南京市数字政府建设工作领导小组办公室

宁数政办发〔2024〕2号

关于印发《南京市政务数据安全管理实施细则》的通知

市数字政府建设工作领导小组各成员单位：

为贯彻落实国家和省数据安全相关工作要求，进一步推进南京市政务数据安全管理工作，经研究现将《南京市政务数据安全管理实施细则》印发给你们，请认真抓好落实。

南京市数字政府建设工作领导小组办公室

2024年6月12日

南京市政务数据安全管理实施细则

第一章 总则

第一条 为深入践行总体国家安全观，进一步规范我市政务数据处理活动（收集、存储、使用、加工、传输、提供、公开和销毁等），保障政务信息系统和政务数据安全，依据有关法律法规和有关规定，结合本市实际，制定本细则。

第二条 本市各级行政机关、事业单位、社会团体或者其他依法经授权、受委托的具有管理公共事务职能的组织（以下简称各部门）的非涉密政务数据处理活动，适用本细则。

第三条 本细则所称政务数据，是指各部门在履行职责过程中产生或者获取的具有原始性、可机器读取、可供社会化再利用的各类数据。

第四条 市委国安委统一领导全市数据安全管理工作，统筹协调推进我市数据安全重大事项和重要工作。市数据局统筹全市政务数据安全保障体系建设，负责全市政务数据安全的组织推进及监督管理工作。市委网信办、市发改委、市工信局、市公安局、市国安局在各自职责范围内承担政务数据安全管理职责。

第五条 各部门对本单位建设、运营和维护的政务信息系统及产生的政务数据安全承担主体责任。各部门主要负责人为本部门政务数据安全第一责任人，分管政务数据安全工作的班子成员为直接责任人。政务数据安全第一责任人每年至少召集一次会议，

组织听取政务数据安全工作整体情况汇报，研究议定重大事项和重要举措。政务数据安全直接责任人定期研究政务数据安全工作或者专题听取阶段性工作汇报。

各部门应当通过文件或者会议纪要等方式完善本单位政务数据安全管理组织架构，明确相关处室、人员具体负责政务数据安全工作。人员发生变化时，应当及时调整更新并报送市数据局备案。

明确本单位各政务信息系统责任人（一般为建设政务信息系统的处室负责人）和具体经办人（一般为政务信息系统项目负责人），建立政务信息系统的数据安全管理架构，制定制度规范，开展安全培训，督促落实政务数据安全要求，组织处置安全事件。

明确一名本单位正式人员负责政务数据安全监督和检查工作，对安全管理制度和标准提出完善和优化建议，督促安全隐患整改。数据安全监检人员原则上不得兼任政务信息系统的数据责任人等角色。

第二章 管理要求

第六条 各部门应当统筹规划本单位政务数据安全工作，将政务数据安全工作列入本单位年度工作要点或者年度重点工作，以工作计划、工作要点、任务清单等形式，分解任务压实责任。

各部门应当依据法律法规、行业标准和上级主管部门的政务数据安全管理要求，建立健全本单位管理制度，包括数据分类分

级、访问控制、风险评估、监测预警、应急处置、数据全生命周期管控、服务外包管理等内容。

各部门应当结合本单位行业要求、特点和政务信息系统建设情况等，制定具体的防护要求和操作规程。

第七条 按照《南京市政务云管理办法》要求，市城市数字治理中心负责市政务云的建设、管理、运行维护和安全保障。各部门新建网络安全等级保护三级及以下非涉密政务信息系统，原则上应当使用市政务云资源。各部门已建网络安全等级保护三级及以下非涉密政务信息系统应当逐步迁移上云。各部门应当做好上云政务信息系统及自行部署的中间件、数据库、政务信息系统的安全管理工作，接受市政务云的安全监管。

使用自建云资源的部门，应当参照《南京市政务云管理办法》相关要求，负责自建云及云上政务信息系统的数据安全管理工作，应当采购通过安全评估的云服务。

第八条 各部门处理个人信息应当遵循合法、正当、必要、诚信、公开、透明的原则，依据相关法律法规和有关文件，采用符合个人信息保护法律法规和政策的安全管理措施。

各部门收集个人信息应当在隐私政策协议或者合同协议中，以显著方式、清晰易懂的语言真实、准确、完整地向个人说明收集信息的目的、范围、方式、种类、存储期限等，充分保障个人信息主体权益。

各部门政务信息系统应当按照个人信息主体同意授权的方式，在授权范围内最小化使用个人信息，批量修改、拷贝、下载等重要操作应当设置内部审批流程，敏感个人信息处理应当采取加密、脱敏、去标识化等安全防护措施，按照国家相关要求使用经检测认证合格的商用密码产品、服务进行保护。

各部门委托第三方进行个人信息处理的，应当签署委托合同，约定处理的目的、期限、方式、个人信息的种类、保护措施以及双方的权利和义务等，并对信息处理活动进行监督。

第九条 各部门对本单位服务外包活动的政务数据安全负主体责任，应当按照国家、省和市有关要求，加强对服务外包方参与本单位政务信息系统建设、运营、维护过程的安全监管。

在选择服务外包方时，应当充分考虑规模能力、安全资质、安全团队、承诺践诺能力等。近三年因违反网络和数据安全相关法律法规，受到行政处罚或者刑事处罚的企业、个人，应当依法限制参与外包活动。

涉及核心数据、重要数据或者一百万人以上个人信息的政务信息系统，基础设施、应用系统、安全防护等建设内容原则上不得由同一服务外包方全部承建。提供政务数据安全相关服务的外包方，不得与系统建设方为同一企业，不得与系统建设方存在直接控制、间接控制或者重大影响的关系。

各部门应当明确服务外包方的数据安全责任。在编制采购文件、签订合同时，应当要求服务外包方严格履行政务数据安全相

关法律法规、制度要求，约定服务外包方的政务数据安全责任与违约责罚内容。对于参与政务信息化项目的服务外包人员，应当要求具备相关从业资质，并签署保密承诺书，明确保密范围、保密责任、违约责任、有效期限等内容，涉及核心数据、重要数据或者一百万人以上个人信息的政务信息系统，应当要求提供人员背景审查结果。

各部门应当要求服务外包方加强日常管理。服务外包方应当明确数据安全责任人，定期开展教育培训，制定政务数据安全事件应急预案，建立应急响应机制，配合开展应急演练。各部门应当常态化评估服务外包方的政务数据安全工作情况，加强访问权限管理，定期开展动态风险评估，及时排查潜在安全风险。评估内容包括管理制度建立和执行情况、技术措施使用情况等。对于评估中发现的问题应当记录到问题清单，并限期整改形成闭环。已发生安全问题的，应当严肃追究责任。

服务外包活动中收集、产生的政务数据由各部门负责管理，数据管理权不向服务外包方迁移。服务外包方应当在委托部门授权范围内开展政务数据处理活动，授权期满后及时移交或者回收权限。未经委托部门同意，不得变更政务数据用途、用法，不得擅自留存、使用、泄露或者向他人提供，不得擅自用于商业用途。

第十条 市数据局组织全市政务数据安全培训与宣传工作，指导各部门制定培训计划并监督培训实施。各部门应当制定本单位政务数据安全年度培训计划，组织开展知识讲座与教育培训。

各部门每年应当至少开展一次全员政务数据安全培训，培训内容应当包括政务数据安全相关法律法规、标准规范、管理制度、操作流程等。各部门每年应当至少开展一次针对政务数据安全岗位人员的数据安全专题培训，培训内容应当包括数据安全管理、数据安全技术、数据安全运营、数据安全合规等。

第十一条 市数据局构建全市统一的用户管理和身份认证中心，对接省级身份认证系统，实现用户统一身份认证。各部门原则上依托市统一身份认证中心构建政务信息系统，明确专人负责用户账户及权限管理，不得委托第三方实施。

各部门应当根据数据访问权限管理有关要求，落实本单位账号管理、口令管理和权限管理等工作，定期进行账号稽核，发生人员变动、项目建设需求变化等情况时应当及时调整权限或者收回账号。

第十二条 市数据局利用技术手段建立全市政务数据安全监测预警能力，对全市重要政务信息系统进行常态化监测分析。各部门应当建立健全本单位风险监测预警与应急处置机制。

各部门负责做好本单位政务信息系统的日常安全监测工作，定期开展系统漏洞扫描、渗透测试、系统加固，开展云主机操作系统、中间件、数据库的补丁升级、病毒库升级等安全工作，对发现的问题和漏洞及时整改修复。各部门负责制定并完善本单位政务数据安全应急预案，或者在本单位总体应急预案中包括政务数据安全内容。各部门每年至少开展一次应急演练，应急演练场

景应当包括数据泄漏（丢失）、滥用、违规使用等。发生安全事件时，应当及时启动应急预案并做好处置工作，并在5个工作日内形成书面报告报送市委网信办和市数据局备案。紧急情况可以先电话联系，后补书面报告。

第十三条 涉及核心数据、重要数据或者一百万人以上个人信息的政务信息系统，各部门应当根据《江苏省数据安全风险评估规范》等相关文件要求，每年组织开展一次风险评估工作并形成评估报告，每年11月底前报送市委网信办和市数据局备案。

政务数据安全风险评估工作应当重点评估安全管理是否到位、安全防护措施是否有效、数据处理活动是否合规、个人信息保护要求是否落实。评估报告应当包括数据的描述、种类、开展数据处理活动情况、数据识别、安全威胁与分析、数据脆弱性分析、数据安全措施确认、安全风险分析和风险控制建议等。

第十四条 各部门应当根据政务数据日志审计管理有关要求，做好本单位政务信息系统的日志收集、存储、识别和综合分析工作，及时排查政务数据安全风险，并采取处置措施。

涉及核心数据、重要数据或者一百万人以上个人信息的政务信息系统，各部门应当每年至少组织两次政务数据安全日志检查，并主动接受市级政务云数据安全审计，针对审计发现的问题应当及时整改。

第三章 数据分类分级管理

第十五条 各部门应当对本单位建设、运营和维护的政务信息系统和政务数据情况进行全面梳理，形成本单位政务信息系统和政务数据资源目录并通过市政务数据共享交换平台报送市数据局备案。目录发生变化的，应当及时更新报送。

第十六条 市数据局会同有关主管部门，按照国家、省分类分级标准规范，依托市政务数据共享交换平台，推动本市政务数据分类分级管理工作。

各部门应当按照国家、省数据分类分级标准规范，在本单位政务数据资源目录基础上，开展本单位政务数据分类分级工作。

工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门应当按照国家、省和行业领域标准，结合本行业、本领域业务特点，开展本行业、本领域数据分类分级工作，并明确相应的监管防护措施。

第十七条 数据分级管控应当按照就高从严原则，根据数据集中数据项的最高级别确定安全保护措施，存在数据属性动态变化或者多项数据共同影响数据分级的，应当充分考虑各项数据关联关系，综合确定保护措施，并根据业务变化情况动态更新。

各部门应当按照数据分类分级管控有关要求，根据本单位数据分类分级情况，对不同级别的数据制定相应的数据安全管控和保护策略。

各部门应当将数据分级管控贯穿数据全生命周期，确保数据在各项处理活动中持续处于有效保护和合法利用的状态。应当对

核心数据、重要数据实行重点保护，按要求定期组织开展目录备案、风险评估、日志审计等活动。

第四章 数据全生命周期管理

第十八条 各部门在收集政务数据时，应当明确收集目的、用途和范围，遵循合法、必要、正当和诚信原则。

在政务数据收集前应当明确收集来源、方式、范围、数量、频度、有效期限等。个人信息主体为未满14周岁的未成年人，应当征得监护人的明示同意。在政务数据收集中应当加强流程管控，规范政务数据收集的方式方法，并留存授权收集过程信息，定期进行检查。加强对收集设备认证鉴权，采取技术手段对收集的数据进行校验和加密，保证数据的完整性、一致性和安全性。

第十九条 各部门应当建立本单位政务数据存储安全管理机制，按照数据分类分级管理要求，执行政务数据存储策略，明确数据存储位置、存储时长、操作流程、访问要求等内容，对存储环境、平台系统采取必要的安全保护措施，定期开展数据备份。存储核心数据、重要数据或者一百万人以上个人信息的，应当采用校验技术、密码技术等措施进行安全存储，保证政务数据存储的完整性、机密性。

第二十条 各部门在开展政务数据使用或者加工活动时，应当采取安全保护措施，确保政务数据使用或者加工全程合法合规、安全可控。

在政务数据使用或者加工前，应当履行审批程序，明确使用或者加工的目的、操作人员、获取方式、权限范围等内容。在政务数据使用或者加工过程中，应当采取安全措施并对政务数据使用或者加工过程进行记录，对政务数据本地下载等敏感操作进行监控，留存相关信息，并定期进行检查，确保政务数据使用或者加工过程中数据不泄漏。在政务信息系统开发、测试、演示等场景中，应当事先对敏感数据进行脱敏处理或者使用模拟数据。

第二十一条 各部门应当根据传输的数据类型、级别和应用场景，采用相应的传输安全措施（安全通道、可信通道、数据加密、双向身份认证、冗余链路等），确保政务数据传输的安全性、可靠性、可用性。传输核心数据、重要数据或者一百万人以上个人信息的，应当采取数据加密和通道加密的组合方式。

在政务数据传输前应当明确双方的身份认证方式、接入方式等，进行身份鉴别和授权处理，设置访问控制规则，依据权限合理传输数据。在政务数据传输中应当记录传输内容和传输过程，并按照规定留存相关的网络日志不少于6个月，定期进行检查。

第二十二条 各部门应当建立本单位政务数据共享目录和开放目录，明确数据共享开放范围，并及时调整更新。有条件共享和开放的政务数据，应当对数据使用申请进行严格审批和授权，明确数据共享开放的目的、申请方、范围、期限、频次等内容。核心数据、重要数据或者一百万人以上个人信息的共享，应当事前开展数据风险评估，并制定约束机制。

政务数据共享开放应当依托市政务数据共享交换平台和开放平台实施，数据提供方和使用方应当约定数据共享开放的范围、使用用途、方式等，明确双方的数据安全责任。应当建立可靠的数据共享开放通道，对政务数据共享开放过程进行监测和记录，并留存相关信息。

第二十三条 各部门应当建立本单位政务数据销毁和存储介质销毁审批机制，明确销毁对象、原因、流程、技术方式，记录并留存销毁活动信息。核心数据、重要数据或者一百万人以上个人信息应当采取不可逆的方式进行销毁处理，防止数据恢复。按照法律规定、合同约定等申请销毁的，应当及时销毁对应政务数据。

第五章 安全监督检查

第二十四条 按照“谁管业务、谁管数据、谁管数据安全”的原则，各行业领域主管部门应当对本行业领域的政务数据安全负指导监管责任。各主管部门应当加强协作配合，推进政务数据跨部门协同监管。

第二十五条 市数据局制定政务数据安全监督检查年度工作计划和实施方案，会同市委网信办、市公安局等部门组织开展政务数据安全监督检查工作。检查工作以查阅资料、查看系统、技术监测、人员访谈等方式开展。检查内容包括但不限于组织架构、制度建设、教育培训、个人信息保护、数据分类分级、数据全生

命周期管理、服务外包管理等。

市数据局牵头对监督检查发现的问题形成问题清单，通知责任方限期整改，并跟踪检查整改成效。各部门应当积极配合市数据局开展政务数据安全监测、检查、审计等监督管理工作，对检查发现的问题及时整改。

第二十六条 市数据局根据政务数据安全监督检查结果对各部门政务数据安全工作进行综合考核评估。重点考核评估各部门政务数据安全日常管理及安全问题整改落实等情况，相关结果纳入全市数字政府绩效考核。

第六章 附则

第二十七条 涉及国家秘密的数据安全管理、数据出境安全管理、国家和省统一建设或者下发的政务信息系统，按照有关法律、法规、规章和文件规定执行。本细则自印发之日起施行。

南京市数字政府建设工作领导小组办公室　　2024年6月11日印发