

江门市政务服务数据管理局

中共江门市委网络安全和信息化委员会办公室

中共江门市委机要和保密局

江门市公安局

文件

江政数〔2021〕116号

关于印发《江门市政务数据安全管理办法》的通知

市有关单位、各市（区）党委网信办、党委机要和保密局、公安局、政务服务数据管理局：

为规范我市政务数据安全工作，根据《中华人民共和国数据安全法》《广东省政务数据资源共享管理办法（试行）》等文件精神，结合本市实际，我们编制了《江门市政务数据安全管理办法》，现印发给你们，请认真贯彻执行。执行过程中遇到的问题径向市政务服务数据管理局反映。

(此页无正文)



中共江门市委网络安全和
信息化委员会办公室

中共江门市委机要和保密局

江门市公安局

2021 年 10 月 13 日

江门市政务数据安全管理办法

第一章 总 则

第一条（目的依据） 为维护国家数据安全和利益，保护个人、组织的合法权益，加强江门市政务数据安全，建立健全政务数据安全保障体系，加快推进“数字政府”建设，促进政务数据资源有序共享和开放，预防政务数据安全事件发生，根据《中华人民共和国数据安全法》《广东省政务数据资源共享管理办法（试行）》（粤府办〔2018〕50号）《广东省数据要素市场化配置改革行动方案》（粤府函〔2021〕151号）《广东省人民政府办公厅关于印发广东省首席数据官制度试点工作方案的通知》（粤办函〔2021〕63号）等有关法律法规要求，结合我市实际，制定本暂行办法。

第二条（基本原则） 维护政务数据安全，坚持国家网络安全观，建立数据安全治理体系，提高数据安全保障能力。坚持保障政务数据安全与促进信息化发展并重、管理与技术统筹兼顾的原则，政务数据安全和信息化工作应同步规划、同步建设、同步管理，切实保障政务数据安全。

第三条（概念定义） 本办法所称政务数据，是指政务部门在依法履职或生产经营活动中制作或获取的，以一定形式记录、保存的文件、资料、图表、图像、音频、视频、电子证照、电子档案和数据等各类数据资源，包括直接或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信息系统形成的数据资源等。

本办法所称政务数据安全，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的状态，以及具备保障持续安全状态的能力。

第四条（适用范围） 本办法适用于江门市行政区域内的非涉密政务数据安全管理工作，面向政务数据、承载政务数据的基础设施和支撑平台，覆盖政务数据处理活动的全过程，包括政务数据的收集、存储、使用、加工、传输、提供、公开等。涉及国家秘密的政务数据，按照国家保密相关规定管理和使用。

第二章 职责分工

第五条（市政务服务数据管理局职责） 市政务服务数据管理局负责组织、指导和协调全市政务数据安全工作；依照国家、省、市政务数据安全法律、法规和标准，编制市政务数据安全总体规划，制定政务数据安全方策略、管理制度和标准规范，协调相关部门建立数据安全技术保障措施和其他必要措施；面向全市政务数据、承载政务数据的基础设施和支撑平台开展政务数据处理活动的风险监测；指导市其他单位开展数据安全保障和数据安全应急处置工作；定期组织开展数据风险评估、数据安全教育培训等工作；建立数据安全管理制度，落实监督检查和考核问责制度。

市委网信办、市委机要和保密局、市公安局等部门依职能监督、检查全市各单位政务数据安全保护工作，组织实施全市政务数据安全年度检查和重要保障时期的专项检查。

第六条（各部门职责） 市各政务部门负责本单位的政务数据安全管理工作，遵循市数据安全管理办法，由首席数据官牵头落实本单位的政务数据安全管理工作，采取技术保障措施和其他必要措施，保障本单位的政务数据处理活动安全。配合上级及市政务数据管理局开展政务数据安全检查 and 调查整改工作。

第三章 安全管理

第七条（组织建设） 市各政务部门的首席数据官是本单位政务数据安全的第一责任人，依据上级及市政务服务数据管理局的指导意见，牵头制定本单位数据安全策略，协调建立数据安全技术保障措施和其他必要措施，配合市政务服务数据管理局组织开展数据安全的风险评估、应急响应、教育培训等工作。未设立首席数据官的部门的分管信息化工作领导为本单位政务数据安全第一责任人。

市各政务部门应在本单位首席数据官或分管信息化工作领导的指导下，进一步明确数据安全岗位和人员，相关人员应具备与数据安全保障要求相匹配的管理和实践经验，实现对数据安全管理人员的角色及职责分配，建立本单位的数据安全制度、流程和完备有效的工作考核机制。

第八条（数据资产管理） 市各政务部门应当根据上级及市政务服务数据管理局的指导意见，依托政务信息化管理系统，建立政务数据资产管理制度，对政务信息系统、政务数据资产进行梳理、确权与登记，编制数据资产清单，明确政务数据资产管理的责任岗位与人员，定期对政务数据资产进行一致性检查并保留检查记录。

第九条（分类分级保护） 市政务服务数据管理局依据国家和广东省政策标准，建立江门政务数据安全分类分级保护制度，并制定配套标准规范。市各政务部门依据分类分级制度和标准，围绕政务数据建立数据生命周期全过程的安全防护体系，对不同级别的数据实施恰当的安全保护措施，加强对个人隐私、个人信息、商业秘密、保密商务信息等数据的保护。

第十条（重要数据保护） 市各政务部门应根据国家、省、行业相关政策要求，结合政务数据分类分级有关标准制度，制定本单位的重要数据目录，加强对重要数据的保护。对关系国家安全、国民经济命脉、重要民生、重大公共利益等的重要数据，实行更加严格的管理，定期评估重要数据及其面临的安全风险，并上报主管部门和有关单位。

第十一条（等级保护及商用密码应用） 市各政务部门应当在网络安全等级保护、商用密码应用基础上，针对政务数据处理活动所涉及的软硬件平台，如门户网站、前置机、数据库、大数据平台、云计算平台、服务器等，建立数据安全保护措施。

第十二条（数据采集安全） 市各政务部门应通过应用系统人工录入或数据接口调用的方式实现政务数据采集，并明确政务数据的采集目的、采集用途、采集渠道、采集流程、采集内容和数据格式，保证政务数据采集的合法性、正当性、必要性和业务关联性，在上级及市政务数据管理局的指导下，定期执行政务数据采集合规性审查。

市各政务部门对政务数据采集涉及的采集环境、采集设施和采集技术采取必要的管控措施，提高政务数据的科学性、准确性和时效性，保证政务数据在采集过程中不被泄露。

第十三条（数据传输安全） 市各政务部门应当制定并执行政务数据安全传输策略和规程，采用安全可信通道或数据加密等安全控制措施，确保政务数据传输过程可信、可控。对关键网络传输链路、网络设备节点实行冗余建设，保障数据传输可靠性和网络传输服务可用性。

第十四条（数据存储安全） 市各政务部门应优先在全市统一的数据存储中心内进行政务数据存储，统一数据存储中心的安全性能、防护级别应与数据级别对应安全要求相匹配。

市各政务部门应制定、落实政务数据存储备份和恢复策略，建立相关灾备措施，定期进行灾难恢复演练。

第十五条（数据使用安全） 市各政务部门应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序使用政务数据，应采取管控措施确保政务数据使用目的合规，使用过程安

全可控、可溯源。

市各政务部门应建立数据处理活动相关平台系统的访问控制措施,为平台系统访问方分配完成职责所需的最小数据使用权限;应对数据安全管理人员、数据使用人员、安全审计人员的角色进行分离设置,涉及授权特定人员超权限处理数据的,由首席数据官审批和记录;应及时清除数据处理活动相关系统中无用账号、默认账号,杜绝多人共用同一系统账号的情况;应采取技术手段实施数据脱敏,对数据脱敏处理过程相应的操作进行记录,满足数据脱敏处理安全审计要求;应采用技术手段对违规使用数据的行为进行有效的识别、监控和预警。

第十六条（数据共享安全） 市政务服务数据管理局应建立统一规范、互联互通、安全可控的政务数据共享交换平台,推动政务数据开放利用。

市各政务部门应遵循公正、公平、便民的原则,按照规定及时、准确地共享政务数据,依法不予共享的除外。各政务部门间的政务数据共享交换,原则上应采用市政务服务数据管理局指定的政务数据共享交换平台,避免自行建立数据交换通道,政务数据共享交换全过程应在政务数据共享交换平台登记并进行日常监控。数据提供方在必要时可与数据需求方签订政务数据共享安全协议,约定政务数据共享过程的安全要求、处理方式、使用范围等,明确政务数据共享双方的权利、义务和责任。

第十七条（数据销毁安全） 市各政务部门对相关政务信息

系统进行测试、升级、改造时，应及时清理政务数据副本，防止政务数据泄露。

市各政务部门在政务数据共享交换、加工处理过程中产生的临时数据，在市各政务部门完成履行法定职责的范围内工作且不再符合法律、行政法规规定的使用政务数据条件和程序时，应予以销毁。

第十八条（云上数据安全） 市各政务部门将政务信息系统部署到政务云后，应按照“系统管理责任不变，数据归属关系不变，安全标准不降低，政务数据不出境”的原则，开展政务信息系统和政务数据的安全管理。

市政务服务数据管理局负责市政务云的数据安全管理与安全防护建设，并对市政务云的政务信息系统和政务数据提供基础性安全技术保障。

市政务服务数据管理局负责制定市政务云的政务信息系统和政务数据安全要求，建立政务信息系统和政务数据的准入机制，并会同网络安全和政务数据相关主管部门监督和检查市政务云的政务数据安全情况。

第十九条（风险评估） 市各政务部门应配合上级及市政务服务数据管理局对政务数据处理活动定期开展数据安全风险评估，明确政务数据处理活动面临的数据安全风险及其应对措施等，形成数据安全风险评估报告，及时整改数据安全风险评估中发现的问题。

第二十条（应急处置） 市各政务部门应建立数据安全应急处置机制，制定政务数据安全事件应急处置预案，发生数据安全事件时启动数据安全应急预案，采取相应的应急处置措施，消除安全隐患，防止危害扩大。

市各政务部门应根据数据安全事件应急预案制定演练计划，并定期组织应急演练，保存演练记录，针对演练中发现的问题，应立即整改。

第二十一条（事件通报） 市各政务部门应建立政务数据安全事件通报机制，开展数据安全事件通报工作，按照规定程序向市政务服务数据管理局通报有关情况，不得瞒报、漏报、谎报、迟报和推诿责任。

第二十二条（供应链审查评估） 市各政务部门应选用符合国家有关规定、安全可控的信息技术产品和服务，审查评估其对政务数据安全影响，并将审查评估结果作为项目立项的必备材料。

第二十三条（委托和外包管理） 市各政务部门委托他人建设和维护政务信息系统，存储和加工政务数据，应当对受托方进行严格的资格审查，以确保受托方符合相关要求。

市各政务部门应建立政务数据外包或委托服务安全管理机制，与受托方签订安全保密协议，监督受托方履行政务数据安全保护义务，受托方不得擅自留存、使用、泄露或者向他人提供政务数据。

第二十四条（教育培训） 市各政务部门首席数据官应推动

建立政务数据安全培训机制，定期开展数据安全意识宣贯培训、数据安全专项技能提升培训，营造数据安全氛围，助力数据安全保障工作落地。

市各政务部门应制定数据安全培训计划，并对培训计划定期审核和更新。每年应至少开展一次数据安全培训，培训结束后对培训效果进行评定、记录和归档。

第二十五条（经费保障） 市各政务部门应建立政务数据安全经费保障机制，将政务数据安全经费纳入本部门年度部门预算，保障政务数据安全工作开展。

第四章 监督管理

第二十六条（监督管理统筹） 市政务服务数据管理局会同市委网信办、市委机要和保密局、市公安局等网络安全和政务数据主管部门，统筹制定政务数据安全监督检查制度，市政务服务数据管理局协调指导市各政务部门开展政务数据安全监督检查。

第二十七条（监督管理配合） 市各政务部门应依照国家和行业有关规定，配合开展政务数据安全监督检查，开放相关网络和数据访问权限，确定政务数据安全监督检查的重点内容和时间安排，记录监督检查结果。

市政务服务数据管理局、市委网信办、市委机要和保密局、市公安局在履行数据安全监督检查职责中，发现政务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责令整改，

情节严重的可对相关政务数据、政务信息系统进行下线处理。对监督检查中发现的失泄密隐患,应立即向保密行政管理部门报告;对监督检查中发现的违法行为,应立即制止;对发生重大及以上政务数据安全事件的单位,根据《中华人民共和国数据安全法》《江门市电子政务外网网络安全管理实施细则》等相关规定,交由有关部门依法处理。

市各政务部门应在市政务服务数据管理局指导下进行整改,消除隐患。

第二十八条（主管部门法律责任） 市政务服务数据管理局、市委网信办、市委机要和保密局、市公安局等网络安全和政务数据主管部门工作人员不依法履行监督检查职责的,根据《中华人民共和国数据安全法》《江门市电子政务外网网络安全管理实施细则》等相关规定处理。

第二十九条（侵害合法利益的法律责任） 违反本办法规定,使自然人、法人或者非法人组织的合法权益受到侵害的,依法承担民事责任。构成犯罪的,依法追究刑事责任。

第五章 附 则

第三十条 本办法由市政务服务数据管理局、市委网信办、市委机要和保密局、市公安局依职能负责解释。

第三十一条 本办法自印发之日起施行。

公开方式：依申请公开

江门市政务服务数据管理局办公室

2021 年 10 月 14 日印发
