CMBJ-202602657

北京市海淀区数据局2026年度合同

合同名称	海淀区教育云国产化服务项目合同		
合同编码	20260703	承办部门	大数据中心

海淀区教育云国产化服务项目合同

项目名称：海淀区教育云国产化服务项目

甲　　方：北京市海淀区大数据中心

乙　　方：中国移动通信集团北京有限公司

合同编号：

签订地点：北京市海淀区

合同正文

依据《中华人民共和国民法典》以及国家其他有关法律法规的规定，甲、乙双方遵循平等自愿、诚实信用的原则，就乙方向甲方提供海淀区教育云平台服务事宜经协商达成一致意见，签订本合同，并共同遵守。

第一条 合同各方

甲方：北京市海淀区大数据中心

乙方：中国移动通信集团北京有限公司

第二条 合同术语定义、解释和适用范围

2.1 云计算服务：云计算服务是一种处理能力可弹性伸缩的计算服务，其管理方式比物理服务器更简单高效。云服务器帮助用户快速构建更稳定、安全的应用，降低开发运维的难度和整体IT成本，使用户能够更专注于核心业务创新。

2.2 海淀区教育云：甲方依托乙方提供的基础设施环境、资源以及服务部署专享的云平台，为海淀区教育领域提供云计算服务。

2.3 下列文件构成本合同的组成部分，应该认为是一个整体，彼此相互解释，相互补充。为便于解释，组成合同的多个文件的优先支配地位的次序如下：1.本合同及其变更、补充协议； 2.中标通知书；3.投标文件；4.招标文件；5.联合协议/分包意向协议（如有）；6. 技术培训方案及售后政策（如有）；7.有关技术文件、图纸（如有）；8. 国家法律、行政法规和规章制度规定或合同约定的作为合同组成部分的其他文件。

第三条 服务内容

本项目主要是甲方通过向乙方购买满足《国家电子政务外网标准－政务云安全防护要求（GW0013-2017）》和《北京市地方标准－政务云平台建设技术要求（DB11/T 2169-2023）》的教育云国产化服务，为海淀区教育信息系统提供基于国产技术架构的云计算服务，提供国产云主机、国产操作系统、国产数据库、国产中间件服务。

教育云国产化服务由私有云平台提供，不接受公有云形式，教育云平台分为教育网区和互联网区，其中教育网区和互联网区物理隔离，通过物理安全隔离交换系统实现两个区域间数据安全交换。两个区域需分别建设计算资源池、存储资源池、网络资源池和安全资源池等。

乙方向甲方提供的服务应满足以下要求：

3.1 专属机房服务要求

1）乙方在北京市海淀区辖区内为甲方提供专属机房，机房应满足网络安全等级保护2.0三级

以及商用密码应用安全性评估三级的要求。

2）乙方建设的区教育云平台应部署在专属机房空间，实现所有计算、存储等设备的物理隔离；

3）提供远程实时视频监控系统，对专属机房空间情况进行实时视频监控。

3.2 云计算资源服务要求

1）云资源数量不少于 4970 核 vCPU/13254GB 内存，提供按使用量付费方式；

2）云主机提供弹性伸缩及快速横向扩展功能；

3）基于国产虚拟化软件创建和管理云主机，提供常见的迁移模式技术支持；

4）提供国产操作系统、国产中间件；

5）提供自动化批量部署云主机能力；

6）提供云主机的日常管理操作能力；

7）云服务可用性大于等于 99.99%。

3.3 云存储资源服务要求

1）云存储的存储空间不少于 550T，提供按使用量付费方式；

2）提供安全、低成本、高持久的云存储服务；

3）提供异地数据备份接口及技术支持服务；

4）数据可靠性大于等于 99.9999%。

3.4 网络资源服务要求

1）提供云上私有网络服务，支持自定义私有 IP 地址段、安全组、路由策略等能力，以在自定义的专有网络中使用云资源；

2）提供云上负载均衡服务，对多台云服务器进行流量分发；

3）提供云上弹性公网 IP 服务，可以灵活配置带宽和绑定云主机实例；

4）提供云上 NAT 网关服务，可以在私有网络内多个云主机共享弹性 IP，访问云外网络；

5）提供云专线服务，可以在数据中心与云上私有网络间构建高速、低时延、稳定安全的连接通道。

6）网络服务可用性大于等于 99.99%。

3.5 资源管理服务要求

1）运维团队提供不少于 5 人专业运维工程师驻场服务，工作日白天（5*8 小时）不少于 4 人值班服务，工作日夜间（5*16 小时）及节假日（24 小时）不少于 1 人值守服务；

2）通过云服务管理平台提供云主机、云存储、负载均衡、云数据库等云资源，以及网络资源及安全策略的配置管理服务，建设一套规范的资源使用与管理制度；

3）提供系统入云部署及云资源使用等方面的技术支持，包括资源开通、管理、监测、配置、故障处理、应急处置等；

4）提供入云系统运行监测及云资源使用优化服务，定期对云资源使用情况进行统计分析，制定资源优化方案及计划，提升云资源使用率；

5）提供网络安全监测、分析、处置服务，对入云系统安全策略及网络安全事件提出处置建议和优化方案；

6）提供云资源管理及入云系统安全监测运维周报；

7）重要时期安全保障服务，在重要节日、重大活动、重要会议等关键时期，为保障信息安全所采取的一系列安全保障措施。

3.6 安全服务要求

1）云平台应满足网络安全等级保护 2.0 三级以及商用密码应用安全性评估三级的要求；

2）提供高效、合理、可靠的安全保障服务，包括但不限于远程接入服务、运维堡垒机、数据库审计、日志审计、web 应用防火墙、主机安全等服务；

3）提供网络流量监控及入侵检测防护，能够有效地监控分析双向网络流量，实时检测发现网络入侵攻击及异常网络行为；

4）提供 Web 应用防火墙（WAF），防护常见 Web 漏洞的攻击，如 SQL 注入、XSS 跨站脚本、CC 攻击等；

5）提供云安全监管平台，具备防勒索、防病毒、防篡改、合规检查等安全能力，实现威胁检测、响应、溯源的自动化安全运营闭环，保护云上资产并满足监管合规要求；

6）提供态势感知，实现资产、漏洞、攻击来源、攻击分布等网络安全态势信息展示；

7）堡垒机提供运维身份鉴别、账号管控、系统操作审计等功能；

8）提供数据库审计，实现数据库的访问行为监控、危险操作告警、可疑行为审计；

9）提供云平台及入云系统整体漏扫服务，每季度至少开展一次，涵盖云平台上的所有关键组件和服务。

3.7 备份服务要求

1）在指定机房建设数据备份平台，实现与教育云平台同城异地数据备份；

2）采用全量备份与增量备份数据策略，备份数据到同城异地备份云，进行周期性备份；

3）支持教育云云主机整机数据、数据库实时备份与恢复；

4）数据备份至备份平台效率1小时不低于500G，恢复至教育云平台效率2小时不低于500G；

5）单个云主机恢复RTO应不大于2小时（基于500GB数据量）。

3.8 服务质量要求

1）故障响应定位服务：需提供技术咨询与故障定位服务，提供7*24 响应；

2）远程巡检服务：需提供服务巡检，对云服务的状态进行远程巡检，以确保云平台正常提供服务；

3）技术文档支持服务：需开放本项目全量文档和知识库，可随时获取技术文档及相关素材；

4）API与SDK支持服务：需提供本项目全量产品的OpenAPI/SDK 接口及工具，方便调用和集成开发；

5）缺陷修复服务：需提供已交付版本产品软件的缺陷修复服务，支持在约定变更时间窗口内完成修复工作。

6）售后服务：需提供每周7天×24小时售后服务，并提供有效的联系方式。

第四条 技术要求

乙方提供的服务应满足以下要求。

4.1 云平台

4.1.1 云管理平台

1）支持用户端主账号或子用户登录云平台用户端，子用户可SSO登录用户端。

2）支持通过密码强度检测、超时登出等选项保护用户账号安全，支持为每个用户提供多因子认证能力。

3）支持用户的生命周期管理，包含创建子用户、修改基本信息、重置密码等。

4）支持子用户权限管理，支持管理子用户的策略配置、用户组关联配置。

5）支持策略管理，包含创建、搜索、编辑和删除策略。

6）支持角色管理，包含创建、搜索、编辑和删除角色。

7）支持主账号的配额管理，包含查看产品列表、查看产品配额详情、搜索产品配额参数、申请产品配额、查看产品配额申请历史。

8）基于规则的告警聚合，可以基于标签灵活定义聚合规则，实现告警的聚合，减少告警数量。

9）支持平台设置巡检任务，巡检任务支持设置执行参数。

10）支持网络设备监控和告警，支持交换机运维管理。

4.1.2 云主机服务

1）支持创建/删除云服务器，能够选择实例规格、实例数量、镜像信息、存储信息、配置主网卡网络信息、配置网络 IP 和带宽、配置辅助网卡信息、配置安全组等。

2）对已创建的实例支持重置密码、更改实例规格、重装系统的操作。

3）支持批量创建云服务器时，设置云服务器的有序主机名和实例名称，并可以自定义起始标识数字。

4）支持公共镜像和自定义镜像。支持自定义镜像生命周期管理，包含导入镜像、创建镜像、共享或取消共享镜像、删除镜像、导出镜像、复制镜像。

5）支持用户粒度设置规格、镜像白名单开放能力。

6）支持实例删除保护，防止通过控制台或 API 误删除。

7）支持通过查看实例监控指标获取监控信息。

8）支持创建部署集，支持强制高可用、非强制高可用策略。

9）支持标签能力，通过标签为资源进行分类。

10）支持实例回收站，在删除实例时，可将实例放入回收站保留一段时间，并根据当前的清除策略一定周期后删除。

11）支持物理机和机架粒度的高可用策略。

12)支持在线扩展容量，扩容期间无需关闭虚拟机，无需卸载云盘；系统盘在线扩容不停业务。

13）应支持异构虚拟化能力。

14）云主机出现故障时，应支持自动重启或者迁移，保障业务连续性。

15）支持设置自动快照策略，可自定义快照时间点、重复日期以及保留时长。

4.1.3 云存储服务

4.1.3.1 弹性块存储

1）具备完整的云盘管理功能，支持创建、挂载、卸载、删除、扩容云盘。

2）支持修改云盘属性信息，支持查询云盘信息，允许筛选云盘状态，支持导出云盘信息。

3）支持创建快照、查看快照创建的进度、查看快照、回滚快照、复制快照、删除快照、编辑快照信息、通过快照创建自定义镜像，创建实例时，支持通过快照创建新数据盘。

4）支持设置自动快照策略，支持按天或按周为备份周期设置自动快照策略，为云盘定期创建快照备份数据。

5）支持手动快照设置保留策略。

4.1.3.2 对象存储

1）支持版本控制功能，保留数据的历史版本，避免数据被误删除。

2）可通过文件列表上传文件、创建文件夹、分片管理、删除文件、下载文件、修改文件访问权限、查看文件详情、管理文件元数据、删除文件夹、搜索文件、重命名文件、复制文件、移动文件、管理文件标签。

3）支持权限管理功能，实现存储授权策略管理。

4）支持配额功能，即可以设置的最大容量。

4.1.3.3 云日志服务

1）支持日志项目、日志主题的增删改查。

2）支持导入从消息队列、对象存储等渠道导入数据。

3）支持通过日志服务控制台实时监控日志服务的资源用量。

4）支持记录日志服务各个功能运行过程中的状态信息、业务运行的行为数据等信息。

4.1.4 云网络服务

4.1.4.1 私有网络

1）支持创建私有网络，创建私有网络时支持同时添加多个子网。

2）支持删除已创建的私有网络，可查看私有网络详情，支持修改私有网络名称、描述信息。

3）支持创建子网、删除子网，支持为子网更换路由表，支持修改子网名称、描述信息。

4）支持创建网卡，可手动/自动分配主私网 IP，以及手动/自动分配辅助私网 IP。

5）支持为网卡关联安全组，解关联安全组，支持删除网卡，支持修改网卡名称、描述信息。

6）安全组支持规则优先级。

7）支持管理网卡 IP 地址，包括增加辅助私网 IP 地址、释放辅助私网 IP 地址。

8）支持流量镜像能力，通过流量镜像，可以按需复制指定网卡的流量，并私网转发到目标网卡或负载均衡进行监控分析。

4.1.4.2 NAT 网关

1）支持创建 NAT 网关，为 NAT 网关绑定/解绑 IP。

2）支持删除 NAT 网关，修改 NAT 网关名称和描述。

3）支持查看 NAT 网关监控指标并配置告警。

4）支持私网 NAT 网关，单私有网络支持多个 NAT 网关。

4.1.4.3 公网 IP

1）支持创建公网 IP、释放公网 IP，支持强制释放。

2）支持修改名称描述、修改带宽上限、支持查看监控指标并配置告警规则。

3）支持为公网 IP 绑定和解绑云资源（包括云服务器/负载均衡/NAT 网关/辅助网卡 IP 地址）。

4）支持直通模式。

4.1.4.4 负载均衡

1）支持创建负载均衡实例、修改负载均衡实例名称和描述。

2）支持变更规格、删除负载均衡实例。

3）支持为负载均衡实例添加监听器、删除监听器、启动监听器、停止监听器和编辑监听器。

4）支持开启/配置健康检查、关闭健康检查。

5）支持创建、删除证书的能力。

6）负载均衡器需支持 GET、HEAD 两种健康检查方法。

7）负载均衡器需支持设置访问控制，可以通过白名单和黑名单控制访问负载均衡的源 IP 地址。

4.1.4.5 应用负载均衡

1）支持创建公网/私网应用负载均衡实例。

2）支持查看实例详情信息，包含实例名称、实例描述、地域、子网、公私网 IP 等基本信息。

3）支持更改实例名称、实例描述等实例基本信息。

4）支持实例删除保护。

5）支持查看实例列表，通过实例 id、公网 IP、实例名称等搜索实例。

4.1.4.6 VPN 连接

1）支持修改 VPN 网关，添加 VPN 网关路由，查看 VPN 网关监控指标并配置告警规则。

2）支持创建、修改、删除 IPsec 连接，查看 IPsec 连接监控指标并配置告警规则。

3）创建 IPSec 连接时，需支持感兴趣流和目的路由等多种路由模式。

4）支持 SSLVPN 连接能力，可实现多个客户端与云上 VPC 之间的网络互通。

4.1.5 云容器服务

4.1.5.1 容器服务

1）支持创建容器集群，支持 Calico VXLAN 和 VPC-CNI 网络模式。

2）支持高可用性部署，允许部署 3、5 或 7 个 Master 节点。

3）支持查看集群详情信息，包括：集群信息、资源用量、网络信息、节点信息、连接信息、事件信息、标签等。

4）支持查看节点详情信息，包括：节点概览、Pod 列表、事件、标签等。

5）能够对集群中的核心组件的异常执行自愈操作（如自动封锁节点、重启服务等）。

6）节点池扩缩容支持灵活的弹性策略。

7)能够可视化地观测集群指定命名空间内服务和负载之间的网络流量信息(HTTP、DNS 等)。

4.1.5.2 镜像仓库

1）支持镜像仓库实例的增删改查

2）支持镜像实例信息展示，包括实例状态、访问域名等。

3）支持实例资源使用状态展示，包括存储容量、资源配额使用状态等。

4）支持镜像仓库命名空间的增删改查。

4.1.6 云平台硬件设备

为满足教育云平台整体性能与业务稳定运行需求，本项目需部署服务器及交换机等硬件设备。服务器提供充足算力、内存与存储资源，支撑多信息系统并发承载；交换机保障平台内数据高效传输与网络连通。设备硬件规格需不低于所列配置，确保平台算力、网络、存储全链路稳定可靠。

4.1.6.1 管控服务器

1）通用计算芯片：配置≥2 颗 CPU 处理器，每颗 CPU 核数≥32，频率≥2.5GHz

2）内存：容量≥1024GB

3）硬盘：配置≥2 块 960G SATA SSD 硬盘，≥1 块 7.68TB NVMe SSD 硬盘

4）网卡：提供≥2 块 25Gb 双口网卡

5）RAID 卡：配置≥1 块 RAID 卡

6）配置冗余电源和风扇

7）支持云管理平台对服务器网卡进行拨测，用于评估和监控网络性能和可用性

8）支持云管理平台对服务器进行监控和日志进行收集

9）不少于 24 台

4.1.6.2 计算服务器

1）通用计算芯片：配置≥2 颗 CPU 处理器，每颗 CPU 核数≥64，频率≥2.4GHz

2）内存：容量≥1536GB

3）硬盘：配置≥2 块 960G SATA SSD 硬盘

4）网卡：提供≥2 块 25Gb 双口网卡

5）RAID 卡：配置≥1 块 RAID 卡

6）配置冗余电源和风扇

7）支持云管理平台对服务器网卡进行拨测，用于评估和监控网络性能和可用性

8）支持云管理平台对服务器进行监控和日志进行收集

9）不少于 17 台

4.1.6.3 块存储服务器

1）通用计算芯片：配置≥2 颗 CPU 处理器，每颗 CPU 核数≥32，频率≥2.5GHz

2）内存：容量≥256GB

3）硬盘：配置≥2 块 960G SATA SSD 硬盘，≥8 块 3.84TB NVMe SSD 硬盘

4）网卡：提供≥2 块 25Gb 双口网卡

5）RAID 卡：配置≥1 块 RAID 卡

6）配置冗余电源和风扇

7）支持云管理平台对服务器网卡进行拨测，用于评估和监控网络性能和可用性

8）支持云管理平台对服务器进行监控和日志进行收集

9）不少于 19 台

4.1.6.4 对象存储服务器

1）通用计算芯片：配置≥2 颗 CPU 处理器，每颗 CPU 核数≥32，频率≥2.5GHz

2）内存：容量≥256GB；

3)硬盘:配置≥2 块 960G SATA SSD 硬盘，≥2 块 1.92TB NVMe SSD 硬盘，≥10 块 20TB HDD

硬盘

4）网卡：提供≥2 块 25Gb 双口网卡

5）RAID 卡：配置≥1 块 RAID 卡

6）配置冗余电源和风扇

7）支持云管理平台对服务器网卡进行拨测，用于评估和监控网络性能和可用性

8）支持云管理平台对服务器进行监控和日志进行收集

9）不少于 8 台

4.1.6.5 数据库中间件服务器

1）通用计算芯片：配置≥2 颗 CPU 处理器，每颗 CPU 核数≥32，频率≥2.5GHz

2）内存：容量≥1024GB

3）硬盘：配置≥2 块 960GB SATA SSD 硬盘，≥8 块 3.84TB NVMe SSD 硬盘

4）网卡：提供≥2 块 25Gb 双口网卡

5）RAID 卡：配置≥1 块 RAID 卡

6）配置冗余电源和风扇

7）支持云管理平台对服务器网卡进行拨测，用于评估和监控网络性能和可用性

8）支持云管理平台对服务器进行监控和日志进行收集

9）不少于 8 台

4.1.6.6 备份一体机

1）通用计算芯片：配置≥2 颗 CPU 处理器，每颗 CPU 核数≥32，频率≥2.1GHz

2）内存：容量≥ 512 GB

3）硬盘：配置≥4 块 3.2TB NVMe SSD 硬盘；配置≥24 块 8TB HDD 硬盘

4）网卡：提供≥4 块 10Gb 双口网卡

5）RAID 卡：配置≥1 块 RAID 卡

6）配置冗余电源和风扇

7）不少于 5 台

4.1.6.7 平台核心交换机

1）主机：L3 以太网交换机主机

2）插槽：业务插槽≥4 个

3）端口：≥24 口 100G 光口；≥2 口 40G 光口；≥24 口 10G 光口

4）支持本项目云管理平台的网络设备监控和告警功能

5）支持本项目云管理平台的交换机运维管理功能

6）配置冗余电源和风扇

7）不少于 4 台，含部署所需的耗材和网络模块

4.1.6.8 汇聚交换机

1）主机：L3 以太网交换机主机

2）端口：≥128 口 100G 光口

3）支持本项目云管理平台的网络设备监控和告警功能

4）支持本项目云管理平台的交换机运维管理功能

5）配置冗余电源和风扇

6）不少于 4 台，含部署所需的耗材和网络模块

4.1.6.9 25GTCP 网络交换机

1）主机：L3 以太网交换机主机

2）端口：≥48 口 25G 光口；≥8 口 100G 光口

3）支持本项目云管理平台的网络设备监控和告警功能

4）支持本项目云管理平台的交换机运维管理功能

5）配置冗余电源和风扇

6）不少于 26 台，含部署所需的耗材和网络模块

4.1.6.10 专线接入交换机

1）主机：L3 以太网交换机主机

2）插槽：业务插槽≥4 个

3）端口：≥8 口 100G 光口；≥2 口 40G 光口；≥24 口 10G 光口

4）支持本项目云管理平台的网络设备监控和告警功能

5）支持本项目云管理平台的交换机运维管理功能

6）配置冗余电源和风扇

7）不少于 4 台，含部署所需的耗材和网络模块

4.1.6.11 带外管理交换机

1）主机：L3 以太网交换机主机

2）端口：≥48 口 1000M 以太网口，≥4 口 10G 光口

3）支持本项目云管理平台的网络设备监控和告警功能

4）支持本项目云管理平台的交换机运维管理功能

5）配置冗余电源和风扇

6）不少于 14 台，含部署所需的耗材和网络模块

4.2 云安全

4.2.1 云平台安全服务

4.2.1.1 安全区域边界能力

4.2.1.1.1 逻辑隔离

1）支持主要防护功能的统一化模板设置能力，模板分为高、中、低三个级别，分别对应不同的安全防护等级进行配置，包括入侵防护策略、病毒防护策略、协议控制策略、流量控制等，可通过 Web 界面进行安全等级切换。

2）支持一键巡检功能，支持按照间隔天数或当天某个时间点设置巡检频率，可以将巡检报告上报给安管系统并通过邮箱发送，巡检报告支持 PDF、Word、HTML 格式，并可设置报告最大保存数。

3）巡检内容包含硬件巡检、运行状态巡检、配置巡检、版本状态巡检。硬件巡检包含设备序列号、设备运行状态、设备名、风扇状态、设备版本信息、系统温度。

4）支持漏洞扫描功能：支持后门类、浏览器类、CGI 类、DNS 类、FTP 类、信息收集类、网络设备类、OpenSSH、WEB 类、蠕虫病毒类等不少于 40 类插件管理；任务管理：支持记录漏洞扫描结果，包括主机地址、危险等级、漏洞名称、漏洞类型、漏洞摘要、端口等信息，支持定时执行漏洞扫描任务，执行周期可以按照每小时、每天、每周、每月、每年选择。

5）服务提供方所提供的能力支撑工具需满足：

机架：2U

国产化：国产化 CPU 与操作系统

接口：配置≥6 个电口，≥4 个千兆光口，≥4 个万兆光口

扩展槽：配置≥1 个扩展槽

性能：网络层吞吐≥40Gbps，应用层吞吐≥18Gbps，TCP 新建连接≥45 万，TCP 并发连接≥2000 万

硬盘：配置≥2T 机械硬盘

电源：配置冗余电源

功能模块：服务期内免费维修，服务期内具备防病毒、上网行为管理、入侵防御特征库升级授权；支持 IPSec VPN 和 SSL VPN 模块（≥200 个并发用户）。

以上能力支撑工具不少于 4 台。

4.2.1.1.2 物理隔离

1）内、外网主机分别具备三系统，即系统 A、系统 B 和备份系统。支持在 WEB 界面上配置启动顺序，在 A 系统发生故障时，可以切换到 B 系统；支持将当前运行系统备份。

2）支持将网口配置成 VLAN 接口，处理相同 VLAN ID 的数据包。

3）支持文件格式特征过滤；并能提供具备图形化界面的文件类型判断工具以帮助用户识别不常见文件类型。

4）支持对外开启 WEB 服务，供用户登录进行文件上传/下载操作。

5）支持病毒检测；支持达梦、人大金仓、Gbase、神通数据库、博阳、瀚高等主流国产数据库。

6）内/外网主机系统分别具有独立管理接口，而不是采用低安全的管理方式，如通过业务口管理或通过内网唯一管理接口完成全部管理等。

7）服务提供方所提供的能力支撑工具需满足：

机架：2U

国产化：国产化 CPU 与操作系统

内网接口：配置≥6 个电口，≥4 个千兆光口，≥4 个万兆光口

外网接口：配置≥6 个电口，≥4 个千兆光口，≥4 个万兆光口

性能：网络层吞吐≥15Gbps、HTTP 并发≥100 万、UDP 延时≤1ms

电源：配置冗余电源

功能模块：服务期内免费维修，服务期内具备反病毒授权，功能模块包括文件交换、FTP 访问、数据库传输、邮件传输、安全浏览、安全通道、消息模块、视频传输模块和工控模块。

以上能力支撑工具不少于 2 台。

4.2.1.1.3 业务防护

1）支持 Web 恶意扫描防护的检测与防御能力，专利级别防护能力。

2）支持反向代理模式、单臂部署模式等。

3）支持对常用 Web 应用攻击 SQL 注入、XSS 攻击检测与防护功能。

4）支持协议识别及解码能力，应支持：URL 解码、XML 解码、JSON 解析、Base64 解码、Unicode 解码、十六进制转换、斜杠反转义、CHR 解码、UTF-7 解码，支持解析 7 层以上混合编解码能力，可实现对多层编码攻击的检测。

5）具备 Shiro 反序列化、代码注入、PHP 反序列化、Webshell、弱口令、命令注入等应用安全防护能力。

6）服务提供方所提供的能力支撑工具需满足：

机架：2U

国产化：国产化 CPU 与操作系统

接口：配置≥6 个电口，≥4 个千兆光口

扩展槽：配置≥2 个扩展槽

性能：网络层吞吐≥12Gbps、应用层吞吐≥6Gbps、HTTP 并发连接≥500 万

硬盘：配置≥128G 固态硬盘

电源：配置冗余电源

功能模块：服务期内免费维修，功能模块包括应用攻击检测及防护、SSL 卸载、区域访问控制、网站锁、缓存加速模块。

以上能力支撑工具不少于 4 台。

4.2.1.1.4 入侵防御

1）支持至少包括规则 ID、规则名称、威胁级别、动作、威胁类型、发布时间等条件进行筛选。

2）系统应支持启发式病毒检测引擎，支持手动上传样本进行鉴定。

3）系统应默认内置不少于 11 种规则集，至少包括严格检测模板、物联网检测模板、WEB 服务器模板、僵木蠕检测模板等，满足不同部署环境下的安全防护需求。

4）支持多种规则变更部署模式，至少包括自动防御模式、试运行模式和手动防御模式。

5）支持 SQL 注入防护和 XSS 攻击防护，检测点支持 URL、Cookie、Reference、Form、

User-Agent、X-Forwarded-For，内置 AI 检测模型，利用机器学习技术对 SQL 注入报文进行分析，检测和识别 SQL 注入行为。

6）服务提供方所提供的能力支撑工具需满足：

机架：2U

国产化：国产化 CPU 与操作系统

接口：配置≥6 个电口，≥4 个千兆光口，≥4 个万兆光口，≥2 个 USB 口

扩展槽：配置≥1 个扩展槽

性能：网络层吞吐≥60Gbps、应用层吞吐≥30Gbps、并发连接≥1000 万，HTTP 新建连接≥15 万

电源：配置冗余电源

功能模块：服务期内免费维修、包含病毒库升级授权及入侵防御特征库升级授权。

以上能力支撑工具不少于 4 台。

4.2.1.2 安全通信网络能力

4.2.1.2.1 流量检测

1）具备综合分析首页场景展示多种数据关联的网络态势。支持选择固定时间周期展示网络态势，时间周期包含：昨天、今天、最近 7 天、最近 15 天，展示的态势详情包括：系统安全态势、攻击阶段、告警事件趋势统计、攻击 IPTOP 汇总统计、受害 IPTOP 汇总统计、告警事件 TOP 展示、告警等级分布统计、设备运行状态监控，支持监控接入流量。

2）支持深度协议解析，包括 http、http2、dhcp、dns、ftp、mysql、imap、bgp、sip、pptp、l2tp 等多种通用协议解析，支持 gtpu、ngap、pfcp 等 5G 协议，支持工控协议的解析，累计支持的深度解析协议种类大于 100 种。

3）支持口令爆破分析场景，支持展示爆破端口、爆破结果、爆破用户名、爆破次数、最近爆破时间等信息。

4）系统具备病毒检测分析场景，支持展示病毒文件名称、病毒名称、协议类型、传播时间等内容。

5）服务提供方所提供的能力支撑工具需满足：

机架：2U

国产化：国产化 CPU 与操作系统

内存：配置≥128G

接口：配置≥6 个电口，≥4 个千兆光口，≥2 个万兆光口，≥2 个 USB 口

扩展槽：配置≥6 个扩展槽

性能：网络层吞吐≥15Gbps、并发连接≥800 万，HTTP 新建连接≥12 万

硬盘：配置≥4T 机械硬盘

电源：配置冗余电源

功能模块：服务期内免费维修，功能模块包括异常终端、信令风暴、非法信令分析场景，支持僵木蠕、挖矿模块。

以上能力支撑工具不少于 2 台。

4.2.1.2.2 通信加密

1）支持管理员分权管理，支持三权分立，包括系统管理员，安全管理员，审计管理员；支持自定义权限模板，为管理员分配管理权限。

2）支持单点登录功能（SSO），支持移动用户登录 VPN 后再登录内部 B/S、C/S 信息系统时不需要二次重复认证。支持针对不同的访问资源设定不同的 SSO 用户名和密码，支持用户自行修改 SSO 账号。

3）支持多系统引导，即系统 A、系统 B 和备份系统，可在管理员界面直接配置启动顺序，支持两个操作系统，管理员可自由选择当前启动系统，每个系统拥有独立的配置文件，且配置文件分别支持加密导入导出。

4）支持 IPSec、SSL、PPTP、L2TP VPN 的统一用户管理和认证体系，实现一次配置，即可适用于全部 VPN 类型接入。

5）同时符合 GM/T 0023《IPSecVPN 网关产品规范》、GM/T 0025《SSL VPN 网关产品规范》、GM/T 0026《安全认证网关产品规范》相关要求，符合 GM/T 0028《密码模块安全技术要求》安全等级二级相关要求。

6）服务提供方所提供的能力支撑工具需满足：

机架：2U

国产化：国产化 CPU 与操作系统

接口：配置≥8 个电口，≥4 个千兆光口

扩展槽：配置≥2 个扩展槽

性能：网络层吞吐≥8Gbps、SSL VPN 加密速度≥400Mbps、SSL VPN 最大并发用户数≥2,000、IPSec VPN 加密速度≥400Mbps、IPSec VPN 最大隧道数≥8,000、≥500 个 SSL VPN 并发用户授



权

电源：配置冗余电源

功能模块：支持 PC 端和移动端同时接入，标配硬件加密卡，服务期内免费维修。

以上能力支撑工具不少于 4 台。

4.2.1.3 安全计算环境能力

4.2.1.3.1 安全计算

1）支持主机常见的端口、进程、软件、系统服务、定时任务、系统软件、内核模块、硬件网卡、常见中间件、web 站点等指纹信息采集和展示，并支持自定义扫描时间与频率。

2）支持记录所有类型资产前后两次的采集差异，按需配置变更白名单。支持 SSH、 RDP 暴力破解识别，其中 SSH 支持自动封禁。

3）支持对容器集群暴露面进行分析，并可视化展示暴露路径。

4）支持检测主机和容器内发生的入侵行为，支持可疑文件落盘行为检测，支持检测常见的反弹 shell，后门驻留，恶意信息收集，权限提升，横向移动，暴力破解等恶意动态行为，支持检测常见的内核态后门。

5）支持应用层反入侵，至少包括 Java，Golang 语言，配置 RASP 进程注入白名单，命中白名单的进程不会被注入。

6）支持至少以下几种行为的关联：同一进程组的进程创建行为、同一进程组的进程网络连接行为、同一进程组的进程 DNS 请求行为、同一进程组的进程文件创建行为。

7）支持检测常见的 Webshell、木马、后门、挖矿程序等恶意二进制静态文件，支持对扫描出的病毒文件一键隔离至文件隔离箱，并且支持一键恢复。

4.2.1.4 安全管理中心能力

4.2.1.4.1 日志审计

1）采用 B/S 模式，无需安装客户端，使用 Web 浏览器访问管理中心，浏览器端无需安装 Java 运行环境。

2）支持 SNMP、Syslog、ODBC/JDBC、文件/文件夹、WMI、FTP、SFTP、SMB、NetBIOS、OPSEC 等多种方式完成日志收集功能。

3）支持主动采集 oracle、sqlserver、mysql、db2、sybase、postgresql、informix、teradata 等数据库日志。

4）支持日志过滤，可自定义过滤条件进行自动化日志过滤，排除繁杂无用的日志，支持一



键清除过滤条件。

5）支持对日志提供在线/离线地图定位，支持源 IP 与目的 IP 分布走向的视网膜图展示，支持事件拓扑分析用于描述整个事件的访问关系及过程，支持多维分析。

6）服务提供方所提供的能力支撑工具需满足：

机架：2U

国产化：国产化 CPU 与操作系统

内存：配置≥32G

接口：配置≥6 个电口，≥8 个千兆光口，≥2 个 USB 接口

扩展槽：配置≥1 个扩展槽

性能：综合日志处理性能 10000EPS、日志采集处理均值 20000EPS、支持≥630 个审计对象授权

硬盘：配置≥128G SSD+3 块 8TB 机械硬盘

电源：配置冗余电源

功能模块：服务期内免费维修

以上能力支撑工具不少于 2 台。

4.2.1.4.2 漏洞扫描

1）支持设置口令猜测参数，包括口令猜测时间、口令猜测次数和口令猜测间隔，间隔时间设置范围为 0-1800 秒。

2）支持对主流操作系统的识别与扫描，包括：Windows、Redhat、Ubuntu、centos、BC_linux、Debian、深度、麒麟、新支点、Fedora、SUSE、slackware、Oracle OS 等。

3）支持对主流虚拟化软件平台的识别与扫描，包括：OpenStack、KVM、Vmware、Xen、Docker、Huawei FusionSphere 等。

4）支持对主流 SCADA/HMI 软件的识别与扫描，包括 Wincc、IGSS、Movicon、Promotic、iFix、WebAccess、ForceControl、KingView 等。

5）支持配置变更监测，可以根据实际情况设置任意检查结果作为变更基线，支持与自身或者其他设备的同类型变更项进行对比，周期性监测系统的文件、目录、启动项、进程等配置信息及变更状态，并支持生成配置变更监测报表。

6）服务提供方所提供的能力支撑工具需满足：

机架：1U

国产化：国产化 CPU 与操作系统

接口：配置≥6 个电口，≥4 个千兆光口，≥4 个万兆光口，≥2 个 USB 口

扩展槽：配置≥1 个扩展槽

性能：主机漏扫和基线核查可扫描 IP 地址总数无限制，单任务最大可扫描 100IP 地址；主机漏扫并发扫描 40IP 地址；基线核查可核查 Windows 系列设备类型；Web 漏扫可扫描子域名或 IP 总数量≥50 个，Web 漏扫并发≥5 个子域名或 IP

电源：配置冗余电源

功能模块：服务期内免费维修，服务期内具备主机漏扫、配置核查、Web 漏扫 3 个模块授权。

以上能力支撑工具不少于 2 台。

4.2.1.4.3 数据库审计

1）支持旁路部署方式，无须在被审计系统上安装软件，对原有网络不造成影响，审计产品的故障不影响被审计系统的正常运行。

2）支持国产数据库人大金仓、达梦、南大通用、神通、高斯、瀚高、巨杉、虚谷、OceanBase、AnalyticDB MySql 、AnalyticDB MySql、AnalyticDB PostgreSQL、RDS MySql、RDS PostgreSQL 等数据库的审计。

3）支持数据库操作类、表、视图、索引、触发器、存储过程、域、会话、数据、授权、游标、事物、表空间、序列、函数等不低于 36 种对象的操作审计。

4）支持审计访问数据库的时间，源/目的 IP，源/目的端口，源/目的 mac，资源账号，数据库名，规则名称，表名，命令，SQL 语句、级别，响应时间、错误码，影响行数，连接方式，客户端程序名，模式名，客户端用户，SQL 执行结果。

5）服务提供方所提供的能力支撑工具需满足：

机架：2U

国产化：国产化 CPU 与操作系统

接口：配置≥10 个电口，≥28 个万兆光口，≥4 个 40G 接口，≥2 个 100G 接口

性能：可审计业务流量≥2000Mbps

硬盘：配置≥2 个 8T 机械硬盘，支持 RAID1

电源：配置冗余电源

功能模块：无限个被审计 DB 服务数的授权，虚拟导流器功能授权≥125。服务期内免费维修。

以上能力支撑工具不少于 2 台。

4.2.1.4.4 态势感知

1）支持不少于 8 块大屏从多角度多维度地进行态势数据的呈现，包括态势总览、外部攻击态势、资产态势、运行态势、脆弱性态势、风险态势、情报态势、流态势等态势大屏。

2）风险态势支持以可视化方式直观展示风险资产/风险安全域评估的逻辑，不同类型的资产由于本身的价值、自身存在脆弱性（漏洞）、受到的威胁（告警/攻击），通过风险计算模型评估风险，以 3D 指标图形方式呈现全网风险资产、风险安全域的统计数量，并支持对数据详情进行钻取。

3）支持形象地展示出安全域的风险矩阵，从可能性和影响性两个角度标注安全域中资产风险的分布情况，通过风险矩阵法，指导管理员进行风险分析，采取相应的风险处置对策。

4）至少提供 30 个内置剧本，并支持剧本的导入导出功能，对每个剧本可进行统计操作，可按照时间轴对执行完成且成功数量、执行中数量、执行异常的数据进行统计呈现，并支持剧本直接点击测试。

5）为保障项目后期设备上线统一管理与良好的联动性，要求本项目逻辑隔离、入侵防御、漏洞扫描、数据库审计等能力的支撑工具为同一品牌，并且其与态势感知能力可以实现无缝对接与联动。

6）服务提供方所提供的能力支撑工具需满足：

机架：2U

CPU：配置≥64 核

内存：配置≥256G

国产化：国产化 CPU 与操作系统

接口：配置≥4 个电口，≥2 个千兆光口，≥2 个万兆光口

扩展槽：配置≥2 个扩展槽

硬盘：配置≥12 个 4T 机械硬盘，支持 RAID50，960G SSD

电源：配置冗余电源

功能模块：提供平台知识库升级服务能力。内置流量采集器、日志采集器、性能采集器，不少于 200 个管理节点授权，9 个应用实例授权。服务期内免费维修。

以上能力支撑工具不少于 2 台。

4.2.1.4.5 运维审计

1）支持包括传统 SSH 字符协议、FTP/SFTP 文件传输协议、RDP/VNC 图形操作协议；支持

对 Mysql、Redis、MongoDB 等主流数据库进行运维操作审计。

2）支持常用的运维协议，具体包括 SSH、TELNET、VNC、RDP、SFTP 等。支持设备账户和密码的自动登录、手工登录和半自动登录模式。

3）支持 SM2/SM3/SM4 等国产密码算法，支持通过国密 SSL 协议访问 Web 管理界面对资产进行访问。

4）管理员注册用户时指定了用户口令，用户首次登录成功后强制要求改密。

5）服务提供方所提供的能力支撑工具具备有效的《商用密码产品认证证书》，满足 GM/T0028《密码模块安全技术要求》第三级要求。

6）服务提供方所提供的能力支撑工具需满足：

机架：2U

接口：≥2 个千兆光口，≥2 个万兆光口

电源：配置冗余电源

功能模块：可管理不低于 1000 个用户，不低于 2000 个设备资源，不低于 10000 个账户，支持不低于 3000 文本协议运维访问并发，支持不低于 1000RDP 图形协议运维访问并发。服务期内免费维修。

以上能力支撑工具不少于 2 台。

4.2.2 云租户安全服务

4.2.2.1 云防火墙服务

1）云防火墙基于云平台内生安全和云原生安全服务，云防火墙服务实例可通过云管平台统一创建、自动化部署和统一管理。与云平台共用同一套身份管理体系，用户在创建相关安全产品实例时，无需在云平台来回切换账号。

2）云防火墙访问控制是基于云平台网络架构实现东西向的访问控制，云防火墙可支持下发策略到安全组进行主机访问控制。

3）支持 VPC 边界防火墙，支持 VPC 间流量引流设置，包括手动引流、自动引流两种方式；支持 VPC 间流量引流场景选择，包括点到点、点到多点、多点互联三种引流场景模式选择。

4）资产暴露分析：提供展示资产入方向流量的概览信息，帮助用户发现暴露在互联网的风险端口，包括访问源 IP TOP5、开放端口 TOP5、资产、开放端口、开放协议、访问源等内容。

5）支持 VPC 互访分析，展示 VPC 间的流量访问关系，包括 VPC 流量速率趋势图、IP 流量大小 TOP10、开放端口 TOP5 等内容。

6）支持配置地址簿，包括 IP 地址簿、端口地址簿，一条访问控制策略最多可配置 20 个地址簿，10 万个 IP 地址。

4.2.2.2 网络威胁检测服务

1）网络威胁检测服务基于云平台内生安全和云原生安全服务，网络威胁检测系统实例可通过云管平台统一创建、自动化部署和统一管理。与云平台共用同一套身份管理体系，用户在创建相关安全产品实例时，无需在云平台来回切换账号。

2）数据流量采集，协议解析支持 HTTP、HTTPS、TCP、UDP、ICMP、DNS、SNMP、SSH、Telnet、RDP、IPsec、GRE、VXLAN、FTP、SMB 等 20+种协议解析检测。

3）漏洞利用攻击检测支持反序列化漏洞、系统漏洞、RDP 漏洞、软件漏洞、Shellcode、SMB 漏洞、拒绝服务漏洞、未授权漏洞、远程命令执行漏洞等漏洞利用攻击检测。

4）支持行为分析，具备对挖矿行为、隐蔽隧道、安全基线模型、C&C 行为、网络扫描、暴力破解等行为的分析检测能力。

5）支持隐蔽隧道专项分析，包括但不限于 gre 隐蔽隧道、icmp 隐蔽隧道、ipsec 隐蔽隧道等隐蔽隧道场景的检测分析。

6）检测防御配置，支持基础防御、虚拟补丁、智能防御、文件威胁检测、邮件威胁检测等检测能力。

4.2.2.3Web 应用防火墙服务

1）服务实例可通过云管平台统一创建、自动化部署和统一管理。与云平台共用同一套身份管理体系，用户在创建相关安全产品实例时，无需在云平台来回切换账号。

2）支持对 OWASP Top 10 漏洞、SQL 注入、命令注入、WebShell、表达式注入、XPath 注入、LDAP 注入、任意文件读&目录遍历、LFI、SSTI、SSRF、XSS 等漏洞的检测及防护。

3）Web 后门，通过对以 asp、php、jsp 或者 cgi 等网页文件形式存在的 Web 命令进行检测，拦截网页木马。

4）支持 CC 攻击防护，对基于对源 IP、自定义 header 等的访问频次统计，对指定目标进行记录、限速或拦截。

5）支持识别公开类型 Bot 并进行分类，支持按 IP 情报进行 Bot 识别和分类，可以对识别出的 Bot 进行告警、拦截或放过。

4.2.2.4 云主机安全服务

1）产品服务实例可通过云管平台统一创建、自动化部署和统一管理。与云平台共用同一套身份管理体系，用户在创建云安全中心实例时，无需在云平台来回切换账号。

2）支持主动获取云内的资产，并且可以根据云内资产变化实时更新资产信息。无需像传统安全产品那样需要配置 IP 范围，被动识别流量中的资产，因同步不及时而导致资产信息遗漏。

3）支持检测常见的反弹 shell，后门驻留，恶意信息收集，权限提升，横向移动，暴力破解等恶意动态行为，具备告警处置能力，包括终止进程与隔离文件等操作。

4）支持对疑似入侵检测行为进行自动化上下文关联，并通过安全攻击图谱可视化展示。支持直观展示进程、文件创建、DNS 解析、网络连接、SSH 登录等原始数据。

5）支持至少以下几种行为的关联：同一进程组的进程创建行为，同一进程组的进程网络连接行为，同一进程组的进程 DNS 请求行为，同一进程组的进程文件创建行为。

6）支持实时监控主机的多种活动，如网络访问、文件操作和进程运行，对高置信度攻击进行实时拦截。

7）支持等保二/三级基线检查所需检查项，帮助用户信息安全等级达到国家标准，满足合规要求。支持 CIS 标准检查项。

4.2.2.5 云堡垒机服务

1）服务实例可通过云管平台统一创建、自动化部署和统一管理。与云平台共用同一套身份管理体系，用户在创建云堡垒机实例时，无需在云平台来回切换账号。

2）提供多网域管理功能，支持通过网络域代理方式连通多个 VPC、异构云等不同网络环境中的服务器资产，实现多网域运维。

3）主机管理支持导入同品牌公共云主机，支持新建、编辑、删除主机资源，支持修改主机的服务端口，支持新建、编辑和删除主机账户，支持新建、修改、删除主机组，支持添加、移除主机组成员，提供密钥管理功能，用户可以创建密钥并将密钥批量关联到主机账户中，提高管理主机账户的效率。

4）支持命令控制策略，控制用户命令的输入，支持命令审批，支持访问控制策略，控制用户登录、文件管理等权限，支持批量修改主机的密码。

5）运维审计支持查看实时会话、历史会话，支持阻断对话。支持堡垒机的登录日志和操作日志。

4.2.2.6 云数据库审计服务

1）支持通过云管平台统一创建、自动化部署和统一管理。与云平台共用同一套身份管理体系，用户在创建数据库审计服务实例时，无需在云平台来回切换账号。

2）可对日志进行细粒度解析，支持审计数据库操作（DM）、对象管理（DD）、控制（DC）等操作语句的审计，解析后的日志记录至少包括访问发生时间、客户端 IP 地址、客户端 MAC、

终端程序、访问账号、访问数据库名、操作表名、SQL 语句、数据库响应时间以及返回结果等关键信息。

3）支持以操作类型、时间、IP 地址、用户名、主机名、终端名、数据库操作类型、数据库表、影响的行、字符串、认证结果、响应时间、返回码、关键字、敏感数据等作为事件识别规则及审计规则。

4）支持服务扫描和发现功能，通过扫描网络中的开放端口以及确定监听这些端口的服务，如主机 IP、端口、主机操作系统、服务的类型等，并实现自动或手动将这些服务添加到数据库引擎。

5）支持对敏感数据分布的服务器进行统计，并以图表的形式展示，可导出为报表。

4.2.3 密码安全服务

4.2.3.1 密码服务

1）集成国密认证的国产密码卡，实现各类密码算法，保证算法的高安全性。支持对称算法国产 SM1、SM4、SM7 算法，摘要算法支持国产 SM3 算法，非对称算法支持国产 SM2、SM9 算法。

2）密钥管理采用多级密钥管理体系，逐层保护。密钥产生时，密码机支持产生高质量的随机密钥；密钥存储时，支持安全存储对称密钥、RSA 密钥和 SM2 密钥，任何时候密钥不以明文形式出现在密码机外。

3）密钥备份恢复。密码机支持内部密钥的安全备份和恢复，可用于实现互备或负载的多台设备间的密钥同步，提供紧急情况下的密钥销毁手段。

4）服务提供方所提供的能力支撑工具具备有效的《商用密码产品认证证书》，满足 GM/T0028《密码模块安全技术要求》第三级要求。

5）至少具备和 5 家主流云厂商云管平台的兼容性证明。

6）服务提供方所提供的能力支撑工具需满足：

机架：2U

接口：≥2 个千兆光口，≥2 个万兆光口

电源：配置冗余电源

功能模块：支持国密算法的 PKI 业务应用；SM2 密钥生成≥10000 对/秒；SM2 签名≥9000 次/秒；SM2 验签名≥5000 次/秒；SM3 摘要≥500 Mbps；SM4 加解密≥500 Mbps。服务期内免费维修。

以上能力支撑工具不少于 4 台。

4.2.3.2 数据保密

1）支持 SSL3.0/TLS1.0/TLS1.1/TLS1.2/TLS1.3/DTLS 等协议；支持证书的配置管理，包括支持产生证书请求、导入外部签发证书、自签发测试证书，以及支持多证书的管理。

2）支持导入密钥、证书和 PKCS12 格式文件，支持在一个服务中同时配置多条证书链，以验证不同 CA 的用户证书。

3）支持基于用户名、群组、角色的访问控制，支持基于用户数字证书信息的访问控制，支持针对目标信息系统的访问控制，支持服务管理、服务器组管理、SSL 策略管理、证书管理等功能。

4）服务提供方所提供的能力支撑工具具备有效的《商用密码产品认证证书》，满足 GM/T0028《密码模块安全技术要求》第三级要求。

5）服务提供方所提供的能力支撑工具需满足：

机架：2U

接口：2 个千兆光口，2 个万兆光口

电源：配置冗余电源

功能模块：RSA2048 并发用户数≥10000；RSA2048 新建连接数≥1000；RSA2048 吞吐量≥300Mbps；SM2 并发用户数≥1000；SM2 新建连接数≥10000；SM2 吞吐量≥300Mbps。服务期内免费维修。

以上能力支撑工具不少于 4 台。

4.2.3.3 国密浏览器服务

1）提供 20 套国密浏览器服务。支持国密算法 SM2、SM3、SM4。在 Chrome 内核、IE 内核下均支持国密 SSL 协议。

2）支持 HTML 和 CSS 解析，支持 JavaScrip 引擎，可以正确地渲染显示页面，支持基本的浏览器操作功能。

3）支持第三方电子认证中心签发的数字证书。

4）支持 NPAPI 控件。

5）服务提供方所提供的能力支撑工具具备有效的《商用密码产品认证证书》，满足 GM/T0028《密码模块安全技术要求》第二级要求。

4.2.3.4 密钥管理服务

1）提供数据加密密钥全生命周期管理能力。支持密钥生成、密钥更新、密钥备份与恢复、

密钥归档、密钥销毁等密钥全生命周期管理，支持非对称密码算法或对称密码算法的密钥管理。

2）支持用户管理，可以查看用户信息、新建用户信息、编辑用户信息、停启用用户、绑定ukey、解绑 ukey、重置密码、删除用户信息。

3）支持日志管理，可以查看管理日志信息、查询管理日志信息、导出管理日志信息、审计管理日志信息、归档管理日志信息。

4）支持配置管理，包括管理认证方式配置、归档周期配置、NTP 配置、网络配置、自动备份。

5）支持 KMIP 密钥管理：支持远程密钥管理，包括密钥的产生、导出、激活、销毁、归档、密钥属性等。

6）服务提供方所提供的能力支撑工具具备有效的《商用密码产品认证证书》。

4.2.3.5 动态令牌认证服务

1）支持动态密码，实现双重因子认证，从而有效保护用户认证安全。

2）支持策略配置，支持配置口令变化周期、认证窗口、自动解锁时间、自动锁定连续错误次数、动态口令长度、二维码有效期、重放检测大小、应急口令有效期。

3）管理服务支持双算法加密套件的 HTTPS 通讯协议，能够自适应客户端浏览器的加密套件；业务服务支持 HTTPS 加密通道，并支持白名单和访问密钥两种方式认证应用客户端的身份。

4）支持硬件令牌、手机令牌；支持完善的令牌生命周期管理，包括激活、挂起、解挂、锁定、废止、查询等功能；支持对令牌的自动锁定/解锁和手动锁定/解锁；支持设置令牌的临时静态密码功能。

5）服务提供方所提供的能力支撑工具需满足：提供不少于 10 个硬件令牌 ，不少于 20 个软件令牌。

6）服务提供方所提供的能力支撑工具具备有效的《商用密码产品认证证书》。

4.4 国产数据库服务

1）支持 ANSI SQL-2003 以上标准；支持 JDBC/ODBC 标准接口；支持 PL/pgSQL 过程语言。

2）支持逻辑备份恢复、物理备份恢复，物理备份支持增量备份、联机热备份、备份压缩、备份集合并等技术，逻辑和物理备份均支持本地和远程备份。

3）支持 HA 故障转移集群和主备同步技术，并且能够支持读写分离以及故障转移功能，支持主从、一主多从、级联复制等架构，从库能设置延迟复制和优选提交复制。

4）支持自主访问控制、基于安全标签的强制访问控制、用户角色三权分立、审计、加密、

身份识别与验证等安全功能。支持全密态等值查询功能和动态脱敏功能。

5）支持系统性能监控动态视图，TOP SQL 信息、内存管理信息、事务信息、线程信息、操作历史等信息。

6）支持通信和存储加密功能，支持库级别的磁盘文件级加密，支持国密算法。

7）根据《财政部 工业和信息化部关于印发《数据库政府采购需求标准（2023 年版）》的通知》财库〔2023〕35 号文件要求，数据库产品需通过中国信息安全测评中心或国家保密科技测评中心的安全可靠测评，且在集中式数据库目录中。

8）具备多模态特性，支持内存引擎、向量数据库引擎，支持基于数据库内核本身，不通过插件或第三方软件的内置行列混存。

9）针对系统管理员用户，可实现表对象的控制权和访问权分离，即系统管理员用户包括初始用户在未经其授权前，只能进行控制操作（DROP、ALTER、TRUNCATE），无权进行 INSERT、DELETE、SELECT 、UPDATE、COPY、GRANT、REVOKE、ALTER OWNER 等访问操作。

10）提供专业的迁移工具进行异构数据库迁移，支持通过扫描 MyBatis 的 mapper 文件进行兼容性评估。

11）具备 64bit 事务 ID（XID)的特性，可有效规避发生 XID 回卷宕机的风险。

12)支持 B-TREE 索引、GIN 倒排索引、Gist 空间索引、UBtree、HybridANN 索引和 Graph_Index 索引，索引可以自动更新，可以自适应标量选择率。支持同一模式（schema）下不同表创建同名索引，支持中文的全文检索功能，能够支持 like 操作符的全文检索，中文全文检索功能不依赖中文词典。

13）提供轻量化数据库运维诊断工具，同一款工具内需同时具备以下能力：支持深度性能诊断能力，包括一键生成火焰图、一键 SQL 健康检查（包括执行计划、表统计、索引统计、列统计、分区统计、SQL 统计和优化参数等详细信息检查）；具备底层系统监控能力，包括一键获取硬盘底层信息、实时网络监控、系统性能数据收集等；支持历史数据回溯分析能力，包括一键历史会话分析、一键历史内存统计以及历史 TPS 统计。支持对物理坏块的分页恢复功能。（注：“一键”可以是图形化工具的一键操作，也可以是单条指令操作）

14）提供命令行辅助运维工具，支持对数据库的 redo/wal 日志生成 WAL 生成速率、按时间段的 WAL 生成量统计、重放和复制延迟分析，支持对文件进行底层健康度检查，验证 xlog 文件的完整性和连续性；可对指定 XLOG 文件区间内的各对象的操作记录分析，包括统计每秒的提交次数、redo 大小、条目数和类型占比；工具同时具备快速配置集群多节点间的 SSH 免密互信，支持设置模式和验证模式，支持通过命令快速共享主目录环境设置。

4.2.3.6 SSL 站点证书服务

1）提供 12 个 SSL 站点证书服务。

2）支持颁发采用国密算法的 SSL 数字证书。

3）支持根证书的发放，可以导入到数据保密服务工具中进行证书的卸载。

4.3 国产操作系统服务

1）中文支持：提供中文输入法支持；支持最新国家标准字符集（如：GB18030-2005）。

2）架构要求：支持飞腾、鲲鹏、龙芯、兆芯、海光、申威等主流国产 CPU，支持 Intel、AMD 等 X86 架构 CPU。

3）文件系统：支持 Ext3、Ext4、GFS2、XFS、NTFS 等文件系统；

4）存储支持：内置支持快速块设备作为慢速块设备缓存以加速 IO；支持 swap 压缩；支持 FCoE、iSCSI，支持将 Ceph 块设备视为常规磁盘设备条目；

5）云原生支持：支持 KVM、Docker、LXC 虚拟化，以及 Ceph、GlusterFS、OpenStack、k8s 等原生技术生态，实现对容器、虚拟化、云平台、大数据等云原生应用的良好支持。

6）配套支持：支持同品牌的高可用集群、云平台软件、服务器虚拟化系统、安全云桌面管理软件等配套产品，需提供产品彩页等证明。

7）数据库兼容性：兼容人大金仓、达梦、神舟通用、南大通用或等同数据库。

8）中间件兼容性：兼容中创、东方通、金蝶、宝兰德或等同中间件。

9)虚拟化及云平台兼容性:支持 KVM 虚拟化,内置单机虚拟化管理程序,支持 KVM、Docker、LXC 等虚拟化方式，内置单机虚拟化管理程序，支持主流云平台华为云、阿里云、腾讯云等。

10）常用应用支持：默认支持 apache http、ftp、DNS、DHCP、NFS、Samba、LDAP 等应用。

11）操作系统产品符合 CGL5.0 标准。

12）根据《关于印发《操作系统政府采购需求标准（2023 年版）》的通知》财库〔2023〕34 号文件要求，操作系统需通过中国信息安全测评中心或国家保密科技测评中心的安全可靠测评，且在操作系统目录中。

4.5 国产中间件服务

1）支持虚拟机、物理机、容器环境部署，支持轻量版本和 springboot 环境使用版本。

2）支持多服务器集群部署、负载均衡，支持 Web 层的集群和 EJB 集群。

3）提供完善的集群技术与 Session 管理，支持 Session 数据配置接入分布式缓存如 Redis 集群等，实现 Session 数据的独立管理。

4）中间件产品支持集群部署，支持故障自动隔离功能，支持对异常退出实例的自动状态检

测，支持单个节点失效并重启后，在集群中能够自动重新提供服务。

5）支持通过界面进行补丁升级、回退操作。

4.6 数据备份服务

1）提供云主机、数据库等数据备份服务，备份系统提供统一管理平台进行管理。

2）支持任意历史时间点的数据恢复，时间精度可以达到百万分之一秒，即 0.000001 秒，RPO ≈0。

3）支持云主机备份作业带宽控制功能，支持云主机备份作业压缩和加密功能。

4）支持代理实现跨网络数据传输，支持业务主机和管理主机所在网络隔离的场景。

5）支持部署一套程序即可实现同一个源库的多作业并发，无需启动多个进程进行并发作业操作。

6）支持缓存技术与断点续传技术。

7）支持区间带宽限速功能，可以根据工作时段灵活配置多条细粒度限速策略。

第五条 计费方式及支付方式

5.1 计费方式

本项目为按照甲方需求以购买服务的方式向乙方购买相关服务，并根据实际购买服务结算费用。

5.1.1 甲方购买服务应按照《服务内容及价格表》（见附件 1）内约定服务内容进行购买，如有其他服务需求，需签订补充协议补充服务内容后再购买。

5.1.2 甲方购买服务的期限不能超过本合同服务期限，如有超出只需计算本合同服务期内实际使用服务内容及数量。

5.1.3 结合以上 5.1.1、5.1.2 条款内容，以甲方最终在本合同服务期内实际使用的服务内容及数量，依据本合同服务期约定的《服务内容及价格表》（见附件 1）进行本合同服务期计费计算。

5.2 支付方式

本项目价款以人民币结算，合同总价款暂定为人民币 9,606,688.80 元，具体结算金额以财政实际批复为准。根据教育云平台所需要的计算资源和存储资源的实际使用量进行结算。

5.2.1 第一笔款：自服务期开始之日起半年内，甲方收到乙方提供的发票后 10 个工作日内，向乙方支付服务费￥4,803,344.40 元（大写：人民币肆佰捌拾万叁仟叁佰肆拾肆元肆角）。

5.2.2 尾款：服务期结束后 60 个工作日内，乙方提供甲方本合同服务期服务费用说明（以本合同 5.1 计费方式条款约定的计费方式计算得出），甲方核实后结算本合同服务期剩余服务费。

5.2.3 合同执行过程中，乙方应按月提供每月实际使用费用账单，如出现本合同服务期服务费用超过本项目预算资金的趋势，乙方应及时提示甲方追加预算。

5.2.4 服务期满一年后，由甲方委托第三方具备相关资质的审计单位对合同所涉及服务费结算进行审核。

5.2.5 乙方知晓甲方支付款项来源于财政拨款，若因财政拨款未及时到账导致甲方付款延迟的，付款时间自动顺延，具体付款时间以财政资金到账时间为准。顺延期间，甲方不承担违约责任。

5.2.6 甲方付款前，乙方应向甲方提供等额、合法、有效的增值税普通发票。因乙方未及时提供发票或者发票有问题，甲方可延迟付款，相应责任由乙方承担，甲方不承担违约责任。

第六条 交付工期及验收

6.1 交付期

6.1.1 乙方在签订合同后 60 个工作日内完成合同规定的区教育云平台搭建和部署，满足业务上线要求。

6.1.2 乙方完成区教育云平台搭建和部署，并通过测试验收后，开始计算服务期，服务期为期一年。在服务期中，乙方需根据服务需求提供相应的资源服务以及现场驻场服务。

6.2 验收

6.2.1 甲方在签订合同后 60 个工作日内对乙方提供的教育云服务进行测试，测试通过即为验收合格。

6.2.2 如乙方提供的区教育云服务未达到项目招标要求，无法通过测试，乙方应在甲方要求的期限内进行整改。若经 2 次整改后仍不合格，甲方有权单方解除合同，乙方应退还甲方已支付的全部款项，并向甲方支付合同暂定总价款 20%的违约金。违约金不足以弥补损失的，乙方应继续予以赔偿。

第七条 双方权利和义务

7.1 甲方的权利和义务

7.1.1 合同执行期间，区教育云使用的基础 IT 资源所有权归乙方所有，教育云服务资源使用流程由乙方根据甲方要求统一制定，教育云服务资源使用权归甲方所有，区教育云上的相关数据所有权归甲方所有。

7.1.2 甲方委托乙方利用教育云服务资源为为全区教育领域相关单位的信息系统提供基础 IT 资源支撑和统一规范服务管理。所有经甲方批准部署在区教育云的信息系统，如涉及乙方提供的第三方软件许可使用，甲方同意遵守相关许可协议的约束；所有经甲方批准部署在区教育云的信息系统，甲方负责协调相关使用单位自行解决云服务器上所需要的非乙方提供的软件版权（许可/使用权），并负责数据的完整性和保密性；甲方负责协调相关使用单位不在区教育云上安装、使用盗版软件，并支持乙方拒绝对使用盗版软件的相关使用单位信息系统在区教育云上部署。若乙方侵犯第三方权利，由乙方自行处理。

7.1.3 甲方应明确要求全区教育领域相关单位用户对于部署在区教育云上的信息系统声明内

容责任自负，如内容中有违反政策法规的情况，由业务所有方承担全部责任。

7.1.4 甲方应按时向乙方缴纳本合同约定的费用。

7.2 乙方的权利和义务

7.2.1 乙方应按照合同约定为甲方提供服务。

7.2.2 乙方对云服务器进行日常维护和监控，以保证其正常运行。

7.2.3 乙方负责提供操作系统，并提供网络环境及教育云安全服务。

7.2.4 乙方为甲方提供每周 7 天×24 小时售后服务，并为甲方提供有效的联系方式。

7.2.5 乙方应严格遵守保密义务，除非双方另有书面约定，乙方承认甲方存放在区教育云上的任何资料、软件、数据等的知识产权均与乙方无关，乙方无权复制、传播、转让、允许或提供他人使用这些资源。

7.2.6 如服务出现任何问题，乙方应优先协调各方资源处理解决，不推卸、推诿。

7.2.7 如果第三方机构或个人对甲方提出质疑或投诉，乙方将通知甲方，甲方有责任在规定时间内进行说明并出具证明材料，如甲方未能提供相反证据或逾期未能反馈的，乙方将采取包括但不限于立即终止服务、中止服务或删除相应信息等处理措施。

7.2.8 因不可抗力因素和甲方原因，造成服务的正常工作中断，乙方不承担责任。

7.2.9 根据甲方需要，在满足乙方技术环境的前提下，乙方应积极配合甲方及其委托的第三方对甲方购买的云服务进行安全审查工作；

7.2.10 云计算服务之间的交互而引起的网络流量属于乙方提供的服务范畴。

7.2.11 在未取得甲方同意的情况下，乙方不得通过任何手段收集、分析、处理、篡改区教育云中的数据。禁止数据以任何方式渠道泄露出去。

7.2.12 乙方不得私自将未经甲方审核的系统部署在区教育云。

第八条 违约责任

8.1 甲乙双方任何一方不履行合同义务或者履行合同义务不符合本合同约定的，均视为违约。守约方可向违约方发出要求其履行合同义务的书面通知，违约方应在通知发出之日起 5 个工作日内采取补救措施，逾期仍未采取措施的，则守约方有权要求违约方继续履行合同义务并赔偿因此造成的损失。

8.2 甲乙双方在完成双方签署的书面确认事项后，任何一方提出变更要求，导致项目进度延迟的，不视为对方违约。

8.3 因甲乙双方任何一方的原因致使另一方遭受第三方追诉的，违约方应赔偿由此给另一方造成的损失。

8.4 因甲方的原因或与甲方具有协作关系的第三方的原因导致项目进度延迟的，乙方不承担违约责任，因此而给乙方增加工作量的，甲方应按照双方协商一致的确认结果给予补偿。

8.5 乙方提供服务过程中可能发生的违约行为及应承担的违约责任见附件：违约行为处罚细则。违约罚款均以人民币结算。

第九条 知识产权及保密

9.1 除以下第九条第 9.2 款另有规定外，甲方和乙方应当各自就其或其雇员、承包商、顾问或代理人获得的关于本合同及本项目（无论是财务上、技术上或其他方面）的全部信息和文件，予以保密。

9.2 以上第九条第 9.1 款不适用于：

9.2.1 已经公布的或能以其他方式公开获得的信息或文件（但不包括以违反本合同的方式公布或获得者）。

9.2.2 已经由一方以不违反任何保密义务的方式获得的信息或文件。

9.2.3 以不违反任何保密义务的方式从第三方获得的信息或文件。

9.2.4 按照法律须披露的信息或文件。

9.2.5 为按照本合同履行一方义务而披露的信息或文件。

9.3 以上第九条第 9.1 款在本合同届满或终止后的十年内仍然有效。甲乙双方对彼此之间相互提供的信息、资料以及本合同的具体内容负有保密责任。

第十条 甲方数据的保存、销毁与迁移

10.1 根据法律有关规定或者行政、司法机构的要求，经甲方同意，乙方可以向第三方或者行政、司法机构提供数据审查。

10.2 除法定及甲乙另行约定外，自本合同服务期满或因任何原因导致本合同提前终止之日起的 60 个工作日内，乙方应继续存储甲方的数据。逾期乙方将不再保留甲方数据，甲方需自行承担其数据被销毁后引发的一切后果。

10.3 甲方要求删除数据或设备在弃置、转售前，乙方需将其所有数据彻底删除，并无法复原。

10.4 乙方承诺甲方启用或弃用云服务时将配合甲方完成数据的迁入和迁出。

第十一条 不可抗力

11.1 本合同中不可抗力指地震、台风、火灾、水灾、战争、罢工以及其他双方共同认同的不能预见、不能避免并不能克服的客观情况。

11.2 如发生不可抗力，以至于任何一方因这种事件的发生而无法履行或无法完全履行其义务，一方对另一方因此而造成的损失不承担责任。但在不可抗力发生期间及结束之后，在合同的履行仍有意义时，受影响的一方仍应在可能的范围内履行己方的义务，以尽可能减少损失的发生。

11.3 遇有上述不可抗力事件的一方，应在可能的时候立即将事件情况通知对方，并在该事件发生后 15 日内向对方提供政府部门开具的有效证明文件，同时提出合同需要延期履行或不能完全履行或不能履行的理由。按照该事件对合同履行的影响程度，由双方友好协商决定继续履行合同或终止合同。

11.4 一方迟延履行后发生不可抗力的，仍应承担违约责任。

第十二条 合同变更

12.1 因项目需求发生变化，需要对合同内容进行变更的，需经双方书面确认。

第十三条 争议解决

13.1 因履行本合同或与本合同有关的一切争议，双方当事人应通过友好协商方式解决，若任一方不愿协商的，双方均可向合同签署地有管辖权的人民法院提起诉讼。除非生效裁判另有规定，各方为解决争议而实际支付的费用（包括但不限于诉讼费、保全费、评估费、拍卖费、执行费、合理的律师费等）由诉讼请求未被支持的一方承担。

13.2 在诉讼过程中，除各方有争议的部分外，本合同其他部分继续有效。

第十四条 服务期限与终止

14.1 本合同自双方法定代表人或授权代表签字并加盖单位公章或合同专用章之日起生效，双方履行完合同规定的义务后自行终止。合同服务期为 2026 年 11 月 1 日至 2027 年 10 月 31 日。

14.2 服务费用按年结算，第一年服务期结束后，在不改变合同其他条款的情况下，甲方可视服务情况与乙方续签合同，续签次数不得超过两次，总服务期限不得超过三年。本合同为第一年服务期合同。

14.3 发生下列情形，服务期限提前终止：

14.3.1 双方协商一致提前终止的。

14.3.2 甲乙任何一方单方面提出终止合同，需提前三个月通知对方，双方协商解决。

14.3.3 甲方违反本合同条款的，包括但不限于未按照合同约定履行付款义务或严重违反法律规定等。

第十五条 合同份数及附件

本合同正本一式柒份，具有同等法律效力。甲方执叁份，乙方执叁份，海淀区政府采购中心执壹份。

附件：1.服务内容及价格表；

2.乙方服务要求及违约行为处罚细则

合同签署页

甲方	单位名称	北京市海淀区大数据中心（盖章）
	法定代表人（或授权代表）	签字：
	项目负责人	常子儒
	电　　话	13439887101
	邮政编码	100081
	地　　址	北京市海淀区中关村南大街 5 号
	纳税人识别号	12110108MB09868857
乙方	单位名称	（盖章）
	法定代表人（或授权代表）	签字：
	项目负责人	张泽辉
	电　　话	13810763310
	开户银行	中国建设银行北京新华支行
	账　　号	11001014600053013746
	邮政编码	100007
	地　　址	北京市东城区东直门南大街 7 号
签署日期		2026 年 7 月 8 日

附件 1.服务内容及价格表

序号	服务内容		规格和要求				单位	数量	单价
一	资源管理及安全服务	资源管理及安全保障服务	1.资源管理服务 1）运维团队提供不少于 5 人专业运维工程师驻场服务，工作日白天（5*8 小时）不少于 4 人值班服务，工作日夜间（5*16）小时及节假日（24 小时）不少于 1 人值守服务； 2）提供云资源、网络资源及安全策略的配置管理服务；提供系统入云部署及云资源使用等方面的技术支持，提供入云系统运行监测及云资源使用优化服务，配合入云系统进行运行故障、安全事件应急处置，提供云资源管理及入云系统安全监测运维周报； 3）重要时期安全保障服务，在重要节日、重大活动、重要会议等关键时期，为保障信息安全所采取的一系列安全保障措施。 2.安全保障服务 1）提供满足国家等保三级防护标准，以及国家密码应用建设的云平台安全防护体系； 2）提供高效、合理、可靠的安全保障服务，包括但不限于远程接入服务、运维堡垒机、数据库审计、日志审计、web 应用防火墙、主机安全等服务； 3）提供云平台及入云系统整体漏扫服务，每季度至少开展一次，涵盖云平台上的所有关键组件和服务。				套	1	160000/月
二	国产云资源服务	云主机	国产 CPU	按使用量计费	1 核	元/月	台	4970	14.02
			内存	按使用量计费	1G	元/月		13254	22.5
		云存储	普通性能	按使用量计费	1TB	元/T/月	T	250TB	102.4
			高性能	按使用量计费	1TB	元/T/月	T	200TB	307.2
			静态存储	按使用量计费	1TB	元/T/月	T	100TB	72.75
		操作系统	国产操作系统	按使用量计费	套	元/套/月	套	487	29
		数据库	国产数据库	按使用量计费	套	元/套/月	套	70	237.5
		中间件	国产中间件	按使用量计费	套	元/套/月	套	50	59
三	备份服务	数据备份	国产化备份平台服务	按使用量计费	1TB	元/T/月	T	550	263

附件 2.乙方服务要求及违约行为处罚细则

第一条 乙方提供的服务要求

1.1 为保障上云系统的正常运行，乙方每天应进行 2 次教育云健康检查，检查内容包括但不限于教育云控制节点、计算节点、存储节点、数据库集群，并将检查报告通报甲方。

1.2 乙方应对检查过程中发现的教育云软硬件风险隐患进行修复维护；在维护操作前，乙方应向甲方提交实施方案，说明处置流程和处置人员，经甲方批准后，严格按方案实施操作，操作完成后向甲方通报结果，并记录备案。

1.3 乙方进行教育云系统版本迭代前，应向甲方提交风险评估报告和测试报告，确保甲方信息系统在不同版本环境下均可稳定运行。

1.4 乙方应根据甲方信息系统上云计划，提前进行教育云扩容所需物理服务器、网络设备、互联网带宽等资源的部署，并保证教育云可用资源冗余不少于现有资源的 20%。

1.5 乙方应根据国家互联网应急中心公布的威胁预警情报对教育云上的系统和软件进行全面的漏洞扫描与病毒查杀，发现问题应及时进行处置并通报甲方。

1.6 乙方应持续优化教育云安全组策略和防火墙入站规则，加强教育云的安全访问控制策略，形成双重保险机制。

1.7 乙方应持续升级完善教育云安全防护系统，加强教育云用户侧的安全防护功能；对涉及民生、教育、医疗、政务等重要信息系统应进行重点防护。

1.8 乙方接到甲方故障通报后，应及时处理，做好相关信息的登记工作，定时向甲方反馈处置进度及结果；故障排除后，乙方应向甲方提交故障发生及处置过程中全部软硬件日志和故障分析报告，明确故障原因和整改措施，并严格落实整改措施，杜绝类似故障再次发生。

1.9 乙方应确保教育云运维人员符合岗位要求，运维人员到岗前，需经过全面系统的技术培训、安全培训、保密事项培训。

1.10 乙方应确保教育云运维团队稳定，运维人员变动需提前一个月通知甲方。

第二条 乙方违约处罚细则

乙方服务期内未能达到合同及附件的约定的服务标准，发生违约行为，甲方将按相应违约行为进行处罚。违约行为分为重大违约行为、严重违约行为和一般违约行为。

2.1 乙方重大违约行为

乙方服务期内的违约行为造成教育云整体故障（非不可抗拒力条件下）或重大安全事故的（根据其严重程度分为 A 级事件和 B 级事件）。乙方触发该 A 级事件或一年内三次及以上 B 级事件违约行为，甲方有权解除本协议，并要求乙方赔偿甲方相应的经济损失。

一年内 B 级事件发生少于三次，罚款金额=当月教育云服务费*30%。

类别		范围	影响	影响时间	事件级别	次数
重大安全事故（乙方主责）	服务中断	教育云整体	因非不可抗力造成超过 30%以上业务系统中断、影响人数 50 万以上、导致 500 万元以上经济损失。	2 小时以上	A 级	1 次
	重大篡改事件	应用系统	在重大或特别重大保障期间，因乙方的安全隐患原因造成的系统被恶意篡改事件。事件发生后乙方未按照应急预案进行处置，造成信息安全事件处置延误。且该事件被国家级机构或媒体通报、市级领导批示或关注的。	30 分钟以上		
	数据丢失	等保三级或重要业务系统的核心业务数据	因非不可抗力造成的教育云超过 3 个业务系统丢失超过 1 个月以上的数据，且确认无法恢复。	——		
	恶意入侵攻击	等保三级或重要业务系统	被第三方安全机构通报教育云存在安全隐患，乙方未在 24 小时内做有效处置或应急防护措施，造成业务系统在重大或特别重大保障期间被恶意篡改或敏感信息泄露事件。	——		
	服务中断	教育云整体	因非不可抗力造成超过 10%至 30%业务系统中断、影响人数 10 万以上、导致 100 万元以上经济损失。	2 小时以上	B 级	一年内 3 次以上
	重大篡改事件	应用系统	因乙方的安全隐患原因造成的系统被恶意篡改事件，事件发生后乙方未按照应急预案进行处置，造成信息安全事件处置延误，且该事件被市级机构或媒体通报、区领导批示或关注的。	30 分钟以上		
	数据丢失	业务系统核心业务数据	因非不可抗力造成 1 个业务系统丢失超过 1 个月以上的数据，且确认无法恢复。	——		
	恶意入侵攻击	业务系统	被第三方安全机构通报教育云存在安全隐患，乙方未在 24 小时内做有效处置或应急防护措施，造成业务	——		

类别		范围	影响	影响时间	事件级别	次数
			系统被恶意篡改或敏感信息泄露事件。			

2.2 乙方严重违约行为

乙方在服务期内的违约行为对用户业务系统产生一定的经济损失，但其影响和经济损失未达到重大违约行为中规定的 B 级事件的。

罚款金额=业务系统所使用的云资源服务费/服务月数*惩罚系数。

序号	问题描述	惩罚系数
1	所提供的云服务器可用性低于 99.95%，数据可用性低于 99.999%，网络可用性低于 99.99%，出现问题并造成重大损失的	200%
2	因未做好系统和数据互备，由于教育云一期服务中断，而导致系统和数据无法正常应用的，但影响未达到 B 级及以上事故影响的	200%
3	因所提供的安全服务出现故障，导致某系统网页被篡改，造成重大影响	600%
4	因所提供的安全服务出现故障，导致某系统数据丢失，造成重大影响	600%
5	因所提供的安全服务出现故障，导致某系统被入侵，造成重大影响	600%
6	在甲方已发出整改通知后未正确处置，出现问题并造成重大事故	200%

2.3 乙方一般违约行为

乙方在服务期的违约行为对用户业务系统造成的影响未达到重大违约行为和严重违约行为的其他违约行为。

罚款金额=业务系统所使用的云资源服务费/服务月数*惩罚系数。

序号	问题描述	惩罚系数
1	所提供的云服务器可用性低于 99.95%，数据可用性低于 99.999%，网络可用性低于 99.99%，出现问题但未造成重大损失的	50%
2	所提供的云服务器可用性低于 99.95%，或数据可用性低于 99.999%，网络可用性低于 99.99%，且在服务期内接到委办局投诉此类情况 3 次以上的	20%
3	在运维期间，甲方对乙方实施月度考核，如乙方连续 3 次未能通过考核，经限期整改后仍不能达到甲方要求的	20%
4	在运维期内，如乙方未能按照用户方的扩容需求，在 14 个自然日内完成教育云的资源扩容，且经管理单位书面通知仍未能限期满足用户需求的	20%
5	因所提供的云服务或安全服务出现故障，造成某系统宕机 2 小时以上	30%

6	因所提供的云服务或安全服务出现故障，造成某系统连续宕机 3 次以上或累计 8 小时以上	60%
7	在甲方已发出整改通知后未正确处置，出现问题的，未造成重大影响	50%

中国移动 China Mobile

中国移动 China Mobile