

《公共数据安全体系建设指南》

（送审稿）编制说明

一、项目背景

2021 年相继颁布了《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》，这两部法律的出台标志着我国在数据安全和个人信息保护方面的法律体系初步建立。《中华人民共和国数据安全法》明确了数据处理者的责任与义务，确立了数据安全监管的法律框架，并对数据安全违法行为规定了相应的法律责任。《中华人民共和国个人信息保护法》则着重保护个人信息权益，规范个人信息处理活动，确立了个人信息处理的基本原则，保障了信息主体的权利。2022 年 12 月 19 日，中共中央、国务院正式对外发布《关于构建数据基础制度更好发挥数据要素作用的意见》，旨在进一步明确数据安全保护的方针和措施，强化数据安全监管，促进数据的合理利用与共享。

公共数据作为数据资源的重要组成部分，关乎国民经济发展中生产生活的各个方面，蕴藏着巨大的经济和社会价值，若能实现有效利用，不仅能发挥其在社会治理中的重要作用，更能推动数字经济的长效发展。但数据利用价值与安全威胁同步显现，由于公共数据构成复杂、涉及范围广、处理环节多样、数据流动频繁，过程中潜藏了诸多安全风险问题，公共数据安全防护面临巨大挑战。因此，基于《中华人民共和国数据安全法》和《深圳经济特区数据条例》，以及已发布

的 DB4403/T 271—2022《公共数据安全要求》等所明确的数据安全要求，结合实际情况，组织开展本文件的研制工作。

本文件的制定和实施，为公共数据安全建设提供一套标准化的指导原则和操作指南，有助于规范公共管理和服务机构在数据处理活动中的行为，落实公共数据安全保护责任与义务。

二、工作简况

（一）任务来源

根据《深圳市市场监督管理局关于下达 2023 年深圳市地方标准计划项目任务的通知》，本文件予以正式立项。本文件由深圳市政务服务和数据管理局提出并归口。

（二）主要起草过程

1. 项目启动

2023 年初，深圳市信息安全管理中心作为牵头单位成立标准编制组，建立工作联络机制，开展筹划立项。

2. 标准立项

2023 年 3 月，深圳市信息安全管理中心提交《深圳市地方标准制修订计划项目建议书》，2023 年 5 月 8 日深圳市市场监督管理局批准立项。

3. 草案编制

2023 年 5 月至 2023 年 8 月，深圳市信息安全管理中心组织内部专家及其他参与起草单位进行多轮次的研讨和交流，确定标准的框架、大纲、主要内容条款等，形成了标准草案。

2023 年 9 月至 2024 年 2 月，深圳市信息安全管理中心组织外部专家对标准草案进行多次评审，广泛收集意见。

2024 年 3 月至 2024 年 4 月，深圳市信息安全管理中心及其他参与起草单位对标准草案进行了进一步修改，形成征求意见稿。

4. 征求意见阶段

2024 年 4 月 25 日至 5 月 8 日，深圳市政务服务和数据管理局发函征求 77 个单位意见，共收到反馈意见 84 条，其中采纳 12 条，无意见 72 条。标准编制组根据收到的反馈意见进行修改，形成送审稿。

2024 年 7 月 4 日，深圳市智慧城市和数字政府标准化技术委员会对拟送审的地方标准进行评议，共收到反馈意见 3 条，其中采纳 3 条，标准编制组根据收到的反馈意见进行修改，进一步完善送审稿。

三、地方标准主要内容的依据以及与国内领先、国际先进标准的对标情况

（一）标准编制原则

由于公共数据复杂多样、影响面广，在标准编制过程中，标准编制工作组根据“整体规划”“分级管理”“分布实施”的编制思路，充分考虑当前公共数据安全现状，遵循以下几个原则：

1. 行业适用性

本文件在编制过程中始终坚持公共数据安全要求建设思路的普遍适用性，同时重点关注建设内容在各公共管理和服务机构的可落地性。

2. 安全合规性

本文件在编制过程中始终遵循与我国现有的法律法规、标准规范等规定相一致的原则，同时也兼顾行业主管及监管部门对公共数据进行安全管理的实际监管要求。

（二）编制依据

第 3 章术语和定义，主要使用了 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》、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》中所界定的术语和定义。

第 4 章通则，主要依据 GB/T 25058—2019《信息安全技术 网络安全等级保护实施指南》第 4 章，并结合 DB4403/T 271—2022《公共数据安全要求》第 4 章编写；

第 5 章公共数据定级，主要依据 GB/T 25058—2019《信息安全技术 网络安全等级保护实施指南》第 5 章、DB4403/T 271—2022《公共数据安全要求》第 5 章，并结合 GB/T 43697—2024《数据安全技术 数据分类分级规则》编写；

第 6 至 9 章内容主要依据 GB/T 25058—2019《信息安全技术 网络安全等级保护实施指南》第 6 至 9 章，并结合 DB4403/T 271—2022《公共数据安全要求》第 7 至 9 章编写。

（三）同类标准编制情况

国家标准层面，数据安全建设相关标准有 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》等。

行业标准层面，电子政务、医疗行业、通信行业、电力行业、金融行业等重要行业均陆续发布数据安全相关建设指南，例如 GB/T 39725—2020《健康医疗数据安全指南》、JR/T 0197—2020《金融数据安全 数据安全分级指南》、YD/T 3802—2020《电信网和互联网数据安全通用要求》等。

地方标准层面，2022 年浙江省发布了 DB33/T 2487—2022《公共数据安全体系建设指南》。

整体来看，在数据安全领域，已发布的相关标准多数属于安全要求与技术规范，建设指南较少，且目前国家及行业层面暂无公共数据安全体系建设相关标准，我市亦无相关地方标准。

四、主要条款的说明以及主要技术指标、参数、试验验证的论述

（一）主要条款说明、技术指标参数

《公共数据安全体系建设指南》依托于 DB4403/T 271—2022《公共数据安全要求》中具体安全要求条款，提出落地实施的建设指南。以下对文件的主要条款进行简要说明。

1. 范围

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

对本文件规范性引用文件进行说明。

3. 术语和定义

对本文件适用的术语进行了说明。

4. 安全体系建设概述

本文件明确了建设原则，包括整体规划原则、分级管理原则、分步实施原则；本文件提出建设内容主要从通用管理安全、通用技术安全及数据处理活动安全三个方面出发；本文件明确了公共数据安全体系建设过程中涉及的各类角色与职责；本文件提出总体建设流程包括数据保护对象定级、总体安全规划、安全设计与实施、安全运行与维护、定级对象终止阶段。

5. 数据保护对象定级

给出确定数据定级对象、公共数据分类分级制度、公共数据分类分级、公共数据定级评审四项活动的详细建设指南，包括活动目标、参与角色、活动输入、活动描述、活动输出。

6. 总体安全规划

给出安全需求分析、安全建设项目规划两项活动的详细建设指南，包括活动目标、参与角色、活动输入、活动描述、活动输出。

7. 安全设计与实施

给出安全方案详细设计、通用管理安全建设、通用技术安全建设、数据处理活动安全建设四项活动的详细建设指南，包括活动目标、参与角色、活动输入、活动描述、活动输出。

8. 安全运行与维护

给出安全评估、风险监测、安全审计、应急处置、监督检查五项活动的详细建设指南，包括活动目标、参与角色、活动输入、活动描述、活动输出。

9. 定级对象终止

给出数据销毁与删除的详细建设指南，包括活动目标、参与角色、活动输入、活动描述、活动输出。

10. 附录

给出了规范性附录主要过程及其活动和输入输出以及资料性附录公共数据安全制度内容说明。

（二）主要试验情况分析

自 2020 年起，为摸清深圳市党政机关数据安全管理工作现状，识别数据安全短板，评估其与数据安全相关政策法规、标准规范差距点，深圳市信息安全管理中心已连续四年对重点单位开展数据安全评估。《公共数据安全体系建设指南》的编制也充分吸纳了评估工作的实践经验。

本文件在草案编制阶段协调了深圳市信息安全管理中心内部某部门作为试点验证部门，对本文件的条款的落地性、实操性进行综合验证，收集反馈意见进行修改。

五、是否涉及专利等知识产权问题

本文件不涉及专利及知识产权问题。

六、重大意见分歧的处理依据和结果

无。

七、实施地方标准的措施建议

为保证标准的有序实施，拟在标准正式发布之后开展标准的宣贯，提高相关人员对标准的理解和应用能力。同时，建立本标准实施的监督和评估机制，定期检查标准执行情况，评估标准实施的效果，并根据评估结果推动标准的修订完善和深化应用。

八、其他需要说明的事项

无。