ICS 35.240.01
CCS L 67

DB33

浙 江 省 地 方 标 准

DB33/T 2487—2022

公共数据安全体系建设指南

Guidelines for the construction of public data security systems

2022-04-26 发布　　2022-05-26 实施

浙江省市场监督管理局　　发 布

目　　次

前　言

本标准按照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。

请注意本标准的某些内容可能涉及专利。本标准的发布机构不承担识别专利的责任。

本标准由浙江省大数据发展管理局提出、归口并组织实施。

本标准起草单位：浙江省大数据发展中心、数字浙江技术运营有限公司、联通数字科技有限公司、浙江省标准化研究院、浙江省数据安全服务有限公司、杭州市数据资源管理局、宁波市大数据发展管理局、温州市大数据发展管理局、湖州市大数据发展管理局、嘉兴市政务服务和数据资源管理办公室、绍兴市大数据发展管理局、金华市大数据发展管理局、衢州市大数据发展管理局、舟山市大数据发展管理局、台州市大数据发展管理局、丽水市大数据发展管理局。

本标准主要起草人：王瑚、金加和、洪吉明、蓝宇娜、孟一丁、党铮铮、赵程遥、毛远庆、张斌、杜永华、池邦芬、笪猛霄、陈焕、包自毅、张新丰、顾闻、徐振华、张晓玮、杜战、蒋纳成、范东媛、叶春雷、孔俊、王沁怡、张伟伟、胡瑞玉、叶红叶、施筱玲、徐峰、蒋迪、甄理、俞巍滔、杜辉、孙茂阳、胡琼达、朱宝剑、叶茜茜、陈玮萍、屠勇刚、韩建良、徐李锐、毛勇增、张岳军、林国、王玲玲。

本标准为首次发布。

引　言

为保障一体化智能化公共数据平台和公共数据安全，强化公共数据安全体系建设，提升公共数据安全主动防御能力、监测预警能力、应急处置能力、协同治理能力，有效防范公共数据篡改、泄漏、滥用，依据《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》《浙江省公共数据条例》制定本标准。

本标准是公共数据安全体系相关系列标准之一。

与本标准的相关标准还包括：

——公共数据分类分级指南（DB33/T 2351—2021）；

——公共数据安全体系评估规范（DB33/T 2488—2022）。

公共数据安全体系建设指南

1 范围

本标准确立了公共数据安全体系建设的总体原则，给出了体系架构以及制度规范子体系、技术防护子体系和运行管理子体系构建的指导性建议。

本标准适用于指导公共数据安全体系建设。

本标准不适用于涉及国家秘密的公共数据及相关处理活动。

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标准必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本标准；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 37973 信息安全技术 大数据安全管理指南

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

DB33/T 2350 数字化改革术语定义

DB33/T 2351 公共数据分类分级指南

3 术语和定义

GB/T 25069、GB/T 37973、GB/T 39477和DB33/T 2350界定的以及下列术语和定义适用于本标准。

3.1

公共数据 public data

国家机关、法律法规规章授权的具有管理公共事务职能的组织以及供水、供电、供气、公共交通等公共服务运营单位(以下统称公共管理和服务机构)，在依法履行职责或者提供公共服务过程中收集、产生的数据。

3.2

公共数据安全 public data security

通过建立制度规范、技术防护和运行管理等必要措施，确保公共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。

3.3

公共数据全生命周期 public data lifecycle

包括公共数据收集、归集、存储、加工、传输、共享、开放、利用、销毁等各个关键环节。

3.4

数据血缘关系 data lineage

数据在产生、处理、流转到消亡过程中，数据之间形成的可回溯的关联关系。

3.5

用户行为画像 user behavior profiling

结合用户角色和用户操作行为,利用关键日志信息进行归类、关联，勾勒出用户行为整体视图，以实现风险分析、预警。

3.6

供应方 supplier

提供公共数据相关产品或服务的企业或其他组织。

4 总体原则及架构

4.1 总体原则

4.1.1 权责一致

公共数据安全体系建设宜遵循谁收集谁负责、谁使用谁负责、谁运行谁负责的原则开展。

4.1.2 分级管理

宜遵循按照公共数据类别和级别采取差异化安全保障措施的原则，高安全级别数据从严保护，低安全级别数据适度保护。

4.1.3 全程可控

宜遵循覆盖公共数据全生命周期的原则，确保公共数据在各个关键环节均得到所需安全保障。

4.1.4 持续优化

宜遵循持续迭代、动态优化的原则，保障数据安全体系满足动态变化的数据安全需求。

4.1.5 协调发展

宜坚持以公共数据开发利用和产业发展促进公共数据安全、以公共数据安全保障公共数据开发利用和产业发展的原则。

4.2 体系架构

公共数据安全体系架构宜包括公共数据安全制度规范子体系、公共数据安全技术防护子体系和公共数据安全运行管理子体系三个部分。公共数据安全体系架构参见图1,公共数据安全建设案例详见附录A。

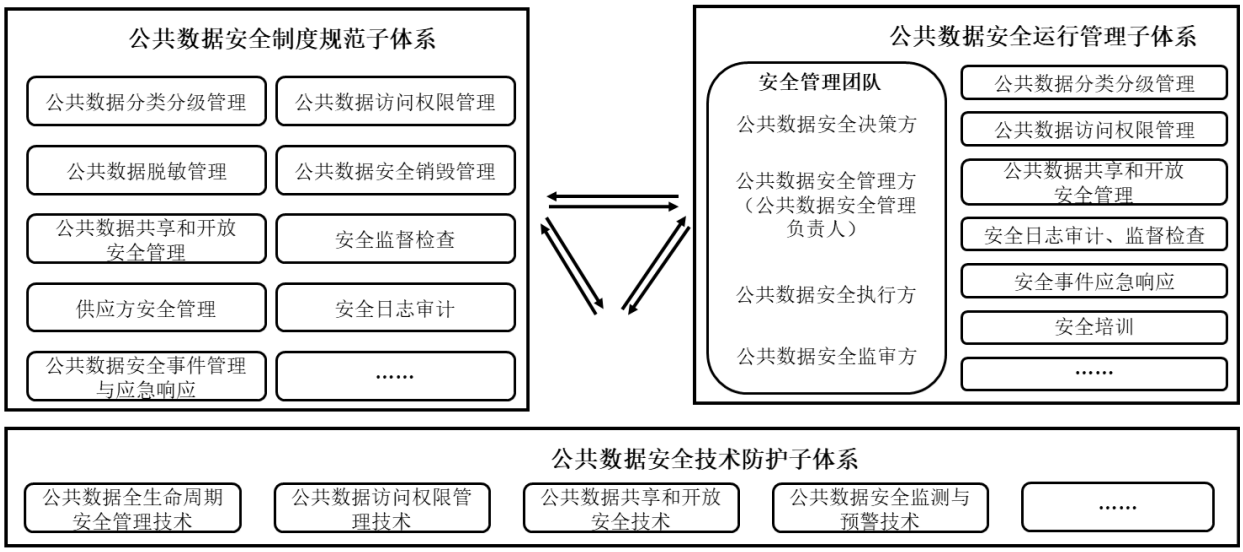

图1　公共数据安全体系架构

5　制度规范子体系

5.1　制度规范子体系架构

制度规范子体系建设宜全面覆盖公共数据全生命周期关键环节，并充分考虑数据回流、数据开发环境等相关场景要求。可按照三级架构建立公共数据安全制度规范子体系：

——一级制度为战略纲领类，是数据安全顶层的管理策略、要求、目标及基本原则。

——二级制度为标准规范类，是根据一级管理要求制定的通用管理办法、标准及规范。

——三级制度为流程细则类，是对上层管理要求的细化和解读，用于指导具体业务场景的工作，确定各环节的具体操作指南、规范，还可包括操作程序、记录、表单等过程性文档。

注：本标准主要围绕二级制度展开。

5.2　数据分类分级管理制度

数据分类分级管理制度的制定可参考 DB33/T 2351，相关案例参见附录 B，内容主要包括：

a)　公共数据分类分级原则、要求、维度和方法等；

b)　公共数据分类分级操作指南和工作流程等；

c)　公共数据类别和级别的变更场景、变更申请审批流程及变更工作要求等；

d)　不同级别的数据安全保障要求等。

5.3　数据访问权限管理制度

数据访问权限管理可基于公共数据访问业务需求，按照仅赋予用户开展工作所必须最小权限的原则制定，内容主要包括：

a)　公共数据载体和公共数据权限管理系统的账号权限安全管理职责分工；

b)　公共数据载体和公共数据权限管理系统的账号权限管理工作要求；

c) 公共数据访问账号权限分配、开通、使用、变更、重置、锁定、注销等的申请审批流程；
d) 具备超级管理员权限或数据批量复制、处理、导出和删除等高风险操作权限账号的安全要求等。

5.4 数据脱敏管理制度

数据脱敏管理制度可基于数据级别及应用场景，结合实际需求制定，内容主要包括：
a) 公共数据脱敏规则；
b) 公共数据脱敏工作的管理要求；
c) 公共数据脱敏工作的技术要求；
d) 公共数据脱敏工作流程等。

5.5 数据共享和开放安全管理制度

数据共享和开放方式不限于数据查询接口、批量数据同步等，可基于各类共享和开放场景制定相应制度，内容主要包括：
a) 各类别和级别公共数据共享和开放安全管理要求；
b) 各类别和级别公共数据共享和开放安全技术要求；
c) 各类别和级别公共数据共享和开放的应用场景；
d) 各类别和级别公共数据共享和开放的工作流程；
e) 各类别和级别公共数据共享和开放的申请审批环节等。

5.6 数据安全销毁管理制度

公共数据安全销毁管理制度宜充分考虑数据销毁的必要性、及时性、可靠性等，内容主要包括：
a) 各类别和级别公共数据销毁对象；
b) 各类别和级别公共数据销毁场景；
c) 各类别和级别公共数据销毁方式；
d) 各类别和级别公共数据销毁流程；
e) 各类别和级别公共数据销毁工作要求等。

5.7 供应方安全管理制度

供应方安全管理制度宜全面覆盖与供应方合作的全过程，内容主要包括：
a) 供应方引入的安全管理要求，包括资质和背景安全审查等；
b) 供应方及供应方人员的安全管理要求，包括终端安全、网络安全、数据安全、保密管理等；
c) 供应方及供应方人员的安全职责、安全考核要求及惩处措施；
d) 供应方及供应方人员的服务安全保护及保密协议及安全承诺书的签订；
e) 供应方人员变更机制；
f) 供应方合作终止机制等。

5.8 安全监督检查制度

宜通过制定监督、检查等制度，保障数据安全管理策略落地，内容主要包括：
a) 公共数据安全管理监督检查内容；
b) 公共数据安全管理监督检查方式；

c） 公共数据安全管理监督检查工作周期；
d） 公共数据安全管理监督检查工作流程等。

5.9 安全日志审计制度

宜通过制定安全日志审计制度，推动各应用、各系统的日志采集及分析，识别数据安全风险，并进行告警及处置，实现问题可追溯。公共数据安全日志审计制度，内容主要包括：

a） 公共数据安全审计日志的采集内容；
b） 公共数据安全审计日志的采集方式；
c） 公共数据安全审计日志标准化要求；
d） 公共数据安全审计日志存储要求；
e） 公共数据安全审计策略和规则；
f） 异常预警及处置工作流程等。

5.10 安全事件管理与应急响应制度

通过公共数据安全事件管理与应急响应制度，及时应对数据安全事件，减少数据安全事件所带来的不利影响，内容主要包括：

a） 公共数据安全事件分类分级方法；
b） 各级别公共数据安全事件发现、上报、处置、溯源、总结等工作流程；
c） 各类别公共数据安全应急预案编制及应急演练工作要求等。

6 技术防护子体系

6.1 技术防护子体系架构

公共数据安全技术防护子体系宜覆盖公共数据全生命周期各环节。公共数据安全技术防护子体系主要包括：

——公共数据全生命周期安全管理技术；
——公共数据访问权限管理技术；
——公共数据共享和开放安全技术；
——公共数据安全监测与预警技术等。

6.2 全生命周期安全管理技术

依据场景按需建立对应安全保障措施，监测和防范数据全生命周期各环节可能存在的安全风险，包括但不限于数据篡改、泄露、滥用、损毁等。建立公共数据全生命周期安全管理技术，主要包括：

a） 数据源统一鉴别技术；
b） 敏感数据识别；
c） 数据分类分级标识技术；
d） 数据脱敏技术，相关案例可参见附录C；
e） 数据加密技术；
f） 传输通道加密技术；
g） 数据血缘关系技术；
h） 数据备份与恢复技术；

i） 数据防泄漏技术；
j） 销毁数据识别技术；
k） 数据有效销毁技术等。

6.3 访问权限管理技术

采用访问权限控制管理技术能力，确保仅赋予用户开展工作所必须的最小权限。公共数据访问权限管理技术，主要包括：

a） 公共数据访问权限集中认证技术；
b） 公共数据访问权限统一入口访问；
c） 基于终端、网络、系统、文件、数据库表以及字段等级别的细粒度访问控制技术。

6.4 数据共享和开放安全技术

宜通过访问控制和接口安全监测与预警等技术，对数据共享和开放全过程实施管控。可通过区块链等技术提升共享开放场景下的数据溯源能力，强化数据共享和开放的安全保障。公共数据共享和开放安全技术，主要包括：

a） 访问控制技术；
b） 接口安全监测与预警技术；
c） 数据溯源技术；
d） 溯源结果可信技术，如区块链等；
e） 隐私计算技术等。

6.5 安全监测与预警技术

可基于数据资产变化、访问行为、操作行为等日志，进行数据安全风险识别和预警，提供处置建议。安全监测与预警技术主要包括：

a） 公共数据安全量化指标配置；
b） 公共数据安全威胁的发现和识别；
c） 数据画像和用户行为画像技术；
d） 风险预警与处置建议等。

7 运行管理子体系

7.1 运行管理子体系架构

可基于制度规范和技术防护子体系，建立公共数据安全运行管理子体系。从人、数据、场景等维度，通过组织机构及人员，将各项制度规范和技术防护手段充分融合落地，实现数据合理、合规、安全地流动与使用。公共数据安全运行管理子体系主要包括：

——安全管理团队；
——公共数据分类分级运行管理；
——公共数据访问权限运行管理；
——公共数据共享和开放安全运行管理；
——公共数据安全日志审计；
——公共数据安全监督检查；

——公共数据安全事件应急响应；
——公共数据安全培训等。

7.2 安全管理团队

数据安全组织架构及人员保障是数据安全体系建设的基础。公共数据安全管理团队构成及职责，主要包括：

a) 公共数据安全决策方：领导公共数据安全管理工作，负责公共数据安全工作的总体监管、协调与重大事项决策；
b) 公共数据安全管理方：根据相关法律法规和制度规范要求，参考本指南建立公共数据安全体系（包括制度规范子体系、技术防护子体系和运行管理子体系），指导公共数据安全要求的落实，推动公共数据安全体系动态更新和持续优化；
c) 公共数据安全执行方：负责落实和配合公共数据安全管理工作；
d) 公共数据安全监审方：对公共数据安全管理工作进行监督、检查和审计，落实公共数据安全监督检查机制，配合安全管理方推动公共数据安全体系动态更新和持续优化；
e) 公共数据安全管理负责人：宜委任具备公共数据安全管理相关专业知识和履职能力的人员作为公共数据安全管理负责人，为其提供人力、技术等必要支持。。

7.3 数据分类分级运行管理机制

宜建立基于数据资源目录的分类分级运行管理机制，主要包括：

a) 公共数据资源管理，包括建立和维护数据资产全景视图；
b) 公共数据智能化分类分级任务发布、审批和定期更新；
c) 公共数据分类分级结果在数据全生命周期安全管理的应用等。

7.4 数据访问权限运行管理机制

宜建立公共数据访问权限运行管理机制，相关案例可参见附录D，主要包括：

a) 公共数据访问账号权限分配、开通、使用、变更、重置、注销等的申请审批、执行和记录；
b) 公共数据访问权限分配表建立和维护；
c) 公共数据访问权限有效时限设置；
d) 公共数据访问权限及时更新；
e) 公共数据访问权限定期核查；
f) 与具有公共数据访问权限的供应方人员签署数据安全保密承诺书；
g) 高风险数据操作权限特殊管控工作等。

7.5 数据共享和开放安全运行管理机制

宜建立公共数据共享和开放安全运行管理机制，主要包括：

a) 公共数据共享和开放安全审核；
b) 公共数据共享和开放接口上线前安全检查；
c) 公共数据共享和开放接口定期安全检查；
d) 长期未用共享和开放数据的识别和处置；
e) 公共数据共享和开放渠道（如批量共享、接口共享、文件导出、邮件、网络、终端等）的敏感数据告警处置等。

7.6 安全日志审计机制

宜建立实时公共数据安全日志审计机制，主要包括：

a) 告警信息研判；
b) 用户行为画像建立；
c) 违规行为处置；
d) 规则库动态更新优化等。

7.7 安全监督检查机制

宜建立周期性数据安全监督检查机制，主要包括：

a) 对公共数据处理环境安全、公共数据访问权限管理、公共数据共享和开放安全管理、公共数据销毁管理、个人信息使用等重要环节的安全管理工作落实情况和效果的安全检查；
b) 安全检查问题通知和整改；
c) 整改情况验证；
d) 对整改不到位的情况的处置等。

7.8 安全事件应急响应机制

宜建立数据安全事件应急响应机制，相关案例可参见附录E，主要包括：

a) 应急预案编制；
b) 应急演练；
c) 应急演练报告编制；
d) 应急预案优化等。

7.9 安全培训机制

宜建立公共数据安全培训机制，主要包括：

a) 公共数据安全培训规划；
b) 专业知识学习激励政策；
c) 公共数据安全工作经验交流；
d) 公共数据安全知识宣传培训；
e) 供应方人员入场前的安全培训等。

8 安全体系评估机制

8.1 评估概述

8.1.1 宜围绕公共数据安全体系建设，建立配套的公共数据安全体系评估机制，通过公共数据安全体系评估工作，推动公共数据安全体系可量化、可评估和持续优化。

8.1.2 评估工作全流程包含确定评估范围、组建评估团队、制定评估方案、实施评估、报告编制以及评估结果应用，详见图2。

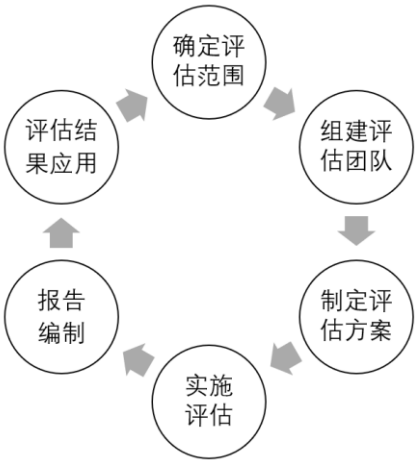

图2　评估工作全流程示意图

8.2　评估时机

可在下列情况开展公共数据安全体系评估工作：

a)　初次系统性开展公共数据安全体系建设的；

b)　按照既定安全体系评估机制，周期性开展公共数据安全体系评估的；

c)　发生安全责任人变更、供应方变更、重大业务变更或网络安全保护等级变更等情况的；

d)　其他需要开展公共数据安全体系评估的。

8.3　评估实施

公共数据安全体系评估工作可依据相关评估规范开展。

8.4　评估结果应用

评估完成后，可将评估结果加以应用，形成闭环。最终评估结果的应用可包括：

a)　总体判断评估对象的公共数据安全体系建设水平。评估结果可作为公共数据处理活动开展的重要参考依据。

b)　研判公共数据安全体系风险隐患，发现公共数据安全防护的薄弱环节。针对评估发现的薄弱环节，制定整改方案和计划，推进公共数据安全体系持续完善、全面优化。

附 录 A
（资料性）
公共数据安全体系建设案例

A.1 现状分析

某市公共数据管理机构为落实《中华人民共和国数据安全法》《浙江省公共数据条例》《浙江省公共数据和电子政务管理办法》《浙江省公共数据开放与安全管理暂行办法》《浙江省数字化改革总体方案》《浙江省一体化智能化公共数据平台建设方案》等法律法规要求，在该市公共数据现有安全举措基础上，参照《公共数据安全体系建设指南》，结合本单位公共数据应用现状，启动一体化智能化公共数据平台安全体系建设工作。该市公共数据安全体系现状如下：

a) 制度规范子体系。已制定出台公共数据安全管理总则等纲领文件和公共数据安全销毁管理、供应方安全管理、安全事件管理与应急响应、公共数据脱敏管理、安全日志审计和监督检查等相关配套制度。公共数据分类分级管理、公共数据开放及共享管理、公共数据访问权限管理等尚未建立。

b) 技术防护子体系。数据共享和开放安全技术能力、访问权限管理技术能力、全生命周期安全管理技术能力初步形成。数据脱敏、安全监测预警技术能力等仍存在缺失或薄弱环节。

c) 运行管理子体系。已具备安全管理负责人、安全日志监审、安全培训等运行管理，安全管理团队也基本形成。数据访问权限运行管理、安全监督检查的监审方及监审机制、安全事件应急响应、分类分级管理、数据共享和开放安全管理等存在缺失或不足。

A.2 建设内容

A.2.1 概述

基于上述现状，该市公共数据安全体系建设工作，从制度规范子体系、技术防护子体系、运行管理子体系三个方面开展，主要包括制定分类分级管理等制度，建设数据脱敏等技术能力，建立分类分级、权限管控、安全事件应急响应等运行管理机制。具体包括三个方面。

A.2.2 优化公共数据安全制度规范子体系

该市公共数据管理机构，依据公共数据安全制度规范子体系指导意见，结合自身数据安全管理方针文件等要求，在二级制度中，优化完善公共数据分类分级管理规范、公共数据共享和开放管理规范、公共数据安全权限管理规范、公共数据回流管理规范、公共数据脱敏技术规范等。

其中分类分级管理规范优化示例参见附录B。

A.2.3 提升公共数据安全技术防护子体系

该市公共数据管理机构，基于该市一体化智能化公共数据平台现状，通过构建公共数据安全技术防护体系，围绕公共数据进行全生命周期的防护。其中重点建设的安全防护能力包括：建立分类分级、数据源监测能力，保障采集阶段安全；建立权限管控、接口监测等防护功能，以及符合国家密码应用要求的密码管理功能实现传输通道及数据库安全，保障数据传输阶段机密性等安全；建立数据目录对数据资产进行管理、容错备份、数据存储加密等能力，保障平台数据存储阶段等安全；建立数据血缘关系分析能力、数据动态脱敏能力，实现数据处理阶段的安全；建立数据加密/脱敏、接口管控、血缘关系分析等安全能力，保障数据交换环节的安全；建立数据销毁及设备软硬销毁能力，保障数据销毁阶段的安全。通过建立敏感数据监测、安全风险监测预警、通讯安全保密等能力，提升公共数据安全防护水平。

其中数据脱敏等作为本次建设关键，主要基于一体化智能化公共数据平台环境，上线适合大数据环境的动态脱敏系统，数据脱敏主要内容参见附录C。

A.2.4 完善公共数据安全运行管理子体系

该市公共数据管理机构参照《公共数据安全体系建设指南》，建立符合一体化智能化公共数据平台技术要求的公共数据安全运行管理体系，本阶段主要从访问权限运行管理机制及安全事件应急响应机制等方面重点落实，详细参见附录D和附录E。

A.3 建设成效

该市公共数据管理机构公共数据安全体系的建设主要依据《公共数据安全体系建设指南》及相关法律法规等要求进行。通过本阶段安全体系建设：

a) 数据安全制度规范体系逐渐完善。现行规范制度覆盖面、合理性、可操作性方面得到优化，新增分类分级、公共数据开放及共享等制度规范，指导开展公共数据安全体系建设，通过定义数据安全责任、事项操作流程，细化分解数据安全评价指标，使安全管理工作可量化、可评估，公共数据处理活动趋向规范化。

b) 数据安全防护技术能力提升。公共数据脱敏等技术应用为数据安全流通提供了有效的安全处理保障，通过公共数据安全事前预防、事中监测、事后审计等整体安全治理，形成常态化风险监测和闭环处置机制，累计发现、处置各类数据安全告警 5500 余次，公共数据安全事件数量周、月统计值均呈下降趋势。

c) 数据安全运行管理体系优化改进。依托大数据平台数据自动识别、数据标识、数据多维展现等能力，降低人工数据录入、提高工作能效，数据分级分类合理性、数据有效性、数据质量大幅上升。依据数据权限授予最小化原则，梳理并重新定义数据管控权限，规避数据权限不清造成的风险隐患。应急演练与应急实战常态化，检验与调整优化应急响应组织架构、响应流程和安全监测能力。

最终，为该市公共数据管理机构提供了公共数据安全制度规范、技术防护、运行管理等抓手，夯实了公共数据安全保障基础。

附 录 B
（资料性）
分类分级管理规范优化示例

分类分级管理规范优化制定的核心内容见表B.1。

表B.1 分类分级规则优化结果示例

级别	数据特征	数据示例	共享属性
L1	可从公开途径获取或者法律法规授权公开的数据	1.公共设施、设备的位置、指标参数、运行状态、统计数据等 2.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情况	无条件共享
L2	数据开放风险低，对公共秩序、公共利益影响较小	1.城市充电桩、公交站等公共服务设施的分布规则及设备状态数据等 2.城市道路车流量、道路、桥梁、隧道等管理数据	受限共享
L3	数据开放风险中等，数据非授权操作后会对个人、企业、其他组织或国家机关运作造成损害	1.传染病统计数据、药品使用统计数据等 2.公共治安视频数据等	受限共享
L4	数据开放风险较高，数据非授权操作后会对个人、企业、其他组织或国家造成严重损害	1.重要公共或基础设施的详细数据 2.高精度的地理、气象测绘数据等 3.各行业监管部门单独规定的本行业高风险数据等	不共享

附 录 C
（资料性）
数据脱敏内容示例

数据脱敏优化制定的核心内容见表C.1。

表C.1 数据脱敏内容表

脱敏对象	敏感等级	范围	敏感数据	参考脱敏算法	脱敏效果示例
个人敏感信息	三级以上（含三级）数据脱敏规则	财产信息	银行账号	掩码：保留前4位和最后4 位，中间用*代替	854Q301202106561243->854Q**********1234
			鉴别信息(口令)	空值插入：指直接删除敏感数据或将其置为NULL值	abc@123a->null
			存折信息	掩码：保留前4位和最后4位，中间用*代替	64679001100413425->646Z*********3425
			房产信息	限制返回：仅仅返回一部分可用数据，只精确到某个区域	开发区胜利明城9幢2单元301->开发区胜利明城
			车架号	掩码：保留最后6位，其余用*代替	LYAFR7OP3BC722222->**********722222
			车牌号	掩码：保留地区编码和流水号最后2位，其余用*代替	浙AIG8577->浙 A***77
			征信信息	掩码：两个字或三个字的至少1个字用*代替，大于三个字的至少2个字用*代替，保留姓	张三->张* 李二强->李** 夏正华->夏**
机构敏感信息	三级以上（含三级）数据脱敏规则	人事管理信息	人事档案	参考本表，个人敏感信息部分	参考本表，个人敏感信息部分
			职员工资性收入	均化：计算公正性收入平均值，然后使用脱敏后的值在均值附件随机分布	
		内部管理信息	增值税税号	掩码：保留前4位和最后4位，其余用*代替	7263002Y6091020864->7263**********0864
			增值税账号	掩码：保留最后4位，其余用*代替	67271616627053041 30->**************4130

附 录 D
（资料性）
访问权限运行管理机制示例

访问权限运行管理机制落实内容包括：

a) 数据权限申请审批授予。按照数据权限分配、开通、使用、变更、重置、锁定、注销流程的要求，利用访问权限管理工具，对数据权限实施申请审批与授予，建立和维护数据权限清单，详见表 D.1。

表D.1 数据权限角色和权限表

角色名称	角色描述
租户审核受理人员	租户审核受理人员
租户信息资源目录申请人员	租户信息资源目录申请人员
租户访客	拥有租户内资源访问权限，只读权限
租户审计人员	负责租户内操作审计
租户审核人员	负责租户内业务审核
租户测试人员	负责租户内数据开发结果测试
租户数据标准开发人员	负责租户内数据标准开发
租户数据标准管理员	负责租户内数据标准管理
租户质量评估人员	负责租户内数据质量评估开发
租户开发人员	负责租户内任务开发
租户管理员	负责租户内任务开发，工作审批等业务处理及租户内用户、角色、项目等公共配置管理
租户标签申请人员	租户标签申请人员

b) 数据权限常规性变更。针对人员离岗、人员岗位变动、系统迭代、系统下线等变更情况，及时进行权限回收，更新数据权限清单，保证数据权限授予的最小化原则。

c) 数据权限定期核查。按照季度进行数据权限定期核查工作，对沉默账号、过期账号、授权范围过大账号等，进行清理；对数据权限使用行为进行监控检查，针对未落实情况及时核实处置。结果记录详见表 D.2。

表D.2 权限核查结果记录表

2021年第四季度数据权限核查结果记录表			
账号名	权限描述	检查记录	处理结果
×××	×××权限、×××权限、	过期账号	账号禁用
×××	×××权限、×××权限、	授权范围过大	锁定账号，重新规划账号权限
×××	×××权限、×××权限、	异常登录和使用	锁定账号，增加账号授权/登录安全措施
配合检查人员（签字）： 检查人员（签字）： 日 期：			

附 录 E
（资料性）
数据安全事件应急响应

数据安全管理方成立数据安全事件应急协调小组（由数据安全管理方人员组成）、监测工作小组、应急工作小组并定义了各小组职责，安全事件应急响应工作按照以下流程开展：

a) 事件判定。发现数据安全事件时（大数据平台安全模块告警、人工主动上报），经监测工作小组确认后立即向应急工作小组报告数据安全事件具体情况，应急工作小组根据应急预案“事件分级”标准初步判定信息安全事件等级，并向应急协调小组报告。

b) 预案启动。Ⅰ级和Ⅱ级事件（Ⅰ级最高）由应急协调小组组长下达应急预案启动指令，并将事件情况上报监管部门提供侦查、协助处理；Ⅲ级和Ⅳ级事件由应急工作小组组长下达应急预案启动指令并报告应急协调小组，应急工作小组接到启动指令后开展应急处置工作。

c) 应急处置。由应急工作小组组长组织开展应急处置工作并协调内外部人员支撑，应急工作小组按事件等级时限要求，向组长汇报应急处置工作进展情况，并配合系统开发、运维方进行安全漏洞定位、漏洞修复、验证确认等工作。

d) 事件报告。应急工作小组对事件进行研究分析和调查处理，向应急协调小组提供《数据安全事件应急响应报告》，报告内容主要包括事件级别、影响范围、影响后果、事件发展趋势和采取的措施等，应急协调小组根据安全事件等级和具体情况向上级监管部门报告。报告格式详见表E.1。

表E.1 数据安全事件应急响应报告

<table>
<tr><td colspan="6">数据安全事件应急响应报告</td></tr>
<tr><td>事件名称</td><td colspan="2"></td><td colspan="3">报告时间：　　年　月　日　时　分</td></tr>
<tr><td>报告人</td><td></td><td>联系电话</td><td></td><td>部门</td><td></td></tr>
<tr><td>影响系统</td><td colspan="2"></td><td>主要用途</td><td colspan="2"></td></tr>
<tr><td>安全事件描述</td><td colspan="5"></td></tr>
<tr><td>已采取的安全措施</td><td colspan="5"></td></tr>
<tr><td>最终判定事件原因</td><td colspan="5"></td></tr>
<tr><td>事件影响状况评估</td><td colspan="5"></td></tr>
<tr><td>事件级别</td><td colspan="5">□特别重大事件（Ⅰ级）　□较大事件（Ⅱ级）
□较大事件　（Ⅲ级）　□一般事件（Ⅳ级）</td></tr>
<tr><td>影响时间</td><td colspan="5"></td></tr>
<tr><td>影响范围</td><td colspan="5"></td></tr>
<tr><td>事件后果</td><td colspan="5"></td></tr>
<tr><td>主要处理过程及结果</td><td colspan="5"></td></tr>
<tr><td>存在问题及建议</td><td colspan="5"></td></tr>
<tr><td>应急协调小组意见</td><td colspan="5"></td></tr>
<tr><td colspan="6">应急协调小组组长签字：
年　月　日</td></tr>
</table>

参 考 文 献

[1] 浙江省公共数据安全管理总则
[2] 浙江省公共数据访问权限管理规范
[3] 浙江省公共数据安全脱敏技术规范
[4] 浙江省公共数据安全销毁技术规范
[5] 浙江省公共数据安全日志审计规范
[6] 浙江省一体化智能化公共数据平台省级数据回流工作细则