ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL —2026

城市运行“一网统管”数据治理规范

Specifications for Data Governance of the "Unified Management through a Single Network" in Urban Operation

（工作组讨论稿）

（本草案完成时间：2026-01-29）

2026 - - 发布　　2026 - - 实施

广西电子商务企业联合会　发布

目　　次

前　言

本文件依据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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

城市运行“一网统管”数据治理规范

1 引 言

为深入贯彻数字中国建设、国家治理体系和治理能力现代化战略部署，落实全国一体化政务大数据体系建设要求，规范城市运行“一网统管”（以下简称“一网统管”）数据治理全流程工作，提升数据资源质量与要素化利用效能，保障数据安全合规流通，筑牢城市治理科学化、精细化、智能化的数据根基，依据国家相关法律法规、顶层政策文件及国家标准，结合全国“一网统管”建设实践经验，制定本团体标准。本标准适用于全国各级城市“一网统管”建设相关的政府部门、企事业单位及社会组织，作为数据治理工作的统一遵循，旨在推动形成上下协同、标准统一、安全可控、服务高效的数据治理新格局，支撑不同规模城市差异化、精准化治理能力提升，引领行业数据治理规范化发展。

2 范围

本标准规定了“一网统管”数据治理的总体原则、数据资源管理、数据技术管理、数据安全管理、数据服务与运营及监督评价等核心领域的强制性（标注“须”）和推荐性（标注“应”）要求，覆盖数据采集、存储、传输、处理、共享、开放、应用、销毁全生命周期。适用于：全国各级地方人民政府（省、市、县、乡四级）“一网统管”建设牵头部门及运行管理相关主管部门（住建、应急、公安、交通、生态环境、民政等）；参与“一网统管”建设、运营、运维的企事业单位（含国企、民营企业、科研机构）；“一网统管”数据提供、使用、审核等各类参与主体的相关数据治理活动。

3 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 35295-2017 信息技术大数据术语

GB/T 36073-2018 数据管理能力成熟度评估模型

GB/T 37973-2019 信息安全技术大数据安全管理指南

GB/T 22239-2019 信息安全技术网络安全等级保护基本要求

GB/T 38667-2020 信息技术大数据数据分类指南

GB/T 40685-2021 信息技术服务数据资产管理要求

GB/T 41479-2022 信息安全技术网络数据处理安全要求

GB/T 42582-2023 信息安全技术个人信息保护工程指南

GB/T 43782-2024 信息安全技术重要数据识别指南

《中华人民共和国数据安全法》（2021年9月1日起施行）

《中华人民共和国个人信息保护法》（2021年11月1日起施行）

《中华人民共和国网络安全法》（2017年6月1日起施行）

《中华人民共和国数据安全法实施条例》（2024年5月1日起施行）

《国务院关于印发促进大数据发展行动纲要的通知》（国发〔2015〕50号）

《关于建立健全政务数据共享协调机制加快推进数据有序共享的意见》（国办发〔2021〕6号）

《“十四五”数字经济发展规划》（国发〔2021〕29号）

《全国一体化政务大数据体系建设指南》（国办发〔2022〕3号）

《政务数据共享开放条例》（国务院令第764号）

《数据要素市场化配置综合改革试点总体方案》（发改高技〔2022〕1042号）

《关于加强城市运行管理“一网统管”建设的指导意见》（建城〔2023〕17号）

4 术语和定义

GB/T 35295-2017、GB/T 36073-2018、GB/T 43782-2024界定的以及下列术语和定义适用于本标准。

4.1 城市运行“一网统管”

指立足国家治理现代化要求，依托数字技术与全国一体化政务大数据体系，构建全域覆盖、全时响应、协同联动的城市运行管理平台，对城市管理、公共安全、应急指挥、交通出行、生态环境、民生服务等核心领域运行状态进行实时监测、智能预警、联动处置和综合研判的新型城市治理模式，是数字政府建设在城市治理领域的核心载体，核心目标是实现“一网感知态势、一网指挥调度、一网协同处置”。

4.2 数据治理

指围绕数据要素全生命周期，开展规划、组织、监督、控制和优化数据资产管理的一系列系统性活动，涵盖数据采集、存储、传输、处理、共享、开放、应用、销毁等各环节，核心目标是保障数据质量、防控数据风险、促进数据共享、释放数据价值，支撑业务协同与决策科学化，是“一网统管”体系有效运行的核心保障。

4.3 数据资源目录

指按照国家统一标准，对数据资源的分类、元数据、共享属性、安全等级、责任主体、应用场景、更新频率等信息进行规范化描述和结构化组织的清单，是衔接全国一体化政务大数据体系、实现数据跨层级、跨部门、跨区域共享开放和高效利用的基础载体，分为基础目录、部门目录和应用目录。

4.4 数据元

通过一组属性描述其定义、标识、表示和允许值的数据单元，是构建数据标准体系、实现数据一致性的核心基础，须与国家基础数据元标准（GB/T 19488）保持一致，分为基础数据元和业务数据元。

4.5 主数据

描述核心业务实体（如人员、组织、地点、物品、事件等）的关键、共享、权威的数据，在多个业务系统和跨部门流程中被重复使用，具有稳定性、唯一性和权威性特征，是保障数据“一数一源、全域一致”的核心支撑。

4.6 数据血缘

描述数据从源头产生到最终应用全流程中的流转路径、转换关系、处理规则和操作历史的元数据集合，分为技术血缘（数据流转的技术链路）和业务血缘（数据关联的业务场景），是实现数据溯源、影响分析、责任追溯的重要手段。

4.7 数据服务

以数据为核心要素，通过标准化接口（如API、SDK等）向用户提供数据访问、查询、核验、分析、可视化等能力的功能单元，分为基础数据服务、增值数据服务，是推动数据资源向数据要素转化、支撑业务应用的核心形态。

4.8 核心数据

指关系国家安全、国民经济命脉、重要民生和公共利益，一旦泄露、篡改或滥用可能造成严重后果的数据，须纳入国家重要数据保护范围，实行重点防护。

4.9 数据要素市场化配置

指通过市场化机制，规范数据要素流通交易，发挥数据要素在资源配置中的核心作用，实现数据价值最大化的过程，“一网统管”数据要素配置须遵循合法合规、安全可控、公平高效原则。

5 总体原则

5.1 统筹规划，顶层引领

须衔接全国一体化政务大数据体系建设要求，在城市级层面进行统一规划和顶层设计，建立健全跨部门、跨层级、跨区域的数据治理协同机制，明确各级主体职责分工，打破数据壁垒和信息孤岛，避免重复建设和资源浪费。数据治理规划须与城市发展战略、国土空间规划、数字政府建设规划深度融合，确保上下协同、全域统筹。

5.2 依法依规，安全可控

须严格遵守国家数据安全、网络安全、个人信息保护等法律法规和标准规范，坚持总体国家安全观，建立健全数据全生命周期安全防护体系，落实数据安全主体责任和领导责任制。强化安全风险防控和应急处置能力，确保国家秘密、商业秘密和个人隐私安全，保障数据治理活动合法合规、安全可控。

5.3 一数一源，标准统一

须确立数据唯一权威来源，统一数据采集、存储、传输、处理、应用等各环节的标准规范，严格对接国家基础数据标准和行业标准。确保同一数据在不同层级、不同部门、不同系统间的一致性、准确性和可比性，从源头提升数据质量，为跨部门业务协同奠定基础。

5.4 质量为先，闭环迭代

应将数据质量作为数据治理的核心目标，建立覆盖数据全生命周期的质量管理闭环体系，明确数据质量责任主体，细化质量评价指标。持续开展数据质量监测、核查、问题整改、效果评估和优化迭代，实现数据质量动态提升，支撑数据可靠应用。

5.5 共享为常态，不共享为例外

在保障安全和隐私的前提下，须严格落实国家政务数据共享开放要求，以促进数据要素有序流通和高效利用为核心，明确数据共享开放范围和边界。除法律法规明确禁止共享的情形外，各类政务数据应无条件或有条件共享，最大限度释放数据要素价值，支撑“一网统管”协同治理。

5.6 业务驱动，实用高效

数据治理活动应紧密对接城市运行管理核心业务需求，聚焦应急处置、民生保障、公共安全、交通治理、生态环保等关键应用场景，以实际应用效果为导向。确保治理成果可用、管用、好用，实现数据治理与业务工作深度融合、双向赋能，避免形式化治理。

5.7 前瞻布局，稳步落地

应积极顺应数字技术发展趋势，合理融入大数据、人工智能、隐私计算、区块链等新技术应用，提升数据治理智能化水平。同时兼顾实操性，结合城市规模和发展阶段，制定差异化的实施路径，确保前瞻性技术与本地实践有机结合、稳步落地。

6 数据资源管理

6.1 数据资源梳理与编目

6.1.1 应全面梳理城市运行管理各部门、各层级的业务职能、信息系统架构和数据资源现状，摸清数据来源、格式、规模、更新频率、关联关系、责任主体等核心信息，形成全域覆盖、底数清晰的数据资源清单，梳理完成后须报城市“一网统管”牵头部门备案。

6.1.2 应依据全国一体化政务数据资源目录编制标准，结合城市运行管理特点，编制覆盖市、区（县）、街道（乡镇）、社区（村）四级联动的“一网统管”数据资源目录，实现与国家、省级数据资源目录的无缝对接和同步更新。

6.1.3 数据资源目录应包含但不限于以下核心元数据：数据资源名称、摘要、提供方、格式、更新频率、共享类型（无条件共享、有条件共享、不予共享）、开放类型（普遍开放、依申请开放、不予开放）、安全等级、关键词、关联业务事项、使用范围、责任联系人、数据元关联信息等，确保目录信息完整规范。

6.1.4 应建立数据资源目录动态管理闭环机制，明确更新流程、责任主体和时限要求，对新增、变更、注销的数据资源，须在5个工作日内完成目录更新和维护，并通过统一的数据共享开放平台向社会和相关部门提供目录查询服务。

6.2 数据分类分级

6.2.1 应参照GB/T 38667-2020及全国一体化政务大数据分类标准，结合城市运行管理核心业务场景，对数据资源进行科学分类，至少应区分以下类别：基础信息数据、人口信息数据、法人信息数据、空间地理信息数据、城市部件与事件数据、公共安全数据、应急管理数据、交通运行数据、生态环境数据、民生服务数据、宏观经济数据、政务服务数据，分类结果须与国家政务数据分类体系保持一致。

6.2.2 须严格依据《中华人民共和国数据安全法》《数据安全法实施条例》及GB/T 43782-2024，建立与国家数据分级体系衔接的数据分级标准，数据级别至少应包括：公开数据、内部数据、敏感数据、核心数据。其中，核心数据应纳入国家重要数据保护范围，明确判定标准和清单，报上级主管部门备案。

6.2.3 应对不同级别的数据，在采集、存储、传输、使用、共享、开放、销毁等全流程环节制定差异化的安全管理策略和技术防护措施，核心数据和敏感数据须实施重点防护，建立专项管理机制。

6.2.4 数据分类分级工作应定期开展复核，至少每年一次，根据国家政策调整、业务需求变化和安全风险评估结果，及时优化分类分级标准和清单。

6.3 数据标准管理

6.3.1 应建立并持续维护与国家、行业标准衔接的“一网统管”数据标准体系，涵盖基础标准、数据元标准、代码集标准、主数据标准、数据交换标准、数据质量标准、数据安全标准、数据服务标准等核心领域，形成完整的标准规范体系，标准体系须报城市“一网统管”牵头部门备案。

6.3.2 须严格遵循国家基础数据元标准（GB/T 19488），制定城市运行管理核心数据元标准，统一关键数据项的名称、定义、标识、格式、值域、代码等要求。重点规范“统一社会信用代码”“公民身份号码”“地址”“城市部件编码”“应急事件分类”等核心数据元的定义和表示规范，核心数据元标准应与国家、省级标准保持一致。

6.3.3 应建立标准符合性审查机制，将数据标准遵循情况纳入信息系统立项、建设、验收和运维的全流程管理，新建信息系统须通过标准符合性审查方可立项；存量系统改造须在规定时限内完成标准适配，不符合标准的数据资源不予接入“一网统管”平台。

6.3.4 应建立数据标准动态更新机制，根据国家政策调整、行业标准更新和城市治理需求变化，及时修订完善数据标准体系，并做好标准宣贯和培训工作，确保各参与主体准确掌握和执行标准。

6.3.5 应建立标准执行情况监测评估机制，定期开展标准执行效果评估，至少每半年一次，根据评估结果优化标准内容和执行流程。

6.4 数据质量管理

6.4.1 应建立覆盖数据全生命周期的质量管理体系，明确数据质量目标、管理组织、职责分工、工作流程和评价指标，将数据质量责任落实到具体部门和岗位，形成“谁产生、谁负责，谁使用、谁反馈，谁治理、谁监督”的责任机制。

6.4.2 应明确数据质量核心维度，至少包括：准确性、完整性、一致性、时效性、可用性和唯一性，并为各维度设定可量化、可考核的评估指标（示例见附录A），建立科学的质量评价模型。

6.4.3 应建立数据质量监控、核查、问题发现、整改、跟踪和评价的闭环管理流程，鼓励采用大数据、人工智能等技术工具开展自动化质量检核，实现数据质量问题早发现、早处置。对发现的质量问题，须明确整改责任主体和时限，整改完成后进行复核，确保问题整改到位。

6.4.4 应建立数据质量问责机制，将数据质量评价结果纳入相关部门和人员的绩效考核体系，对数据质量严重不达标、造成重大影响的单位和个人依法依规追究责任。

6.4.5 应定期开展数据质量综合评估，至少每季度一次，形成质量评估报告，作为优化数据治理策略和流程的重要依据。

6.5 数据资产管理

6.5.1 应参照GB/T 40685-2021及国家数据资产登记管理要求，对“一网统管”涉及的数据资产进行全面登记、确权、估值和运营，建立数据资产管理制度，明确数据资产权属和管理责任，数据资产登记信息须纳入全国政务数据资产登记系统。

6.5.2 应建立标准化的数据资产目录，清晰描述数据资产的基本信息、业务信息、技术信息、管理信息和价值信息，实现数据资产可管、可控、可追溯，数据资产目录应与数据资源目录联动更新。

6.5.3 应积极探索符合国家要求的数据资产价值评估方法和定价机制，结合数据资产的稀缺性、可用性、安全性、合规性等因素，开展数据资产价值评估试点，形成可复制、可推广的评估模式，为数据要素市场化配置奠定基础。

6.5.4 应建立数据资产运营监测机制，定期评估数据资产利用效率和价值释放情况，至少每半年一次，优化数据资产配置，提升数据资产价值。

6.5.5 数据资产运营应遵循合法合规、安全可控原则，禁止违规交易和滥用数据资产，保障数据资产流转安全。

7 数据技术管理

7.1 数据架构管理

7.1.1 应设计科学合理、适配全国一体化政务大数据平台架构的“一网统管”数据架构，明确数据源层、数据采集层、数据存储与计算层、数据治理层、数据服务层和数据应用层的功能定位和技术要求，实现各层级无缝衔接、协同联动，架构设计须报上级政务数据主管部门备案。

7.1.2 应推动数据存储的合理布局，根据数据热度、访问频率、安全等级、存储周期等因素，采用在线、近线、离线等分层存储策略，结合分布式存储、云存储等技术，构建高效、可靠、可扩展的数据存储体系，满足海量数据存储需求。核心数据须采用多副本存储，确保数据可靠性。

7.1.3 应构建逻辑集中、物理分布的城市运行管理主题数据库、专题数据库和业务库，聚焦应急指挥、交通治理、生态环保等核心场景，推进多源数据融合分析，支撑城市运行管理深度应用和智能决策。主题数据库建设应遵循国家政务数据主题库建设标准。

7.1.4 数据架构设计应兼顾稳定性和灵活性，支持新技术应用和业务场景扩展，符合国家政务信息系统集约化建设要求，避免技术架构碎片化。应定期开展架构适配性评估，至少每年一次，根据评估结果优化架构设计。

7.2 数据集成与交换

7.2.1 须依托全国一体化政务数据共享交换平台，建立统一、高效、安全的“一网统管”数据交换共享平台，支撑跨部门、跨层级、跨区域、跨系统的数据安全流通，实现与国家、省级数据交换平台的互联互通，平台建设须符合国家政务数据交换平台技术标准。

7.2.2 数据交换应优先采用标准化服务接口（API）方式，减少批量文件交换，接口设计应符合国家政务数据交换接口标准，具备可监控、可管理、可追溯、高可用等特性，支持数据实时和准实时交换。接口调用应进行身份认证和权限管控。

7.2.3 须实现关键数据全流程数据血缘追踪，完整记录数据从源头到消费端的流转路径、转换规则、操作主体和时间等信息，支持数据影响分析、问题溯源和责任追溯。核心数据血缘信息须永久留存。

7.2.4 应建立数据交换异常处理机制，对数据交换过程中的中断、错误、延迟等异常情况进行实时监测和自动告警，告警响应时限不超过30分钟，及时处置并恢复数据交换，确保数据交换连续可靠，异常处置情况须记录存档。

7.3 数据平台与技术工具

7.3.1 应采用成熟稳定、安全可控、自主创新的技术平台和工具，支撑海量多源异构数据的采集、存储、计算、治理和服务，优先选用通过国家安全审查的国产化软硬件产品，提升技术自主可控水平，核心技术产品须纳入国家自主创新产品目录。

7.3.2 平台应具备数据集成、数据开发、数据质量管控、数据资产管理、数据服务编排、数据安全管控、可视化分析等核心功能，支持分布式计算、流式计算等技术，满足海量数据高效处理需求，平台性能指标应符合国家政务大数据平台性能要求。

7.3.3 应积极运用大数据、人工智能、隐私计算、区块链等新技术，提升数据治理的智能化水平、数据价值挖掘能力和数据安全防护能力。探索隐私计算在跨部门数据共享中的应用，实现“数据可用不可见”；运用区块链技术实现数据溯源和责任追溯，确保数据流转可信任。

7.3.4 应建立技术平台和工具运维管理机制，定期开展系统巡检、性能优化、安全加固和版本升级，至少每月一次系统巡检，每季度一次性能优化和安全加固，确保平台稳定运行，运维记录须存档备查。

7.3.5 应建立技术人员培训机制，定期开展技术培训和技能考核，提升技术人员的数据治理能力和安全防护意识，培训记录须存档备查。

8 数据安全管理

8.1 安全总体要求

8.1.1 须严格遵守《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》《中华人民共和国网络安全法》、GB/T 22239-2019、GB/T 37973-2019和GB/T 41479-2022等法律法规和标准要求，落实网络安全等级保护2.0制度，建立健全数据安全治理体系，数据安全管理须纳入城市网络安全工作总体部署。

8.1.2 须明确数据安全责任部门和管理职责，制定数据安全总体策略和管理制度，建立跨部门数据安全协同工作机制，定期开展数据安全风险评估，至少每半年一次，落实数据安全主体责任和领导责任制，安全责任须层层压实。

8.1.3 数据处理活动应符合国家网络安全等级保护制度要求，根据数据分级结果和业务场景重要性，实施差异化的安全防护措施，核心数据和敏感数据须采取最高级别的安全防护，安全防护措施须定期开展合规性检测。

8.1.4 须将数据安全纳入“一网统管”体系建设全流程，开展安全同步规划、同步建设、同步运行，确保安全措施贯穿数据全生命周期，安全设施建设投入占比不低于“一网统管”建设总投入的15%。

8.2 全生命周期安全管控

8.2.1 数据采集安全：明确数据采集源和采集范围，确保采集行为合法合规，不得超范围采集数据。对采集个人信息的，应依法取得个人同意或符合法定情形，明确采集目的和使用范围，做好采集记录，采集记录须留存至少3年。

8.2.2 数据传输安全：须采用加密传输通道（如HTTPS、VPN、专线等）保障数据传输过程中的机密性和完整性，建立数据传输身份认证和授权机制，防止数据传输过程中被窃取、篡改或泄露，传输日志须留存至少6个月。

8.2.3 数据存储安全：根据数据分级采取加密存储、访问控制、数据脱敏、备份恢复等安全措施，核心数据和敏感数据须采用加密存储，加密算法须符合国家密码标准。建立数据存储备份和容灾恢复机制，核心数据须实现实时备份，备份数据须异地存放，定期开展备份演练，至少每季度一次，确保数据可恢复。

8.2.4 数据使用安全：建立严格的访问授权和审批流程，遵循最小必要原则授予访问权限，对敏感数据和核心数据的使用进行安全审计和操作留痕，操作日志须留存至少1年。禁止未经授权使用和泄露数据，对异常访问行为实时监测和告警。

8.2.5 数据共享与开放安全：在进行数据共享和开放前，须开展安全风险评估，对共享和开放数据进行脱敏、脱密处理，符合安全和隐私保护要求。共享数据应通过统一平台进行，建立共享数据使用监管机制；开放数据应经过严格的脱敏和审核，确保不泄露国家秘密、商业秘密和个人隐私，开放数据审核记录须留存至少3年。

8.2.6 数据销毁安全：建立数据销毁管理制度，明确数据保存期限，对不再需要且超过保存期限的数据，采用不可恢复的方式安全销毁，做好销毁记录，销毁记录须留存至少3年。销毁过程须进行全程监督，确保数据彻底清除。

8.3 个人信息与重要数据保护

8.3.1 处理个人信息应遵循合法、正当、必要和诚信原则，公开处理规则，明示处理目的、方式和范围，不得非法收集、使用、加工、传输、提供、公开个人信息，个人信息处理活动须符合《个人信息保护法》及相关标准要求。

8.3.2 须建立个人信息保护影响评估机制，在处理敏感个人信息、利用个人信息进行自动化决策、委托处理个人信息、向第三方提供个人信息等场景下，必须开展个人信息保护影响评估，并留存评估报告至少3年。

8.3.3 须识别城市运行管理中的重要数据，参照国家重要数据目录，建立本地重要数据保护目录，实施更加严格的安全保护措施，定期向有关主管部门报备重要数据处理情况，报备周期不超过6个月。

8.3.4 对涉及个人信息和重要数据的操作，须建立全程审计和追溯机制，确保操作行为可追溯、责任可追究，审计记录须留存至少1年。

8.3.5 禁止向境外提供核心数据和重要数据，确需提供的，须按照国家相关规定办理安全评估手续，未经评估或评估未通过的，不得向境外提供。

8.4 安全监测与应急响应

8.4.1 须建立数据安全监测预警机制，部署安全监测设备和工具，实时监测数据泄露、篡改、滥用等安全事件和异常行为，及时发出安全预警，预警响应时限不超过15分钟，提升安全事件发现能力。

8.4.2 须制定数据安全事件应急预案，明确应急组织架构、应急响应流程、处置措施和责任分工，定期组织应急演练，至少每年一次，提升应急处置能力，演练记录须留存备查。

8.4.3 发生数据安全事件时，须立即启动应急预案，采取有效处置措施，控制风险扩大，按照国家相关规定及时向有关主管部门报告，报告时限不超过2小时，并通知受影响的个人和单位，做好后续善后工作，事件处置记录须留存至少3年。

8.4.4 应建立跨部门、跨区域数据安全应急协同机制，加强与公安、网信、应急等部门的沟通协作，提升重大数据安全事件联合处置能力，定期开展协同应急演练，至少每半年一次。

9 数据服务与运营

9.1 数据共享管理

9.1.1 应基于数据资源目录，建立“需求提出、申请审核、授权使用、效果评价、动态优化”的全流程数据共享闭环流程，简化审核环节，无条件共享数据审核时限不超过1个工作日，有条件共享数据审核时限不超过3个工作日，提升共享效率，确保数据按需共享。

9.1.2 依托统一的数据共享交换平台，为各部门、各层级提供便捷、高效、安全的数据共享服务，支持批量数据共享和实时接口调用，满足跨部门业务协同需求，平台服务可用性不低于99.9%。

9.1.3 建立共享数据使用效果反馈机制，定期收集数据使用部门的反馈意见，至少每季度一次，持续优化共享数据内容和质量，提升数据共享服务水平，反馈处理结果须及时向使用部门回复。

9.1.4 禁止数据使用部门将共享数据用于与业务无关的用途，禁止未经授权向第三方转让、泄露共享数据，对违规使用共享数据的行为依法依规追究责任，违规行为处理结果须存档备查。

9.2 数据开放管理

9.2.1 在保障安全和个人隐私的前提下，按照国家公共数据开放要求，制定“一网统管”公共数据开放目录，明确开放数据的范围、格式、更新频率和使用条件，通过政府数据开放平台向社会有序开放数据，开放目录至少每年更新一次。

9.2.2 开放数据应提供多种可机读格式（如JSON、XML、CSV等），并提供清晰的元数据描述、使用指南和接口说明，方便社会公众和企业获取使用，开放数据更新频率不低于每月一次（静态数据除外）。

9.2.3 鼓励社会力量对开放数据进行创新应用，培育数据应用生态，提升数据社会价值和经济价值，对优秀数据应用案例进行推广示范，定期开展优秀案例评选活动，至少每年一次。

9.2.4 建立开放数据使用监管机制，对开放数据的使用情况进行监测，及时处置违规使用开放数据的行为，确保开放数据安全合规利用，违规行为处置结果须向社会公开（涉及隐私的除外）。

9.3 数据服务化

9.3.1 推动数据资源向数据服务转变，将常用数据查询、分析、核验、可视化等能力封装成标准、可复用的数据服务接口（API），统一接口规范和调用流程，提升数据服务的易用性和可扩展性，接口响应时间不超过500毫秒。

9.3.2 建立数据服务市场或商店，对数据服务进行统一发布、申请、授权、计量和计费管理，实现数据服务的规范化运营，支撑数据要素市场化配置，计费标准须符合国家相关规定。

9.3.3 围绕城市运行管理核心业务场景，为“一网统管”各业务应用提供便捷、稳定的数据服务支撑，实现数据服务与业务应用深度融合，提升业务办理效率和决策科学性，数据服务支撑业务覆盖率不低于95%。

9.3.4 建立数据服务质量评价机制，定期评估数据服务的可用性、稳定性、准确性和响应速度，至少每季度一次，持续优化数据服务质量，评价结果须作为服务优化的重要依据。

9.4 数据运营与生态建设

9.4.1 设立专门的数据运营团队或明确运营职责，负责数据资产的日常运营、推广和价值挖掘，制定数据运营计划，提升数据资源利用效率，运营计划至少每年更新一次。

9.4.2 建立数据治理社区，组织开展数据治理培训、交流研讨等活动，提升各参与方的数据意识、业务能力和技术水平，营造良好的数据治理氛围，培训活动至少每半年一次。

9.4.3 推动产学研用合作，联合高校、科研机构、企业等力量开展数据治理技术研发、应用创新和标准制定，构建健康、可持续的城市数据生态，合作项目须定期开展成果评估。

9.4.4 探索建立数据要素激励机制，鼓励数据提供方和使用方积极参与数据治理和应用创新，激发数据要素活力，激励措施须符合国家相关法律法规要求。

10 监督与评价

10.1 监督机制

10.1.1 城市“一网统管”建设牵头部门应牵头负责数据治理工作的统筹协调、监督指导和考核评估，建立健全跨部门监督工作机制，定期开展数据治理专项监督检查，至少每半年一次，检查结果须向同级政府报告。

10.1.2 各相关部门和单位应建立健全内部数据治理监督机制，明确监督职责，定期开展内部自查自纠，至少每季度一次，确保本标准要求落实到位，自查结果须存档备查。

10.1.3 鼓励引入第三方专业机构对数据治理能力、数据安全、数据质量、服务效能等进行独立审计和评估，提升监督的专业性和公正性，审计评估结果作为改进工作的重要依据，第三方审计评估至少每年一次。

10.1.4 建立社会监督机制，公开监督举报渠道，接受社会公众对数据治理工作的监督举报，举报响应时限不超过2个工作日，及时回应社会关切，举报处理结果须向举报人反馈。

10.2 评价与改进

10.2.1 应建立科学完善的数据治理成效评价指标体系（示例见附录B），定期对数据治理工作的组织、制度、过程、技术和成效进行综合评价，核心指标可包括：数据资源目录覆盖率、数据标准遵循率、数据质量问题解决率、数据共享需求满足率、数据服务调用量、数据安全事件发生率、业务应用赋能效果等，综合评价至少每半年一次。

10.2.2 应定期开展数据治理成熟度评估，至少每年一次，参考GB/T 36073-2018数据管理能力成熟度评估模型，结合国家相关要求和城市实际情况，开展成熟度评级，识别存在的问题和改进方向，评估结果须报上级主管部门备案。

10.2.3 须将数据治理评价结果纳入地方政府绩效考核和相关部门履职评价体系，权重不低于5%，强化评价结果运用，推动各部门落实数据治理责任，考核结果作为评优评先的重要依据。

10.2.4 应根据评价结果、国家政策调整和业务发展需求，制定针对性的改进措施，建立数据治理持续改进机制，明确改进责任主体和时限，定期跟踪改进效果，实现数据治理能力的迭代提升，更好支撑“一网统管”体系建设和城市治理现代化。

11 附则

本标准由广西电子商务企业联合会负责解释。本标准自发布之日起试行，试行期为一年。试行期满

后，根据实施反馈情况进行修订和完善。各相关单位可依据本标准制定具体的实施细则。若本标准与国家新颁布的法律法规或强制性标准有不一致之处，应以国家法律法规和强制性标准为准。本标准所引用的规范性引用文件如有更新，其最新版本适用于本标准。广西电子商务企业联合会将根据技术发展和应用需求，适时组织对本标准的复审与修订工作，以保障其持续的先进性和适用性。本标准的有效实施，有赖于各级医疗机构、主管部门、技术服务商和各相关方的共同努力，通过规范智慧医院数据互联互通共享技术，推动医疗健康数据资源有效整合与安全共享，提升医疗服务质量和效率，促进智慧医院建设规范化发展，为推进健康中国建设提供技术支撑。