

DB4403

深 圳 市 地 方 标 准

DB4403/T XXX—XXXX

公共数据安全体系建设指南

Guidelines for the construction of common data security systems

(送审稿)

XXXX-XX-XX 发布

XXXX-XX-XX 实施

深圳市市场监督管理局 发布

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 通则 1

 4.1 建设原则 1

 4.2 建设内容 2

 4.3 建设角色 2

 4.4 建设流程 2

5 公共数据定级 3

 5.1 公共数据定级工作流程 3

 5.2 确定数据定级对象 4

 5.3 分类分级制度制定 5

 5.4 公共数据分类分级 5

 5.5 公共数据定级评审 5

6 总体安全规划 5

 6.1 总体安全规划工作流程 5

 6.2 安全需求分析 6

 6.3 安全建设项目规划 7

7 安全设计与实施 7

 7.1 安全设计与实施工作流程 7

 7.2 安全方案详细设计 9

 7.3 通用管理安全建设 10

 7.4 通用技术安全建设 13

 7.5 数据处理活动安全建设 15

8 安全运行与维护 16

 8.1 安全运行与维护工作流程 16

 8.2 安全评估 18

 8.3 风险监测 18

 8.4 安全审计 19

 8.5 应急处置 19

 8.6 监督检查 21

9 定级对象终止 21

| | |
|-------------------------------|----|
| 9.1 定级对象终止工作流程 | 21 |
| 9.2 数据销毁与删除 | 21 |
| 附录 A（规范性） 主要过程及其活动和输入输出 | 23 |
| 附录 B（资料性） 公共数据安全制度内容说明 | 26 |
| 参考文献 | 34 |

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和数据管理局提出并归口。

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、深圳市盐田区网络安全和信息化中心、深圳市盐田区政务服务中心、深圳市南山区智慧城市运营中心、深圳市宝安区信息中心、鹏城实验室、中国电子技术标准化研究院、金砖国家未来网络研究院中国分院、深圳市智慧城市科技发展集团有限公司、深圳国家金融科技测评中心有限公司、蚂蚁科技集团股份有限公司。

本文件主要起草人：张军、董安波、李苏、罗菁春、林宇群、穆端端、赵剑、轩豪男、潘志斌、童子琦、方兴、周顿科、魏凤玲、李佳雯、包亚鹏、陈崇滨、林生锐、林军、廖英豪、姚俊华、颜军、郭志远、束建钢、何延哲、林楨、刘慧洋、王志、吴飞、黄焱、罗丰、吴祖顺、白晓媛。

公共数据安全体系建设指南

1 范围

本文件提供了公共数据安全体系建设的指导，给出了公共数据定级、总体安全规划、安全设计与实施、安全运行与维护、定级对象终止等流程与需要考虑要点的有关信息。

本文件适用于指导公共管理和服务机构公共数据安全体系建设，也适用于指导处理大量个人信息的服务平台数据安全建设。

本文件不适用于指导涉及国家秘密或者法律法规另有规定的公共数据安全建设。

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 20986—2023 | 信息安全技术 | 网络安全事件分类分级指南 |
| GB/T 25069—2022 | 信息安全技术 | 术语 |
| GB/T 35273—2020 | 信息安全技术 | 个人信息安全规范 |
| GB/T 37988—2019 | 信息安全技术 | 数据安全能力成熟度模型 |
| 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 43697—2024 | 数据安全技术 | 数据分类分级规则 |
| DB4403/T 271—2022 | 公共数据安全要求 | |
| DB4403/T 439—2024 | 公共数据安全评估方法 | |

3 术语和定义

GB/T 25069—2022、GB/T 35273—2020、GB/T 37988—2019、DB4403/T 271—2022、DB4403/T 439—2024界定的术语和定义适用于本文件。

4 通则

4.1 建设原则

公共数据安全体系建设过程遵循下列原则：

- 整体规划原则：依据DB4403/T 271—2022，从通用管理安全、通用技术安全与数据处理活动安全三方面出发，整体规划公共数据安全体系建设；
- 分级管理原则：按照公共数据类别和级别采取差异化安全保护措施，高安全级别数据从严保护，低安全级别数据适度保护；
- 分步实施原则：通过公共数据定级、总体安全规划、安全设计与实施、安全运行与维护、定级对象终止等步骤，分阶段推进公共数据安全体系建设。

4.2 建设内容

依据DB4403/T 271—2022中第7至9章及附录内容进行公共数据安全建设，建设内容涵盖通用管理安全要求、通用技术安全要求及数据处理活动安全要求等，对于不同的安全等级需达到相对应的安全要求水平，按照DB4403/T 271—2022中6.7规定的安全等级与安全要求的关系确定应落实的安全要求，如基本安全要求、三级增强安全要求、四级增强安全要求。

4.3 建设角色

公共数据安全体系建设过程中涉及各类角色，其职责内容如下：

- a) 数据运营、使用部门：负责按照国家、地方相关公共数据安全保护政策文件和技术规范，明确本部门公共数据保护对象的安全保护等级，必要时报其行政主管部门或行业监管部门备案或审核批准；根据确定的公共数据保护安全等级，进行相应等级的规划设计、安全建设或改建工作，使用符合国家有关规定的网络安全产品及服务，依照制定的各项公共数据安全管理制度，定期对公共数据保护对象安全措施落实情况进行自查或他查，发生数据安全事件时，采取应急处置措施等；
- b) 数据安全管理机构：负责按照国家、地方相关公共数据安全保护管理规范和技术标准，落实本单位公共数据安全管理工作，依据本单位明确的公共数据安全方针、策略及目标，制定各项公共数据安全管理制度，设立数据安全岗位人员，管理及指导数据运营、使用部门落实公共数据安全保护工作；公共管理和服务机构在开展公共数据安全体系建设前明确具体部门承担本角色与职责；
- c) 数据合作方：负责根据公共管理和服务机构委托，按照国家、地方相关公共数据安全保护管理规范和技术标准，协助公共管理和服务机构完成公共数据保护相关工作，包括但不限于确定公共数据保护对象及安全等级、安全需求分析、规划与设计、安全建设、运行与维护；
- d) 数据安全专家：负责评审公共数据保护相关工作的可行性、合理性及有效性，并能提供专业的评审意见，数据安全专家可从内部或外部机构选取。

4.4 建设流程

公共数据安全体系建设包括公共数据定级、总体安全规划、安全设计与实施、安全运行与维护、定级对象终止五个阶段，各个阶段的主要过程、活动、输入和输出宜按照附录A执行。建设流程见图1。

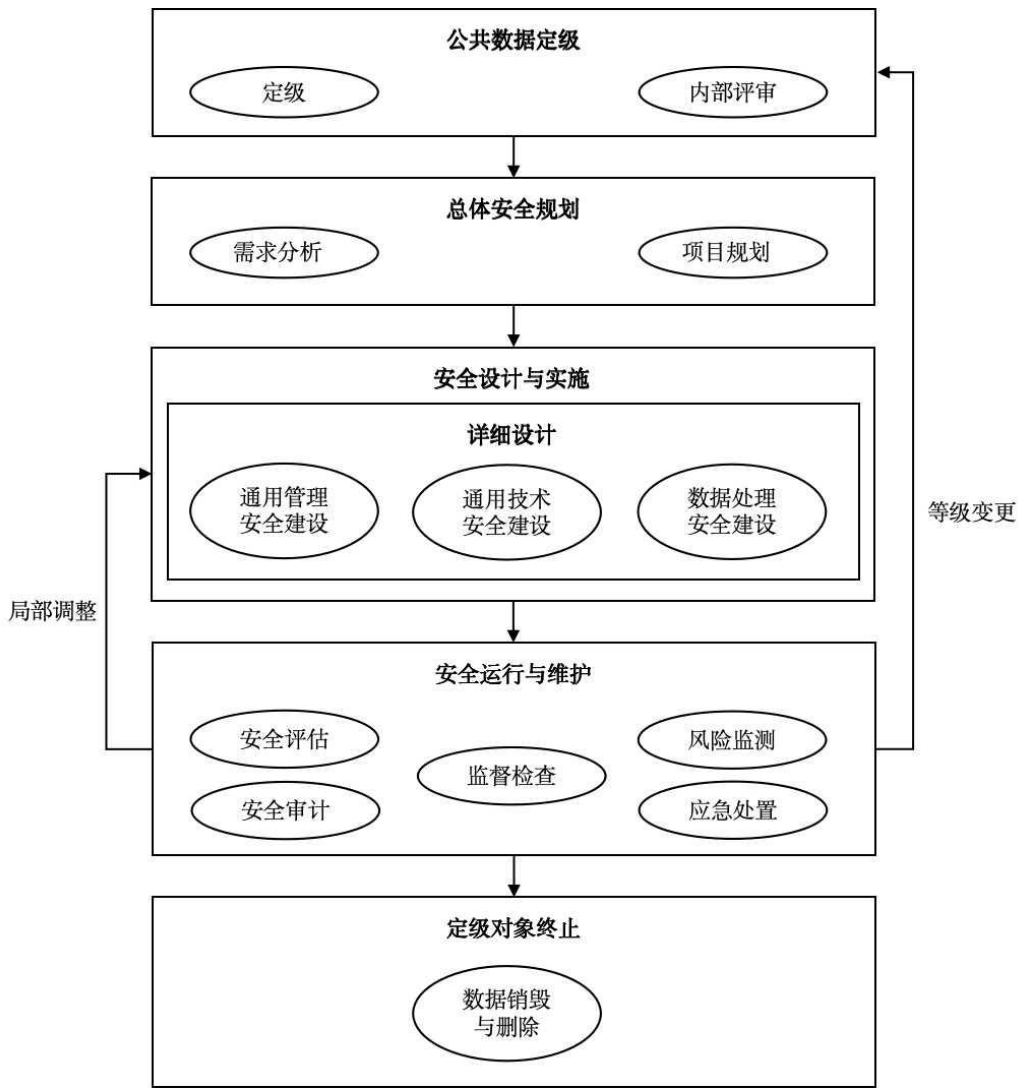


图1 公共数据安全体系建设流程

在安全运行与维护阶段，公共数据定级对象如因政策法规、安全形势、业务形态发生变化等原因需要局部调整，而其安全等级并未改变时，从安全运行与维护阶段进入安全设计与实施阶段，重新设计、调整和实施安全措施，确保持续满足数据安全保护要求；当公共数据定级对象发生重要变更导致安全等级发生变化时，从安全运行与维护阶段进入定级阶段，重新开始新一轮公共数据安全等级保护建设流程。

5 公共数据定级

5.1 公共数据定级工作流程

5.1.1 公共管理和服务机构参照 DB4403/T 271—2022 第 6 章，或 GB/T 43697—2024 第 5 至 7 章，进行公共数据定级，确定其对应安全等级，国家或行业另有规定的，从其规定。定级结果经过内部组织评审确认。

5.1.2 公共数据定级的工作流程及其工作目标、参与角色与阶段输入输出见表 1。

表 1 公共数据定级工作流程

| 主要流程 | 工作目标 | 参与角色 | 阶段输入 | 阶段输出 |
|----------|--|--|--|---|
| 确定数据定级对象 | 依据法律法规、政策文件及标准，明确具体数据定级对象，并根据确定的定级对象，开展后续数据安全建设相关工作。 | 数据安全管理机构，数据运营、使用部门，数据合作方（可选）。 | 法律法规、政策文件及标准，如 GB/T 43697—2024、DB4403/T 271—2022。 | 数据定级对象描述文件（基本安全要求）。 |
| 分类分级制度制定 | 明确公共数据类别及级别划分的依据、原则、要求、维度、方法等内容，使公共数据分类分级实施更具指导性及落地性。 | 数据安全管理机构，数据合作方（可选）。 | 法律法规、政策文件及标准，如 GB/T 43697—2024、DB4403/T 271—2022。 | 数据分类分级管理制度（基本安全要求）。 |
| 公共数据分类分级 | 依据数据分类分级管理制度，梳理公共数据类别，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，确定公共数据级别。 | 数据安全管理机构，数据运营、使用部门，数据合作方（可选）。 | 数据分类相关标准规范，如 GB/T 43697—2024、DB4403/T 271—2022，公共数据承载系统开发建设文档，数据库表信息，其他相关数据分类分级文件、工具。 | 业务系统（数据库）清单（基本安全要求），数据资产分类分级（数据子类或数据字段）清单（基本安全要求），数据血缘管理工具（四级增强安全要求）。 |
| 公共数据定级评审 | 根据公共数据定级相关标准规范等文件，确定数据保护对象的安全保护等级，通过对定级结果的内部评审、审核，以保证定级结果的准确性；依据本地区公共数据安全管理相关政策文件，按需整理相关备案或报批材料，并向受理单位提交备案或报批材料。 | 行政主管部门（可选），数据安全管理机构，数据运营、使用部门，数据安全专家（可选） | 法律法规、政策文件及标准，如 GB/T 43697—2024、DB4403/T 271—2022，数据分类分级制度，业务系统（数据库）清单，数据资产分类分级（数据子类或数据字段）清单。 | 公共数据安全等级定级评审记录（基本安全要求）。 |

注：本文件提及的基本安全要求、三级增强安全要求及四级增强安全要求，来源于 DB4403/T 271—2022 第 7 至 9 章对应的安全要求。

5.2 确定数据定级对象

结合 GB/T 43697—2024、DB4403/T 271—2022 相关要求，由数据安全管理机构牵头，组织数据安全岗位人员、数据运营、使用部门，数据合作方，确定数据定级对象，数据定级对象包括数据库和数据子类，也可为数据子类下的具体数据字段，并梳理数据定级对象的信息，包括关联的业务系统名称及其

功能描述、数据库类型及基本信息、IP 地址、网络拓扑、安全防护设备、各类数据处理场景、使用及维护人员、用户群体、可能涉及的重要数据类型、敏感个人信息类型等。数据定级对象涉及的业务、系统、数据、设备、人员、制度、流程等均纳入数据安全体系建设范围。

5.3 分类分级制度制定

数据安全机构制定并发布数据分类分级管理制度（见附录 B），用于指导后续公共数据分类分级及定级评审工作。

5.4 公共数据分类分级

针对待建设的公共数据及关联业务系统，由数据安全机构牵头，数据运营、使用部门及数据合作方采用人工或自动化工具，数据运营、使用部门配合开通网络访问权限，开展资产梳理工作，形成业务系统（数据库）清单及数据资产分类分级（数据子类或数据字段）清单，清单内容参照 DB4403/T 271—2022 附录 A 执行；公共数据分类分级可参照 GB/T 43697—2024、DB4403/T 271—2022 等标准执行，选取合理的分类原则及分级标准：

- a) 采用人工识别公共数据资产类别及级别，数据管理人员对数据库表信息进行人工调研，方式包括人员访谈、问卷调查、上机核查等；
- b) 采用扫描类工具识别公共数据资产类别及级别，基于端口、协议类型的扫描手段梳理目标环境中存在的数据库信息；通过敏感数据特征匹配技术，梳理数据库中存在的资产分布情况及数量；通过数据库信息扫描技术，梳理账户及权限信息；
- c) 建立数据血缘管理工具，通过对元数据管理以历史事实的方式记录每项数据的来源、处理过程、应用对接情况等，记录数据表在治理过程中的全链路血缘关系，基于血缘关系信息，进行数据安全影响分析，如基础数据表需修改字段时，评估其对数据仓库的影响。

5.5 公共数据定级评审

公共管理和服务机构确定数据保护对象安全等级后，组织行政主管部门、数据安全机构、数据运营、使用部门、内部或外部数据安全专家召开内部评审会议，对定级结果的合理性进行评审，出具评审意见，并根据最终定级结果，留存定级评审记录。

6 总体安全规划

6.1 总体安全规划工作流程

6.1.1 根据数据保护对象的定级情况，结合数据类别、关联的业务系统或数据流等情况，通过分析及明确数据保护对象的安全需求，设计合理的、满足安全等级要求的总体安全建设方案，指导后续的安全建设工程实施。

6.1.2 总体安全规划的工作流程及其工作目标、参与角色与阶段输入输出见表 2。

表2 总体安全规划工作流程

| 主要流程 | 工作目标 | 参与角色 | 阶段输入 | 阶段输出 |
|----------|--|--|--|---|
| 安全需求分析 | 根据公共数据保护对象的安全等级,依据 DB4403/T 271—2022 第 7 至 9 章及附录 B. 2,明确安全保护需求,对比差距分析后提出具体可落地的安全建设需求,形成公共数据安全建设总体方案,以便于后续安全建设项目的规划。 | 行政主管部门(可选),数据安全管理机构,数据运营、使用部门,数据合作方(可选)。 | 公共数据及其承载的业务系统、网络、管理、现有安全措施等详细描述文件,公共数据安全等级定级评审记录, DB4403/T 271—2022。 | 公共数据安全需求分析报告(基本安全要求),公共数据安全建设总体方案(基本安全要求)。 |
| 安全建设项目规划 | 依据公共数据保护对象总体安全需求,结合公共管理和服务机构公共数据安全中长期发展规划和安全建设资金状况,设计分期分批建设内容,并将建设内容组合成不同项目,最终确定安全建设项目规划。 | 数据安全管理机构、数据合作方(可选)。 | 公共数据安全需求分析报告,公共数据安全中长期发展规划(如有),公共数据安全建设总体方案。 | 公共数据安全建设项目列表(含建设内容)(基本安全要求),公共数据安全建设项目规划(基本安全要求)。 |

6.2 安全需求分析

本项内容包括:

- a) 数据安全管理机构牵头,组织数据运营、使用部门及数据合作方,依据DB4403/T 271—2022 第7至9章及附录B.2,明确数据保护对象安全需求,形成公共数据安全需求分析报告(见附录B);针对已投入运营、使用的数据保护对象,依据8.2进行差距评估,针对差距点明确具体可落地的安全建设需求;依据表3设定安全建设需求的紧迫度,用于决策计划安排与资源投入比例;

表3 紧迫度说明

| 紧迫度 | 描述 |
|-----|---|
| 高 | 满足以下情况之一,尽快组织落实: 1. 不满足当前法律法规相关要求; 2. 可能影响国家安全或严重损害社会秩序和公共利益; 3. 直接影响公共管理和服务机构生产或运营发展; 4. 可能引发重大数据安全事件,导致大量数据泄露。 |
| 中 | 满足以下情况之一,计划组织落实: 1. 不满足公共数据安全相关标准; 2. 可能影响社会秩序和公共利益、个人信息主体,造成轻微或一般损害; 3. 可能影响公共管理和服务机构生产或运营发展; 4. 可能引发一般数据安全事件,导致少量数据泄露,但不涉及重要数据。 |
| 低 | 满足以下情况之一,有条件落实: 1. 可能影响公共管理和服务机构数据安全能力提升; 2. 可能引发轻微数据安全事件,导致少量不敏感数据泄露。 |

- b) 数据安全管理机构组织数据运营、使用部门依据各项安全建设需求紧迫度及实施难易程度，明确安全需求的建设部门、建设步骤、建设时间、建设预算等；
- c) 公共管理和服务机构依据DB4403/T 271—2022第7至9章及附录B.2，围绕通用管理安全、通用技术安全及数据处理活动安全三方面，结合安全需求分析结果，建立公共数据安全建设的体系框架，形成公共数据安全建设总体方案（见附录B）。

6.3 安全建设项目规划

本项内容包括：

- a) 公共数据安全建设总体方案明确主要的建设内容，涵盖安全基础设施、网络安全、系统平台与应用、标准体系、人员能力等方面，并将其适当分解，主要建设内容可分解但不限于以下内容：
 - 1) 公共数据安全能力，包括公共数据安全管理制度体系、安全管理机构与人员；
 - 2) 公共数据安全技术能力，包括数据分类分级、风险监测、安全管控、应急处置、安全审计；
 - 3) 公共数据处理活动安全能力，包括数据收集、存储、传输、使用、加工、开放共享、交易、出境及销毁与删除。
- b) 将不同建设内容组合成不同安全建设项目，描述不同建设项目解决的主要安全问题及所达到的目标，对项目进行支持或依赖等相关性分析，对项目进行预期效果分析，描述项目具体工作内容及建设方案，形成安全建设项目列表；
- c) 对公共数据安全建设内容、方案等文档进行整理，形成公共数据安全建设项目规划（见附录B）。

7 安全设计与实施

7.1 安全设计与实施工作流程

7.1.1 按照公共数据安全建设总体方案及规划的内容，分期分步落地安全措施，在安全方案详细设计后，通用管理安全、通用技术安全及数据处理活动安全建设过程可同步开展；本章描述整体安全体系建设内容，公共数据保护对象按照实际安全建设需求参考执行。

7.1.2 安全设计与实施的工作流程及其工作目标、参与角色与阶段输入输出见表4。

表4 安全设计与实施工作流程

| 主要流程 | 工作目标 | 参与角色 | 阶段输入 | 阶段输出 |
|----------|--|---|--|-----------------------|
| 安全方案详细设计 | 根据公共数据安全建设总体方案及规划内容,要求将具体建设措施落实在通用管理安全、通用技术安全、数据处理活动安全方面，整理形成文档，使后续建设过程具有依据。 | 数据安全管理机构，数据运营、使用部门，候选数据合作方（含数据安全产品、服务供应商）等。 | 公共数据安全建设总体方案，公共数据安全建设项目规划，各类数据安全产品与服务信息，候选数据合作方评价材料。 | 公共数据安全详细设计方案（基本安全要求）。 |

表4 安全设计与实施工作流程（续）

| 主要流程 | | 工作目标 | 参与角色 | 阶段输入 | 阶段输出 |
|--------------|-----------------|---|---|---|---|
| 通用管理 安全建设 | 安全管理机构与人员的设立 | 公共管理和服务机构建立数据安全管理机构，明确数据安全责任人，通过配备管理机构的人员岗位、人员分工、岗位培训等，保证人员具备其岗位职责匹配的技术及管理能力和能力，从而提供数据安全能力上的保障。 | 数据安全管理机构，数据合作方（可选）等。 | DB4403/T 271—2022，安全管理机构及角色说明书。 | 数据安全管理机构及人员岗位职责说明书（基本安全要求），人员安全管理执行记录，如保密协议、培训记录、考核记录等（基本安全要求）。 |
| | 安全策略与管理制度的建设和修订 | 依据国家数据安全相关政策、标准、规范，制定、修订公共管理和服务机构内部的总体数据安全策略及数据安全管理制度体系，落实公共数据保护配套的数据安全管理、技术及处理活动各环节应遵循的行为规范和操作规程。 | 数据安全管理机构，数据运营、使用部门等。 | 法律法规、政策文件及标准，如DB4403/T 271—2022，公共数据安全详细设计方案，安全管理机构及角色说明书，网络安全管理体系及执行记录文档等。 | 数据安全总体策略（基本安全要求），数据安全管理制度体系（基本安全要求），数据安全管理制度四层文档（三级增强安全要求），数据安全管理制度评审修订记录（基本安全要求），数据安全保护措施执行记录（基本安全要求）。 |
| 通用管理安全建设 | | 根据公共数据安全详细设计方案，通用技术安全建设涵盖数据分类分级、数据安全评估、数据安全风险监测、数据安全管控、数据安全应急处置及数据安全审计六个方面，从安全产品或服务采购、安全控制的开发、安全控制的集成来实现建设所需的功能、性能和安全性。 | 数据安全管理机构，数据运营、使用部门，候选数据合作方（含数据安全产品、服务供应商）等。 | 公共数据安全详细设计方案，各类数据安全产品与服务信息，候选数据合作方评价材料等。 | 需采购的安全产品及服务清单（基本安全要求），安全控制开发过程文档（基本安全要求），安全控制集成报告（基本安全要求）。 |
| 数据处理活动安全建设 | | 根据公共数据安全详细设计方案，数据处理活动安全建设涵盖数据收集、存储、传输、使用、加工、开放共享、交易、出境、销毁与删除9个环节，从制度流程、技术工具及人员能力实现数据处理各环节的安全管理及技术措施落地。 | 数据安全管理机构，数据运营、使用部门，数据合作方（如有）。 | 公共数据安全详细设计方案，各类数据安全产品与服务信息，候选数据合作方评价材料等。 | 数据处理活动安全管理制度及执行过程文档（基本安全要求）、数据处理活动安全技术工具清单（基本安全要求）。 |

7.2 安全方案详细设计

本项内容包括：

a) 通用管理安全的设计

- 1) 从公共管理和服务机构数据安全组织机构设立、职责分工和沟通协作方面考虑，主要涵盖总体数据安全策略、数据安全管理机构与人员方面，公共管理和服务机构制定总体的数据安全策略，明确管理目标、原则、要求等内容，用于指导机构数据安全管理工作；通过正式发文的形式，设立数据安全管理机构，指定数据安全责任人，明确数据安全机构及责任人的职责内容，加强数据安全岗位人员的管理及职责分工，跨部门沟通协作等，具体建设落实指导见 7.3；
- 2) 从公共管理和服务机构数据安全管理制度体系及流程建立、执行落实方面考虑，主要涵盖数据安全管理制度体系方面，公共管理和服务机构建立健全数据安全管理制度体系，通过正式、有效的方式发布管理制度，加强个人信息的保护等，具体建设落实指导见 7.3；
- 3) 通过定期组织数据安全培训、考核、考证，提升内部人员数据安全意识及技术能力，具体建设落实指导见 7.3。

b) 通用技术安全的设计

- 1) 公共管理和服务机构配备相关岗位人员，开展数据安全技术落地工作，定期培养主要涵盖数据分类分级、数据安全评估、数据安全风险监测、数据安全管控、数据安全应急处置及数据安全审计方面，具体建设落实指导见 7.4；
- 2) 公共管理和服务机构制定数据安全技术相关规范，用于指导数据安全岗位人员安全措施的落地工作，数据安全岗位人员依据制定的技术规范，定期执行并留存执行记录文档，主要涵盖数据分类分级、数据安全评估、数据安全风险监测、数据安全管控、数据安全应急处置及数据安全审计方面，具体建设落实指导见 7.4；
- 3) 从公共管理和服务机构具备数据安全技术手段或产品工具落实公共数据安全要求考虑，公共管理和服务机构通过安全功能优化、安全产品部署、配备自动化技术工具等层面，确保安全措施的有效落地，主要涵盖数据分类分级、数据安全风险监测、数据安全管控、数据安全应急处置及数据安全审计方面，具体建设落实指导见 7.4；
- 4) 从公共管理和服务机构数据安全岗位人员的安全意识及相关专业能力考虑，公共管理和服务机构定期开展数据安全岗位人员技术能力培训工作，数据安全岗位人员充分理解并具备数据安全工作落实的能力，主要涵盖数据分类分级、数据安全评估、数据安全风险监测、数据安全管控、数据安全应急处置及数据安全审计方面，具体建设落实指导见 7.4。

c) 数据处理活动安全的设计

- 1) 公共管理和服务机构制定数据处理各项活动规范文档，用于指导数据安全岗位人员安全措施的落地工作，数据安全岗位人员依据制定的规范文档，定期执行并留存执行记录文档，主要涵盖数据收集、存储、传输、使用、加工、开放共享、交易、出境、销毁与删除处理环节，具体建设落实指导见 7.5；
- 2) 公共管理和服务机构通过优化承载公共数据的业务系统数据处理活动过程中的安全功能（如数据加密、完整性校验、数字水印、隐私计算、日志记录等）及配备数据安全产品工具（如数据备份与恢复工具、数据脱敏工具、数字水印工具、自动化审计工具等），提升公共数据处理活动过程中的安全保障能力，主要涵盖数据存储、数据传输、数据使用、数据加工、数据开放共享、数据销毁与删除方面，具体建设落实指导见 7.5；
- 3) 数据安全岗位人员充分理解数据处理活动各环节具备的安全措施，了解相关合规要求，并基于业务建立有效的落地方案及执行，熟练使用相关数据安全技术产品及工具等，主要涵盖数据收

集、存储、传输、使用、加工、开放共享、交易、出境、销毁与删除处理环节，具体建设落实指导见 7.5。

7.3 通用管理安全建设

7.3.1 安全管理机构与人员的设立

7.3.1.1 数据安全管理机构的确立

本项内容包括：

- a) 结合公共管理和服务机构的整体组织架构情况，可常设一个实体或虚拟团队，形成数据安全管理机构，一般可由信息安全管理部的人员组成，落实数据安全保护工作，一般由数据安全管理机构领导承担数据安全责任人的职责；
- b) 依据《中华人民共和国个人信息保护法》，处理个人信息达到国家网信部门规定数量的，指定专门的个人信息保护负责人，落实个人信息安全保护工作，并公开个人信息保护负责人联系方式，将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责部门。

7.3.1.2 角色及岗位职责说明

本项内容包括：

- a) 制定数据安全管理机构及人员岗位职责说明书（见附录B），以书面形式描述数据安全管理机构、数据安全责任人、个人信息保护负责人的责任及权限范围，并征求相关人员的意见，保证责任明确，确保所有风险有人负责应对：
 - 1) 数据安全管理机构职责主要为统筹管理和协调全局数据安全工作，对公共数据安全工作进行整体规划与建设，落实数据安全管理制度体系建设，协同数据运营、使用部门落实数据安全具体的保护工作，留存数据安全制度执行记录等；按照相关法律法规、规章制度的要求编制公共数据资源目录，加强数据安全保护；严格管理数据合作方，与数据合作方签订合作协议及数据安全保密协议，明确双方数据安全保密责任与义务，宜定期审核数据合作方资质背景、数据安全保障能力等，并组织动态合规评估；健全数据安全事项审批程序，针对数据类别级别变更、数据权限变更、重大数据操作及外部系统接入等事项，按照审批程序执行审批过程；针对三级及以上的公共数据保护对象，重大数据处理活动还需建立逐级审批机制，定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；
 - 2) 数据安全责任人职责主要为组织制定数据保护计划并落实，组织开展数据安全影响分析和风险评估，督促整改安全隐患，组织按要求向有关部门报告数据安全保护和事件处置情况，组织受理并处理数据安全投诉和举报事项等；
 - 3) 个人信息保护负责人职责主要为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。
- b) 以书面形式描述数据安全管理机构内部的数据管理员、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；针对四级公共数据保护对象，关键事务岗位配备多人共同管理，从内部人员中选拔从事关键数据岗位的人员。数据安全岗位职责描述包括：
 - 1) 数据管理员负责数据存储、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，可由安全管理员兼任；针对三级及以上的公共数据保护对象，还需配备专职安全管理员承担数据安全管理员工作；
 - 3) 数据安全审计员负责数据安全审计等。

7.3.1.3 人员安全管理

本项内容包括：

- a) 数据安全机构依据人员安全管理制度，对涉及公共数据安全运营及运维的内外部人员加强管理，涉及人员录用、人员培训、人员考核、保密协议、离岗离职、外部人员管理等方面，留存相关执行记录；
- b) 数据安全机构依据人员安全管理制度，与内部数据岗位人员、数据合作方人员签订书面的数据安全保密协议（见附录B），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；
- c) 数据安全机构加强人员数据安全意识及能力培训，依据数据安全教育培训制度（见附录B），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，留存培训记录；针对三级及以上的公共数据保护对象，还需依据不同数据岗位制定不同的培训计划，对数据安全基础知识、岗位操作规程等进行培训，并定期对不同数据岗位人员进行技能考核，留存考核记录文档；
- d) 数据安全机构组织数据岗位人员考取相关资质证书，持证上岗。

7.3.2 安全策略与管理制度的建设和修订

7.3.2.1 制定数据安全总体策略文件

本项内容包括：

- a) 数据安全机构或公共管理服务行政主管等部门等高层领导组织负责制定数据安全总体策略，可在现有网络安全策略基础上进行完善补充，也可单独制定。数据安全策略结合公共管理服务整体情况考虑，既不能对当前业务发展造成严重影响，也需考虑业务长远发展的安全需求，由公共管理和服务机构高层领导组织协商，基于法律法规、政策文件及标准，确定数据安全中长期发展要求。数据安全总体策略的编制、评审、发布具备正式流程，正式发布后组织开展宣贯和解读活动，确保策略的有效性和及时性，此项为基本安全要求；
- b) 定期论证和评审数据安全策略，此项为三级增强安全要求，主要包括：
 - 1) 明确数据安全策略评审频率，如周期性评审、一次性评审、政策法规变动评审、数据安全风险评估发现重大风险事项时评审等；
 - 2) 数据安全策略评审内容，如数据安全策略文件的合理性和完整性，数据安全策略文件落地执行情况等；
 - 3) 数据安全策略评审跟踪验证，如数据安全策略需调整时，由数据安全责任人负责协调处理，动态调整保持适用性。

7.3.2.2 建立健全数据安全管理制度体系

本项内容包括：

- a) 数据安全机构负责建立健全数据安全管理制度体系（见附录B），通过正式、有效的方式发布，如纸质文件印发、办公系统发布、邮件发送等，并对制度版本进行控制，形成版本记录；定期组织制度评审会，对数据安全管理制度文档的合理性及适用性进行论证及修订，保留评审记录表。此项为基本安全要求，主要包括：
 - 1) 数据安全政策；
 - 2) 数据安全管理机构与人员安全管理；
 - 3) 数据分类分级（包括数据分类分级、敏感个人信息安全保护及重要数据安全保护）；

- 4) 数据安全评估;
 - 5) 数据安全风险监测;
 - 6) 数据访问权限管控;
 - 7) 数据安全应急与处置;
 - 8) 数据安全审计;
 - 9) 数据活动安全管理要求（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）;
 - 10) 数据安全教育培训;
 - 11) 数据合作方管理;
 - 12) 个人信息安全保护;
 - 13) 个人信息保护合规制度（针对重要互联网平台、用户数量巨大、业务类型复杂的个人信息处理者）;
 - 14) 投诉、举报受理处置制度;
 - 15) 个人信息主体保护权利渠道和机制等。
- b) 数据安全管理机构负责持续完善数据安全管理制度，形成由安全策略、管理制度、操作规程、记录表单构成的四层数据安全管理制度体系架构，每一层作为上一层的支撑，此项为三级增强安全要求，制度体系架构见图5，具体包括：

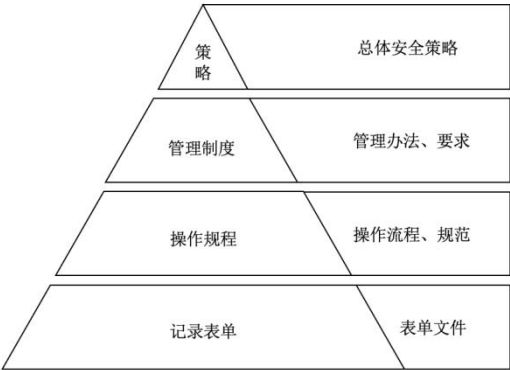


图 5 数据安全管理制度体系架构

- 1) 第一层是安全策略，由高层领导组织形成的决策层牵头指导、编制并发布，明确数据安全工作的总体方针和策略，是数据安全工作的战略导向；
- 2) 第二层是管理制度，由数据安全管理机构形成的管理层牵头编制并发布，是数据安全管理的指导文件，如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、个人信息安全保护等，明确相关角色的权利和义务，面向对象（人员、流程、应用、工具等）提出要求；
- 3) 第三层是操作规程，由数据安全管理机构牵头，组织数据运营、使用部门等涉及公共数据处理的部门，依据二级文件制定的管理办法、要求，制定符合公共数据各类处理场景的操作执行文件，是数据安全落地执行的指南，如建立数据分类分级操作规范、数据安全风险评估规范、数据安全事件应急处置、数据脱敏安全操作规程等；
- 4) 第四层是记录表单，是数据安全运营执行过程中的记录文档，如数据分类分级资产清单、数据访问申请表、数据安全事件报告表、数据安全教育培训签到表等。

7.4 通用技术安全建设

本项内容包括：

a) 安全产品或服务采购：

- 1) 数据安全管理机构配备数据安全管理员负责数据分类分级、数据安全评估、数据安全风险监测、数据安全应急处置、数据安全管控工作；配备数据安全审计员负责数据安全审计工作；
- 2) 数据安全管理机构根据数据分类分级、数据安全评估、数据安全风险监测、数据安全应急处置、数据安全管控、数据安全审计建设落地情况，制定符合公共数据保护对象应用场景的管理规范、操作指引、审批流程、记录及报告模板等文档；
- 3) 根据公共数据安全详细设计方案，从数据分类分级、数据安全评估、数据安全风险监测、数据安全管控、数据安全应急处置及数据安全审计六个方面评估相关产品或服务的采购，明确产品或服务采购的原则、范围、技术指标要求、方式等；对于产品的功能、性能及安全性指标，可依据第三方测试机构所出具的产品测试报告，也可依据公共管理和服务机构自行组织的选型测试结果；对于安全服务的采购，结合数据合作方的评价结果作为参考依据；产品或服务的选择，需考虑使用环境、安全功能、成本（包括采购和维护成本）、易用性、可扩展性、与其他产品或服务的互动和兼容等因素，选择符合网络安全产品使用有关规定的的安全产品，选择符合国家密码管理相关规定的密码产品，选择有相关领域资质的安全服务机构；可能涉及安全产品或服务采购的安全技术建设见表 5；

表 5 安全产品或服务采购

| 建设内容 | 可能涉及的安全产品 | 可能涉及的安全服务 | 建设需求描述 |
|----------|--|---|----------------------------|
| 数据分类分级 | 实现自动化或半自动化数据资产识别及分类分级的平台或工具。 | 通过专家或技术人员人工开展数据分类分级服务工作，输出业务系统（数据库）清单、数据资产分类分级（数据子类或数据字段）清单等。 | 见 5.3。 |
| 数据安全评估 | 通过在数据安全评估工具上实现自行评估，得出评估记录并自行导出评估报告。 | 通过专家或技术人员协助开展数据安全评估服务工作，输出相关评估报告，如数据安全风险评估、数据安全合规性评估、个人信息保护影响评估、数据出境安全评估、移动应用程序个人信息安全评估等。 | 见 8.2。 |
| 数据安全风险监测 | 实现自动化或半自动化数据安全风险监测的平台或工具。 | 通过专家或技术人员协助开展数据安全风险监测运营服务工作，输出数据安全风险监测报告，如驻场安全运营、周期性安全运营等。 | 见 8.3。 |
| 数据安全审计 | 实现自动化或半自动化数据安全审计的平台或工具。 | 通过专家或技术人员协助开展数据安全审计服务工作，输出周期性的数据安全审计报告。 | 见 8.4。 |
| 数据安全应急处置 | 实现数据安全应急处置工单处理的平台或工具。 | 通过专家或技术人员协助开展数据安全事件应急处置工作，输出数据安全事件应急预案、数据安全事件总结分析报告、数据安全事件应急演练方案及报告等。 | 见 8.5。 |
| 数据安全管控 | 实现数据安全访问控制的平台或工具；实现敏感数据防泄漏的平台或工具；实现数据接口安全管理的平台或工具。 | 通过专家或技术人员协助开展数据安全访问控制、数据防泄露、数据接口管理的服务工作，如驻场安全运营，涉及数据账号及权限梳理、敏感数据泄露分析、数据接口资产梳理及安全检测等。 | 见 DB4403/T 271—2022 中 8.4。 |

- 4) 数据安全管理员及数据安全审计员充分理解并熟悉相关技术产品功能、性能、安全性等，在测试产品部署后，经过培训可熟练操作并应用到数据各类场景中，能够进行各类产品或服务选型及测试，对比优劣势。
- b) 安全控制的开发：
 - 1) 数据安全管理机构、数据运营、使用部门组织内部研发人员或外部研发机构，对需安全控制功能开发的应用进行设计、编码、测试及验收；
 - 2) 数据安全管理机构制定开发环境适用的安全管理制度、流程文档，如开发软硬件资源申请、测试数据申请、测试账号申请、开发环境及人员安全管理等；
 - 3) 对于一些不能通过采购现有安全产品来实现的安全措施及功能，可通过专门设计、开发来实现，安全控制的开发应与系统的应用开发同步设计、同步实施；针对运行中的系统应用，则在不影响系统应用正常运行的前提下，对系统应用进行安全控制开发；根据公共数据安全详细设计方案，分析安全控制功能开发需求，并进行概要设计及详细设计，按照设计编码实现，通过安全性测试，实现所需的安全控制功能，最终留存安全控制开发过程文档；可能涉及安全控制功能开发见表 6；

表 6 安全控制功能开发

| 建设内容 | 可能涉及的安全控制功能 | 建设需求描述 |
|----------|--|----------------------------|
| 数据分类分级 | 实现自动化或半自动化数据资产识别及分类分级的功能，涉及数据资产的识别及分类、数据资产的级别划分。 | 见 5.3。 |
| 数据安全评估 | — | — |
| 数据安全风险监测 | 实现自动化或半自动化数据安全风险监测的功能，涉及数据资产识别、数据风险监测及预警等。 | 见 8.2。 |
| 数据安全审计 | 实现自动化或半自动化数据安全审计的平台或工具，涉及数据处理活动各环节审计、数据操作账号审计、数据接口审计、审计日志留存等。 | 见 8.3。 |
| 数据安全应急处置 | — | — |
| 数据安全管控 | 实现数据访问、操作的身份鉴别与权限控制功能；实现敏感数据下载、外发管控功能，包括自动拦截、监测预警、调用审批等；实现数据接口统一安全管理功能，包括接口识别、身份鉴别、安全传输、日志记录等。 | 见 DB4403/T 271—2022 中 8.4。 |

- 4) 开发人员充分理解安全控制功能需求，具备相应的开发能力；测试人员能制定安全功能测试用例，并开展安全功能测试工作，记录测试结果反馈开发人员。
- c) 安全控制的集成：
 - 1) 将不同软硬件产品进行集成，依据安全详细设计方案，将安全产品、开发的安全控制模块与各种公共数据承载的应用进行整合联动，必要时可将安全实施、风险控制、质量控制等有机结合，实现数据安全态势、监测通报预警、应急处置追踪溯源等安全措施，构建统一的数据安全管理平台；

- 2) 数据安全管理员具备数据安全态势分析、风险监测预警及通报、数据安全事件应急处置、流量或日志追踪溯源等能力。

7.5 数据处理活动安全建设

本项内容包括：

- a) 数据安全机构制定数据处理活动安全管理制度（见附录B），围绕数据收集、存储、传输、使用、加工、开放共享、交易、出境、销毁与删除提出安全管理要求；
- b) 数据子类或数据字段安全技术能力建设按照DB4403/T 271—2022中附录B规定的安全要求执行，数据处理活动过程涉及的技术或工具建设内容包括但不限于：
 - 1) 数据收集：具备技术手段对收集的数据进行识别及完整性校验，个人信息收集具备获得个人信息主体明示同意的功能，按照 GB/T 35273—2020 中 5.1 至 5.6 规定的要求开展个人信息收集工作；针对三级及以上的公共数据保护对象，收集外部数据前，采取技术手段保证收集数据的机密性、完整性和可用性；针对数据子类或数据字段，收集前采用身份鉴别技术进行访问控制，记录数据收集日志，按需实现数据分类分级标识功能；
 - 2) 数据存储：具备异地数据备份恢复能力；针对三级及以上的公共数据保护对象，具备异地数据实时备份能力；针对四级公共数据保护对象，具备异地灾难备份中心，实现数据的实时切换能力；个人生物识别信息与个人身份信息分开存储，仅存储个人生物识别信息的摘要信息；超出个人信息存储期限的，如账户注销、系统下线、冗余备份数据、个人信息主体要求删除等场景下，具备数据删除或匿名化处理能力；具备数据处理环节关联信息系统的冗余，涉及软硬件设备及数据；具备勒索病毒事前预警、事中阻断及事后恢复的保障能力；针对 3 至 4 级数据子类或数据字段，在确保不影响系统正常运行前提下，采取符合国家要求的密码算法对数据字段进行加密或摘要值计算后存储；涉及个人生物识别信息，仅存储其摘要信息；按需采用 DBMS 工具字段权限管理模块实现访问控制；
 - 3) 数据传输：数据传输两端具备基于密码技术的通信方实体鉴别，以及数据传输的机密性、完整性保护能力；针对三级及以上的公共数据保护对象，具备关键网络传输线路及核心设备的冗余建设；针对四级的公共数据保护对象，具备数据原发和接收行为的抗抵赖功能；针对数据子类或数据字段，采取符合国家要求的密码技术（如通道加密、内容加密）实现敏感数据安全传输；
 - 4) 数据使用：具备动态或静态脱敏的技术工具，对不同数据使用场景的数据进行脱敏处理；针对三级及以上的公共数据保护对象，大量汇聚数据时具备安全技术措施不暴露敏感数据，具备数字水印技术，对不同数据使用场景实现数据防泄漏及溯源能力；针对数据子类或数据字段，采用动态或静态脱敏、隐私计算技术，实现不同数据场景的安全使用；
 - 5) 数据加工：针对三级及以上的公共数据保护对象，具备对数据加工的过程进行评估与监控的技术能力，对数据加工过程的数据操作行为进行日志记录、审计，对异常数据操作行为（如大批量敏感数据下载、删除、外发等）及时邮件、短信等方式预警与处置（如自动拦截）；加工后产生的新数据，采用安全措施如符合国家要求的密码技术进行安全存储与传输，确保不存在泄露风险；针对数据子类或数据字段，采用动态或静态脱敏、隐私计算技术，实现不同数据场景的安全加工；
 - 6) 数据开放共享：公共数据提供部门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；涉及政务信息的共享，履行 GB/T 39477—2020 第 6 章确定的共享数据安全要求，涉及分类分级、加密、脱敏、身份鉴别、权限管控、防泄漏、备份恢复、操作记录及审计等技术措施；针对三级及以上的公共数据保护对象，宜采取数字水印等技术，确保共享数据可溯源，宜采用多方安全计算、同态加密等数据隐私计算技术实现数据共享的安全性；针对数据子类或数据字段，采用动态或静态脱敏、隐私计算技术，实现不同数据场景的安全开放共享；

- 7) 数据交易：按照相关法律法规、规章制度的要求开展数据交易，加强交易过程的数据安全保护，如数据分类分级、数据加密、数据脱敏、身份认证、入侵防护、安全监测、隐私计算等技术保护措施；针对数据子类或数据字段，采取日志或流量方式记录数据交易过程，确保数据交易可溯源；
 - 8) 数据出境：访问公共数据的境内用户，采取网络技术限制流量路由至境外；
 - 9) 数据销毁与删除：具备数据销毁与删除相关的技术或工具，如物理粉碎、消磁、多次擦写等；针对三级及以上的公共数据保护对象，数据销毁与删除方式确保无法恢复。
- c) 数据处理活动环节人员能力的建设：
- 1) 数据收集：数据安全管理员充分理解数据收集相关法律法规、规章制度要求、安全及业务需求；收集外部机构数据前，能对外部机构数据源的合法性、合规性进行鉴别；对个人信息的收集，能识别是否最小必要收集，是否遵循 GB/T 35273—2020 中 5.1 至 5.6 规定的要求开展个人信息收集工作；
 - 2) 数据存储：数据管理员熟练操作异地数据备份恢复系统，在数据受到侵害时，能实现备份数据的恢复；
 - 3) 数据传输：数据管理员能识别公共数据中涉及的重要数据，采取管理措施，限制相关人员通过离线或即时通信方式传输重要数据；
 - 4) 数据使用：数据安全管理员熟悉并能开展数据安全风险评估工作，在数据公开前，评估公开数据的内容与种类、公开方式、公开范围、安全保障措施、可能的风险与影响范围等；针对三级及以上的公共数据保护对象，数据安全管理员对接入或嵌入的第三方应用具备安全检测能力，确保数据的使用符合双方约定要求；
 - 5) 数据加工：涉及数据加工处理活动，数据安全管理员充分理解数据加工安全及业务需求，具备对参与加工活动的机构或个人进行合法性、正当性的评估能力，并识别加工处理活动是否可能危害国家安全、公共安全、经济安全和社会稳定；针对三级及以上的公共数据保护对象，数据安全管理员具备对加工过程涉及的业务应用、网络环境、终端环境开展安全风险检测的技术能力，确保数据不被泄露、破坏；
 - 6) 数据开放共享：数据安全管理员充分理解公共数据开放共享相关法律要求、安全及业务需求；
 - 7) 数据交易：数据安全管理员充分理解公共数据交易相关法律要求、安全及业务需求；
 - 8) 数据出境：数据安全管理员充分理解公共数据出境相关法律要求、安全及业务需求，熟知国家相关政策法规明确的数据出境安全评估及网络安全审查工作要求；
 - 9) 数据销毁与删除：数据安全管理员充分理解公共数据销毁与删除安全及业务需求，具备数据销毁与删除工具操作能力。

8 安全运行与维护

8.1 安全运行与维护工作流程

8.1.1 安全运行与维护是公共数据安全保护过程中确保安全运行的必要环节，涉及安全运行与维护各项机制的建立，本文件主要关注安全评估、风险监测、安全审计、应急处置及监督检查五个过程，安全运行与维护阶段涉及的其他过程可参照相关标准或指南。

8.1.2 安全运行与维护的工作流程及其工作目标、参与角色与阶段输入输出见表 7。

表 7 安全运行与维护工作流程

| 主要流程 | 工作目标 | 参与角色 | 阶段输入 | 阶段输出 |
|------|--|--|---|---|
| 安全评估 | 基于公共数据保护对象定级情况，依据 DB4403/T 439—2024 安全评估启动条件，开展数据安全评估工作，发生风险并跟踪整改。 | 数据安全管理机构，数据运营、使用部门，数据合作方（可选）。 | 公共数据及其承载的业务系统、网络、管理、现有安全措施等详细描述文件，公共数据安全等级定级报告，业务系统（数据库）清单，数据资产分类分级（数据子类或数据字段）清单，DB4403/T 271—2022，DB4403/T 439—2024。 | 公共数据安全评估报告（基本安全要求），公共数据安全风险清单（基本安全要求），公共数据安全整改建议（基本安全要求）。 |
| 风险监测 | 通过确定公共数据安全风险监测对象，结合以往公共数据安全评估风险清单，配备安全风险监测工具，识别安全风险监测信息，分析发现的数据安全风险，评价风险可能造成的范围、影响程度，形成安全风险监测分析报告，及时预警及通报。 | 数据安全管理机构，数据运营、使用部门。 | 公共数据安全详细设计方案，公共数据安全风险清单。 | 风险监测对象列表（基本安全要求），风险监测状态信息（基本安全要求），风险监测分析报告（基本安全要求）。 |
| 安全审计 | 通过开展数据安全审计工作，识别数据访问与操作违规行为、数据处理活动不合规、数据安全制度体系不完备、制度执行记录缺失等安全问题，持续开展自查及改进工作。 | 数据安全管理机构、数据运营、使用部门。 | 公共数据安全详细设计方案，数据处理活动涉及的业务流量及日志，数据安全管理制度及执行记录等。 | 数据安全审计方案（基本安全要求），数据安全审计报告（基本安全要求）。 |
| 应急处置 | 通过建立完善的应急处置机制，如组建应急组织、配备应急资源、制定应急预案、组织应急培训及演练等，保证数据安全事件的应急工作反应迅速、协调有序。 | 行政主管部门（可选），行业监管部门（可选），数据安全管理机构，数据运营、使用部门及其他关联部门。 | 公共数据安全详细设计方案，数据安全事件应急预案，网络流量与日志信息等。 | 数据安全事件应急预案及培训记录（基本安全要求），数据安全事件应急演练方案及报告（基本安全要求），安全事件上报记录（基本安全要求），安全事件处置报告（基本安全要求），安全事件总结报告（基本安全要求）。 |
| 监督检查 | 公共管理和服务机构按照公共数据安全相关监督检查要求及标准，定期开展监督检查工作，持续提升安全保障能力。 | 行政主管部门（可选），行业监管部门，数据安全管理机构。 | 公共数据安全评估报告，数据安全相关自查报告等。 | 监督检查材料（基本安全要求），监督检查报告（基本安全要求）。 |

8.2 安全评估

本项内容包括：

- a) 由数据安全管理机构牵头，组织数据运营、使用部门，基于公共数据保护对象，梳理数据安全现状，可通过以下维度开展信息调研工作：
 - 1) 数据资产情况：根据公共数据及其承载的业务系统、网络、管理、现有安全措施等详细描述文件、业务系统（数据库）清单、数据资产分类分级（数据子类或数据字段）清单，对公共数据的现状、使用情况进行调研、分析，确定业务的关联关系、访问的关键路径、数据的流向及演变过程等；
 - 2) 组织安全保障能力：对公共数据保护对象涉及的数据安全能力进行调研，包括数据安全组织架构及岗位人员、数据安全管理制度流程、数据安全设备部署情况等，识别现有数据安全技术能力及技术平台策略配置情况，技术能力包括但不限于数据分类分级、数据访问控制、数据风险监测、数据防泄漏、数据加解密、数据脱敏；
 - 3) 数据处理活动情况：识别公共数据保护对象涉及的数据处理活动，如数据收集、存储、传输、使用、加工、开放共享、交易、出境、销毁与删除等，明确数据处理活动中数据安全能力情况。
- b) 由数据安全管理机构牵头，组织数据运营、使用部门、数据合作方，参照DB4403/T 439—2024开展公共数据安全评估工作，输出公共数据安全评估报告及对应的风险清单、整改建议（见附录B）。

8.3 风险监测

本项内容包括：

- a) 确定安全风险监测对象：

依据数据安全风险监测管理制度（见附录B），数据安全管理机构协同数据运营、使用部门对公共数据保护对象可能造成安全风险的关键要素进行分析，确定安全风险监测的对象，可能包括但不限于承载公共数据的业务应用系统与接口、主机系统、终端系统、网络系统、安全产品，也可能涉及外部机构业务应用系统；根据确定的监测对象，分析监测的必要性、可行性、成本等因素，形成监测对象列表；

- b) 安全风险监测状态信息收集：

- 1) 针对三级及以上的公共数据保护对象，公共管理和服务机构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，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；
- 2) 针对三级及以上的公共数据保护对象，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；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；
- 3) 公共管理和服务机构配备自动化安全风险监测工具或安全风险检测人员，明确监测工具部署方式、安全风险监测范围、风险类型及等级、涉及的数据类型及数量等，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；收集安全风险监测状态信息，包括网络流量、日志信息、安全报警和性能状况等；
- 4) 数据安全管理员熟练使用安全风险监测工具，对工具收集的安全风险监测状态信息进行初步梳理及筛选；如未配备自动化安全风险监测工具，则数据安全管理员具备人工安全风险检测技术能力，定期采用安全漏洞扫描、渗透测试、人工流量及日志审计手段，收集安全风险检测状态信息。

- c) 监测状态分析和报告：

- 1) 公共管理和服务机构配备自动化安全风险监测工具，对监测的安全风险识别与评价，及时触发告警，导出安全风险监测分析报告；

- 2) 数据安全管理员通过工具或人工方式，对收集的安全风险监测状态信息进行影响分析，根据监测的安全风险类型、关联的数据类型及数量、影响程度，判断安全风险等级，以确定是否有必要做出响应，做到安全风险闭环管理，最终输出风险监测分析报告（见附录 B）。

8.4 安全审计

本项内容包括：

a) 确定数据安全审计对象：

- 1) 数据安全管理机构制定数据安全审计制度（见附录 B），审计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，明确审计目的、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，审计周期为每年至少一次，审计方式包括现场座谈、调阅资料、技术检测等；
- 2) 数据安全审计员能明确数据安全审计的对象，涉及公共数据访问及操作行为、数据安全事件、数据处理活动安全合规、数据安全管理制度及执行记录等；针对三级及以上的公共数据保护对象，审计对象涉及数据账号操作及应用接口调用情况；熟悉数据安全审计流程、内容，编制数据安全审计方案。

b) 数据安全审计分析：

- 1) 公共管理和服务机构配备数据安全审计相关工具，明确审计工具的部署方式、审计范围、审计策略、审计结果等，审计结果保存不少于 180 天；数据安全审计相关工具具备审计数据处理活动涉及的业务流量或操作日志功能，发现可能存在的内外部违规操作行为、数据安全事件，针对三级及以上的公共数据保护对象，还能审计数据账号操作及应用接口调用情况；
- 2) 数据安全审计员熟练使用数据安全审计相关工具，基于工具的审计结果，评价审计结果的真实性；数据安全审计员充分理解公共数据安全相关法律法规、标准规范要求，具备人工审计数据处理活动合规性、数据安全制度体系及执行过程完备性的能力。

c) 数据安全审计报告：

- 1) 公共管理和服务机构配备数据安全审计相关工具，具备审计告警功能，可筛选时间段导出安全审计报告；
- 2) 数据安全管理员根据审计分析结果进行影响分析，评价安全问题影响程度，确定是否有必要做出响应，做到安全审计问题闭环管理，最终输出周期性数据安全审计报告（见附录 B），每年至少一次。

8.5 应急处置

8.5.1.1 应急准备

本项内容包括：

a) 公共管理和服务机构依据本市、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，包括但不限于：

- 1) 建立应急组织，包括应急管理的领导机构、办事机构、专项应急指挥机构、基层应急机构、应急专家组及数据合作方应急人员等，明确相关职责和权限、各机构之间的合作和分工协调方式；
- 2) 公共管理和服务机构针对各类专项应急预案，配备应急预案执行所需通信、装备、数据、队伍、交通运输、经费和治安等保障资源；
- 3) 公共管理和服务机构定期组织应急培训，制定专项培训计划，宣贯应急职责、合作与分工、应急预案启动条件和流程等；

- 4) 公共管理和服务机构定期开展应急演练, 制定数据安全事件应急演练方案(见附录B), 明确应急预案演练规模、方式、范围、内容、组织、评估总结等内容, 应急演练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, 输出数据安全事件应急演练报告(见附录B)。
- b) 数据安全管理机构制定数据安全事件应急预案(见附录B), 应急预案内容包括但不限于应急组织及工作职责、数据安全事件分类分级、监测与预警、应急响应及处置、应急资源保障、应急培训及演练、应急联系方式, 参考文件包括但不限于:
 - 1) 数据安全事件应急预案宜参考《国家网络安全事件应急预案》、《深圳市数字政府网络安全和数据安全事件应急预案》;
 - 2) 数据安全事件分类分级宜参考《国家网络安全事件应急预案》中1.4及附件1、GB/T 20986—2023的第5至6章、《深圳市数字政府网络安全和数据安全事件应急预案》的第1.4至1.5;
 - 3) 数据安全事件应急演练宜参考GB/T 38645—2020的第4至9章。
- c) 应急组织机构人员充分理解并熟悉应急职责、合作与分工、流程、处置措施等内容。

8.5.1.2 应急监测与响应

本项内容包括:

- a) 数据安全管理机构依据数据安全事件应急预案, 明确安全事件上报情形, 包括但不限于:
 - 1) 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, 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, 并主动报告有关行政主管部门, 必要时向市网信部门报告;
 - 2) 发生数据泄露、毁损、丢失、篡改等数据安全事件时立即启动应急预案, 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、公安部门和有关行政主管部门报告;
 - 3) 针对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, 及时上报关键信息基础设施安全保护工作部门。
- b) 数据安全事件应急处置过程中, 采取相关日志、流量分析工具或人工方式对事件的日志或流量关联分析进行溯源, 造成严重事件的应追溯到事件主体; 针对三级及以上的公共数据保护对象, 日志记录能完整跟踪和记录数据收集、分析、加工、挖掘等过程, 保证在发生事件时溯源数据能重现相应过程; 针对四级的公共数据保护对象, 数据处理活动关联系统具备确保溯源数据真实性和保密性的能力;
- c) 数据安全事件应急人员具备应急监测与响应能力, 包括但不限于:
 - 1) 基于网络流量、日志信息、安全告警、性能状况、来自外部安全标准与法律法规变更信息、安全预警信息等, 及时发现安全风险、事件, 记录并分析影响程度, 判断是否有必要做出响应、处置及上报;
 - 2) 具备安全事件处置能力, 根据安全事件等级, 制定安全事件处置方案, 包括安全事件处置方法以及应采取的措施等, 并按照流程进行处置;
 - 3) 在安全事件得到解决后, 对于未知事件进行事件记录, 分析事件发生原因, 总结应急处置经验, 记录信息并补充所需信息, 使安全事件成为已知事件并文档化, 对安全事件处置过程进行总结, 制定安全事件处置报告并保存。

8.5.1.3 后期评估与改进

本项内容包括:

- a) 数据安全管理机构基于数据安全事件处置报告、数据安全应急演练报告, 不断检验和完善应急处置机制, 更新数据安全事件应急预案版本;

- b) 数据安全事件应急人员能根据应急响应过程，评估应急过程的合理性、处置及时性等，调查事件原因，追溯安全责任，形成安全调查评估结果，输出安全事件总结报告。

8.6 监督检查

行政主管部门、行业监管部门依据公共数据安全相关要求制定数据安全监督检查方案；数据安全管理机构依据公共数据安全监督检查方案、标准规范，准备相应的监督检查所需材料，如数据安全管理机构组织架构及岗位设立描述文档、数据安全管理制度体系及执行过程记录、数据安全技术体系建设现状等。

9 定级对象终止

9.1 定级对象终止工作流程

9.1.1 定级对象终止阶段是公共数据保护对象实施过程的最后环节，当定级对象处于被转移、终止或废弃等情形，采取合理的方式处理存储的敏感数据，该阶段关注数据销毁与删除活动中，对数据合理处理的过程。

9.1.2 定级对象终止的工作流程及其工作目标、参与角色与阶段输入输出见表 8。

表 8 定级对象终止工作流程

| 主要流程 | 工作目标 | 参与角色 | 阶段输入 | 阶段输出 |
|---------|---|----------------------------|--------------------|--|
| 数据销毁与删除 | 公共数据保护对象因组织解散、业务终止等原因，在符合相关政策法规、协议约定的情况下，可能面临数据销毁或删除的情况，需要采取合理的方法进行数据销毁与删除。 | 数据安全管理机构，数据运营、使用部门及其他关联部门。 | 待销毁、删除的设备、介质及数据清单。 | 数据销毁与删除规程（基本安全要求），数据销毁、删除处理记录文档（基本安全要求）。 |

9.2 数据销毁与删除

本项内容包括：

- a) 识别销毁与删除的数据资产：
 - 1) 数据安全管理机构 制定数据销毁与删除规程（见附录 B），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；数据销毁与删除的场景包括但不限于组织解散、业务终止、过多备份、数据超出保存期限、用户退出服务、节点失效、数据试用结束、委托处理活动结束后、约定删除数据、数据迁移或暂存（如业务运营需要、软硬件升级、备份恢复、存储介质故障、业务改造、存储环境变更等）、GB/T 35273—2020 中 8.3 规定个人信息删除情形；
 - 2) 负责数据销毁、删除的人员根据不同场景，识别待销毁、删除的数据资产，如设备、存储介质、数据、对应负责人、所处位置以及当前的状态等，列出清单。
- b) 数据的销毁与删除：
 - 1) 根据数据销毁、删除的不同场景，不同类型的存储介质（闪存、移动硬盘、固态硬盘、硬盘、磁带、光盘等），采用物理破坏（如高压击穿、粉碎）、消磁（如消磁机）、覆写（如数据覆写软件）、销毁密钥、执行固件擦除命令等方式，将数据进行销毁、删除；针对三级及以上的公共数据保护对象，在境内对数据采取无法恢复的方式完成销毁、删除操作；

- 2) 负责数据销毁、删除的人员熟练使用数据销毁、删除相关工具，熟悉销毁、删除流程。
- c) 负责数据销毁、删除的人员对数据销毁、删除操作过程进行记录，留存记录文档。

附 录 A
(规范性)
主要过程及其活动和输入输出

公共数据安全建设工作的主要过程及其活动和输入输出见表 A. 1。

表 A. 1 主要过程及其活动和输入输出

| 主要阶段 | 主要过程 | 活动 | 活动输入 | 活动输出 |
|--------|----------|----|--|--|
| 公共数据定级 | 确定数据定级对象 | | 法律法规、政策文件及标准，如 GB/T 43697—2024、DB4403/T 271—2022 | 数据定级对象描述文件（基本安全要求） |
| | 分类分级制度制定 | | 法律法规、政策文件及标准，如 GB/T 43697—2024、DB4403/T 271—2022 | 数据分类分级管理制度（基本安全要求） |
| | 公共数据分类分级 | | 数据分类相关标准规范，如 GB/T 43697—2024、DB4403/T 271—2022 公共数据承载系统开发建设文档、数据库表信息 其他相关数据分类分级文件、工具 | 业务系统（数据库）清单（基本安全要求） 数据资产分类分级（数据子类或数据字段）清单（基本安全要求） 数据血缘管理工具（四级增强安全要求） |
| | 公共数据定级评审 | | 法律法规、政策文件及标准，如 GB/T 43697—2024、DB4403/T 271—2022 数据分类分级制度 业务系统（数据库）清单 数据资产分类分级（数据子类或数据字段）清单 | 公共数据安全等级定级评审记录（基本安全要求） |
| 总体安全规划 | 安全需求分析 | | 公共数据及其承载的业务系统、网络、管理、现有安全措施等详细描述文件 数据安全评估报告 数据安全风险清单 数据安全整改建议 DB4403/T 271—2022 | 公共数据安全需求分析报告（基本安全要求） 公共数据安全建设总体方案（基本安全要求） |
| | 安全建设项目规划 | | 公共数据安全需求分析报告 公共数据安全中长期发展规划（如有） 公共数据安全建设总体方案 | 公共数据安全建设项目列表（含建设内容）（基本安全要求） 公共数据安全建设项目规划（基本安全要求） |

表 A.1 主要过程及其活动和输入输出（续）

| 主要阶段 | 主要过程 | 活动 | 活动输入 | 活动输出 |
|---------|------------|-----------------|--|--|
| 安全设计与实施 | 安全方案详细设计 | 通用管理安全的设计 | 公共数据安全建设总体方案 公共数据安全建设项目规划 各类数据安全产品与服务信息 候选数据合作方评价材料 | 公共数据安全详细设计方案（基本安全要求） |
| | | 通用技术安全的设计 | | |
| | | 数据处理活动安全的设计 | | |
| | 通用管理安全建设 | 安全管理机构与人员的设立 | DB4403/T 271—2022 安全管理机构及角色说明书 | 数据安全管理机构及人员岗位职责说明书（基本安全要求） 人员安全管理执行记录，如保密协议、培训记录、考核记录等（基本安全要求） |
| | | 安全策略与管理制度的建设和修订 | 法律法规、政策文件及标准，如 DB4403/T 271—2022 公共数据安全详细设计方案 安全管理机构及角色说明书 网络安全管理体系及执行记录文档等 | 数据安全总体策略（基本安全要求） 数据安全管理制度体系（基本安全要求） 数据安全管理制度四层文档（三级增强安全要求） 数据安全管理制度评审修订记录（基本安全要求） 数据安全管理制度执行记录（基本安全要求） |
| | 通用技术安全建设 | 安全产品或服务采购 | 公共数据安全详细设计方案 各类数据安全产品与服务信息 候选数据合作方评价材料等 | 需采购的安全产品及服务清单（基本安全要求） |
| | | 安全控制的开发 | | 安全控制开发过程文档（基本安全要求） |
| | | 安全控制的集成 | | 安全控制集成报告（基本安全要求） |
| | 数据处理活动安全建设 | | 公共数据安全详细设计方案 各类数据安全产品与服务信息 候选数据合作方评价材料等 | 数据处理活动安全管理制度及执行过程文档（基本安全要求） 数据处理活动安全技术与工具清单（基本安全要求） |

表 A.1 主要过程及其活动和输入输出（续）

| 主要阶段 | 主要过程 | 活动 | 活动输入 | 活动输出 |
|-------------|----------|--------------|---|--|
| 安全运行 与维护 | 公共数据安全评估 | | 公共数据及其承载的业务系统、网络、管理、现有安全措施等详细描述文件 公共数据安全等级定级报告 业务系统（数据库）清单 数据资产分类分级（数据子类或数据字段）清单 DB4403/T 271—2022 DB4403/T 439—2024 | 公共数据安全评估报告（基本安全要求） 公共数据安全风险清单（基本安全要求） 公共数据安全整改建议（基本安全要求） |
| | 风险监测 | 确定安全风险监测对象 | 公共数据安全详细设计方案 | 风险监测对象列表（基本安全要求） |
| | | 安全风险监测状态信息收集 | | 风险监测状态信息（基本安全要求） |
| | | 监测状态分析和报告 | | 风险监测分析报告（基本安全要求） |
| | 安全审计 | 确定数据安全审计对象 | 公共数据安全详细设计方案 数据处理活动涉及的业务流量及日志 数据安全管理制度及执行记录等 | 数据安全审计方案（基本安全要求） |
| | | 数据安全审计分析 | | 数据安全审计报告（基本安全要求） |
| | | 数据安全审计报告 | | |
| | 应急处置 | 应急准备 | 公共数据安全详细设计方案 数据安全事件应急预案 网络流量与日志信息等 | 数据安全事件应急预案及培训记录（基本安全要求） 数据安全事件应急演练方案及报告（基本安全要求） |
| | | 应急监测与响应 | | 安全事件上报记录（基本安全要求） 安全事件处置报告（基本安全要求） |
| | | 后期评估与改进 | | 安全事件总结报告（基本安全要求） |
| | 监督检查 | | 公共数据安全评估报告 数据安全相关自查报告等 | 监督检查材料（基本安全要求） 监督检查报告（基本安全要求） |
| 定级对象 终止 | 数据销毁与删除 | | 待销毁、删除的设备、介质及数据清单 | 数据销毁与删除规程（基本安全要求） 数据销毁、删除处理记录文档（基本安全要求） |

附 录 B
(资料性)
公共数据安全制度内容说明

公共数据安全制度内容说明见表 B. 1。

表 B. 1 公共数据安全制度内容说明

| 主要阶段 | 制度名称 | 内容说明 |
|--------|--------------------|--|
| 公共数据定级 | 数据分类分级管理制度 | <ul style="list-style-type: none">● 公共数据分类分级的目的、原则、范围、定义、权责；● 公共数据分类分级的标准程序和操作指南；● 不同级别数据安全保障要求；● 公共数据类别和级别的变更审批流程及要求。 |
| | 公共数据安全等级定级 评审记录 | <ul style="list-style-type: none">● 公共数据保护对象概述，例如数据类别及量级、关联业务系统或数据流、关联部门、边界等；● 公共数据保护对象定级说明，如定级依据、初步定级结果、评审意见、最终定级结果等。 |
| 总体安全规划 | 公共数据安全需求分析 报告 | <ul style="list-style-type: none">● 引言，如背景、目标、依据等，概述数据安全需求分析的重要性；● 需求概述，对数据安全需求的总体描述；● 公共数据安全评估现状，涉及通用管理安全、通用技术安全、数据处理活动安全；● 公共数据安全具体需求分析，列出安全需求项，并进行详细说明，设定需求的紧迫度；● 计划与实施建议，给出数据安全需求的实施计划和建议，包括时间安排、资源需求和关键任务；● 总结，对整个报告进行总结，提出数据安全的建议和改进措施。 |
| | 公共数据安全建设总体 方案 | <ul style="list-style-type: none">● 引言，如建设背景与目标、建设依据、建设原则等，概述组织机构业务特点及数据安全挑战；● 建设内容，给出整体的建设框架图，依据各项安全建设需求紧迫度及实施难易程度，分期建设，明确安全需求的建设部门及负责人、建设时间等；● 建设可行性分析；● 建设效益分析。 |

表 B.1 公共数据安全制度内容说明（续）

| 主要阶段 | 制度名称 | 内容说明 |
|---------|--------------------|---|
| 总体安全规划 | 公共数据安全建设项目规划 | <ul style="list-style-type: none"> ● 规划建设的依据和原则； ● 规划建设的目标和范围； ● 公共数据保护对象安全现状； ● 公共数据安全中长期发展规划； ● 公共数据安全建设体系框架； ● 公共数据安全建设规划 ● 公共数据安全建设技术规划； ● 公共数据处理活动安全建设规划； ● 安全建设项目投资估算； ● 其他。 |
| 安全设计与实施 | 数据安全管理机构及人员岗位职责说明书 | <ul style="list-style-type: none"> ● 数据安全组织与职责； ● 数据安全岗位设置； ● 数据安全人员管理，如背景调查、签署保密协议、日常安全管理、调离岗管理、人员考核、外部人员管理、数据安全培训等。 |
| | 数据安全保密协议 | <ul style="list-style-type: none"> ● 保密内容、范围及权限； ● 人员调离岗保密要求； ● 保密期限； ● 违约责任； ● 纠纷解决途径等。 |
| | 数据安全教育培训 | <ul style="list-style-type: none"> ● 教育培训目标，如明确数据安全教育培训的目标和重要性，强调员工对数据安全的责任和义务； ● 教育培训计划，如制定针对不同岗位和职责的教育培训计划，确定培训内容、形式和频率； ● 培训课程内容，如数据安全基础知识、数据安全政策法规标准规范、数据安全意识、数据安全技能等； ● 培训形式，如在线培训、现场培训； ● 培训资源和材料，如培训资料、手册、宣传海报、PPT 等； ● 考核与认证，如设立培训考核机制，测试、问卷调查等方式进行考核评估；或组织培训认证，获取数据安全资质证书； ● 培训记录和统计，如记录培训过程、统计培训效果、参与率等； ● 管理责任和监督，如确定责任部门和人员、建立监督机制。 |

表 B.1 公共数据安全制度内容说明（续）

| 主要阶段 | 制度名称 | 内容说明 |
|---------|--------------|---|
| 安全设计与实施 | 数据安全总体策略 | <ul style="list-style-type: none"> ● 公共数据安全目标； ● 公共数据安全原则，如定义数据合法合规原则、业务发展原则等； ● 公共数据分类分级策略，如定义数据分类分级原则、分类分级方法、分类分级指导文件以及分类分级管控措施等； ● 公共数据处理活动范围，如定义数据处理活动和场景，包括但不限于收集、存储、传输、使用、加工、开放共享、交易、出境、销毁与删除； ● 个人信息保护策略，如定义个人信息处理遵循知情同意、目的明确、安全保护等原则； ● 数据安全违规处理，如定义数据安全违规事件等级、影响程度，相应处罚规定等； ● 第三方供应链管理策略，如第三方数据开放权限、管控措施、审查手段等； ● 数据安全应急处置流程，如针对不同重要程度的数据安全事件，对应的处置措施。 |
| | 敏感个人信息保护管理制度 | <ul style="list-style-type: none"> ● 个人信息保护目的、原则、范围、定义、权责等； ● 个人信息在采集、使用等过程中的要求、规范； ● 个人信息保护的保障措施； ● 个人信息保护监督检查策略，投诉、举报受理策略。 |
| | 重要数据安全保护管理制度 | <ul style="list-style-type: none"> ● 重要数据保护目的、原则、范围、定义、权责等； ● 重要数据识别原则、识别流程； ● 重要数据在采集、使用等过程中的要求、规范； ● 重要数据安全事件上报机制。 |
| | 数据合作方管理制度 | <ul style="list-style-type: none"> ● 数据合作方审查，如合作方背景、安全资质、数据安全保障能力等； ● 数据合作方安全管理要求，如安全培训与宣贯、签署保密承诺书、第三方人员访问权限管理、离场安全管理、问责与处置等。 |
| | 投诉、举报受理处置制度 | <ul style="list-style-type: none"> ● 投诉、举报处置目的、依据、原则； ● 投诉、举报受理渠道，如官网、移动应用程序、公众号、电话热线等； ● 投诉、举报受理责任部门和人员； ● 投诉、举报受理处置措施； ● 投诉、举报受理反馈等。 |

表 B.1 公共数据安全制度内容说明（续）

| 主要阶段 | 制度名称 | 内容说明 |
|---------|------------------|--|
| 安全设计与实施 | 个人信息保护合规制度 | <ul style="list-style-type: none"> ● 个人信息保护目的、依据、原则； ● 个人信息处理内容，如个人信息收集、存储、使用、加工、传输、提供、公开、删除等，提供合规处理的要求； ● 个人信息处理规则； ● 敏感个人信息处理规则； ● 个人信息跨境提供规则（如有）； ● 责任与义务。 |
| | 数据安全开发管理制度 | <ul style="list-style-type: none"> ● 安全开发目的、依据、原则； ● 安全开发责任部门和人员； ● 开发资源申请管理，如开发软硬件资源、测试数据、测试账号、开发环境、开发人员等； ● 安全编码管理，如开发人员遵循安全编码规范，避免业务逻辑漏洞，正确处理敏感数据等； ● 安全测试管理，如人工安全检测、工具扫描，识别潜在的安全问题和风险，并提供改进建议； ● 开发测试人员安全管理，如内外部人员的安全管理； ● 开发测试环境管理，如物理环境、网络环境、终端环境等； ● 试运行安全管理； ● 安全发布和部署，如正确配置、加密传输、权限管理等； ● 验收管理，如系统验收、开发过程文档验收等。 |
| | 数据处理活动安全管理 制度 | <ul style="list-style-type: none"> ● 数据收集：明确数据类型及收集渠道、目的、用途、范围、频度、方式等； ● 数据存储：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；明确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； ● 数据传输：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； ● 数据使用：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；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；根据不同数据使用场景明确安全处理措施（如去标识化、匿名化等），降低数据敏感度及暴露风险； |

表 B.1 公共数据安全制度内容说明（续）

| 主要阶段 | 制度名称 | 内容说明 |
|---------|--------------|---|
| 安全设计与实施 | 数据处理活动安全管理制度 | <ul style="list-style-type: none"> ● 数据加工：数据加工前，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；委托他人加工处理数据的，签订的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，书面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；加工重要数据的，建立登记、审批机制并留存记录； ● 数据开放共享：公共数据提供部门与公共数据使用部门签署相关协议，书面明确数据使用目的、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；公共数据提供部门建立内部审批机制，明确数据对外共享目的、范围、期限、频次等内容； ● 数据交易：按照相关法律法规、规章制度的要求开展数据交易，明确交易过程的数据安全保护要求，如建立数据安全交易管理体系、数据分类分级管理、数据处理活动安全管理、数据安全人员管理、数据安全事件应急机制等； ● 数据出境：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监管要求，符合国家法律、行政法规规定情形的，明确提前开展数据出境安全评估及网络安全审查工作，严禁未经授权数据出境行为；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； ● 数据销毁与删除：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；针对三级及以上的公共数据保护对象，明确规定在中国境内对介质存储的数据进行销毁或删除。 |
| 安全运行与维护 | 公共数据安全评估报告 | <ul style="list-style-type: none"> ● 项目概述，如评估背景、目标、依据、过程； ● 评估对象描述，如被评估机构描述、系统描述； ● 评估指标，如基本评估指标、不适用评估指标； ● 单项评估情况，如通用管理安全、通用技术安全、数据处理活动安全； ● 整体评估，如评估子项、评估子项间、评估类、整体评估； ● 评估结论； ● 安全问题及整改建议； ● 附录 A：公共数据安全评估表； ● 附录 B：技术安全监测结果。 |

表 B.1 公共数据安全制度内容说明（续）

| 主要阶段 | 制度名称 | 内容说明 |
|---------|--------------|---|
| 安全运行与维护 | 数据安全风险监测管理制度 | <ul style="list-style-type: none"> ● 数据安全风险监测目的、依据、原则； ● 数据安全风险监测对象、方法，如监测工具、监测范围； ● 数据安全风险监测内容，如数据流转轨迹异常、数据操作行为异常、数据访问身份异常等； ● 数据安全风险监测预警机制； ● 数据安全风险监测上报机制等。 |
| | 风险监测分析报告 | <ul style="list-style-type: none"> ● 工作概述，如工作内容、监测工具部署位置、方式等； ● 数据安全监测运营概览，如监测资产范围、监测运营统计、风险趋势等； ● 数据安全监测运营详情，如数据安全风险、数据安全预警、数据安全事件等； ● 总结与整改建议。 |
| | 数据安全审计制度 | <ul style="list-style-type: none"> ● 数据安全审计概述，如背景、目的、原则等； ● 数据安全审计组织与职责； ● 数据安全审计周期、内容与要求； ● 数据安全审计方式与流程； ● 数据安全审计处理与后续跟踪等。 |
| | 数据安全审计报告 | <ul style="list-style-type: none"> ● 审计目标和范围，如数据安全审计的目标、范围和时间段，明确对哪些方面进行了审查和评估； ● 审计方法和程序，如数据安全审计使用的方法和程序，包括风险评估、检查和测试等具体操作步骤； ● 审计问题和风险，如审计过程中发现的安全问题、漏洞和潜在风险，详细描述每个问题的影响程度和建议的解决方法； ● 合规性审计，如评估是否符合相关法律法规和行业标准； ● 安全事件和违规审计，如审计过去一个周期内发生的安全事件、违规行为和数据泄露等情况，并分析其原因和影响； ● 内部安全管理执行落实情况审计，如审计过去一个周期内组织内部对安全管理制度执行及记录情况； ● 建议和改进措施，如提供针对发现的安全问题和风险的建议和改进措施，以加强数据安全控制和管理； ● 审计记录和意见，如总结整个审计过程的结果，提供对组织或系统数据安全状况的评估，包括强调优点、指出不足和给出建议。 |

表 B.1 公共数据安全制度内容说明（续）

| 主要阶段 | 制度名称 | 内容说明 |
|---------|--------------|--|
| 安全运行与维护 | 数据安全事件应急预案 | <ul style="list-style-type: none"> ● 总则，如编制目的、依据、事件定义和分类、事件分级、适用范围、工作原则； ● 组织机构和职责； ● 监测与预警，如风险管理、监测、预警分级、预警研判与发布、预警响应、预警接触； ● 应急响应及处置，如先期处置、事件报告、应急响应、响应升级、应急结束、善后与恢复； ● 调查评估与事件总结； ● 预防工作，如日常管理、应急演练、培训； ● 应急资源保障，如机构与人员、技术支撑队伍、物资保障、经费保障、责任与奖惩； ● 相关附件与模板，如技术支撑队伍通讯表、安全事件上报记录、安全事件处置报告、安全事件总结报告等。 |
| | 数据安全事件应急演练方案 | <ul style="list-style-type: none"> ● 演练目标和范围，如明确演练的目标、范围和参与人员，包括内部员工、相关部门、外部合作伙伴等；明确应急演练的场景； ● 应急响应团队，如确定并指派应急响应团队成员，包括负责人、技术专家等，并明确各自的职责和权限； ● 事件识别和报告，如根据不同演练场景设立明确的事件识别和报告机制，包括如何发现和确认安全事件，并迅速汇报给应急响应团队； ● 紧急处置和隔离，如建立紧急处置和隔离措施，包括暂停受影响系统、断开网络连接、备份关键数据等，以防止事件的进一步扩散和损害； ● 事故调查和分析，如安排专业人员进行安全事件的调查和分析，确定事件的起因、范围和影响，并收集证据以备日后追溯和法律诉讼需要； ● 通信与沟通，如建立有效的内部和外部沟通渠道，包括应急响应团队之间的协作、上级领导和相关利益方的沟通，以及与媒体和用户的适时沟通； ● 修复和恢复，如制定相应的修复措施，并确保及时执行修复工作，以恢复受影响系统和数据的正常运行； ● 事后总结和改进，如对演练过程进行评估和总结，发现问题和不足，并提出改进意见和措施，以提高应急响应能力和防范措施； ● 更新和培训，如根据演练过程中的反馈和改进意见，及时更新应急响应计划和培训材料，加强员工的安全意识和技能； ● 相关附件与模板，如演练脚本、演练报告模板等。 |

表 B.1 公共数据安全制度内容说明（续）

| 主要阶段 | 制度名称 | 内容说明 |
|---------|--------------|---|
| 安全运行与维护 | 数据安全事件应急演练报告 | <ul style="list-style-type: none"> ● 演练背景、目的； ● 演练基本情况，如演练时间与地点、演练单位及人员、演练内容、演练平台与场景、应急响应流程； ● 应急演练过程，如演练环境说明、演练准备阶段、发现阶段、启动阶段、检测阶段、抑制阶段、根除阶段、恢复阶段、结束阶段； ● 问题和改进建议，如演练出现的不足之处和建议； ● 总结和结论，如总结演练整体效果、成果、改进空间、下一步计划。 |
| 定级对象终止 | 数据销毁与删除操作规程 | <ul style="list-style-type: none"> ● 数据销毁与删除场景，如组织解散、业务终止、过多备份、数据超出保存期限、用户退出服务、节点失效、数据试用结束、委托处理活动结束后、约定删除数据、数据迁移或暂存、GB/T 35273—2020 中 8.3 规定个人信息删除情形； ● 数据销毁与删除方式，如物理破坏（如高压击穿、粉碎）、消磁（如消磁机）、覆写（如数据覆写软件）、删除密钥、执行固件擦除命令等方式； ● 数据销毁与删除审批机制，设置相关监督角色，记录数据销毁与删除操作过程。 |

参 考 文 献

[1] GB/T 20984—2022 信息安全技术 信息安全风险评估方法

[2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

[3] GB/T 25058—2019 信息安全技术 网络安全等级保护实施指南

[4] GB/T 37964—2019 信息安全技术 个人信息去标识化指南

[5] GB/T 37973—2019 信息安全技术 大数据安全管理指南

[6] GB/T 38645—2020 信息安全技术 网络安全事件应急演练指南

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

[8] GB/T 41479—2022 信息安全技术 网络数据处理安全要求

[9] GB/T 41817—2022 信息安全技术 个人信息安全工程指南

[10] JR/T 0171—2020 个人金融信息保护技术规范

[11] JR/T 0223—2021 金融数据安全 数据全生命周期安全规范

[12] YD/T 3813—2020 基础电信企业数据分类分级方法

[13] YD/T 3956—2021 电信网和互联网数据安全评估规范

[14] 中华人民共和国第十二届全国人民代表大会常务委员会. 中华人民共和国网络安全法. 2016年

[15] 中华人民共和国第十三届全国人民代表大会常务委员会. 中华人民共和国数据安全法. 2021年

[16] 中华人民共和国第十三届全国人民代表大会常务委员会. 中华人民共和国个人信息保护法. 2021年

[17] 深圳市第七届人民代表大会常务委员会. 深圳经济特区数据条例. 2021年

[18] 中央网络安全和信息化委员会办公室. 关于印发国家网络安全事件应急预案的通知：中网办发〔2017〕4号. 2017年

[19] 深圳市政务服务和数据管理局. 关于印发深圳市数字政府网络安全和数据安全事件应急预案的通知：深政数〔2022〕56号. 2022年
