ICS 35.020
CCS X 04

T/ACCEM

团　　体　　标　　准

T/XXX XXXX—XXXX

食品大数据应用管理规范

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国商业企业管理协会　　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。

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。

本文件由北京立先标准技术有限公司、北京信睿浩扬科技有限公司提出。

本文件由中国商业企业管理协会归口。

本文件起草单位：xxxxxxx，xxxx，xxxx

本文件主要起草人：xxx

食品大数据应用管理规范

1 范围

本标准规定了大数据应用管理平台的术语和定义、产品标识、技术要求、试验方法、检验规则及标志、包装、运输和贮存。

本标准适用于适用于食品生产、加工、流通、销售等全产业链企业，包括食品生产企业、餐饮服务商、电商平台及冷链物流运营商；同时涵盖市场监管部门、第三方检测机构及科研单位等监管与研究主体。

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。

《中华人民共和国食品安全法》

《食品安全国家标准》

《食品安全法》及其实施条例（明确数据记录保存义务）

《市场监管总局关于食品信息化追溯体系建设的指导意见》（2020年）

《国务院办公厅关于运用大数据加强对市场主体服务和监管的若干意见》

《国家卫生健康委办公厅关于进一步优化食品企业标准备案管理工作的通知》(国卫办食品发〔2024〕4号)

《信息技术互联网国际标准》（ISO/IEC 11801）

GB/T 43705-2025《科学数据安全分类分级指南》

GB/T 45574-2025《 数据安全技术 敏感个人信息处理安全要求》

GB/T 35274-2023 《信息安全技术 大数据服务安全能力要求》

GB/T 35273-2020《信息安全技术个人信息安全规范》

GB/T 35589-2017《大数据技术参考模型标准》

3 术语和定义

下列术语和定义适用于本文件。

3.1 食品大数据 Food big data

在食品生产、加工、流通、消费、监管等环节中产生的，具有规模大、类型多、速度快、价值密度低等特征的数据集合。

4 数据标准规范

4.1 数据分类与敏感度

各平台单位在开展科学数据安全分类工作时，应符合GB/T 43705-2025 5.2章节关于科学数据分类方法与过程要求进行开展。

4.1.1 数据分类

按照业务场景划分

4.1.1.1 生产数据

包括原料采购、加工工艺、设备运行、质量检测等数据。

4.1.1.2 流通数据

涵盖物流轨迹、仓储环境、销售渠道、消费者反馈等数据。

4.1.1.3 监管数据

包含政府抽检结果、风险预警、企业资质、食源性疾病报告等数据。

4.1.1.4 消费者数据

涉及饮食偏好、健康指标、购买行为等个人信息。

4.1.2 敏感度分级

敏感数据应符合 GB/T 45574-2025 5.2章节关于个人信息收集合法性原则，根据数据泄露或滥用的风险划分

4.1.2.1 一级（公开数据）

产品标签信息，如食品营养成分表、公开的行业统计数据。

4.1.2.2 二级（内部数据）

企业生产经营数据（非核心商业机密）、非个人身份关联的消费行为数据。

4.1.2.3 三级（敏感数据）

消费者手机号（需脱敏），个人健康信息、未公开的检测结果、企业核心配方及工艺数据。

4.1.2.4 四级（核心机密）

涉及国家安全的食品供应链数据、重大食品安全事件的未公开调查记录。

4.2 数据采集与存储

4.2.1 采集要求

4.2.1.1 跨部门协同

需采用区块链技术构建分布式采集架构，通过智能合约实现农业、市场监管、卫健等部门数据的可信上链，解决 “数据孤岛” 问题。

4.2.1.2 质量控制

需明确数据采集频率、格式（如结构化 JSON、时序数据）及校验规则，确保数据完整性（缺失值填充策略）、准确性（传感器校准标准）。

4.2.1.3 来源追溯

应对每笔数据标注采集主体、时间、设备编号等元信息，通过区块链哈希值实现全生命周期溯源。存储要求。

4.2.1.4 存储架构

采用 “联盟链 + 数据湖” 混合存储模式，敏感数据加密后存储于区块链节点，公开数据存储于中心化数据湖，支持 PB 级数据扩展。

4.2.1.5 格式统一

建立统一的数据描述语言（如食品标签编码、污染物指标字典），支持跨系统检索。

4.2.1.6 备份策略

关键数据实施 “3+2” 多节点冗余备份（3 个活跃节点 + 2 个冷备节点），冷数据按季度归档，存储介质符合 GB/T 35274-2023 的物理安全要求。

4.3 数据处理与分析模型

进行数据采集和模型分析时，相关标准应符合GB/T 35589-2017第五章节，GB/T 35273-2020关于个人隐私保护部分的相关要求。

4.3.1 处理流程

4.3.1.1 清洗与集成

通过规则引擎过滤噪声数据，利用实体识别技术整合多源异构数据（如企业 ERP 数据与监管平台数据），数据清洗效率需达到 95% 以上。

4.3.1.2 脱敏处理

对敏感字段采用差分隐私（ε- 差分隐私模型）、同态加密等技术，确保分析过程中个人信息不可还原。

4.3.1.3 日志审计

记录数据处理全流程日志，包括清洗规则、脱敏算法、模型训练参数等，支持监管部门合规审计。

4.3.2 分析模型

4.3.2.1 预测性分析

基于 LSTM 神经网络构建食品保质期预测模型，结合传感器数据实现货架期预警，预测准确率不低于 90%。

4.3.2.2 溯源分析

通过区块链智能合约实现 “农田到餐桌” 全链条追溯，支持问题食品 1 小时内定位源头。

4.3.2.3 知识图谱

整合食品成分、营养属性、消费偏好等数据，构建食品领域知识图谱，支撑个性化食谱推荐与健康膳食建议。

5 数据功能规范

5.1 数据分析功能

5.1.1 食品安全监测

实时分析污染物检测数据，结合 GIS 地图可视化展示风险区域，异常数据触发三级预警（黄色、橙色、红色）。

5.1.2 供应链优化

通过物流数据与销售数据关联分析，优化仓储布局与配送路径，降低冷链损耗率 15% 以上。

5.1.3 消费者洞察：

基于机器学习分析饮食行为数据，为企业提供产品研发方向（如低糖食品趋势预测），为公众生成个性化营养报告。

5.2 数据共享功能

5.2.1 跨部门共享

跨部门共享：通过区块链的多方安全计算（MPC）技术，实现监管部门间数据 “可用不可见”，如市场监管局与卫健委共享食源性疾病数据时，仅输出分析结果而不泄露原始数据。

5.2.2 企业间协作

建立数据共享接口规范（如 REST API），支持上下游企业按需获取供应链数据（如原料溯源信息），响应延迟不超过 500ms。

5.2.3 公众查询

开放经脱敏的食品抽检结果、营养成分等数据，通过官方平台提供可视化查询服务。

5.3 数据追溯功能

5.3.1 全链条追溯

利用区块链不可篡改特性，记录食品生产、加工、运输、销售各环节数据，消费者可通过扫码查询产品全生命周期信息，包括原料来源、加工工艺、质检报告等。

5.3.2 事件追踪

对食品安全事件，支持从消费端反向追溯至生产环节，快速定位问题源头（如某批次原料污染事件）。

5.3.3 责任界定

通过数据时间戳与操作日志，明确各环节责任主体，为监管执法提供证据支撑。

6 数据应用规范

6.1 食品生产环节

6.1.1 智能管控

通过传感器数据实时监控生产环境（温度、湿度、压力等），结合 AI 模型预测设备故障，提前 24 小时发出维护预警，降低停机损耗。

6.1.2 质量控制

基于在线检测数据（如金属异物、微生物指标）自动触发预警，实现不合格产品实时拦截。

6.1.3 绿色生产

分析能耗数据，优化生产工艺，推动低碳减排（如冷链物流能耗优化）。

6.2 食品流通环节

6.2.1 冷链监控

通过物联网设备采集运输途中的温湿度数据，确保生鲜食品品质，异常时自动报警并调整配送路线，确保生鲜食品中心温度波动≤±1℃。

6.2.2 防伪验证

利用区块链哈希值对食品包装进行唯一标识，消费者可通过官方 APP 验证真伪，打击假冒伪劣。

6.2.3 需求预测

结合历史销售数据与市场趋势，为经销商提供库存预警，减少食品损耗（如临期食品提前促销）。

6.3 食品监管环节

6.3.1 风险预警

整合抽检数据、舆情信息与消费投诉，构建食品安全风险评估模型，提前识别潜在隐患（如某类食品添加剂超标风险）。

6.3.2 协同监管

通过跨部门数据共享，实现从农田到餐桌的全链条监管，如农业农村部门与市场监管部门联动查处违规使用农药问题。

6.3.3 应急响应

对突发食品安全事件，快速调取相关企业生产数据、流通轨迹，辅助制定召回方案与处置策略。

7 数据安全与隐私保护规范

7.1 数据网络安全防护

7.1.1 边界防护

部署下一代防火墙（NGFW）、入侵检测与防御系统（IDPS），阻断非法网络攻击。

7.1.2 访问控制

采用零信任架构（Zero Trust），基于身份认证（如多因素认证）与权限最小化原则，限制数据访问范围。

7.1.3 日志审计

对数据操作（如查询、修改、删除）进行全量日志记录，支持安全事件溯源与合规审计，符合 GB/T 35274-2023 的安全审计要求。

7.2 数据安全加密要求

7.2.1 传输加密

数据在公网传输时采用 TLS 1.3 协议加密，敏感数据（如个人健康信息）采用国密算法（SM4）加密。

7.2.2 存储加密

对敏感数据字段（如身份证号、银行账户）实施字段级加密，区块链节点存储的隐私数据采用同态加密技术，确保计算过程中数据不可见。

7.2.3 密钥管理

建立密钥生命周期管理机制，定期更新加密密钥，密钥存储符合国家密码管理局相关标准。

7.3 数据隐私保护策略

7.3.1 合规要求

遵循《个人信息保护法》《数据安全法》，对个人信息处理需获得明确授权，禁止未经同意的跨境传输。

7.3.2 去标识化

对消费者数据采用匿名化处理（如哈希脱敏、数据泛化），确保无法通过数据反推个人身份。

7.3.3 隐私计算

在数据分析场景中，采用联邦学习、可信执行环境（TEE）等技术，实现 “数据不动模型动”，保护数据隐私的同时完成联合建模。