重庆市电子政务云平台安全管理办法（试行）

第一章 总 则

第一条 为规范重庆市电子政务云平台（以下简称政务云平台）安全管理，切实保障政务云平台安全稳定运行，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》《中华人民共和国密码法》以及《重庆市政务数据资源管理暂行办法》《重庆市电子政务云平台管理暂行办法》等规定，制定本办法。

第二条 政务云平台的安全建设、服务应用、运行维护及其相关安全管理工作，适用本办法。

第三条 本办法所称政务云平台，是指承载于重庆市电子政务外网和互联网，为全市非涉密政务信息化建设（含灾备）统一提供物理空间、计算、存储、安全、支撑软件等基础资源和运行保障服务的公共服务平台。

本办法所称云租户，是指租用政务云平台提供的服务开展信息化建设、运维的用户单位。

第四条 政务云平台安全管理工作应当遵循统筹规划、规范有序、防患未然、确保安全的基本原则。

政务云平台的建设、运行维护、使用应当遵守国家的法律法规，任何单位和个人不得利用政务云平台侵犯国家、集体利益以及公民合法权益，不得利用政务云平台从事违法犯罪活动。

第五条 市大数据主管部门统筹政务云平台的安全管理工作，组织制定安全管理制度，协调、指导、监督政务云服务商做好政务云平台的安全管理工作。

市网信部门负责统筹协调政务云平台网络安全工作和相关监督管理工作。市公安部门负责指导、监督本区域政务云平台的网络安全等级保护和关键信息基础设施保护工作，实施网络安全保卫和打击网络违法犯罪。市密码管理部门、市电信主管部门、市电子政务外网主管部门和其他有关机关依照网络安全、数据安全、密码管理有关法律、行政法规，在各自职责范围内负责政务云平台网络安全保护和监督管理工作。

第六条 按照“谁建设、谁负责，谁拥有、谁负责，谁运行、谁负责”的原则，云租户负责部署至政务云平台的信息系统及其数据资源的安全管理工作；政务云服务商负责政务云平台物理环境、计算、存储等基础设施（资源）及其服务的安全管理工作，协助云租户开展信息系统及其数据资源的安全管理工作，接受云租户的网络安全监管。

政务云服务商应当协助各云租户加强对信息系统及其数据资源的安全管理工作。

第二章 基础设施安全

第七条 政务云平台应当保证安全技术措施同步规划、同步建设、同步使用，确保其具有支持业务稳定、持续运行的性能和安全防护能力。

政务云平台安全防护措施的规划、设计、建设、维护等应当符合关键信息基础设施保护、网络安全等级保护、密码应用等相关要求。

政务云平台应当依法开展网络安全等级保护定级备案工作，备案及其测评结果应当及时向市大数据主管部门报备。

第八条 政务云服务商应当及时将使用政务云平台的云租户情况向市网信部门、市公安部门、市国安部门、市大数据主管部门报备。

云租户情况发生变化的，应当在发生变化之日起2日内将相应的变化情况向市网信部门、市公安部门、市国安部门、市大数据主管部门报备。

第九条 政务云平台应当按照《云计算服务安全评估办法》及时通过云计算服务安全评估。安全评估未通过或者已过有效期且未开展复评的，不予通过验收。

第十条 政务云平台的互联网区与政务外网区之间、业务区与管理区之间、各云租户之间、云主机与物理主机之间等应当采取物理和逻辑控制并用的隔离措施，确保政务云平台的边界安全。

政务云平台应当采取边界防护、访问控制、入侵防范、安全审计、可信验证、恶意代码和垃圾邮件防范等方式方法，加强政务云区域边界、云租户、云主机的安全防护工作。

第十一条 政务云平台机房的设计和建设应当满足数据中心建设相关规范。政务云服务商应当加强对政务云平台机房的监控，严格限制人员与运行中的设备进行物理接触，保证政务云平台机房内基础设施安全。

因开展安全检查、设备维护等确需物理接触的，政务云服务商应当书面授权，并登记形成台账。

第十二条 政务云平台不得使用可能涉及危害公共安全或国家安全的设施设备。

政务云平台的设施设备为政务云平台专用，不得转卖、抵押、毁坏或者用作其他用途。需要维护、维修或者检测政务云平台设施设备的，应当严格按照程序和规范进行操作。需要处置政务云平台设施设备的，应当事先经过专业的安全技术处理。

第十三条 政务云平台应当使用符合国家法律法规和有关规范的网络、密码产品、技术及服务，积极应用安全可靠的技术、产品及服务。适用关键信息基础设施安全保护要求的，还应当按照相关规定加强供应链安全管理。

政务云服务商应当加强政务云平台供应链安全审核及管理，评估可能存在的安全风险，并采取相应的预防、管控措施。

第三章 数据与应用安全

第十四条 政务云平台应当按照国家相关规范建立必要的容灾备份设施和机制，确保具备有效的灾难恢复能力和业务连续性保障能力。

政务云平台应当接入两家以上基础电信运营商的网络，保障网络冗余。

政务云平台应当具备向云租户提供数据和备份存储的位置查询，以及数据备份操作记录的功能。

第十五条 政务云服务商应当对所提供的云服务进行安全保密承诺，采取有效管理和技术措施，确保信息系统和数据的保密性、完整性、可用性，未经授权不得访问、修改、留存、披露、利用、转让、销毁云租户的数据。政务云服务商或者其他服务商对云租户的虚拟机或者数据进行操作时，应当先行获得相关云租户的授权，并保留对数据的操作记录。

云租户应当按照网络安全、数据安全有关要求，做好数据采集、数据加密、数据脱敏、数据共享与开放、数据销毁等工作，采取数据分类分级保护措施，并对重要信息系统、重要数据进行容灾备份。

不同云租户存储在政务云平台上的数据应当实行安全隔离，防止被非授权访问或非法获取。政务云服务商应当提供支撑安全隔离所需的环境或者资源。

第十六条 政务云服务商应当建立信息系统迁移规范，明确云租户迁入、迁出流程及步骤。迁移前，云租户应当与政务云服务商共同制定信息系统安全迁移实施方案，采取相关安全措施，保障信息系统安全迁移。

第十七条 政务云服务商应当将对云租户的虚拟机、镜像、快照的操作日志记录提供给云租户进行审计，并积极配合网信部门、公安部门、大数据主管部门等单位对政务云平台的远程操作管理、资源调度、弹性扩展等行为进行审计。

政务云服务商应当根据网络安全管理要求和云租户日志管理需求，制定审计事项清单，明确审计记录内容，妥善保存审计记录，定期对审计记录进行分析和审查。任何单位和个人不得非法对审计记录进行未授权访问、篡改或者删除。

第四章 运维安全

第十八条 政务云服务商应当配备专门的安全管理机构，组建合理规模的本地化运维团队，及时、有效响应安全运维和故障恢复需求。

政务云服务商应当建立安全运维管理制度，完善安全操作规范和工作流程，加强日常监督和考核，确保各项安全管理措施有效落实。

第十九条 政务云服务商应当将安全管理团队名单向市大数据主管部门和所服务的云租户报备，加强录用审查和离岗管理。安全团队人员需要变动的，政务云服务商应当提前30日将变动情况向市大数据主管部门和相关云租户报备。

市大数据主管部门、政务云服务商应当对政务云平台安全管理团队成员和关键岗位人员开展必要的背景调查。

政务云服务商应当定期对人员稳定性进行评估，评估可能存在的安全风险，并采取相应的预防、管控措施。

第二十条 政务云服务商应当依据网络安全等级保护相关要求，定期对政务云平台开展网络安全等级保护测评。

政务云服务商应当向云租户提供必要的安全服务和密码服务，支撑云租户开展信息系统网络安全等级保护测评和密码应用安全性评估。

政务云服务商和云租户应当对网络安全等级保护测评和密码应用安全性评估中发现的问题，认真开展安全建设、整改加固和运行监控。

第二十一条 政务云平台应当加强网络运行、访问的监测和控制，采取防范计算机病毒、网络攻击、网络侵入等危害网络安全行为的技术措施，监测、记录网络运行状态，并按规定留存相关的网络日志不少于6个月。

政务云服务商应当定期开展渗透测试、漏洞扫描和风险评估工作，原则上漏洞扫描不低于每月1次、经依法授权开展的渗透测试不低于每季度1次、风险评估不低于每年1次，及时对发现或者获知的政务云平台安全漏洞进行修复、处置，定期更新相关安全补丁，并开展相关有效性、兼容性测试。

政务云服务商应当按照市网信部门、市公安部门等要求，及时将政务云平台和云租户的安全数据、政务云平台网络核心资产数据等汇聚到指定的网络安全态势感知平台。

第二十二条 政务云服务商应当提升敏感信息监测能力，积极配合提供有效的网页篡改、非法信息发布等监测服务。

第二十三条 政务云服务商应当每日对政务云平台开展安全巡检，对相关设施设备和安全防护措施的可用性、有效性进行检查。政务云服务商还应当安排专职人员定期对安全设备的告警进行有效性分析，及时发现和处置安全隐患。

政务云服务商应当将相关的巡检、分析情况告知云租户，及时将安全风险、安全威胁披露给云租户，协助云租户做好安全防护工作。

第二十四条 政务云服务商可以向云租户开放访问控制策略的调整功能和权限。但是，云租户制定的访问控制策略不合理或者不按照规范调整访问控制策略导致的网络安全事故，由相关云租户自行承担责任和损失。

政务云服务商应当协助云租户配置合理有效的访问控制策略，并留存访问控制策略调整日志。

第五章 应急管理

第二十五条 政务云服务商应当定期开展安全培训，针对不同岗位设置不同的安全培训课程，并开展培训考试或者验证。培训内容应当包含自然灾害类、消防类、故障类、入侵类、病毒木马类、DDOS拒绝服务等应急内容。

第二十六条 政务云服务商应当制定政务云平台应急预案，并定期针对自然灾害类、消防类、故障类、入侵类、病毒木马类、DDOS拒绝服务等内容开展应急演练。演练频率不低于每年1次。

应急预案应当根据应急演练等情况不断进行修订，并向市网信部门、市公安部门、市国安部门、市大数据主管部门报备。

第二十七条 政务云服务商应当提供安全值守服务，支持电话值守、网上值守等响应方式。

在重要节日、重大活动等时期，政务云服务商还应当专门制定保障方案，采取24小时不间断的现场值守措施。

第二十八条 各云租户应当把应急值守纳入单位应急管理工作范畴，完善制度、明确责任，妥善做好部署至政务云平台的信息系统及其数据资源的应急值守工作。

政务云服务商应当积极协助各云租户做好应急值守工作。

第二十九条 政务云服务商在处置网络安全事件或者对政务云平台实施影响云租户业务连续性的操作时，应当事先通知云租户，并协助云租户采取相应的预防、处置措施。

云租户出现影响政务云平台安全稳定运行的事件时，政务云服务商应当及时通告云租户和相关主管部门，并暂时中断相关云服务，待安全事件处理完毕后再恢复服务。

第三十条 政务云平台网络安全事件应急处置按照国家、市网络安全事件应急管理相关规定执行。

政务云服务商和云租户应当按照相关规定，在2个小时内向网信部门、公安部门、大数据主管部门等报告政务云平台网络安全事件相关情况。

市大数据主管部门应当结合政务云平台监管的风险问题，定期实施典型事故预警，避免网络安全事件的发生。

第六章 监督管理

第三十一条 市发展改革部门、市财政部门、市大数据主管部门依据市级政务信息化项目管理职责分工，将政务云平台及相关信息系统的安全建设、整改、维护等内容纳入市级政务信息化项目审批（审核）、管理的重要内容，督促、指导政务云服务商和相关云租户提升安全管理能力。

第三十二条 市大数据主管部门应当会同市网信部门、市公安部门等，常态化对政务云平台的安全建设、安全运维、安全整改、应急值守等情况进行检查，采取技术手段对政务云平台安全风险进行动态监测。检查频率不低于每季度1次。

对检查中发现的安全风险问题，市大数据主管部门应当及时向政务云服务商通报，并督促政务云服务商进行整改。

市大数据主管部门可以委托第三方专业技术机构，对政务云服务商落实安全管理责任和措施、安全风险排查和整改、应急演练和值守等情况进行检查。

第三十三条 市大数据主管部门应当将政务云平台安全管理作为政务云服务验收和评价的重要内容，统筹开展验收和评价工作，督促政务云服务商改进服务。

政务云服务商应当定期将政务云平台云资源使用情况及网络安全运行保障情况书面向各云租户报告，保障云租户权益。报告提交频率不低于每月1次。

第三十四条 审计机关在政务信息化项目及其资金审计或者其他审计中，依法依规对政务云平台安全管理工作进行审计监督。

第三十五条 因政务云服务商技术、管理等原因，导致政务云平台发生重大网络安全事件的，市大数据主管部门和相关云租户应当依据合同约定，与政务云服务商解除服务合同，依法依规开展责任追究和损失追偿。政务云服务商退出服务时，应当完整返还数据资产，并保证数据满足相关可用性和持续性要求；应当继续保留相关网络日志不少于6个月，配合有关部门开展安全追溯工作。

各云租户与政务云服务商终止服务后，政务云服务商应当取消原服务资源访问权限，协助云租户做好相关数据、信息系统的迁移和下线工作，并经云租户确认后在7日内有效销毁数据。

第七章 附 则

第三十六条 市级各部门、各区县（自治县）大数据主管部门可以根据本办法，组织制定本部门、本区县（自治县）政务云平台的安全管理实施细则。

第三十七条 本办法自印发之日起执行。