数据安全治理指南

编制说明

标准起草工作组

2025 年 4 月

目　录

1 必要性

本标准旨在为各类组织提供系统性、可落地的数据安全治理框架，通过整合法律法规要求、技术防护手段与行业场景需求，构建覆盖数据全生命周期及基础设施的多层级防护体系，解决数字化转型中面临的数据安全管理碎片化、风险滞后性等核心挑战。其意义在于帮助组织实现合规底线坚守与数据价值释放的平衡：一方面响应《数据安全法》《个人信息保护法》等法规要求，规避数据滥用与泄露风险；另一方面支撑政务、工业互联网、车联网等场景下的数据安全流通与高效利用，推动跨行业技术协同与标准互认，为数字经济发展筑牢可信、开放的数据生态基础，助力数字中国战略的深化实施。

2 工作简述

2.1 任务来源

本标准根据四川省网络空间安全协会数据安全团体标准制修订计划立项，由四川省网络空间安全协会归口，由成都信息工程大学牵头组织编制。

2.2 起草单位

本标准牵头起草单位：成都信息工程大学；

本标准参加起草单位：成都久信信息技术股份有限公司、成都理工大学、全域数据信息安全重点联合实验室西南实验室。

2.3 起草过程

2024 年 8 月，成都信息工程大学向四川省网络空间安全协会提交《数据安全治理指南》团体标准项目建议书；

2024 年 10 月，召开《数据安全治理指南》团体标准启动会议，会议讨论了标准的大纲，确定了标准起草的总体框架、主要内容、人员分工等；

2024 年 12 月，由四川省网络空间安全协会邀请专家对《数据安全治理指南》立项评审，标准立项，成立标准起草工作组。

2025 年 3 月，完成了团体标准《数据安全治理指南》草案稿编写；

2025 年 4 月，专家对意见修改稿进行了评审，团体标准《数据安全治理指南》文本质量达到征求意见稿发布要求。

3 标准编制原则和主要内容

3.1 编制原则

本标准的制定工作遵循合规性导向、科学性与系统性、可操作性、动态适应性风险管理导向的原则。

a) 合规性导向原则：严格遵循国家法律法规及政策要求，包括但不限于《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等，将法律条款转化为可落地的治理要求，确保标准内容与现行法律框架的一致性。

b) 科学性与系统性原则：基于现有的数据安全治理框架和国内实践经验，结合数据生存周期管理理论，构建覆盖数据分类分级、风险评估、技术防护、组织管理的系统性治理体系，确保逻辑严谨、结构完整。

c) 可操作性原则：聚焦组织实际需求，以“场景驱动、流程规范”为核心，针对数据采集、存储、传输、使用、共享、销毁等全生命周期环节，明确具体控制措施和管理流程，提供可落地的实施指南。

d) 动态适应性原则：充分考虑技术演进（如人工智能等新兴技术应用）和业务场景变化，强调治理框架的灵活性和扩展性，支持组织根据业务需求和技术发展动态调整治理策略。

e) 风险管理导向原则：以数据安全风险评估为核心驱动，贯穿治理全过程（识别、分析、处置、监控），结合数据资产价值、威胁可能性及影响程度，实现风险分级管控，推动资源优化配置。

3.2 主要内容

本标准共分为 7 章，主要技术内容包括：

1．范围；

2．规范性引用文件；

3．术语和定义；

4．数据安全治理总体要求；

5．数据安全治理框架；

6．数据安全治理实施过程；

7．数据安全风险评估与治理。

4 技术论证与效果

本标准的制定以国家法律法规为根本遵循，结合《网络安全法》《数据安全法》《个人信息保护法》等法律要求，明确数据分类分级、风险评估、跨境传输等核心技术条款，并充分参考《数据安全技术 数据分类分级规则》《信息技术服务 治理 第 5 部分：数据治理规范》等国家标准，细化数据资产管理和全生命周期防护的技术指标。技术路线的设计融合了国家标准与行业实践经验，借鉴相关隐私框架等国际规范，结合金融、医疗、政务等领域的场景化需求（如医疗数据脱敏、金融交易数据完整性保护），形成“分层管控、场景驱动、动态防御”的技术实施路径：在基础能力层，依托数据资产发现、分类分级构建治理基线，通过加密、脱敏等技术保障静态数据安全；在过程控制层，基于数据生存周期（采集、传输、存储、使用、共享、公开、销毁等），集成轻量化 API 安全网关、动态访问控制（ABAC）、数据血缘追踪等工具链实现精细化管控；在智能防护层，引入 AI 驱动的异常检测、威胁情报联动及自动化响应（SOAR）技术，提升实时监测与主动防御能力。标准编制过程中所涉技术方案不包含已知必要专利，若未来实施需采用专利技术，将严格遵循《国家标准涉及专利的管理规定》确保合规授权。本标准发布后，预期将显著提升数据安全整体水平，通过统一技术规范降低数据泄露与滥用风险，推动重点行业数据安全合规率提升，同时为跨域数据共享和公共数据开放提供可信框架，助力释放千亿级数据资产价值，破解数据“沉睡”难题。在产业发展层面，标准将引导安全厂商加速研发符合规范的国产化数据加密、隐私计算产品，推动技术生态成熟，并通过设定统一技术门槛规范市场秩序，遏制低质服务，促进数据安全产

业向专业化、标准化转型。此外，标准提出的跨境数据流动合规技术路径，将增强我国企业在全球数字贸易中的竞争力，为数字中国建设提供技术支撑与安全保障。

5 对标情况

本标准严格遵循《网络安全法》《数据安全法》《个人信息保护法》等法律法规的合规要求，并与《GB/T 36073-2018 数据管理能力成熟度评估模型》《GB/T 43697-2024 数据安全技术 数据分类分级规则》等现行国家标准相衔接，形成从法律约束到技术落地的完整链条。在数据治理框架设计上，结合《GB/T 34960.5-2018 信息技术服务 治理 第5部分：数据治理规范》的管理要求和《GB/T 44109-2024 数据治理实施指南》的实践路径，细化数据分类分级、全生命周期安全防护等操作性规范；同时参考《国家数据标准体系建设指南》的总体规划，强化跨行业场景的适应性，确保治理要求与现有标准体系兼容互认，为组织提供合规可行、覆盖全流程的治理指引。

6 标准实施建议

为确保本标准的有效落地，建议建立多部门协同推进机制，由网信、工信、市场监管等部门联合制定配套实施细则，明确责任分工与考核机制，推动地方性法规、行业规范与标准的衔接；技术层面需同步研发数据分类分级、风险评估等工具平台，并提供开源参考实现，降低中小企业实施门槛；过渡期内可通过试点示范、分行业分场景逐步推广，优先覆盖政务、金融、医疗等高风险领域，同时组织第三方机构开展合规咨询服务与能力评估；推广过程中应加强标准宣贯培训，将数据安全治理纳入企业数字化转型考核指标，鼓励行业协会制定团体标准及最佳实践指南，形成“国家标准引领、行业标准细化、企业标准创新”的协同实施生态。

7 需要说明的主要问题

本标准在编制过程中未出现需要说明的主要问题。

8 其他说明事项

无。