ICS 35.240.01
CCS L 67

DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T XXXXX—XXXX

公共数据安全技术要求

Basic requirements for common data security

送审稿

2022-XX-XX 发布　　2022-XX-XX 实施

深圳市市场监督管理局　　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。

本文件由深圳市政务服务数据管理局提出。

本文件由深圳市政务服务数据管理局归口。

本文件起草单位：深圳市信息安全管理中心、全知科技（杭州）有限责任公司。

本文件主要起草人：李苏、董安波、穆端端、轩豪男、魏凤玲、王勰思、姚冬炎、董亮。

公共数据安全技术要求

1 范围

本文件规定了深圳市公共数据安全技术要求，主要包括公共数据通用管理安全要求、数据通用技术安全要求及数据处理活动基本安全要求，安全要求分为公共数据通用基本安全要求及三、四级增强安全要求，数据级别定为第一至二级需满足通用基本安全要求；数据级别定为第三级需在通用基本安全要求基础上，满足第三级增强安全要求；数据级别定为第四级需在通用基本安全要求和第三级增强要求基础上，满足第四级增强安全要求；第五级别数据为非常重要的监督管理对象，不在本文件描述。

本文件适用于深圳市公共管理和服务机构进行数据安全能力自评估或建设依据，还适用于第三方数据安全服务机构对公共管理和服务机构数据安全能力进行差距评估，以及数据统筹监管部门评判公共管理和服务机构以及提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者的数据安全保障能力。

注：数据分级方法见第6章。

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 35273—2020 信息安全技术 个人信息安全规范

GB/T 39477—2020 信息安全技术 政务信息共享 数据安全技术要求

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 37988—2019 信息安全技术 数据安全能力成熟度模型

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

3 术语和定义

GB/T 35273—2020、GB/T 37988—2019界定的以及下列术语和定义适用于本文件。

3.1

数据处理 data processing

指数据的收集、存储、使用、加工、传输、提供、开放等活动。

[来源：深圳经济特区数据条例，第二条（六）]

3.2

公共数据 common data

公共管理和服务机构在依法履行公共管理职责或者提供公共服务过程中产生、处理的数据，本文件提及的数据均指公共数据。

[来源：深圳经济特区数据条例，第二条（五）]

3.3

重要数据 key data

指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接影响国家安全、经济运行、社会稳定、公共健康和安全的数据。

3.4

核心数据 core data

指关系国家安全、国民经济命脉、重要民生、重大公共利益等数据。

[来源：中华人民共和国数据安全法，第二十一条]

3.5

敏感个人信息 personal sensitive information

指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，第二十八条]

3.6

公共管理和服务机构 public administration and service institutions

本市国家机关、事业单位和其他依法管理公共事务的组织，以及提供教育、卫生健康、社会福利、供水、供电、供气、环境保护、公共交通和其他公共服务的组织。

[来源：深圳经济特区数据条例，第二条（九）]

3.7

匿名化 anonymization

指个人数据经过处理无法识别特定自然人且不能复原的过程。

[来源：深圳经济特区数据条例，第二条（七）]

3.8

数据合作方 data cooperator

指与公共管理和服务机构进行业务合作、技术支撑和数据服务的，可能接触到机构内外部公共数据的外部单位。

3.9

安全多方计算 Secure Multi-Party Computation

指在无可信第三方情况下，安全地计算一个约定函数，保证各方数据安全的同时，得到预期计算的结果。

3.10

同态加密 Homomorphic Encryption

指处理加密的数据输出的结果解密后，与处理未加密的原始数据输出的结果保持一致，以保证数据保密性的同时，对隐私数据进行处理分析。

4 总体原则和要求

4.1 总体处理原则

为规范深圳市公共数据安全的基本要求，防范和抵御数据可能面临的各类安全风险，公共管理和服务机构在处理数据过程中，应遵循以下原则，法律、行政法规另有规定的除外：

a) 合法正当原则：任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据，数据处理活动过程不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

b) 权责一致原则：采取技术和其他必要的措施保障数据的安全，对数据处理活动中涉及的组织、公众和个人的合法权益负责。

c) 目的明确原则：数据处理活动应具有明确、清晰、具体的目的。

d) 明示同意原则：与数据相关的主体拥有对其数据的处理目的、方式、范围等规则知情权，在进行数据处理活动前应向主体明示，并获得授权同意。

e) 最小必要原则：数据处理活动应仅处理可满足特定公共服务为目的所需的最少数据类型和数量。

f) 公开透明原则：以明确、易懂和合理的方式公开处理公共数据的范围、目的、规则等，并接受外部监督。

g) 全程可控原则： 采取必要管控措施确保数据处理活动各环节的保密性、完整性和可用性，记录数据处理过程，记录内容清晰可追溯。

4.2 总体安全要求

公共管理和服务机构应严格遵守《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》等法律法规，在个人信息及数据安全处理活动相关条款基础上，落实本文件安全要求。

承载公共数据的信息系统应依据GB/T 22239—2019的安全要求，同步规划、建设、运营信息系统，并对信息系统组织开展定级备案、等保测评、安全整改工作；数据处理过程涉及的密码技术应符合GB/T 39786—2021等相关国家标准规定；涉及关键信息基础设施相关信息系统安全要求应符合《关键信息基础设施安全保护条例》等相关安全要求。

5 总体安全框架

本文件依据数据安全相关的国家法律法规、政策要求、国家标准规范、政务行业标准等，聚焦深圳市公共数据安全，总体框架围绕公共数据安全要求展开，旨在提升公共管理和服务机构在数据安全建设、管理、运营方面的能力，框架结构如图1：

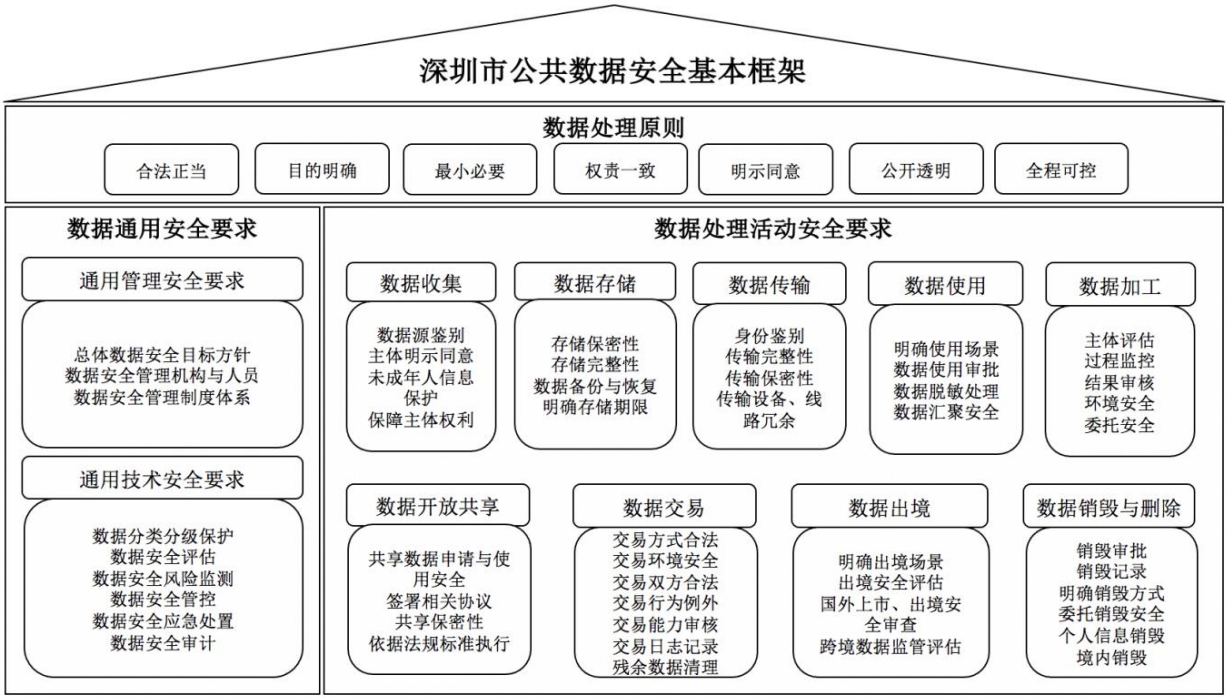

图1 公共数据安全技术要求基本框架

6 安全技术要求

6.1 分级概述

在公共数据分类基础上，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、社会秩序和公共利益或者个人信息主体、公共管理和服务机构合法权益造成的损害程度，对公共数据分级。

6.2 确定定级对象

数据定级对象可以是最小数据类，也可以是最小数据类下的具体数据字段。

6.3 定级要素

数据定级对象的定级要素包括:

a) 受侵害的客体：

1）个人信息主体及公共管理和服务机构的合法权益；

2）社会秩序和公共利益；

3）国家安全。

b) 对客体的侵害程度：

1）造成一般损害；

2）造成严重损害；

3）造成特别严重损害。

对客体的侵害程度应结合数据遭受篡改、破坏、泄露或者非法获取、非法利用时涉及的数据类型、数据量、数据影响面综合考虑进行判定。

6.4 定级要素与安全等级关系

依据 GB/T 22240—2020 关于业务信息安全等级保护定级规则，定级要素与安全等级的关系如下表所示：

表 1 定级要素与安全等级关系

受侵害的客体	客体侵害程度		
	一般损害	严重损害	特别严重损害
个人信息主体及公共管理和服务机构的合法权益	第一级	第二级	第二级
社会秩序和公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

6.5 定级流程

数据定级流程如图 2 所示。

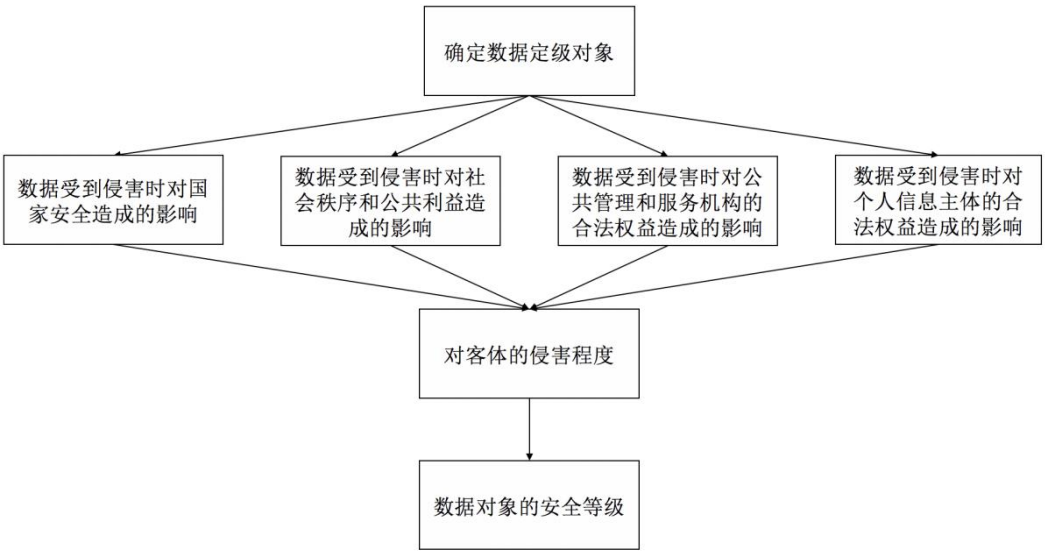

图 2 公共数据安全级别定级流程

数据对象定级采取“就高不就低”原则，根据对客体侵害程度判定的最高级别作为初步确定的安全等级；数据对象安全等级初步确定为第二级及以上的，公共管理和服务机构依据本文件组织专家进行评审，最终确定其安全保护等级；数据对象安全等级初步确定为第一级的，公共管理和服务机构可依据业务需求不进行评审。

数据处理活动过程中，数据类别及级别发生变更的，应及时对变更后数据重新分类及级别判定，数据级别可能发生变更的场景包括但不限于数据汇聚融合、加工、脱敏、超过时效等。

7 通用管理安全要求

7.1 总体数据安全目标方针

7.1.1 通用基本安全要求

应明确公共数据安全管理的总体方针，包括管理目标、原则、要求等内容，制定或修订完善总体安全管理框架，公共数据安全管理应作为重点内容，纳入总体安全管理范畴。

7.1.2 第三级增强安全要求

第三级无增强安全要求。

7.1.3 第四级增强安全要求

第四级无增强安全要求。

7.2 数据安全管理机构与人员

7.2.1 通用基本安全要求

7.2.1.1 机构管理

本项要求包括：

a) 应设立数据安全管理机构，明确数据安全责任人，落实数据安全保护责任；
b) 数据安全责任人履行职责包括但不限于：
   1) 组织制定数据保护计划并落实；
   2) 组织开展数据安全评估，整改安全隐患；
   3) 组织按要求向有关部门或网信部门报告数据安全保护和事件处置情况；
   4) 组织受理并处理用户投诉和举报事项等。
c) 数据安全管理机构应明确数据管理员、数据安全管理员、数据安全审计员等岗位职责，落实岗位人员，保障数据安全管理与审计工作开展。相关岗位职责应包括：
   1) 数据管理员一般由数据库管理员担任，负责数据存储、数据权限分配、数据资产梳理等；
   2) 数据安全管理员负责数据权限审批、数据分类分级、数据安全风险检测与评估、数据安全事件应急响应处置、教育培训等；
   3) 数据安全审计员负责数据安全审计等。
d) 处理个人信息达到国家网信部门规定数量的公共管理和服务机构，应指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。

7.2.1.2 人员管理

本项要求包括：

a) 应与内部数据岗位人员、数据合作方人员签订保密协议，明确数据访问范围、操作权限、人员调离岗保密要求、保密期限、违约责任等，有效约束操作行为；
b) 应制定数据安全培训计划，定期组织数据安全培训工作，每年至少一次；针对机构全员，培训内容包括但不限于数据安全意识、法律法规等；针对数据岗位人员，培训内容包括但不限于标准规范、技能培训、应急响应、应急演练等，留存培训记录；
c) 宜组织数据岗位人员考取相关资质证书，持证上岗。

7.2.2 第三级增强安全要求

第三级无增强安全要求。

7.2.3 第四级增强安全要求

第四级无增强安全要求。

7.3 数据安全管理制度体系

7.3.1 通用基本安全要求

本项要求包括：

a) 应建立健全个人信息和数据安全保护制度体系，制度体系内容包括但不限于数据安全政策、组织机构与人员管理、数据分类分级、数据安全评估、数据安全风险监测、数据访问权限管控、数据安全应急与处置、数据安全审计、数据处理活动安全管理要求（包括数据收集、存储、传输、使用、加工、开放共享、交易、出境、销毁等）、数据安全教育培训、数据合作方管理等；

b) 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督。

7.3.2 第三级增强安全要求

第三级无增强安全要求。

7.3.3 第四级增强安全要求

第四级无增强安全要求。

8 通用技术安全要求

8.1 数据分类分级保护

8.1.1 通用基本安全要求

本项要求包括：

a) 应结合数据资产识别技术手段，梳理数据资产，并明确数据资产类型、数据量、存放位置、数据关联系统、数据共享情况、数据出境情况等；

b) 应明确数据分类标准，依据数据资源属性特征，将数据合理划分类别，形成数据资源分类目录；

c) 应明确数据安全等级，依据数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用时，对国家安全、社会秩序和公共利益或者个人信息主体、公共管理和服务机构合法权益造成的侵害程度确定安全等级；

d) 应在数据分类分级基础上，形成数据资产清单，明确差异化防护措施要求。

8.1.2 第三级增强安全要求

应定期评审数据的类别和级别，如需变更数据所属类型或级别，应依据变更审批流程执行变更。

8.1.3 第四级增强安全要求

第四级无增强安全要求。

8.2 数据安全评估

8.2.1 通用基本安全要求

本项要求包括：

a) 应结合自身数据安全要求，制定数据安全风险评估方法，明确风险评估目的、范围、依据、评估流程、评估频率、实施评估、综合评估分析等内容；
b) 处理敏感个人信息或者国家规定的重要数据、核心数据的机构，应按照有关规定定期开展风险评估，并向有关主管部门报送风险评估报告；
c) 在出现法律法规重大更改或增删、业务活动发生重大变化、数据资产发生重大变化、发生重大数据安全事件、数据安全管理方针发生变化等重大情况变化时进行局部或全面数据安全风险评估，形成数据安全风险评估报告；
d) 涉及国家、行业存在数据安全合规监管要求的机构，应定期开展数据安全合规性评估，并向有关主管部门报送合规性评估报告。
e) 涉及敏感个人信息处理、个人信息自动化决策、委托处理、他人提供（含境外）、公开、其他对个人权益有重大影响的个人信息处理活动等，应事先开展个人信息保护影响评估，评估记录至少保存三年。

8.2.2 第三级增强安全要求

第三级无增强安全要求。

8.2.3 第四级增强安全要求

第四级无增强安全要求。

8.3 数据安全风险监测

8.3.1 通用基本安全要求

本项要求包括：
a) 应建立数据安全风险监测预警机制，制定合理有效的风险监测指标；
b) 应对数据安全事件和可能引发数据安全事件的风险隐患进行收集、分析判断和持续监控预警，建立数据安全监测预警流程，有效保障业务系统所承载数据资产的机密性、完整性、可用性；
c) 应具备常态化数据安全风险监测能力，持续监测数据安全风险，风险类型包括但不限于账号风险、权限风险、异常操作行为、数据出境风险、数据暴露面风险等；
d) 应配备专人负责数据安全风险监测工作，定期出具风险监测报告；
e) 应加强数据安全风险闭环管理，持续提升数据安全风险处置能力；
f) 应定期对数据安全风险监测工作的有效性、全面性进行审核验证。

8.3.2 第三级增强安全要求

第三级无增强安全要求。

8.3.3 第四级增强安全要求

第四级无增强安全要求。

8.4 数据安全管控

8.4.1 通用基本安全要求

8.4.1.1 数据访问权限管控

本项要求包括：

a） 应明确数据管理、审计类账号权限开通、分配、使用、变更、注销等安全管理要求；
b） 应对账号及对应权限进行记录，并在账号或权限发生变更时及时更新，重点关注离职人员账号回收、管理权限变更、沉默账号、复活账号；
c） 应严格控制账号访问、操作权限，明确账号申请审批流程；
d） 应对账号进行统一身份认证、操作行为记录；
e） 应对业务系统之间的数据访问采取身份鉴别、访问控制、安全审计、资源控制等技术措施；
f） 应对涉及数据重大操作行为（如敏感个人信息、重要数据、核心数据批量下载、上传、删除、共享和销毁等）设置内部审批流程，并记录操作行为。

8.4.1.2 数据防泄露管控

应在网络层面对数据流转、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。

8.4.1.3 数据接口管控

本项要求包括：
a） 应在数据接口调用前进行身份鉴别，通过技术手段限制非白名单接口接入；
b） 应对数据接口定期开展安全检测，及时发现并处置数据安全风险隐患；
c） 应对数据接口实施调用审批流程，定期开展接口日志审计。

8.4.2 第三级增强安全要求

8.4.2.1 数据访问权限管控

应对数据跨网络区域传输采取安全管控措施，包括但不限于网络及应用层的访问控制策略，控制粒度为端口级。

8.4.2.2 数据防泄露管控

应在终端层面对数据流转、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，并在网络层面对异常数据操作行为及时定位和阻断。

8.4.2.3 数据接口管控

本项要求包括：
a） 应对异常数据接口调用行为实现自动预警、拦截功能；
b） 应对开放数据接口的平台相关接口数据交互行为进行监测，对接口访问行为进行审计；
c） 应建立数据接口全生命周期管理机制，形成接口清单，动态更新接口活动状态。

注：开放数据接口的平台包括但不限于数据开放平台、数据共享交换平台、数据交易平台、大数据平台、能力开放平台。

8.4.3 第四级增强安全要求

8.4.3.1 数据防泄露管控

应在终端层面对异常数据操作行为及时定位和阻断。

8.5 数据安全应急处置

8.5.1 通用基本安全要求

本项要求包括：

a) 应建立数据安全应急处置机制，依据本市、本区、本行业网络安全事件应急相关文件开展应急处置工作；
b) 发生数据泄露、毁损、丢失、篡改等数据安全事件时应立即启动应急预案，采取相应的应急处置措施，及时告知相关权利人，并按照有关规定向市网信、公安部门和有关行业主管部门报告；
c) 数据安全应急处置后应分析事件发生原因，总结应急处置经验，调整数据安全策略，形成事件调查记录和总结报告，避免再次发生类似情况；
d) 发生个人信息泄露、毁损、丢失等数据安全事件，或发生数据安全事件风险明显加大时，应立即采取补救措施，及时以电话、短信、邮件或信函等方式告知个人信息主体，并主动报告有关主管部门，必要时应向市网信部门报告；
e) 应采取技术手段对数据安全事件进行溯源，造成严重事件的应依法追究事件主体责任；
f) 应根据应急预案明确的数据安全事件场景定期开展应急演练，每年至少一次，事件场景包括但不限于数据泄露、丢失、滥用、篡改、毁损、违规使用等。

8.5.2 第三级增强安全要求

本项要求包括：
a) 应跟踪和记录数据收集、分析、加工、挖掘等过程，保证溯源数据能重现相应过程。
b) 关键信息基础设施系统数据在发生重要数据泄露、较大规模个人信息泄露时，应及时上报关键信息基础设施安全保护工作部门。

8.5.3 第四级增强安全要求

本项要求包括：
a) 应对数据处理活动实现数据审计，保证数据处理各环节操作可追溯；
b) 应采取技术手段保证溯源数据真实性和保密性。

8.6 数据安全审计

8.6.1 通用基本安全要求

本项要求包括：
a) 应配备数据安全审计员，加强数据安全审计管理，数据安全审计的覆盖面包括数据收集、数据存储、数据传输、数据使用、数据加工、数据开放共享、数据销毁与删除等数据处理活动各环节，书面明确审计策略、审计对象、审计内容、审计周期、审计结果、审计问题跟踪等要求；
b) 应对数据处理活动环节实施日志留存管理，日志记录至少包括时间、IP地址、操作账号、操作内容、操作结果等，在发生安全事件时可提供溯源取证能力，日志保存时间不少于180天；
c) 应定期对数据处理活动各环节日志进行数据安全审计，每年至少一次，形成数据安全审计报告。

8.6.2 第三级增强安全要求

应定期对数据账号操作及接口调用情况进行安全审计。

8.6.3 第四级增强安全要求

第四级无增强安全要求。

9 数据处理活动安全要求

9.1 数据收集

9.1.1 通用基本安全要求

本项要求包括：

a) 应对数据收集来源进行鉴别和记录，确保数据收集来源的合法性、正当性，明确数据类型及收集渠道、频度、方式等；
b) 收集外部机构数据前，应对外部机构数据源的合法性、合规性进行鉴别，并对数据收集过程中的网络环境、系统进行安全评估，确保收集数据的机密性、完整性和可用性；
c) 个人信息收集应遵循合法、正当、必要和诚信原则，并获得个人信息主体的明示同意，不得通过误导、欺诈、胁迫或者其他违背个人信息主体真实意愿的方式获取其同意；
d) 应依据GB/T 35273—2020第5章开展个人信息收集工作；
e) 提供公共服务的移动互联网应用程序，应依据《常见类型移动互联网应用程序必要个人信息范围规定》收集个人信息，不应因个人信息主体不同意收集非必要个人信息，而拒绝个人信息主体使用移动互联网应用程序。

9.1.2 第三级增强安全要求

第三级无增强安全要求。

9.1.3 第四级增强安全要求

第四级无增强安全要求。

9.2 数据存储

9.2.1 通用基本安全要求

本项要求包括：

a) 应明确数据存储相关安全管控措施，如加密、访问控制、数字水印、完整性校验等；
b) 应采用密码技术保证敏感个人信息、重要数据、核心数据在存储过程中的保密性；
c) 应明确本地数据备份与恢复安全策略，建立数据备份恢复操作规程，说明数据备份周期、备份方式、备份地点；建立数据恢复性验证机制，保障数据的可用性与完整性；
d) 应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地；
e) 个人生物识别信息应与个人身份信息分开存储，原则上不应存储原始个人生物识别信息(如样本、图像等)，仅存储个人生物识别信息的摘要信息。

9.2.2 第三级增强安全要求

本项要求包括：

a) 应采用校验技术或密码技术保证数据在存储过程中的完整性；
b) 应提供异地实时备份功能，利用通信网络将数据实时备份至备份场地；
c) 应提供数据处理环节关联信息系统的热冗余，保证数据的高可用性；
d) 个人信息存储期限应为实现个人信息主体授权使用目的所必需的最短时间,法律法规另有规定或者个人信息主体另行授权同意的除外，超出个人信息存储期限后，应对个人信息进行删除或匿名化处理。

9.2.3 第四级增强安全要求

本项要求包括：

a) 应采用密码技术保证数据在存储过程中的完整性；
b) 应建立异地灾难备份中心，提供数据的实时切换。

9.3 数据传输

9.3.1 通用基本安全要求

本项要求包括：

a) 应明确数据传输相关安全管控措施，如传输通道加密、数据内容加密、数据接口传输安全等；
b) 应对数据传输两端进行身份鉴别，确保数据传输双方可信任；
c) 应采用校验技术保证数据在传输过程中的完整性；
d) 应对敏感个人信息、重要数据、核心数据采用通道加密或内容加密的方式进行传输；
e) 应对离线或即时通信方式传输的敏感个人信息、重要数据、核心数据采取加密、脱敏等安全措施，确保传输安全性；
f) 应对关键网络传输线路及核心设备实施冗余建设，确保数据传输的网络可用性。

9.3.2 第三级增强安全要求

本项要求包括：

a) 应采用校验技术或密码技术保证数据在传输过程中的完整性；
b) 应采用密码技术保证数据在传输过程中的保密性。

9.3.3 第四级增强安全要求

本项要求包括：

a) 应采用密码技术保证数据在传输过程中的完整性；
b) 在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

9.4 数据使用

9.4.1 通用基本安全要求

本项要求包括：

a) 应明确数据使用业务场景的目的、范围、审批流程（含权限授予、变更、撤销等）、人员岗位职责等，鼓励在保障安全的情况下，开展数据利用；
b) 应明确数据统计分析、展示、发布、公开披露等不同数据使用场景的安全管理要求；
c) 应根据不同数据使用场景采用处理措施（如去标识化、匿名化等），降低数据敏感度及暴露风险。

9.4.2 第三级增强安全要求

应采取技术措施保证汇聚大量数据时不暴露敏感信息。

9.4.3 第四级增强安全要求

第四级无增强安全要求。

9.5 数据加工

9.5.1 通用基本安全要求

本项要求包括：

a) 应对参与数据加工活动的主体进行合法性、正当性的评估，确保参与数据加工活动的主体为合法合规的组织机构或个人；
b) 应在数据加工前，书面明确数据加工目的、范围、期限、规则及数据加工主体的责任与义务；
c) 应对数据加工的过程进行评估与监控，对数据加工过程的数据操作行为进行记录、审计；
d) 应对数据加工结果进行评估，如产生新数据，应对新数据进行安全审核，确保新数据不存在数据泄露风险；
e) 应提供安全的数据加工环境，包括网络环境、终端环境等，避免加工过程导致数据泄露、数据破坏等安全风险；
f) 委托他人加工处理数据的，应与其订立数据安全保护合同，明确双方安全保护责任；委托加工处理个人信息的，应约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督，不应超出已征得个人信息主体授权同意的范围。

9.5.2 第三级增强安全要求

应对数据加工的过程进行评估与监控，对数据加工过程的数据操作行为进行记录、审计，对异常数据操作行为及时预警、处置。

9.5.3 第四级增强安全要求

第四级无增强安全要求。

9.6 数据开放共享

9.6.1 通用基本安全要求

本项要求包括：

a) 公共数据开放共享应依据《深圳经济特区数据条例》第三章第二、三节条款执行；
b) 公共数据提供部门应与公共数据使用部门签署相关协议，明确数据使用目的、供应方式、保密约定、数据共享范围、数据安全保护要求等内容；
c) 公共数据提供部门应采用国家相关标准规定的密码技术，保障数据共享过程的保密性和完整性；
d) 政务信息资源交换平台的政务信息共享应依据GB/T39477—2020执行。

9.6.2 第三级增强安全要求

可采用多方安全计算、同态加密等数据隐私计算技术实现数据共享的安全性。

9.6.3 第四级增强安全要求

第四级无增强安全要求。

9.7 数据交易

9.7.1 通用基本安全要求

本项要求包括：

a) 数据交易主体可通过依法设立的数据交易平台进行数据交易，也可由交易双方依法自行交易；

b) 设立数据交易平台的机构应建立安全、可信、可控、可追溯的数据交易环境，制定数据交易、信息披露、自律监管等规则，并采取有效措施保护个人数据、商业秘密和国家规定的重要数据；
c) 设立数据交易平台的机构应对数据交易主体双方进行审核，确保交易双方均为合法组织机构；
d) 应确保数据交易行为符合国家相关法律、法规的要求，以下情形不可进行交易：
   1) 交易的数据产品和服务包含个人数据未依法获得授权；
   2) 交易的数据产品和服务包含未经依法开放的数据；
   3) 法律、法规规定禁止交易的其他情形。
e) 设立数据交易平台的机构应对数据交易过程进行记录，形成数据交易日志，数据交易日志至少包括：交易唯一标识、交易时间、数据供给方、数据需求方、交易数据标识、数据标签、交易价格、交易模式、交易结果、交易量等；
f) 在数据交易结束后数据交易供给方应及时关闭相关数据接口，清理残余数据。

9.7.2 第三级增强安全要求

本项要求包括：
a) 设立数据交易平台的机构应对数据交易供给方进行安全评估，证明具备向数据交易需求方安全交付数据的能力；
b) 数据交易供给方应对数据交易需求方进行安全评估，证明具备对交易数据实施安全保护的能力。

9.7.3 第四级增强安全要求

第四级无增强安全要求。

9.8 数据出境

9.8.1 通用基本安全要求

本项要求包括：
a) 应明确数据出境业务场景，严格遵守国家法律、行政法规数据出境安全管理办法，严禁未授权数据出境行为；
b) 向境外提供个人信息或者国家规定的重要数据前，应按照有关规定申请数据出境安全评估，进行国家安全审查，法律、行政法规另有规定的，从其规定。
c) 掌握超过国家相关规定的用户个人信息数量的机构赴国外上市，或存在核心数据、重要数据或大量个人信息出境风险的情形，应向网络安全审查办公室申报网络安全审查。

9.8.2 第三级增强安全要求

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。

9.8.3 第四级增强安全要求

第四级无增强安全要求。

9.9 数据销毁与删除

9.9.1 通用基本安全要求

本项要求包括：

a) 应建立数据销毁与删除规程，明确数据销毁与删除场景、方式及审批机制，设置相关监督角色，记录数据销毁与删除操作过程；
b) 如因业务终止或组织解散，无数据承接方的，应及时有效销毁其控制的数据，法律、法规另有规定的除外；
c) 委托数据合作方完成数据处理后，应及时销毁委托相关的数据，法律、法规另有规定或者双方另有约定的除外；
d) 根据要求、约定删除数据或完成数据处理后无需保留源数据的，应及时删除相关数据；
e) 应依据《深圳经济特区数据条例》第二十五条及GB/T 35273—2020 8.3章节执行个人信息删除操作；
f) 应在中国境内对介质存储的数据进行删除或销毁。

9.9.2 第三级增强安全要求

应对存储数据的介质或物理设备采取难恢复的技术手段，如物理粉碎、消磁、多次擦写等。

9.9.3 第四级增强安全要求

第四级无增强安全要求。

附 录 A
（资料性）
公共数据分类示例

公共数据分类可按照线分类法进行分类，深圳市公共管理和服务机构应收集内部所有业务系统的数据资源，梳理数据资源类别，依据线分类法，按照业务数据属性或特征，将公共数据按照基础库或其它库题分为若干大类，并根据类别及数据隶属关系，将每个大类的数据分为若干层级，同时每个层次也可分为若干子类，同一分支的同层级子类构成并列关系，不同层级子类之间构成隶属关系，最终形成数据资源目录树，如图 A.1 所示。

由于公共数据涉及教育、卫生健康、供水、供电、供气、供热、金融、电信、公共交通等行业，因此各行业可依据其行业制定的分类分级标准开展数据分类分级工作，例如金融行业可依据 JR/T 0171—2020《个人金融信息保护技术规范》及 JR/T 0197—2020《金融数据安全 数据安全分级指南》、电信行业可依据 YD/T 3813—2020《基础电信企业数据分类分级方法》，其它行业暂无已发布的行业标准参考的，则可依据本标准的公共数据分类方法执行。

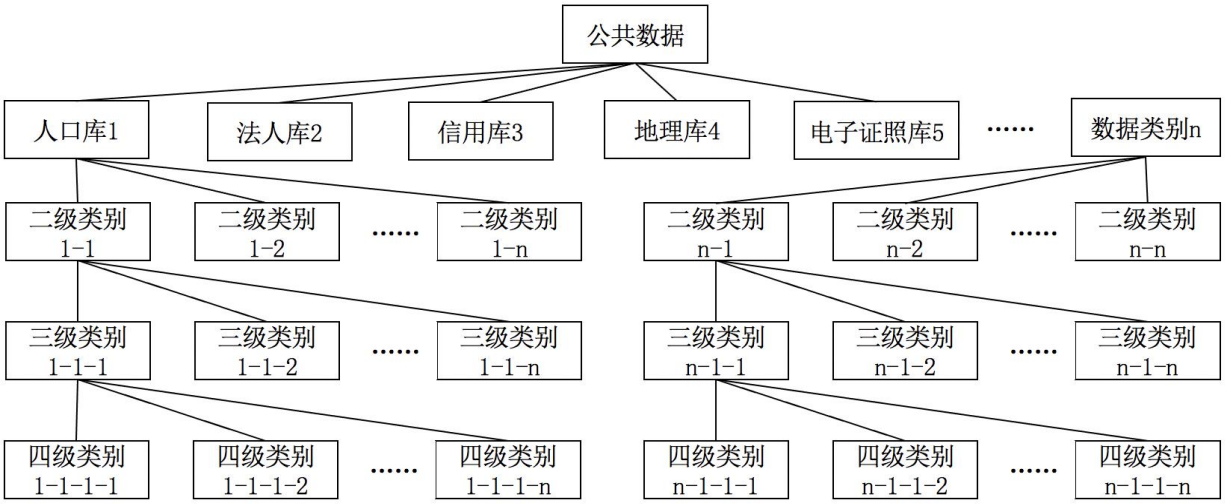

图 A.1 公共数据资源分类示例

参 考 文 献

[1] GB/T 37932—2019 信息安全技术 数据交易服务安全要求

[2] GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南

[3] YD/T 3813—2020 基础电信企业数据分类分级方法

[4] JR/T 0223—2021 金融数据安全 数据全生命周期安全规范

[5] 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

[6] ISO/IEC 27001:2013 Information security management system requirements

[7] 中华人民共和国国务院.关键信息基础设施安全保护条例[EB/OL].2021-07-30.

[8] 国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、国家市场监督管理总局办公厅.常见类型移动互联网应用程序必要个人信息范围规定[EB/OL].2021-03-12.

[9] 工业和信息化部办公厅.关于做好2020年电信和互联网行业网络数据安全管理工作的通知[EB/OL].2020-05-14.

[10] 深圳市人民代表大会常务委员会.深圳经济特区数据条例[EB/OL].2021.07.06.