

T/CABEE

团体标准

T/CABEE CCSA XXXX—XXXX

公共租赁住房数字化运营管理平台 技术要求

Technical requirements for digital operation and management platform of public
rental housing

（征求意见稿）

（本草案完成时间：2025 年 6 月 20 日）

2025 – XX – XX 发布

2025 – XX – XX 实施

中国建筑节能协会

中国通信标准化协会

联合发布

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 1

5 总体架构 2

6 物联终端 2

6.1 通用要求 2

6.2 视频监控 3

6.3 智能消防 3

6.4 智能门锁 3

6.5 智能表具 3

6.6 体征监测 3

6.7 其他设备设施 3

7 网络通信层 4

7.1 协议接入 4

7.2 边缘计算 4

7.3 智能传输 4

8 数据层 4

8.1 概述 4

8.2 数据汇聚 4

8.3 数据存储 4

8.4 数据处理 4

8.5 数据分析 5

9 应用层 5

9.1 租赁管理 5

9.2 设备管理 6

9.3 审核管控 6

9.4 服务管理 7

9.5 运营管理 7

9.6 系统配置 8

10 终端服务层 9

10.1 监管终端 9

10.2 Web 管理终端 9

10.3 移动终端 9

10.4 开放接口 9

10.5 SDK 开发支持 9

11	安全保障	10
11.1	系统安全	10
11.2	设备安全	10
11.3	数据安全	11
11.4	隐私保护	11
12	运维管理	11

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：

本文件主要起草人：

公共租赁住房数字化运营管理平台技术要求

1 范围

本文件给出了公共租赁住房（以下简称“公租房”）数字化运营管理平台的总体架构，规定了公租房数字化运营管理平台的物联终端、网络通信层、数据层、应用层、终端服务层的技术要求，以及安全保障和运维管理的核心要求。

本文件适用于公租房数字化运营管理平台（以下简称“数字化平台”）的设计、建设、升级及日常运维活动，为运营机构、技术服务商及监管部门提供技术参考依据。

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 9706.1 医用电气设备 第1部分：基本安全和基本性能的通用要求
- GB/T 20986 信息安全技术 网络安全事件分类分级指南
- GB 21556 锁具安全通用技术条件
- GB/T 22239 信息安全技术 网络安全等级保护基本要求
- GB/T 35273 信息安全技术 个人信息安全规范
- GB/T 36626 信息安全技术 信息系统安全运维管理指南
- GB/T 38637.2—2020 物联网 感知控制设备接入 第2部分：数据管理要求
- GB/T 39680 信息安全技术 服务器安全技术要求和测评准则
- GB/T 43697 数据安全技术 数据分类分级规则
- GB 50116 火灾自动报警系统设计规范
- GB 50166 火灾自动报警系统施工及验收标准
- GB 55029 安全防范工程通用规范
- CJ/T 188 户用计量仪表数据传输技术条件
- GA 374 电子防盗锁
- GA/T 701 安全防范 指纹识别应用 出入口控制指纹识别模块通用规范
- GA/T 1127 安全防范视频监控摄像机通用技术要求
- GM/T 0014 数字证书认证系统密码协议规范

3 术语和定义

JGJ/T 433界定的以及下列术语和定义适用于本文件。

3.1

公租房数字化运营管理平台 Public rental housing digital management platform

利用数字技术，对租赁住房运营中的租户入住与退出管理、租金收缴管理、房屋使用管理、维修保养管理及综合管理等核心业务，实施操作与管理的信息系统。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

BLE：蓝牙低功耗（Bluetooth Low Energy）

IP：防护等级（Ingress Protection）

MQTT：消息队列遥测传输协议（Message Queuing Telemetry Transport）

NB-IoT: 窄带物联网 (Narrow Band Internet of Things)
OTA: 空中激活 (Over-the-Air)
SDK: 软件开发工具包 (Software Development Kit)

5 总体架构

数字化平台采用分层架构, 由物联终端、网络通信层、数据层、应用层、终端服务层5个部分构成, 安全保障及运维管理作为支撑体系, 通过开放接口汇聚第三方物联网数据, 同时保留与公共服务机构、第三方平台进行数据资产交互或联动的扩展能力。总体架构见图1。

各组成部分具体描述如下:

- a) 物联终端包括视频监控、智能门锁、智能表具、体征监测和其他设备设施, 为平台提供基础信息;
- b) 网络通信层包括协议接入、边缘计算和智能传输, 确保各类物联终端能够稳定、安全地接入平台;
- c) 数据层包括数据汇聚、数据处理、数据存储和数据分析, 为上层应用提供数据服务;
- d) 应用层包括租赁管理、设备管理、审核管控、服务管理、运营管理和系统配置, 实现设备监测、智能分析、租赁业务全生命周期管理等核心功能;
- e) 终端服务层包括 Web 终端、移动终端、监管终端、开放接口和 SDK 开发支持, 提供终端服务接入;
- f) 安全保障体系为各层提供数据加密、访问控制等安全防护;
- g) 运维管理体系负责数字化平台监控、故障处理及性能优化。

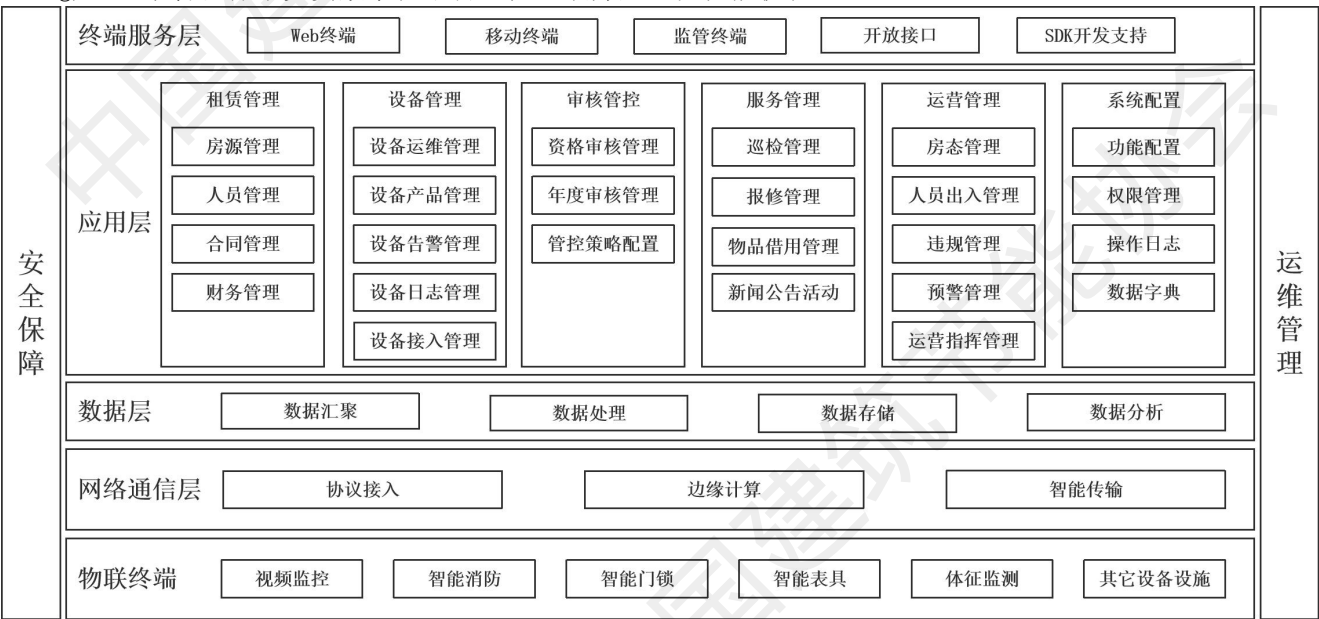


图 1 总体架构

6 物联终端

6.1 通用要求

公租房配置的物联终端满足下列要求:

- a) 应支持 MQTT、Modbus 等主流通信协议, 适配数字化平台接口, 非标准协议的处理应符合 7.1 b) 的要求;
- b) 智能门锁、火灾探测报警器等关键设备应具备本地数据缓存能力, 缓存时间应不少于 24h;
- c) 设备固件应支持远程 OTA 升级, 并保证升级过程的完整性;

- d) 智能门锁、体征监测等设备宜具备简洁操作界面，便于老年人、残障人士等特殊人群的使用需求；
- e) 设备防护等级不应低于 IP54，同时工作温度范围应满足不同地域与季节的使用要求，宜为-10℃~55℃。

6.2 视频监控

视频监控设备的部署应符合GB 55029的规定，并满足下列要求：

- a) 视频监控设备的功能及性能应符合 GA/T 1127 的规定；
- b) 应具备自动检测视频信号缺失、遮挡、异常转动，告警信息分级推送至数字化平台；
- c) 周界摄像机应具备夜间报警灯光联动功能；
- d) 视频数据存储应不小于 30d，并支持与公共安全视频监控联网系统联动功能；
- e) 宜集成人脸识别、行为分析、车牌识别等智能算法。

6.3 智能消防

智能消防设备涵盖火灾探测报警及消防设备，其部署及功能应符合GB 50116和GB 50166的规定，并满足下列要求：

- a) 应实时监测剩余电流、温度及烟雾浓度；
- b) 本地声光报警应与数字化平台/移动端告警同步触发，延迟时间应不大于 1min；
- c) 消火栓泵和排烟设备应能在火灾时自动启动，状态信号上传延迟不应大于 30s；
- d) 声光报警应覆盖楼道与电梯厅，报警信息应直接传输至物业值班室；
- e) 电池供电设备续航时间宜不少于 3 年。

6.4 智能门锁

智能门锁应符合GB 21556、GA 374和GA/T 701的规定，并满足下列要求：

- a) 应具备近场通信和远程通信能力，可通过短距离或远距离通信方式与数字化平台连接；
- b) 应支持指纹、人脸等生物特征识别，以及密码等开锁方式；
- c) 应具备防撬报警、低电预警、连续输入错误超过 5 次触发报警等功能，并实时上报至数字化平台；
- d) 应具备内/外门开门记录存储及上报功能，记录数据应同步传输至数字化平台；
- e) 断网时应自动重连网络，且无需人工干预配置。

6.5 智能表具

智能表具（含水、电、气、暖等类型）应符合所属行业标准，并满足下列要求：

- a) 户用计量仪表数据的传输技术条件应符合 CJ/T 188 的规定；
- b) 应具备机械读数电子化功能，支持远程抄表及自动校时功能，冻结数据保存时间应不少于 30d；
- c) 单电池供电寿命应不少于 5 年，断网期间数据宜自动补报；
- d) 宜支持 OTA 远程升级。

6.6 体征监测

适老型体征监测设备应符合GB 9706.1的规定，并满足下列要求：

- a) 应具备心率、血压、血氧等基础参数监测功能，且宜具备跌倒监测与睡眠分析功能；
- b) 数据异常时，应在 30s 内触发本地报警，并同步推送至数字化平台；
- c) 监测数据宜加密存储且保存周期不少于 6 个月，并设置分级访问权限；
- d) 宜采用非接触式监测技术，单次充电续航时间宜不少于 30d，断网时应保存关键数据；
- e) 宜与社区相关系统联动，报警信息触发后应启动应急响应机制。

6.7 其他设备设施

公租房宜配置的其他设备设施包括但不限于电梯控制、楼宇门禁、智能家居及医疗辅助等系统、设备，其功能及部署应符合国家、行业现行相关标准，并满足下列要求：

- a) 电梯控制系统应实时监测运行状态、故障信息及轿厢人员异常行为，故障数据应上传至数字化平台，且与门禁系统联动；
- b) 门禁设备应支持刷卡、生物识别等身份认证方式，异常闯入事件应触发本地声光报警并同步推送至数字化平台；
- c) 医疗辅助设备宜具备与数字化平台、医疗服务平台的联动能力；
- d) 智能家居设备（包括但不限于照明、空调、窗帘控制器等）宜支持远程控制及场景联动。

7 网络通信层

7.1 协议接入

应实现异构设备统一接入与协议解析，并应满足下列要求：

- a) 支持蜂窝网络（4G/5G/Cat.1）、Wi-Fi、BLE、Zigbee 及 NearLink 混合组网；
- b) 适配 MQTT、Modbus 标准协议，非标协议通过解析引擎自动转换至平台标准格式；
- c) 实时监测设备在线率与信号强度，离线超过 1h 触发告警工单。

7.2 边缘计算

应部署近端算力节点降低核心负载，并应满足下列要求：

- a) 视频分析、消防报警等实时业务处理延迟不大于 1min；
- b) 断网时关键数据本地缓存时间不少于 24h；
- c) 边缘节点算力支持按需扩容。

7.3 智能传输

应构建分级传输与网络容灾体系，并应满足下列要求：

- a) 紧急业务（消防报警、应急呼叫）传输延迟不大于 1min；
- b) 高优先级业务（门禁异常、体征异常）传输延迟不小于 20s；
- c) 骨干网应采用双链路冗余设计，故障切换时间不大于 10s。

8 数据层

8.1 概述

数据层承担数字化平台全要素数据的汇聚、处理、存储及分析功能，通过网络通信层实时采集安防监控、环境监测、设施状态监测等设备数据，经由安全通信网络传输至数字化平台，为运营管理提供数据支撑。

8.2 数据汇聚

数据汇聚功能实现多源异构数据的统一接入与分级处理，应符合下列要求：

- a) 支持多模态数据融合接入，覆盖视频监控流、传感器时序数据、设备日志及业务单据等类型；
- b) 建立数据分级传输机制，关键业务数据优先保障传输时效性；
- c) 具备网络异常情况下的数据缓存与续传能力。

8.3 数据存储

应基于数据安全级别与业务访问频率实施分级存储策略，并应满足下列要求：

- a) 高频访问数据存储于分布式数据库，个人敏感信息独立部署于安全区并加密；
- b) 周期性业务数据采用关系型或时序数据库存储，含敏感字段数据采用商用密码算法加密；
- c) 归档类数据使用对象存储系统保存，证件影像等敏感资料加密存储。

8.4 数据处理

数据处理操作应建立数据质量控制与安全保护机制，并应满足下列要求：

- a) 设备运行异常数据实现自动标记与故障分析；

- b) 租户个人信息实施动态脱敏与静态加密双重防护；
- c) 完整记录数据处理过程的元数据。

8.5 数据分析

数据分析功能应构建多维度智能分析体系，为运营决策提供数据支撑，并符合下列要求：

- a) 应生成空置率趋势分析、租金收缴率统计、维修工单响应时效等运营决策指标；
- b) 应构建租户行为分析模型，识别长期空置、违规转租等异常居住行为并生成风险预警；
- c) 应支持分析结果自动生成结构化报告，适配不同终端展示需求；
- d) 宜具备能耗数据分析功能，并提供能效优化建议和异常耗能定位；
- e) 宜建立分析模型定期优化机制，确保模型预测准确性。

9 应用层

9.1 租赁管理

9.1.1 房源管理

房源管理应实现房源全生命周期数字化管控，覆盖房源信息管理、租约管理及设备联动等核心业务环节，具体应符合以下要求：

- a) 支持单个房源信息录入，必填信息包括但不限于小区名称、楼栋号、单元号等基础属性，并提供整栋房源批量创建功能；
- b) 提供标准模板下载与批量导入能力，数字化平台自动校验数据完整性并生成错误报告；
- c) 具备对房源全量信息维护功能，包括但不限于设备状态监控、费用规则配置及历史租约追溯；
- d) 空置房源删除具备二次确认功能，支持同小区房源批量绑定房型模板；
- e) 租约管理覆盖入住办理、续签审核及退租结算全流程，应急密码生成后加密发送且限时有效；
- f) 实时监测智能设备运行状态，异常离线或数据超限时自动告警；
- g) 按条件筛选导出房源数据，格式兼容标准类型并包含租约状态；
- h) 记录房源状态变更历史，核心城区空置超期触发分级预警。

9.1.2 人员管理

人员管理应建立租户全周期服务与监管机制，涵盖资格核验、权限控制及特殊保障等关键环节，并应符合下列要求：

- a) 租户资格失效后冻结门禁权限并启动退租流程，保留申诉救济通道；
- b) 身份核验失败时触发人工复核流程，核验记录纳入服务质量评估；
- c) 特殊人群优先分配策略需留存政策依据及审批记录；
- d) 租金减免操作应同步推送电子通知书及政策依据文件。

9.1.3 合同管理

合同管理应建立电子化全流程管控体系，覆盖合同生成、履约监控及补贴核发等关键业务节点，并应符合以下要求：

- a) 电子合同模板内置法定签章，租金条款关联地方指导价并定期更新；
- b) 合同续签前自动启动资格复审，未通过复审的终止合同并保留申诉期；
- c) 租金逾期时发送催缴通知并依法计算滞纳金；
- d) 财政补贴发放数据需与民政系统校验，异常数据转入人工处理。

9.1.4 财务管理

财务管理应基于智能化技术实现资金全流程监管，覆盖费用核算、收缴管理及信用评估等核心业务，并应符合以下要求：

- a) 自动生成含费用明细的电子账单，支持多渠道推送及下载；
- b) 提供线上支付与线下代收服务，异常缴费流水标记复核；
- c) 智能表具数据定期同步生成用量账单，异常用量触发核查；

- d) 定期生成租金收缴分析报告并支持多维度对比；
- e) 欠租行为纳入信用管理体系前需履行告知程序。

9.2 设备管理

9.2.1 设备运维管理

设备运维管理覆盖设备全生命周期，具体应符合下列要求：

- a) 建立设备全生命周期档案，记录设备型号、供应商、安装位置、维修历史及备件更换等信息；
- b) 制定设备维护计划，按类型设定保养周期并生成逾期维护督办工单；
- c) 管理备件库存台账，库存不足时触发采购申请并与维修工单关联；
- d) 分析设备故障率及修复时效指标，优化维护策略并生成退役建议。

9.2.2 设备产品管理

设备产品管理规范设备管理流程，具体应符合下列要求：

- a) 维护标准设备型号库，定义技术参数模板并实施新增型号技术评审；
- b) 管理供应商资质及合作协议，对劣质供应商实施采购权限管控；
- c) 预设设备配置模板，支持批量参数导入及固件升级策略配置；
- d) 记录设备软硬件版本信息，版本变更时触发升级提醒。

9.2.3 设备告警管理

设备告警管理应建立闭环处置机制，并应符合下列要求：

- a) 配置设备运行阈值及分级告警规则；
- b) 紧急告警实时推送至指定终端并要求确认接收状态；
- c) 记录告警处理过程及解决方案，未及时处理时升级工单优先级；
- d) 定期生成告警统计分析报告并优化运维策略。

9.2.4 设备日志管理

设备日志管理覆盖从采集到分析的全过程，重点确保日志数据的完整性和可审计性，并应符合下列要求：

- a) 自动采集设备操作日志、运行日志及通信日志；
- b) 支持组合条件检索日志并关联操作人信息；
- c) 采用防篡改技术固化日志数据，保留期限不低于设备报废后 2 年；
- d) 分析日志数据识别风险模式并触发预防性维护。

9.2.5 设备接入管理

设备接入管理应符合下列要求：

- a) 协议接入符合 7.1 的要求；
- b) 实时监测设备运行状态和通信质量，包括设备在线状态和连接稳定性等核心指标；
- c) 自动处置异常设备，对连续离线超过设定阈值的设备生成维护工单，对频繁断连设备触发告警及重连机制。

9.3 审核管控

9.3.1 资格审核管理

租户的资格审核管理宜构建全流程数字化审核体系，确保审核工作的规范性和高效性，并应符合下列要求：

- a) 支持线上线下多渠道受理，线上通道覆盖移动端及监管终端，线下对接政务服务窗口；
- b) 调用电子证照库自动获取申请人身份证、户口簿等基础证件信息；
- c) 生成标准化申请表模板，强制填写户籍类型、婚姻状况、工作单位及社保缴纳信息；
- d) 建立智能预审规则，核验户籍合法性、收入合规性及住房持有状态；
- e) 高风险申请自动触发人工复核流程，需补充材料清单由数字化平台动态生成；

- f) 提供审核进度可视化查询功能，关键节点推送通知并同步公示信息至地方监管平台；
- g) 异议申诉需在规定时间内提交补充材料，逾期未提交视为放弃申诉。

9.3.2 年度审核管理

自然年度审核管理应建立自动化动态监控机制，实现资格持续跟踪与信用联动管理，并应符合下列要求：

- a) 数字化平台定期推送年审通知，租户可在线更新收入证明、家庭成员变更等信息；
- b) 逾期未提交年审材料的自动冻结租赁权限；
- c) 动态核查租户收入变化、住房变动及信用记录，发现显著异常时生成预警；
- d) 复审结果按合规性分级处理，包括合同续期、限期整改或强制退房。

9.3.3 管控策略配置

管控策略配置应实现灵活可调的政策规则管理，支持多维度参数设置与动态优化，并应符合下列要求：

- a) 支持动态配置审核规则，涵盖准入条件、材料清单、信用评估权重等参数；
- b) 设定分级审核权限，按行政层级分配材料初审、现场核查及紧急干预职能；
- c) 提供数据看板展示区域审核通过率、办理时效及风险分布等核心指标；
- d) 生成策略优化建议报告，辅助主管部门调整人才引进、特殊人群保障等政策。

9.4 服务管理

9.4.1 巡检管理

巡检管理应建立标准化任务调度与执行机制，实现设备预防性维护闭环管理，并应符合下列要求：

- a) 按设备类型预设巡检周期，自动生成任务清单并关联责任人；
- b) 智能分配工单，优先匹配具备特种设备资质的工程师处理紧急任务；
- c) 记录现场签到信息、设备状态数据及隐患处理建议；
- d) 生成标准化巡检报告并更新设备档案，异常数据触发后续维修流程。

9.4.2 报修管理

报修管理应满足高效便捷的服务响应机制，实现故障全流程跟踪与服务质量管控，并应符合下列要求：

- a) 支持多渠道提交报修申请，需包含故障描述、现场影像及定位信息；
- b) 按故障类型智能分派工单，结合地理位置与工单负荷优化优先级；
- c) 提供工单进度实时查询功能，关键节点同步推送状态通知；
- d) 工单关闭后自动收集满意度评价，低满意度评价触发复检机制。

9.4.3 物品借用管理

物品借用管理满足租借服务流程，实现物品全周期追踪与权责明确管理，并应符合下列要求：

- a) 支持线上申请公共物品借用，需填写事由、期限及责任承诺；
- b) 自动校验借用者信用记录及物品库存状态，超期未归还触发预警；
- c) 按借用时长自动计费并与租金账户联动结算，生成电子凭证；
- d) 记录物品损耗情况，异常损坏启动赔偿程序并更新台账。

9.4.4 新闻公告管理

新闻公告管理支持精准化信息发布与反馈机制，并应符合下列要求：

- a) 按公告类型定向推送至目标租户群体，支持政策解读、应急通知等分类；
- b) 通过多终端同步发布信息并追踪阅读状态；
- c) 租户反馈自动归类至知识库或生成客服工单；
- d) 历史公告分类归档，支持关键词检索及标准化格式导出。

9.5 运营管理

9.5.1 房态管理

房态管理应实现房源全生命周期数字化管控，覆盖状态定义、变更审批及数据联动更新，并应符合下列要求：

- a) 定义房源使用状态分类并关联维修工单信息，标注预计恢复时间；
- b) 状态变更需经审批流程，保留完整历史变更记录供追溯；
- c) 提供多维度房源状态可视化看板，支持楼栋、户型等条件筛选；
- d) 租约签约/解约及维修完成时自动更新房态数据。

9.5.2 人员出入管理

人员出入管理应构建智能化安全管控机制，规范访客通行与区域权限管理，并应符合下列要求：

- a) 实施访客线上预约登记制度，核验身份信息与授权范围；
- b) 生成动态通行凭证并设定使用范围与时效限制；
- c) 记录关键区域出入轨迹，支持视频监控数据联动调取。

9.5.3 违规管理

违规管理应建立闭环处置与信用联动机制，覆盖事件上报、处置跟踪及信用影响全流程，并应符合下列要求：

- a) 支持多渠道违规事件上报，提交现场证据材料；
- b) 自动校验违规关联信息，高风险事件转人工复核并启动应急响应；
- c) 跟踪违规处置全流程，逾期未整改升级至监管部门处理；
- d) 违规记录同步至信用档案并影响续租资格。

9.5.4 预警管理

预警管理应实现风险分级响应与处置闭环，确保实时监测与应急联动，并应符合下列要求：

- a) 支持对疑似转租/群租、疑似无人、合同到期、特殊人群开门、设备状态异常等情况的预警功能，并建立完整的预警记录；
- b) 对接物联网设备实时监测数据，异常状态触发分级预警；
- c) 紧急预警实时推送至相关方并启动应急处置流程；
- d) 记录预警处理过程及预防措施，未及时处置自动升级管理权限。

9.5.5 运营指挥管理

运营指挥管理应建立集中化管控系统，实现运营任务的统一调度与执行监控，并应符合下列要求：

- a) 整合房源状态、设备告警、违规事件等实时数据，生成全局运营态势视图；
- b) 支持管理人员在线派发工单、调整资源分配，并跟踪任务执行进度；
- c) 提供应急指挥功能，紧急事件触发多部门协同处置流程；
- d) 记录指挥决策全过程，包括指令内容、执行人员及处置结果。

9.6 系统配置

9.6.1 功能配置

功能配置应提供灵活可扩展的业务规则定义能力，满足流程、字段及预警的个性化配置需求，并应符合下列要求：

- a) 流程配置支持业务审批流程与自动化规则定义，支持设置节点条件及动态分配审批人；
- b) 字段配置允许自定义表单字段类型并关联数据字典，支持必填项规则与校验逻辑设置；
- c) 预警配置预设多场景阈值规则及响应策略，包括设备异常和安防告警等场景。

9.6.2 权限管理

权限管理应实现精细化访问控制，基于角色模型规范组织、菜单及数据权限分配，并应符合下列要求：

- a) 组织架构支持树形层级配置，关联部门与岗位信息；

- b) 角色控制分配菜单访问、操作按钮及接口调用权限；
- c) 数据权限按角色限制数据可见范围，如本部门房源信息；
- d) 用户绑定支持账号关联角色与数据权限，允许多角色叠加。

9.6.3 操作日志

操作日志应确保用户行为的完整追溯与安全审计，满足合规性管理要求，并应符合下列要求：

- a) 完整保存用户登录信息和业务操作行为；
- b) 操作日志存储采用防篡改技术，保留期限不低于业务数据生命周期；
- c) 日志查询支持多维度组合检索条件；
- d) 日志追溯提供标准化格式导出功能。

9.6.4 数据字典

数据字典应提供统一的枚举值管理与数据关联服务，保障数字化平台数据一致性，并应符合下列要求：

- a) 字典类型支持列表型和树形结构两类；
- b) 数据关联支持静态维护或动态关联业务表；
- c) 服务支撑通过标准化 API 提供枚举值服务；
- d) 一致性保障自动同步变更至关联业务模块。

10 终端服务层

10.1 监管终端

监管终端服务应实现与地方监管平台的数据对接，提供多维度监管数据的可视化展示与实时同步能力，并应符合下列要求：

- a) 通过数据看板实时监控房源空置率、设备告警、异常行为等核心指标，数据格式符合地方监管平台接入规范；
- b) 动态生成区域风险热力图、违规事件分布图等可视化图表，支持与地方监管平台的数据看板联动展示；
- c) 配置关键指标阈值及预警规则，触发预警时同步推送至地方监管平台应急处置模块。

10.2 Web 管理终端

Web管理终端应实现全功能业务操作平台，满足后台管理人员的日常运营需求，并应符合下列要求：

- a) 后台管理界面支持房源全生命周期配置与工单审核流程；
- b) 生成多维度运营分析报表并支持自定义模板导出；
- c) 策略规则引擎提供可视化配置工具。

10.3 移动终端

移动终端服务应建立移动化服务体系，覆盖租户自助服务与现场运维需求，并应符合下列要求：

- a) 租户端集成在线报修、合同签署、费用缴纳等自助服务；
- b) 运维端支持工单进度跟踪、设备巡检签到及应急密码管理；
- c) 实时推送预警通知与政策公告信息。

10.4 开放接口

开放接口服务应构建标准化数据交互通道，保障各平台间安全高效对接，并应符合下列要求：

- a) 提供标准化 RESTful API 接口文档，支持房源数据查询、设备状态获取等核心功能调用；
- b) 实施 OAuth 2.0 协议进行接口权限管控，按角色分配数据访问范围；
- c) 接口版本兼容性保障，旧版本接口保留过渡期不宜低于 6 个月。

10.5 SDK 开发支持

SDK开发支持应提供完善的开发者服务，降低第三方系统集成门槛，并应符合下列要求：

- a) 提供多平台（Android/iOS/Web）SDK 工具包，封装设备控制、身份认证等基础能力；
- b) 开发文档包含快速接入指南、代码示例及异常处理规范；
- c) 支持第三方系统通过 SDK 实现与数字化平台深度集成。

11 安全保障

11.1 系统安全

11.1.1 安全架构

数字化平台应采用分层防御架构，覆盖网络边界防护、主机安全加固、应用安全防护及数据安全隔离，并应至少符合GB/T 22239中关键信息系统安全防护的二级要求。

11.1.2 访问控制

访问控制应建立严格的权限管理体系，防范越权操作和数据泄漏风险，并应符合下列要求：

- a) 建立基于角色的精细化权限管理办法，确保权限分配遵循最小化原则；
- b) 对系统管理员、数据维护人员等特权账户实施动态口令、生物特征等多因素认证；
- c) 设置会话空闲超时机制，强制中断后需重新进行身份认证。

11.1.3 漏洞与风险管理

漏洞与风险管理应构建主动防御机制，降低数字化平台安全风险，并应符合下列要求：

- a) 数字化平台正式运行前应通过第三方机构渗透测试，测试范围涵盖业务逻辑漏洞、接口安全等方面；
- b) 应建立漏洞响应机制，对高危漏洞应立即启动修复流程，优先处置；
- c) 不应使用未提供长期支持版本的第三方软件组件。

11.1.4 安全审计

安全审计应实现全流程操作可追溯，保障行为合规性和责任可认定，并应符合下列要求：

- a) 完整记录用户操作日志，包含登录时间、操作内容、目标数据及操作结果等关键要素，日志留存周期满足合规审计要求；
- b) 审计记录通过数字签名或区块链存证技术确保不可篡改；
- c) 支持基于异常行为特征（如高频数据导出、非工作时间访问）的实时告警功能。

11.1.5 应急响应

应急响应应具备快速恢复能力，最大限度减少安全事件影响，并应符合下列要求：

- a) 应遵循 GB/T 20986 的规定，制定数字化平台的专项应急预案，定期开展攻防演练；
- b) 核心业务系统的数据恢复时间不宜超过 2h。

11.2 设备安全

11.2.1 平台设备

平台设备应建立全面的安全防护机制，保障基础设施的可靠运行，并应符合下列要求：

- a) 服务器设备符合 GB/T 39680 的规定并依据该标准对服务器设备进行测评；
- b) 网络设备配置地址解析协议防欺骗、动态主机配置协议监听及端口隔离等安全策略，并在关键网络节点部署流量异常监测系统；
- c) 存储设备采用全磁盘加密技术，备份数据异地存放且物理隔离，密钥管理系统独立于业务网络。

11.2.2 终端设备安全

平台应对接入的终端设备安全管控机制，重点通过数字化平台侧安全能力实现设备接入认证与行为监控，保障终端数据安全。具体应符合下列要求。

- a) 数字化平台建立终端设备身份认证机制，针对设备硬件条件实施差异化安全策略，并符合下列要求：
 - 1) 对具备数字证书管理能力的设备，符合 GM/T 0014 的规定；
 - 2) 对资源受限设备，建立“一机一密”的强认证体系，采用预置安全密钥方式实现设备唯一性认证；
- b) 数字化平台部署动态白名单管控功能，拒绝未授权设备接入。设备身份标识信息与数字化平台白名单实时比对校验，发现异常设备立即启动连接阻断并生成安全告警。

11.3 数据安全

数据安全应遵循国家标准并覆盖数据全生命周期，并应符合下列要求：

- a) 数据分类分级符合 GB/T 43697 规定，建立动态管理体系，标注公开、内部、敏感三级敏感等级，业务规则或法规变更后及时完成分类分级标准更新；
- b) 敏感数据存储与传输采用符合 GM/T 0018 的商用密码算法加密，主密钥通过硬件密码机保护并定期轮换，电子合同、图像文件等非结构化数据实施加密保护，终端设备数据加密符合 GB/T 38637.2—2020 第 8 章规定；
- c) 业务接口通信强制启用 TLS 1.3 协议并禁用不安全密码套件，移动端与云端数据传输通道实现端到端加密并支持 X.509 证书双向认证，租金结算等关键业务指令附加 SM2 数字签名且验签过程应在安全隔离环境中执行；
- d) 数据库应实施透明数据加密，备份数据应加密后异地存储，关键业务数据存储应满足 RAID 6 冗余标准并实施多重备份策略，日志文件应与业务数据存储介质物理隔离且访问权限实施分离控制；
- e) 测试环境使用生产数据时应进行脱敏处理，数据销毁应留存完整审计日志，业务数据留存期满后应完成不可逆删除。

11.4 隐私保护

11.4.1 个人信息处理

个人信息处理应符合 GB/T 35273 的规定，且遵循最小必要原则并保障租户权利，并应符合下列要求：

- a) 收集租户信息前得到租户同意并确认，明确数据用途、存储期限及第三方共享范围；
- b) 生物特征等敏感个人信息处理取得单独明示同意，并提供在线授权撤回功能；
- c) 个人信息采集范围限制于租赁合同履行必需内容。

11.4.2 隐私权利保障

隐私权利保障应建立便捷的租户行权渠道和审计机制，并应符合下列要求：

- a) 提供线上个人信息查询、更正、注销入口，常规请求应在合理时限内响应；
- b) 个人数据访问日志完整记录操作者身份、时间及数据类型，保留周期需满足法定审计要求。

11.4.3 第三方数据管控

第三方数据管控应实施严格的共享监管和责任追溯，并应符合下列要求：

- a) 向第三方提供数据时，签订数据保护协议，明确安全责任及违约条款；
- b) 通过 API 接口传输个人数据时，实施字段级脱敏与实时流量监控；
- c) 发现第三方数据违规行为时，在 24h 内终止数据提供。

12 运维管理

数字化平台运维管理应遵循 GB/T 36626 的规定，通过体系化实施安全策略管控、风险动态评估、数字化平台分级防护、运行监测审计及应急响应处置等核心运维活动，建立涵盖人员、流程、技术的持续改进机制，确保运维过程合规性、服务可用性及安全事件可控性。