山西省人民政府办公厅文件

晋政办发〔2023〕30号

山西省人民政府办公厅
关于印发山西省政务数据安全管理办法的通知

各市、县人民政府，省人民政府各委、办、厅、局：

《山西省政务数据安全管理办法》已经省人民政府同意，现印发给你们，请认真贯彻执行。

山西省人民政府办公厅

2023年5月22日

（此件公开发布）

山西省政务数据安全管理办法

第一章　总　则

第一条　为加强全省政务数据安全管理，规范政务数据处理活动，维护国家安全、社会秩序和公共利益，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》等法律法规，结合我省实际，制定本办法。

第二条　本办法所称政务数据，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（以下简称政务部门）在依法履职过程中收集和产生的各类数据。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使用的状态，具备保障政务数据的完整性、保密性、可用性的能力。

第三条　本省行政区域内对政务数据进行收集、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，适用本办法。

涉及国家秘密、商业秘密、个人信息的政务数据处理活动，按照有关法律、法规规定执行。

第四条　政务数据安全管理采取政府主导、分工负责、积极防

御、综合防范的方针，坚持保障政务数据安全与促进信息化发展相协调、管理与技术统筹兼顾的原则。

第五条 县级以上网信部门统筹协调本行政区域内政务网络数据安全和相关监管工作。

县级以上人民政府公安机关在职责范围内负责本行政区域内政务数据安全监督、管理等工作。

县级以上人民政府确定的政务信息管理部门负责组织协调有关单位开展政务数据安全保障工作。

保密、国家安全、密码、通信管理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。

第六条 各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。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。

第二章 安全制度

第七条 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。政务部门应当将安全管理贯穿于数据处理活动中。

第八条 政务部门应当明确本部门负责政务数据安全管理的机构，建立健全政务数据安全管理制度，落实安全保护责任，定期开展数据安全意识教育和专项技能培训。

第九条 政务信息管理部门应当指导督促本级政务部门对政务数据进行分类分级管理。政务部门按照政务数据分类分级规则和标准确定数据类别和安全保护级别，对重要数据进行重点保护，对核心数据在重要数据保护基础上实施更严格的管理和保护，在政务数据全生命周期采取差异化管理措施。

第十条 政务部门应当和参与本部门数据处理活动的人员签订安全保密协议，必要时对其进行安全背景审查。

第十一条 政务部门委托政务信息系统建设、运维运营等单位开展政务数据处理活动，应当与其签订合同和保密协议等，明确数据安全保护义务，并监督其履行到位。受托方处理政务数据后，政务部门的数据安全主体责任不变。

受托方应当依照法律、法规规定及合同约定履行政务数据安全保护义务，承担基础运行环境及技术保障服务安全管理责任，保证政务部门对政务数据的访问、使用、支配，不得擅自留存、访问、修改、使用、泄露、销毁或者向他人提供政务数据。

第十二条 涉及政务数据出境的，应当遵守《数据出境安全评估办法》等有关法律法规规定。

第三章 安全管理

第十三条 开展政务数据收集活动时，应当遵循“一数一源”的原则，明确收集的范围、目的和用途，保证数据收集的合法性、正当性和必要性，对数据收集的环境、设施和技术采取必要的安全管

理措施。

政务部门可以通过共享方式获取的政务数据资源，不再重复收集。

第十四条 开展政务数据存储活动时，应当选择与政务数据分级保护要求相匹配的存储载体，依照相关规定对数据进行加密存储，对移动存储介质进行严格管理。有容灾备份要求的，应当按照有关规定建立数据容灾备份机制。

第十五条 在法定职责范围内开展政务数据使用活动时，应当依照法律、法规等有关规定采取管控措施，确保数据使用过程合规、可控、可追踪溯源。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进行。

第十六条 开展政务数据加工活动时，应当遵循合法、正当、必要的原则，采取必要的安全管理和技术措施，防止数据泄露，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。

第十七条 开展政务数据传输活动时，应当根据传输的政务数据安全级别和应用场景，制定数据传输安全策略，采用安全可信通道或数据加密等安全管理措施，确保政务数据传输过程安全可信。

第十八条 开展政务数据提供活动时，应当按照分类分级要求，对政务数据进行内部审查，明确数据提供方式、使用范围、应用场景以及安全保护措施、责任义务等，必要时可与使用单位签订数据安全协议。

第十九条 政务部门应当遵循公正、公平、便民的原则，在确保国家安全、商业秘密和个人合法权益不受损害的前提下，编制可开放的政务数据目录，并对开放的政务数据进行清洗、脱敏、脱密、格式转换等处理。依法不予公开的除外。

开展政务数据公开活动时，应当按照有关规定进行安全风险评估，明确公开数据的内容与类型、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，并进行动态调整。

第二十条 开展政务数据销毁活动时，应当建立政务数据销毁制度，严格履行审批程序，采取必要措施予以销毁。

第二十一条 利用互联网等信息网络开展政务数据处理活动的，应当在网络安全等级保护制度的基础上，履行上述数据安全保护措施，统筹协调网络与数据安全保护工作。备案级别在第三级以上的网络系统要定期开展等级测评，并向属地公安机关报送等级测评报告。

第四章 安全保障

第二十二条 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。

第二十三条 政务部门和政务信息系统建设、运维运营等单位应当加强政务数据安全风险监测，发现政务数据安全缺陷、漏洞等风险时，应当立即采取补救措施。

第二十四条 政务部门及政务信息系统建设、运维运营等单

位应当制定政务数据安全事件应急预案，组织协调重要数据和核心数据安全事件应急处置工作，定期开展应急演练。

发生政务数据安全事件时，应当立即依法启动应急预案，采取应急处置措施，按照规定及时告知用户并向网信、公安、政务信息管理等有关部门报告。

第二十五条 政务部门及政务信息系统建设、运维运营等单位从事政务数据处理活动时，应当建立日志记录规范，并对异常操作行为进行监控和告警，保障重要操作行为可追踪溯源。日志留存时间不少于6个月，并定期进行安全审计，形成审计报告。政务部门及政务信息系统建设、运维运营等单位应当配合有关主管部门组织的数据安全审计活动。

第五章 安全责任

第二十六条 政务信息管理部门应当建立政务数据监督检查制度，确定政务数据安全监督检查的对象、内容和流程等，并建立信息通报机制。

第二十七条 政务部门在履行本部门、本行业政务数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

第二十八条 政务部门不履行本办法规定的政务数据安全保护义务的，由有关主管部门责令限期改正；造成政务数据安全隐患

或导致安全事件发生的，对责任单位进行书面通报，并对直接负责的主管人员和其他直接责任人员依法给予处分；构成犯罪的，依法追究刑事责任。

第二十九条 履行政务数据安全监管职责的工作人员滥用职权、玩忽职守、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。

第六章 附 则

第三十条 本办法由省政务信息管理局负责解释。

第三十一条 本办法自2023年7月1日起施行，有效期2年。

抄送：省委各部门，省人大常委会办公厅，省政协办公厅，省法院，省检察院，各人民团体，各新闻单位。
各民主党派山西省委。

山西省人民政府办公厅 2023年5月22日印发