

中共连云港市委网络安全和信息化委员会办公室

《网络数据安全规范管理规范》 连云港市地方标准编制说明

一、标准编制背景和目的意义

数据资源已成为国家基础战略性资源和社会生产的创新要素。2021年9月1日，《数据安全法》颁布实施，明确将数据安全上升到国家安全范畴，提出建立健全全流程数据安全管理制度，采取相应的技术措施和其他必要措施，保障数据安全。

近年来，连云港市各级党政机关、重点行业部门汇聚大量网络数据，在释放数字经济发展潜力、促进数字经济加快成长的同时，面临严峻的网络数据安全风险。对于基层而言，以网络数据管理、个人信息保护为基础的管理制度规范尚未完善，基层部门单位开展数据全生命周期管理、数据运营管理、监测预警与应急处置等缺乏指导和参考，网络数据安全体系建设工作缺乏有效落实和严格执行的基础，网络数据安全保障体系建设亟待提升，这要求我们深刻认识网络数据安全的重要性和紧迫性，坚持安全与发展并重，积极应对复杂严峻的安全风险与挑战，加速构建网络数据安全保障体系。近年来，在上级主管部门指导下，连云港市委网信办会同相关职能部门，探索开展网络数据安全监督管理工

作，通过强化顶层设计，构建了“1+5+24”工作体系。组织基础摸排，形成数据资产清单。排查安全风险，掌握重点部门重点行业风险隐患。对10家重点单位开展网络数据安全风险评估，组织对8款重点APP合规检测通报。制定相应管理制度，规范指导网络数据安全管理工作。在实践中总结了一些方法，积累了部分经验，也发现了些许不足，在此基础上，为便于今后的工作开展，急需出台一套网络数据安全管理工作规范，对连云港市网络数据安全工作进行规范管理。

“安全发展、标准先行”，标准化作为当前社会治理和公共服务的重要抓手，标准化工作是保障网络数据安全的重要基础，是规范管理活动、实现科学管理的有效手段。编制《网络数据安全管理工作规范》将不仅梳理建立工作程序及规范，而且明确具体工作要求，强化对网络数据安全管理工作、数据处理活动、网络数据安全运营工作的指导规范，进一步提升网络数据安全整体防护水平，服务和保障连云港市数字经济高质量发展。

二、任务来源

根据市市场监督管理局2023年2月23日《关于公开征集2023年度连云港市地方标准项目的通知》（连标联办发〔2023〕1号）要求，市委网信办报送《网络数据安全管理工作规范》地方标准申请书和标准草案稿。经市市场监督管理局技术初审、立项审查、专家论证，2023年6月28日以《关于下达2023年度第三批连云港市地方标准项目计划的通知》（连市监标函〔2023〕92号），正式批准《网络数据安全管理工作规范》立项。

三、编制过程

（一）项目参与单位

《网络数据安全规范》归口单位是中共连云港市委网信办。

参编单位有：中共连云港市委网信办、连云港市政务服务管理办公室、连云港市大数据管理中心、连云港市人力资源和社会保障局、连云港市城建控股集团有限公司快页信息技术有限公司、联通数字科技有限公司、凭阑江苏实验室科技有限公司。

（二）主要工作过程

第一阶段（2023年4月至6月）主要任务：成立了标准起草组，确定起草组成员，明确任务分工，制定了标准编制工作方案，确定了标准的技术内容、适用范围和体系框架，编制形成草案初稿，提交上报《网络数据安全规范》地方标准申请书和标准草案稿，并于2023年6月通过市市场监督管理局立项批准。

第二阶段（2023年7月至9月）主要任务：在广泛收集资料和调研的基础上，根据法律法规及标准规范对标准草案中网络数据安全要求内容进一步修改完善，形成《网络数据安全规范》初稿。

第三阶段（2023年10月至11月）主要任务：起草组组织对标准初稿开展讨论修改，经内部讨论修改不断完善。10月20日，组织开展《网络数据安全规范》专家论证会，省相关单位专家对标准提出建议意见，起草组修改完善后形成征求意见稿。

第四阶段（2023年11月至12月）主要任务：11月22日至12月5日以书面形式征求9个县区（功能板块）、28家部门及11名专家意见，收到4位专家反馈意见22条，进一步修改完善

形成《网络数据安全规范》（送审稿）。

四、标准编制原则和确定标准主要内容的依据

（一）编制原则

本文件按 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》编制，标准编制的主要依据如下原则：

1. 科学性。标准编制的目标清晰，具有合理层次结构，力求体现网络数据安全管理的特殊性、发展性，力求要素设定先进合理，坚持一定的前瞻性。

2. 协调性。本文件引用相关技术标准的部分内容，所提出的概念、准则、性能要求与我国现行的法律、法规、政策及相关标准相协调。本文件与国家已经发布的网络安全法、数据安全法、个人信息保护法、数据安全规范系列标准等多项相关法律法规和标准规范相协调。

3. 先进性。通过本文件制定，提出网络数据安全安全管理、数据处理活动、安全运营基本要求，更好地指导开展网络数据安全管理和技术实践，有效提高网络数据安全保护能力。

4. 统一性。标准的问题和术语保持一致。对于同一个概念使用同一个术语，每个选用的术语尽可能只有唯一的含义，标准的不同部分的结构及章节编号尽可能相同。

5. 规范性。标准起草前，确定标准的预计结构和内在关系，尤其考虑内容的划分，遵循现行网络数据安全基础标准的有关条款，并保持协调。

6. 适用性。标准的内容适合于界定范围内的研究对象，并且易于被其他的标准或文件所引用。标准易于被实施，具有良好的

可操作性。

（二）编制依据

1. 范围

本文件规定了网络数据安全安全管理、数据处理活动、安全运营基本要求。本文件适用于网络数据处理者的网络数据安全合规管理，网络数据监管者的监督管理、检查评估工作。

2. 规范性引用和参考文件

标准中所涉及数据、指标、技术内容的确定是根据标准编制单位的技术数据及近年来实践经验积累，并参考了国内外相关文献资料。

GB/T25069—2022 信息安全技术术语

GB/T 31167 信息安全技术 云计算服务安全指南

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 37988 信息安全技术 数据安全能力成熟度模型

GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求

（三）编制框架

本文件编写遵循“统一、协调、简化、优化”标准化原理。在标准的主要结构框架、规范性要素的确定上仔细斟酌。框架结构标准由7章组成，基本框架为范围、规范性引用文件、术语和定义、总体框架和要求、安全管理要求、数据处理活动要求、安全运营要求和监督考核。

五、重大意见分歧的处理依据和结果

标准送审查前，书面形式征求9个县区（功能板块）、28家

部门及 11 名专家意见，共收到 4 家单位及 4 位专家反馈意见 26 条，经讨论研究采纳 15 条，部分采纳 2 条，未采纳 9 条，共收到反馈意见 22 条，在征求意见过程中没有出现重大分歧意见。

六、与相关法律法规和标准的关系

本文件与现行法律、法规，以及现有国家标准、行业标准无冲突和矛盾。

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》的规定编制。标准的部分内容与现行有效的标准保持一致，引用标准中标注年份的，则以该标准为依据；没有标注年份的，则以该标准的最新版为依据。

七、实施推广建议

（一）适合地域

本标准适用于连云港市域范围，对周边地区具有一定参考价值。

（二）适合领域

（1）适合于网络数据处理者开展网络数据安全管理工作。

（2）适用于网络数据监管者开展监督检查、检查评估。

（三）推广注意事项

本文件为推荐性标准，实际采用时可根据情况扩展或适当调整。

本文件发布后建议监管主管部门、数据处理业务部门通过组织宣贯、培训、网络等多种形式进行学习，加强标准的贯彻落实，并于 1 年内通过部门行业内开展网络数据安全管理工作落地实施推广应用，发挥本文件规范作用。

八、其他应当说明的事项

无其他需要说明的事项。