ICS
CCS 点击此处添加 CCS 号

DB3307

浙 江 省 金 华 市 地 方 标 准

DB 3307/T XXXX—2024

城镇环卫收运数字化信息系统建设与运维规范

（征求意见稿）

2024－XX－XX 发布　　XXXX－XX－XX 实施

金华市市场监督管理局　　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××××提出。

本文件由××××归口。

本文件起草单位：浙江利珉环境科技有限公司、金华市住房和城乡建设局、金华市标准化研究院、金华市环卫服务中心等

本文件主要起草人：

城镇环卫收运数字化信息系统建设与运维规范

1 范围

本标准规定了城镇环卫收运数字信息系统建设基本、建设要求、运维要求和服务评价与改进等内容。

本标准适用于城市环卫收运数字化信息系统建设与运维管理。

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 20984 信息安全技术 信息安全风险评估规范

GB/T 22239—2019 信息安全技术 信息系统安全等级保护基本要求

GB/T 36626 信息安全技术 信息系统安全运维管理指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字化环卫运维信息系统

由物理层（基础设施层）、传输层、数据层、应用层构成，利用数字化手段，实现远程可视环卫作业、管理和服务的信息系统。

4 基本要求

4.1 城市环卫收运数字化运维信息系统应按照各功能模块要求总体设计、分步实施。

4.2 遵循统一的技术要求与管理要求，同时应满足不同监管主体对数据展示形式的需求。

4.3 应在具备基础维护功能，能对关键数据字段进行自定义配置管理。

4.4 系统运行的通信网关、应用服务和数据库服务应独立部署，数据库服务应支持大数据存储与检索等。

4.5 系统安全应符合 GB/T 22239—2019 第二级要求。

5 建设要求

5.1 基础设施

根据数字化环卫现状和需求，对照数字化环卫信息系统管理规范构架，配套设备类型包括但不限于车载视频终端、车载信息监控终端、RFID 电子标签、人员定位终端、垃圾桶监控终端、自称重终端设备等，且以上设施设备应能在系统里注册、配置、诊断、状态查询、测试等功能。

5.2 系统建设

5.2.1 运维系统架构

主要由物理层（基础设施层）、传输层、数据层、应用层组成，架构图示例见图1。

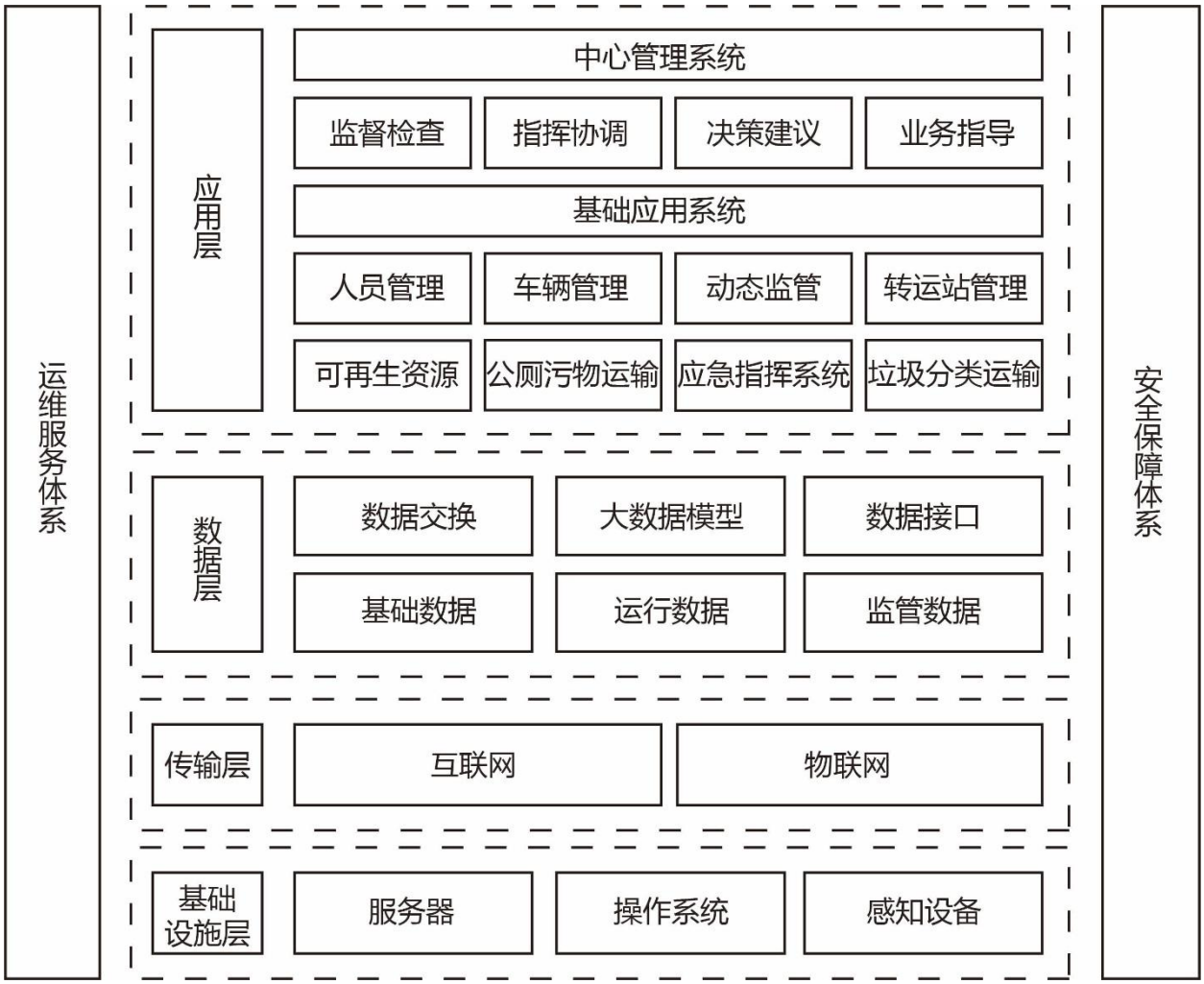

图 1 数字化运维信息系统架构

5.2.2 信息系统功能模块构成

系统的功能模块应包括但不限于以下模块：

——系统管理；
——基础数据；
——人员管理；
——车辆管理；
——设施设备管理；
——转运站管理；
——分类运输；
——视频监控；
——排班管理；

——应急指挥；
——事件管理；
——数据处理分析；
——项目看板；
——移动端程序。

5.2.3 系统管理

应包括系统菜单管理、配置管理、角色管理和系统日志管理等功能，对信息系统的系统权限分配、操作登录信息等实现管理。

5.2.4 基础数据模块

应包括人员档案、车辆档案、设施设备档案、网格管理、事件类型等基础数据的录入和管理，便于区分各类信息。

5.2.5 人员管理模块

应能对收运活动中人员的异动、奖惩、培训、保险、工作日志等信息进行全方位管理，主要记录人员在职期间的履历信息。

5.2.6 车辆管理模块

应包括电动保洁车、作业车辆、公务车辆等分类模块，具体包含对车辆维修、保险、加油、垃圾清运量、作业范围、定位等运营信息。

5.2.7 设施设备管理模块

设备管理模块应包括垃圾桶、深埋桶、中转站、垃圾驿站、信息采集硬件、摄像头等设备的管理。具体模块信息中应能对设备基本状态进行监控、对设备运营数据分析等功能。

5.2.8 转运站管理模块

应包含对转运站内收运过程中的垃圾类型、垃圾称重记录、车辆进出站记录、站内空气质量指标等信息进行记录等功能。

5.2.9 分类运输模块

应包括收运过程中各类垃圾的来源信息、分类信息、垃圾量、运输路径等，同时包含市民投放互动等功能。

5.2.10 视频监控模块

视频监控模块应包括数字化环卫的远程预览和远程控制功能，能对视频和车辆作业过程进行监控，模块应满足以下要求：

——视频显示页面应提供多窗口展示视频信息，点击某个窗口可以实现此窗口全屏化展示，可根据摄像头的数量自动展示窗口数量，最少展示四个窗口；
——模块应具备球机信息系统控制功能，调节设备的方向，实现 360 度无死角监控；
——模块应至少提供视屏的历史回放、倒放、截图和视频下载功能；
——应具备配置信息，至少应包括视频的 IP、端口号、用户名、密码、通道数量和不同品牌视频监控设备自动切换信息；

——环卫作业车辆应安装不少于三个摄像头，分别用于监控驾驶员实时状态、车辆作业左右两侧状态、车辆后下部作业状态。

5.2.11 排班管理模块

排班管理模块应能对环卫运输中转等作业过程进行排班，排班主要内容应包括收集作业排班、转运作业排班等排班信息。

5.2.12 应急指挥管理模块

包括对各类突发状况的记录，根据实时信息数据与监测，智能科学的调度作业人员和车辆，达到快速响应，提升应急处理能力。

5.2.13 事件管理模块

事件管理模块应能对收运过程中发生的事件、状态，进行上报和流转，实现收运过程中的无纸化、流程化管理。

5.2.14 数据处理分析模块

报表中心模块应能对收运过程中的人员、设备、排班、事件、车辆等运维数据实现数据汇总分析的功能。数据报表应包括人员考勤表、人员信息表、作业车辆日报、周报、月报、排班管理信息表、维修月报、加油月报、垃圾清运量月报、事件月报、考核月报等，支持管理人员进行深度分析和决策。

5.2.15 项目看板模块

应支持实时反映作业过程中各类指标数据，通过图表、数学模型等形式将各类数据具象化、直观化，并对异常情况进行预警或报警。

5.2.16 移动端程序

应可实用移动端程序或APP,实现考勤、事件上报、各类信息报送审批等移动办公功能。

6 运维要求

6.1 管理

应按照GB/T 36626指导信息系统安全运维管理体系建立和运行。

6.2 系统管理制度

应建立相应的管理制度，包括但不限于人员管理制度、信息系统建设管理制度、资产管理制度、设备设施管理制度、文档管理制度、用户管理制度、变更管理制度、备份与恢复管理制度、事件管理制度、应急预案管理制度等。

6.3 授权和审核

6.3.1 应明确授权审核部门、人员、审核事项等。

6.3.2 应针对信息系统变更、重要操作、物理访问等事项建立审核程序，按照审核程序执行审核过程，对重要活动建立逐级审核制度。

6.3.3 应记录审核过程并保存审核文档。并定期审查审核事项，及时更新需授权和审核的项目、审核

部门和审核人等信息。

6.3.4 应对考核结果进行记录并保存。

6.4 设施设备管理

应建立并实施设备设施管理，包括注册、状态查询、测试、诊断等功能，应定期对设备设施进行维护,出现故障后能及时排除并修复。

6.5 日志管理

日志应包括本地日志、远程设备日志、报警日志。能够将系统运行情况和用户操作记录自动生成日志，且所有日志能够导出，并具有禁止修改日志数据的保护功能。

6.6 维护和检查

6.6.1 应制定系统维护和检查的方案。

6.6.2 系统管理员应定期检查服务器的运行状态、安全防护策略、系统账号及权限运行状态。

6.6.3 信息管理员应定期对信息系统进行全面检查，检查内容包括现有设备设施上限情况、数据维护的情况等。

6.7 安全维护

6.7.1 信息系统

6.7.1.1 应按照 GB/T 20984 的要求，定期对信息系统面临的风险和威胁、薄弱环节以及防护措施的有效性进行信息安全风险评估。

6.7.1.2 应根据业务需求、系统风险评估结果、系统安全分析确定信息系统的访问控制策略。

6.7.1.3 应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装。

6.7.1.4 应指定专人对信息系统进行管理，划分系统管理员和系统操作员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则，应设置安全审计员角色，仅赋予日志查看权限，负责对系统各类用户的操作行为进行审计、跟踪分析、监督检查、事件上报等。

6.7.1.5 应依据操作手册对信息系统中信息系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作。

6.7.1.6 应定期对运行日志和审计数据进行分析，及时发现异常行为。

6.7.2 恶意代码防范

6.7.2.1 应提高所有用户的恶意代码防范意识，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，应进行扫描检查。

6.7.2.2 应及时更新防病毒软件版本及

6.7.2.3

6.7.2.4 恶意代码库版本。

6.7.2.5 应定期检查信息系统恶意代码，对截获的恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

6.7.3 应急防范

应具有防雷击、过载、断电、电磁干扰和人为破坏等综合安全防护措施。

6.7.4 密码管理

6.7.4.1 应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。
6.7.4.2 相关系统、应用使用密码应符合国家密码管理相关规定。

6.7.5 外部人员访问

6.7.5.1 应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案。
6.7.5.2 对外部人员允许访问的区域、系统、设备、信息等内容应按照相关规定执行。

6.7.6 变更

6.7.6.1 应建立变更管理制度，信息系统发生变更前，对变更影响进行分析并形成变更方案，方案经评审后方可实施，实施后应妥善保存所有文档和记录。
6.7.6.2 应建立中止变更并从失败变更中恢复的操作规范，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

6.7.7 备份与恢复

6.7.7.1 应识别需要定期备份的重要业务信息、系统数据及软件系统等。
6.7.7.2 应根据数据的重要性和数据对信息系统运行的影响，制定数据的备份策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换周期等。
6.7.7.3 应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存。
6.7.7.4 应定期检查和测试备份介质的有效性，确保可用。

6.7.8 安全事件处置

6.7.8.1 应制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责。
6.7.8.2 应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等。
6.7.8.3 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程,总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存。
6.7.8.4 对造成系统中断和造成信息泄密的安全事件应采取专门措施进行事件处置。
6.7.8.5 应报告所发现的安全弱点和可疑事件，但任何情况下均不应尝试验证弱点。
6.7.8.6 当有重大安全事件时，应立即采取控制措施，按照有关规定逐级上报，积极协助信息安全事件的调查，做好善后处理工作。

6.7.9 应急预案

6.7.9.1 应制定应急预案，包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容。
6.7.9.2 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障。
6.7.9.3 应对相关人员进行应急培训，至少每年培训一次。
6.7.9.4 应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期。
6.7.9.5 应定期审查应急预案，根据实际情况调整相关内容，并按照执行。

7 服务评价与改进

7.1 应建立数字化运维信息系统运行服务过程及客服定制化服务项目相关的评价标准和改进机制，定期开展服务质量评价。

7.2 应建立数字化运维信息系统服务质量投诉反馈机制，提供方便、可靠的服务投诉电话、邮箱等渠道，并建立相应的处理机制。

7.3 应定期开展服务回访或满意度调查，收集平台使用者的意见和建议，不断完善信息化平台功能，以提高服务质量和服务水平。