附件

广东省公共数据安全管理办法
（二次征求意见稿）

第一章 总则

**第一条（目的依据）** 为了规范公共数据处理活动，保障公共数据安全，促进数据资源有序开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，依据《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》《广东省公共数据管理办法》等相关法律、法规、规章的规定，结合本省实际，制定本办法。

**第二条（适用范围）** 本省行政区域内行政机关以及具有公共事务管理和公共服务职能的组织（以下统称“公共管理和服务机构”）开展公共数据处理活动及其安全监管，适用本办法。

涉及国家秘密、商业秘密、个人信息的，按照相关法律、法规、规章的规定执行。

**第三条（基本原则）** 公共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，保障公共数据依法开放、共享和开发利用。

**第四条（组织领导）** 县级以上人民政府负责组织领导本行政区域内公共数据安全管理工作，协调解决与公共数据安全管理有关的重大问题。

**第五条（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、本领域公共数据安全监管职责。

网信、保密、国家安全、密码管理、通信管理、公安、审计等主管部门按照本办法和有关法律、法规、规章的规定，在各自职责范围内承担公共数据安全监管职责。

各级公共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公共数据安全管理工作。

**第六条（公共管理和服务机构职责）** 公共管理和服务机构是本机构公共数据安全管理的责任主体，负责下列工作：

（一）明确公共数据安全管理的目标、制度、数据安全责任人和管理机构；

（二）按照相关法律、法规、规章的要求编制本机构的公共数据资源目录，加强数据保护；

（三）采取措施保障公共数据安全，加强安全管理；

（四）法律、法规、规章规定的其他公共数据安全管理职责。

**第七条（适老适残等无障碍公共服务）** 公共管理和服务机构提供智能化公共服务，应当充分考虑老年人、残疾人等群体的需求，避免以数据安全为由对群众享受公共服务造成障碍。

第二章 基础制度体系

**第八条（登记备案制度）** 省公共数据主管部门应当建立承载公共数据处理活动相关平台或者系统的登记备案制度，组织公共管理和服务机构备案公共数据安全保护情况，内容包括数据安全负责人、管理机构、数据信息、平台或者系统信息、数据安全保障情况、数据安全评估情况、数据安全审计情况、等级保护情况、密码应用情况等。

因承载公共数据处理活动相关平台或者系统关闭，或者发生较大变更，可能影响公共数据安全保护的，公共管理和服务机构应当自变化之日起15个工作日内申请登记备案撤销或者变更。

**第九条（数据分类分级规则）** 省公共数据主管部门牵头制定公共数据分类分级指南，明确分类分级的原则和规则等，特别是重要数据、核心数据的识别及分级保护规则。

地级以上市的公共数据主管部门应当根据国家和省公共数据分类分级相关规定，增补本地公共数据的分类分级规则。

行业主管部门应当根据国家、省、地级以上市公共数据分类分级有关规定，增补本行业、本领域公共数据的分类分级规则。

**第十条（数据分级安全防护）** 公共管理和服务机构应当按照分类分级规则，建立健全本机构公共数据分类分级管理制度，采取数据安全防护措施，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。不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护。

**第十一条（等级保护制度和商用密码应用）** 公共管理和服务机构应当按照国家网络安全等级保护制度、商用密码应用要求，采取数据脱敏、加密保护、安全认证等安全保护措施，保障公共数据安全。

**第十二条（纠错机制）** 数源部门对所采集公共数据的真实性、准确性、完整性负责。用数单位发现公共数据不真实、不准确、不完整或者不同部门提供的数据不一致的，应当及时通过省政务大数据中心或者直接反馈至数源部门。数源部门应当在约定的期限内予以核实，并及时更正、补充。

**第十三条（删除机制）** 有下列情形之一的，用数单位应当主动删除公共数据；用数单位未删除的，数源部门有权要求限期删除：

（一）公共数据处理目的已实现、无法实现或者为实现公共数据处理目的不再必要；

（二）用数单位停止履行职能或者提供服务；

（三）公共数据保存期限已届满；

（四）用数单位违反法律、法规、规章或者违反约定处理公共数据；

（五）法律、法规、规章规定的其他情形。

法律、法规、规章另有规定的，或者删除公共数据从技术上难以实现的，用数单位应当停止除存储和采取必要的安全保护措施之外的处理。

第三章 全生命周期数据安全管理

**第十四条（数据收集安全）** 数源部门开展公共数据收集活动时，应当明确收集的目的、范围、用途、渠道等，保证公共数据收集合法、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。

**第十五条（数据存储安全）** 开展公共数据存储活动时，应当根据需要采取脱敏、加密、校验等措施，保障公共数据的存储安全。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。

应当依据法律、法规、规章的规定或者约定的方式和期限存储数据。超过存储期限的数据，应当利用不可恢复手段及时清除。

**第十六条（数据使用加工安全）** 开展公共数据使用加工活动时，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加工数据，应当采取管控措施确保数据使用加工合规，过程安全可控、可溯源。使用加工重要数据和核心数据的，还应当加强访问控制，建立登记、审批机制并留存记录。

利用数据挖掘、关联分析等技术手段开展加工处理活动时，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。利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。

在使用加工过程中，不得超出合理范围使用，不得滥用公共数据侵犯公共利益或者他人合法权益。

**第十七条（数据传输安全）** 开展公共数据传输活动时，应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。公共管理和服务机构原则上应当通过省政务大数据中心传输公共数据，数据传输应当采取校验技术、密码技术、安全传输通道等措施，保障公共数据传输过程可信、可控。因特殊情况不通过省政务大数据中心传输公共数据的，应当采取必要安全技术措施保障数据传输安全。

**第十八条（数据提供安全）** 数源部门向省政务大数据中心提供公共数据，省政务大数据中心向用数单位提供公共数据，或者数源部门向用数单位直接提供公共数据时，应当明确公共数据提供的范围、数量、条件、程序等。

用数单位应当明确告知数源部门提供数据的范围、使用方式、时限、用途以及相应的安全保护措施、违约责任等。数源部门有权对用数单位的数据安全保护能力进行核实，必要时与用数单位签订单独的数据安全协议。

**第十九条（数据公开安全）** 公共数据公开前应当开展数据安全风险评估，明确公开数据的内容与种类、公开方式、公开范围、安全保障措施、可能的风险与影响范围等。涉及敏感个人信息、商业秘密信息的，以及可能对公共利益或者国家安全产生重大影响的，不得公开，法律、法规、规章另有规定的除外。

开展公共数据公开活动时，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。

第四章 数据安全支撑保障

**第二十条（集中统一风险评估、报告、信息共享、监测预警机制）** 公共数据主管部门根据国家统一部署和法律、法规、规章的相关规定，建立数据安全风险评估、报告、信息共享、监测预警机制，加强数据安全风险信息的获取、分析、研判、预警工作。

**第二十一条（风险监测及评估）** 公共管理和服务机构应当加强风险监测，依法定期开展数据安全评估，及时整改数据安全评估发现的问题，排查安全隐患，采取必要的措施防范数据安全风险。数据安全评估可与关键信息基础设施安全检测评估、网络安全等级保护测评、商用密码应用安全性评估相衔接，避免重复评估、测评。

**第二十二条（应急处置）** 各行业、各领域主管部门应当制定公共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。公共管理和服务机构应当制定本单位公共数据安全事件应急预案。发生公共数据安全事件时，公共管理和服务机构应当按照应急预案及时开展应急处置；事件处置完成后，应当在规定期限内形成总结报告，报送各行业、各领域主管部门；涉及重要数据和核心数据的数据安全事件，还应当及时向公共数据主管部门和其他有关主管部门报告应急处置进展情况。

公共管理和服务机构应当根据应急预案定期开展应急演练，保存演练记录，针对演练中发现的问题，应当立即进行整改。

**第二十三条（安全审计）** 公共管理和服务机构在公共数据处理过程中，应当记录全生命周期数据处理、权限管理、配置管理等日志，并对异常操作行为进行监控和告警，保障重要操作行为可溯源。日志留存时间不少于六个月，并定期进行安全审计，形成审计报告。公共管理和服务机构应当配合有关主管部门组织的数据安全审计活动。

**第二十四条（委托安全）** 公共管理和服务机构委托他人建设、维护信息系统或者存储、加工数据，应当对受托方的数据安全保护能力、资质进行核实，确保符合国家、行业主管部门的相关要求，相关安全责任不随委托关系转移。委托方应当建立数据外包或者委托服务安全管理机制，与受托方签订安全保密协议，监督并定期检查受托方依照法律、法规、规章的规定和合同约定履行数据安全保护义务的情况。受托方应当依照法律、法规、规章的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露、销毁或者向他人提供公共数据。

**第二十五条（人员管理）** 公共管理和服务机构应当加强人员管理，明确在人员录用、人员培训、人员考核、保密协议、离岗离职、外部人员管理等方面的管理规定并严格落实。委托开展公共数据处理活动的，委托方应当对受托方加强监督管理，受托方应当与相关人员签订保密协议，做好人员背景调查，严格实施权限管理，定期进行人员活动审查。

第五章 监督与法律责任

**第二十六条（通报与监督检查）** 各级公共数据主管部门应当建立健全数据安全监测预警和信息通报制度，会同同级网信、密码、公安、通信管理等相关监管部门开展公共数据安全检查，并按照规定向同级网信、公安、保密等监管部门报送数据安全监测预警、数据安全事件、数据安全漏洞等信息。

**第二十七条（公共数据主管部门责任）** 公共数据主管部门不履行或者不正确履行本办法规定职责的，由本级人民政府或者上级主管部门责令改正；拒不改正或者情节严重的，由有权机关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。

**第二十八条（其他主管部门监管责任）** 网信、保密、国家安全、密码管理、通信管理、公安、审计、工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门未按照规定履行数据安全监督管理职责的，由本级人民政府或者上级主管部门责令改正；拒不改正或者情节严重的，由有权机关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（公共管理和服务机构责任）** 公共管理和服务机构违反本办法规定，有下列行为之一的，由本级人民政府或者上级主管部门责令改正；拒不改正或者情节严重的，由有权机关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：

（一）未制定公共数据安全管理的目标、制度，未落实数据安全责任人和管理机构的；

（二）未按照规定编制、更新、报送公共数据资源目录的，向本级公共数据主管部门提供的数据和本机构所掌握的数据不一致或者不符合有关规范、无法使用的；

（三）未采取有效措施保障公共数据安全，存在安全隐患或者发生公共数据泄露、篡改、未授权访问等安全事件的。

（四）其他违反法律、法规、规章规定的行为。

**第三十条（投诉举报）** 自然人、法人和非法人组织有权对违反本办法规定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，应当对投诉、举报人的个人信息予以保密，保护投诉、举报人的合法权益。

第六章 附则

**第三十一条（概念界定）** 本办法下列用语的含义：

（一）公共数据，是指各级公共管理和服务机构，在依法履行职责、提供公共服务过程中制作或者获取的，以电子或者非电子形式对信息的记录。

（二）公共数据处理，包括公共数据的收集、存储、使用、加工、传输、提供、公开等。

（三）公共数据安全，是指通过采取必要措施，确保公共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）数源部门，是指根据法律、法规、规章确定的某一类公共数据的法定采集部门。

（五）省政务大数据中心，是指在“数字政府”改革模式下，集约建设的省市一体化政务大数据中心，分为省级节点和地级以上市分节点，是承载数据汇聚、共享、分析等功能的载体。

**第三十二条（实施时间）** 本办法自2022年 月 日起实施，试行3年。