

T/ACCEM

团 体 标 准

T/ACCEM XXXX—2025

数字经济安全管理规范

Specification for Security Management in the Digital Economy

（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

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 基本原则 1

5 安全管理体系要求 1

 5.1 组织架构 1

 5.2 制度框架 1

6 关键技术要求 2

 6.1 数字基础设施安全 2

 6.2 数据与网络安全 2

 6.3 应用场景安全 2

7 数据安全和隐私保护 2

8 风险应对与应急处置 2

9 实施与监督 2

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。

本文件由济南市章丘区能源和价格服务中心、北京光程科技有限公司提出。

本文件由中国商业企业管理协会归口。

本文件起草单位：×××

本文件主要起草人：×××

数字经济安全管理规范

1 范围

本标准规定了数字经济活动的安全管理要求，涵盖数据全生命周期安全、数字技术应用安全、数字基础设施保护、风险防控与应急处置等内容，适用于企业、政府机构及第三方服务提供方。

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 35273《信息安全技术 个人信息安全规范》

GB/T 37988《数据安全能力成熟度模型》

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字经济

以数据为关键要素，通过数字技术与实体经济融合形成的新经济形态。

3.2

数据要素市场

涵盖数据采集、存储、加工、交易、应用等环节的市场化配置体系。

3.3

数字安全风险

包括数据泄露、算法滥用、基础设施攻击等威胁。

1. 关键数字基础设施：定义涵盖能源、交通、金融等核心领域的高度依赖数字技术的系统 4。
2. 数据信托：解释第三方受托管理数据的权责模型及合规边界。
3. 隐私增强技术（PETs）：列举同态加密、联邦学习、差分隐私等技术原理与应用场景 5。
4. 数字安全成熟度：划分初始级、可重复级、已定义级、量化管理级、优化级五级评价体系

4 基本原则

- 4.1 安全与发展并重：在保障安全的前提下激活数据要素价值。
- 4.2 分级分类管理：依据数据敏感度和应用场景实施差异化管控。
- 4.3 全链条协同治理：政府、企业、行业组织共建责任共担机制。
- 4.4 技术合规双驱动：以技术创新提升防护能力，以标准规范约束行为边界。

5 安全管理体系要求

5.1 组织架构

- 5.1.1 设立专职数字安全管理部门，明确决策层、执行层、监督层职责。
- 5.1.2 建立跨部门协同机制，定期开展安全风险评估与合规审计。

5.2 制度框架

- 5.2.1 制定《数据分类分级指南》《安全事件应急预案》等内部规范。
- 5.2.2 落实数据跨境流动、算法透明度等合规要求。

6 关键技术要求

6.1 数字基础设施安全

- 6.1.1 数据中心、云计算平台需符合物理环境安全与容灾备份标准。
- 6.1.2 5G、物联网设备需通过安全认证，防范供应链风险。

6.2 数据与网络安全

- 6.2.1 采用加密、脱敏、访问控制等技术保护数据完整性。
- 6.2.2 部署入侵检测系统（IDS）、防火墙等防范网络攻击。

6.3 应用场景安全

- 6.3.1 人工智能算法需通过可解释性评估，避免歧视性结果。
- 6.3.2 区块链应用需确保节点身份验证与智能合约代码安全。

7 数据安全与隐私保护

- 7.1 数据采集：遵循最小必要原则，获取用户明示同意。
- 7.2 数据流通：通过数据交易所或可信平台进行合规交易。
- 7.3 跨境传输：遵守国家数据出境安全评估制度。

8 风险应对与应急处置

- 8.1 建立安全事件分级响应机制，明确报告流程与时限。
- 8.2 定期开展攻防演练，提升全员安全意识和应急能力。

9 实施与监督

- 9.1 合规审计：第三方机构每年开展安全能力评估，结果向社会公示。
 - 9.2 持续改进：根据技术演进与政策调整更新标准内容。
-