2023 年 8 月，组织进行了大量的社会调研工作，对当前数据现状进行了调研分析。同时成立了《信息安全管理 数据分类分级指南》工作组，确定工作职责，并制定编写工作的进度计划。

（二）开展调研。2023 年 9 月，工作组成员广泛收集、查阅相

关的文献资料、规范和标准。认真研读了相关国家和行业规范标准、相关书籍、技术文件，并系统梳理数据安全、数据分类分级相关材料。

（三）形成讨论稿。2023 年 10 月，在前期项目研究、文献资料分析、信息调研的基础上，结合标准编制规范要求，工作组召开多次会议，确立了标准结构，组织专门人员编写，形成《信息安全管理 数据分类分级指南》（讨论稿）。

（四）工作组集中工作。2023 年 11 月-12 月，工作组召开多次专家研讨会集中工作，对标准文本的框架、内容、格式等方面进行了全面讨论，形成《信息安全管理 数据分类分级指南》（征求意见稿），公开面向社会征求意见。

三、指南编制原则

（一）科学性

本指南的制定充分遵照国内相关法律法规，标准主要内容科学合理，严格按照 GB/T 1.1-2020 的规定编写，且确保与国家标准、行业标准中的术语和定义保持一致。

（二）实用性

本文件编写的原则是实事求是，能够适用于大部分政府机构，企、事业单位，为政府机构，企、事业单位对信息安全分类分级的理解、解释和信息交流提供支撑，为后续各单位建设数据分类分级提供案例和指导性作用。

（三）适用性

《信息安全管理 数据分类分级指南》是在不违背现行相关技术

规定的前提下，查阅、收集和整理国内近年来出版的有关资料和文献的基础上，总结国内外众多数据分类分级方法、维度、流程，结合实际企业数据情况，制定了本指南。

四、指南主要内容

本指南根据数据安全管理活动进行分类分级操作的梳理，共分为范围、规范性引用文件、术语和定义、信息安全管理分类原则、信息安全管理分级原则、数据分类、数据分级、数据分类分级变更8个部分:

（一）范围

本文件适用于企业数据的分类分级原则、方法，和数据分级保护工作，适用对象为有一定数据量、有数据分类分级要求的企业。

（二）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。

《中华人民共和国个人信息保护法》

GB/T 4754-2017 国民经济行业分类

GB/T 10113-2003 分类与编码通用术语

GB/T 25069-2022 信息安全技术 术语

GB/T 35295-2017 信息技术 大数据 术语

GB/T 38667-2020 信息技术 大数据 数据分类指南

GB/T 35273-2020 信息安全技术 个人信息安全规范

JR/T 0197—2020 金融数据安全 数据安全分级指南

（三）基础术语

《中华人民共和国个人信息保护法》、GB/T 10113-2003、GB/T 25069-2022、GB/T 35295-2017、GB/T 35273-2020 界定的以及下列术语和定义适用于本文件。同时该章节包含了个人信息、敏感个人信息、组织数据、商业秘密、核心数据、重要数据、一般数据、衍生数据、类别、分类、分类维度、线分类法、面分类法、上位类、下位类的定义。

（四）信息安全管理分类原则

本章节定义了信息安全管理分类原则。工作组按照数据特征和分类应具有的特性，定义了稳定性原则、可执行性原则、分类多维原则、动态调整原则来保证分类建立的准确性。

（五）信息安全管理分级原则

本章节定义了信息安全管理分级原则。工作组依据数据安全相关标准和规则，定义了安全性原则、时效性原则、自主性原则、合理性原则、客观性原则、就高不就低原则、关联叠加效应原则来保证分级划分的科学合理性。

（六）数据分类

本章节定义了数据分类维度、分类方法及建设流程，其主要目的是便于数据管理和使用，从个人信息、组织对象、组织经营、共享开放、数据对象视角出发给出了多个维度的数据分类参考思路。同时按照分类准备、分类判定、分类审批、分类实施、结果核查、分类成果应用、维护与改进的建设流程实施数据分类。

（七）数据分级

本章节定义了数据分级规则、分级级别及相关分级操作流程，包括分级注意事项、分级规则、分级流程。根据其影响对象及影响程度，将数据从高到低分为核心（5 级）、重要（4 级）、敏感（3 级）、一般（2 级）和公开（1 级）五个安全级别。并且按照数据资产梳理和分类、数据定级准备、数据级别判定、数据级别审核、数据级别批准落地实施数据分级建设。

（八）数据分类分级变更

本章节定义了数据分类分级变更，包括数据变更概述、数据级别变更流程、数据聚合与数据分类分级的变更、数据时效性与数据分类分级变更、数据的获取与提供、数据的逻辑加工，考虑不同变更场景情况，规范数据分类分级变更，使变更更具标准化。

五、与有关的现行法律、法规和强制性国家标准的关系

本指南符合国家有关法律、法规、强制性标准及相关产业政策要求，与有关法律、法规和国家、行业标准相协调，没有矛盾。

六、重大分歧意见的处理经过和依据

本指南在制定过程中未出现重大分歧意见。

七、作为强制性标准或推荐性标准的建议

建议本指南为山东数据交易流通协会推荐性团体标准。

八、废止现行有关标准的建议

无其他现行标准的废止建议。

九、其他应予说明的事项

无。

标准工作组

2023 年 12 月 29 日