ICS 35.240.01
CCS L 67

DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T 646—2025

公共数据安全体系建设指南

Guidelines for the construction of public data security systems

2025-06-24 发布　　2025-07-01 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：董安波、张军、穆端端、李苏、罗菁春、林宇群、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、王志红、林军、廖英豪、姚俊华、颜军、郭志远、束建钢、何延哲、林桢、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

本文件给出了公共数据安全体系建设的通则，以及公共数据定级、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体系建设。

本文件不适用于涉及国家秘密或者法律法规另有规定的公共数据安全体系建设。

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 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：

a) 整体规划原则：根据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；

b) 分级管理原则：宜对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；

c) 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

根据 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宜达到相对应的安全要求水平，安全等级与安全要求的关系见 DB4403/T 271—2022 中 6.7，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。总体建设内容见图 1。

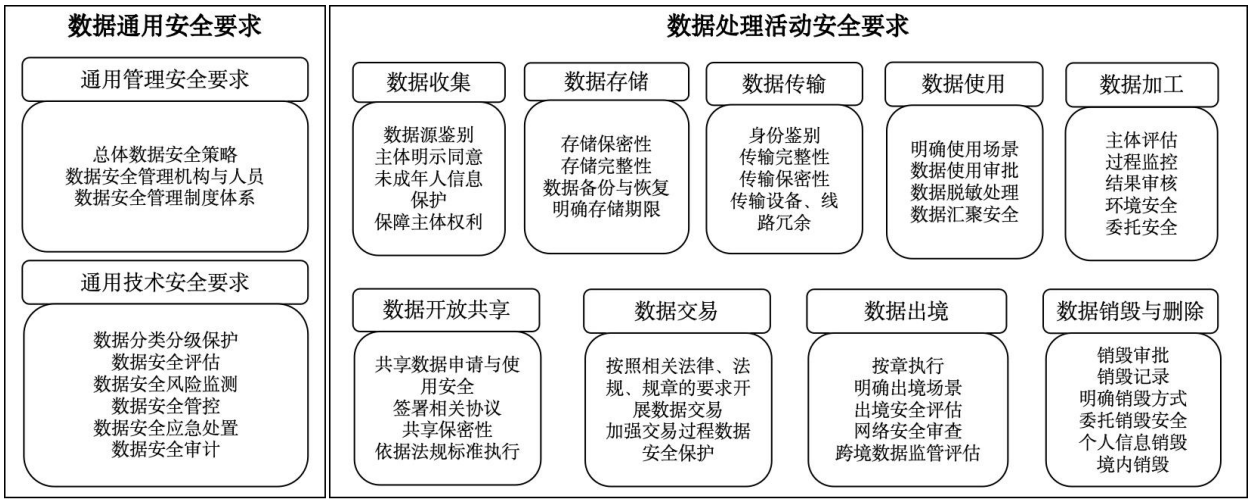

图 1　公共数据安全体系建设内容

4.3　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，各阶段及流程的输入输出说明见附录 A。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局部调整，但公共数据定级对象的安全等级并未改变时，按需进入总体安全规划阶段；如发生重要变更导致安全等级发生变化时，则进入公共数据定级阶段，重新开始新一轮公共数据安全体系建设工作。总体建设流程见图 2。

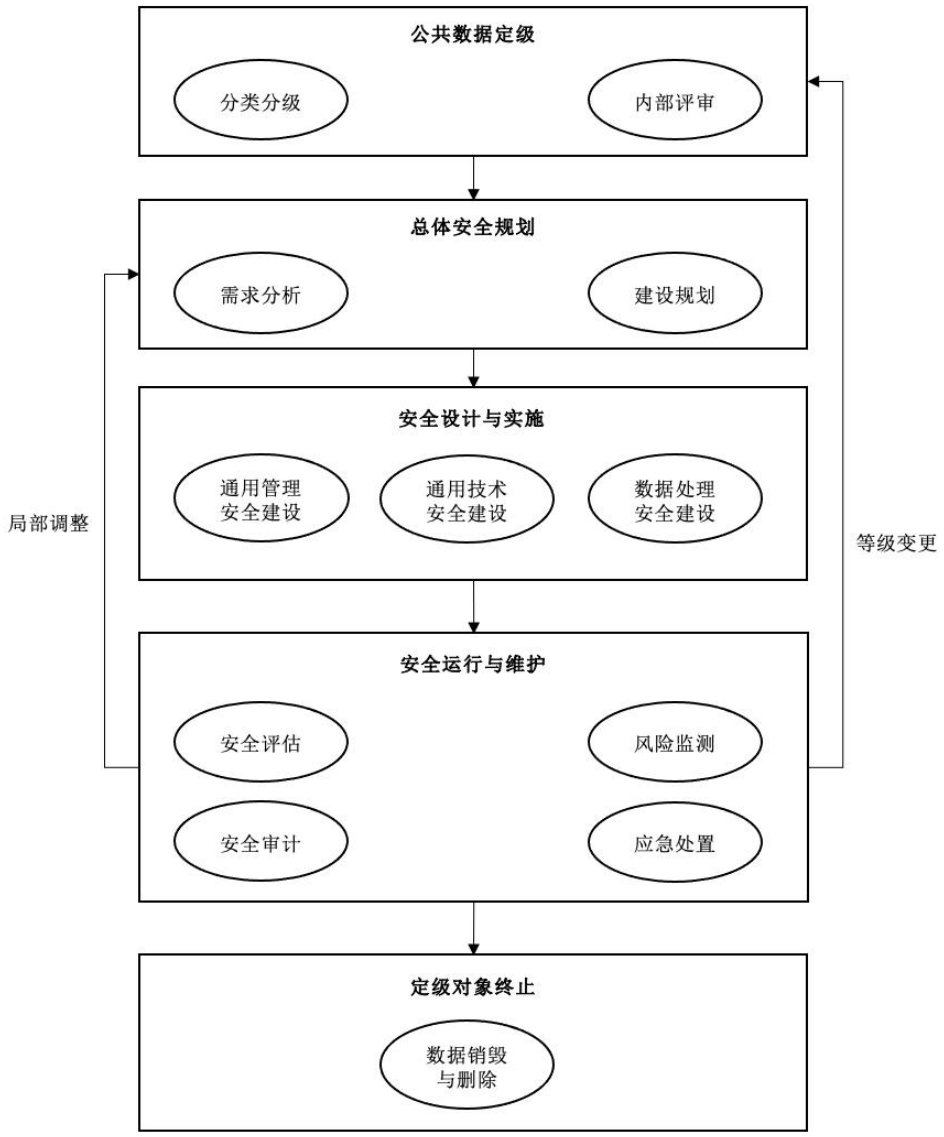

图2　公共数据安全体系建设流程

5　公共数据定级

5.1　概述

公共管理和服务机构宜按照 DB4403/T 271—2022 第 6 章，或 GB/T 43697—2024 第 5 至 7 章，或其他公共数据分类分级相关标准，确定数据定级对象，进行数据分类，确定数据对应安全等级，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。

5.2　确定数据定级对象

按照相关标准确定数据定级对象，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。通过梳理数据定级对象的信息，包括关联的业务系统名称及系统功能描述、数据库类型及基本信息、互联网协议地址（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，初步明确数据定级对象范围，形成业

务系统（数据库）清单，清单内容可按照 DB4403/T 271—2022 附录 A。数据定级对象关联的业务应用、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 公共数据分类分级

采用人工或辅助自动化扫描类工具，开展数据分类分级工作，并组织内部评审确定定级合理性，输出数据分类分级（数据子类或数据字段）清单，分类分级工作内容包括但不限于：

a) 采用人工识别公共数据类别及级别，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；
c) 通过敏感数据特征匹配技术，梳理数据库中存在的数据分布情况及数量；
d) 通过数据库信息扫描技术，梳理账户及权限信息；
e) 形成数据资产分类分级（数据子类或数据字段）清单，清单内容可按照DB4403/T 271—2022附录A。

6 总体安全规划

6.1 概述

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，明确数据保护对象的安全需求，规划安全建设目标，设计总体数据安全建设框架，指导后续的安全设计和实施。

6.2 安全需求分析

宜按照 DB4403/T 271—2022 第 7 至 9 章及 B.2，从数据保护对象建设初期，明确数据安全建设需求，与承载公共数据的业务系统同步规划、同步建设，输出公共数据安全需求分析报告，见附录 B 中的序号 1；若是已投入运营、使用的数据保护对象，则依据本文件 8.2 章节，对数据保护对象安全现状进行调研，围绕通用管理安全、通用技术安全及数据处理活动安全三个方面进行差距评估分析，针对差距点明确安全需求。

6.3 安全建设规划

6.3.1 依据公共数据安全需求分析报告，从数据保护对象总体安全建设目标出发，确定数据安全体系建设整体框架，综合分析各项安全建设需求紧迫度及实施难易程度，进行分阶段规划，明确不同建设阶段的建设部门、建设内容、建设步骤、建设时间、建设预算等，对预期建设效果进行效益分析，输出公共数据安全建设总体方案，见附录 B 中的序号 2。

6.3.2 公共数据安全建设总体方案宜涵盖数据安全管理、数据安全技术及数据处理活动三方面，涉及内容包括：

a) 公共数据安全管理能力，包括公共数据安全管理制度体系、安全管理机构与人员等；
b) 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、安全审计等；
c) 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、出境及销毁与删除等。

7 安全设计与实施

7.1 概述

宜参考公共数据安全建设规划的内容，分期分步落地安全措施，涵盖通用管理安全、通用技术安全及数据处理活动安全建设过程，可同步开展；通用管理安全涉及安全管理机构与岗位设立、安全策略与管理制度建设和修订、安全人员能力建设，通用技术安全涉及安全产品或服务采购、安全控制开发、安全控制集成，数据处理活动安全涉及数据收集、存储、传输、使用、加工、开放共享、交易、出境及销毁与删除。

7.2 通用管理安全建设

7.2.1 安全管理机构与岗位设立

7.2.1.1 确定数据安全管理机构

7.2.1.1.1 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，依据单位实际情况可由数据管理、网络安全管理或业务运营等相关部门人员组成，落实数据安全保护工作，数据安全管理机构高层管理人员可承担数据安全责任人的职责。

7.2.1.1.2 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。

7.2.1.1.3 数据安全管理机构职责为统筹管理和协调全局数据安全工作，职责具体包括：

a) 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及数据安全具体的保护工作，留存数据安全制度执行记录等；
b) 宜参考相关法律法规、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；
c) 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；
d) 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，可依据审批程序执行审批过程；
e) 针对重要的公共数据保护对象，重大数据处理活动宜建立逐级审批机制，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。

7.2.1.2 明确角色及岗位职责

7.2.1.2.1 制定数据安全管理人员岗位职责说明书，见附录 B 中的序号 3，以书面形式描述数据安全责任人、个人信息保护负责人的责任及权限范围，确保职责明确，所有风险落实到人，相关岗位职责包括：

a) 数据安全责任人职责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；
b) 个人信息保护负责人职责为对个人信息处理活动以及采取的保护措施等进行监督。

7.2.1.2.2 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，相关岗位职责包括：

a) 数据管理员负责数据存储、数据权限分配、数据资产梳理等；

b) 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，宜配备专职安全管理员承担数据安全管理员工作；
c) 数据安全审计员负责数据安全审计等。

7.2.1.3 人员安全管理

依据人员安全管理制度，落实人员安全管理要求，开展以下工作：
a) 对涉及公共数据安全运营及运维的内外部人员加强管理，包括人员录用、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) 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中的序号4，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，约束操作行为；
c) 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中的序号5，定期组织数据安全培训工作，每年至少一次，培训内容包括但不限于数据安全意识、政策法规、技能培训，留存培训记录；不定期组织数据岗位人员考取相关资质证书，持证上岗。

7.2.2 安全策略与管理制度建设和修订

7.2.2.1 制定数据安全总体策略文件

制定数据安全总体策略，见附录 B 中的序号 6，数据安全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。策略的编制、评审、发布具备正式流程，发布后组织开展宣贯和解读活动。针对三级及以上的公共数据保护对象，宜定期论证和评审数据安全策略，明确数据安全策略评审频率、评审内容，并进行评审跟踪验证，动态调整以保持适用性。

7.2.2.2 建立健全数据安全管理制度体系

7.2.2.2.1 建立健全数据安全管理制度体系，见附录 B 中的序号 7，通过正式、有效的方式发布制度，可使用纸质文件印发、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。
7.2.2.2.2 定期组织制度评审会，对数据安全管理制度的合理性及适用性进行论证，及时修订，保留评审记录表。
7.2.2.2.3 针对三级及以上的公共数据保护对象，持续完善数据安全管理制度，宜形成由安全策略、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，体系架构具体包括：
a) 第一层是安全策略，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；
b) 第二层是管理制度，是数据安全管理工作的指导文件，宜制定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制度，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；
c) 第三层是操作规程，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，可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规范、数据脱敏安全操作规程等；
d) 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，可制定数据分类分级资产清单、数据访问申请表、数据安全事件报告单、数据安全教育培训签到表等。

7.2.3 安全人员能力建设

7.2.3.1 通用安全管理涉及的人员安全能力建设，要求相关人员具备较强的数据安全保护意识，积极参加机构内部组织的安全培训；充分理解并能贯彻落实发布的各项数据安全管理制度要求，熟练执行内部各项审批流程，积极考取人员安全能力证书，持证上岗。

7.2.3.2 通用安全技术涉及的人员安全能力建设，要求相关人员充分理解并熟悉各类数据安全技术产品或服务类型，宜掌握的能力包括：

a) 安全产品或服务采购阶段，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) 安全控制开发与集成阶段，相关开发人员能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。

7.2.3.3 数据处理活动涉及的人员安全能力建设涵盖整个数据处理活动全流程，具体包括：

a) 数据收集：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，并按照GB/T 35273—2020中5.1至5.6规定开展个人信息收集工作；
b) 数据存储：熟悉异地数据备份恢复机制，在发生数据安全事件可能导致数据损坏、丢失时，能实现备份数据的恢复；
c) 数据传输：熟悉身份鉴别、数字签名、数字证书、安全传输协议等内容，能确保数据传输通道的安全性和可靠性;对数据传输过程中的风险进行评估,在发生安全事件时迅速响应和处理；
d) 数据使用：熟悉数据使用的场景及安全需求；针对三级及以上的公共数据保护对象，能对接入或嵌入的第三方应用具备安全检测能力，确保数据使用符合双方约定要求；
e) 数据加工：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，并能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，宜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；
f) 数据开放共享：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；
g) 数据交易：充分理解公共数据交易相关法律要求、安全及业务需求；
h) 数据出境：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；
i) 数据销毁与删除：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。

7.3 通用技术安全建设

7.3.1 安全产品或服务采购

7.3.1.1 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，可能涉及的安全产品或服务采购见表 1。采购需要考虑的要点如下：

a) 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；
b) 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；
c) 产品或服务的选择，宜考虑使用环境、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。

表1　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
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
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，宜包含数据安全风险评估、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
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，宜包含驻场安全运营、周期性安全运营等
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
数据安全应急处置	实现数据安全应急处置的平台或工具	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
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，宜包含驻场安全运营，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

7.3.2　安全控制开发

7.3.2.1　现有安全产品不满足安全功能需求时，可通过定制设计、开发来实现，安全控制的开发宜与系统的应用开发同步设计、同步实施。可能涉及的安全控制功能开发见表2。

7.3.2.2　分析安全控制功能开发需求，并进行概要设计及详细设计，进行编码实现，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。实施过程涉及如下：

a)　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；

b)　制定开发测试环境适用的安全管理制度、流程文档，宜包含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。

表 2　安全控制功能开发

建设内容	可能涉及的安全控制功能
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。
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。
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。
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。

7.3.3　安全控制集成

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，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。

7.4　数据处理活动安全建设

7.4.1　数据收集

7.4.1.1　可采取哈希算法、数字签名、奇偶校验、多副本对比等技术手段对收集的数据进行识别及完整性校验。

7.4.1.2　应用程序涉及个人信息收集功能，收集前采取个人信息主体主动点击等明示同意的方式，具体按照 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。

7.4.1.3　针对三级及以上的公共数据保护对象，收集外部数据前，采取密码算法、完整性校验、冗余设计等措施保证收集数据的机密性、完整性和可用性。

7.4.2　数据存储

7.4.2.1　采取可靠的数据备份系统，实现异地数据备份恢复能力；数据处理环节关联信息系统采取热冗余方式建设，包括软硬件设备，确保数据存储可用性；采取安全漏洞管理、威胁情报监测、网络访问隔离等方式实现勒索病毒攻击事前预警能力;通过部署防病毒软件,及时检测与阻断勒索病毒攻击扩散，实现事中阻断能力；通过实时数据备份及备份数据恢复，实现勒索病毒攻击事后恢复能力。

7.4.2.2　针对三级及以上的公共数据保护对象，采取异地数据实时备份方式，确保数据可用性。

7.4.2.3　针对四级公共数据保护对象，建设异地灾难备份中心，实现数据的实时切换能力。

7.4.2.4　涉及个人生物识别信息存储的，宜采取库表分离存储、存储设备隔离等方式，实现个人生物识别信息与个人身份信息分开存储，且仅存储个人生物识别信息的摘要信息。
7.4.2.5　超出个人信息存储期限的账户注销、系统下线、冗余备份数据、个人信息主体要求删除等场景下，采取数据删除或匿名化的处理方式。

7.4.3　数据传输

7.4.3.1　可采取密码认证、生物识别、多因素认证、单点登录等身份鉴别技术，对数据传输两端通信方实体进行鉴别，基于密码技术实现数据传输的机密性、完整性保护能力。
7.4.3.2　针对三级及以上的公共数据保护对象，对关键网络传输线路及核心设备进行冗余建设。
7.4.3.3　针对四级的公共数据保护对象，宜采取数字签名等机制，实现数据原发和接收行为的抗抵赖功能。

7.4.4　数据使用

7.4.4.1　采用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。
7.4.4.2　针对三级及以上的公共数据保护对象，大量汇聚数据时采取数据访问权限控制、数据脱敏等措施确保不暴露敏感数据，采用数字水印技术，对不同数据使用场景实现数据防泄漏及溯源能力。

7.4.5　数据加工

7.4.5.1　针对三级及以上的公共数据保护对象，建设数据加工过程安全监控功能，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（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，自动拦截。
7.4.5.2　加工后产生的新数据，采用安全保护措施，可使用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。

7.4.6　数据开放共享

7.4.6.1　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，宜按照 GB/T 39477—2020 第 6 章确定的共享数据安全要求，采取分类分级、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。
7.4.6.2　针对三级及以上的公共数据保护对象，采取数字水印等技术，确保共享数据可溯源，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。
7.4.6.3　宜参考相关法律法规、规章制度的要求开展数据开放活动，通过公共数据开放平台向社会开放数据，平台具备识别公共数据开放条件，包括无条件开放、有条件开放和不予开放三类，避免公共数据不合理开放。

7.4.7　数据交易

宜参考相关法律法规、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，可使用数据分类分级、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。

7.4.8　数据出境

宜参考相关法律法规、规章制度的要求进行数据出境活动，加强出境过程的数据安全保护，开展数据出境安全评估、个人信息出境标准合同签订、个人信息保护认证等。

7.4.9　数据销毁与删除

具备数据销毁与删除相关的技术或工具，可使用物理粉碎、消磁、多次擦写等技术手段；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。

8 安全运行与维护

8.1 概述

通过安全评估、风险监测、安全审计、应急处置对公共数据安全建设工作进行运行与维护，确保公共数据安全，防止安全漏洞或攻击事件发生，及时发现异常行为，迅速恢复业务的正常运转。

8.2 安全评估

8.2.1 基于公共数据保护对象，调研数据安全现状。可基于以下维度开展调研：

a) 数据资产情况：根据公共数据及承载的业务系统、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；

b) 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、数据安全管理相关制度流程、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；

c) 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，明确数据处理活动中数据安全能力情况。

8.2.2 依据 DB4403/T 439—2024 第 5 至 10 章节开展公共数据安全评估工作，输出公共数据安全评估报告，见附录 B 中的序号 8。

8.3 风险监测

8.3.1 确定监测对象

8.3.1.1 依据数据安全风险监测管理制度，见附录 B 中的序号 9，数据安全管理机构协同相关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。监测对象可为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、安全产品等。

8.3.1.2 根据确定的监测对象，结合监测的必要性、可行性、成本等因素，形成监测对象列表。

8.3.2 开展监测工作

8.3.2.1 配备自动化安全风险监测工具，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。监测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。

8.3.2.2 使用自动化安全风险监测工具收集安全信息，包括网络流量、日志信息、安全报警和性能状况等，数据安全管理员对工具收集的安全信息进行初步梳理及筛选，形成风险监测状态信息。

8.3.2.3 未配备自动化安全风险监测工具的情况下，数据安全管理员宜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，形成风险监测状态信息。

8.3.3 分析与报告

8.3.3.1 数据安全管理员通过工具或人工方式，对收集的安全信息进行影响分析，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，确定是否响应并记录安全风险，并对安全风险进行闭环管理，输出风险监测报告，见附录 B 中的序号 10。

8.3.3.2 针对三级及以上的公共数据保护对象，宜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。

8.4 安全审计

8.4.1 确定审计对象

8.4.1.1 依据数据安全审计制度，见附录 B 中的序号 11，数据安全管理机构协同相关部门对公共数据保护对象可能造成审计风险的关键要素进行分析，确定安全审计对象。涉及对象可为承载公共数据的业务应用系统与接口日志或流量信息、数据处理活动人员操作记录、数据安全管理制度体系执行记录等。

8.4.1.2 根据确定的审计对象，结合审计的必要性、可行性、成本等因素，输出审计对象列表。

8.4.2 开展审计工作

8.4.2.1 制定数据安全审计方案，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。

8.4.2.2 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。

8.4.2.3 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，审计对象包括数据账号操作及应用接口调用情况。

8.4.2.4 数据安全审计员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，基于数据安全审计相关工具，对审计结果的真实性负责。

8.4.2.5 宜参考相关法律法规、规章制度的要求开展个人信息保护合规审计工作。

8.4.3 分析与报告

根据审计结果进行影响分析，评价安全问题影响程度，确定是否响应，并对安全审计问题闭环管理，周期性输出数据安全审计报告，见附录 B 中的序号 12，每年至少一次；涉及个人信息保护合规审计工作，可参考相关法律法规、规章制度要求，输出个人信息保护合规审计报告，见附录 B 中的序号 13。

8.5 应急处置

8.5.1 应急准备工作

8.5.1.1 制定数据安全事件应急预案，见附录 B 中的序号 14，组建应急处置团队，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；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；数据安全事件应急预案具体内容可参考国家、省、市级应急预案编写，包括但不限于《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》、GB/T 20986—2023 第 4 至 5 章节。

8.5.1.2 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 中的序号 15，明确应急演练规模、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 中的序号 16。

8.5.1.3 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，确保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。

8.5.2 应急监测与响应

8.5.2.1 依据数据安全事件应急预案，明确安全事件上报情形。需要上报的情形包括但不限于：

a) 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；
b) 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，并按需向市网信、公安部门和有关行政主管部门报告；
c) 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。

8.5.2.2 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，造成严重事件的追溯到事件主体。

8.5.2.3 数据安全事件应急人员及时处置数据安全事件，检测事件影响范围，采取处置措施抑制事件加剧，根除事件发生风险，恢复数据正常运行，输出数据安全事件处置报告。

8.5.3 后期评估与改进

8.5.3.1 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。

8.5.3.2 数据安全事件应急人员根据应急响应过程，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。

9 定级对象终止

9.1 概述

当定级对象处于被转移、终止或废弃等情形，宜采取合理的方式处理存储的敏感数据，进行数据销毁与删除。

9.2 数据销毁与删除

9.2.1 识别销毁与删除的数据资产

9.2.1.1 制定数据销毁与删除规程，见附录 B 中的序号 17，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。

9.2.1.2 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、约定删除数据、数据迁移或暂存（包括业务运营需要、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。

9.2.1.3 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，包括设备、存储介质、数据、对应负责人、所处位置以及当前的状态等内容，列出清单。

9.2.2 进行数据的销毁与删除

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（高压击穿、粉碎）、消磁、覆写、销毁密钥、执行固件擦除命令等方式，将数据进行销毁、删除。

9.2.3 留存销毁与删除记录

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
（资料性）
主要阶段及流程和输入输出说明

公共数据安全建设工作的主要阶段及流程和输入输出说明见表 A.1。

表 A.1 主要阶段及流程和输入输出说明

主要阶段	主要流程		阶段输入	阶段输出
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	业务系统（数据库）清单
	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 业务系统（数据库）清单 其他相关数据分类分级文件、工具	数据资产分类分级（数据子类或数据字段）清单 数据血缘管理工具（四级增强安全要求）
总体安全规划	安全需求分析		公共数据及承载的业务系统、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 公共数据安全相关标准规范，如DB4403/T 271—2022	公共数据安全需求分析报告（基本安全要求）
	安全建设规划		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（基本安全要求）
安全设计与实施	通用管理安全建设	安全管理机构与岗位设立	法律法规、政策文件及标准，如 DB4403/T 271—2022 公共数据安全建设总体方案 安全管理机构及角色说明书等	数据安全管理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）

表 A.1　主要阶段及流程和输入输出说明（续）

主要阶段	主要流程		阶段输入	阶段输出
安全设计与实施	通用管理安全建设	安全策略与管理制度建设和修订	法律法规、政策文件及标准，如DB4403/T 271—2022 公共数据安全建设总体方案 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） 数据安全管理措施执行记录（基本安全要求）
		安全人员能力建设	法律法规、政策文件及标准，如DB4403/T 271—2022 公共数据安全建设总体方案等	人员能力建设过程记录，如人员培训、能力证书、工作执行记录等（基本安全要求）
	通用技术安全建设	安全产品或服务采购	法律法规、政策文件及标准，如DB4403/T 271—2022 公共数据安全建设总体方案 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		安全控制开发过程文档（基本安全要求）
		安全控制集成		安全控制集成相关平台（基本安全要求）
	数据处理活动安全建设		法律法规、政策文件及标准，如DB4403/T 271—2022、GB/T 35273—2020、GB/T 39477—2020 公共数据安全建设总体方案 各类数据安全产品与服务信息等	数据处理活动执行过程文档（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、三级增强安全要求、四级增强安全要求）
安全运行与维护	安全评估		公共数据及承载的业务系统、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 公共数据安全相关标准规范，如DB4403/T 271—2022、DB4403/T 439—2024 等	公共数据安全评估报告（基本安全要求）

表 A.1　主要阶段及流程和输入输出说明（续）

主要阶段	主要流程		阶段输入	阶段输出
安全运行与维护	风险监测	确定监测对象	公共数据安全总体设计方案 数据安全风险监测管理制度 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、安全产品等 自动化安全风险监测工具等	安全风险监测对象列表（基本安全要求）
		开展监测工作		风险监测状态信息（基本安全要求）
		分析与报告		风险监测报告（基本安全要求）
	安全审计	确定审计对象	公共数据安全总体设计方案 数据安全审计制度 承载公共数据的业务应用系统与接口日志或流量信息 数据处理活动人员操作记录 数据安全管理制度体系执行记录 数据安全审计相关工具等	安全审计对象列表（基本安全要求）
		开展审计工作		数据安全审计方案（基本安全要求）
		分析与报告		数据安全审计报告（基本安全要求）、个人信息保护合规审计报告（按需）
	应急处置	应急准备工作	公共数据安全总体设计方案 相关标准、规范，如《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》、GB/T 20986—2023 应急培训计划 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（基本安全要求） 数据安全事件应急演练报告（基本要求）
		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）
定级对象终止	数据销毁与删除	识别销毁与删除的数据资产	公共数据安全相关标准规范，如DB4403/T 271—2022、DB4403/T 439—2024 等 数据销毁与删除工具	数据销毁与删除规程（基本安全要求） 待销毁、删除的设备、介质及数据清单（基本安全要求）
		进行数据的销毁与删除		–
		留存销毁与删除记录		数据销毁、删除处理记录文档（基本安全要求）

附 录 B
（资料性）
公共数据安全建设关联文件内容说明

公共数据安全建设关联文件内容说明见表 B.1。

表 B.1 公共数据安全建设关联文件内容说明

主要阶段	序号	文件名称	内容说明
总体安全规划	1	公共数据安全需求分析报告	● 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； ● 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； ● 总结，提出数据安全的建议和改进措施。
	2	公共数据安全建设总体方案	● 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，分期分阶段建设，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、效益分析； ● 建设投资估算等。
安全设计与实施	3	数据安全管理人员岗位职责说明书	● 数据安全管理人员职责、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。
	4	数据安全保密协议	● 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。

表 B.1　公共数据安全建设关联文件内容说明（续）

主要阶段	序号	文件名称	内容说明
安全设计与实施	5	数据安全教育培训制度	● 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、形式，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。
	6	数据安全总体策略	● 公共数据安全管理目标、原则； ● 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； ● 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。
	7	数据安全管理制度体系	● 数据安全管理制度体系宜包含但不限于以下文件： ● 数据安全总体策略； ● 数据安全管理组织机构与人员安全管理制度； ● 数据分类分级制度（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）； ● 数据安全评估制度； ● 数据安全风险监测制度； ● 数据访问权限管控制度； ● 数据安全应急与处置制度； ● 数据安全审计制度； ● 数据处理活动安全管理要求； ● 数据安全教育培训制度； ● 数据合作方管理制度； ● 个人信息安全保护制度； ● 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）； ● 投诉、举报受理处置制度； ● 个人信息主体保护权利渠道和机制。

表 B.1　公共数据安全建设关联文件内容说明（续）

主要阶段	序号	文件名称	内容说明
安全运行与维护	8	公共数据安全评估报告	● 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。
	9	数据安全风险监测管理制度	● 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及上报机制。
	10	风险监测报告	● 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。
	11	数据安全审计制度	● 数据安全审计概述，如背景、目的、原则、组织与职责等； ● 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。
	12	数据安全审计报告	● 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； ● 审计内容，如合规性审计、安全事件和违规审计、内部安全管理执行落实情况审计等； ● 建议和改进措施、审计记录和意见。
	13	个人信息保护合规审计报告	● 个人信息保护合规审计概述，如背景、目的、原则等； ● 个人信息保护合规审计组织与职责与安排； ● 个人信息保护合规审计要点； ● 审计问题和风险、建议和改进措施、审计记录和意见等。

表 B.1　公共数据安全建设关联文件内容说明（续）

主要阶段	序号	文件名称	内容说明
安全运行与维护	14	数据安全事件应急预案	● 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。
	15	数据安全事件应急演练方案	● 演练目标与范围，明确演练目标、范围和参与人员、场景； ● 应急响应团队组成，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； ● 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； ● 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； ● 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； ● 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。
	16	数据安全事件应急演练报告	● 演练背景、目的、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	17	数据销毁与删除操作规程	● 数据销毁与删除场景； ● 数据销毁与删除方式； ● 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 20986—2023 信息安全技术 网络安全事件分类分级指南

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

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

[5] GB/T 37964—2019 信息安全技术 个人信息去标识化指南

[6] GB/T 37973—2019 信息安全技术 大数据安全管理指南

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

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

[9] GB/T 41479—2022 信息安全技术 网络数据处理安全要求

[10] GB/T 41817—2022 信息安全技术 个人信息安全工程指南

[11] JR/T 0171—2020 个人金融信息保护技术规范

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

[13] YD/T 3813—2020 基础电信企业数据分类分级方法

[14] YD/T 3956—2021 电信网和互联网数据安全评估规范

[15] 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

[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.中华人民共和国数据安全法.2021年

[17] 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

[18] 中华人民共和国国务院第 40 次常务会议.网络数据安全管理条例.2024 年

[19] 中华人民共和国国家互联网信息办公室 2024 年第 15 次室务会会议.个人信息保护合规审计管理办法.2025 年

[20] 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

[21] 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：中网办发文〔2017〕4 号.2017 年

[22] 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