广州市政务数据安全管理办法

第一章 总则

第一条（目的与依据） 为了规范政务数据处理活动，保障政务数据安全，促进政务数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，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》等相关法律法规规定，结合本市实际，制定本办法。

第二条（适用范围） 本市各级行政机关及法律法规授权或者受行政机关委托行使行政职能的事业单位和社会组织实施的政务数据采集、使用、管理行为，适用本办法。

本市行政区域内的电力、水务、燃气、通信、公共交通以及城市基础设施服务等公共企事业单位和社会团体涉及公共服务的数据采集、使用、管理行为，参照本办法执行。

涉及国家秘密的政务数据安全管理，或者法律法规对政务数据安全管理另有规定的，按照相关规定执行。

第三条（术语解释） 本办法下列术语的含义：

（一）政务部门，是指本市各级行政机关及法律法规授权或者受行政机关委托行使行政职能的事业单位和社会组织。

（二）政务数据，是指政务部门在履行职责过程中制作或者获取的，以一定形式记录、保存的文件、资料、图表等各类数据，包括政务部门直接或者通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的数据。

（三）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的状态，以及具备保障持续安全状态的能力。

（四）政务信息系统，是指市本级行政事业单位使用市本级财政资金建设、运行管理或使用的，用于支持政务部门工作或履行其职能的各类信息系统。

第四条（管理原则） 政务数据安全管理应当遵循以下原则：

（一）政务数据安全管理应当坚持安全与发展并重，遵循统筹规划、权责统一、综合防范的原则。

（二）保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序流通。

（三）政务数据安全工作与信息化工作应当同步规划、同步建设、同步使用。

第二章 职责分工

第五条（组织领导） 市、区人民政府负责组织领导本行政区域内政务数据安全管理工作，协调解决与政务数据安全有关的重大问题。

第六条（主管部门职责） 工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域政务数据安全监管职责。

网信、保密、国家安全、密码管理、公安、审计等主管部门依照本办法和有关法律、行政法规的规定，在各自职责范围内承担政务数据安全监管职责。

市、区政务数据主管部门按照本办法和有关法律、法规、规章的规定，负责统筹协调本行政区域内政务数据安全管理工作。

第七条（政务部门职责） 政务部门作为本部门政务数据安全管理的责任主体，负责下列工作:

（一）明确政务数据安全管理的目标、数据安全责任人和管理机构。

（二）建立健全政务数据内部安全管理制度，加强风险监测，针对重要数据定期开展风险评估，建立应急处置机制，监督受政务部门委托建设、维护政务信息系统的供应商履行相应的政务数据安全保护义务，落实政务数据安全保护责任，保障政务数据安全。

（三）建立政务数据安全经费保障制度，将政务数据安全经费纳入本单位年度财务预算。

（四）建立政务数据安全培训制度，定期开展政务数据安全意识教育与政务系统数据安全操作基础培训，对政务系统管理人员、运维人员和政务系统安全从业人员进行数据安全专项技能培训。

（五）法律、法规、规章规定的其他政务数据安全管理职责。

第三章 数据基础设施安全管理

第八条（数据基础设施等级保护工作） 市电子政务外网、政务云平台、政务大数据平台等政务数据基础设施主管部门按照国家等级保护制度要求和技术标准，依法开展等级保护工作。

第九条（关键信息基础设施安全自查） 政务部门应当根据本部门关键信息基础设施清单，每年至少对清单内关键信息基础设施进行一次网络安全检测和风险评估，及时整改安全问题。

第十条（政务信息系统等级保护工作） 政务部门应当按照国家等级保护制度要求和技术标准，对政务信息系统开展等级保护工作。

新建政务信息系统或者政务信息系统发生重大变更时，应当首先确定政务信息系统的安全保护等级，并同步建设符合该安全保护等级要求的安全保护设施。

第十一条（商用密码应用） 政务部门应当按照国家商用密码应用要求，对政务信息系统采用密码技术，并定期开展密码应用安全性评估，保障政务数据安全。

第四章 数据生命周期安全管理

第十二条（数据分类分级） 市政务数据主管部门应当会同有关部门，根据国家和省数据分类分级相关规定，增补本地政务数据的分类分级规则。

政务部门应当根据国家、省、市政务数据分类分级相关规定，落实政务数据安全保护工作。

第十三条（数据收集安全） 政务部门开展政务数据收集活动时，应当明确收集的目的、范围、用途、渠道等，保证政务数据收集合法、正当，应当采取必要的安全管控措施，确保环境、设施、人员等安全可控。

第十四条（数据存储安全） 开展政务数据存储活动时，应当根据需要采取脱敏、加密、校验等措施，保障政务数据的存储安全。针对重要数据和核心数据，应当建立数据容灾备份及恢复机制。

第十五条（数据使用与加工安全） 开展政务数据使用与加工活动时，应当在其履行法定职责的范围内依照法律、法规、规章规定的条件和程序使用与加工数据，应当采取管控措施确保数据使用与加工合规，过程安全可控、可溯源。

不得超出合理范围使用政务数据，不得滥用政务数据侵犯公共利益与个人合法权益。

利用数据挖掘、关联分析等加工政务数据的，应当采取安全技术措施防止敏感个人信息、商业秘密等信息的泄露。

第十六条（数据传输安全） 开展政务数据传输活动时，应当根据传输的数据类型、级别和应用场景，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。对关键网络传输链路、网络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。

第十七条（数据提供和公开安全） 政务数据提供和公开活动应按照有关数据提供、数据公开或数据共享开放等要求，依法依规有序开展。

共享的政务数据用于政务部门履行职责需要，政务部门不得直接或者以改变数据形式等方式提供给第三方，不得篡改信息内容，也不得用于或者变相用于其他目的。

开展政务数据公开活动时，应当按照相应规定实施数据公开管控措施，保障公共数据的公开范围、公开渠道、公开流程、公开内容和公开时效等合法、正确、有效；依法确定为国家秘密的信息，法律、行政法规禁止公开的信息，以及公开后可能危及国家安全、公共安全、经济安全、社会稳定的数据信息，不予公开；涉及商业秘密、个人隐私等公开会对第三方合法权益造成损害的敏感信息，不得公开，第三方同意公开或不公开会对公共利益造成重大影响的除外。

第五章 供应链安全管理

第十八条（全流程管理） 政务部门应当监督受委托建设、维护政务信息系统的供应商依照法律法规的规定和合同约定履行政务数据安全保护义务，包括建立健全政务数据安全防护体系。

政务部门应当加强监督，防止供应商发生擅自留存、使用、泄露或者向他人提供政务数据，擅自将数据用于其他用途，擅自向境外提供数据等违法违规和违反合同约定的行为。

在供应商参与政务信息化建设和运维过程中涉及敏感个人信息的，政务部门应当监督供应商按照有关法律法规要求采取备份、加密、访问控制等必要措施。

第十九条（采购管理） 政务部门优先采购安全可信的数据安全产品和服务，按照国家有关规定与产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

第二十条（权限管理） 政务部门应当加强政务信息系统的权限管理，建立最小授权的访问控制策略，对数据库、操作系统等的最高管理员权限必须由政务部门指定专人负责，不得擅自转交供应商人员管理使用，防范越权访问带来的数据泄露、篡改、删除等风险。

第二十一条（技术支撑与保障） 政务部门应督促供应商在政务信息化建设和运维过程中建立有效的技术支撑和保障机制，包括开展各类数据

终端的安全巡检、加固和防护技术工作，事前预防、事中发现、事后处置的保障机制，确保数据安全事件可定责、可追溯。

第六章 个人信息安全管理

第二十二条（个人信息生命周期的要求） 政务部门应当加强对个人信息收集、保存、使用、共享、转让、公开披露等信息处理环节的保护，保障个人的合法权益和社会公共利益。

第二十三条（个人信息保护制度的要求） 政务部门执行国家个人信息保护制度，制定内部管理制度和操作规程，对收集、使用的公民、企业信息，应当采取相应措施保护，不得出售或者非法向他人提供。在发生或者可能发生信息泄露时，应当立即采取补救措施。

第二十四条（个人信息收集使用的要求） 政务部门不得收集与其履行职能无关的个人信息，不得违反法律、法规的规定收集、使用及向第三方提供个人信息。

第二十五条（个人信息转移或委托的要求） 政务部门为履行职能开展个人信息处理过程中，需要将个人信息转移或委托给其他组织或机构使用的，应当与该组织或机构达成个人信息保护约定，明确个人信息使用范围和保护责任。未经委托方同意，受托人不得转委托他人处理个人信息。

第二十六条（个人信息存储的要求） 政务部门收集和产生的个人信息应当在中华人民共和国境内存储。

第七章 应急处理及通报

第二十七条（应急处理机制） 政务数据主管部门应当会同网信、公安、国家安全、保密等主管部门制定政务数据安全事件的应急预警、响应、通报、支援处理和灾难恢复机制。

第二十八条（应急预案与演练） 政务部门应当制定政务数据安全事件应急预案，设立或者指定应急工作管理部门，落实数据安全责任；定期开展数据安全应急演练，并对演练情况进行评估，及时整改演练中发现的问题。

第二十九条（安全事件处置与通报） 政务部门在发生政务数据安全事件时，应当及时进行处置，并按照规定及时向本级政务数据主管部门报告，不得瞒报、缓报、谎报和推诿责任。

第八章 监督检查

第三十条（监督检查工作机制） 政务数据主管部门通过随机抽查、定期检查等方式对政务数据安全进行监督检查。

第三十一条（评估机制） 政务部门应定期开展本单位政务数据风险评估，识别威胁、脆弱性、已有安全控制措施及主要安全风险，确定风险处置的优先级，形成风险评估报告。

市政务数据主管部门应会同有关部门建立政务数据安全工作的评估

机制，指导本行政区域内政务数据安全管理工作。

第三十二条（投诉处理） 任何个人、组织有权对违反数据安全相关法律法规的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。

有关主管部门应当对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益。

第三十三条（责任条款） 有关部门及工作人员违反本办法，不履行职责的，由有权机关责令改正；构成违法犯罪的，依法追究相应的法律责任。

第三十四条（实施时间） 本办法自 x 年 x 月 x 日起施行。