包府办发〔2025〕77号

包头市人民政府办公室
关于印发包头市政务云安全管理办法的通知

各旗、县、区人民政府，稀土高新区管委会，市直各部门、单位：

经市人民政府同意，现将《包头市政务云安全管理办法》印发给你们，请结合实际认真贯彻落实。

2025年12月16日

（此件公开发布）

包头市政务云安全管理办法

第一章　总　则

第一条　为深入贯彻网络强国重要思想，全面落实《党委（党组）网络安全工作责任制实施办法》，进一步强化包头市政务云平台（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和承载的政务数据安全，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》、《中华人民共和国密码法》、《关键信息基础设施安全保护条例》（国令第 745 号）等法律法规及相关政策规定，以铸牢中华民族共同体意识为工作主线，结合包头市实际，制定本办法。

第二条　本办法适用于市本级政务云平台的使用、管理以及基于政务云平台部署的政务信息系统（以下简称云上政务信息系统）及其数据的安全管理。

政务云平台指依托云计算技术，整合计算、存储、网络、安全等资源，通过电子政务外网和互联网，为市本级非涉密政务信息系统提供统一基础设施及服务的云服务平台。

云服务商指通过公开招标等法定程序确定，提供政务云平台服务的具有相应资质和能力的服务机构。

云使用单位指依据本办法规定在政务云平台部署政务信息系统

的市本级财政预算单位。

第三条　在市委网信委领导下，市委网信办、市委国安办、市委保密机要局、市公安局、市行政审批政务服务与数据管理局等单位，按照各自工作职能协同对政务云平台进行安全监督，指导云服务商和云使用单位落实安全责任。

第四条　安全管理遵循“谁使用谁负责、谁建设谁负责、谁管理谁负责”的原则，清晰界定权责，强化分工协作。

（一）云使用单位负责本单位的云上政务信息系统及其数据安全、用户权限管理和日常安全防护工作。政务信息系统上云部署后，其安全管理责任主体、数据归属不随上云而转移。

（二）云服务商负责政务云平台资源层及所提供云服务的安全，提供基础安全技术支撑和平台级安全保障，配合开展安全检查、实网攻防、应急演练等工作。

（三）市行政审批政务服务与数据管理局所属事业单位市大数据中心，负责开展政务云平台安全检查、云上政务信息系统风险隐患通知通报、跟踪督促整改落实等工作。

第二章　安全管理

第五条　政务云平台安全管理

（一）政务云建设须安全可控。云服务商搭建的政务云平台硬件设备应符合国家关于信息技术应用创新和关键设备安全可控的相

关规定，并具备完善的业务连续性管理体系和灾备能力（含平台灾备、业务连续性保障等）。

（二）建立健全安全管理体系。政务云平台须通过国家云计算服务安全能力评估，每年开展网络安全等级保护测评、商用密码应用安全性评估，并在相关评估、测评报告出具后 15 个工作日内提交市大数据中心存档。

（三）建立健全运维管理制度。政务云平台原则上不支持进行远程运维操作；关键数据须每日备份，平台系统操作日志保存时间不得少于 6 个月。

（四）建立健全安全巡检制度。云服务商须每日对设备与系统状态进行巡检，对密码资源池的有效性进行验证，实施安全事件零报告制度；每月对政务云平台进行漏洞扫描、日志审计和安全态势分析，并向主管部门上报月度安全运行报告。

（五）强化供应链安全管理。云服务商对其分包业务、使用的开源软件、第三方组件等承担安全责任，须在使用或引入前进行安全风险评估，并签订安全协议。

（六）服务退出与数据清除机制。云服务商终止服务，应提前 90 天向主管部门提交申请，并积极配合云使用单位进行系统迁移；终止服务后，云服务商须彻底清除相关数据，并向主管部门报送数据清除报告。

第六条　政务云平台接入网络安全管理

（一）落实网络安全管理责任。政务云平台接入的外部网络安

全管理遵循“谁提供谁负责、谁使用谁负责”的原则，通信运营商须确保接入政务云平台的外部网络结构合理、网络畅通、网络设备运行稳定；网络使用单位须落实网络安全主体责任，建立并严格执行网络访问安全管理制度。

（二）强化网络边界安全防护。接入政务云平台的外部网络（如互联网、电子政务外网、部门专网）须由通信运营商和云服务商在网络边界部署防火墙、入侵防御等安全措施，通过防火墙实现网络对接。

（三）全面落实接口安全管理。云服务商须对接入政务云平台的每一个外部网络接口进行安全管理。

第七条　政务信息系统安全管理

（一）落实安全防护与灾备要求。政务信息系统上云，须部署安全防护措施（如防火墙、入侵检测系统 IDS/入侵防御系统 IPS、终端安全防护等），并使用符合国家密码管理要求的商用密码技术、产品和服务进行保护；云使用单位对其部署在政务云上的政务信息系统和数据资源，应同步落实系统和数据的本地及异地容灾备份。

（二）落实网络安全主体责任。云使用单位须按期对本单位部署的云上政务信息系统开展等级保护测评、渗透测试、安全风险评估、商用密码应用安全性评估等工作；须与系统承建单位、运维单位签订保密协议和安全责任书，清晰界定数据访问权限、操作规范和安全责任。

（三）建立健全安全访问管理制度。云使用单位须对本单位部

署的云上政务信息系统建立完善的安全访问管理制度，覆盖运维终端、关联终端、VPN 账号、零信任账号、各类管理账号、口令、操作行为等要素，明确专人负责管理，实施最小权限原则和操作审计。

（四）建立健全运维管理制度。云使用单位须制定并严格执行日常运维管理制度（含变更管理、配置管理、漏洞管理、陪同旁站制度等），及时修复漏洞、定期分析日志并进行安全加固，运维和管理操作日志保存时间不得少于 6 个月。

第八条　数据安全管理

（一）保障政务数据安全。云服务商须采取严格的技术和管理措施，禁止未经云使用单位授权访问、查看、复制、篡改、泄露、损毁或非法转移云上政务信息系统数据。

（二）落实数据分类分级与备份保护要求。云使用单位应严格执行国家数据分类分级保护制度及相关标准，落实数据安全保护责任。对云上政务信息系统涉及的重要数据和核心数据须进行识别、目录管理和重点保护，按相关要求实施容灾备份，备份策略（频率、保留周期）应满足业务恢复时效性和法律法规要求。

（三）严格遵守数据出境安全规定。涉及数据出境行为的，必须严格遵守《中华人民共和国数据安全法》、《数据出境安全评估办法》（国家互联网信息办公室令第 11 号）、《网络数据安全管理条例》等相关规定。

第九条　云上政务信息系统运维安全管理

（一）规范机房实地操作管理。信息系统运维人员进入政务云

机房实地操作，须执信息系统所属单位授权函，进行实名登记，操作全程须由云服务商工作人员陪同旁站。

（二）规范远程运维安全准入。云上政务信息系统进行远程运维，须由系统所属单位履行内部审批手续，进行实名登记并以最小权限向云服务商申请限时开通 VPN、零信任等安全通道进行操作。

（三）严格远程运维通道管理。VPN、零信任等远程运维账号及临时安全通道的开通，遵循“一次一用、单次有效”的原则；需长期开通相关通道的，须由系统所属单位向网络安全主管部门进行申请，经审核同意后，云服务商方可开通相关通道。

第十条　安全监测与应急管理

（一）强化安全监测与应急通报。云服务商须对政务云平台基础设施和平台层安全进行 7×24 小时监测预警；发现涉及云上政务信息系统的安全漏洞、隐患、攻击行为时，应当立即告知市大数据中心和涉事政务信息系统所属单位，并确保相关信息准确送达，同时提供必要的技术信息支持。

（二）严格安全隐患闭环管理。云使用单位须对其部署的云上政务信息系统进行网络和数据安全监测预警；在发现安全隐患或收到相关部门告知的安全隐患后，须立即启动响应，于 5 个工作日内完成漏洞修复、风险处置与整改工作，并书面反馈至预警部门，抄送市大数据中心。

（三）健全应急预案体系与演练机制。云服务商应制定政务云平台总体应急预案，并定期更新完善；各云使用单位应制定相应的

云上政务信息系统专项应急预案，并保持动态修订。云服务商每半年应牵头组织至少一次综合应急演练（涵盖网络攻击、数据泄露、系统故障、灾备切换等典型场景），各云使用单位需积极参与、协同配合。

（四）规范应急响应与事件报告流程。政务云平台发生《国家网络安全事件应急预案》定义的Ⅲ级（较大）及以上网络安全事件，云服务商须立即按照应急预案进行应急处置，并在确认事件后 30 分钟内向网络安全主管部门进行报告，持续通报进展，事后须提交详细的事件分析报告。

（五）强化事件应急响应与联动处置。云上政务信息系统发生《国家网络安全事件应急预案》定义的Ⅲ级（较大）及以上网络安全事件，云使用单位须立即按照应急预案进行应急处置，并在确认事件后 30 分钟内向网络安全主管部门进行报告，持续通报进展，事后须提交详细的事件分析报告。云服务商须全力配合云使用单位做好应急处置，控制影响范围、减少损失。

第三章　监督管理

第十一条　安全监管

（一）落实安全责任协议签署。政务信息系统上云前，云使用单位须与云服务商签订《包头市政务云平台安全责任协议》，清晰界定双方的安全管理职责与责任边界。未签订安全责任协议的系统禁

止接入政务云平台。

（二）严格上云系统安全准入核验。新上云政务信息系统正式运行前，市大数据中心须核验其《网络安全等级保护测评证书》、密码应用方案和相关安全检测报告（如安全测评报告、渗透测试报告等）。对未达到安全合规要求的政务信息系统，不得批准其进行互联网访问或对外进行数据交换。

（三）常态化开展安全调度与检查。市大数据中心每月开展政务云平台安全调度，每季度组织专项检查，及时通知通报云上政务信息系统风险隐患，并跟踪督促整改落实。

（四）建立退出机制。对存在重大安全隐患且无法整改或整改后仍不符合安全要求的云上政务信息系统，可暂停政务云服务或责令其限期退出政务云平台。

第十二条　责任追究

云服务商因违反相关网络和数据安全法律法规或本办法规定，导致发生《国家网络安全事件应急预案》定义的Ⅲ级（较大）及以上网络安全事件，由网络安全执法部门追究其法律责任；云使用单位网络和数据安全责任落实情况、隐患整改完成率及安全事件发生情况由市委网信办、市公安局等纳入年度网络安全考核。

第四章　附　则

第十三条　各旗县区、稀土高新区可参照本办法制定政务云安

全管理实施细则。

第十四条　为适应网络安全和信息技术发展，确保本办法的时效性与可操作性，市行政审批政务服务与数据管理局应跟踪国家法规政策及技术发展趋势，定期评估本办法实施效果，并按程序适时修订完善本办法。

第十五条　本办法自发布之日起实施，有效期五年。

抄送：市委办公室。
市人大常委会办公室、政协办公室。
市委网信办、市委国安办、市委保密机要局。

包头市人民政府办公室　　2025 年 12 月 18 日印发