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　根据2020年10月30日贵阳市第十四届人民代表大会常务委员会第三十二次会议通过　2021年5月27日贵州省第十三届人民代表大会常务委员会第二十六次会议批准的《贵阳市人民代表大会常务委员会关于修改和废止部分地方性法规的决定》修正）

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管理，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。县级人民政府领导本辖区大数据安全管理工作。

第五条 市级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。县级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。

市级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。县级公安机关按照职责负责本辖区大数据安全监督管理工作。

市级大数据主管部门统筹协调本市大数据安全保障体系建设。县级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、管理规范和操作规程，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 市级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级公安机关。

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 市级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。

县级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,处以1万元以上10万元以下罚款，对直接负责的主管人员处以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。