郑州市人民政府
关于印发郑州市政务数据安全管理实施细则的通知

郑政〔2023〕7号

各开发区管委会，各区县（市）人民政府，市人民政府各部门，各有关单位:

现将《郑州市政务数据安全管理实施细则》印发给你们，请认真贯彻执行。

郑州市人民政府

2023年3月2日

郑州市政务数据安全管理实施细则

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，根据《中华人民共和国保守国家秘密法》《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》《中华人民共和国密码法》《关键信息基础设施安全保护条例》《河南省政务数据安全管理暂行办法》《郑州市政府信息资源共享管理办法》等法律、法规和有关规定，结合本市实际，制定本细则。

第二条　本细则所称政务部门是指我市各级行政机关及法律、法规授权具有公共事务管理职能的组织。

政务数据是指任何以电子或者其他方式对政务相关信息的记录。

政务数据安全是指通过采取必要措施，确保政务数据处于有效保护和合法利用状态，以及具备保障持续安全状态的能力。

政务信息系统是由政务部门建设、运行或使用的，用于直接支持政务部门工作或履行其职能的各类信息系统。

第三条　本细则适用于我市各级政务部门的非涉密政务数

据收集、存储、传输、共享、开放、使用、销毁等行为及相关管理工作。涉及国家秘密和工作秘密的政务数据，按照相关法律、法规、规章、标准执行。

第四条 政务数据安全管理要全面贯彻落实总体国家安全观。采取积极防御、综合防范；统一协调、统筹规划；分级管理、分工负责的方针，坚持安全与发展并重，管理与技术统筹兼顾。

第五条 实行政务数据安全责任制，按照“谁主管谁负责、谁运行谁负责、谁使用谁负责”的原则，保障政务数据全生命周期安全。基于复制、流通、交换等同时存在多个政务数据安全责任人的，分别承担各自安全责任。

第二章 职责分工

第六条 网信部门负责统筹协调、检查指导和相关监督管理等工作。公安、保密、国家安全、密码管理、通信管理等部门按照本细则和有关法律、法规、规章的规定，在各自职责范围内承担政务数据安全监管职责。

第七条 市大数据管理机构作为我市政务数据主管部门，负责组织、指导和协调本级政务数据安全管理工作，履行下列职责：

（一）依照国家、省、市政务数据安全法律、法规、规章和标准，编制政务数据安全发展总体规划，制定政务数据安全标准，建立考核评价制度，指导各政务部门开展政务数据安全工作；

（二）健全完善政务数据分类分级安全管理制度，制定政务数据分类分级指南，为政务数据安全管理和安全资源配置提供指导;

（三）组织建设和完善政务数据安全保障基础设施，建立政务数据安全管理与测评机制，健全数据安全专家队伍;

（四）负责组织政务数据安全培训，提升政务数据安全保障能力;

（五）会同网信、公安部门，按照各自职责分工对政务部门进行政务数据安全检查,对发现的问题提出指导建议并督促整改;

（六）完成上级交办的其他政务数据安全工作，指导下级政务数据主管部门开展政务数据安全工作;

（七）法律、法规、规章规定的其他职责。

第八条 区县（市）政务数据主管部门按照职责开展政务数据安全管理工作，会同本级网信、公安部门开展政务数据安全检查，建立政务数据安全监测预警、信息通报和应急处置机制等。

第九条 政务部门负责本部门的政务数据安全工作，履行下列职责:

（一）执行国家、省、市政务数据安全法律、法规、规章和标准，履行数据安全保护义务，明确政务数据安全负责人和管理机构，落实政务数据安全责任制;

（二）制定政务数据安全计划，实施数据安全防护技术措施，开展政务数据处理活动风险评估，有效应对政务数据安全事件，

防范违法犯罪活动;

（三）制定政务数据安全事件应急预案，定期开展应急演练;

（四）建立政务数据安全培训制度，定期组织开展政务数据安全培训;

（五）承担其他法律、法规、规章要求的政务数据安全工作。

第十条 各级财政部门应当加强本级政务数据安全经费保障，确保政务数据安全运行。

第三章 建设与运行

第十一条 政务部门建设政务信息系统应当严格遵守有关法律、法规、标准规范，同步编制政务数据安全建设方案，同步建设政务数据安全防护系统，同步开展政务数据安全运行工作，定期评估，不断提高政务数据安全防护水平。

第十二条 政务部门应当编制政务信息系统和政务数据资源清单，明确管理责任机构与人员，定期按照清单对政务信息系统和政务数据资源进行一致性检查，并保留检查记录。

第十三条 政务部门应当依法确定政务信息系统建设、运维、运营等单位。建设、维护政务信息系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督建设、运维、运营等单位履行相应的数据安全保护义务。

建设、运维、运营单位应当依照法律、法规的规定和合同约

定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

第十四条 政务部门应当依据“谁建设谁负责、谁主管谁督促、谁使用谁要求”的原则，建立机房管理制度，保障机房的物理环境安全。

第十五条 政务部门应当进行必要的安全性评估工作，加强对服务器上的应用、服务、端口的安全管理，定期实施漏洞扫描、恶意代码检测，及时升级系统安全补丁，完善密码防护系统。

第十六条 政务部门应当采取集中管控、用户识别、访问控制、安全审计等技术防护措施，严格落实终端计算机的安全管理。

第十七条 政务部门应当明确收集数据的目的、依据、范围和用途，确保数据收集的合法性、正当性、必要性和业务关联性。对数据收集的环境、设施和技术采取必要的防护措施，确保数据的完整性、一致性和真实性。对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应依法予以保密，不得泄露或者向他人非法提供。

第十八条 政务部门应当选择安全性能、防护级别与数据安全等级相匹配的存储载体，严格管控移动存储介质的使用，防止移动存储介质在不同网络区域之间交叉使用造成恶意代码的传播和数据泄露。

政务部门应当制定政务数据备份和恢复策略，落实相关灾备措施，定期进行灾难恢复演练。

第十九条 政务部门应当对涉及工作秘密的数据采取脱敏、加密等处理措施，严格落实政务数据的安全处理机制。

第二十条 政务部门应当制定并执行数据安全传输策略，采用安全可信通道或数据加密等安全防控措施,确保传输过程可信、可控。对关键传输链路、重要设备节点实行冗余配置，保障数据传输可靠性和网络传输服务可用性。

第二十一条 政务部门应当坚持“共享为原则、不共享为例外”的原则，采取加密、脱敏、备份、审计等措施妥善保护政务数据。政务数据使用单位对于共享的政务数据须落实同等数据安全管理责任。

第二十二条 政务部门使用政务数据应当签订安全保护协议，明确数据使用的依据、目的、范围、方式及相关需求，获得的政务数据未经授权不得提供给第三方,不得擅自用于其他场景。

第二十三条 政务部门应当履行数据安全审查职责，遵循需求导向、分类分级、公平公正、安全可控、统一标准、便捷高效的原则，按照规定及时、准确地开放政务数据。

第二十四条 政务部门应当制定数据清理和数据销毁制度，建立数据清理、数据销毁的审批和记录流程，对数据清理和数据销毁过程进行备案，确保全过程可审计。

第二十五条 政务部门应当遵循统一的政务数据分类分级规则，配套差异化的安全控制措施，实现对政务数据的分类分级保护。

第二十六条 政务部门为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。

第二十七条 政务部门在中华人民共和国境内收集和产生的重要数据应当在境内存储，确需向境外提供的，应当按照相应的规定进行安全评估，确保数据出境安全。

第二十八条 政务部门应当落实网络安全等级保护、商用密码应用等要求，定期开展政务信息系统网络安全等级保护和商用密码应用安全性评估工作。

第二十九条 政务部门可委托具有资质的第三方机构，按照规定对政务数据处理活动开展风险评估,对发现的问题及时整改。

第三十条 市、区县（市）政务数据主管部门应当建立数据安全风险评估、报告、信息共享、监测预警机制，加强本地区数据安全风险信息的获取、分析、研判、预警工作。

第三十一条 市、区县（市）政务数据主管部门应当对政务数据的全生命周期建立数据安全溯源机制，发现安全问题，快速定位，及时解决。

第三十二条 市、区县（市）政务数据主管部门应当定期开展政务数据安全意识教育与政务数据安全操作基础培训，对系统建设、运维人员和政务数据安全从业人员进行针对性专项技能培训。

第四章　安全检查与应急处理

第三十三条　市、区县（市）政务数据主管部门会同本级网信、公安部门建立政务数据安全检查制度，对政务数据应用的安全性、合规性进行检查；政务部门应当配合检查，对检查中发现的问题及时整改。

第三十四条　市政务数据主管部门会同网信、公安等部门建立应急协调机制，负责全市重大政务数据安全事件处置的组织、指挥和协调。政务部门应按照本级政务数据主管部门和上级业务主管部门要求，建立政务数据安全应急管理机制，明确应急工作机构、事件上报流程及应急处置措施。

第三十五条　政务数据出现下列情形之一时，政务部门应当立即启动应急预案，采取补救措施，并及时报送同级网信、公安、政务数据主管等部门：

（一）发现重大网络安全隐患、漏洞或关键设备节点、重要系统受到攻击遭到破坏的；

（二）公民、法人或者其他组织信息泄露、毁损、丢失，造成重大影响或经济损失；

（三）行政机关及事业单位等网站数据被篡改；

（四）国家、省、市政务数据安全主管部门通报的事件；

（五）其他发生的政务数据安全事件。

第五章　责任追究

第三十六条　政务部门违反本细则，有下列行为之一的，由有关主管部门责令改正，并依法追究相应责任:

（一）未采取数据分类分级保护措施的;

（二）未履行个人信息保护义务的;

（三）违规向境外提供数据的;

（四）未落实网络安全等级保护和商用密码应用安全性评估工作要求的;

（五）拒绝、阻碍安全检查和未按要求进行整改的。

第三十七条　公职人员违反本细则，有下列行为之一的，由有关主管部门根据情节轻重依法给予相应的处理，构成犯罪的，依法追究刑事责任:

（一）不履行或者不正确履行职责，玩忽职守，贻误政务数据安全管理工作的;

（二）泄露政务数据，或者泄露因履行职责掌握的公民、法人或者其他组织信息的;

（三）处置政务数据安全事件，存在瞒报、缓报、谎报、迟报和推诿责任行为的;

（四）拒不提供必要的支持与协助，干扰事件调查的。

第三十八条　违反本细则规定的，按照有关法律、法规、规章处理。侵害公民、法人或者其他组织合法权益的，依法承担民

事责任。构成犯罪的，依法追究刑事责任。

第六章　附　则

第三十九条　本细则自公布之日起施行，原《郑州市人民政府关于印发郑州市政务数据安全管理暂行办法的通知》（郑政〔2020〕22号）同时废止。