

DB 3206

南 通 市 地 方 标 准

DB 3206/T 1108—2025

“互联网+明厨亮灶”智慧监管规范

Specification for the intelligencel management of "internet and bright kitchen"

2025 - 04 - 14 发布

2025 - 05 - 01 实施

南通市市场监督管理局 发 布

目 次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 基本要求 2

5 设备技术要求 3

6 平台建设要求 4

7 平台安全维护 7

参考文献 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。

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。

本文件由南通市海门区市场监督管理局提出。

本文件由南通市市场监督管理局归口。

本文件起草单位：南通市海门区市场监督管理局、南通市质量技术和标准化中心、智锐达仪器科技南通有限公司、南通市海门区食品行业协会。

本文件主要起草人：秦强、周俊如、季磊、周鸣镝、郁卫丰、张新宇、施晓玲、严雪松、俞春华、花忠、朱慧涓、陆威、徐东利、袁苏雅、顾燕、汤海霞、朱伟军、岑洪斌。

"互联网+明厨亮灶"智慧监管规范

1 范围

本文件规定了“互联网+明厨亮灶”智慧监管的基本要求、设备技术要求、平台建设要求和企业管理要求。

本文件适用于南通市餐饮服务单位“互联网+明厨亮灶”的管理。

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 20984-2022 信息安全技术—信息安全风险评估方法

GB/T 22239-2019 信息安全技术—网络安全等级保护基本要求

GB/T 25070-2019 网络安全等级保护安全设计技术要求

GB/T 27306 食品安全管理体系 餐饮业要求

GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 28827.3-2012 ITSS 信息技术服务 运行维护 第3部分：应急响应规范

GB 31654 食品安全国家标准 餐饮服务通用卫生规范

GB 50395 视频安防监控系统工程设计规范

GA/T483-2004 计算机信息系统安全等级保护工程管理要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

互联网+明厨亮灶 internet + bright kitchen

餐饮单位主要通过视频监控和互联网技术，接入可视化展示和监管系统，展示餐饮单位后厨食品加工制作关键过程，实现互联网平台管理，接受消费者和监管部门等共同监督的一种明厨亮灶形式。

3.2

AI智能监控 artificial intelligence monitoring

通过远端视频采集装置，实现对监控区域内的人员着装、鼠患、人员动态操作等行为视频采集和对不规范经营行为实行实时自动抓拍、智能分析、分级预警等功能。

3.3

专间 private room

处理或短时间存放直接入口食品的专用加工制作间，包括冷食间、生食间、裱花间、中央厨房和集体用餐配送单位的分装或包装间等。

3.4**AI算法 artificial intelligence algorithms**

AI算法是一种特殊的计算机程序，旨在通过模拟人类思维和决策过程，使计算机能够执行复杂的任务并解决问题。

4 基本要求**4.1 经营资质**

餐饮服务单位应持有合法有效的食品经营许可证或小餐饮备案证明，并依许可或备案范围从事食品生产经营活动。

4.2 场所与布局

餐饮服务单位建设场所与布局、餐饮基础设施设备应符合GB/T 27306、GB 31654和《餐饮服务食品安全操作规范》的要求。

4.3 原料采购

餐饮服务单位应建立严格的原料采购制度，对供应商进行资质审核，将食材采购信息实时上传至智慧监管平台，确保食材来源可追溯。

4.4 成品质量

餐饮服务单位应确保菜品质量。鼓励餐饮服务单位提供菜品营养信息和成分表。

4.5 人员管理

餐饮服务单位应设置食品安全管理员，加强人员培训和管理，直接接触食品的从业人员按时办理健康证并上传智慧监管系统。

4.6 信息公示

餐饮服务单位应提供自己的二维码，通过扫码能够正常显示餐饮服务单位的明厨亮灶建设、许可信息、评定结果、食品添加剂公示、人员健康证、主要食材采购等信息。

4.7 异常处理

餐饮服务单位通过商户 APP 收到异常预警信息时，应及时查看并处理异常信息。处理完成后，于 7

个自然日内反馈处理结果，完成监管闭环。

5 设备技术要求

5.1 监控摄像头安装

餐饮服务单位根据厨房面积大小和实际供餐加工经营场所安装相应数量的高清摄像头，能清晰监控到食品粗加工区域、烹调区域、专间、餐饮具洗消间、库房等关键控制区域的卫生状况、从业人员的工作情景等，安装要求见表1。

表 1 摄像头安装要求

安装位置	监控覆盖要求
粗加工区	需监控水池分类清洗、切配过程的场景。
烹饪区	需监控工作人员穿戴、地面、工作台面及设施设备的场景。
专间	需监控工作人员穿戴、操作台面、设施设备及食品加工过程的场景。
消洗间	需监控餐饮具回收、清洗、消毒、保洁的场景。
库房	需监控食品原料储存（分类分架、离地离墙10cm）、食品原料使用和留样冰箱等场景。

5.2 摄像头技术要求

摄像头应满足：

- a) 应具备防油污、防烟雾、防火光、防水雾、耐高、耐腐蚀性；
- b) 镜头护盖应可拆卸、便于清洗或更换；
- c) 外壳防护等级应满足IP67要求；
- d) 应不低于400万像素，清晰度1080P以上；
- e) 应支持不少于2路码流，编码标准应支持H264、H. 265或SVAC编码格式；
- f) 接口协议应符合GB/T 28181的规范。

5.3 视频存储

所有摄像头的视频资料至少存储 15 天，推荐选择至少 1TB 以上的硬盘容量的硬盘录像机（DVR）或网络录像机（NVR）。同时，也可以考虑使用计算机硬盘或云端存储作为备份或扩展存储容量的选择，确保不会因网络问题导致存储图像不完整和抓拍数据丢失。

5.4 算法服务器

算法服务器应满足一定性能，硬件指标见表 2。

表 2 算法服务器硬件指标

主体	型号
GPU	RTX4070Ti/RTX4090 以上
CPU	i9-24 核以上
内存	32G 以上
操作系统	Ubuntu16. 04/18. 04

5.5 异常抓拍

- AI 智能监控餐饮服务单位的食品加工操作过程，需具备算法分析功能，应包括但不限于以下内容：
- a) 后厨出现动物，如老鼠、猫、狗等；
 - b) 从业人员着装不规范，如未佩戴工作帽、未佩戴口罩、未穿工作服等；
 - c) 从业人员行为不规范，如在后厨抽烟、玩手机等；
 - d) 厨房卫生不整洁，如垃圾桶未加盖、堆放杂物、厨具长时间未清洗等；
 - e) 摄像头断电或断开网络连接。

6 平台建设要求

6.1 “互联网+明厨亮灶”平台

由监管部门主导，建立统一的“互联网+明厨亮灶”平台，将餐饮服务单位的主体信息、监控线路、监管数据等整合到该平台。整个平台由视频监控、算法服务器、数据推送、监管平台和商户 APP 共同组成系统，见图 1 所示。

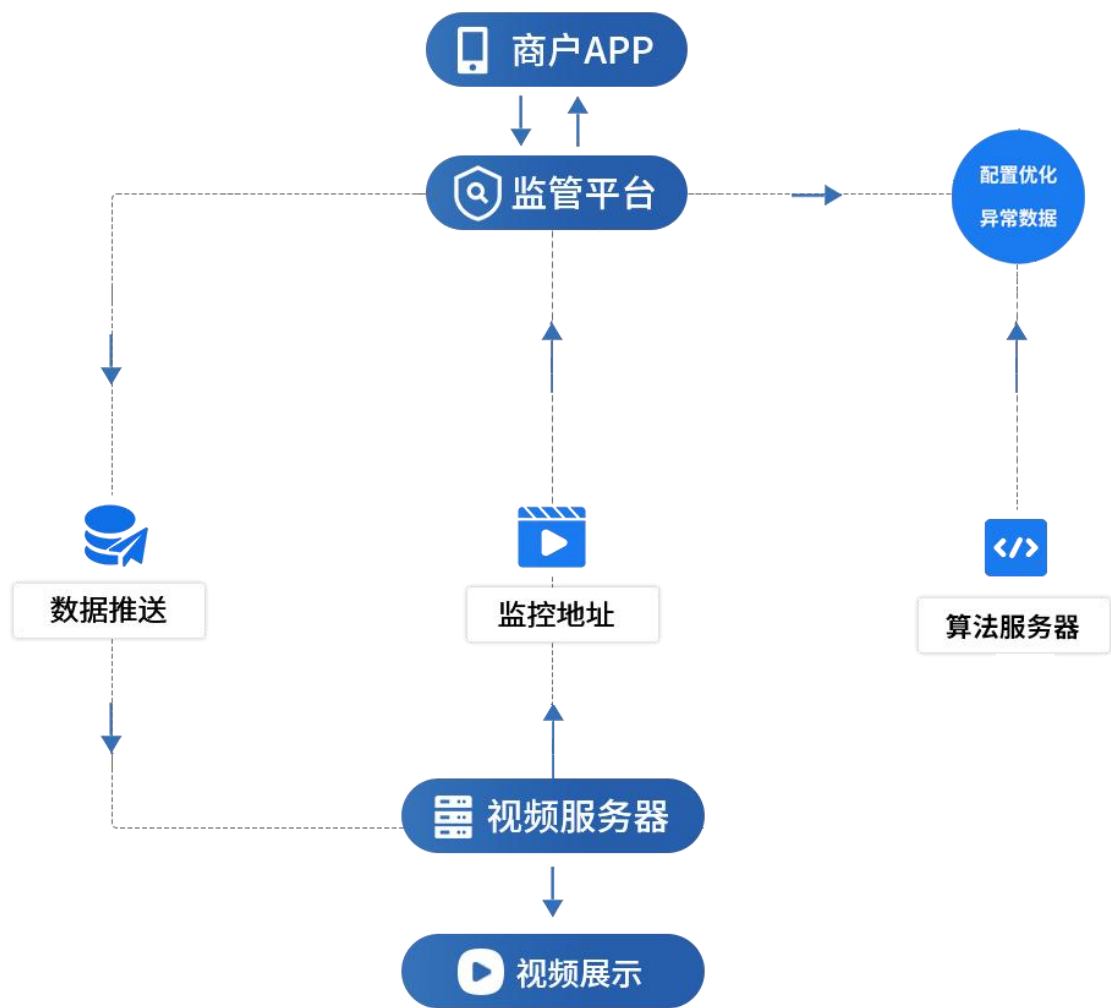


图 1 监管平台架构图

6.2 实时监控

实时监控应包括但不限于以下功能：

- 实时采集：通过部署高清摄像头，覆盖厨房的粗加工区、烹饪区、专间、洗消区、库房等关键区域，实时采集视频数据；
- 存储与回放：支持视频数据的本地或云端存储，提供历史回放功能，便于追溯问题；
- 多设备管理：集中管理多个摄像头，支持远程控制（如角度调整、焦距切换）。

6.3 算法服务器

算法服务器应包括但不限于以下功能：

- AI 智能分析：通过环境监测、行为监测、数据监测智能分析发现问题；
- 事件触发：实时推送异常警报至监管平台和商户 APP，并记录事件日志；
- 模型优化：通过机器学习持续提升识别准确率，支持自定义规则扩展。不断优化完善明厨亮灶 AI 算法，增加能够识别的异常行为，提高异常行为的识别准确率和预警及时率；
- 系统维护：定期对系统进行升级和维护，确保系统的稳定性和可靠性。

6.4 数据推送

数据推送应包括但不限于以下功能：

- 实时传输：通过消息队列（如 Kafka、RabbitMQ）或 API 接口，将算法分析结果（如警报、评分）实时推送至下游模块；
- 数据标准化：统一数据格式（如 JSON），确保监管平台和商户 APP 高效解析；
- 报告生成：定期推送卫生检查报告、整改通知等结构化数据，支持 PDF/Excel 导出；
- 可靠性保障：采用冗余传输机制，确保关键数据不丢失。

6.5 监管平台

6.5.1 实时监控与录像

能实时查看辖区内所有接入商户的厨房画面及录像回放，应包括但不限于以下功能：

- 地图模式：显示管辖范围内的门店列表、门店在地图上的标注、摄像头运行概况，支持夜间模式和日间模式，责任主体有聚合模式和离散模式，缩放地图比例尺最后可点击地图上的门店进入视频直播；
- 列表模式：可按照区县、分局的层级进行查看视频监控的概况；
- 视频直播：门店摄像头的视频直播功能，提供流畅和高清两种分辨率的视频流，且提供四宫格、九宫格等播放形式；
- 摄像头管理：对接入的摄像头进行管理和维护，包含摄像头位置、品牌、型号、所属门店、通道号、AI 设置等，可以选择敏感或隐私摄像头是否开放给消费者等功能。

6.5.2 异常预警

能接收并处理异常信息，下发预警通知，跟踪处理进度，应包括但不限于以下功能：

- 监控抓拍预警：AI 智能监控检测到异常行为，能立即通过手机小程序、APP、短信、电话等方式向监管人员、经营主体发出预警信息；
- 异常门店查询：可以查询门店名称、所属区域、门店类型、主体业态、异常次数、已处理次数、处理率等信息；
- 异常数据查询：可以查询门店名称、所属区域、摄像头位置、异常分类、异常事件、异常时间、处理状态、处理时间、详情等信息，并支持列表\四宫格\九宫格的样式查看；

——健康证查询：可以查询所有商户上传的工作人员健康证信息，并对逾期健康证做出预警、临期健康证做出提醒。

6.5.3 数据统计与分析

平台可以统计区域内的违规类型分布、商户排名、趋势图表，对收集到的监控数据从异常总量、异常平均量、异常处理率、异常门店占比、异常风险占比几个方面来进行统计分析，监管人员能从监管端远程掌握餐饮服务单位的食品安全状况，发现存在的问题和隐患。

6.5.4 权限分级

支持多级监管角色（如省/市/区级），按权限分配数据访问范围。

6.5.5 档案管理

档案信息应包含门店名称、经营者名称、联系电话、联系地址、统一社会信用代码、许可证编号、店铺类型、主体业态、营业执照（图片）、经营许可证（图片）、门头照片等，监管平台能对餐饮服务单位的档案管理维护。

6.5.6 信息公示

信息公示应包括但不限于以下功能：

- 视频监控公示：包含每个摄像头的视频直播功能，根据实际监管要求，可设置为不公示；
- 异常抓拍公示：包含由摄像头抓拍到的异常总量、异常时间、异常分类、异常图片等信息，根据实际监管要求，可设置为不公示；
- 证照信息公示：包含了餐饮服务单位的基本信息，突出营业执照、食品经营许可证、小餐饮备案证明。

6.6 商户APP

商户 APP 应包括但不限于以下功能：

- 异常处理：通过算法智能抓拍到的异常信息，会在 APP 中进行展示。商户需要对发现的异常情况做出对应的处理操作，提交整改反馈（如文字、照片）。
- 实时自查：商户可以通过 APP 查看厨房的实时监控画面及历史视频片段。
- 信息管理：商户可以在门店信息发生变化时通过 APP 进行修改变更。
- 健康证管理：商户可以通过 APP 上传工作人员的健康证，系统会自动推送健康证临期提醒和逾期预警。

7 平台安全维护

7.1 系统安全

系统安全应符合GB/T 22239中信息安全等级二级（含）以上的要求。

7.1.1 网络安全

网络安全应包括以下内容：

- 网络架构：关键设备冗余设计，划分子网或网段，绘制实时网络拓扑图；
- 访问控制：部署防火墙，按用户或网段级控制访问权限，限制访问用户数量；
- 入侵防护：检测端口扫描、拒绝服务攻击等行为，并记录网络设备日志；
- 边界完整性：防止内部用户非法外联，监控网络流量和用户行为。

7.1.2 主机安全

主机安全应包括以下内容：

- 机房选址：需具备防震、防风、防雨能力；
- 身份鉴别：操作系统和数据库用户需强密码策略（复杂度、定期更换），远程管理需加密传输；
- 安全审计：覆盖所有用户行为，记录事件类型、时间及结果，保护日志防篡改；
- 资源控制：限制终端登录方式、超时锁定及系统资源使用上限。

7.1.3 应用安全

应用安全应包括以下内容：

- 身份认证：专用登录模块，确保用户唯一性，支持登录失败处理，如锁定账户等；
- 通信安全：敏感数据加密传输，校验数据完整性，如校验码技术等；
- 资源控制：数据有效性检查，限制并发会话数，故障时保留部分功能。

7.1.4 数据安全

数据安全应包括以下内容：

- 数据保护：检测数据完整性和保密性，重要数据加密存储；
- 备份恢复：定期备份关键数据，确保系统可用性，关键设备冗余，如双机热备等。

7.2 系统维护

7.2.1 维护内容

系统维护应包括以下内容：

- a) 硬件设备提供保修服务和现场备件的更换安装服务、定期现场巡检、维护性软件及版本升级支持服务、现场故障诊断及故障排除技术支持服务等；
- b) 对应用系统所属服务器、操作系统、数据库定期进行状态检查；
- c) 定期对操作系统、应用系统及数据库开展补丁升级、病毒查杀以及安全日志的查看和管理等；
- d) 应用系统软件的安装、升级、维护，并对应用系统的升级维护工作做好相应记录；
- e) 对系统中的业务数据定期进行更新，对数据库进行安装、升级、维护以及参数调整，定期对数

数据库的数据进行备份；

- f) 对数据结构及代码进行维护，对数据库系统的性能进行监控，做好系统优化工作。
- g) 对系统管理员的账号密码进行设置，杜绝弱口令，对应用系统及操作系统的安全漏洞进行整改，做好中间件防护。

7.2.2 维护事项和频率

系统维护事项和频率见表 3。

表 3 维护流程和频率

维护事项	维护频率
日常巡检	每日数据备份
应用系统漏洞扫描	每 1 个月一次
应用系统补丁升级（发现漏洞后）	及时处理
应用系统数据备份（如果是实时备份，则维护时间就是实时）	每周一次
应用系统病毒查杀	每周一次
更改所有维护相关密码（必须改为强口令）	每 2 个月一次
查看应用系统运行日志	每周一次
发现运行日志异常	及时处理

7.2.3 维护沟通机制

建立系统维护沟通机制，指定一名工作负责人，确保通讯畅通，能提供在线（微信）、现场技术等支持处理相关工作。

7.2.4 维护服务方案

根据事先制定的技术建设实施、维护方案，进行相关技术服务，包括但不限于：

——技术支持时效响应：1 小时内响应客户故障申诉，2 小时内解决基本故障；

——软件升级服务：备份现有服务器的所有文件及数据、安装部署选定好的新版本安装包、运行新版本升级程序、恢复原有数据文件，检查相关功能可用性，确认无误后新版本上线；

——巡检服务：定期进行服务状况巡检，并记录服务器状态。

7.2.5 保密承诺

“互联网+明厨亮灶”平台使用者应认真遵守国家保密法律法规和本单位的保密制度，履行保密义务。

7.3 应急处理方案

7.3.1 硬件系统故障

建立完善的系统服务监控体系，能第一时间发现系统故障；建立应急系统，当故障无法在 10 分钟内解决，切换至备份系统；备份相关数据，并做好异地备份，记录故障分析报告。

7.3.2 网络系统故障

对系统进行网络监控，系统发生故障应及时问询网络服务商，找出网络问题根源，如无法在 10 分钟内解决，切换至备份子系统并记录网络故障分析报告。

7.3.3 软件系统故障

软件系统发生故障时，应及时查看软件故障原因，做出风险等级判断，根据风险等级，判断回退软件系统版本或升级软件版本，分析记录软件故障原因并记录文档。

7.3.4 黑客攻击

应对黑客攻击时，应关闭服务器系统，封锁或删除被攻破的账号，阻止可疑用户进入。系统管理员应及时清理系统，恢复数据程序、系统和网络正常，并修复相关系统漏洞。不能准确判断黑客攻击行为和采取防范措施的，报告网络应急小组，请求支援。处置结束后，将事发经过、处置方式归类成文档并保存。

7.3.5 业务数据损坏

业务数据发生损坏时，系统管理员应及时检查、备份业务系统当前数据，调用备份数据后，检查当前数据和历史数据的差别，做好相关补录工作并记录故障分析报告。

7.3.6 重大事故报警

确定为重大事故，比如网站信息被非法篡改，留存非法信息画面，保存相应系统访问日志。向公安局网络警察支队报警，并请求安全技术厂商和安全技术服务商，对事故进行分析，找出入侵 IP。详细记录事故现象、攻击方法、攻击源头，形成报告，作为报警依据。

参 考 文 献

- [1] 餐饮服务食品安全操作规范（国家市场监管总局公告 2018 年第 12 号）

