# 晋城市人民政府办公室文件

晋市政办〔2024〕4号

## 晋城市人民政府办公室<br>关于印发晋城市政务数据安全管理<br>实施细则的通知

各县（市、区）人民政府、开发区管委会，市人民政府各委、办、局:

《晋城市政务数据安全管理实施细则》已经市人民政府同意，现印发给你们，请认真贯彻执行。

晋城市人民政府办公室

2024年1月29日

（此件公开发布）

# 晋城市政务数据安全管理实施细则

## 第一章　总　则

**第一条**　为加强全市政务数据安全管理，建立健全政务数据安全保障体系，根据《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》《中华人民共和国密码法》《山西省政务数据安全管理办法》等法律法规和有关规定，结合我市实际，制定本细则。

**第二条**　本细则适用于本市行政区域内非涉密政务数据进行收集、存储、使用、加工、传输、提供、公开和销毁等处理活动，以及政务数据安全保护和监督管理的工作。涉及国家秘密和工作秘密的，按照有关法律、法规规定执行。

**第三条**　本细则所称政务部门是指各级人民政府、县级以上人民政府所属部门、列入党群工作机构序列但依法承担行政职能的部门以及法律、法规授权的具有公共管理和服务职能的组织。

本细则所称政务数据是指政务部门在履行职责过程中收集、产生和管理的各类信息资源，包括直接或通过第三方依法授权管理和因履行职责需要形成的文字、数字、符号、图片和音视频等数据。

本细则所称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，保障政务数据全生命周期处于安全可控状态。政务信息系统是由政务部门建设、管理或使用的，用于支持政务部门履职的各类信息系统。

**第四条** 政务数据安全管理遵循“谁提供、谁负责，谁流转、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。

**第五条** 各级各部门对本单位的政务数据安全负有主体责任，主要负责人是政务数据安全的第一责任人，各级政务数据管理部门负有监督管理责任。

## 第二章 职责与分工

**第六条** 网信部门统筹协调政务网络数据安全和相关监管工作。公安机关履行网络安全等级保护和政务数据安全等工作的监督、检查、指导职责。国家安全机关负责统筹协调涉及国家安全工作的相关政务数据安全监管工作，防范和打击危害国家安全的违法犯罪活动。

保密、密码等主管部门按照各自职责，做好政务数据安全管理相关工作。各行业主管部门负责本行业、本领域数据安全监管。

**第七条** 市政务数据管理部门负责组织、指导和协调全市政务数据安全管理工作，履行下列职责：

（一）依照国家、省有关法律、法规和标准，制定政务数据

安全相关政策和工作制度，指导、协调和监督各级各部门开展政务数据安全工作；

（二）建设政务数据安全保障基础设施和政务数据安全平台，构建一体化政务数据安全管理与防护体系；

（三）会同网信、公安等部门组织开展政务数据安全检查、风险评估、安全培训和应急演练等工作；

（四）会同网信、公安等部门建立政务数据安全监测预警、信息通报和应急处置等机制，通报政务数据安全信息，调查处理政务数据安全事件；

（五）完成上级交办的其他政务数据安全工作。

**第八条** 各县（市、区）政务数据管理部门，负责制定辖区内政务数据安全工作制度，建立政务数据安全事件应急机制、数据安全通报机制，组织协调有关单位开展政务数据安全保障、政务数据安全培训和应急演练工作，会同本级网信、公安等部门开展政务数据安全检查等工作。

**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）贯彻落实国家、省、市政务数据安全法律、法规和标准，明确本部门负责政务数据安全管理工作的机构及责任人，制定政务数据安全管理工作制度；

（二）做好本部门所申请政务云服务的安全管理工作，维护好相关信息系统和政务数据的安全，定期开展政务数据安全风险

评估和安全检查;

（三）制定政务数据安全事件应急预案，定期开展应急演练，配合有关部门进行政务数据安全检查和事件调查，对存在的问题及时整改;

（四）定期组织开展政务数据安全教育培训，提升数据安全相关人员管理能力;

（五）保障政务数据安全相关经费，将政务数据安全建设和人员培训经费纳入本部门年度预算。

## 第三章　数据安全管理

**第十条**　政务部门建设政务信息系统依照有关法律、法规、规章及相关标准，同步编制政务信息系统安全建设方案、密码应用方案，同步建设政务信息系统安全防护系统，同步开展政务信息系统安全运行保障工作。

政务信息系统建设应当优先采用符合国家规定、安全可控的信息技术和产品，使用符合国家密码管理要求的技术、产品和服务。

**第十一条**　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等级保护测评、密码应用安全性评估和政务数据安全风险评估，定期开展漏洞扫描、恶意代码检测，及时升级安全补丁，完善密码防护措施。

**第十二条** 政务部门委托政务信息系统建设、运维、运营单位开展政务数据处理活动，应当严格管理实施过程，履行相关审批程序，监督其履行相应的数据安全保护义务。

**第十三条** 政务部门应当加强政务信息系统的权限管理，建立严格的授权访问机制，政务信息系统、数据库、机房等的最高管理权限必须由专人负责，不得擅自委托建设、运维、运营等单位人员管理使用。

**第十四条** 政务部门应当建立信息系统安全防护管理体系，加强对服务器上的应用、服务、端口等的安全管理，系统账号按照“最小权限”原则进行分权管理，建立和完善密码保障体系，提升密码安全防护能力。

建立政务信息系统接入审查机制，在接入电子政务外网前应对接入方案进行审核、风险扫描和安全评估，确认达到政务数据安全要求并签订安全协议后方可授权接入电子政务外网。

建立政务信息系统部署审查机制，政务信息系统应当完成安全评估后方可上线运行。

**第十五条** 政务信息系统的建设模式、部署方式、运维形式发生调整变化后，政务部门的数据安全主体责任不变，管理标准不变。

**第十六条** 政务部门应当遵循统一的政务数据分类分级规则，对政务数据进行保护。

**第十七条** 政务部门应当建立日志审计机制，明确安全审计

日志收集的内容、方式、存储和标准化等要求，及时处置数据安全问题。

**第十八条** 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，涉及政务数据出境的，应当遵守有关法律法规规定。

**第十九条** 政务部门可以委托具有资质的第三方机构，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。

**第二十条** 建设、运维、运营等单位应当依照法律法规规定和合同约定履行数据安全保护义务，不得擅自留存、访问、修改、使用、泄露、销毁或向他人提供政务数据。

## 第四章 数据全生命周期管理

**第二十一条** 政务部门应当建立政务数据资源全生命周期安全防护体系，制定政务数据收集、存储、使用、传输、共享、销毁等制度及规范，加强身份与权限管理、数据保护与审计，利用数据防泄漏、数据加密、数据脱敏、数据恢复等技术，保障政务数据全生命周期安全。

**第二十二条** 数据收集。政务部门应当遵循“一数一源”的原则，明确收集政务数据的目的、用途、方式、频率和范围等，确保政务数据收集的完整性、准确性、时效性；可通过共享交换平台获取的政务数据资源，不再重复收集。

**第二十三条** 数据存储。政务部门应当选择与政务数据分类分级保护要求相匹配的存储载体，对数据进行加密存储。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。制定政务数据备份和恢复策略，落实相关灾备措施。

**第二十四条** 数据使用。政务部门应当明确数据使用的依据、目的、范围、方式、场景及相关责任，确保数据使用过程合规、可控、可追溯。使用其他部门的政务数据，原则上应当通过政务数据共享交换平台，落实同等数据安全管理责任，未经授权不得提供给第三方，不得擅自用于其他场景。

**第二十五条** 数据加工。政务部门应当采用数据加密、脱敏、隐私计算等技术手段，确保数据不外泄，不得超出数据授权的许可范围和限制条件，不得将结果数据或产品用于其他用途。

**第二十六条** 数据传输。政务部门应当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。对关键传输链路、重要设备节点采取冗余措施，保障数据传输可靠性和网络传输服务可用性。

**第二十七条** 数据提供。政务部门应当明确数据授权使用的主体、用途、方式、范围、期限、应用场景、安全保护措施和责任义务等，与使用单位签订数据安全协议，按照分类分级要求对政务数据进行内部审查。对涉密、涉敏数据应当进行安全评估，脱密、脱敏后再提供。

**第二十八条** 数据公开。政务部门应当编制可开放的政务数据目录,明确公开数据的内容、类型、公开方式、公开范围、安全保障措施、可能的风险与影响范围以及更新频率等,对开放的政务数据进行清洗、脱敏、脱密、格式转换等处理，并进行动态调整。

**第二十九条** 数据销毁。政务部门应当制定数据清理、数据销毁的制度，建立相关审批、记录和备案流程，确保全过程可审计。

## 第五章 监督检查与应急处理

**第三十条** 政务数据管理部门会同本级网信、公安等部门建立政务数据安全监督检查制度,对各部门开展政务数据安全监督检查。

**第三十一条** 政务数据安全监督检查内容:

（一）贯彻落实国家、省、市政务数据安全有关规定情况;

（二）研究部署政务数据安全工作情况;

（三）建立和执行政务数据安全制度情况;

（四）制定政务数据安全应急预案并组织演练情况;

（五）开展政务数据安全培训情况;

（六）对发现和通报的安全隐患及时排查和处置情况;

（七）落实网络安全等级保护和商用密码应用情况;

（八）政务数据安全经费保障情况;

（九）上级部门要求的其他安全工作情况。

**第三十二条** 政务数据安全监督检查流程:

（一）安排部署。政务数据管理部门制定政务数据安全监督检查方案，确定检查重点、内容和时间安排。

（二）自查评估。政务部门按照政务数据安全监督检查要求开展自查，形成自查报告报政务数据管理部门。

（三）实地检查。政务数据管理部门会同网信、公安等部门组织人员进行检查复核，对发现的问题提出处理意见。

（四）整改提高。政务部门根据处理意见整改完成后，整改情况报送政务数据管理部门。

**第三十三条** 对监督检查中发现的重大安全隐患和安全管理缺陷，由政务数据管理部门责令有关单位限期整改,涉及失泄密隐患的向保密主管部门报告,存在违法行为的应立即制止，并提请公安机关依法查处。

**第三十四条** 有下列情形之一的，政务部门应当立即启动应急预案，采取补救措施，并及时报送本级网信、公安、政务数据管理等部门:

（一）发现重大网络安全隐患、漏洞或基础网络、重要系统受到外部攻击遭到破坏;

（二）公民、法人信息或重要政务数据泄露、毁损、丢失，造成重大影响或经济损失;

（三）党政机关及事业单位等网站数据被篡改;

（四）国家、省、市有关部门通报的事件;

（五）发生其他重大政务数据安全事件。

## 第六章　责任追究

**第三十五条**　政务部门违反本细则规定，不履行、怠于履行政务数据安全保护义务的，由政务数据管理部门责令限期整改;因故意或过失造成政务数据存在安全隐患或导致安全事件发生的，由政务数据管理部门对责任单位进行书面通报，并追究相关责任；构成犯罪的，依法追究刑事责任。

**第三十六条**　履行政务数据安全监管职责的工作人员玩忽职守、滥用职权、徇私舞弊的，由有关主管部门根据情节轻重依法给予处分；构成犯罪的，依法追究刑事责任。

## 第七章　附　则

**第三十七条**　本细则由市大数据应用局负责解释。

**第三十八条**　本细则自 2024 年 3 月 1 日施行，有效期二年。

抄送：市委各部门，市人大常委会办公室，市政协办公室，市法院，市检察院，各人民团体，各新闻单位。

市属各事业单位，驻市各单位，各大中型企业。

晋城市人民政府办公室　　2024年1月29日印发