

ICS XXXX

CCS X XX

团体标准

T/SISA XXXX-XXXX

“一网统管”数据安全能力要求

“One network unified management” data security capability requirements

(征求意见稿)

20XX-XX-XX 发布

20XX-XX-XX 实施

上海市信息安全行业协会

发布

目次

前言..... III

引言..... IV

1 范围..... 1

2 规范性引用文件..... 1

3 术语和定义..... 1

 3.1 一网统管 one network unified management..... 1

 3.2 数据安全 data security..... 1

 3.3 数据安全能力 data security capability..... 1

 3.4 公共管理和服务机构 public management and service institutions 2

4 “一网统管”平台..... 2

 4.1 “一网统管”业务数据..... 2

 4.2 “一网统管”业务场景..... 2

 4.3 整体架构..... 3

 4.4 核心架构..... 3

5 “一网统管”数据安全基本原则..... 4

 5.1 保密性..... 4

 5.2 完整性..... 4

 5.3 隐私性..... 4

 5.4 合规性..... 4

 5.5 分类分级..... 4

6 “一网统管”数据安全职责划分..... 4

 6.1 概述..... 4

 6.2 数据归集阶段..... 5

 6.3 数据加工阶段..... 5

 6.4 数据共享阶段..... 5

7 “一网统管”数据安全管理能力要求..... 5

 7.1 组织管理..... 5

 7.2 制度流程..... 6

 7.3 人员管理..... 6

 7.4 合作方管理..... 7

8 “一网统管”数据安全运营能力要求..... 7

 8.1 分类分级..... 7

 8.2 风险评估..... 7

 8.3 认证授权..... 8

 8.4 监测预警..... 8

 8.5 安全审计..... 8

 8.6 应急处置..... 9

9 “一网统管”数据处理活动安全能力要求.....9

 9.1 数据采集 9

 9.2 数据存储 9

 9.3 数据传输 10

 9.4 数据加工使用 10

 9.5 数据开放共享 10

 9.6 数据删除销毁 11

参 考 文 献.....12

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。

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。

本文件由上海市信息安全行业协会归口。

本文件主要起草单位：上海市杨浦区城市运行管理中心、上海赛博网络安全产业创新研究院、杭州阿里云飞天信息技术有限公司、上海电信工程有限公司、上海脉策数据科技有限公司、上海汉邦京泰数码技术有限公司、上海络安信息技术有限公司。

本文件主要起草人：闫俊平、薄凌云、骆华、惠志斌、周雨霏、卢虹羽、李宁、杨鸣、王成瑜、王岚、刘晨、周群。

引 言

城市运行“一网统管”，是提升城市治理科学化、精细化、智能化水平的重要抓手。“一网统管”属于综合性、融合性场景应用，参与者众多、主体多元，汇聚各类静态数据和动态数据，需要配套完善的标准制度作为支撑。当前，在“一网统管”数据安全能力领域，尚无相关国家、地方和团体标准规范。但在“一网统管”平台建设管理中，出现了业务场景和处置对象更加复杂和特殊，接入部门数据安全能力参差不齐等问题，制定“一网统管”数据安全能力标准有利于保障数据安全，解决管理痛点。

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，经调查研究，充分借鉴和吸收了杨浦区城市运行管理中心“一网统管”的建设经验，参考国内先进标准，在广泛征求意见的基础上进行编制，为上海市公共管理和服务机构开展“一网统管”数据安全能力建设提供参考。

“一网统管”数据安全能力要求

1 范围

本文件规定了“一网统管”数据安全能力要求，文件内容包括“一网统管”平台的架构、数据安全基本原则、数据安全职责划分，以及对“一网统管”数据安全管理能力、数据安全运营能力、数据处理活动方面安全能力的要求。

本文件适用于上海市公共管理和服务机构开展“一网统管”数据安全保护工作，为其数据安全能力建设提供参考和指引。

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 37988—2019 信息安全技术 数据安全能力成熟度模型

DB31/T 1446—2023 公共数据安全分级指南

3 术语和定义

GB/T 25069—2022、GB/T 43697—2024界定的以及下列术语和定义适用于本文件。

3.1 一网统管 one network unified management

“一网统管”以数据和技术为支撑，通过数据汇聚、治理、分析、管理，使用算法充分挖掘数据价值，以数据流驱动业务流程再造，推动跨层级、跨部门、跨平台“高效处置一件事”，构建经济、社会、城市三大治理统筹推进和有机衔接治理体系，赋能高质量发展、高品质生活和高效能治理。

3.2 数据安全 data security

是指通过采取必要措施，确保数据处于有效保护和合理利用的状态，以及具备保障持续安全状态的能力。

[来源：GB/T 37988—2019]

3.3 数据安全能力 data security capability

组织机构在组织建设、制度流程、技术工具以及人员能力等方面对数据的安全保障能力。

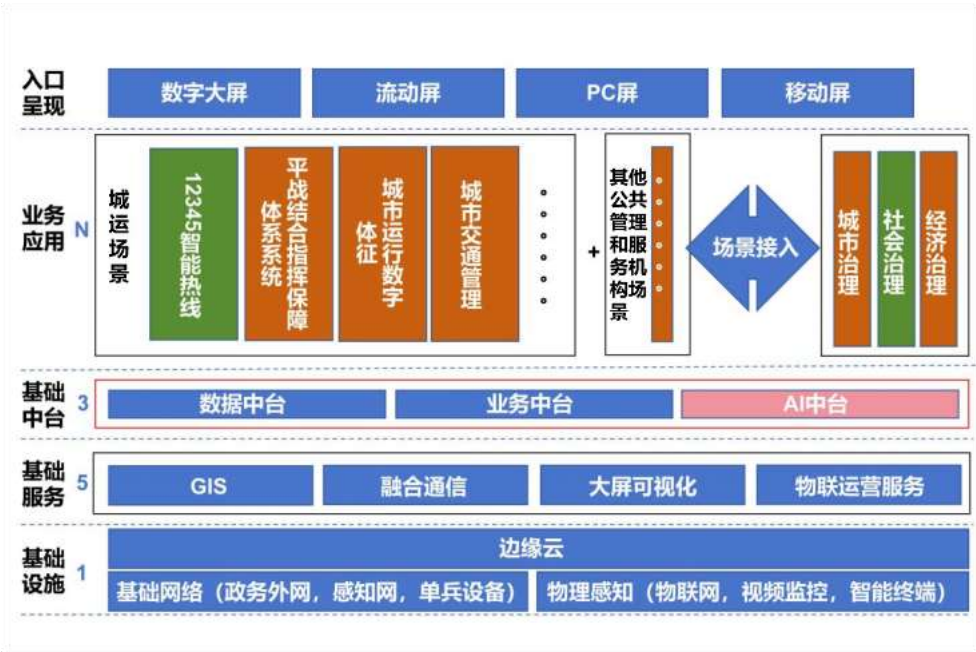
[来源：GB/T 37988—2019]

3.4 公共管理和服务机构 public management and service institutions

国家机关、事业单位，经依法授权具有管理公共事务职能的组织，以及供水、供电、供气、公共交通等提供公共服务的组织。

[来源：DB31/T 1446—2023]

4 “一网统管”平台



图：“一网统管”平台示例

4.1 “一网统管”业务数据

“一网统管”业务数据是公共管理和服务机构在依法履行公共管理和公共服务职责过程中收集和产生的数据，包含发现、受理、立案、派遣、处置、核查、结案、监督、评价等环节数据，包括：“人、地、事、物、情、组织”基础数据、服务类数据等。

4.2 “一网统管”业务场景

4.2.1 城市治理

“一网统管”城市治理业务场景包括但不限于如下内容：

- a) 自然资源高效利用
- b) 城市精细化建设管理
- c) 韧性城市
- d) 平安城市
- e) 数字生态环境保护

4.2.2 社会治理

“一网统管”社会治理业务场景包括但不限于如下内容：

- a) 党建
- b) 个人数字服务
- c) 数字法治

4.2.3 经济治理

“一网统管”经济治理业务场景包括但不限于如下内容：

- a) 企业全生命周期服务
- b) 经济综合运行分析
- c) 综合监管

4.3 整体架构

4.3.1 三级平台

“一网统管”的三级平台包括：

- a) 市级平台：重点进行标准建设，统管全局；
- b) 区级平台：重点在连通上下、衔接左右，发挥系统枢纽和实战平台作用；
- c) 街道平台：重点形成基层综合执法和联勤联动的新机制。

4.3.2 五级应用

“一网统管”五级应用履行各自管理职能，每一级为下一级赋能，上一级帮助下一级解决共性难题，并开展疑难杂症会商，共同确保城市安全有序运行。“一网统管”五级应用包括：

- a) 市级应用
- b) 区级应用
- c) 街道应用
- d) 网格应用
- e) 居委应用

4.4 核心架构

4.4.1 入口呈现层

“一网统管”入口呈现层针对不同用户提供多样化的人机交互系统界面，通过数字大屏、流动屏、PC屏、移动屏等，为组织机构、用户等展现应用层的信息资源，搭建应用场景和用户交互的桥梁。

4.4.2 业务应用层

“一网统管”业务应用层是实际功能的集合，来自业务管理的实际应用场景，“一网统管”平台全面覆盖城市治理、社会治理、经济治理应用场景。

- a) 城市运行是“一网统管”平台的核心业务应用，包括交通、环保、应急应用等；
- b) 社会治理是“一网统管”平台的重要业务应用，包括网格化管理、12345 政务服务应用等；
- c) 经济治理是“一网统管”平台的特色业务应用，包括招商引资、产业发展应用等。

4.4.3 基础中台层

“一网统管”基础中台层是平台的业务中台，包括数据中台、业务中台、AI中台等；

- a) 数据中台是“一网统管”平台的数据存储，数据汇集的基础，包括城运主题库等；
- b) 业务中台是“一网统管”平台的事件流程、事件处理的基础，是业务支撑和流程中心；
- c) AI中台是“一网统管”平台搭建智能应用、智能决策的基础。

4.4.4 基础服务层

“一网统管”基础服务层是平台的基础支撑服务，包括数据服务、应用服务、安全服务等；

- a) GIS 是“一网统管”平台的数据共享、交换、分析基础；
- b) 融合通信是“一网统管”平台的跨部门信息共享与协同的通信基础；
- c) 大屏可视化是“一网统管”平台重要的数据展示方式，用于实时监控、应急指挥等；
- d) 物联运营服务是“一网统管”平台的物联感知基础。

4.4.5 基础设施层

“一网统管”基础设施层是平台的底层支撑，包括基础网络、感知设施、数据中心等；

- a) 基础网络是“一网统管”平台的数据传输算力底座，包括政务外网、感知网、互联网等；
- b) 物理感知是“一网统管”平台的数据采集算力底座，包括物联网、视频监控、智能终端等；
- c) 边缘云是“一网统管”平台网络边缘的计算位置，以及这些物理位置上的硬件和软件。

5 “一网统管”数据安全基本原则

5.1 保密性

采用技术和管理手段保证“一网统管”业务数据的保密性，并记录数据处理日志及确保日志的保密性。

5.2 完整性

采用完整性校验的技术和管理手段，并对“一网统管”业务数据的完整性进行监测。

5.3 隐私性

采用技术和流程以保护个人信息主体的个人信息，涉及个人信息的情形应符合GB/T 35273等国家标准的有关要求。

5.4 合规性

数据处理活动应符合法律法规、政策文件、标准规范等的相关要求。

5.5 分类分级

对“一网统管”业务数据进行分类和分级，并对不同类别不同级别的数据建立相应的全流程数据安全保护措施。涉及敏感个人信息的，宜采取更强的保护措施。

6 “一网统管”数据安全职责划分

6.1 概述

对公共管理和服务机构进行“一网统管”平台数据安全职责划分时，应从数据归集阶段、数据加工阶段、数据共享阶段考虑。数据归集阶段涉及数源单位等数据资源提供方，和作为数据归集部门的城市运行管理中心；在数据加工阶段涉及城市运行管理中心等数据加工部门和第三方供应商；在数据共享阶段，涉及城市运行管理中心等共享数据提供方，和接入“一网统管”平台的其他公共管理和服务机构等共享数据接收方。

6.2 数据归集阶段

6.2.1 数据资源提供方

数据资源提供方的数据安全职责包括但不限于：

- a) 负责本单位的数据治理，保证推送到前置机的数据符合质量规范要求和安全要求，并满足应用需求；
- b) 负责本单位数据采集和后续使用的安全：遵循合法正当、最小必要原则收集数据，科学合理界定本单位允许流通的公共数据范围，评估、审批城市运行管理中心在具体场景下的数据使用需求。

6.2.2 数据归集部门

数据归集部门的数据安全职责包括但不限于：

- a) 负责数据归集和清洗加工，保证经过清洗和转换后的数据符合质量规范要求和安全要求；
- b) 负责“一网统管”平台（包括其子平台、城市运行场景业务库、前置机等）的安全；
- c) 负责传输通道的安全，监测数据传输情况，发现异常情况及时通知相关机构并立即停止相关服务；
- d) 负责数据的安全存储，对数据泄漏情况进行监测。

6.3 数据加工阶段

6.3.1 数据加工部门

数据加工部门的数据安全职责包括但不限于：

- a) 负责数据的安全开发，形成城市运行场景业务库，避免发生数据滥用或损害数据主体合法权益的情况；对公共数据与社会数据的融合开发负安全责任；
- b) 对选择和监督第三方供应商负安全责任。

6.3.2 第三方供应商

第三方供应商的数据安全职责包括但不限于：

- a) 对其提供的技术产品和服务，以及受委托处理公共数据的行为负安全责任；
- b) 承担数据保密义务，不恶意留存所接触到的数据；
- c) 配合、接受相关的安全背景调查、资质审查与能力评估，提供充分的证明材料。

6.4 数据共享阶段

6.4.1 共享数据的提供方

共享数据的提供方的数据安全职责包括但不限于：

- a) 负责数据的安全提供，决定共享的数据形式，包括原始数据、加密数据、脱敏数据、结果数据等；
- b) 负责评估具体场景下数据共享的合理性、必要性；
- c) 负责监督数据接收方安全使用数据、不对外提供数据。

6.4.2 共享数据的接收方

共享数据的接收方的数据安全职责包括但不限于：

- a) 负责对接收到的城市运行数据进行安全存储和使用；
- b) 不随意改变数据的使用方式和范围，不重标识个人信息主体；
- c) 不私自复制、逾期留存和对外提供数据。

7 “一网统管”数据安全能力要求

7.1 组织管理

“一网统管”平台数据安全组织管理能力包括但不限于如下要求：

- a) 城市运行管理中心、其他参与数据处理活动的公共管理服务机构应共同建立数据安全组织管理框架，明确领导机构，涵盖决策层、管理层、执行层（监督层）和操作层，明确数据安全责任人，落实数据安全保护责任；
- b) “一网统管”数据安全责任人履行职责包括但不限于：
 - 1) 组织制定数据保护计划并落实；
 - 2) 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；
 - 3) 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；
 - 4) 组织受理并处理数据安全投诉和举报事项等。
- c) 应指定“一网统管”个人信息保护负责人，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。

7.2 制度流程

“一网统管”平台数据安全制度流程能力包括但不限于如下要求：

- a) 明确“一网统管”数据安全管理制度范围，制定符合业务战略、应用场景的，满足本级数据安全要求的安全目标、管理策略、方针和原则；
- b) 城市运行管理中心自行或授权数据安全管理机构负责数据安全制度的制定；建立健全数据安全保护制度体系，制度体系内容包括但不限于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、数据处理活动安全管理要求、数据安全教育培训、数据合作方管理、个人信息安全保护等；
- c) 建立基于应用场景的“一网统管”业务流程管理机制，实现数据的可管可控，包括：
 - 1) 绘制业务流程图，制定流程说明，明确控制目标及关键因素，流程图应包括参加活动的主体及角色，关键活动或主体及角色之间发生的事件，事件交互产生的业务数据，确保业务流程彼此关联，并明示优先级、明确业务目标等；
 - 2) 业务流程的描述包含业务流程图中的业务环节、参与的主体及角色、承担的职责和分工、事件交互产生的业务数据及用途、目标完成的评价指标等。
- d) 建立数据安全的投诉、举报受理处置制度，受理后进行调查取证，一经查实，应依法采取停止传输、消除等处置措施；
- e) 制定“一网统管”所涉及的个人信息保护的制度流程，包括依法向个人告知，处理规则集中公开展示，以及定期自行或者委托专业机构对其处理个人信息遵守法律、行政法规的情况进行合规审计的制度；
- f) 通过正式、有效的方式发布“一网统管”数据安全管理制度，并进行版本控制；定期对数据安全制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订；
- g) 根据不断演进的业务需求场景，建立数据安全持续改进优化机制，对当前数据安全合规性和执行效果进行评估，不断进行优化和迭代。

7.3 人员管理

“一网统管”平台数据安全人员管理能力包括但不限于如下要求：

- a) 应设置城市运行管理中心、应急管理、市场监管、住建部门、交通部门等城市运行重点保障部门中的数据安全相关的岗位和人员，负责“一网统管”相关部门的数据安全管理，并推进相关工作的开展和实施；
- b) 应明确数据管理员、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。相关岗位职责应包括：
 - 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；

- 3) 数据安全审计员负责数据安全审计等。
- c) 加强数据安全人员管理，明确规定人员录用、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管理要求并严格落实；加强信息化专业技术人才、具有大数据专业技能人员上岗、选拔；应对“一网统管”数据安全负责人和关键岗位的人员进行安全背景审查；
- d) 应与内部数据岗位人员、数据合作方人员签订保密协议，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；
- e) 应制定数据安全培训计划，定期组织数据安全培训工作，每年至少一次；针对机构全员，培训内容包括但不限于“一网统管”业务知识、数据安全相关法律法规、政策文件等；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、应急演练等，留存培训记录；
- f) 应组织数据岗位人员考取相关资质证书，持证上岗。

7.4 合作方管理

“一网统管”平台合作方管理数据安全能力包括但不限于如下要求：

- a) 应建设“一网统管”数据合作方安全管理机制，如对接合作方的安全能力进行选择、评价、管理、监督的机制；
- b) 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；
- 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，对接收、使用本单位数据的合作方的数据使用行为进行约束；
- d) 应设置合作方访问权限，包括合作方对数据与系统的访问、修改权限应限于最小必要范围，采取技术措施确保合作方对敏感数据的访问及操作能被实时监督或监测；
- e) 应对合作方接入的系统、使用的技术工具进行技术检测，或合作方提供专业第三方机构评估的数据安全报告，避免引入木马、后门等。

8 “一网统管”数据安全运营能力要求

8.1 分类分级

“一网统管”平台数据安全分类分级能力包括但不限于如下要求：

- a) “一网统管”业务数据安全执行方应全面梳理管辖的数据资源，确定拟分级的数据对象和范围，编制“一网统管”业务数据目录；
- b) 公共服务和管理机构可按数据主体、主题、业务等不同的属性对“一网统管”业务数据进行分类，数据分级需要组织城市运行管理中心、大数据中心、数源单位等相关领导、业务专家、安全专家等共同确定；
- c) 公共服务和管理机构可根据法律法规、业务、规划、实际业务需求等，对敏感数据进一步分级，根据不同级别的数据，选择恰当的管理和技术措施实施安全有效保护；
- d) 对核心数据、重要数据的数据安全能力要求应参照国家法律法规、政策文件、标准规范规定的数据安全要求；
- e) 当“一网统管”业务数据内容、应用场景，或者影响对象和程度发生变化后，宜考虑重新对数据进行分级，数据分级发生变化的情形包括但不限于：
 - 1) 数据分级对象发生了增加、减少、改变等情况；
 - 2) 数据在汇聚、加工、分析等过程中级别发生变化或产生新数据（如脱敏后的数据、统计产生的数据等）；
 - 3) 数据应用场景发生变化导致数据级别变化。

8.2 风险评估

“一网统管”平台数据安全风险评估能力包括但不限于如下要求：

- a) 定期开展重要数据及敏感个人信息数据的安全评估，识别数据资产价值，识别数据资产的脆弱性及安全威胁，客观评定数据安全风险等级，形成数据安全风险评估报告；

- b) 及时整改数据安全评估中发现的风险隐患和问题，完善数据安全保护措施；
- c) 在接入新的“一网统管”应用场景前、开放共享前，以及涉及合作方管理等场景中，应进行数据安全动态评估，形成数据安全风险评估报告，明确整改措施并严格执行。

8.3 认证授权

“一网统管”平台数据安全认证授权能力包括但不限于如下要求：

- a) 应建立身份认证管理系统，实现“一网统管”平台对接入的公共管理和服务机构人员访问数据资源的统一身份鉴别，用户身份标识应具有唯一性、复杂性，并定期更换；
- b) 应根据数据的安全级别，选择单因素身份认证、双因素身份认证或多重身份认证的方式，采用口令技术、密码技术、生物技术等一种或两种及以上组合的鉴别技术，来授予接入“一网统管”平台的公共管理和服务机构对系统及数据的访问权限；
- c) 应建立平台接入的授权审批流程，明确用户账号分配、开通、使用、变更、注销等安全细则，依据最少够用、职权分离原则对数据权限申请和变更进行审核，严格控制管理员权限账号数量；
- d) 应支持系统管理员、安全管理员、安全审计员“三权分立”设置权限范围，避免超级用户；
- e) 定期清理多余、重复、过期的账户和角色，及时回收转岗离职人员账号、沉默账号，跨部门、跨主体建立工作人员管理与身份认证管理、权限管理的关联控制；
- f) 建立定期更新和审核的敏感数据权限清单，对于数据批量复制、下载、导出、修改、删除等数据敏感操作采取多人审批授权或操作监督，并进行日志审计。

8.4 监测预警

“一网统管”平台数据安全监测预警能力包括但不限于如下要求：

- a) 建立并定期更新针对“一网统管”系统的风险分析库，明确风险评估场景，尤其是“一网统管”平台业务数据流通场景、个人信息处理场景；
- b) 具备数据安全风险监测技术工具，支持实时发现数据安全风险、识别数据资产及其面临的威胁和自身脆弱性，并支持数据安全风险可视化展示。包括但不限于以下工具：
 - 1) 数据泄露防护工具，以深层内容识别为核心，基于敏感数据内容策略定义，监控数据的外传通道，对敏感数据外传进行审计或控制；
 - 2) 数据泄露监测工具，包括互联网敏感数据泄露排查和监控、暗网敏感数据泄露排查和监控、违法黑产交易监控等，基于监测结果进行通报预警，并联动做溯源与加固；
- c) 建立“一网统管”系统下的预警信息报告机制，明确各接入组织的数据安全监控和异常情况报告义务及流程；
- d) 建设“一网统管”系统异常行为监测指标，包括 IP 地址、账号、访问频次、使用场景等，对批量访问、传输、下载、导出敏感数据的行为进行安全监控、分析、跟踪和告警；
- e) 应具备针对“一网统管”系统的数据风险评估标准和工具，并每年至少一次开展全面的数据安全风险评估。

8.5 安全审计

“一网统管”平台数据安全审计能力包括但不限于如下要求：

- a) 应要求接入“一网统管”平台的公共管理和服务机构对城市运行管理数据授权访问、收集、批量复制、提供、公开、销毁、数据接口调用、下载、导出等重点环节进行日志留存管理；日志记录内容应包括执行时间、操作账号、处理方式、授权情况、IP 地址、登录信息等，以识别和追溯数据操作和访问行为；
- b) 城市运行管理中心应对数据归集、加工和共享过程的数据操作行为进行日志记录与留存，以追溯、还原数据的开发与流通过程；
- c) 建立数据安全审计体系，设立合理有效的审计策略，具备统一的数据访问和操作日志监控审计技术；围绕数据的全生命周期过程的数据访问和操作进行监控、审计、分析，及时发现异常数

据流向、异常数据操作行为，进行告警和追溯，输出审计报告，并对以下行为或事件进行重点监控、审计：

- 1) “一网统管”平台业务数据与社会数据的融合开发行为，外发行为；
- 2) 数据的访问权限与实际访问控制的一致性，用户实际使用权限与审批目的的一致性；
- 3) 特权用户的数据操作行为，敏感数据相关的操作行为；
- 4) 对数据的批量复制、下载、导出、修改、删除等高风险行为；
- 5) 对个人信息处理行为；
- 6) 数据安全事件。

8.6 应急处置

“一网统管”平台数据安全应急处置能力包括但不限于如下要求：

- a) 城市运行管理中心应根据“一场景一预案”原则制定安全处置应急预案、定期组织应急演练；
- b) 其他接入“一网统管”平台的公共管理和服务机构应制定针对性应急预案并交城市运行管理中心审核；
- c) 应在应急预案中定义数据安全事件的类型，明确不同类别级别事件的处置流程和方法；
- d) 发现数据安全重大风险或发生安全事件时，应立即启动应急预案、采取应急措施，并及时报告相关安全监管部门；安全事件对个人、其他组织造成危害的，还应将安全事件和风险情况、危害后果、已经采取的补救措施等通知利害关系人；
- e) 应记录应急演练安全事件处置结果和应急策略，对告警进行响应并记录处置过程，建立“一网统管”数据安全事件应急效果的量化评估方法；
- f) 应在应急事件处理中具备拦截、阻断数据外发能力，及其数据清除的能力。

9 “一网统管”数据处理活动安全能力要求

9.1 数据采集

“一网统管”平台数据采集安全能力包括但不限于如下要求：

- a) 应按照相关法律法规、规章的要求编制“一网统管”业务数据资源目录规范，加强数据采集的安全保护；“一网统管”业务数据在整个采集、转化、传输过程中应依据授权使用，不被非法冒充、窃取、篡改、抵赖；
- b) 根据数据源单位、存储状态、数据应用方法、数据类型等，结合“一网统管”平台建设规划以及业务场景需求，定义整体数据采集框架；
- c) 明确数据采集原则、采集目的与用途、采集范围与方式、采集周期和频率和保存期限，确保数据采集的合法性、必要性、正当性；遵循数据最小化原则，只采集满足业务所需的最少数据；遵循质量保障原则，制定数据质量保障的策略、规程和要求；对采集的数据进行分类分级标识，并对不同类和级别的数据实施相应的安全管理策略和保障措施；
- d) 在数据采集中的各个环节，应使用数据安全相关技术以保障数据在采集过程中的安全，包括但不限于数据安全监测、安全审计、数字签名、数据加密等技术或手段；
- e) 对数据源、数据采集的环境、设施、技术采取必要的安全机制和管控措施，对产生数据的数据源进行鉴别和记录，确保采集数据的机密性、完整性和真实性；物联网数据等存在计算场景的，对计算后的数据状态进行审计和评估，确保数据完整性、可用性；
- f) “一网统管”平台如有涉及个人信息采集，应遵循合法性要求、收集个人信息的最小化要求、收集个人信息时的授权同意、收集个人敏感信息时的明示同意；在与国家安全、国防安全直接相关的，与公共安全、公共卫生、重大公共利益等直接相关的，及其他法律规定的情况，个人信息控制者收集、使用个人信息无需征得个人信息主体的授权同意。

9.2 数据存储

“一网统管”平台数据存储安全能力包括但不限于如下要求：

- a) 城市运行管理中心应充分考虑使用第三方数据存储平台保存“一网统管”数据的安全风险，除对存储系统中的数据如个人信息数据等进行有效控制外，还需承担数据的存储安全管理责任；
- b) 将“一网统管”中不同类别和级别的数据分开存储，并建立物理或逻辑存储隔离授权机制，具备多租户存储的安全隔离能力；
- c) 采用数据库加密系统等工具对“一网统管”数据进行加密存储，有条件的可应用区块链服务，区块链应支持联盟链的统一配置管理，支持数据上链存证不可篡改，支持数据的分布式存储、访问控制、合规性、跨链互操作性、高可用性和可扩展性以及数据备份和恢复的能力，以确保数据存证的安全、可靠和有效；
- d) 实施数据用户身份标识与鉴别、数据访问控制等安全控制措施；进行数据库审计，具备数据库操作日志采集和事件管控能力，对使用和外发的文件进行解析与扫描，实时识别、监控、保护组织的敏感数据；对即将发生、正在发生的泄露敏感数据行为进行审计留痕，按照预置策略及时阻断并告警，监视和保护静止、移动和使用中的数据并防止敏感数据传输到外部，有效避免数据泄露带来的安全风险；
- e) 采用数据备份/恢复工具等，提供数据备份与恢复功能，同时考虑数据存储的保密性、完整性和多副本一致性；建立数据存储冗余策略和管理制度，及数据备份与恢复操作过程规范；
- f) 对归档数据建立安全保护机制。

9.3 数据传输

“一网统管”平台数据传输安全能力包括但不限于如下要求：

- a) 区分“一网统管”平台不同数据形态和安全域内、安全域间等不同数据传输场景，建立相应的数据传输安全策略和操作规程；
- b) 数源单位应建立数据传输安全策略相应的安全控制措施，以保证数据在传输过程中的保密性；
- c) 城市运行管理中心依照数据传输场景，对数据传输相关方进行身份鉴别，并对传输数据加密传输；
- d) 采用基于密码技术的完整性和机密性保护机制，保护数据传输过程中的完整性和机密性，防止数据篡改和泄露；
- e) 使用监控技术与机制对数据传输接口进行审核及监控，发现数据传输失败/错误等安全事件，并自动应急处置；
- f) 如发现数据泄露事件，及时告警并应急处置。

9.4 数据加工使用

“一网统管”平台数据加工使用安全能力包括但不限于如下要求：

- a) 对参与“一网统管”涉及的数据加工使用活动的主体进行合法性、正当性的评估，确保参与数据加工活动的主体为合法合规的组织机构或个人；
- b) 应明确“一网统管”业务数据加工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；
- c) 遵循最小授权原则，提供数据细粒度访问控制机制，限定用户可访问数据范围，具备完整的数据使用操作记录；
- d) 采用技术措施，对“一网统管”业务数据进行加密、脱敏和去标识化处理；
- e) 规定“一网统管”中数据加工使用及委托加工使用过程中的数据查询、数据读写、数据索引、数据分析等重要操作的规范，明确数据正当使用的原则，记录操作信息；
- f) 对数据加工使用过程进行评估、监控、审计，对异常数据操作行为及时预警、处置；
- g) 委托他人加工使用数据的，应与其订立数据安全保护合同，明确双方安全保护责任；
- h) 应对数据加工使用结果进行评估，如产生新数据，应对新数据进行安全审核，确保新数据不存在数据泄露风险。

9.5 数据开放共享

“一网统管”平台数据开放共享安全能力包括但不限于如下要求：

- a) 根据业务场景，“一网统管”的数据开放共享应满足政府相关部门、城市基础设施、企业信息系统和个人设备的业务需求；
- b) “一网统管”业务数据共享应参照上海市公共数据“三清单”要求，公共管理和服务机构按照“一次采集、共享使用”原则开展数据共享的需求清单、责任清单和负面清单编制；
- c) 数据开放共享前，数据提供方应按照数据分类分级要求进行安全性评估，确保数据完成脱敏和去标识化；
- d) 数据提供方应检测开放共享的数据资源是否含有非公开信息能力，确保数据合规；涉及个人信息的数据内容，应根据业务对个人信息进行必要的加密处理；
- e) 数据提供方与“一网统管”业务数据使用部门签署相关协议，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；
- f) 数据提供方对数据开放共享过程记录日志，及时清除开放共享过程中缓存的数据；数据开放共享过程中采用标签、指纹、水印等技术，建立数据共享台账，确保责任可追溯；
- g) 对数据开放共享使用 API 的接口传输、授权、监控等环节建立安全防护措施，对 API 接口数据交换内容进行识别和管控；
- h) 数据提供方对数据开放共享的过程进行监控，确保数据安全合规，未超出授权范围。

9.6 数据删除销毁

“一网统管”平台数据删除销毁安全能力包括但不限于如下要求：

- a) 城市运行管理中心、数源单位等应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；
- b) 城市运行管理中心、数源单位等应使用规范的工具或产品，采用可靠技术手段及时销毁符合销毁条件的数据，确保数据不可还原；
- c) 对于数据存储介质的销毁，应使用国家权威机构认证的设备或国家认定资质的销毁服务提供商对存储介质设备进行物理销毁。

参 考 文 献

- [1] GB/T 36625.3-2021 智慧城市 数据融合 第3部分：数据采集规范
- [2] GB/T 36625.4-2021 智慧城市 数据融合 第4部分：开放共享要求
- [3] GB/T 20984-2022 信息安全技术 信息安全风险评估方法
- [4] GB/T 22239-2019 信息安全技术网络安全等级保护基本要求
- [5] GB/T 22240-2020 信息安全技术网络安全等级保护定级指南
- [6] GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南
- [7] GB/T 35273—2020 信息安全技术 个人信息安全规范
- [8] GB/T 41479-2022 信息安全技术 网络数据处理安全要求
- [9] GB/T 37973—2019 信息安全技术 大数据安全管理指南
- [10] DB31/T 1241-2020 公共数据“三清单”管理规范
- [11] DB11/T 1918—2021 政务数据分级与安全保护规范
- [12] DB4403/T 439-2024 公共数据安全评估方法
- [13] DB4403/T 271-2022 公共数据安全要求
- [14] CJ/T545-2021 城市运行管理服务平台数据标准
- [15] CJJ/T312-2021 城市运行管理服务平台技术标准
- [16] 丁红发，孟秋晴，王祥，蒋合领. 面向数据生命周期的政府数据开放的数据安全与隐私保护对策分析[J]. 情报杂志，2019
- [17] 梁满，刘迎风. 上海公共数据安全运营管理思考与实践[J]. 网域前沿，2022
- [18] 刘辰昀，刘佼，储昭武. 上海市公共数据标签管理体系研究及应用[J]. 学术研讨，2022
- [19] 严炜炜，谢顺欣，潘静，陆伟. 数据分类分级：研究趋势、政策标准与实践进展[J]. 数据科学，2022