

贵阳市人民代表大会常务委员会公告

2018年8月16日

《贵阳市大数据安全管理条例》经2018年6月5日贵阳市第十四届人民代表大会常务委员会第十三次会议通过，2018年8月2日贵州省第十三届人民代表大会常务委员会第四次会议批准，现予公布，自2018年10月1日起施行。

贵阳市大数据安全管理条例

(2018年6月5日贵阳市第十四届人民代表大会常务委员会第十三次会议通过
2018年8月2日贵州省第十三届人民代表大会常务委员会第四次会议批准)

第一章 总 则

第一条 为了加强大数据安全管理，维护国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进大数据发展应用，推动实施大数据战略，根据《中华人民共和国网络安全法》等有关法律法规的规定，结合本市实际，制定本条例。

第二条 本条例适用于本市行政区域内大数据发展应用中的安全保护、监督管理以及相关活动。

涉及国家秘密的大数据安全，按照有关保密法律法规的规定执行。

本条例所称大数据安全，是指大数据发展应用中，数据的所有者、管理者、使用者和服务提供者（以下简称安全责任单位）采取保护管理的策略和措施，防范数据伪造、泄露或者被窃取、篡改、非法使用等风险与危害的能力、状态和行动。

本条例所称大数据，是指以容量大、类

型多、存取速度快、应用价值高为主要特征的数据集合，是对数量巨大、来源分散、格式多样的数据进行采集、存储和关联分析，发现新知识、创造新价值、提升新能力的新一代信息技术和服务业态。

本条例所称数据，是指通过计算机或者其他信息终端及相关设备组成的系统收集、存储、传输、处理和产生的各种电子化的信息。

第三条 实施大数据安全管理，应当坚持正确的网络安全观，遵循统一领导、政府管理、行业自律、社会监督、风险防控、权责统一、包容审慎、支持创新的原则。

第四条 市人民政府统一领导本市大数据安全管理工作。区（市、县）人民政府领导本辖区大数据安全管理工作。

第五条 市网信部门负责统筹协调全市大数据安全监督管理工作，组织开展全

市关键信息基础设施监管等工作。区（市、县）网信部门按照职责负责综合协调本辖区大数据安全监督管理工作。

市公安机关负责开展大数据安全的等级保护、日常巡查、执法检查、信息通报、应急处置等监督管理工作。区（市、县）公安机关按照职责负责本辖区大数据安全监督管理工作。

市大数据主管部门统筹协调本市大数据安全保障体系建设。区（市、县）大数据主管部门按照职责负责本辖区大数据安全管理的相关工作。

保密、国家安全、密码管理、通信管理等主管部门按照各自职责，做好大数据安全管理的相关工作。

第六条 安全责任单位应当加强大数据安全能力建设，履行大数据安全保护职责，接受有关主管部门监督管理和社会监督。

第七条 县级以上人民政府以及网信、公安、大数据等主管部门和安全责任单位、大众传播媒介按照各自职责，做好大数据安全宣传教育工作。

第八条 市人民政府设立统一的大数据安全监管服务、投诉举报平台，建立相应的工作机制。

任何单位和个人都有权投诉举报危害大数据安全的行为；有关部门应当对投诉举报予以保密。

第二章 安全保障

第九条 安全责任单位应当根据职责明确、意图合规、质量保障、数据最小化、最小授权操作、分类分级保护和可审计的原则，采取有效措施保护数据的保密性、完整性、真实性、可控性、可靠性和可核查性。

第十条 安全责任单位的法定代表人或者主要负责人是本单位大数据安全的第一责任人。

安全责任单位应当根据数据的生命周期、规模、重要性和本单位的性质、类别、规模等因素，建立安全管理内控制度和支撑保障机制，明确安全管理负责人，落实不同岗位的安全管理职责；关键信息基础设施的运营者还应当设置专门安全管理机构。

第十一条 安全责任单位应当根据数据类型、级别、敏感程度以及数据安全能力成熟度等要求，制定安全规则、管理规范 and 操作规程，采取相应的安全管理策略、管理措施和技术手段实施有效管理。

第十二条 安全责任单位应当按照大数据安全等级保护要求进行系统安全功能配置，制定实施系统配置技术管理规程、软件采购使用限制策略和外部组件使用安全策略，规定配置管理的审批、操作流程，提供符合规范标准的管理与服务，对系统重要配置进行及时更新。

第十三条 安全责任单位应当制定完善访问控制策略，采取授权访问、身份认证等技术措施，防止未经授权查询、复制、修改或者传输数据。对个人信息和重要数据实行加密等安全保护，对涉及国家安全、社会公共利益、商业秘密、个人信息的数据依法进行脱敏脱密处理。

第十四条 安全责任单位应当建立大数据安全审计制度，规定审计工作流程，记录并保存数据分类、采集、清洗、转换、加载、传输、存储、复制、备份、恢复、查询和销毁等操作过程，定期进行安全审计分析。

第十五条 存储数据，应当选择安全性能、防护级别与其安全等级相匹配的存

储载体，并且依法进行管理和维护。

销毁数据，应当按照数据分类分级建立审查机制，明确销毁对象、流程和技术等要求，设置相关监督角色，以不可逆方式销毁数据内容。

第十六条 安全责任单位服务外包业务涉及收集、存储、传输或者应用数据的，应当依法与外包服务提供商签订安全保护协议，采取安全保护措施，并对导出、复制、销毁数据等行为进行监督。

第十七条 支持依法成立的大数据行业组织依照法律、法规和章程的规定，制定行业安全规范和服务标准，对其会员的大数据安全行为进行自律管理，组织开展大数据安全教育、业务培训，推进大数据安全合作、交流，提高大数据安全管理水平和从业人员素质。

第十八条 市人民政府应当建立联席会议制度，研究、解决大数据安全工作的重大事项、重点工作和重要问题。

县级以上人民政府应当整合大数据安全防范、保障等资源，建立重点领域工作联动、会商、约谈、通报、巡查和决策咨询等机制，统筹有关职能部门履行大数据安全监督管理职责，防范安全风险。

第十九条 市人民政府建立大数据安全靶场和产品检验场地，对大数据安全新技术、新应用、新产品进行测试、检验，定期开展攻防演练，促进大数据安全城市建设。

第二十条 县级以上人民政府应当采取资金扶持、开设绿色通道等措施，支持大数据安全技术产业发展、安全技术研发应用和安全管理方式创新。

鼓励企业、科研机构、高等院校、职业学校和相关行业组织建立教育实践和培训基地，开设相关专业课程，加强人才交

流，多形式培养、引进和使用大数据安全人才。

第二十一条 市公安机关负责大数据安全投诉举报平台的运行、维护和管理工作，公布投诉举报方式等信息，即时受理投诉举报，按照规定时限回复；对不属于本部门职责的，移送有关部门处理。有关部门处理后，应当按照规定时限反馈市公安机关。

安全责任单位应当建立大数据安全投诉举报制度，公布投诉举报方式等信息，接受和处理用户及相关利害关系人的投诉举报。

第二十二条 网信、公安、大数据、标准化、工业和信息化等主管部门应当加强大数据安全的国家标准、行业标准和地方标准的宣传、培训，引导、鼓励安全责任单位采用大数据安全国家推荐标准、行业标准和地方标准。

鼓励支持教育、科研机构和企业参与大数据安全的国家标准、行业标准和地方标准的研究、制定。

鼓励安全责任单位运用区块链等新技术手段，优化数据聚通用架构，强化信任认证和防篡改设计，提升大数据安全防护水平。

第二十三条 市大数据主管部门应当配合制定大数据安全保护标准体系，指导数据资源分类分级、数据安全能力成熟度认定和数字认证等相关工作。

第二十四条 县级以上人民政府以及有关部门应当通过报刊杂志、电台电视台、门户网站、微信微博等途径，运用安全宣传周、主题日、专题会、研讨班、应用场景展示、竞赛等形式，经常性地对公众以及大数据安全重点领域、重点行业、重点单位、重点人群等组织开展大数据安全法

律法规、形势政策和知识技能的宣传培训。

安全责任单位应当制定计划，对员工、用户以及本单位的重点部位、重点设施、重点岗位安全工作人员开展大数据安全法律法规、知识技能等教育、培训和考核，提升大数据安全意识和防护技能水平。

第三章 监测预警与应急处置

第二十五条 市公安机关负责大数据安全监管服务平台的日常维护管理，加强对平台监测信息、监督检查信息和上级通报信息的分析、安全形势研判和风险评估，按照规定发布安全风险预警或者信息通报。

区（市、县）公安机关应当及时落实上级公安机关通过大数据安全监管服务平台发布的各项指令。

第二十六条 县级以上人民政府应当根据国家和省的规定，落实大数据安全应急工作机制，明确工作责任、程序和规范；制定大数据安全事件应急预案，明确应急处置组织机构及其职责、事件分级、响应程序、保障手段和处置措施；定期组织演练，评估演练效果，分析存在问题，总结处置经验，提出改进和完善应急预案的意见。

发生大数据安全事件时，县级以上人民政府应当依法按程序启动应急预案，组织网信、公安、大数据等主管部门针对事件的性质和特点，采取应急措施处置。

第二十七条 安全责任单位应当制定大数据安全事件预警通报制度和应急预案，建立和实施安全事件预警、舆情监控、风险评估和应急响应的策略、规程，保持与有关主管部门、设备设施及软件服务提供商、安全机构、新闻媒体和用户的联络、协作。

发生大数据安全事件时，安全责任单位应当依法按程序启动应急预案，采取相应措施防止危害扩大，保存相关记录，告知可能受到影响的用户，按照规定向有关主管部门报告。

第四章 监督检查

第二十八条 县级以上人民政府应当将大数据安全管理工作纳入年度目标绩效考核。

第二十九条 县级以上人民政府应当建立健全大数据安全工作监督检查机制，明确监督检查的牵头部门、责任分工、内容、重点、目标、方式和标准。

监督检查的情况，应当在有关主管部门之间互通和共享。

第三十条 公安机关应当监督、检查、指导安全责任单位建立、落实大数据安全管理的各项制度和技术措施，依法查处大数据安全违法案件。

第三十一条 大数据主管部门应当结合监督检查大数据安全责任落实的情况，定期组织开展大数据安全风险评估，发布评估报告。

第三十二条 有关主管部门在监督检查、风险评估和攻防演练中，发现安全责任单位存在安全问题的，应当及时提出改进建议，发出整改意见并且督促整改。

安全责任单位应当根据有关主管部门的整改意见进行整改，并且反馈整改情况。

第三十三条 公安、大数据主管部门应当建立大数据安全管理诚信档案，记录违法信息，纳入统一的信用共享平台管理。

第五章 法律责任

第三十四条 安全责任单位不履行本条例第十条、第十一条、第十二条、第十

三条、第十四条和第二十七条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害大数据安全等后果的，处1万元以上10万元以下罚款，对直接负责的主管人员处5000元以上5万元以下罚款。

第三十五条 违反本条例规定的其他行为，依据《中华人民共和国网络安全法》等法律、法规的相关规定处理。

第三十六条 安全责任单位中的国家机关不履行本条例规定的大数据安全保护

职责的，由其上级机关或者有关机关责令改正；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。

大数据安全监督管理有关主管部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第六章 附 则

第三十七条 本条例自2018年10月1日起施行。

关于《贵阳市大数据安全管理条例》的说明

贵阳市人大常委会

贵州省人大常委会：

2018年6月5日，贵阳市第十四届人民代表大会常务委员会第十三次会议审议通过了《贵阳市大数据安全管理条例》（以下简称《条例》），按照法律规定，决定报请批准。现作如下说明：

一、立法必要性

发展大数据，是当今信息化、互联网时代的趋势、技术和手段。坚持先行先试、创新引领，制定大数据安全地方性法规，切实依法保障大数据安全，对于推动实施国家大数据战略、建设国家大数据（贵州）综合试验区、促进我市大数据产业发展应用尤为重要，十分必要。

（一）创新性贯彻落实中央、省、市要求，引领推动实施大数据安全保护工作的需要

习近平总书记2017年12月8日在中央政治局第二次集体学习时指出：推动实

施国家大数据战略，建设数字中国，要切实保障国家数据安全，加强政策、监管、法律的统筹协调，加快法规制度建设。近年来，国家、省、市相继出台一系列大数据、互联网建设实施文件，对大数据安全管理的风险防范、安全保护、法规制度建设等提出了具体要求。2017年2月，国家发改委、工信部、中央网信办批复我省建设国家大数据（贵州）综合试验区，明确将“开展大数据制度创新试验”作为七大系统性试验任务之一，我市作为该试验区的核心区，肩负着制度创新、率先作为的重任。贯彻落实中央、省、市有关要求，有必要制定首部大数据安全管理的地方性法规。

（二）促进大数据发展应用，建设大数据及网络安全示范试点城市，保障大数据安全的需要

作为国家大数据（贵州）综合试验区

的核心区，我市近年来在大数据发展及创新应用方面取得了显著成效，积累了较为丰富的经验。一批新技术、新产品、新模式不断涌现，形成了创业创新、产业生态等一批示范基地和集聚区，我市深入推进大数据政务、商用、民用，在41家市直部门实施“数据铁笼”，在贵阳筑民生综合平台上向市民提供社区服务、教育等8个试点领域100项以上服务。公安部批复在我市建设国家大数据及网络安全示范试点城市 and 大数据安全靶场，打造大数据及网络安全自主创新中心、应用示范中心和政府监管中心，搭建“块数据指挥中心”“核心数据平台”“大数据安全监管服务平台”等多个综合防护平台，总结提炼有关大数据及网络安全建设、管理的成果，研究国家有关技术标准规范，上升为地方性法规内容，可以为国家大数据安全保障探索可复制的经验。

（三）坚持安全与发展并重并举，以安全保障促进政府、企业、社会数据共享开放的需要

随着数据技术的不断成熟和数据共享开放的日益增速，数据安全面临着严重挑战，推进政府数据共享开放的同时伴随着安全风险。《贵阳市政府数据共享开放条例》2017年5月1日起施行，全市已实现对54家单位、211个系统、1176项数据目录字典的集中存储和统一管理，已有52个部门2685个数据集、API 303个、612万条数据实现了深度关联开放。防攻击、防泄露、防窃取、防篡改、防非法使用等风险与危害，确保数据安全，成为贯穿政府数据共享开放全过程的前提。有必要采取相应的安全保障措施，有效维护国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，确保数据共享开放在安全

有序的环境下运行。

（四）坚持问题导向，进一步细化《网络安全法》规定

全国人大常委会在2012年12月作出《关于加强网络信息保护的决定》的基础，2016年11月7日又制定了《网络安全法》，以国家法律对建设、运营、维护和使用网络以及网络安全的监督管理进行了规范。作为设区的市，根据《立法法》第七十二条的规定，制定大数据安全管理方面的地方性法规，针对大数据发展应用中的安全规范和监督管理做出规范，是在《立法法》第七十二条第二款城乡建设与管理的范畴开展立法，落实和细化《网络安全法》的有关规定和要求，也是推动《网络安全法》等法律有效实施的措施。而且，在该法实施不满3个月的时间，全国人大常委会就进行了执法检查，报告指出了实施“一法一决定”存在的七个突出问题，其中不少需要而且可以通过进一步加强立法和制度建设来加以解决。

二、制定过程

2016年7月11日，中共贵阳市委九届六次全会明确以大数据为引领加快打造创新型中心城市，作为贵阳当前和今后一个时期的重大使命，提出要“围绕数据安全风险，加强相关立法研究，制定有关地方性法规、规章。建立健全数据安全管理制度，落实信息安全等级保护，加强安全风险评估、检查和监督”。据此，我市于2016年11月启动了《条例》的调研起草，成立了由市人大常委会主任、党组书记李忠同志任组长，相关负责人为成员的立法领导小组，统筹领导和推进该项立法工作。

市公安局作为起草责任单位牵头深入开展前期调研，并分别委托中国政法大学、中国人民公安大学、大数据战略重点实验

室承担文本起草工作。在收集、学习研究国家、省、市关于大数据安全的相关法律、法规、规章和文件规定的基础上，深入全市40家“数据铁笼”部门和56家大数据企业开展立法调研，整合委托起草的3个文稿并反复修改形成了《条例》初稿。同时，为了更好地落实立法权限和取得上级人大的立法指导，市人大常委会有关领导多次带队赴省人大常委会请示汇报并征求意见，经省人大常委会法工委向全国人大常委会法工委作了请示。2017年12月14日，全国人大常委会法工委作出了该立法在设区的市的立法权限范围和有关法规规范内容的答复意见。

市政府于2017年12月22日召开常务会议通过了关于提请审议《条例（草案）》的议案。2017年12月27日市十四届人大常委会第八次会议进行了初次审议。会后，市人大常委会法工委根据市委主要领导同志的批示，对常委会组成人员审议意见、专委会初审意见、议案文本、《网络安全法》的相关规定、全国人大常委会关于检查网络安全“一法一决定”的报告等进行研究分析，参阅有关数据安全方面的研究成果资料，围绕落实和细化《网络安全法》相关规定，实地走访考察，并学习研究目前国家制定和拟制定的信息安全技术国家标准规范、行政法规草案等，修改形成了草案征求意见稿，向社会和有关各方征求意见。

2018年3月8日至4月8日，除了通过省、市级媒体向社会公开征求意见外，还向有关部门发函征求意见；听取了省人大法制、财经、内司委和常委会法工委、省公安厅、省大数据局、省保密局、省网信办等16个省级单位的意见和建议；向大数据国家工程实验室等科研机构征询了意

见。5月8日，市十四届人大常委会第十二次会议对《条例（草案）》进行了第二次审议。

二审后，常委会法工委认真研究了二审意见和省人大法制委、常委会法工委的修改意见建议；还对二审中市监察委员会提出的修改意见，与其共商做出相应修改。在2018中国国际大数据产业博览会期间召开“大数据安全地方立法高层咨询论证会”，听取了来自国内的专家、学者意见建议，与会专家一致认为，贵阳市作为国家大数据（贵州）综合试验区的核心区和全国唯一的大数据及网络安全示范试点城市，将大数据安全与大数据产业发展同步规划、同步建设，并强力推进大数据安全立法，是以立法引领制度创新的有益实践，是非常重要和非常有意义的立法行动。《条例（草案）》起草调研详实、文本逻辑清晰，对推进大数据安全立法进程有积极的引领和推动作用。会后，经与市公安局、市法制局共同研究，认真吸纳专家提出的意见建议，修改形成草案三审文本；5月30日，市人大法制委员会召开第十一次全体会议，听取常委会法工委三审修改情况介绍，对草案进行统一审议，形成草案三审稿。6月2日，市十四届人大常委会第二十九次主任会议同意将草案三审稿提请常委会审议。

三、需要说明的问题

《条例》共六章37条，对立法目的、大数据安全及数据概念、政府及其部门职责、安全保障、监测预警与应急处置、监督检查、法律责任等作出了规范。

（一）关于大数据安全和数据的概念

《条例》把调整范围确定为对本市行政区域内大数据发展应用中数据的安全保护、监督管理以及相关活动的规范。《条例》

第二条第三款围绕大数据安全的责任主体类型、风险危害表现形式，将大数据安全定义为：大数据发展应用中，数据的所有者、管理者、使用者和服务提供者（以下简称安全责任单位）采取保护管理的策略和措施，防范数据伪造、泄露或者被窃取、篡改、非法使用等风险与危害的能力、状态和行动。关于数据的概念，《条例》第二条第四款明确：“本条例所称数据，是指通过计算机或者其他信息终端及相关设备组成的系统收集、存储、传输、处理和产生的各种电子化的信息。”考虑到《贵州省大数据发展应用促进条例》对大数据概念作了规定，故本条例不再重复表述。

（二）关于政府及部门职责

为了落实和细化《网络安全法》的有关规定，明晰数据安全监督管理的部门职责，《条例》第五条分别明确规定了网信部门、公安机关、大数据主管部门的各自职责，以及保密、国家安全、密码管理、通信管理等主管部门按照各自职责做好数据安全管理工作。还在第四章监督检查中对有关主管部门的监管职责作了细化，以避免大数据安全管理权责不清、各自为战、执法推诿、效率低下等问题，防止出现“九龙治水”、多头管理等现象。

（三）关于安全责任单位的安全保护义务

为落实《网络安全法》第二十一条等保护制度要求，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改等进行了规定。《条例》第九条至第十五条对安全责任单位采取安全措施的原则、落实大数据安全保护责任，采取防范危害大数据安全行为技术措施，采取监测记录数据运行状态和网络安全事件的技术措施，采取数据分类、备份和加

密措施，增强大数据系统安全功能配置，存储和销毁数据等作出了相应规范。

（四）关于宣传培训规范要求

增强网络以及大数据安全意识，是一项极其重要的基础工程。《条例》坚持发展与安全、建设与安全、使用与安全并重，在第七条明确：“县级以上人民政府以及网信、公安、大数据等主管部门和安全责任单位、大众传播媒介按照各自职责，做好大数据安全宣传教育工作”；同时，第十七条明确行业组织“组织开展大数据安全教育、业务培训”，第二十二条明确相关主管部门“加强大数据安全的国家标准、行业标准和地方标准的宣传、培训”，第二十四条明确政府和有关主管部门对“公众以及大数据安全重点领域、重点行业、重点单位、重点人群等组织开展大数据安全法律法规、形势政策和知识技能的宣传培训”，安全责任单位对“员工、用户以及本单位的重点部位、重点设施、重点岗位安全工作人员开展大数据安全法律法规、知识技能等教育、培训和考核”等作了具体规范。

（五）关于建立统一投诉举报平台

投诉无门、部门之间推诿扯皮，是全国人大常委会网络安全执法检查指出的一个突出问题。为了解决大数据安全的举报难、投诉难、立案难的现象，《条例》在第八条第一款规定“市人民政府设立统一的大数据安全监管服务、投诉举报平台，建立相应的工作机制”的基础上，进一步在第二十一条明确：“市公安机关负责大数据安全投诉举报平台的运行、维护和管理工作，公布投诉举报方式等信息，即时受理投诉举报，按照规定时限回复；对不属于本部门职责的，移送有关部门处理。有关部门处理后，应当按照规定时限反馈市公安机关。安全责任单位应当建立大数据安

全投诉举报制度，公布投诉举报方式等信息，接受和处理用户及相关利害关系人的投诉举报。”

（六）关于监测预警、应急处置

大数据安全风险具有很强的隐蔽性，安全态势感知是做好大数据安全最基本、最基础的工作。《条例》第三章细化《网络安全法》监测预警与应急处置的相关规定，第二十五条、第二十六条和第二十七条通过平台对监测信息、监督检查信息和上级通报信息的分析、安全形势研判和风险评估，发布安全风险预警或者信息通报，实现对重要大数据安全风险的全天候实时、动态监测，市、区（市、县）人民政府、市公安局、安全责任单位等在监测预警与应急处置方面的要求等等作出了具体规

范。

（七）关于法律责任

依据《网络安全法》第五十九条第一款的规定，《条例》第三十四条对国家机关以外的安全责任单位不履行第十条至第十四条、第二十七条规定的安全保护义务的行为，设置了具体明确法律责任。根据《网络安全法》第七十二条、第七十三条第二款的规定，《条例》第三十六条明确了安全责任单位中的国家机关不履行规定的大数据安全保护义务，大数据安全监督管理有关主管部门的工作人员玩忽职守、滥用职权、徇私舞弊尚不构成犯罪等行为，规定了依法给予处分的法律责任。

以上说明连同《条例》文本，请一并审议。

贵阳市人民代表大会常务委员会 关于加强人民法院执行工作的决定

（2018年8月29日贵阳市第十四届人民代表大会常务委员会第十五次会议通过）

为全面推进依法治国，维护法律尊严，充分保障人民法院生效裁判及其他法律文书的执行，实现当事人合法权益，形成解决执行难的长效机制，努力让人民群众在每一个司法案件中都感受到公平正义，根据《中华人民共和国各级人民代表大会常务委员会监督法》、《中华人民共和国民事诉讼法》、《中华人民共和国行政诉讼法》等法律及有关规定，结合我市实际，特作如下决定：

一、依法执行生效裁判及其他法律文书是宪法和法律赋予人民法院的重要职责，是全面推进依法治国的重要内容，是

维护公民、法人和其他组织合法权益、促进社会诚信建设、实现社会公平正义的重要途径，对推进法治贵阳建设、优化我市营商环境、促进地方经济社会发展有着重要的意义。

二、全市各级国家机关、企事业单位、社会组织和个人都应当支持人民法院执行工作，自觉履行生效法律文书。任何单位、组织和个人都不得规避、阻碍、抗拒和干预人民法院执行。负有协助执行义务的单位、组织和个人，应当依法及时协助人民法院执行，拒不履行协助义务的，人民法院除责令其履行协助义务外，还可依法采