柳州市政务数据安全管理实施细则

第一章 总 则

第一条 为加强柳州市政务数据安全管理，建立健全政务数据一体安全保障体系，预防政务数据安全事件发生，依据《中华人民共和国网络安全法》、《广西政务数据安全管理办法》、《中共柳州市委办公室 柳州市人民政府办公室关于印发<柳州市政务数据资源管理与应用改革实施方案>的通知》（柳办发〔2020〕4号）等有关法律、文件，结合我市实际，制定本细则。

第二条 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，对政务数据安全和信息化工作实行统一协调、分级管理、分工负责。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，切实保障政务数据共享开放和融合应用安全。

第三条 政务数据安全实行“一把手负责制”，各级各部门对本级本部门的政务数据安全负有主体责任，主要负责人是政务数据安全的第一责任人，各级大数据管理部门负有监督管理责任。

第四条 本细则所称政务数据，是指各级各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非涉密数据资源及其次生数据资源，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非涉密数据资源等。

第五条 本细则所称政务数据安全，是指通过采取必要措施，保障政务数据在采集、传输、存储、处理、应用以及废弃全生命周期过程中，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，防范对政务云、网络、信息系统和数据的攻击、入侵、干扰和非法使用以及意外事故，保障政务数据全生命周期的保密性、完整性、可用性等安全特性的能力。

第六条 本细则适用于柳州市政务数据安全管理工作。涉及国家秘密和工作秘密的数据安全管理，严格按照国家保密法律、法规和制度执行。

第二章 职责分工

第七条 市大数据发展局负责组织、指导和协调全市政务数据安全统筹管理工作，履行下列职责：

（一）依照国家、自治区网络安全法律、法规和标准，编制政务数据安全发展战略和总体规划，制定我市政务数据安全相关政策，指导各级各部门开展政务数据安全工作，研究解决涉及政务数据安全的重大事项，监督本级各部门政务数据安全规划和建设；

（二）牵头建设政务数据一体安全保障体系，构建一体安全保障机制；

（三）会同市委网信办、市公安局建立政务数据安全管理专家队伍，组织开展政务数据安全检查、风险评估和等级保护建设工作；

（四）会同市委网信办、市公安局等有关网络安全主管部门建立政务数据安全监测预警、信息通报和应急处置等协同联动机制，通报政务数据安全信息，调查处理重大政务数据安全事件。

第八条 市信息化建设管理中心负责市本级政务数据安全防护体系建设，负责政务数据安全指导、监督工作，履行下列职责：

（一）指导市级各部门、重点行业的政务数据安全保障工作，开展政务数据安全培训；

（二）对政务数据调度使用的安全情况进行全流程监控，并提供技术支持；

（三）负责市本级电子政务外网、壮美广西·柳州市云和柳州市数据共享交换平台安全防护技术和管理体系建设及运维。建立应急管理和容灾备份机制，满足重要的政务数据同城、异地备份的需求；

（四）建立全市政务数据安全管理责任和评价考核制度，制定政务数据安全检查方案。

第九条 市直各部门负责本部门的政务数据安全工作，履行下列职责：

（一）根据国家、自治区政务数据安全的法律、法规，依照国家、自治区政务数据安全的规章与标准，编制政务数据安全工作计划，制定人员、资产、采购、外包、系统建设与运维、备份、应急等方面的政务数据安全管理工作制度；

（二）明确本部门负责政务数据安全管理工作的机构及政务数据安全员岗位职责，落实政务数据安全责任制；

（三）负责做好本部门所申请政务云服务的安全管理工作，以及维护好相关信息系统和政务数据的安全；

（四）采取技术措施、管理措施和其他必要措施，保障政务数据安全、稳定运行，有效应对政务数据安全事件，防范违法犯罪活动，维护政务数据的完整性、保密性和可用性；

（五）落实政务数据安全经费保障政策，全力支持建设和完善政务数据安全保障基础设施，同时积极开展政务数据安全等级保护建设、风险评估、安全自查、安全培训等工作，保障政务数据安全；

（六）建立政务数据安全信息通报机制，配合大数据管理部门进行政务数据安全检查和事件调查，对发现的问题进行整改。

第十条 各县（区）大数据管理部门负责辖区内政务数据安全监督管理工作，履行下列职责：

（一）依照国家、自治区、柳州市政务数据安全法律、法规、规章和标准，制定辖区内政务数据安全工作制度，指导、协调和监督辖区内各单位政务数据安全工作，并积极组织辖区内各单位开展政务数据安全培训工作；

（二）建立辖区内政务数据安全事件应急机制、数据安全投诉举报制度和通报制度，向本级网络安全主管部门通报辖区内各单位的政务数据安全信息，协助调查处理辖区内的政务数据安全事件，及时处置和报告数据安全事件，组织数据安全教育培训。组建信息安全应急处置小组，就各县区、各部门的应用系统、数据和网络及其它配套设施制定信息安全事件应急预案，每年至少组织一次信息安全应急演练。

第三章 安全管理

第十一条 各级各部门应建立政务数据安全培训机制，定期开展政务数据安全意识教育与政务数据设备、系统安全操作基础培训，对信息系统建设、运维人员和政务数据安全管理人员进行专项技能培训，培训计划和培训内容应具有针对性，应包括针对不同岗位工作的数据安全意识、数据安全管理和数据安全技能等方面。

第十二条 各级各部门应按照网络安全等级保护制度要求和技术标准，在现有系统基础上组织开展风险评估和等级保护定级备案工作，按照国家和行业有关规定进行等级保护测评，未达到安全保护等级标准要求的，应及时进行整改。同时，新建政务信息系统或者政务信息系统发生重大变更时，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措施。

第十三条 各级各部门应遵循统一领导、统筹规划、强化管理、使用高效、重在防范、全面审查的原则，建立政务数据安全信息通报机制，开展信息通报工作，按照规定程序向本级大数据管理部门和本级网络安全主管部门通报有关情况，不得瞒报、漏报、谎报、迟报和推诿责任。

第十四条 各级各部门选用的信息技术产品和服务应符合国家有关规定，采购的数据安全产品和服务应经过国家认证。

第十五条 涉及政务数据技术外包服务的，应建立安全管理相关机制，确保外包服务安全可靠。

第十六条 各级各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，确保政务数据安全工作能够有序开展。

第十七条 各级各部门有暂时保留的数据中心的，应依照网络安全相关标准要求，完善数据中心基础设施安全建设。建立健全数据中心安全管理制度，加强日常检查和管理。

第十八条 各级政务外网管理单位应按照“同步规划、同步建设、同步运营”的原则，加强电子政务外网安全防护的规划、建设和日常保障工作。会同本级安全主管部门组织开展网络安全监测、检查、处置、风险评估和应急演练。严格控制PC终端、移动式设备接入、无线接入等网络接入行为，明确接入方式、访问控制、身份鉴别、安全审计等措施要求，形成网络接入日志并定期审计。

第十九条 各单位将信息系统部署到壮美广西·柳州市云后，应按照“系统管理责任不变，安全标准不降低，敏感信息不出境”的原则，负责信息系统和数据资源的安全管理，完善本单位信息系统和数据资源安全防护和管理体系建设。市信息化建设管理中心和各县区大数据管理部门协助做好相关工作。

各级大数据管理部门定期组织开展信息系统安全检查工作，对发现的安全风险问题及时督促相关单位限期整改，并定期通报安全状况。

各级大数据管理部门与政务云服务使用单位签订保密协议，未经使用单位授权，不得访问、修改、披露、利用、转让、销毁服务使用单位数据资源。

第二十条 各级各部门应建立信息系统安全防护管理体系，加强对服务器上的应用、服务、端口等的安全管理，系统账号按照“最小权限”原则进行分权分域管理，定期更新恶意代码特征库及系统补丁，定期实施漏洞扫描、恶意代码检测和人工渗透测试，并对存在的安全隐患进行及时加固，建立和完善密码保障体系，提升密码安全防护能力。

建立政务信息系统接入审查机制，在接入电子政务外网前应对接入方案进行审核、风险扫描和安全评估，确认达到国家、自治区、柳州市政务数据安全要求并签订安全协议后方可授权接入电子政务外网。各县区大数据管理部门负责接入审查工作，各部门协助做好相关工作。

建立政务信息系统上云审查机制，在政务信息系统管理单位完成系统部署上云后，由政务云管理单位组织安全评估，评估通过后方可上线运行。

建立健全政务信息安全运行、维护管理制度和人员队伍，设置专职信息安全人员。信息安全人员应通过市信息化主管部门组织的信息安全培训和考核，持证上岗。涉密信息系统的人员管理遵循保密工作主管部门有关规定。

第二十一条 各政府网站主办单位应提高信息安全防护能力，至少每季度对本部门政府网站信息内容开展巡查抽检。定期组织开展网站业务培训，把提升网上履职能力作为培训内容，不断提高知网、懂网、用网的意识和水平。指定专人负责政府网站信息内容和安全运行，明确栏目责任人，严格审校流程，加强内容审核和保密审查。建立24小时值班制度，及时处理突发事件，编辑、审核和发布相关稿件。及时发现问题、纠正错漏并作好记录。

第二十二条 政务数据安全管理遵循“谁提供、谁负责，谁流转、谁负责，谁使用、谁负责”的原则。各级各部门应建立政务数据资源全生命周期安全防护体系，政务数据实施分级分类管理。实行资产登记，编制资产清单，明确资产管理责任部门与人员，定期对资产进行一致性检查并保留检查记录。

明确政务数据安全责任部门及责任人，制定政务数据采集、传输、存储、使用、共享、销毁等制度及规范，加强身份与权限管理、数据保护与审计，利用数据防泄漏、数据加密、数据脱敏、数据恢复等技术，保障政务数据全生命周期安全。

第二十三条 各级各部门应制定终端计算机管理制度，严格执行终端计算机的安全管理，采取集中管控、用户识别、访问控制、安全审计、病毒防御、补丁修复等技术防护措施，防止病毒入侵，数据泄露。

第二十四条 各级各部门应制定移动存储介质的管理机制，防止移动存储介质在不同网络区域之间使用时造成恶意代码传播、数据泄露或损坏。

第二十五条 各级各部门应制定政务数据安全事件应急处置预案，定期开展应急演练，针对演练中发现的问题，应立即进行整改，并按照规定程序进行通报。并对演练情况进行总结，不断完善政务数据安全事件处置工作预案。

第二十六条 各级各部门应制定自然人、法人和非法人组织数据保护制度，对在提供服务过程中收集、使用的自然人、法人和非法人组织数据，应采取相应措施严格保护，不得私自泄露、篡改或者毁损，不得非法向他人提供。

收集、使用自然人、法人和非法人组织数据，应遵循合法、正当、必要的原则，不得收集与其提供的服务无关的自然人、法人和非法人组织数据，不得违反法律、法规的规定收集、使用和向第三方提供自然人、法人和非法人组织数据。将数据转移或委托给其他组织或机构使用的，应与该组织或机构签订数据保护协议，明确数据使用范围和保护责任。涉及敏感数据的，需脱敏后方可应用。

当发生自然人、法人和非法人组织数据安全事件发生后或风险明显加大时，各级各部门应立即启动应急预案，采取相应措施防止危害扩大，保存相关记录，按照规定及时向本级大数据管理部门和网信、公安等部门报告。

第四章 监督管理

第二十七条 各级大数据管理部门应依照国家、自治区要求，实行政务数据安全年度监督检查和专项监督检查制度，将政务数据安全监督检查工作列入年度计划，并会同本级网络安全管理部门进行政务数据安全监督检查。

第二十八条 各级大数据管理部门应依照国家和行业有关规定，确定政务数据安全年度监督检查重点、内容和时间安排，通知辖区内各单位。

第二十九条 各级大数据管理部门在年度或专项监督检查中应详细记录监督检查情况，并提出处理意见，被监督检查单位根据处理意见进行整改。

第三十条 各级大数据管理部门对监督检查中发现的重大安全隐患，应责令有关单位立即排除；对监督检查中发现的安全管理缺陷或安全隐患，应向有关单位提出限期整改要求，并向本级安全主管部门报告；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，并提请公安部门依法查处。

第三十一条 被检查单位应配合监督检查，按照监督检查要求开展自查，对发现的问题进行整改后，将自查结果和整改情况上报组织监督检查的大数据管理部门。大数据管理部门持续跟进整改情况组织各有关单位进行复检，确保不再出现类似问题。

第三十二条 政务数据安全保障工作实行一票否决制，对发生政务数据重大及以上安全事件的单位，取消本年度政务信息化相关评优评奖资格，并按照绩效管理相关规定扣除相应绩效分数。

第三十三条 各级各部门违反本细则规定的，由各级大数据管理部门责令限期改正，逾期未改正的，将进行通报并在相关考核中扣分；拒不改正或者造成严重后果的，对责任单位主要负责人进行约谈。

第三十四条 各级大数据管理部门工作人员不依法履行监督检查职责，或者有玩忽职守、滥用职权、徇私舞弊行为，尚不构成犯罪的，由政府管理机关依法予以行政处分。构成犯罪的，移交司法机关处理。

第三十五条 违反本细则规定，使自然人、法人或者非法人组织的合法利益受到侵害的，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

第三十六条 本细则由柳州市大数据发展局负责解释。

第三十七条 本细则自发布之日起正式实施。