海南省政府大数据推进工作领导小组办公室

琼数组办〔2022〕1号

海南省政府大数据推进工作领导小组办公室关于印发《海南省政务数据分类分级指南（试行）》的通知

各市、县、自治县人民政府，省委各部门，省直各单位：

为深入贯彻落实《海南省大数据开发应用条例》《海南省公共信息资源管理办法》和《海南省公共信息资源安全使用管理办法》相关要求，进一步规范政务数据资源分类分级工作，我们制订《海南省政务数据分类分级指南（试行）》，现予印发，请遵照执行。

海南省政府大数据推进工作领导小组办公室

2022年1月27日

（此件主动公开；联系人：傅力圆，联系电话：15091991998）

海南省政务数据分类分级指南

（试行）

目录

引言

根据《海南省公共信息资源管理办法》（琼府〔2018〕39号）和《海南省公共信息资源安全使用管理办法》（琼府办〔2019〕18号）相关要求，对政务数据资源实施分类分级共享开放。本指南规定了政务数据分类分级的流程、要点、方法等内容，本省政务数据共享开放主体根据本指南对政务数据进行分类分级，并采取相应风险防控和安全保障措施，全面保障本省政务数据共享开放工作有力有序开展。

海南省政务数据分类分级指南
（试行）

第一章 目标

按照《中华人民共和国数据安全法》等相关要求，为加强我省数据资源整合和安全保护，制定数据隐私保护制度和安全审查制度，进一步制定完善适用于大数据环境下的数据分类分级安全保护制度，以加强对政务数据的安全保障，促进政务数据的安全开发利用。

第二章 范围

本指南适用于各级行政机关、事业单位、社会团体或者其他依法经授权、受委托的具有公共管理职能的组织（以下简称政务部门）数据分类分级管理。海南省水务、电力、燃气、通信、公共交通、民航、铁路等公用事业运营单位涉及公共属性数据共享开放，可参考本指南进行分类分级。

本指南提供通用、共性参考原则和方法，各数据共享开放主体根据本行业、本区域的法律法规和相关规定，对本指南进行调整、补充，并制定本机构政务数据共享开放分类分级细则。

涉及国家、省级和市级秘密的政务数据管理，按照相关保密法律、法规的规定执行，不纳入本指南规范定义。

第三章 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。

《中华人民共和国网络安全法》

《中华人民共和国数据安全法》

《中华人民共和国个人信息保护法》

GB/T7027-2002 信息分类和编码的基本原则与方法

GB/T10113-2003 分类与编码通用术语

GB/T21063.4-2007 政务信息资源目录体系

GB/T25069-2010 信息安全技术 术语

GB/Z28828-2012 信息安全技术 公共及商用服务信息系统个人信息保护指南

GB/T35295-2017 信息技术 大数据 术语

GB/T37988-2019 信息安全技术数据安全能力成熟度模型

GB/T35273-2020 信息安全技术 个人信息安全规范

GB/T38667-2020 信息技术 大数据 数据分类指南

发改高技〔2017〕 政务信息资源目录编制指南（试行）1272 号

国务院办公厅秘书局 政务服务事项数据目录编制规范相关要求-2021

《海南省大数据开发应用条例》

《海南省公共信息资源管理办法》（琼府〔2018〕39号）

《海南省公共信息资源安全使用管理办法》（琼府办〔2019〕18号）

第四章 术语和定义

4.1. 省政务信息资源管理机构

省政务信息资源管理机构特指省大数据管理局。

4.2. 政务数据

政务数据是指各级行政机关、事业单位、社会团体或者其他依法经授权、受委托的具有公共管理职能的组织（政务部门），在履行职责过程中产生或者获取的具有原始性、可机器读取、可供社会化再利用的各类数据。

4.3. 数据分类

按照政务数据具有的某种共同属性或特征（包括数据对象、重要程度、共享属性、开放属性、应用场景等），采用一定的原则和方法进行区分和归类，以便管理和使用政务数据。

4.4. 数据分级

按照政务数据遭到破坏（包括攻击、泄露、篡改、非法使用等）后对国家安全、社会秩序、公共利益以及个人、法人和其他组织的合法权益（受侵害客体）的危害程度对政务数据进行定级，为数据全生命周期管理的安全策略制定提供

支撑。

4.5. 分类维度

用于实现数据分类的某个或某些共同特征。

4.6. 分级维度

用于实现数据分级的某个或某些共同特征。

4.7. 数据脱敏

通过一系列数据处理方法对原始数据进行处理以屏蔽敏感信息的一种数据保护方法。

4.8. 数据安全

指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

4.9. 数据处理

包括数据的收集、存储、使用、加工、传输、提供、公开等。

第五章 总体要求

5.1. 数据范围

本省各级政务部门在依法履行职责过程中获得的各类政务数据资源。

5.2. 组织保障

建立政务数据分类分级组织保障体系，明确组织领导、业务管理、数据安全管理等相关部门的职责和人员岗位角色要求。

5.3. 管理流程

建立政务数据分类分级制度保障，明确分类分级的原则、方法和要求，确立日常管理流程和操作规程，制定考核评价等机制。

5.4. 技术要求

使用技术手段实现政务数据安全分类分级的人工/自动属性标识，并人工/自动维护数据资产清单，定期对数据资产安全属性进行评审和修订。

第六章 数据分类

6.1. 分类原则

6.1.1. 兼容性

数据分类应遵循国家、地方、部门法律法规、相关标准的要求。

6.1.2. 科学性

分类时应该选择政务数据相对稳定的本质属性或者特征进行科学的分类，分类规则应相对稳定。

6.1.3. 系统性

在对政务数据分类时，应该遵循其本身存在的逻辑关系，每个类目占有唯一的位置，既要相互联系又要体现区别。

6.1.4. 规范性

所使用的词语或短语能确切表达数据类目的实际内容范围，内涵、外延清楚，保证用语简洁，在已有标准数据用

语的情况下，使用标准数据用语。

6.1.5. 实用性

政务数据分类要确保每个类目下要有数据，不设任何没有意义的类目，数据类目划分要符合用户对政务数据的普遍认识。

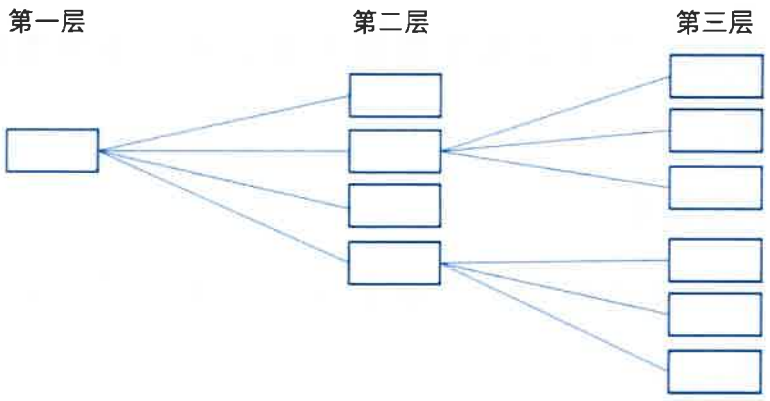
6.1.6. 可扩展性

同一层次类目的设置，应留有足够的发展余地，以便在增加新的类目时，不打乱原来建立的分类。

6.2. 分类方法

6.2.1. 线分类法

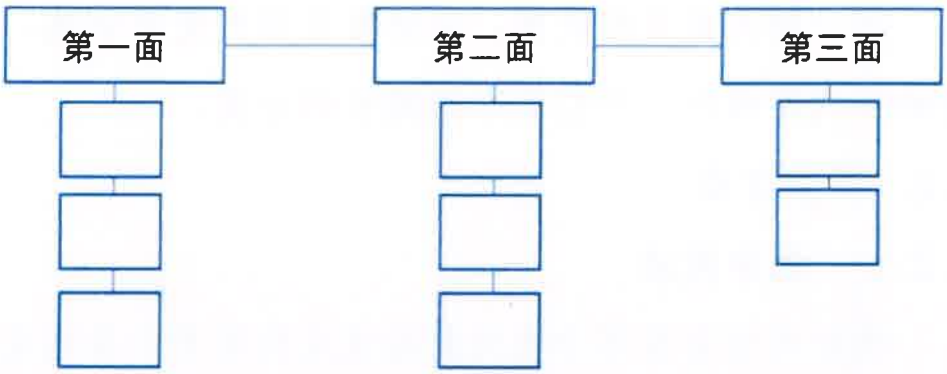
线分类法旨在将分类对象按选定的若干个属性或特征，逐次分为若干层级，每个层级又分为若干类别。同一分支的同层级类别之间构成并列关系，不同层级类别之间构成隶属关系。同层级类别互不重复，互不交叉。线分类法适用于针对一个类别只选取单一分类维度进行分类的场景。



6.2.2. 面分类法

面分类法是将所选定的分类对象，依据其本身的固有的

各种属性或特征，分成相互之间没有隶属关系即彼此独立的面，每个面中都包含了一组类别。将某个面中的一种类别和另外的一个或多个面的一种类别组合在一起，可以组成一个复合类别。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。



6.2.3. 混合分类法

混合分类法是将线分类法和面分类法组合使用，克服这两种基本方法的不足，得到更为合理的分类。混合分类法的特点是以其中一种分类方法为主，另一种做补充。混合分类法适用于以一个分类维度划分大类、另一个分类维度划分小类的场景。

6.3. 分类维度

数据分类维度分为数据管理、业务应用、安全保护、数据对象等。

6.3.1. 数据管理维度

6.3.1.1. 按数据产生方式分类

按照数据的产生方式（参照 GB/T 38667-2020 规定的按产生方式分类），将海南省政务数据分为：

a）依据数据被获取或被采集方式：人工采集数据、信息系统产生数据、感知设备产生数据。

b）依据数据被加工的程度：原始数据和二次加工数据等。

6.3.1.2. 按数据结构化特征分类

根据数据的结构化程度（参照 GB/T 38667-2020 规定的按结构化特征分类），将海南省政务数据分为：结构化数据和非结构化数据。

6.3.1.3. 按数据更新周期分类

按照数据更新的频率（参考国家电子政务办《政务数据目录编制规范》的更新周期分类），将海南省政务数据分为：实时、每日、每周、每月、每季度、每半年、每年、其他（“其他”由部门明确具体的更新周期，如每三年）等。

6.3.1.4. 按数据存储方式分类

根据政务数据储存方式，分为：关系型数据库存储数据、键值数据库存储数据、列式数据库存储数据、图数据库存储数据、文档数据库存储数据等。

6.3.1.5. 按数据质量分类

根据数据完整性、时效性、准确性等维度的质量要求对数据进行分类，分为：高质量数据、普通质量数据、低质量数据等。

6.3.2. 业务应用维度

6.3.2.1. 按所属领域分类

按照数据所属行业领域（参考国家电子政务办《政务数据目录编制规范》的所属领域），将海南省政务数据分为科技创新、商贸流通、社会救助、城建住房、教育文化、工业农业、机构团体、地理空间、资源能源、市场监管、生活服务、生态环境、交通运输、安全生产、社保、就业、医疗卫生、信用服务、公共安全、财税金融、气象服务、政府统计、医疗保障、法律服务等，以及应急响应、突发状况产生的数据。

6.3.2.2. 按共享属性分类

政务数据资源目录中的数据（依据国家电子政务办《政务数据目录编制规范》）按照共享属性分为无条件共享、有条件共享和不予共享。列入有条件共享和不予共享类政务数据范围的，应当说明理由，并提供有关法律、法规、规章依据。

a）可以提供给所有政务部门共享使用的，为无条件共享数据。

b）可以部分提供或者按照特定要求提供给相关政务部门共享使用的，为有条件共享数据。列入有条件共享数据的，数据提供单位应当明确共享条件。

c）不宜提供给政务部门共享使用的，为不予共享数据。列入不予共享数据的，应当有法律、行政法规或者国务院政策依据。

6.3.2.3. 按开放属性分类

按照《海南省大数据开发应用条例》，政务数据资源目录中的数据按照开放属性分为不予开放类、有条件开放类和无条件开放类三类。

a）不予开放类包括：开放后危及国家安全、公共安全、经济安全和社会稳定的；涉及商业秘密、个人隐私的；因数据获取协议或者知识产权保护等不予开放的；法律、法规规定不得开放的。

b）有条件开放类包括：涉及商业秘密、个人隐私，其指向的特定公民、法人或者其他组织同意开放，且法律、法规未禁止的；开放将严重挤占公共基础设施资源，影响政务数据处理效率的；开放安全风险难以评估的。

c）无条件开放类包括：除不予开放类与有条件开放类政务数据以外的其他政务数据。

6.3.3. 安全保护维度

按照安全隐私保护维度，从数据的重要程度等对政务数据资源目录中的数据进行安全保护维度分类，包括核心数据、重要数据和一般数据。

a）核心数据：对政务部门履行职能过程中获取的极其重要的政务数据资源；

b）重要数据：关键信息基础设施运营者在境内运营中收集、产生、控制的不涉及国家秘密，但与国家安全、经济发展、社会稳定，以及公共利益密切相关的政务数据资源。

关于重要数据的分类与范围参照国家和本省有关法律法规和标准执行；

c）一般数据：政务部门履行职能过程中产生的可存储的数据，不包含核心数据和重要数据。

6.3.4. 数据对象维度

对政务数据资源目录中的数据进行数据对象维度分类，包括个人、组织和客体。

a）个人：指自然人，包括属性数据和行为数据；

b）组织：指本省政府部门、企事业单位以及其他法人、非法人组织和团体，包括属性数据和业务数据；

c）客体：指本省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。

第七章 数据分级

7.1. 分级原则

7.1.1. 合理性原则

数据级别宜具有合理性，数据定级不宜过高或过低，级别划定过低可能导致数据不能得到有效保护；级别划定过高可能不利于利用，也可能导致不必要的业务开销。

7.1.2. 时效性原则

数据的分级具有一定的有效期，数据的级别可能因时间变化按照一些预定的安全策略发生改变。

7.1.3. 客观性原则

数据的分级规则是客观并可以被校验的，即通过数据自身的属性和分级规则就可以判定其分级。

7.1.4. 可执行性原则

数据级别划分应满足相关法律、法规及监管要求，避免对数据进行过于复杂的分级规划，保证数据分级使用和执行的可行性。

7.2. 分级维度

根据政务数据在国家安全、经济建设、社会生活中的重要程度，以及一旦遭受到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益侵害程度等因素，将政务数据划分为高敏感数据（4级）、低敏感数据（3级）、一般敏感数据（2级）、非敏感数据（1级）。数据级别与判断标准如表1所示：

表1 数据级别与判断标准

数据级别	级别标识	侵害程度
4级	高敏感	数据泄漏后会对个人人身安全、法人正常运作或国家机关正常运作造成严重损害
3级	低敏感	数据泄露后会对个人、法人、其他组织或国家机关正常运作造成损害
2级	一般敏感	数据泄露后无危害，仅对特定公众和群体有益，且可能对其他公众和群体产生不利影响

1级	非敏感	数据泄露后无危害

7.3. 分级要求

数据分级由实施分级和分级合规性审查两大环节。

7.3.1. 实施分级要求

a）数据安全分级由数源部门完成，并应细化到数据项级，法律、法规另有规定的除外。数据集的级别根据下属数据项的最高级来定级。

b）政务数据的分级结果将直接决定该政务数据的共享和开放要求、共享和开放的范围，以及共享和开放前的审批和管理要求等。

c）应加强个人信息和重要数据保护，按照就高从严原则确定安全等级，未提供明示共享依据的个人信息等级不得低于2级；法律法规明确保护的政务数据，数据安全等级应定为3级以上；没有任何安全属性标识的政务数据，默认为2级。

d）数据定级应充分考虑数据聚合情况、数据体量、数据时效性、数据脱敏处理等因素，可根据实际升高或降低数据安全级别。

7.3.2. 合规性审查

数源部门的数据分级结果应由省政务信息资源管理机构进行合规性审查。

7.4. 分级操作流程

7.4.1. 确定受侵害的客体

确定受侵害的客体时，首先判断是否侵害国家安全，然后判断是否侵害社会秩序或公共利益，最后判断是否侵害公民、法人和其他组织的合法权益。

侵害国家安全的事项包括①影响国家政权稳固和领土主权、海洋权益完整②影响国家统一、民族团结和社会稳定③影响国家社会主义市场经济和文化实力④其他影响国家安全的事项。

侵害社会秩序的事项包括①影响国家机关、企事业单位、社会团体的生产秩序、经营秩序、教学科研秩序、医疗卫生秩序②影响公共场所的活动秩序、公共交通秩序③影响人民群众生活秩序④其他影响社会秩序的事项。

侵害公共利益的事项包括①影响社会成员使用公共设施②影响社会成员获取公开数据资源③影响社会成员接受公共服务等方面④其他影响公共利益事项。

侵害公民、法人和其他组织的合法权益是指受法律保护的公民、法人和其他组织所享有的社会权利和利益等受到损害。

7.4.2. 综合判定侵害程度

侵害程度是客观方面的不同外在表现的综合体现，在针对不同的受侵害客体进行侵害程度的判断时，参照以下不同的判别基准：①如果受侵害客体是公民、法人或其他组织的合法权益，则以本人或本单位的总体利益作为判断侵害程度的基准②如果受侵害客体是社会秩序、公共利益或国家安

全，则以整个行业或国家的总体利益作为新侵害程度的基准。

7.4.3. 综合判定数据等级

根据政务数据被破坏时所侵害的客体以及相应客体的侵害程度，综合判定数据等级。

7.4.4. 确定共享开放策略

根据应用场景，结合数据级别，审核数据的被授权情况，评估数据申请使用主体的数据开发能力、安全保护能力及相关风险，确定政务数据共享开放策略。

7.4.5. 动态调整数据分级

根据应用场景及形势发展，动态调整政务数据分级、共享开放策略和安全管控措施。

7.5. 数据安全级别升降级

7.5.1. 数据升降级主要因素

a）从数据聚合考虑，聚合了多家业务部门的数据宜从高定级。

b）从数据体量来考虑，大量数据聚合宜升级。

c）从数据时效性考虑，历史数据可考虑降 1 级处理，但需明确历史数据的含义，并明确某时间点之前的数据。

d）在原始数据发生变化时需要重新进行级别判定，此时数据可能发生升级或降级。

e）已公开披露的数据可降低安全等级。

f）个人信息处理者处理敏感个人信息的，除个人信息

保护法第十七条第一款规定的事项外，还应当向个人告知处理敏感个人信息的必要性以及对个人权益的影响；依照本法规定可以不向个人告知的除外。脱敏数据宜单独定级。经有效脱敏后的数据，可降 1-2 级，但视情况处理。

g）处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

7.5.2. 数据聚合与数据级别变更

因业务需要，需要将相同或不同级别的数据汇聚在一起进行分析、处理时，数据级别变更应遵循以下原则：

a）聚合数据需经数据处理部门重新定级。

b）聚合数据安全级别一般不低于所汇聚的原始数据的最高级别。

c）需降低聚合数据安全等级的，应由省政务信息资源管理机构组织评估、协调后进行判定。

d）原则上不允许原始数据落地，仅允许获取数据分析、处理的结果。原始数据、临时数据使用应在中间存储环节有效清除。

7.5.3. 数据汇总、分析、加工与数据级别变更

因业务需要，对数据进行汇总、分析、加工后产生的数据，若与原始数据之间存在较大差异，宜对新产生的数据重新定级，定级的结果可能高于、等于、低于原始数据。

7.6. 不同等级数据开放和共享要求

7.6.1. 数据共享与数据级别

数据共享按分发范围分为部门内部共享和部门外部共享，按属性分为无条件共享、有条件共享和不予共享三类。因业务需要，从外部机构获取数据或将本机构数据提供给相关部门，应注意以下几点：

a）获取第 2 级及以上的行政相对人（法人、自然人）数据应有法律、法规、规章等规定或主体授权。没有法律法规依据或主体授权的数据，应受到严格的访问控制，严禁以任何形式共享。

b）数据共享应遵循履职需要、最小够用原则。

c）未进行安全属性标识的数据不得部门外部共享。

d）第 1 级数据应无条件共享，第 2 级以上数据部门外部共享应经过授权审批，第 3 级以上数据部门内部共享也需要经过部门内部审批。

e）不予共享类数据，必须有相应法律、法规和政策依据。

f）行政相对人对数据共享有特殊要求且合法合理的，应从其约定。

g）因依法履职需要使用非涉密共享数据，且有法律、法规、政策等依据或主体授权的，可直接获得授权使用共享数据。

7.6.2. 数据开放与数据级别

政务数据按开放属性分为无条件开放类、有条件开放类

和不予开放类三类。

a）一般而言，第 1 级数据可以直接对外开放，第 4 级数据严禁对外开放。

b）获取第 2 级以上的数据原则上应通过有条件开放方式获取。

c）通过有条件开放方式获取的数据不得用于申请之外的用途。

e）获取有条件开放类数据的用户应落实政务数据开放利用协议中约定的安全保障措施。

7.7. 数据定级与安全管控措施

与数据定级对应的安全管控措施参见表 2。

表 2　数据定级与相应安全管控措施

数据级别	数据采集	数据传输	数据存储	数据访问	部门内部共享	部门外部共享	数据开放	数据销毁
4级	数据采集设备应符合安全认证，且具备必要的传输加密和访问授权机制	加密传输，且传输环境应可信可控	分布式存储；必须保存在可信或可控的信息系统或物理环境中	需设置细颗粒度的身份标识与鉴别机制；建立访问控制矩阵，明确可访问用户和可访问内容；应宜采用口令、密码、生物识别等两种或两种以上组合的鉴别技术对用户进行身份鉴别	审批要求：根据单位内部数据管理要求确定	审批要求：数据共享开放主体审批和数源部门授权后有条件共享	审批要求：数据共享开放主体审批和信息主体授权后有条件开放	业务终止时需以不可逆的方式销毁有关数据或脱敏存储，有存档要求的从其规定
					技术要求：脱敏	技术要求：脱敏	技术要求：脱敏	
3级	数据采集设备应符合安全认证，采集环境安全，采集流程和方式符合相应要求	应在可信可控环境中传输；通过互联网和无线方式传输时应加密	分布式存储；应保存在可信或可控的信息系统或物理环境中。非可信或离线环境应进行加密存储	需设置粗颗粒度的身份标识与鉴别机制；应建立访问控制矩阵，明确可访问用户和可访问内容；宜采用口令、密码、生物识别等鉴别技术对用户进行身份鉴别	审批要求：根据单位内部数据管理要求确定。	审批要求：数据共享开放主体审批和数源部门授权后有条件共享。	审批要求：数据共享开放主体审批和信息主体授权后有条件开放。	业务终止时需以不可逆的方式销毁有关数据或脱敏存储，有存档要求的从其规定
					技术要求：参照有关法律法规和标准执行	技术要求：视情况脱敏	技术要求：视情况脱敏	

数据级别	数据采集	数据传输	数据存储	数据访问	部门内部共享	部门外部共享	数据开放	数据销毁
2级	数据采集流程和方式符合相应要求	通过互联网和无线方式传输时应进行加密	应保存在可信或可控的信息系统或物理环境中。非可信或离线环境应进行加密存储	需设置粗颗粒度的身份标识与鉴别机制。应建立访问控制矩阵，明确可访问用户和可访问内容。宜采用口令、密码、生物识别等鉴别技术对用户进行身份鉴别	审批要求：对于有条件共享的，数据共享开放主体审批和数源部门授权后有条件共享	审批要求：对于有条件共享的，数据共享开放主体审批和数源部门授权后有条件共享	审批要求：数据共享开放主体审批后有条件开放或无条件开放	业务终止时需脱敏存储，有存档要求的从其规定
					技术要求：参照有关法律法规和标准执行	技术要求：视情况脱敏	技术要求：视情况脱敏	
1级	数据采集流程和方式符合相应要求	不需要进行传输加密	可存储在经过安全认证的公有云上	可不设置身份标识与鉴别机制	审批要求：无	审批要求：无	审批要求：无	自行决定数据处理方法
					技术要求：无	技术要求：无	技术要求：无	

第八章 分类分级实施流程

数据分类分级实施流程如下图：

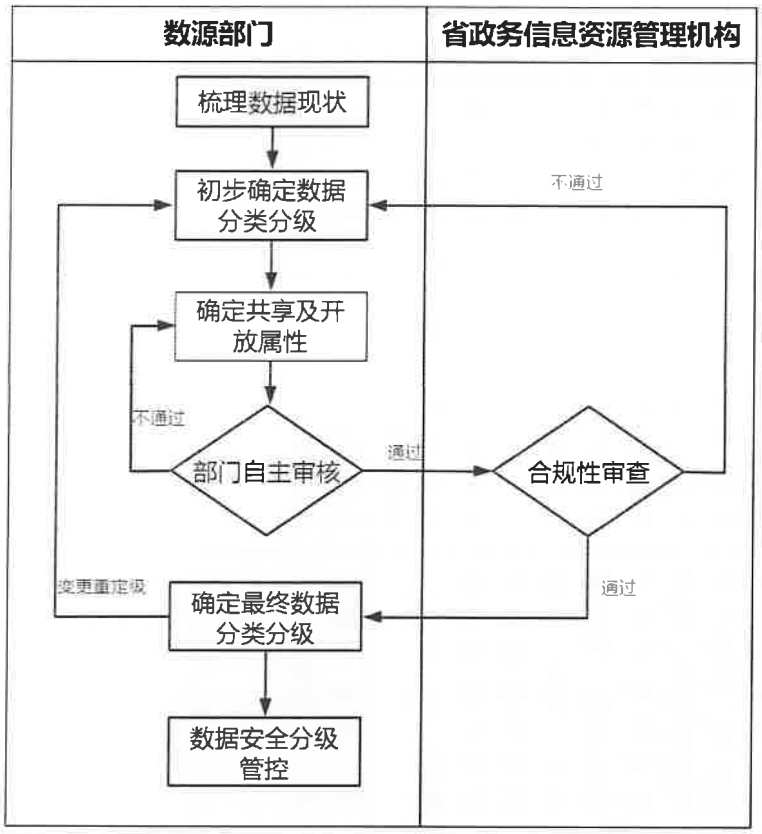


图 1 数据分类分级实施流程图

8.1. 启动阶段

梳理数据现状。数源部门梳理本部门的数据范围，明确数据所属系统名称、信息资源格式、更新频率、数据表英文名称等。

8.2. 实施阶段

a）初步确定数据分类分级。数源部门结合自身业务，按照本指南初步判定数据在确定各分类维度的分类类别和数据安全等级。

b）确定共享及开放属性。数源部门根据数据安全等级，确定数据的共享属性和开放属性，对于将政务数据列为不予共享或有条件共享类的，须申明理由，明确相关共享条件，并提供相应的法律法规、规章或者党中央、国务院政策依据。

c）部门自主审核。数源部门应对数据在各维度的初步分类结果及数据分级结果进行部门内部自主审核，审核通过后提交至省政务信息资源管理机构审查。

8.3. 评估阶段

合规性审查。省政务信息资源管理机构对数源部门的数据分类和分级结果进行合规性审查。

8.4. 完成阶段

确定最终数据分类分级。经省政务信息资源管理机构合规性审查通过后，最终确定数源部门的数据在各维度分类下的结果和数据安全等级。数源部门应定期组织对分类分级结果的合理性、有效性进行评估，当数据状态、服务范围等方面发生变化时，及时对分类分级结果进行调整，并记录变更过程。

8.5. 使用阶段

数据安全分级管控。各部门应当按照数据安全分级管控要求，在日常工作过程中对各级数据实施不同程度的安全保护措施，在数据共享和开放过程中遵循数据出口的安全管控要求。

第九章 附录

政务数据分级示例

级别	影响程度	数据示例
1级	数据泄露后无危害	1.公共机构、设施的位置、指标参数、运行状态、统计数据等，如金融服务机构数据、地表水水质自动检测数据； 2.公布后的国民经济和社会发展统计数据，如固定资产投资统计数据； 3.行政许可和其他对外管理服务事项办理数据，如保安公司开展保安业务备案数据、食品流通许可证数据； 4.环境保护、公共卫生、安全生产、食品药品、产品质量的监督检查数据，如工业产品质量监督抽查数据； 5.奖励、认定类数据，重大项目批准实施数据，如工业设计中心认定数据、重点工业项目数据等； 6.法律、法规、规章和国家有关规定，应当公开的内容，如物业服务分等收费指导标准等； 7.组织发布在网站、宣传册中或任何其他公开来源的数据； 8.组织涉及行政、司法行为、公共事项必须披露的数据； 9.依据法律法规必须公开的数据，如“企业信息公示暂行条例”中明确应公开的内容； 10. 其他。
2级	数据泄露后无危害，仅对特定公众和群体有益，且可能对其他公众和群体产生不利	1. 依申请公开的政府信息； 2. 未公开的行业发展统计数据； 3.可以间接识别到数据权主体，但不直接反映数据权主体的行为活动、经营状况等敏感数据，如机动车报废数据； 4.不能识别到具体数据权主体身份但包含其敏感信息的数据，如非实名公交卡刷卡数据等； 5.组织规范日常管理和运营的制度、规范、手册、流程图、

级别	影响程度	数据示例
	影响	信息系统等； 6. 组织水、电、气等资源消耗数据； 7. 组织缴纳税务、社保、公积金等数据； 8. 组织应披露但未到披露时间节点的各类信息，如财务报表等； 9. 城市公共卫生间、充电桩、公交站等公共服务设施的分布及状态等； 10. 城市道路车流量、道路、桥梁、隧道等可通行数据； 11. 其他。
3 级	数据泄露后会对个人、法人、其他组织或国家机关正常运作造成损害	1. 特殊领域的统计数据，如传染病统计数据、药品使用统计数据等； 2. 可反映出数据权主体活动、经营状况的数据，如自然人、法人和非法人组织的水、电、气等资源消耗数据，缴纳税务、社保、公积金等数据； 3. 个人一般信息：个人未主动公开的性别、民族、工作经历、教育程度、服兵役情况、居委会、单位名称、电子邮箱等数据； 4. 技术信息：非关键基础设施的技术设计、技术样品、质量控制、应用试验、工艺流程、工业配方、化学配方、制作工艺、制作方法、计算机程序等； 5. 经营信息：发展规划、竞争方案、管理诀窍、客户名单、货源、产销策略、财务状况、投融资计划、标书标底、谈判方案等； 6. 公共治安视频数据等； 7. 敏感个人信息（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）；

级别	影响程度	数据示例
		8. 其他。
4 级	数据泄漏后会对个人人身安全、法人正常运作或国家机关正常运作造成严重损害。	1. 重要公共或基础设施的详细数据； 2. 高精度的地理、海洋、气象测绘数据等； 3. 监管部门规定的核心数据等； 4. 其他。

海南省政府大数据推进工作领导小组办公室　2022年1月27日印发