任务书

一、项目背景或概况

2019 年 4 月，市经济信息化局印发了《北京市市级政务云管理办法》，市教委作为市级单位严格按照“上云为常态，不上云为例外”的原则，将现有信息系统逐步向政务云迁移。同年 7 月，市经济信息化局印发了《关于加快政务信息系统入云工作的函》，要求加快推进政务信息系统入云工作。其中的云基础资源（计算、存储、网络、远程管理等）由北京市数字教育中心统筹，安全服务由北京教育融媒体中心自行招标。

二、采购目标

本项目的总体目标是通过租用政务云平台服务，对北京教育融媒体中心融媒体平台的运行环境进行持续优化，提供可靠、稳定、安全的政务云服务，具体包括：

1、提供政务云安全类服务，包括安全服务和王键检测监测、审计服务及日常维护、应急响应等工作。

2、提供 7*24 运维保障，做好重大活动和节假日应急值守保障服务，确保各系统在政务云环境中可靠稳定运行。

3、服务期内，投标人须完成信息系统的日常运维和安全运维服务工作（包括但不限于：云平台服务、日常技术支持、系统日常维护、服务规范、安全及保密要求、响应的及时性），确保入云系统安全、

稳定的运行。

三、服务内容

（一） 云端抗 DDOS 服务

按照采购人的有关管理规定及应用系统的需求，根据流量提供云端抗 DDOS 服务，避免业务遭受拒绝服务攻击（攻击流量在 20G 以内）

（二） 云端 APT 防护服务

按照采购人的有关管理规定及应用系统的需求，对未知攻击威胁进行检测和防护，发现隐蔽威胁、木马后门等异常威胁。

（三） 主机杀毒服务

按照采购人的有关管理规定及应用系统的需求，对云主机进行定期的病毒查杀，杀毒软件集中控制，对网络性能无影响。

（四） 主机防护

按照采购人的有关管理规定及应用系统的需求，提供符合等保三级要求的主机权限管理及安全防护。

（五） 主机安全加固

按照采购人的有关管理规定及应用系统的需求，针对漏扫或等级测评结果对操作系统进行安全加固，用以解决等级测评结果中所显示的漏洞。

（六） 主机漏洞扫描

按照采购人的有关管理规定及应用系统的需求，为用户提供针对主机层面的安全扫描服务，并反馈相关结果。

（七） 主机日志分析

按照采购人的有关管理规定及应用系统的需求，对主机系统日志进行采集分析处理，发现各种安全威胁、异常行为事件。并定期为用户提供分析报告，协助用户进行整改工作。

（八） 数据库审计服务

按照采购人的有关管理规定及应用系统的需求，对所有用户的数据库操作进行审计，支持 Oracle、SQL-Server、DB2、MySQL 等数据库审计。

（九） 渗透测试服务

按照采购人的有关管理规定及应用系统的需求，提供渗透测试服务，主要依据安全专家已经掌握的安全漏洞信息，模拟黑客的真实攻击方法对系统和网络进行非破坏性质的攻击性测试，能够最大限度挖掘安全漏洞，提升系统抵御黑客攻击的能力。

（十） 运维服务

投标人提供的政务云环境应在安全等保三级基础上，按各业务系统具体安全需求，开展相应等保评估、检查、整改等工作。

1、服务规范

投标人须严格按照《北京市市级政务云管理办法》以及采购人制定的管理办法及流程等相关制度，开展标准化运维工作。

2、服务方式

投标人需利用监控系统或人工对机房环境、硬件设备及应用系统的运行情况进行 7*24 小时的不间断巡检监控，及时发现安全隐患，通知相关人员及时处理，并形成监控报告。

投标人负责设立技术支持热线，并安排专人值守，为运维工作提供 7*24 小时热线支持服务。投标人针对采购人要求的云平台运维服务相关内容，需指定专业技术能力较强的工程师，根据采购人要求配合开展相关维护服务。

3、安全及保密要求

投标人须严格遵守采购人的相关信息安全规定，不得利用系统维护服务时的便利将采购人数据及其他信息进行擅自修改或透漏给第三方。

4、响应的及时性

投标人应当提供高效的系统维护服务，有效防范系统风险，系统对应负责人 7*24 小时电话畅通，能够在系统发生除宕机外的其他故障问题时，能够协调人力资源在 1 小时内到达运维现场提供服务。系统发生宕机问题时，供应商应在 30 分钟内响应，在 4 个小时之内使系统恢复正常，故障处理完毕后提供相关系统宕机报告。

5、重点保障要求

投标人应具备完善的系统服务保障体系，配备足够的技术人员，在重大节假日、重大活动及业务高峰期内加大运维保障力度，保证期间系统平稳运行。

（十一） 迁移服务

由于目前业务系统属于生产系统，保障业务系统连续性是关键。如涉及跨云平台迁移，需在不中断业务的前提下，自合同生效之日起一周内完成全部系统迁移。供应商需具备类似项目经验，可根据业务特点制定应用系统迁移部署方案，配合用户完成系统迁移部署、运行和安全保障，最终保证现有业务系统可平滑迁移至中标单位云平台。具体要求如下：

根据采购人需求，完成应用系统的迁移部署，迁移过程中保证应用系统不中断。

五、运维团队要求

服务期内，投标人须设有 7×24 小时电话响应服务、具备运维团队，提供售后服务保障。团队成员应明确职责，架构清晰，岗位设置合理，且具备与本项相关的项目经验。

投标人须提供 1 名项目经理及若干名项目团队专职人员，为本项目提供服务。项目经理需按照采购人要求，承担云资源服务保障具体工作，技术支持人员要求如下：

项目经理具有信息系统项目管理师（高级）证书；

技术负责人具有 CISP 证书；

团队成员（除项目经理和技术负责人之外）具有 CISP 等证书。

六、商务要求

（一）服务地点

采购人指定地点。

（二）服务期限

自签订合同之日起至项目正式验收结束时止。

（三）验收服务标准

中标人所提供资源应满足招标文件及相关合同规定的要求。保证合同期内系统安全稳定运行，不因硬件故障导致服务中断 12 小时。服务期满后 30 个工作日开始对合同项目进行验收。中标人应当在采购人指定的验收日前向采购人提交验收报告。验收报告的内容包括但不限于，合同规定的各项服务清单，各系统设备运行情况。

七、保密要求

（1）中标人因承接本合同约定项目所知悉的该项目信息或采购人信息，以及在项目实施过程中所产生的与该项目有关的全部信息均为采购人的保密信息，中标人应按照采购人关于保密工作的相关要求，对上述保密信息承担保密义务。投标人须严格遵守信息安全规定，不

得利用系统维护服务时的便利对采购人数据及其他信息擅自修改或透漏给第三方。

（2）中标人应对上述保密信息予以妥善保存，并保证仅将其用于与完成本合 同项下约定项目实施有关的用途或目的。在缺少相关保密条款约定时，对上述保密信息,中标人应至少采取适用于对自己商业秘密进行保护的同等保护措施和审慎程度进行保密。

（3）中标人保证将保密信息的披露范围严格控制在直接从事该项目工作且因工作需要有必要知悉保密信息的工作人员范围内,对中标人非从事该项目的人员一律严格保密。

（4）中标人应保证在向其工作人员披露采购人的保密信息前，认真做好员工 的保密教育工作，明确告知其将知悉的为采购人的保密信息,并明确告知其需承担的保密义务及泄密所应承担的法律责任，并要求全体参与该项目的人员签署书面《保密协议》。

（5）任何时间内，一经采购人提出要求，中标人应按照采购人指示在收到采购人书面通知后 5 日内将含有保密信息的所有文件或其他资料归还采购人，且不得擅自复制留存。

（6）非经采购人特别授权，采购人向投标人提供的任何保密信息并不包括授予中标人该保密信息包含的任何专利权、商标权、著作权、商业秘密或其它类型的知识产权。