**浦东教育云租用服务项目招标需求**

一、说明

**1 总则**

1.1 投标人应具备国家或行业管理部门规定的，在本市实施本项目所需的资格（资质）和相关手续（如果有），由此引起的所有有关事宜及费用由投标人自行负责。

1.2 投标人对所提供的系统应当享有合法的所有权，没有侵犯任何第三方的知识产权、技术秘密等权利，而且不存在任何抵押、留置、查封等产权瑕疵。

1.3 投标人提供的货物应当是全新的、未使用过的，货物和相关服务应当符合招标文件的要求，并且其质量完全符合国家标准、行业标准或地方标准。

1.4 投标人应如实准确地填写投标货物的规格型号、技术参数、品牌、产地等相关信息，因上述信息内容填写不完整、不准确，而导致投标文件被误读、漏读，由投标人自行负责，为此投标人需承担其投标文件在评标时被扣分甚至被认定为无效投标的风险。

★1.5若本项目涉及国家强制认证产品（信息安全产品、3C认证产品、强制节能产品、电信设备进网许可证等），则根据国家有关规定，投标人提供的产品必须满足强制认证要求。（详见第一章投标人须知及前附表21.3（9））

★1.6投标人提供的产品和服务必须符合国家强制性标准。

1.7 采购人在技术需求和图纸或图片（如果有）中指出的工艺、材料和货物的标准以及参照的技术参数或型号仅起说明作用，并没有任何限制性和排他性，投标人在投标中可以选用其他替代标准、技术参数或型号，但这些替代要在不影响功能实现的前提下，并在可接受范围内接受偏离。

1.8 投标人在投标前应认真了解采购人的使用需求、使用条件（使用空间、能源条件等）和其他相关条件，一旦中标，应按照招标文件和合同规定的要求提供货物及相关服务。

1.9 投标人应根据本章节中详细技术规格要求，采用市场主流产品或按照要求提供定制产品参加竞标。同时，**请投标人务必注意：无论是正偏离还是负偏离，都不得与招标要求相差太大，否则将可能影响投标人的得分**。一旦中标，投标人应按投标文件的承诺签订合同并提供相应的产品和服务。

1.10本项目如涉及软件开发，则开发软件（包括软件、源程序、数据文件、文档、记录、工作日志、或其它和该合同有关的资料的）的全部知识产权归采购人所有。投标人向采购人交付使用的软件系统已享有知识产权的，采购人可在合同文件明确的范围内自主使用。支撑该系统开发和运行的第三方编制的软件的知识产权仍属于第三方。如采购人使用该软件系统构成上述侵权的，则由投标人承担全部责任。

1.11投标人认为招标文件（包括招标补充文件）存在排他性或歧视性条款，可在收到或下载招标文件之日起七个工作日内提出，并附相关证据。

二、项目概况

**2项目名称**

浦东教育云租用服务项目

**3项目地点**

浦东新区。

**4 招标范围与内容**

4.1 项目背景及现状

（1）项目背景

云计算，是加快推进教育信息化，促进教育应用健康可持续发展的重要途径之一。中央政府多次发布相关的规划、指导意见，推动行业信息化发展。2015年1月30日，国务院发布了《关于促进云计算创新发展培育信息产业新业态的意见》。意见指出，到 2017年，云计算在重点领域的应用得到深化，产业链条基本健全；形成若干具有较强创新能力的公共云计算骨干服务企业；云计算系统集成能力显著提升等规定，到2020年，云计算应用基本普及，云计算服务能力达到国际先进水平，掌握云计算关键技术，形成若干具有较强国际竞争力的云计算骨干企业。云计算信息安全监管体系和法规体系健全。云计算成为我国信息化重要形态和建设网络强国的重要支撑，推动经济社会各领域信息化水平大幅提高。

2022年，《浦东新区教育数字化转型工作方案》指出：要“重构浦东教育数字化转型“1134”体系”，“其中，第一个‘1’是指一张浦东教育基础云网，包括浦东教育专网、浦东教育混合云、学校校园网络，它是孕育浦东教育数字化转型的新动能。”浦东教育云是浦东教育基础云网的重要组成部分，为浦东新区基础教育各类教育机构和学校提供优质的基础计算存储资源，用以部署各类教育、教学应用平台，并提供相关运维和安全服务。

结合《教育部等六部门关于推进教育新型基础设施建设构建高质量教育支撑体系的指导意见》、《上海市教育发展十四五规划》、《浦东新区全面推进城市数字化转型“十四五”规划》等政策指导意见，浦东教育云作为浦东数字化转型1134体系的关键云网基石，将发挥越来越重要的作用。在未来的三年内，各类智慧教育应用需求蓬勃发展，基于三大助手的智能化教学、两个100所“人工智能教与教人工智能”、区校一体化的数字基座、约50所智慧校园等各类智慧教育应用需求对浦东教育云提出更高的资源和能力要求。在满足存量应用部署的需求上，需满足存量应用国产化改造及新增应用信创部署的需求，以及相关的配套服务需求。

（2）项目现状

浦东基础教育系统内区域层面的重点应用基本已全部部署在浦东教育云平台上，包括浦东教育人力资源协同管理平台、会计核算中心财务平台、浦东新区适龄幼儿入园报名系统、浦东教师专业发展支持系统、教学质量管理系统、浦东新区人工智能与编程教育项目、浦东新区教育大数据中心智能服务平台等；学校层面也有较多应用部署在浦东教育云平台上，包括智慧校园及门户网站等。截至2023年10月，原浦东教育云共承载140个应用系统，部署773台云主机和3台物理机，虚机分配vCPU共计4763核、内存共计13548GB、存储共计1091TB。

为满足浦东新区教育数字化转型的进一步发展需求，需购买新一轮的浦东新区教育云租用服务（三年），通过集约化专业服务提高信息化基础设施运行质量、降低整体计算资源基础设施投入成本，统一建立和管理安全防护体系，进一步提升浦东新区教育信息化发展能级。存量系统期初全部由非信创资源池承载，新增系统全部由信创资源池承载。随着国产化演进的推进，按需将部分非信创资源逐步变更为等量的信创资源，变更上限为期初采购非信创资源总量的20%（服务期内不额外支付费用）。

如涉及云平台迁移，中标服务商应保障整体云平台及存量应用迁移的及时性、数据完整性、系统稳定性、IP地址的一致性，并承担相关的全部迁移成本。

4.2 项目招标范围及内容

本项目采购服务主要为采购浦东教育云租用服务，为浦东新区教育单位各类业务系统提供计算、存储、网络等基础教育云资源服务，并提供国产操作系统、国产数据库、定制云盘、短信服务等基础应用支持服务，以及配套的云安全服务和运维服务。

4.3本项目工期为：自合同签订之日起36个月，具体以合同约定为准。

**5 承包方式**

5.1 依据本项目的招标范围和内容，中标人以包系统设计、包供货、包安装集成调试、包质量、包安全的方式实施总承包。

5.2本项目不允许分包。

**6 合同的签订**

6.1 本项目合同的标的、价格、质量及验收标准、考核管理、履约期限等主要条款应当与招标文件和中标人投标文件的内容一致，并互相补充和解释。

**7 结算原则和支付方式**

7.1 结算原则

7.1.1本项目合同结算价以审计价为准，中标人的中标单价不变，实际工作量以采购人或第三方按照招标文件规定的验收标准核定为准。

7.1.2发生设备维修的，如该设备尚在质保期内的，采购人不另行支付相关费用；如在质保期外的，单价按照投标文件中明确的备品备件单价（含维修人工费）计取，数量按实结算。如投标文件中没有类似备品备件单价可参照的，则由合同双方协商确定维修单价。

7.2 支付方式

7.2.1 本项目合同金额采用**分期付款**方式，在采购人和中标人合同签订，按下款要求支付相应的合同款项。

7.2.2分期付款的时间进度要求和支付比例具体如下：

（1）合同签订后30日内，支付合同总金额40%的预付款；

（2）项目通过第一年度服务验收后30日内，采购人向中标人支付合同总金额的20%。

（3）项目通过第二年度服务验收后30日内，采购人向中标人支付合同总金额的20%。

（4）项目通过第三年度服务总验收后30日内，采购人向中标人支付合同尾款。

7.3中标人因自身原因造成返工的工作量，采购人将不予计量和支付。

7.4采购人不得以法定代表人或者主要负责人变更，履行内部付款流程，或者在合同未作约定的情况下以等待竣工验收批复、决算审计等为由，拒绝或者延迟支付中小企业款项。如发生延迟支付情况，应当支付逾期利息，且利率不行低于合同订立时1年期贷款市场报价利率。

三、技术质量要求

**8 适用技术规范和规范性文件**

《基于云计算的电子政务公共平台技术规范》（GB/T 33780.1-2017）

《IP网络技术要求--网络性能参数与指标》（YD/T 1171-2001）

《综合布线系统工程设计规范》(GB50311-2016）

《数据中心电信设施标准》（ANSI/TIA-942-A-2012）

《数据中心设计规范》（GB50174-2017）

《信息系统密码应用基本要求》（GB/T39786-2021）

《信息安全技术网络安全等级保护基本要求》（GBT22239-2019）

《信息安全技术网络安全等级保护安全设计技术要求》（GBT25070-2019）

《信息安全技术网络安全等级保护测评要求》（GBT28448-2019）

《信息安全技术网络安全等级保护安全管理中心技术要求》（GBT36958-2018）

《信息安全技术操作系统安全技术要求》（GBT20272-2019）

《信息安全技术数据库管理系统安全技术要求》（GBT20273-2019）

《信息安全技术信息系统灾难恢复规范》（GBT20988-2007）

《上海市重要网络和信息系统密码应用与安全性评估工作指南（2023 版）》

各投标人应充分注意，凡涉及国家或行业管理部门颁发的相关规范、规程和标准，无论其是否在本招标文件中列明，中标人应无条件执行。标准、规范等不一致的，以要求高者为准。

**9 招标内容与质量要求**

9.1工作量清单

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 服务内容 | | 单位 | 第一年总量 | 第二年总量 | 第三年总量 | 备注 |
| 一、云资源服务 | | | | | | | |
| 1 | 云主机资源 | 可用CPU（不超分） | 核 | 1822 | 2476 | 2922 |  |
| 2 | 可用内存（不超分） | GB | 21980 | 29112 | 33760 |  |
| 3 | 裸金属 | 可用CPU（不超分） | 核 | 60 | 80 | 120 |  |
| 4 | 可用内存（不超分） | GB | 576 | 768 | 1152 |  |
| 5 | 云存储资源 | 可用生产存储（不超分） | TB | 1583 | 1940 | 2260 |  |
| 6 | 可用备份存储（不超分） | TB | 847 | 1027 | 1187 |  |
| **二、专线网络服务** | | | | | | | |
| 7 | 专线网络服务 | 双路接入教育城域网（单路不低于40G） | 路 | 2 | 2 | 2 |  |
| **三、云安全服务** | | | | | | | |
| 8 | 云安全服务 | 非信创与信创云平台安全配套服务、信创云平台密码服务及租户密码资源池底座 | 套 | 1 | 1 | 1 |  |
| **四、基础应用支持服务** | | | | | | | |
| 9 | 国产操作系统license服务 | 按需提供，麒麟/统信等 | 套 | 300 | 620 | 1080 |  |
| 10 | 国产数据库license服务 | 按需提供，达梦/人大金仓等 | 套 | 15 | 30 | 35 |  |
| 11 | 短信服务 | 多网合一短信服务 | 百万条/套 | 1 | 1 | 1 |  |
| 12 | 云盘服务 | 存储空间(账号与浦东教育统一认证平台对接，不少于4万个） | TB | 24 | 30 | 36 |  |
| 五、云平台业务连续性服务 | | | | | | | |
| 13 | 云平台业务连续性服务 | 需保障云平台业务连续性。若存量系统需迁移，需在中标后1个月内完成原云平台应用迁移 | 一次性 | 1 | 0 | 0 |  |

**说明：1、上表中所列为本次招标的核心工作内容，投标人不得减少核心工作内容数量。**

**2、上表所列数量为采购基准量，每一年对应数量为当年累计到达数，实际报价以此为基础，实际提供量不小于采购基准量。**

9.2具体技术质量需求

**9.2.1整体建设目标**

项目目标：为夯实浦东教育数字化转型的设施基础，提供符合区域整体发展要求的教育云租用服务，构建标准云资源服务体系、应用支撑体系、云安全运维体系，建成浦东新区云资源公共服务信息化支撑体系，实现教育云端全区覆盖。支持以数据赋能课堂教学和教师研训等创新应用部署，提供符合教育者要求的服务供给，为浦东教育数字化转型提供新动能。

本项目采购服务主要为浦东新区教育单位各类业务系统提供计算、存储、网络等基础教育云资源服务，并提供国产操作系统、国产数据库、定制云盘、短信等基础应用支持服务，以及配套的云安全服务和运维服务。主要包括：

（1）教育云资源服务

提供计算、存储、网络等基础教育云资源服务，服务期开始后满足存量应用部署在非信创资源池、新增应用和存量改造应用部署在信创资源池上的需求。并支持使用过程中存量应用按需迁移至信创资源池。

（2）专线网络服务

中标人提供的机房需具备与浦东教育城域网高速互联基本条件，云平台双路接入教育城域网（单路带宽能力不低于40Gbps）。

（3）基础应用支持服务

为支持后续应用系统国产化改造需求，以及满足智慧教育应用发展要求，提供符合信创要求的国产服务器操作系统license、国产数据库license、教育云盘服务、短信服务。

（4）安全配套与运维服务

依托专项运维团队，提供安全配套服务和一站式运维服务。提供平台级安全服务和密码服务，云平台每年通过等保2.0三级测评，信创云平台每年通过密码测评。运维服务结合云管平台对云资源深度融合统一管理和运维，关注用户感知，提供平台资源精细化管理和重保支持等服务，持续提升运营服务质量。

（5）云平台业务连续性服务

本期项目要确保平台服务的业务连续性，中标人需在中标后1个月内提供满足目前平台应用承载现状资源量的平台整体能力，并负责完成云平台整体的无缝割接，确保整体云平台应用的平滑迁移，保障业务IP地址不变以确保业务连续性服务，平台核心应用迁移业务中断时间不超过30分钟，采购人不再额外支付现有云平台应用的迁移费用。

**9.2.2系统参考架构**

本次浦东教育云平台分为信创资源池和非信创资源池两部分。两个资源池共用云平台出口网络，信创资源池需符合国密要求。存量云资源池架构如下：

网络架构：根据不同业务区域的隔离需求划分区域，分为核心交换区、管理区、业务区、存储区。其中，核心交换区承载南北和东西向流量，出口区与浦东教育城域网对接；管理区提供统一的运营运维、灾备等管理系统；存储区为其他各区按需提供相应的存储资源以及数据备份等。

业务区域：业务区分为混合业务区、教育内网业务区（存量）和若干专属业务区（4个以内）。混合业务区承载教育直接面向互联网用户的业务系统，同时承载教育内网业务系统；教育内网业务区承载教育内网业务系统；财务专区等专属业务区独立使用服务器、合并使用交换机与存储），按需扩展。支持按照业务隔离要求，进行计算、存储和网络的物理隔离，也可以参考财务专区模式，仅计算资源物理隔离，其余逻辑隔离。存储区提供各分区的存储资源。

安全能力：提供日志审计、数据库审计、入侵防御、WAF、堡垒机、安全态势感知和探针等平台安全能力。

负载均衡：提供负载均衡能力。

网络出口：通过两路不低于4万兆高速链路接入教育专网核心层，根据云主机IP地址不同，提供教育网或互联网访问能力。

云平台整体分为核心交换区、管理区、业务区，存储区所有区域骨干链路上涉及数据转发设备均需冗余配置。平台支持IPv4/IPv6双栈。

**9.2.3整体服务要求**

中标人需向采购人提供采购需求文件中列明的所有内容的培训和维护服务，提供浦东教育云租用服务，确保服务内容全面且完善。在服务质量方面，中标人需按照约定的服务标准提供各类售后服务，并负责其提供的服务的日常维护及升级工作，确保服务的稳定性和可靠性。

（1）中标人需提供多种技术支持方式，包括热线电话、电子邮件或在线网站等，提供每周7天\*24小时电话响应服务。中标人需提供每周5天\*8小时的日常运维服务，并在重大节点加强保障措施，以确保浦东教育云平台的整体可用性不低于99.99%。

（2）日常监控与巡检工作：中标人需对浦东教育云平台进行日常的监控与巡检，包括监控告警的处理以及巡检中的异常处理等；在执行过程中，中标人需制定完善的维护管理规定，并按照规定中的维护项目、周期和要求，制定详细的作业计划并予以执行。

（3）服务升级：中标人应当承诺，如在日常运维过程中涉及到相关设备服务功能、性能等方面需要升级更新需求，中标人应当在2个工作日内作出响应。经采购人确认升级方案后，中标人按照计划完成升级任务。

（4）云资源扩容：在服务期内，信创云资源申请超过采购基准量时，中标人需要先免费提供云资源使用。采购人为中标人预留3个月扩容时间，发起资源扩容需求。扩容上限为采购基准量的20%。

（5）浦东教育云平台故障处理：处理浦东教育云平台发生的各类软硬件、通信线路等故障，确保上层业务系统能够正常稳定运行；其中故障处理流程需要电子化并规定处理时限及当前处理环节的责任部门和责任人。

（6）业务系统迁移割接与浦东教育云平台软硬件升级割接：中标人需在割接前制定完善的操作实施方案，在方案中尽量降低对上层业务系统的影响。对于任何可能影响上层业务系统的操作，必须进行全面的影响评估，并提前通知采购人具体的操作计划安排。只有在采购人的相关业务部门同意后，方可执行相关操作。此外，中标人需根据采购人的要求提供相关报告，以确保割接工作的准确性和完整性。

（7）系统中断：在因平台软件版本升级等需要中断系统进行平台升级的情况下，中标人需提前至少72小时（若发生重大自然灾害除外）通知采购人，以便采购人做好相关准备工作。在征得采购人同意后，方可进行实施。

（8）中标人提供的平台软件层服务应当包含相应的软件安装介质、软件安装手册、软件使用技术支持以及使用培训等服务。

（9）应急演练与应急响应：针对浦东教育云平台高可用设计特性和各组件的重要性，中标人需进行针对性应急演练，制订相应的应急预案，每年至少组织2次应急演练活动。当发生重大应急事件时，中标人需在采购人的主导下实施应急响应措施，并在事件结束后提交相关事件报告。

（10）安全加固：中标人需定期对浦东教育云平台各个基础组件进行安全策略配置、安全扫描和系统漏洞的加固；

（11）配置实施及管理：中标人需对浦东教育云平台各软硬件设备进行基础配置、IP配置、角色用途、账号密码等的统一配置实施及配置管理，以确保平台正常运行并满足业务需求。

（12）故障处理和响应：中标人须确保对合同服务中出现的故障做出及时响应，并为此制定相应的保证措施。为有效管理故障处理，中标人应建立健全的故障管理体系。该体系应明确故障等级、职责分工及处理界面，确保每个处理流程均有详尽的记录，并明确落实到中标人的相关部门和处理接口人员。针对不同等级的故障，中标人应设定合理的处理时长和故障恢复时限，以确保快速、准确地解决各类故障问题。

（13）节假日保障：在重大节假日期间，中标人需对浦东教育云平台运行和信息安全进行重点保障；以确保平台的稳定性和安全性。

（14）中标人应制定浦东教育云平台使用规范、安全防护管理办法等规范标准，协助各级部门进行相关业务应用系统的部署、运行和安全保障。

（15）中标人应建立一套健全的运维和安全管理制度，以确保项目的顺利实施和长期稳定运行。该制度应包括但不限于以下几个方面：

①日常运行维护管理。例如：故障处理、配置变更、安全策略优化、运行监控等。

②安全保障和监控预警工作。例如：渗透测试、漏洞扫描、安全巡检、应急响应等，安全运维保障制度符合等保2.0第三级标准。

③运维人员管理制度。例如：运维团队人员服务管理、机房进出人员管理等。

**9.2.4服务期考核要求**

9.2.4.1 每年服务期完成80%以上的运维期后，由采购人组织进行专家运维考核评估评分，总分100分，含运维质量保障考核、运维用户满意考核、信息/网络安全、运维总结文档考核四项内容，分值分别为45分、20分、10分、25 分。

（1）运维质量保障

运维故障中，一般故障6小时解决，未达要求的每次扣2分；云平台服务中断等重大故障1小时解决，未达要求的每次扣5分。其他运维需求根据工作量双方协商承诺完成时间，超过协商时间未完成的，应书面说明原因，采购人对原因说明不予认同的，每次扣5分。

（2）运维用户满意

以问卷调查等形式，调查相关教育单位用户，对运维项目的正常运行、功能模块、效率及便捷性、安全性能、运行稳定性、故障处理响应速度及结果、服务水平及保障能力、总体评价等方面的评价情况。满意度采用“五等级制”题目，由“满意”、“较满意”、“一般”、“不满意”和“很不满意”等五个类似组合选项组成。最终得出的满意度按照【（选择“满意”样本数+“较满意”样本数×0.8+“一般”样本数×0.6+“不太满意”×0.4+“很不满意”×0.2）/总样本数×100%】计算得出分数。

（3）信息/网络安全

中标人主动发现运行中的信息安全问题，及时进行处理并未造成通报，不予扣分。对于上级单位和国家相关机构发出的信息/网络安全问题通知，立即进行处置，未造成重大影响的，每次扣5分。对于以上信息/网络安全问题通知，未及时进行处置或者立即进行处置但造成重大影响或被通报的，扣10分。

（4）运维总结文档

由专家对本年度运维工作总结的书写情况（至少包含①运维项目概述、②运维内容及总结、③考核指标完成情况、④系统故障情况分析、⑤运维记录五项内容）进行评估。运维工作总结内容描述均完整合理，条理清晰明白，文档字体格式一致美观，得25分；运维工作总结内容描述比较完整合理，条理比较清晰明白，文档字体格式一致美观，得20分；运维工作总结内容描述一般，条理一般，文档字体格式一般，得15分；运维工作总结内容描述差或条理差或文档字体格式差，得10分；

9.2.4.2 年度运维评估考核后，总评分高于80分（含80分）为运维服务达标；总评分低于 60分（含60分），甲方向乙方提出整改要求，乙方整改后依然不合格，甲方有权提前终止合同。

9.2.4.3 由于中标方服务质量不达标的情况，根据不达标情况，专项落实对采购人的赔偿。因运维事故造成的用户严重损失另行赔付，赔付金额不超过当期服务费用的30%。

附参考打分表（实际以合同约定为准）：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **指标项** | **指标内容** | **指标要求** | **评价细则** | **得分** |
| 运维质量保障（45分） | 保证故障修复和定期巡检等运维服务的及时性和有效性 | 根据工作量双方协商承诺完成时间并按时完成 | 运维故障中，一般故障6小时解决，未达要求的每次扣2分；云平台服务中断等重大故障1小时解决，未达要求的每次扣 5 分。其他运维需求根据工作量双方协商承诺完成时间，超过协商时间未完成的，应书面说明原因，采购人对原因说明不予认同的，每次扣5分。 |  |
| 运维用户满意（20分） | 用户对运维项目的正常运行、功能模块、效率及便捷性、安全性能、运行稳定性、故障处理响应速度及结果、操作培训、服务水平及保障能力、总体评价等方面的评价情况 | 总体满意 | 以问卷调查等形式，调查相关教育单位用户，对运维项目的正常运行、功能模块、效率及便捷性、安全性能、运行稳定性、故障处理响应速度及结果、服务水平及保障能力、总体评价等方面的评价情况。满意度采用“五等级制”题目，由“满意”、“较满意”、“一般”、“不满意”和“很不满意”等五个类似组合选项组成。最终得出的满意度按照【（选择“满意”样本数+“较满意”样本数×0.8+“一般”样本数×0.6+ “不太满意”×0.4+“很不满意”×0.2）/总样本数×100%】计算得出分数。 |  |
| 信息/网络安全（10分） | 主动发现漏洞等网络安全问题，及时进行处理 | 不造成通报 | 中标人主动发现运行中的信息安全问题，及时进行处理并未造成通报，不予扣分。 |  |
| 对于上级单位网络安全问题通知，应立即进行处置 | 不造成重大影响 | 对于上级单位和国家相关机构发出的信息/网络安全问题通知，立即进行处置，未造成重大影响的，每次扣5分。对于以上信息/网络安全问题通知，未及时进行处置或者立即进行处置但造成重大影响或被通报的，扣10分。 |  |
| 运维总结文档（25分） | 本年度运维工作总结的书写情况（含①运维项目概述、②运维内容及总结、③考核指标完成情况、④系统故障情况分析、⑤运维软硬件设备清单、⑥备品备件使用及库存清单、⑦运维记录七项内容） | 专家验收通过 | 运维工作总结内容描述均完整合理，条理清晰明白，文档字体格式一致美观，得25分；运维工作总结内容描述比较完整合理，条理比较清晰明白，文档字体格式一致美观，得20分；运维工作总结内容描述一般，条理一般，文档字体格式一般，得15分；运维工作总结内容描述差或条理差或文档字体格式差，得10分 |  |

**10 技术指标要求**

#### 10.1项目配置需求

|  |  |  |
| --- | --- | --- |
| **服务分类** | **服务内容** | **服务描述** |
| 云资源服务 | 云主机资源 | **资源配置要求：**  提供虚拟机，可以根据业务需要申请可用CPU资源和可用内存资源。  （1）非信创部分：  第一年虚拟化服务器CPU资源按可用物理核不低于1052物理核，可用内存资源不低于13180GB；第二年虚拟化服务器CPU资源按可用物理核不低于1264 物理核，可用内存资源不低于15928GB；第三年虚拟化服务器CPU资源按可用物理核不低于1264物理核，可用内存资源不低于15928GB。  （2）信创部分：  第一年虚拟化服务器CPU资源按可用物理核不低于770 物理核，可用内存资源不低于8800GB；第二年虚拟化服务器CPU资源按可用物理核不低于1212 物理核，可用内存资源不低于13184GB；第三年虚拟化服务器CPU资源按可用物理核不低于1658物理核，可用内存资源不低于17832GB。  **资源性能要求：**  （1）非信创：单台宿主机配置不低于2路10核CPU、384G内存，CPU主频不低于2.2 GHz。  （2）信创：单台宿主机配置不低于2路32核CPU、1024G内存，CPU主频不低于2.2 GHz，CPU架构: x86\_64，硬盘不低于1块480G SSD、1块1920G SSD，网络接口：≥10GE\*2。 |
| 裸金属 | **资源配置要求：**  **（1）非信创部分：**  第一年、第二年、第三年服务器CPU资源不低于60物理核，内存资源不低于576GB；  **（2）信创部分：**  第一年服务器CPU和内存资源暂无需求；第二年服务器CPU资源不低于20物理核，内存资源不低于192GB；第三年服务器CPU资源不低于60物理核，内存资源不低于576GB。  **资源性能要求：**  非信创单台配置不低于2路10核CPU、192G内存，CPU主频不低于2.2 GHz。  信创单台配置不低于2路10核CPU、192G内存，CPU主频不低于2.2 GHz，CPU架构：x86\_64；网络接口：≥25GE MOC2.0\*4。 |
| 云存储资源 | **资源配置要求：**  提供存储资源，可以根据业务申请用于生产过程中数据存储，以及数据备份存储空间。生产存储SSD存储的占比不低于10%，两个区域各自不少于5%。  （1）非信创部分：  第一年用于生产过程中数据存储可用空间不低于1093TB，用于数据备份可用空间不低于602TB；第二年用于生产过程中数据存储可用空间不低于1136TB，用于数据备份可用空间不低于625TB；第三年用于生产过程中数据存储可用空间不低于1136TB，用于数据备份可用空间不低于625TB。  （2）信创部分：  第一年用于生产过程中数据存储可用空间不低于490TB，用于数据备份可用空间不低于245TB；第二年用于生产过程中数据存储可用空间不低于804TB，用于数据备份可用空间不低于402TB；第三年用于生产过程中数据存储可用空间不低于1124TB，用于数据备份可用空间不低于562TB。  资源性能要求：  非信创：生产存储：2台双控，单台不小于512GB缓存；备份存储：单台双控，不小于64GB缓存。  信创：支持分布式EC和三副本数据冗余保护。生产存储：CPU主频≥2.2GHz；备份存储：CPU主频≥2.2GHz。 |
| 专线网络服务 | 专线网络服务 | 双路接入浦东教育城域网（单路不低于40G） |
| 云安全服务 | 云安全服务 | 1套，非信创与信创云平台安全配套服务、信创云平台密码服务及租户密码资源池底座 |
| 基础应用支持服务 | 国产操作系统license | 按需提供麒麟/统信等国产服务器版操作系统License及支持服务。第一年提供License不低于300套；第二年提供License不低于620套；第三年提供License不低于1080套。 |
| 国产数据库license | 按需提供达梦/人大金仓等国产数据库license及支持服务。第一年提供License不低于15套，第二年提供License不低于30套，第三年第一年提供License不低于35套。 |
| 短信服务 | 支持多网合一的短信服务，每年不少于100万条 |
| 云盘服务 | 与浦东教育统一认证平台对接，采用网页方式和客户端方式浏览和操作；服务全区老师，为区级应用和校级试点学校提供云盘服务。考虑业务增长及试点校增加，逐年增加容量规划，第一年提供不低于24TB，第二年提供不低于30TB，第三年提供不低于36TB。 |
| 多云管理服务 | 多云管理平台服务 | 本期需要构建统一云管平台服务，方案应确保非信创云和信创云的统一管理、以及多云接入能力，满足业务弹性伸缩和快速部署要求，实现资源信息、业务信息、运维信息、安全态势信息的展现，准确而高效、精简而全面地传递信息，充分展现浦东教育云的整体运行情况，提供安全可靠的统一的资源服务管理 |
| 云平台业务连续性服务 | 云平台业务连续性服务 | 需保障云平台业务连续性。若存在存量系统迁移，需提供一次性迁移服务，完成整体云平台应用的平滑迁移。涉及原云平台和应用服务商的迁移配合费，由中标人负责。 |

#### 10.2具体技术参数要求

##### 10.2.1机房配套环境要求

投标人提供的物理设备需要按独立的机房区域划分给云平台使用，机房环境需满足云平台承载不中断和高度稳定的要求。

|  |  |  |
| --- | --- | --- |
| **项目** | | **参数要求** |
| 供电 | 供电可用率 | 机房配备双路市电，机架供电可用率为99.97%(百分之九十九点九七)，即用户托管的电源系统每月电力中断时间累积不超过 13分钟 |
| UPS | 机房托管IT设备的不间断供电系统应采用冗余等级为N+1的交流 UPS系统；UPS 系统蓄电池组放电时间不少于满载15分钟； |
| 双路市电 | 提供双路一类市电保障；电压等级10KV，市电容量两路共10000KVA及以上。（如有请提供供电公司相关账单证明） |
| 柴油发电 机 | 机房所在建筑或园区采用柴油发电机作为后备电源，油机数量满足N+1 配置，并可持续不间断供电6小时及以上，提供与加油站签署供油协议，油品不低于沪六标准级别柴油，并承诺 3小时内到场。 |
| 机柜 PDU | 每个机柜要提供两条PDU。机柜两路供电，都有不间断电源保障。（含 PDU电源系统） |
| 制冷 | 机房空调 | 机房所在建筑内制冷系统配置高效能精密空调按照双路市电及油机进行不间断的电源供给，保障空调运行不受电力影响，配制的精密空调满足 N+1的冗余配置，冷通道相对湿度：相对湿度（不大于60%），露点温度（5.5-15℃）且不得结露。服务器进风温度：21℃--26℃ |
| 安防 | 视频监控 | 机房、网络接入间、主要走道和其它重要部位应安装摄像机监视，重要机架及机柜应单独设摄像机监视，录像保存时间不得少于 30 天。 |
| 门禁 | 机房重要部位应安装门禁设备，划分不同人员进出不同区域的权限 |
| 保安 | 安保人员每周7天×24小时值守和监控，机房运维人员每周7天×24小时值班 |
| 消防 | 消防要求 | 消防系统符合本地消防相关标准，通过消防局验收； |
| 网络 | 网络接入 | 具备丰富的专网资源接入能力，具备连通至浦东教育城域网核心节点等重要节点的专线光纤线路。 |
| 运行维护 | 巡检 | 机房每天进行7次及以上例行巡检，并对机房设备运行状态、环境状态进行详细记录。 |
| 应急机制 | 做好机房应急预案，在网络、电力、安全等各方面提供协助，确保采购人应 急人员、设备和供应商能在最短时间内能够进入机房进行应急处置。 |

##### 10.2.2云资源服务技术要求

提供以云主机为主的计算资源服务，云主机可像传统主机一样工作，同时具备更高的弹性资源使用能力、扩展能力、迁移能力，具备更灵活的配置式和快速部署能力。可以通过云平台门户申请虚拟主机资源，对云主机执行重启、关机、启动、销毁、调整配置、远程连接等操作利用虚拟机可以构建与传统物理机一样的计算环境，承载业务应用运行，主要包含处理器（CPU）、内存和硬盘等组件。可根据需求快速创建或销毁一台或多台虚拟机，动态调整配置，快速响应业务需求。提供虚拟机，可以根据业务需要申请可用CPU资源和可用内存资源。

结合计算资源使用，可为虚拟机环境提供各种性能需求和容量需求的存储资源，虚拟硬盘支持创建、挂载、删除和快照等操作。

###### 10.2.2.1非信创云资源技术要求

**（1）云平台功能要求**

|  |  |  |
| --- | --- | --- |
| **指标名称** | | **指标要求** |
| 弹性云主机 | 云主机创建 | 需满足可单台或批量创建不小于100台，创建可指定名称、CPU、内存、系统盘类型、数据盘类型/大小/数量、选择VPC、安全组、添加多块网、弹性IP（不使用、新分配、使用已有）、登录方式（密码、证书）、指定密码。 |
| 云主机管理 | 开机、关机、重启、删除、VNC登录、重装（当前系统）、重置密码、变更规格（升级、降级，关机情况下）、制作镜像（关机情况下）、查询 |
| 云主机规格 | 标准规格：  ➀4vCPU-8G  ➁8vCPU-16G  自定义规格：  最低1核1G、最高32Vcpu-128G |
| 操作系统 | 支持各类主流操作系统，配合用户安装 |
| 云主机特性 | 1、支持SR-IOV方案，东西向流量10G  2、支持GPU实例，满足媒体转码、3D模型等应用场景  3、支持存储密集型实例，满足高IO业务需求  4、支持计算优化型实例  5、支持云主机HA，当云主机宕机时，支持在该宿主机上自动启动云主机；当云主机所在宿主机宕机时，在其它宿主机上自动重启云主机 |
| 云硬盘 | 单块或批量创建 | 创建可指定可用分区、容量、磁盘名称、磁盘类型、通过备份创建 |
| 规格 | SATA（普通IO）、SSD（超高IO） |
| 云备份 | 手动备份 | 支持系统盘、数据盘，首次全备，后续增量，备份数据压缩存储 |
| 自动备份 | 支持按需自动数据备份 |
| 备份创建 | 支持本地/远程备份，支持永久增量备份，每次只需备份变化数据块，减少备份数据量，降低备份成本。 |
| 备份恢复 | 支持云主机整机备份和回滚。 |
| 云镜像 | 虚拟机导出私有镜像 | 支持基于虚拟机创建自定义镜像。 |
| 迁移云主机镜像导入 | 支持自定义镜像导入 |
| 共享镜像 | 将私有镜像共享给区域节点的其它租用、接受别人共享的镜像、基于共享镜像创建云主机 |
| 管理操作 | 基于镜像创建云主机、删除、查询 |
| 弹性负载均衡 | 类型 | 内网负载均衡、外网负载均衡 |
| ELB实例管理 | 创建、停用/启用、调整带宽、删除 |
| 监听器管理 | 修改参数、添加后端云主机、删除 |
| 后端云服务器管理 | 移除、查看健康检查状态 |
| 物理裸机服务 | 不同物理裸机服务满足 | 提供物理裸机服务，支持多台物理机共享同一磁盘卷进行读写 |
| 虚拟私有云 | 创建管理VPC | 支持指定网段、子网名称、可用区、子网名称、网段、网关、DHCP（启动、停用）、DNS设置 |
| 创建管理子网 | 支持子网名称、可用区、子网名称、网段、网关、DHCP（启动、停用）、DNS的设置、修改和删除 |
| 申请弹性IP | 带宽选择（新建、已有）、新建选择计费模式/带宽值 |
| 弹性IP管理 | 绑定、解绑、释放、监控 |
| 云监控 | 总览 | 监控指标数-各项指标数不少于：云主机9个、VPC2个、块存储4个、ELB8个、弹性伸缩5个添加关注指标（可添加9个，可选服务、指标、监控对象） |
| 添加告警规则 | 指定参数：名称、描述、服务类型、指标、监控对象、阈值、出现次数、监控周期、是否发送通知、触发场景（出现告警、恢复正常、数据不足） |
| 告警规格管理 | 启用、停止、修改、删除、查看（告警详情、告警指标趋势） |
| 实例监控管理 | 导出监控报告、查看历史监控信息（3h、12h、24h、1week、1month、自定义时间段）、聚合算法设定（周期、方法-平均、最大、最小、方差）、添加告警规则 |
| 添加告警规则 | 指定参数：名称、描述、服务类型、指标、监控对象、阈值、出现次数、监控周期、是否发送通知、触发场景（出现告警、恢复正常、数据不足） |
| 告警规格管理 | 启用、停止、修改、删除、查看（告警详情、告警指标趋势） |
| 实例监控管理 | 导出监控报告、查看历史监控信息（3h、12h、24h、1week、1month、自定义时间段）、聚合算法设定（周期、方法-平均、最大、最小、方差）、添加告警规则 |

**（2）云资源平台功能要求**

虚拟化管理平台：云资源管理平台要求基于开放的OpenStack架构，并针对云计算数据中心场景进行设计和优化，提供统一的虚拟化功能和资源池管理能力、云基础服务组件和工具、开放标准化的API接口。支持虚拟机和物理机的融合管理、多数据中心融合管理。采用业界主流的虚拟化技术，支持主流的服务器、存储、网络设备以及主流的操作系统、中间件、数据库等软件产品。云资源管理平台需保障平台可用性和业务可用性，支持openstack管理节点主备或负载均衡部署模式，支持弹性伸缩。技术规格要求：

|  |  |  |
| --- | --- | --- |
| **指标名称** | | **指标要求** |
|  | 计算虚拟化 | 支持虚拟机基本的生命周期管理动作，包括创建、删除、启动、关闭、重启等。 |
| 支持虚拟机迁移，使用同一共享存储的主机之间将处于运行态的虚拟机由当前所在的主机迁移到另一台主机上，在迁移的过程中不影响用户对虚拟机的使用。 |
| 支持虚拟机HA(High Available)机制，提升虚拟机的可用度，允许虚拟机出现故障后能够重新在资源池中自动启动虚拟机。 |
| 支持对虚拟机镜像的生命周期管理，支持镜像的创建、上传、删除、下载、查询等操作。 |
| 支持虚拟机之间亲和性部署规则 |
| 网络虚拟化 | 支持SR-IOV网卡直通技术，允许在虚拟机之间高效共享 PCIe 网卡设备，使VM可以直接使用物理的网卡资源实现网络通信，使VM具备高性能、低时延的网络收发能力。 |
| 支持用户虚拟机IP与MAC绑定，防止IP和MAC地址仿冒，防止用户虚拟机DHCP Server仿冒。 |
| 支持SDN功能，提供自动化网络部署功能 |
| 存储虚拟化 | 支持多台虚拟机共享同一磁盘卷进行读写，方便Oraclerac业务部署 |
| 支持存储多路径功能，通过自动优选路径和IO负载均衡选路算法优化，提升存储链路的可靠性和性能。 |
| 支持虚拟机运行时快照功能，虚拟机快照内容包括：虚拟机的电源状态(打开、关闭、挂机)、内存、硬盘、网卡以及CPU寄存器。 |
| 可靠性要求 | 管理节点配置负荷分担部署模式，在保障系统运行的可靠性的情况下，可以平滑扩容管理节点，以便管理更大规模的集群。 |
| 系统支持对Openstack的管理节点的数据备份与恢复操作。支持每日备份、立即备份。备份介质支持第三方FTP或对象存储。 |
| 通过心跳检测机制，实时监控管理进程，及时检测管理进程进程故障或僵死，并支持自动重启状态异常的进程。 |
| 软件合法授权 | | 项目所提供的虚拟化软件和虚机系统软件产品皆为正版软件。如出现版权问题，由中标人承担。 |

###### 10.2.2.2 信创云资源技术要求

|  |  |  |
| --- | --- | --- |
| **指标名称** | | **指标要求** |
| 弹性计算服务 | 生命周期管理与维护 | 支持云主机生命周期管理和维护，包括但不限于创建、启动、关闭、重启、更换操作系统，其中创建、启动、关闭、重启应支持批量操作，提升管理员操作效率。 |
| 指标监控 | 支持对云主机CPU、内存、硬盘等基础指标进行监控，同时支持对云主机系统中的各进程CPU、内存、打开文件数进行监控，为用户提供系统级、主动式、细粒度监控服务。 |
| 功能要求 | 支持云服务器支持完整的虚拟机特性，包括在线变更实例规格、离线变更实例规格、热迁移、冷迁移等。如有请提供功能界面截图证明材料。 |
| 可靠性 | 支持云主机按宿主机、机架、网络交换机物理拓扑的调度能力，提升业务的可靠性。 |
| 裸金属弹性计算服务 | 弹性裸金属实例规格 | 支持弹性裸金属实例规格，提供无虚拟化性能开销和特性损失的计算实例，同时支持VT-x嵌套虚拟化，具备再次虚拟化的能力。满足用户对物理独占、超高性能业务负载的要求。 |
| 挂载云盘 | 裸金属实例可支持最多1+32云盘，支持云盘热插拔，支持基于NVMe协议的云盘多重挂载功能。 |
| 可靠性 | 支持裸金属宕机迁移，当弹性裸金属服务器发生硬件故障时，自动重启迁移到其他裸金属服务器上。如有请提供功能界面截图证明材料。 |
| 兼容性/开放性 | 应支持与其它云产品（例如存储、网络、数据库等）无缝对接，并且完全兼容云主机实例的镜像系统，具体可以使用云主机镜像创建裸金属实例，使用云盘创建裸金属实例的系统盘、数据盘，使用云内VPC网络。 |
| 弹性计算块存储 | 在线变更云盘类型 | 分布式存储支持在不中断业务的前提下，在线变更云盘类型（全闪/混闪）。 |
| 同时创建快照 | 支持为一台或者多台云服务器实例中的多块云盘同时创建快照，并且提供崩溃一致性快照能力。 |
| 快照存储 | 块存储的快照可被自动上传到对象存储中，不占用块存储空间；并且可从对象存储中直接调用快照文件实现回滚、创建新云盘等操作。如有请提供功能界面截图证明材料。 |
| 安全性 | 支持分布式EC和三副本数据冗余保护，三副本模式下，数据三副本支持分布在3个机柜或3对接入交换机上。 |
| 对象存储 | 对象上传 | 支持对象的简单上传、追加上传、下载、删除、列举、复制，获取对象的元数据、创建多段上传任务。 支持列举存储空间、创建存储空间、删除存储空间、列举存储空间内对象、获取存储空间的元数据。 |
| 接口要求 | 对象存储服务支持RESTful API接口、兼容Amazon S3接口，通过开发工具包SDK或直接通过RESTful API进行基础和高级对象存储操作，提供key-value键值对形式的对象存储服务 |
| 对象及租户要求 | 单个对象最大可支持48.8TB，单租户最大可支持10000个bucket并提供界面截图；每个bucket的生命周期最多可容纳1000规则。 |
| 生命周期管理 | 支持生命周期规则，定期自动将过期的对象删除。支持针对同一个桶内的不同对象，按照对象名称的前缀和对象标签来匹配生命周期规则。 |
| 专有网络服务 | VPC创建及隔离 | 支持用户创建自己的专有网络，同时支持自定义配置IP地址、子网、路由表 。支持不同VPC之间的安全隔离。 |
| 共享VPC | 支持共享VPC，支持按租户和资源集的VPC资源共享。VPC的所有者可以将VPC共享给同一组织的租户。 |
| 访问控制 | 支持用户可以创建网络ACL配置入向/出向规则，进行网络访问控制功能，从而实现对一个或多个子网流量的访问控制。 |
| 负载均衡服务 | 总体要求 | 负载均衡服务采用通用服务器架构实现。提供4层TCP/UDP和7层HTTP/HTTPS协议类型的服务。支持支持单实例监听带宽配置，对同一个负载均衡实例下挂的不同监听设置带宽限速，且已有的监听带宽上限支持在线修改。 |
| 配置实例规格 | 负载均衡支持配置多种实例规格，不同规格的实例限定了最大并发连接数、每秒最大新建连接数、每秒最大查询请求数。可以在线变更实例规格。如有请提供功能界面截图证明材料。 |
| 访问控制 | 负载均衡提供监听级别的访问控制，基于监听配置IP地址段白名单，只有在白名单中的IP地址才允许访问负载均衡。 |
| API网关服务 | 总体要求 | 覆盖API全生命周期管理，包括API设计、开发、测试、发布、运维监测、安全管控、下线等API各个生命周期阶段 |
| 功能要求 | 支持全链路签名验证，特别是后端签名，提供网关和后端服务之间的认证。 |
| 云管理平台 | 云产品资源管控 | 提供IaaS/PaaS/SaaS类云产品及服务的资源操作控制台支持添加/修改/删除多个同构云平台地址和账号，以及边缘节点的地址和账号，从而实现对相关云平台的纳管能力，并提供仪表盘展示云环境的资源概览信息，以及相关资源实例的列表信息 |
| 角色管理 | 提供角色创建、修改、删除、禁用功能，支持自定义业务角色，设置角色所具有的操作权限，并将角色管理给相关用户，支持复制/查询角色 |
| 组织和资源集管理 | 支持创建/修改/删除/级联删除/查询组织、变更资源组织归属。同级组织和资源集的资源要进行资源隔离，但是上级组织可以管理所有其下级组织和资源集的资源。 |
| 云运维管理系统 | 云主机运维 | （1）支持查看所有云主机列表，以及实例所在的物理机和集群详情。支持根据云主机实例ID、私网IP、公网IP查找云主机。  （2）支持启动、停止、重启、登录、迁移云主机。  （3）支持查询并查看云盘详情、卸载目标云主机上的云盘、查看操作审计、创建快照和查看快照。  （4）支持查看安全组列表，包括安全组所在Region、网络类型、专有网络ID、关联实例和创建时间。支持查看安全组的基本信息、安全组规则（包括入方向和出方向）以及安全组所关联的云服务器实例详情。  （5）支持以拓扑形式查看云服务器的关联资源，包括云服务器所在的服务器、集群、云盘、所属的VPC等关联信息 |
| 系统管理 | （1）支持云平台统一认证授权，运维管理员登录到云平台运维系统中，即可实现对云平台所有的组件进行运维或者免登录跳转运维。  （2）支持用户管理，支持新建、修改、删除用户，支持用户绑定登录策略，支持查看当前用户的个人信息。 支持用户组管理，可以将多个用户加入到一个用户组中，并为其添加相同的角色。支持角色管理，角色是一组访问权限的集合。支持预置基础角色。支持创建、修改、删除角色。 |
| 资源管理 | （1）支持展示云平台部署产品概览，包括部署云产品总数，正常及异常的产品数，支持图形化展示产品软件的部署状态。  （2）支持查看每个集群的详细信息，包括集群名称，所属产品，集群状态，包含机器等。支持按产品名称、集群名称查询产品/集群，支持按产品部署状态筛选正常/异常产品。 |
| 网络诊断 | 支持一键分析网络实例运行状态，提供可视化、自动化的网络诊断能力，包括DNS/负载均衡/弹性公网IP/边界路由器/物理专线/NAT网关实例，支持查看网络实例拓扑、支持显示诊断详情、诊断项描述、诊断结果。如有请提供功能界面截图证明材料。 |

##### 10.2.3专线网络服务技术要求

云平台和网络一体化的搭建和部署，应满足“云网融合”原则，实现与浦东教育城域网高速互联，并按照统一互联网出口的安全管理要求进行集中管理，整体设计规范、合理、有效，实现云与浦东教育城域网的融合和系统部署。

浦东教育云非信创平台与浦东教育城域网核心设备采用双链路互联（不在同一机房的需提供不同局向的双路由专线），单路带宽能力不少于40G，满足教育云业务系统的网络需要。信创私有云专线与非信创私有云网络出口设备相连，利用非信创私有云网络出口能力。

##### 10.2.4云安全服务技术要求

###### 10.2.4.1基本要求

浦东教育云平台应按网络安全等级保护基本要求第三级建设，满足《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）第三级安全测评通用要求和云计算安全扩展要求。结合国家信息安全等级保护相关要求和云计算安全扩展要求，构建由安全管理体系和安全技术体系两部分构成的浦东教育云安全保障体系。

中标人应建立健全配套的安全制度与规范，提供完整的安全服务方案，制定信息安全总体策略并发布安全管理制度，建立授权审批管理办法及信息安全事件应急预案。如：中标人可提供教育云管理办法、运维制度、应急预案等。

中标人提供的服务应具有较高的安全性，能为教育用户提供完善的安全策略方案，并且具有实施安全防护方案的技术能力，提供包括但不限于防火墙、IPS、态势感知、WEB应用防火墙、主机安全防护、堡垒机、综合日志审计、数据库审计等服务。每季度至少一次平台系统漏洞扫描，每年针对教育云信创云和非信创云资源池分别提交符合信息安全等级保护三级标准测试证明。

中标人为信创云资源池提供密码服务，建设云管平台的云密码服务平台，提供虚拟密码服务管理功能，每年通过密码应用安全性评估。针对信创云上的租户密码服务，本项目预投入建设基础密码资源池能力，可支持为上云用户提供安全认证网关服务、时间戳服务、签名验签服务、可信密码服务等，提供有竞争力的服务目录单价，由应用需求方另行结算。

###### 10.2.4.2平台安全要求

云平台要符合等保2.0三级的要求，需要从安全物理环境、安全通信网络、安区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理方面提供安全服务，从而满足平台网络安全、系统安全、数据安全等的安全需要。信创云资源池密码应用服务方面，云平台侧的密码应用架构主要通过密码应用基础设施、云平台侧数据安全服务和安全管理等部分，对云平台进行密码应用建设，满足云平台侧密码应用需求。

10.2.4.2.1非信创云安全能力要求

按信息安全等级保护第三级标准，提供包括且不限于以下安全服务(可以由同一台和多台设备实现)：

（1）安全物理环境

中标人用于建设教育云的机房需具备防盗窃和防破坏、防雷击、防火、防水和防潮、防静电、温湿度控制、电力供应等能力。

（2）安全区域边界

教育云平台区域边界及核心处网络边界处均应部署安全访问控制设备，通过部署防火墙，实现所划分安全域间的隔离和访问控制，建立租户VPC边界，提供独立日志审计。

（3）安全通信网络

提供IPS入侵防御能力，提供对恶意代码防护的能力，提供独立日志审计。

（4）安全计算环境

Web应用防护：针对教育云平台及云租户应用，提供双重waf防护能力，教育云应用需要通过硬件waf进行防护，对重要应用通过软waf进行双重防护，提升网站安全性，实现基于HTTP/HTTPS/FTP协议的蠕虫攻击、木马后门、间谍软件、灰色软件、网络钓鱼等基本攻击行为、CGI扫描、漏洞扫描等扫描攻击行为、SQL注入攻击、XSS攻击等Web攻击的应用防护。

（5）安全管理中心

数据库审计能力：针对教育云平台提供数据库审计能力，对访问数据库服务器的行为实现全方位审计，保护数据库的安全。

安全态势感知能力：针对教育云平台安全态势进行展现，通过采集云平台安全事件数据，对海量日志等信息进行深度分析，同时关联网络攻击事件，多维度、可视化地呈现全网的安全风险状况，结合云端的威胁情报，生成全方位的安全全景视图，使用户能够快速准确地掌握网络当前的安全态。

堡垒机运维审计能力：提供云平台及租户堡垒机运维审计功能，保护教育云内部网络不被未经授权访问，验证用户身份，并根据权限授予用户对内部网络的访问权限，记录所有用户的访问活动，包括登录、命令运行和文件操作等以便进行安全审计和追踪。

综合日志审计能力：提供云平台综合日志审计能力，云平台所有设备日志需要通过综合日志审计统一收集分析，并满足网络安全法，日志留存满足6个月的要求；将所有设备日志收集过来，并集中审计，及时发现各种安全威胁、异常行为事件，为管理人员提供全局的视角，确保客户业务的不间断运营安全；实现信息资产的统一管理、监控资产的运行状况，协助管理员全面审计信息系统整体安全状况。

系统漏洞扫描：每季度提供云平台漏洞扫描服务，扫描范围包括，服务器、网络设备安全设备等，并针对检测出的高危漏洞进行加固。

关键指标要求如下：

| **服务名称** | **指标要求** |
| --- | --- |
| 防火墙 | 实现所划分安全域间的隔离和访问控制，建立租户VPC边界，提供独立日志审计（单台出口边界防火墙吞吐量不低于40Gbps；单台核心防火墙吞吐量不低于80Gbps） |
| IPS | 提供对恶意代码防护的能力，提供独立日志审计（单台每秒新建链接数不低于15万，最大并发链接数不低于800万） |
| WEB应用防火墙（WAF） | 实现基于HTTP/HTTPS/FTP协议的蠕虫攻击、木马后门、间谍软件、灰色软件、网络钓鱼等基本攻击行为、CGI扫描、漏洞扫描等扫描攻击行为、SQL注入攻击、XSS攻击等Web攻击的应用防护。licenses不限制数量。 |
| 数据库审计 | 对访问数据库服务器的行为实现全方位审计，存储空间不小于1T（提供实例数不少于8个） |
| 安全态势感知 | 支持展示出口互联网流量情况，包括上下行流量速率统计、应用流量分布、应用流量排行、应用流量趋势、用户流量分布、区域流量排行等；支持展示内部网络流量情况，包括被访问资产分布、应用流量分布、资产访问用户趋势、访问流量用户分布、访问目的区域排行等；支持按照已失陷、高危、低危、影响内网、影响外网统计风险用户的数量，并且能够列表展示风险用户的明细，支持展示对应安全事件的建议处置方式，提供具体排查工具，具体升级补丁，防护策略等建议内容；支持自定义处置建议编辑，后续出现同样安全事件时，可自动显示编辑后的处置建议，支持通过时间段、统计源、统计对象、用户名、用户组进行访问互联网访问行为进行统计； |
| 堡垒机 | 监控和记录操作人员对云平台各类设备的操作行为，拦截非法访问和恶意攻击，对不合法命令进行命令阻断，过滤掉所有对目标设备的非法访问行为，并对内部人员误操作和非法操作进行审计监控，以便事后责任追踪。支持至少1200资产的管理。 |
| 综合日志审计 | 可实时展示关联事件数量趋势、平台自身性能实时监控图（CPU、内存、磁盘）；支持按照日志类型进行查询，支持操作日志、审计日志、流量日志、威胁日志、主机日志等11大类70子标签进行分类；支持多条件查询，包含开始时间、结束时间、动作类型、设备名称、日志等级、用户名、源IP、目的IP、协议等条件进行过滤查询展示；支持多类型、多厂商安全设备、网络设备、操作系统、应用日志适配分析；支持用户自定义统计效果，可选择饼状分布图、折线趋势图、柱状比较图；支持全文检索原始日志，检索字段变色高亮；支持任意信息、任意时间进行内容查询匹配，支持可选包含/不包含匹配方式。平台具备的日志来源采集数量为无限制，采集范围包括但不限于网络安全设备、网络设备、云平台等。日志存储≥7.2T，满足日志保存6个月要求。 |
| 系统漏洞扫描 | 每季度进行一次对业务系统进行漏洞扫描，并提供安全加固建议 |
| 等保测评服务 | 云平台每年通过安全等保三级测评。 |

10.2.4.2.2信创云安全服务

| **指标名称** | | **指标要求** |
| --- | --- | --- |
| 基础安全服务 | 功能要求 | 云安全基础防护，提供全局用户及平台集中管理能力和专有云日志分析功能 |
| 流量安全监控 | 网络访问行为进行封禁 | 支持对可疑的网络访问行为进行一键封禁，禁止可疑IP地址出和入方向的网络访问。 |
| 威胁检测 | 威胁日志支持一键封禁IP、一键加白等操作，实现对告警的快速处理。 |
| 安全防护策略 | 支持四层防护策略，根据基于源IP、目的IP及端口设置流量观察与阻断策略； |
| 端口扫描欺骗策略 | 支持端口扫描欺骗策略，可添加需要防护的IP和端口，对恶意端口扫描行为进行欺骗。如有请提供端口扫描欺骗策略编辑页面截图证明。 |
| 态势感知 | 态势监控 | 态势监控通过安全态势监控视角，集中呈现云租户的云环境安全风险情况，包含风险指数、指数趋势、资产保护率、风险资产分布、TOP5安全漏洞风险、TOP5安全基线风险、TOP5风险资产、风险威胁趋势、网络攻击分布、TOP5网络攻击、异常行为分布、TOP5异常行为等监控指标，支持切换成高分辨的大屏界面，应用于云环境网络安全的实时监控，同时支持一键导出安全态势快照； |
| 云产品检查 | 云产品检查-云租户产品服务的安全配置检查，包括数据安全、访问控制、安全防护、身份认证、容灾备份、日志审计、监控告警等基线类型，支持面向云主机，云数据库，对象存储，负载均衡等云产品服务进行安全检测检查，应用于云产品的安全合规性扫描检查及管理； |
| 资产网络链路透视 | 支持资产网络链路透视，以图形化的方式呈现云主机资产的网络连接和公网透出路径，支撑网络问题排查、暴露面风险收敛、威胁溯源等。 |
| Web应用防火墙 | 攻击防护策略 | 支持http、https协议流量识别；具备http协议深层解码能力，解码深度不低于10层，解码方式包括：URL解码、JSON解码、Base64解码、Base64（RFC 2045）解码、16进制转换、二进制解码、斜杠反转义、XML解析、PHP反序列化解析、UTF-7解码； |
| 站点配置 | 支持以站点为配置粒度的BOT防护功能：  （1）支持至少2种验证方式，并可以将常见搜索引擎一键置白，例如：百度、谷歌、必应、360、今日头条、Yandex等搜索引擎设置  （2）支持动态混淆防护：对需要保护的网页内容进行混淆变形，对业务逻辑以及存在的漏洞点起到隐藏保护作用  （3）支持动态令牌验证：对请求增加令牌信息，提高自动化工具进行重放重放攻击或请求伪造方式对防护服务器进行保护  （4）支持页面防调试：阻止用户通过浏览器进行调试的方式发现页面的攻击点" |
| 防护能力 | 提供动态混淆防护，如动态令牌验证、请求混淆、页面混淆，有效防护各种自动化渗透测试攻击。如有请提供功能界面截图证明材料。 |
| 云安全管理中心 | 全局安全态势 | 集中呈现云平台和所有云租户的全局安全态势、资产风险态势、风险威胁态势，应用于云环境网络安全的实时监控，支持全局安全态势、资产风险态势、风险威胁态势三种态势监控视角，并支持高分辨率的大屏呈现，同时支持一键导出安全态势快照；  全局安全态势包含组织总数、风险指数、指数趋势、TOP5风险组织、资产总数、资产保护率、风险资产分布、威胁事件统计及分布、外部攻击源地理位置分布等监控指标； |
| 安全分析 | 基于预定义或自定义安全分析规则，针对标准化日志进行关联分析，生成IOC威胁事件，还原完整攻击路径，提炼关键性证据信息，定位攻击源；支持云环境全局威胁事件集中呈现，包括威胁名称、威胁类型、ATT & CK ID、威胁描述、处置建议、网络协议、源/目的IP及端口、匹配已知威胁情报、域名、文件名、进程信息等关键信息； |
| 安全分析 | 基于主机异常行为、网络攻击、威胁事件，自动化智能威胁溯源，以图形化的方式还原攻击路径，定位攻击源及攻击目标；支持三种大风险类型的溯源分析，包括业务风险威胁（包含DDoS攻击、蠕虫病毒等）、计算资源非法利用（包含挖矿、计算资源异常、扫描探测、远控木马、隐匿隧道等）、数据安全风险（包含弱口令、暴力破解、勒索软件等）；支持图形化的威胁溯源分析结果呈现，还原攻击链进程路径，图形化溯源结果支持自定义布局及导出 |
| 敏感数据保护 | 总体要求 | 提供不低于100台物理主机上的数据资产提供安全能力。 |
| 数据资产 | 支持一键发现并接入云上数据资产，支持范围：对象存储、云数据库、表格存储、大数据计算服务。支持免输入密码一键授权数据识别、数据脱敏、数据审计权限。如有请提供功能界面截图证明材料。 |
| 资产地图 | 资产地图：支持统计敏感数据、异常事件等数据安全态势数据，动态展示数据异常情况。 |
| 识别规则 | 支持基于内置及用户自定义的识别规则，实现针对敏感数据的识别能力。提供对结构化数据、半结构化数据、非结构化数据进行敏感数据的自动识别能力，通过样本扫描、特征萃取、特征对比和文件聚类等算法，实现116种敏感数据的精准识别。支持解析169种文件类型（包括文本、办公类文档、压缩嵌套文件），支持OCR技术识别图片敏感数据。 |
| 数据库审计 | 总体要求 | 提供不低于20个数据库实例 |
| 监控 | 支持丰富的探针参数，包括抓包网卡配置、服务器和探针的CPU占用率、内存占用率等灵活配置。管理平台对探针的管理能力丰富，支持插件的配置、挂起、唤醒、停止、卸载、状态监控和日志查看；支持下载探针安装包。数据库：Oracle、MySQL、SQL Server、达梦、南大通用、人大金仓、神通等数据库的审计。 |
| 审计能力 | 支持配置返回行数和内容大小控制返回结果集大小，降低系统开销。应具备漏洞攻击规则库，漏洞攻击规则应至少包括：漏洞名称、CVE标识、CNNVD、漏洞类型、影响范围等内容。支持在全局启用结果集审计，也支持按照规则进行结果集审计，可以针对特定访问行为，审计结果集。可以针对每条规则配置不同告警次数限制，灵活控制告警频率。如有请提供功能界面截图证明材料。 |
| 审计规则 | 支持IP地址、数据库用户、时间、对象、应用用户、操作系统用户、客户端工具、数据库实例分组，并且分组对象可以直接在规则中引用。 |
| 堡垒机 | 总体要求 | 提供不低于1000个租户侧授权，提供不低于平台侧500台服务器物理机授权。 |
| 用户安全策略 | 支持用户安全策略功能，如密码锁定次数、密码有效期、密码复杂度、用户有效期、用户登录客户端限制等。 |
| 多级架构管理 | 支持用户/用户组的多级架构管理，可以复制、剪切、粘贴、移除用户/用户组，实现用户/用户组架构的灵活调整。支持用户的移交功能，可以将用户的群组属性和权限交接给其它用户。 |
| 多级架构管理 | 支持主机/主机组的多级架构管理，可以复制、剪切、粘贴、移除主机/主机组，实现主机/主机组架构的灵活调整。 |
| 漏洞扫描 | 总体要求 | 提供针对云上弹性计算服务物理机漏扫防护能力。 |
| 风险检测配置 | 基于无状态扫描技术，结合动态检测和静态匹配两种扫描模式，提供自动化、高性能的精准Web漏洞扫描、弱口令扫描能力。 |
| 主机资产识别 | 支持主机资产的内外网识别，同时获取资产存活/更新状态、关联域名、操作系统、端口、服务、中间件、地理位置、漏洞信息、WAF、CDN、指纹、来源、扫描时间等信息。 |
| 主机安全防护 | 总体要求 | 提供针对云上弹性计算服务物理机主机安全防护能力。 |
| 重点关注资产 | 支持展示重点关注的资产，漏洞，异常，配置缺陷，事件等信息 |
| 端口及漏洞检查 | 支持主机维度进行资产暴露盘点，可提供资产、暴露方式、暴露组件、暴露端口、可被利用的漏洞、暴露链路拓扑图及暴露风险详情等信息；  基线检查：支持对主机进行安全基线检查；检查对象包括Linux、Windows、Redis和Tomcat等；对检查不通过项目，可显示详情并提供修复建议，还支持安全配置基线一键修复，支持在控制台上手工设置加固后的基线配置详情已进行一键修复；基线检测标准应支持等保模板、CIS模板；  漏洞管理：至少应覆盖Windows操作系统漏洞、Linux操作系统漏洞、应用组件漏洞等，并支持漏洞一键修复，并提供漏洞修复参考标签，如远程利用、命令执行等，便于行方参照标签进行漏洞修复优先级排序 |
| 告警类型 | 支持的告警类型：进程异常行为、异常登录、异常事件、敏感文件篡改、异常网络连接、异常账号、应用入侵事件、持久化后门、应用威胁检测、网站后门、恶意进程（云查杀）、 恶意脚本 |
| 加密服务管控服务（平台侧） | 功能要求 | 提供网络配置、导出镜像、升级、重启等功能。 |
| 云密码机实例操作 | 提供底座云密码机实例的开通、配置、释放、删除等功能。 |
| 信创密码机 | 提供通过国密检测认证的云密码机，支持信创密码机。 |
| 数据影响 | 管理VSM管理的数据影像，可以用于恢复操作。 |
| 配套加密机性能 | 总体要求 ：  1、基于KVM虚拟化技术，提供虚拟密码机功能；支持虚拟金融数据密码机、服务器密码机、签名验签服务器等多种形态的密码设备；  2、产品符合国家密码管理局相关管理要求，符合GM/T 0028安全等级第二级要求；（如有请提供证书证明）  3、产品具有国家强制性产品认证证书；  硬件要求 ：  1、至少提供4个网络端口,网络接口需要提供bond高可用模式，2个千兆电口，2个万兆光口，网络端口可支持10g、25g光口。  2、为了防止数据窃听，设备不得存在USB接口；  3、支持设备状态灯显示运行状态，包括不限于电源状态灯、运行状态灯、告警灯等；  4、支持应急状态下，物理密钥销毁按钮对密钥进行销毁；  5、设备内存≥128G、存储≥1T、信创密码卡等部件。  6、电源：双模块冗余电源，交流直流自适应；  密码算法 ：  1、集成国密认证的二级信创密码卡实现各类密码算法，保证算法的高安全性；  2、对称算法：支持国产SM1/SM4算法、以用国际通用算法DES、TDES、AES；  3、摘要算法：支持国产SM3和通用SHA1/SHA256/SHA384/SHA512等算法；  4、非对称算法：支持SM2、RSA、ECC等算法；  宿主机功能 ：  1、宿主机可对接云管控平台，对宿主机和虚拟密码机进行统一的资源管理、状态监控；  2、宿主机根据指令要求动态创建、加载、停止、销毁、启动、恢复虚拟密码机。  虚拟密码机功能：  1、权限管理：虚拟密码机管理使用USBkey认证；初始管理员可增加多个管理员；同一套Ukey可管理多个虚拟密码机；  2、设备管理员身份认证：设备管理员采用SM2算法实现身份认证、建立安全通道；  3、支持虚拟密码机数量 ≥8个；"  性能要求，整机：  1、SM2产生 ≥20000次/秒  2、SM2签名 ≥20000次/秒  3、SM2验签 ≥15000次/秒  4、RSA2048 产生 ≥20次/秒  5、RSA2048 签名 ≥5000次/秒  6、RSA2048验签 ≥15000次/秒  7、SM3摘要(tps) ≥45000次/秒  8、SM4 加解密(tps)≥45000次/秒" |
| 云平台应用身份认证服务 | 安全设备统一认证 | 支持对接RADIUS实现对防火墙、堡垒机等设备的统一认证 |
| 配置策略 | 支持配置密码策略、短信、邮件网关；支持配置OTP认证；对接UEBA、实人认证等 |
| 数据同步 | 支持组织机构、账户的创建以及AD、LDAP、SCIM接口等方式同步数据 |
| 账户管理 | 针对账户的管理功能，不限于启用/禁用、重置密码、启用/禁用二次认证等功能 |
| 日志查询 | 支持根据账户、应用、日志类型进行日志查询，并提供日志导出、设计报表功能 |
| 日志 | 提供账户级别的登录、退出日志 |
| SSL VPN | 总体要求 | 1、产品具符合国家密码管理局相关管理要求，符合GM/T 0028安全等级第二级要求；（如有请提供证书证明）  2、产品符合GM/T 0024、GM/T 0025规范要求，支持国密标准SSLv1.1协议；（如有请提供证书证明）  3、支持国际算法SSL v3/TLS 1.0/1.1/1.2/1.3认证模式；  4、采用厂商自有知识产权的信创密码卡； |
| 硬件要求 | 1、至少提供4个网络端口，2个千兆电口，2个万兆光口；  2、设备不得存在USB接口；  3、设备内存≥32G、存储≥1T。  4、支持设备状态灯显示运行状态，包括不限于电源状态灯、运行状态灯、告警灯等；  5、支持应急状态下，物理密钥销毁按钮对密钥进行销毁； |
| 密码算法 | 1、集成国密认证的二级信创密码卡实现各类密码算法，保证算法的高安全性；  2、对称算法：支持国产SM1/SM4算法、以用国际通用算法DES、TDES、AES；  3、摘要算法：支持国产SM3和通用SHA1/SHA256/SHA384/SHA512等算法；  4、非对称算法：支持SM2、RSA、ECC等算法； |
| SSL网关功能 | 1、符合GM/T0024 规范要求  2、支持国密SSL卸载  3、支持国际算法SSLv3/TLS 1.0/1.1/1.2/1.3认证模式  4、支持国密双证双向HTTPS应用交付功能  5、支持一个地址端口上RSA与SM2同时自适应  6、支持正向SSL加载安全代理模式，将HTTP协议转换为HTTPS协议  7、支持SSL协议转换（如将RSA算法SSL转换为SM2国密SSL）  8、支持内部产生密钥、生成CSR证书请求、支持GSMA组织指定多根多曲线协议  9、支持国密X509数字双证书、支持国际标准的X509数字证书 |
| SSL VPN功能 | 1、符合GM/T0024 规范要求  2、支持国际算法SSLv3/TLS 1.0/1.1/1.2/1.3认证模式  3、支持IP协议与TCP/UDP/ICMP协议的加密传输  4、SSL VPN隧道支持使用UDP传输协议进行加速  5、支持国密X509数字双证书、支持国际标准的X509数字证书  6、支持导入密钥、证书和PKCS12格式文件 |
| 性能要求 | 1、RSA2048并发用户数≥10000；  2、RSA2048新建连接数≥3000；  3、RSA2048吞吐量≥300Mbps；  4、SM2并发用户数≥10000；  5、SM2新建连接数≥3000；  6、SM2吞吐量≥300Mbps； |
| 其他要求 | 配套SSL VPN需提供国密浏览器10套、国密个人数字证书及智能密码钥匙。 |

###### 10.2.4.3.租户级国密技术要求

在信创云资源池上，预投入建设租户级基础密码资源池能力，可支持为上云用户提供安全认证网关服务、时间戳服务、签名验签服务、可信密码服务等租户密码应用服务，提供有竞争力的服务目录单价，由应用需求方另行结算。中标服务方可提供满足租户应用通过密评的密码环境要求。

10.2.4.3.1.国密硬件要求

|  |  |
| --- | --- |
| **用途：云密码机** | |
| **要求** | **具体要求** |
| 总体要求 | 符合国家密码管理局相关管理要求，符合GM/T 0028安全等级第二级要求；（如有请提供证书证明） |
| 密码算法和协议要求 | 支持签名和验签名、基于密钥的完整性保护、数据加解密及安全密钥存储等功能，且所有密码运算都基于国家商用密码算法； |
| 技术参数 | 支持SM2非对称密钥生成、获取公钥，256位SM2密钥对生成≥26000次/秒； |
| 支持SM2非对称密钥私钥签名、验签功能，256位SM2签名≥26000次/秒，256位SM2验签≥24000次/秒； |
| 支持SM2非对称密钥公钥加密、解密，256位SM2加密≥16000次/秒，256位SM2解密 ≥30000次/秒； |
| 支持SM4对称密钥生成，且支持ECB和CBC模式加解密，SM4计算效率≥3000Mbps； |
| 支持SM3算法数据摘要运算，支持MAC和HMAC，SM3计算效率≥3000Mbps |
| 支持海量密钥存储，存储量大于100万条 |
| 功能要求 | 支持基于虚拟化技术的自动化部署，虚拟的密码机以文件镜象加密存储；云平台管理端可调用云密码管理服务平台的接口实现远程创建虚拟加密机镜象，远程调用不同的虚拟密码机镜象，实现虚拟密码机的自动化部署、启用、卸载、销毁等； |
| 安全存储服务器密码机核心程序：服务器密码机使用带有逻辑加密功能的芯片对核心程序进行存储，防止非法读出； |
| 管理要求 | 管理软件能够针对云密码机和虚拟密码机进行运行状态监控，包括服务正常运行情况、业务连接数、CPU、内存占用率、磁盘使用率等业务状态,支持三权分立角色管理和国密强身份认证； |
| 支持对云密码机日志信息和访问控制信息进行基于商用密码算法的完整性保护； |

10.2.4.4.2.国密软件要求

|  |  |
| --- | --- |
| **用途：签名验签服务系统** | |
| **要求** | **具体要求** |
| 部署要求 | 签名验签服务能够部署在云端虚拟机中，并且能与CA、云密码机进行联动，与CA配合完成证书的验证，与云密码机配合完成签名和验签功能； |
| 功能要求 | 支持配置信任多个CA根证书，可验证不同CA机构签发的符合SM2证书标准的签名结果。 |
| 支持制作数字签名，支持对数据原文制作数字签名，签名结构符合SM2证书国家标准。 |
| 支持配置记录日志的类型，如业务日志、管理员日志、Debug日志、错误日志，并可根据需求开启或关闭，支持错误和故障日志完整保留，并可进行下载。 |
| 监管要求 | 支持签名验签服务运行状态监控，包括服务正常运行情况、业务连接数、CPU、内存占用率、磁盘使用率等业务状态，提供信息提取接口便于第三方网络管理软件进行信息提取； |
| 支持故障定位功能，错误签名或验签信息必须有详细的日志，譬如验签的原文、验签的时间等。 |
| 密评要求 | 签名验签服务应用程序与服务申请应用、云密码机之间的数据传输应采用基于商用密码算法的机密性和完整性保护； |
| 签名验签服务的访问控制信息、日志信息能够自主进行基于商用密码算法的完整性保护。 |

|  |  |
| --- | --- |
| **用途：时间戳服务系统** | |
| **要求** | **具体要求** |
| 部署要求 | 时间戳服务能够部署在云端虚拟机中，并且能与CA/RA系统、签名和验证签系统、云密码机进行联动，与签名和验签系统、CA/RA系统配合完成证书的验证与签名功能； |
| 功能要求 | 能够与第三方授时中心、卫星授权时间源进行时间同步，确保所签发时间戳时所获取的时间的有效性； |
| 监管要求 | 支持签名验签服务运行状态监控，包括服务正常运行情况、业务连接数、CPU、内存占用率、磁盘使用率等业务状态，提供信息提取接口便于第三方网络管理软件进行信息提取； |
| 安全要求 | 时间戳服务可采用分级权限管理，支持初始化管理员和操作员，负责管理员、操作员权限的判断。 |
| 可靠性要求 | 部署后可保证在当一台物理机器出现问题时，时间戳服务能够漂移至其他物理机，不影响业务系统的正常运行。 |
| 密评要求 | 承载时间戳服务的虚拟机，其运维管理支持集中的安全管理通道，身份认证基于商密证书的强身份认证或支持基于商用密码算法的信任链； |
| 时间戳服务的访问控制信息、日志信息能够进行基于商用密码算法的完整性保护。 |
| 时间戳服务应用程序与服务申请应用、云密码机之间的数据传输应采用基于商用密码算法的机密性和完整性保护； |

|  |  |
| --- | --- |
| **用途：安全认证网关服务系统** | |
| **要求** | **具体要求** |
| 总体要求 | 符合国家密码管理局相关管理要求，符合GM/T 0028安全等级第二级要求；（如有请提供证书证明） |
| 部署要求 | 安全认证网关服务能够部署在云端虚拟机中，并且能与CA、云密码机进行联动，与CA配合完成证书的验证，通过云密码机提供的密钥运算生成非对称证书请求； |
| 功能要求 | 支持多证书链功能，可同时支持多个证书颁发机构颁发的证书功能 |
| 支持身份认证、密钥交换和加密传输 |
| 提供双向身份验证功能，支持动态黑名单 |
| 支持MIME数据类型过滤技术的 SSL代理 |
| 支持应用的 Web 静态数据缓存 |
| 监管要求 | 支持服务运行状态监控，包括服务正常运行情况、业务连接数、CPU、内存占用率、磁盘使用率等业务状态； |
| 支持故障定位功能，客户端访问失败必须有详细的日志，譬如报错信息、时间等。 |
| 密评要求 | 安全认证网关服务应用程序与服务申请应用、云密码机之间的数据传输应采用基于商用密码算法的机密性和完整性保护； |
| 安全认证网关服务的访问控制信息、日志信息能够自主进行基于商用密码算法的完整性保护。 |

|  |  |
| --- | --- |
| **用途：数据库加密服务系统** | |
| **要求** | **具体要求** |
| 总体要求 | 符合国家密码管理局相关管理要求，符合GM/T 0028安全等级第二级要求；（如有请提供证书证明） |
| 兼容OceanBase数据库、达梦数据库、瀚高数据库、人大金仓数据库、神通数据库、南大通用数据库等数据库厂商产品 |
| 兼容鲲鹏、海光、飞腾、龙芯等芯片等产品 |
| 部署要求 | 数据库加密服务能够部署在云端虚拟机中，与云密码机进行联动，通过云密码机提供的密钥管理和运算能力，通过客户端应用免改造对应用数据实现加解密 |
| 性能参数 | SM4 加/解密速率为 200Mbps/200Mbps |
| 支持的数据库实例个数≥10 个 |
| 支持的加密字段≥100 个 |
| 功能要求 | 系统可以对数据字段项设置加密规则，提供数据库列级加密，并支持对不同字段列设置不同的密钥和加密算法 |
| 支持应用系统免改造加密，支持字段级别的数据内容加密，支持图形化自定义能力，提供历史数据管理；提供灵活的加密状态和非加密状态的双向转换 |
| 支持模糊查询 |
| 数据库中的敏感数据以密文方式存储，通过数据库客户端工具查看时，敏感数据以密文方式显示，防止敏感数据泄露 |
| 加密字段中写入明文数据时，系统能够识别并能对明文数据进行加密 |
| 监管要求 | 支持服务运行状态监控，包括服务正常运行情况、业务连接数、CPU、内存占用率、磁盘使用率等业务状态； |
| 支持故障定位功能，客户端访问失败必须有详细的日志，譬如报错信息、时间等。 |
| 密评要求 | 数据库加密服务应用程序与服务申请应用、云密码机之间的数据传输应采用基于商用密码算法的机密性和完整性保护； |
| 数据库加密服务的访问控制信息、日志信息能够自主进行基于商用密码算法的完整性保护。 |

|  |  |
| --- | --- |
| **用途：文件加密存储服务系统** | |
| **要求** | **具体要求** |
| 总体要求 | 符合国家密码管理局相关管理要求，符合GM/T 0028安全等级第二级要求；（如有请提供证书证明） |
| 部署要求 | 文件加密服务能够部署在云端虚拟机中，与云密码机进行联动，通过云密码机提供的密钥管理和运算能力，提供应用免改造实现文件加密存储。 |
| 性能参数 | SM4加密128KB数据运算平均速率≥1500Mbps，SM4解密128KB数据运算平均速率≥1500Mbps |
| 在千兆网络环境下，512kB大小文件的平均读访问带宽超过50MB/s，写访问带宽超过90MB/s |
| 可将传统文件系统中512KB海量小文件＜5MB/s的访问迁移速度，提升至＞50MB/s(千兆网)乃至＞200MB/s（万兆网）。支持系统内部和系统间的高速迁移 |
| 功能要求 | 支持数据文件混合管理：文件聚合存储，实现10亿个文件以上海量大小数据文件的统一管理 |
| 支持任意目录结构，任意目录层级；支持更深的目录深度（目录深度可以超过20级以上），更长的目录名（目录名可以超过40字节），单目录下更多的文件数（单目录下可以存储超过1亿文件和1亿目录） |
| 支持强访问控制(应用白名单)，只有用户授权的应用才可访问用户数据 |
| 支持慢磁盘监测，并根据运行状态提供告警机制 |
| 支持HDFS协议，提供JAVA接口以及Rest Ful接口，支持透明访问 |
| 监管要求 | 支持服务运行状态监控，包括服务正常运行情况、业务连接数、CPU、内存占用率、磁盘使用率等业务状态； |
| 支持故障定位功能，存储过程必须有详细的日志，譬如报错信息、时间等。 |
| 密评要求 | 文件加密存储服务应用程序与服务申请应用、云密码机之间的数据传输应采用基于商用密码算法的机密性和完整性保护； |
| 文件加密存储服务的访问控制信息、日志信息能够自主进行基于商用密码算法的完整性保护。 |

|  |  |
| --- | --- |
| **用途：密码服务管理平台系统** | |
| **要求** | **具体要求** |
| 总体要求 | 符合国家密码管理局相关管理要求，符合GM/T 0028安全等级第二级要求；（如有请提供证书证明） |
| 部署要求 | 支持云环境部署，可集中部署和分布式部署； |
| 功能要求 | 支持虚拟密码机、签名验签服务、时间戳服务、电子签章服务的动态添加删除功能； |
| 支持加解密服务、认证服务和完整性保护等密码运算，并支持这些运算的统计功能，且能根据管理需求添加并显示相应统计功能； |
| 提供虚拟密码设备、密码资源配置、密码资源分组等进行统一管理。支持设备注册、注销、隔离、恢复。设备信息包含IP、端口、部署数据中心、厂商、设备型号、设备序列号、所属系统等 |
| 为业务系统提供底层的密码运算服务支撑，包括密钥访问处理、密码运算等。 |
| 提供密码设备监控功能，包括设备状态、CPU利用率、内存使用情况、磁盘空间、设备服务链接数等。 |
| 密钥管理要求 | 为业务系统及模块提供以密钥生命周期为主线的密钥管理功能，包含密钥的生成、存储、分发、备份、更新、撤销、归档和恢复等信息进行采集、存储、查询及分析等； |
| 持密钥同步服务功能，多个密钥管理系统之间具有密钥同步功能 |
| 所有密钥需按照国家采购人认可的密钥生成方法产生，不使用软件、人工等伪随机数方法产生；密钥生成装置需为硬件设备；能生成高质量随机数、对称密钥和非对称密钥；必须以加密方式导出密钥生成装置的密钥； |
| 支持密钥同步服务功能，多个密钥管理系统之间具有密钥同步功能 |
| 监管要求 | 支持云密码机集群管理，支持虚拟密码机、签名验签服务、时间戳服务、电子签章服务资源池管理和监控； |
| 可靠性要求 | 支持将密码服务协议转换处理完成后得到的服务请求分发到负载均衡模块，支持加密设备之间的业务负载功能，业务请求采用轮转调度算法实现负载均衡。 |
| 密评要求 | 承载密码管理服务平台的虚拟机，其运维管理支持集中的安全管理通道，其身份认证基于商密证书的强身份认证或支持基于商用密码算法的信任链； |
| 密码管理服务平台的访问控制信息、日志信息能够进行基于商用密码算法的完整性保护。 |
| 密码管理服务平台应用程序与服务申请应用、云密码机之间的数据传输应采用商用密码算法进行机密性和完整性保护； |

|  |  |  |
| --- | --- | --- |
| **用途：密码评估系统** | | |
| **规格** | **指标要求** | |
| 根据密评要求和相关解答定义出对应的密码风险符合度报告，用户可自行进行密评符合度评估 | 总体要求评估功能 | 总体要求评估模块：对密码算法，密码技术，密码产品，密码服务进行安全符合度评估 |
| 密码功能要求评估 | 密码功能评估模块：能够对密码功能的机密性，完整性，真实性，不可否认性进行符合度评估 |
| 安全管理评估功能 | 1.制度评测模块：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准制定制度管理符合度评测功能 |
| 2.人员评测模块：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准制定人员管理评测功能 |
| 3.实施评测：根据信息系统密码应用基本要求规定，实现实施管理评测功能模块，涵盖规划，建设，运营三部分 |
| 4.应急评测：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准制定应急管理符合度评测功能 |
| 安全技术评测功能 | 1.物理和环境安全评估模块：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准进行物理和环境安全评估 |
| 2.网络和通信评估模块：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准进行网络和通信安全评估 |
| 3.设备和计算安全评估模块：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准进行设备和计算安全评估 |
| 4.应用和数据安全评估模块：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准进行应用和数据安全评估 |
| 5.密钥管理评估模块：根据信息系统密码应用基本要求规定，对等级保护二级和三级的标准进行密钥管理安全评估 |
| 分析功能 | 1.综合评分功能：能够对各个模块的评测结果进行打分和分析 |
| 2.建议功能：根据评测结果自动出具建议报告 |
| 3.能力矩阵图：根据系统各个模块收集到的信息制作能力矩阵分析图，能够清晰分析出系统的薄弱点和优势点 |

##### 10.2.5云基础应用支持服务要求

（1）国产化操作系统license服务

分批提供国产化主流服务器版操作系统license服务，满足新增业务系统及存量国产化改造的需求，为各类应用的国产化操作系统改造提供能力支持。

操作系统版本不低于银河麒麟高级服务器操作系统V10/中标麒麟高级服务器操作系统V7、统信服务器操作系统V20。按采购人需求提供。

三年分批数量预估如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务内容 | 单位 | 第一年 | 第二年 | 第三年 |
| 国产化操作系统license服务 | 套/年 | 300 | 620 | 1080 |

（2）国产化数据库license服务

分批提供国产数据库license服务，支持单机器单实例部署，也支持同一数据库构建多个实例的模式，以满足不同用户的需求。

数据库版本不低于：达梦数据库管理系统[简称：DM]V8.1、人大金仓数据库KingbaseES V8。按采购人需求提供。

三年分批数量预估如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务内容 | 单位 | 第一年度 | 第二年度 | 第三年度 |
| 国产化数据库license服务 | 套/年 | 15 | 30 | 35 |

（3）云盘服务

浦东教育定制云盘服务主要为区级及校级用户提供云盘服务，帮助用户解决访问、共享、存储、管理数据的难题，可实现突发访问、下载需求，满足特殊时期的大量用户访问诉求。原浦东教育云盘与浦东教育统一认证平台对接，采用网页方式浏览和操作。本期教育盘三年目标为服务全区老师，为区级应用和校级试点学校提供云盘服务。云盘需要提供客户端服务，并考虑业务增长及试点校增加，逐年增加容量规划，三年依次为24T、30T、36T。

|  |  |  |
| --- | --- | --- |
| 指标 | 指标项 | 指标要求 |
| 文件管理 | 文件上传 | 支持50G以内的单文件稳定秒传 |
| 上传下载不限速 |
| 支持自动备份 |
| 支持断点续传 |
| 预览 | 支持常见office、图片、音频、视频在线预览 |
| 搜索 | 支持全盘、全文搜索 |
| 恢复 | 支持回收站 |
| 邮件 | 支持绑定任意邮箱，在云盘中发送文件 |
| 版本管理 | 支持历史版本管理 |
| 后台管理 | 账号 | 支持云盘账号按需管理 |
| 空间 | 支持云盘内存储空间分域管理 |
| 支持云盘内存储空间按需分配 |
| 配置权限 | 支持根据业务需求配置文件操作权限规则 |
| 协同办公 | 共享文件 | 支持文件和共享文件管理 |
| 外链分享 | 支持文件外链分享，按需设置分享权限 |
| 微信文件可直接保存至云盘 |
| 权限管理 | 支持多级权限管理 |
| 在线预览 | 无需下载，云端在线编辑文件 |
| 在线编辑 | 多人实时在线编辑 |
| 服务可用性 | 服务可用性 | 服务可用性不低于99.95% |
| 安全性 | 安全传输 | SSL网银级别加密传输 |
| MD5校验技术 |
| 有效抵御网络攻击 |
| 病毒查杀 | 支持云端文件杀毒功能 |
| 安全策略 | 支持安全组策略：提供虚拟防火墙功能，可以实现云主机、云数据库服务中间的安全域划分和网络访问限制和隔离 |
| 可靠性 | 多点备份 | 存储数据多点备份 |
| 负载均衡 | 底层设备采用分布式和负载均衡架构，无单点故障，切换不影响上层应用运行 |
| 兼容性 | 兼容性/开放性（接口、引擎等） | 支持最新版主流浏览器，支持国密浏览器 |
| 其他 | 扩展 | 建设浦东教育云盘专属页面，通过开放接口和已有浦东教育统一认证平台（浦东目前有5.5万教职员工账号）打通，需支持全面对接并提供服务。 |
| 使用端 | 支持网页版、PC客户端（与网页版功能一致，包括文件管理、协同办公、后台管理） |

（4）短信服务

每年提供100万条的短信发送服务。

**具体服务要求：**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 覆盖全国 | 能够支持发送包括省内、省外的所有用户(含携号转网用户)，支持发送全国归属地的手机用户； |
| 上下行统一 | 用户接收到消息后，能直接对此短信号码进行回复；采购人可接收到用户回复的内容； |
| 支持长短信 | 当发送字数超过单条短信限定的字数时，可把多条短信内容合并成一条长短信进行发送； |
| 短信验证码 | 多网合一专属通道，与工信部携号转网平台实时互联。变量灵活，支持带入变量，内容灵活。 |
| 异步通知 | 可在后端服务处理完成任务时，回调通知用户。进而减少用户、Web前端和后端服务之间大量不必要的轮询请求。 |
| 数据统计 | 可查看请求量、发送成功量、失败量等统计数据；通过日期、手机号等维度查看发送详情。 |
| 短连接 | 通信双方以客户-服务器方式建立TCP连接，应答与请求在同一个连接中完成。系统采用客户/服务器模式，操作以客户端驱动方式发起连接请求，完成一次操作后关闭此连接。通信双方之间的消息发送后等待T秒后未收到响应，应立即重发，再连续发送N-1次后仍未得到响应则停发。 |

##### 10.2.6服务管理平台要求

多云服务管理平台：本期需要构建统一云管平台服务，方案应确保非信创云和信创云的统一管理、以及多云接入能力，满足业务弹性伸缩和快速部署要求，实现资源信息、业务信息、运维信息、安全态势信息的展现，准确而高效、精简而全面地传递信息，充分展现浦东教育云的整体运行情况，提供安全可靠的统一的资源服务管理，请提供相关证明材料。

多云服务管理平台需对接现有浦东教育云网一体化运维管理平台，确保业务连续性。

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 整体视图 | 资源展示：展现多云整体平台的资源概览，包括不同资源池的资源总量，资源使用情况等。 |
| 业务展示：立足于平台资源用户，展现平台上各个用户的资源使用量，使用率，对平台上资源的分布，用户的比重有直观了解。 |
| 运维展示：展示平台上各个资源的告警信息，以期做到准确分析，提前预警的能力 |
| 安全态势：包括漏洞发现及修复；配置及性能信息采集、日志预处理、虚拟化云安全平台安全日志采集、软硬件安全子系统日志采集（如waf、探针、IPS等）。 |
| 统一的资源管理 | 通过浦东教育云多云服务管理平台对部署在多云上的虚拟化资源和物理资源进行统一管理，满足业务弹性伸缩和快速部署要求。展示全量的资源信息，包括资源的自有属性以及与业务相关的信息；形成一套统一的操作流程，屏蔽资源的厂商，达到操作的规范性、便捷性以及一致性。 |
| 展示云服务器、物理设备、网络资源、服务器、存储设备等资源的信息，展现它们的自有属性值，此外还应展现资源关联学校、应用的信息。 |
| 可以对虚拟化资源进行管理，包括虚机的创建、关闭、启动；网络资源的自主可配，裸金属服务器等物理设备的管理等。 |
| 提供各种资源的查询，全量信息的导出功能。 |
| 统一的运营管理 | 按照浦东教育服务流程，提供定制化的审批流程，支持包括但不限于云资源服务、专网接入服务、学校网站服务、网站群服务、VPN服务、教育网无线服务等服务，实现按角色分权分域，满足不同业务场景的周期管理，并支持流程节点的变更短信通知，提高处置效率。 |
| 提供完整的服务生命周期管理，将资源池下计算、存储、网络资源以服务的形式提供给用户，用户可以从服务目录上申请，对于已经申请的服务，用户可以使用、维护、变更、释放。 |
| 对资源的变更进行记录，包括资源所属学校，资源属性变更的详细数据，资源变更的操作记录。 |
| 对资源的变更进行记录，包括资源所属学校，资源属性变更的详细数据，资源变更的操作记录。 |
| 统一的运维监控 | 通过浦东教育云多云服务管理平台，使得监控运维一体，实现维护的及时性，促使问题得到精准、快速的解决，保障教育云的平稳运行。 |
| 对资源进行监控，提供多种性能数据。 |
| 可自定义的设置性能阈值，资源性能超过阈值时，进行告警。 |
| 设定规则，监控判断系统中疑似存在的僵尸主机。 |
| 根据运维经验，形成一套运维规则，方便后续的自动化运维。 |
| 统一的认证体系 | 支持对接浦东教育统一认证平台，同步学校、教职工信息； |
| 支持云管统一认证体系，支持从统一认证平台登陆，按照统一认证账号进行角色权限的分权分域。 |
| 统一的服务管理 | 提供运维日志审计，对文件进行完整性校验，及归档处理 |
| 提供通知服务，通过平台发送相关通知 |
| 提供统一的RESTFUL API接口，方便功能的扩展以及进行二次开发。 |
| 提供可定制化的报表，满足不同用户的需求。 |

##### 10.2.7业务连续性服务要求

若存在存量系统迁移，则中标人需对存量业务提供对应资源量证明，并提供一次性迁移服务。中标人应详细描述针对现有云平台及应用的整体迁移制定相关迁移服务方案，迁移方案包括但不限于业务迁移调研、业务迁移评估，业务迁移规划、迁移组织及职责分工、迁移实施方案设计、迁移回退方案、迁移应急预案等内容，以确保不影响采购人业务连续性；同时，需提供满足目前平台应用承载现状资源量的平台整体能力证明，负责完成云平台整体的无缝割接，确保整体云平台应用的平滑迁移，平台核心应用迁移业务中断时间不超过30分钟，保障业务IP地址不变以确保业务连续性服务。

中标人需具备提供浦东教育局及下属单位应用和数据迁移上云的服务能力，包括应用入云迁移前期调研、配合设计及实施服务，迁移过程中能具备相应数据备份保障能力，提供迁移部署实施过程中的迁移工具和服务。

应用迁移服务需支持对整个迁移过程可视化、可控制、可回退，支持以在线的方式对主机系统进行迁移，操作可图形化，整个过程操作时，可以回退，迁移时的数据需要进行加密，保证安全。投标人应具备丰富的类似项目系统迁移上云经验。如有近3年内教育类、政务类信息系统迁移案例，请提供相应证明材料。

**11质量标准和验收方案**

11.1本项目采用现场运维、服务检查方式验收。投标人完成的服务项目应达到的质量标准应符合国家、地方及相关政府管理部门和行业与本项目有关的各项技术标准、规范要求，并满足采购人 实际需求，前述标准、规范等不一致的，以要求高（严格）的为准。

11.2投标人定期交付服务期间的形成的各种技术文档、管理制度和运维记录。包括周报、月报等常规性周期性记录；也包括重点工作、专项技术分析、技术建议等文档。

11.3投标人所交付的服务还应符合国家和上海市有关安全、环保之规定。

11.4本项目验收将由采购人组织进行，采购人也可委托第三方组织验收。

11.5浦东教育云平台，应满足《GBT2223 9-2019信息安全技术网络安全等级保护基本要求》三级要求，并在验收前提供本服务期内达标的网络安全三级等保测评报告。

11.5 具体教育云服务指标要求如下：

| 指标名称 | 指标要求 |
| --- | --- |
| 平台可用性 | 中标人应承诺在合同期内云平台整体可用性每年不低于99.99%，即每年实际可用时间/(实际可用时间+不可用时间)。（经用户授权的系统正常升级、更新、维护导致服务停机以及经认定非因云平台服务提供商引起的系统失效不包含在故障时间内） |
| 数据存储持久性 | 中标人承诺在合同期内数据可靠性应不低于99.99%，即每年完好数据/(完好数据+丢失数据)。 |
| 数据可迁移性 | 中标人承诺用户能够控制数据的迁移，保证启用或弃用该云服务时，数据能迁入和迁出。 |
| 数据私密性 | 中标人应承诺用户应有加密或隔离等手段保证同一物理资源池的用户数据互不可见。 |
| 信息安全责任事故考核 | 服务期间不发生发生信息安全责任事故。若因中标人原因，发生信息安全责任事故，应承担由此给采购人造成的实际损失。信息安全责任事故是指由中标人提供的机房、网络、安全、虚拟机、物理机、存储、运维等方面出现问题引起的信息安全责任事故。经采购人认定由非中标人引起的信息安全责任事故不包含在内。 |
| 系统保密考核 | 服务期间不发生数据外泄等系统保密事件。因中标人原因，导致发生数据外泄等系统保密事件，应承担由此给采购人造成的实际损失。 |
| 资源交付服 务响应时间 | 中标人承诺资源开通、变更完成后交付用户时间-收到需求时间，标准需求不超过2 个工作日占比80%以上，最多不超过5个工作日。 |
| 重大通信保障 | 重大活动期间，按需提供每周7天\*24小时服务保障工作，10分钟内响应。重大故障和关键故障在2小时内到达现场。在故障发生的情况下，根据事件严重性及时响应并提供快速问题解决；包括手工杀毒等重大安全事件补救。 |
| 上云系统安全服务 | (1)上云系统安全服务工单：受理时间每周5天\*8小时，响应时间≤20分钟。堡垒机工单：完成堡垒机的账号开通、变更，资产导入、变更。WAF工单：配置防护站点及策略，根据日志，开启防护。防火墙工单：完成防火墙策略的开通变更。  (2)解决上云系统已开通的安全服务在使用过程中出现的问题：每周7\*24小时服务保障工作，15分钟内响应。重大故障和关键故障在2小时内到达现场。对上云使用单位在安全服务开通或使用中遇到的问题，给出解决方案、优化建议，提供安全工程师知识与经验 |
| 故障恢复时间 | 中标人承诺一般事件需在360分钟内恢复、重大事件需在60分钟内恢复、特别重大事件需在30分钟内恢复。  说明：  一般事件：单个应用系统发生中断或无法正常管理，应用部分不稳定或不能进行正常运行。  重大事件：云平台发生故障造成多个应用系统发生中断或无法正常管理，应用部分不稳定或不能进行正常运行；云平台链路不能提供足够带宽影响应用正常使用。  特别重大事件：云平台发生故障造成系统失效或崩溃，丢失数据等，且没有临时替代解决方案；系统硬件故障、系统崩溃（死机和自动重启）且不能再启动、磁盘信息丢失、系统或应用服务无法启动、网络链接失效、文件损毁等。 |
| 应急演练 | 每个验收服务期内不少于2次。全服务期不少于8次。 |
| 运维响应时限 | 中标人应提供每周5天\*8小时时限内的快速日常服务，包括需求受理、云平台、网络、安全等，运维应答和响应最多不超过10分钟 |
| 培训要求 | 每年不少于2次，全服务期不少于8次 |

**12人员及设备配备要求**

投标人要求指派专门的项目经理或服务经理管理驻场人员。投标人要求提供项目实施团队清单，实施团队22人。项目经理职责包括但不限于把控服务计划和实施进度、监督并提升服务交付质量、与 客户沟通待协商问题、汇报工作里程碑、负责管理维护相关文档。

（1）项目经理1人，需具有高级工程师，如具有PMP项目管理的能力证书请提供相关证明文 件；

（2）技术经理1人，需具备高级工程师，如具有云计算架构师、PMP/PRINCE2、CDCP认证专业的能力证书请提供相关证明文件；

（3）项目实施团队20人，其中具备中级工程师及以上能力证书的不少于10人，具备PMP、网络、云平台、安全、高低压电工专业能力证书之一的不少于10人。

投标人提供专业运维团队对整个机房中设备和云平台进行每周7天×24小时运维监控，日常运维团队16人（其中4人现场每周5天\*8小时驻场服务）。具备中级工程师及以上能力证书不少于 3人，具备网络、云平台、安全、高低压电工专业能力证书之一的不少于10人。若出现有人员离职等情况，要求确保人员、工作的无缝衔接。合同期内，不得在采购人不同意的情况下，更换项目经理和驻场人员。

投标人要求在合同签订后的10天内，落实全部人员到位。运维人员需具备相关领域的认证资质或经验证明，为保障项目服务质量，运维服务团队成员需具备相关工作能力和经验，并提供相关证明材料。

项目实施和运维团队人员都需为服务提供商自身员工，需出具在职证明材料。

**13安全文明作业与应急处置要求**

**13.1 安全文明作业要求**

中标人派驻在采购人办公场所的人员应遵守所在地管理要求，包括但不限于安全生产、防疫要求等。

中标人在浦东教育云的各项运维工作，不得违反浦东教育专网安全管理制度，危害浦东教育专网安全、稳定运行。

（1）投标人及其劳务分包商应具备上海市或有关行业管理部门规定的在本市进行相关服务所需的资质（包括国家和本市各类专业工种持证上岗要求）、资格和一切手续（如有的话），由此引起的所有有关事宜及费用由投标人自行负责。

（2）在提供服务期间为确保服务区域及周围环境的整洁和不影响其他活动正常进行，中标人应严格执行国家与上海市有关安全文明施工管理的法律、法规和政策，积极主动加强和落实安全文明施工及环境保护等有关管理工作，并按规定承担相应的费用。中标人若违反规定而造成的一切损失和责任由中标人承担。

（3）中标人在项目实施期间，必须遵守国家与上海市各项有关安全作业规章、规范与制度，建立动用明火申请批准制度，安全用电等制度，确保杜绝各类事故的发生。

（4）建立健全安全生产工作责任体系和组织管理网络，建立安全生产监管制度，配备专职安全监管人员，对施工作业安全进行现场监督；按照“横向到边，纵向到底”责任制要求将安全责任分解，中标人法定代表人与项目部、项目部与下属各责任部门必须签订安全协议书；定期召开安全生产工作会议；组织开展安全生产检查。

（5）各投标人在投标文件中要结合本项目的特点和采购人上述的具体要求制定相应的安全文明施工措施，同时应适当考虑购买自己员工和第三方责任保险，并在报价措施费中列支必须的费用清单。

**13.2应急处置要求**

（1）中标人须建立突发事件应急处置方案，应急预案应包括组织领导体系、预警和预防机制、应急响应工程措施、临时交通组织方案、保障措施（包括应急人员、物资、机械设备、资金等）等内容。

（2）建立应急指挥领导小组，负责应急救援总体指挥，并落实各部门职责和相关措施。

（3）与气象、交警、消防、医疗等部门建立联动机制，如过程中发生重特大安全事故，中标人应快速、及时赶到现场，实施紧急处置，并协同有关单位和部门做好善后处理和稳定工作。

（4）组建一支具有综合救援能力的应急救援队伍，一旦紧急情况发生，能在最短时间内到达现场进行应急处置。

（5）定期检查应急救援物资与机具，确保物资储备数量充足、机具设备完好可用。

（6）定期或不定期开展多方式多类别的应急演练，提高应急队伍的响应速度、救援水平和协同能力，并根据演练过程总结和结果评估，完善应急预案。

（7）建立应急值守制度，安排专职人员，监测、收集各类信息；一旦发现突发性的紧急事件，在启动应急响应的同时，必须及时将情况上报业主，上报的应急信息必须实事求是，不得瞒报、谎报和拖延不报，上报形式可用电话口头初报，随后再书面报告；业主应急值班联系电话：\*\*，传真：\*\*。

**14售后服务要求（包括延伸服务要求）**

**14.1 售后服务**

为本项目提供浦东新区范围内固定的售后服务团队，且能提供良好的技术支持。

**14.2 具体服务承诺**

中标人需提供全部采购内容的运维服务，按照服务质量保证的服务标准提供各种售后服务。在中标人服务期内，负责本项目的维护工作，确保系统安全、稳定、正常地运行并对由于设计、功能的缺陷而产生的故障负责。中标人提供每周7天\*24小时的运维服务保障。

在此期间如发生系统运作故障，或出现瑕疵，中标人将按照售后服务的承诺提供保修和维护服务。中标人提供运维热线电话、电子邮件和在线网站等技术支持方式：

（1）电话支持：客户通过拨打中标人指定的运维热线电话，提供每周7天×24小时电话响应服务。由中标人工程师进行电话支持。

（2）远程技术支持：在采购人保证服务器网络联通的情况下，通过远程诊断、电话支持、电子邮件等方式进行技术支持。

（3）现场支持：如果不能通过远程技术支持方式解决系统的技术故障，在用户提出现场支持要求后的24小时内，中标人将派遣工程师赶赴现场分析故障原因，制定故障排除方案，提供故障排除服务。

运维服务内容包含但不限于：

①日常监控：

对教育云平台进行日常监控，包括监控告警的处理等。

②故障处理：

处理教育云发生的各类平台软硬件、通信线路等故障，确保上层业务系统能够正常稳定运行；其中故障处理流程需要规定处理时限及当前处理环节的责任部门和责任人。

需对服务过程出现的故障响应做出相关保证。故障响应及时率100%，故障修复及时率100%。应建立完善的故障管理体系，按照故障等级不同，需要有不同的处理时长和故障恢复时限。

③安全服务：

需对云平台内部系统安全做出相关保证，需提供业务侧的标准安全内容。

④节假日保障：

重大节假日期间进行运行和信息安全的重点保障。中标人如具备重大事件运营保障能力和经验，请在投标文件中提供相关证明文件。

**15 项目的保密和知识产权**

15.1 中标人保证对其提供的服务及出售的标的物享有合法的权利，应保证在其出售的标的物上不存在任何未曾向采购人透露的担保物权，如抵押权、质押权、留置权等。

15.2采购人委托开发软件的知识产权归采购人所有。中标人向采购人交付使用的信息系统已享有知识产权的，采购人可在合同文件明确的范围内自主使用。

15.3在本合同项下的任何权利和义务不因中标人发生收购、兼并、重组、分立而发生变化。如果发生上述情形，则中标人的权利随之转移至收购、兼并、重组后的企业继续履行合同，分立后成立的企业共同对采购人承担连带责任。

15.4 中标人应遵守合同文件约定内容的保密要求。如果采购人提供的内容属于保密的，应签订保密协议，且双方均有保密义务。中标人不得利用工作之便外泄资料或做其他用途，否则中标人需承担由此引起的法律责任和赔偿采购人的经济损失。本款规定的效力及于中标人及中标人的所有雇用人员。

15.5浦东新区教育云平台上的数据所有权归各云应用系统所有人所有，未经数据所有人同意，中标人不得通过任何手段收集、分析、处理教育公共云平台中的数据。禁止篡改数据，或将数据以任何方式或渠道泄露出去。未经数据所有人许可，中标人不得将本次招标的相关文件、资料等提供给任何第三方。

15.6 如采购人使用该标的物构成上述侵权的，则中标人承担全部责任。

**16 技术培训**

中标人需根据本项目特点，建立涵盖多方面能力培训的能力中心。具体包括浦东教育云平台使用和管理能力培训、软件支撑层操作系统使用和管理能力培训、软件支撑层数据库使用和管理能力培训。为确保培训质量，中标人需安排具备专业资质的培训讲师进行授课，并提供完整的培训教材和详细的课程计划表。

所有培训费用（含培训教材费）及各项支出需纳入各服务项费用中，不得另行单独报价。

16.1技术文件：

中标人应为所有被培训人员提供培训用文字资料及本系统的详细技术文件。

培训结束后10个工作日内向采购人提交完整的培训过程材料，包括：培训总结报告、培训方案、学员须知、学员签到记录表、参训学员名单信息和考核结果、培训课程安排表、培训专家授课课件、学员培训满意度测评问卷及问卷分析报告等。

16.2技术服务：

（1）投标人应具有健全的培训管理制度和管理流程、培训计划。

（2）培训目标为项目所涉及的主管部门、教育单位及相关运维单位的负责人等，投标人需采取集中培训、远程培训等多种形式的培训组织方式。培训内容包括软件的使用及维护培训，使受训者能够独立、熟练地完成系统运行维护与操作，实现依据本合同所规定的系统运行保障的目标。

（3）培训时间与日期由采购人和中标人共同商定，每年不少于2次。

四、投标报价须知

**17 投标报价依据**

17.1 投标报价计算依据包括本项目的招标文件（包括提供的附件）、招标文件答疑或修改的补充文书、工作量清单、项目现场条件等。

17.2招标文件明确的项目范围、实施内容、实施期限、质量要求、售后服务、管理要求与标准及考核要求等。

17.3工作量清单说明

17.3.1 工作量清单应与投标人须知、合同条件、项目质量标准和要求等文件结合起来理解或解释。

17.3.2采购人提供的工作量清单是依照采购需求测算出的主要工作内容，允许投标人对工作量清单内非核心工作内容进行优化设计，并依照优化后的方案进行报价。各投标人应认真了解招标需求，如发现核心工作内容和实际采购需求不一致时，应立即以书面形式通知采购人核查，除非采购人以答疑文件或补充文件予以更正，否则，应以工作量清单为准。

**18****投标报价内容**

18.1 本项目报价为全费用报价，是履行合同的最终价格，除投标需求中另有说明外，投标报价（即投标总价）应包括项目前期调研、数据收集和分析、方案设计、项目研发、基础环境集成实施、智能化安装工程、硬件集成实施、软件开发和集成实施、安全集成实施、系统调试及试运行、验收和评估、操作培训、售后服务、投入使用这一系列过程中所包含的所有费用。

18.2 投标报价中投标人应考虑本项目可能存在的风险因素。投标报价应将所有工作内容考虑在内，如有漏项或缺项，均属于投标人的风险，其费用视作已分配在报价明细表内单价或总价之中。投标人应逐项计算并填写单价、合计价和总价。

18.3在项目实施期内，对于除不可抗力因素之外，人工价格上涨以及可能存在的其它任何风险因素，投标人应自行考虑，在合同履约期内中标价不作调整。

18.4 投标人按照投标文件格式中所附的表式完整地填写《开标一览表》及各类投标报价明细表，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

**19投标报价控制性条款**

19.1 投标报价不得超过公布的预算金额或最高限价，其中各分项报价（如有要求）均不得超过对应的预算金额或最高限价。

19.2 本项目只允许有一个报价，任何有选择的报价将不予接受。

19.3 投标人提供的服务应当符合国家和上海市有关法律、法规和标准规范，满足合同约定的服务内容和质量等要求。不得违反法规标准规定或合同约定，不得通过降低服务质量、减少服务内容等手段进行恶性低价竞争，扰乱正常市场秩序。

★19.4经评标委员会审定，投标报价存在下列情形之一的，该投标文件作无效标处理：

19.4.1减少工作量清单中核心工作内容数量；

19.4.2 投标报价和技术方案明显不相符的。

五、政府采购政策

**20 节能产品政府采购**

20.1 按照财政部、发改委发布的《关于印发〈节能产品政府采购实施意见〉的通知》（财库[2004]185号）和《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的要求，采购人采购的产品属于“节能产品品目清单”中的，在技术、服务等指标同等条件下，应当优先采购节能产品。采购人需购买的材料产品属于政府强制采购节能产品品目的，投标人必须选用节能产品。

20.2投标人如选用节能产品的，则应在投标文件中提供国家确定的认证机构出具的、处于有效期之内的节能产品的认证证书；反之，该产品在评标时不被认定为节能产品。

**21环境标志产品政府采购**

21.1 按照财政部、环保总局联合印发的《关于环境标志产品政府采购实施的意见》（财库[2006]90号）和《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）的要求，采购人采购的产品属于“环境标志产品品目清单”中的，在性能、技术、服务等指标同等条件下，应当优先采购环境标志产品。

21.2投标人如选用环境标志产品的，则应在投标文件中提供国家确定的认证机构出具的、处于有效期之内的环境标志产品的认证证书；反之，该产品在评标时不被认定为环境标志产品。

**22 促进中小企业发展**

22.1 中小企业（含中型、小型、微型企业，下同）的划定按照《中小企业划型标准规定》（工信部联企业【2011】300号）执行，参加投标的中小企业应当提供《中小企业声明函》（具体格式见“投标文件格式”），反之，视作非中小企业，不享受相应的扶持政策。如项目允许联合体参与竞争的，则联合体中的中小企业均应按本款要求提供《中小企业声明函》。

22.2 依据市财政局2015年9月发布的《关于执行促进中小企业发展政策相关事宜的通知》，事业单位、团体组织等非企业性质的政府采购供应商，不属于中小企业划型标准确定的中小企业，不得按《关于印发中小企业划型标准规定的通知》规定声明为中小微企业，也不适用《政府采购促进中小企业发展管理办法》。

22.3 如项目允许联合体参与竞争的，组成联合体的大中型企业和其他自然人、法人或者其他组织，与小型、微型企业之间不得存在投资关系。

22.4对于小型、微型企业，按照《政府采购促进中小企业发展管理办法》（财库【2020】46号）和《关于进一步加大政府采购支持中小企业力度的通知》（财库【2022】19号）规定，其报价给予**10%**的扣除，用扣除后的价格参与评审。

22.5如项目允许联合体参与竞争的，且联合体各方均为小型、微型企业的，联合体视同为小型、微型企业，其报价给予**10%**的扣除，用扣除后的价格参与评审。反之，依照联合体协议约定，小型、微型企业的协议合同金额占到联合体协议合同总金额30%以上的，给予联合体**4%**的价格扣除，用扣除后的价格参与评审。

22.6供应商如提供虚假材料以谋取成交的，按照《政府采购法》有关条款处理，并记入供应商诚信档案。

**23** **促进残疾人就业（注：仅残疾人福利单位适用）**

23.1 符合财库【2017】141号文中所示条件的残疾人福利性单位视同小型、微型企业，享受促进中小企业发展的政府采购政策。残疾人福利性单位属于小型、微型企业的，不重复享受政策。

23.2 残疾人福利性单位在参加政府采购活动时，应当按财库【2017】141号规定的《残疾人福利性单位声明函》（具体格式详见“投标文件格式”），并对声明的真实性负责。