信阳市深化“放管服效”改革推进审批服务便民化领导小组办公室文件

信“放管服效”组〔2021〕24号

关于印发《信阳市政务数据安全管理暂行办法》的通知

各县、区人民政府，各管理区、开发区，市政府有关部门：

为加强政务数据安全管理，建立健全政务数据安全保障体系，预防政务数据安全事件发生，现将《信阳市数据安全管理暂行办法》印发给你们，请结合实际，认真抓好贯彻落实。

信阳市深化“放管服效”改革推进
审批服务便民化领导小组办公室
2021年8月20日

信阳市政务数据安全管理暂行办法

第一章 总则

第一条 为加强政务数据安全管理，建立健全政务数据安全保障体系，预防政务数据安全事件发生，依据《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》等法律、行政法规制定本办法。

第二条 本办法适用于信阳辖区的非涉密政务数据安全管理。涉及国家秘密的政务数据，按照国家保密法律、法规、制度进行管理和使用。

第三条 本办法所称政务数据，是指行政机关在依法履行职责过程中制作或获取的，以一定形式记录、保存的文件、资料、图表等各类数据，包括行政机关直接或通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的数据资源等。

第四条 本办法所称数据安全管理，是指通过采取必要措施，防范对网络、系统、数据的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络、系统处于稳定可靠运行的状态，保障政务数据的完整性、保密性、可用性。

第五条 本办法所称政务数据安全事件，是指由于各种原因导致政务信息系统出现关键业务中断、系统瘫痪、关键数据丢失或核心数据失窃等现象，给国家安全、社会稳定或公众利益等造成重大影响和严重经济损失的事件。

第六条 政务数据安全采取“主动防御、综合防范”方针，坚持保障政务数据安全与促进应用发展相协调、管理与技术并重的原则，实行统一协调、分级管理、分工负责，与信息化工作同步规划、同步建设、同步实施、同步发展。

第二章 职责与分工

第七条 市级及各县、区人民政府负责加强本辖区内政务数据安全工作的领导，统筹处置政务数据安全事件，对在政务数据安全管理工作中做出突出贡献的单位和个人，按照有关规定给予表彰和奖励。

第八条 市政务服务和大数据管理局负责统筹推进全市政务安全保障体系建设，完善数据安全管理制度和技术支撑能力，指导监督政务数据安全保障工作，对工作开展情况进行年度总结，向市人民政府及有关部门报告处置辖区内各行政机关的政务数据安全事件。

各县、区政务服务和大数据管理局，各管理区、开发区政务服务和大数据管理机构按照职责负责本辖区政务数据安全管理相关工作。

第九条 各行政机关负责本单位的政务数据安全工作，建设和完善政务数据安全保障基础设施，开展政务数据安全等级保护、风险评估、安全自查、安全培训等工作，保护政务数据安全，制定信息安全应急预案，及时报告和处置政务数据安全事件。

第三章 安全管理

第一节 一般要求

第十条 【组织管理】各行政机关的法定代表人或主要负责人是本单位政务数据安全的第一责任人，各行政机关应按照法律法规和相关标准，指定本单位数据安全管理部门，明确数据安全管理岗位和职责。

第十一条 【安全教育培训】各行政机关应当建立政务数据安全培训制度，定期开展政务数据安全意识教育与政务数据设备安全操作培训，对系统建设、运维人员和政务数据安全从业人员进行专项技能培训。

第十二条 【等级保护】各行政机关应当按照国家等级保护制度要求和技术标准开展政务系统定级工作，建设符合要求的政务数据安全保护设施，并将定级结果和备案证明材料报送本级政务大数据主管部门。

第十三条 【数据外包管理】各行政机关应当建立政务数据技术外包服务和远程技术服务安全管理措施。需要外包服务或远程技术服务的，应当与服务提供商签订安全保密协议。

第二节 数据归集安全

第十四条 【数据归集安全】各行政机关归集的数据应确保来源真实有效、合法正当，同时应明确数据共享范围和

用途。市级及各县（市、区）政务大数据主管部门归集的数据应保留原始表，以满足溯源、数据质量核查等需求。

第十五条 【数据源鉴别及记录】各行政机关在政务数据归集过程中，应对不同的数据归集场景定义数据溯源策略和机制，确保管理人员能够追踪其加工和计算数据的原始数据来源。

第十六条 【数据质量管理】各行政机关应建立数据归集过程中的质量管理规则，明确数据质量监控范围及监控方式，并对在线和离线归集到的数据进行监控，实现对异常数据的发现和处理。

第三节 数据传输安全

第十七条 【数据传输安全】各行政机关在数据采集、共享交换、开放等数据传输环节中，应当制定并执行数据安全传输策略和规程，采用安全可信通道或数据加密等安全控制措施，确保传输过程可信、可控。

第十八条 【数据传输校验和变更】各行政机关应对传输数据的完整性进行检测，并提供异常数据的恢复技术方案；数据传输方式和安全策略变更前，需要进行评估和审核。

第四节 数据存储安全

第十九条 【数据存储方式】各行政机关在选择政务数据存储载体时，应选择安全性能、防护级别与数据安全等级相匹配的存储载体，应采用符合国家认定的密码算法对高敏感数据进行加密存储。

第二十条 【数据备份与恢复】各行政机关应建立数据存储冗余策略，明确定义数据复制、备份和恢复的范围、频率、工具、过程、日志记录规范、数据保存时长等；应建立数据复制、数据备份与恢复的定期检查和更新工作程序，确保数据副本或备份数据的有效性。

第二十一条 【数据访问控制】各行政机关应建立数据资源安全访问策略，授予数据使用者为完成工作所需要的最小权限；应采用多种方式对数据资源访问主体的身份进行鉴别；应采用必要的措施使数据使用者的访问和修改等行为具有不可抵赖性。

第五节 数据处理安全

第二十二条 【数据脱敏】各行政机关应建立数据脱敏规范，明确需要脱敏处理的应用场景和处理方法；应提供面向使用者的定制化数据脱敏功能，可基于场景需求自定义脱敏规则；应提供数据脱敏处理过程日志记录，满足数据脱敏处理安全审计要求。

第二十三条 【数据处理环境】各行政机关应采取数据处理日志管理，记录用户数据处理和加工操作，以备后期追溯；应支持对用户数据处理进行审计，确定用户对数据的加工未超出所申请数据使用目的。

第六节 数据使用安全

第二十四条 【数据分析安全】各行政机关应对数据分析结果进行评估，确保衍生数据不超过原始数据的授权范围

和安全使用要求；应对利用多源数据进行大数据分析的过程进行日志记录，以满足对分析结果质量、真实性和合规性的溯源要求；应避免分析结果输出中包含可恢复的个人信息、重要数据等，从而防止个人信息、重要数据等敏感信息的泄漏。

第二十五条 【数据共享开放安全】各行政机关共享开放本部门政务数据，应当遵守保守国家秘密、政府信息公开等法律、法规的规定，并按照数据安全、隐私保护和使用需求等确定本部门政务数据的共享开放范围；应建立规范的数据共享开放审核流程，确保没有超出数据提供者所允许的数据授权使用范围。

市政务服务和大数据管理局应建立数据库表服务、接口服务的安全规范；应制定数据服务安全控制策略，提供对数据服务访问的安全限制和安全控制措施，并对数据服务调的参数进行限制或过滤；应统一收集数据服务调用日志记录，对数据调用情况进行定期审计。

第七节 数据销毁安全

第二十六条 【数据销毁安全】各行政机关应制定数据清理和过期数据销毁策略，对于需要依法销毁的数据，各行政机关应当采取必要措施予以销毁，并对销毁过程进行记录和备案；应提出各类数据销毁场景应采用的销毁手段，明确销毁方式和销毁要求；应建立数据销毁的审批和记录流程，指定人员监督数据销毁操作过程。

第四章 数据分级

第二十七条 根据不同类别政务数据遭篡改、破坏、泄露或非法利用后，可能对国家安全、社会稳定或公众利益等带来的潜在影响，将政务数据分为一级、二级、三级等 3 个级别。

第二十八条 潜在影响符合下列条件之一的数据为三级数据:

（一）易引发特别重大事件，或造成直接经济损失特别巨大;

（二）对经济发展、公众利益、社会秩序乃至国家安全造成严重负面影响，且负面影响难以消除。

第二十九条 潜在影响符合下列条件之一的数据为二级数据:

（一）易引发较大或重大事件，给政府造成较大负面影响，或直接经济损失较大;

（二）引发的级联效应明显，影响范围涉及多个行业、区域或者多个行政机关，或影响持续时间长，或可导致大量个人、企业信息被非法获取;

（三）恢复政务数据或消除负面影响所需付出的代价较大。

第三十条 潜在影响符合下列条件之一的数据为一级数据:

（一）对政务系统及设备的正常运行影响较小；

（二）给政府造成负面影响较小，或直接经济损失较小；

（三）受影响的企业和个人数量较少、区域范围较小、持续时间较短；

（四）恢复政务数据或消除负面影响所需付出的代价较小。

第三十一条 市政务服务和大数据管理局负责制定政务数据分类分级制度规范，指导、协调本级行政机关开展政务数据分类分级工作。各县、区政务服务和大数据管理局，各管理区、开发区政务服务和大数据管理机构负责指导和推动本辖区内政务数据分类分级工作。

第三十二条 各行政机关应按照政务数据分级情况，做好防护工作。针对三级数据采取的防护措施，应能抵御来自国家级敌对组织的大规模恶意攻击；针对二级数据采取的防护措施，应能抵御大规模、较强恶意攻击；针对一级数据采取的防护措施，应能抵御一般恶意攻击。

第三十三条 各行政机关在做好数据安全管理的前提下适当共享开放一、二级数据，充分释放政务数据的潜在价值。二级数据只对确需获取该级数据的授权部门共享开放。三级数据原则上不对社会开放，且需严格控制授权部门共享知悉范围。

第五章 监督检查和事件处置

第三十四条 政务大数据主管部门可以委托第三方专业机构对本辖区政务数据安全开展调查评估，各行政机关对发现的问题应当及时整改。

第三十五条 各行政机关应设立或指定工作机构，负责政务数据安全事件应急处置工作；应制定政务数据安全事件应急处置预案，定期开展应急演练，并对演练情况进行评估，补充修订应急预案。

第三十六条 各行政机关政务数据出现泄漏、毁损、丢失等情形，或者存在数据安全风险时，应当立即采取补救措施，并按照规定向本级政务大数据主管部门和网信部门报告，并于应急工作结束后 15 日内补充上报事件处置情况。

第七章 附则

第三十七条 法律、法规授权的具有公共事务管理职能的事业单位和社会组织的政务数据安全管理工作，执行本办法。

供水、供电、燃气、通信、民航、铁路、道路客运等公用事业运营单位在依法履行公共管理和服务职责过程中采集和产生的各类数据资源的安全管理，参照本办法。法律、法规另有规定的，依照其规定。

第三十八条 本办法自发布之日起施行。