合同编号：DXHSPJ-F-2026008

合　同　书

项目名称： 2026年武汉市东西湖区交易中心数据存储服务

甲方（采购人）： 武汉市东西湖区行政审批局

乙方（中标人）： 中金数据（武汉）超算技术有限公司

签订地： 湖北省武汉市东西湖区

签订日期： 2026 年 1 月 20 日

本合同由甲乙双方根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《中华人民共和国民法典》等相关法律法规规定，按平等、自愿、诚实、信用的原则拟定，甲、乙双方均应遵守法律规定和合同约定，并各自履行应负的全部责任和义务。

第一条 项目基本情况

1. 项目名称：2026 年武汉市东西湖区交易中心数据存储服务

2. 项目编号：HBCZ-2503051708-254293

3. 政府采购计划备案号：420112-2025-03265

4. 项目概况：经武汉市东西湖区行政审批局（采购人）授权湖北省成套招标股份有限公司（第三方采购代理机构）于 2025 年 12 月 24 日公开招标，确认中金数据（武汉）超算技术有限公司为中标单位，承担本次项目的服务供应任务；经采购人、中标人双方友好协商，依据招、投标文件的约定签订本合同文书。

第二条 合同组成和定义

2.1 本合同由下列各部分组成：

2.1.1 本合同正文；

2.1.2 附件一《工作内容说明书(SOW)和服务水平协议(SLA)》；

2.1.3 附件二《中金云资源服务订单》；

2.1.4 附件三《中金云平台客户入网安全责任书》；

2.1.5 附件四《服务质量综合评审表》

2.2 本合同所用术语的含义，由附件一《工作内容说明书SOW和服务水平协议SLA》定义。

第三条 服务内容与服务期限

3.1 甲方委托乙方提供《2026年武汉市东西湖区交易中心数据存储服务》的云资源服务（以下称“本项目”），为公共资源交易中心不见面开标系统及政府采购电子交易系统相关数据及服务器提供存储服务（含云主机、云硬盘、网络通信及安全防护等服务）以支持系统运行，具体服务内容清单详见附件二：《中金云资源服务订单》。

3.2 本合同履行期限：2026 年 1 月 20 日至 2027 年 1 月 19 日；服务期满后，根据服务质量考核结果，甲方（采购人）可以选择续签服务合同，续签合同最多不超过 2 年。

3.3 乙方应在本合同签定生效之日起 5 个工作日内交付本项目的云服务资源，同时配合甲方完成云资源验收。

第四条 合同价款及付款方式

4.1 合同价款总额为人民币￥489,150.00 元（大写：肆拾捌万玖仟壹佰伍拾元整 ）。本合同价款总额为含税金额，税率为 6 %。

4.2 甲方采用□现金 □支票 ☑汇付的方式向乙方支付合同款项。

4.3 付款方式：具体付款方式如下：

合同签订后 5 个工作日内，乙方向甲方交付云平台资源，并向甲方提供合同价款 40 %的发票；甲方收到发票后 5 个工作日，向乙方支付合同价款的 40 %，计人民币￥195,660.00 元（大写：壹拾玖万伍仟陆佰陆拾元整）；

本合同服务期满前一个月进行云平台的服务质量考核，考核后乙方向甲方提供合同价款 60 %的发票，甲方收到发票后 5 个工作日，向乙方支付合同价款的 60 %，计人民币￥293,490.00 元（大写：贰拾玖万叁仟肆佰玖拾元整）。

4.4 乙方收款信息：

户名：中金数据（武汉）超算技术有限公司

开户行：交通银行武汉硚口支行

银行账号：4214 2103 1012 0023 2508 9

开户行号：301521004009

4.5 甲方开票信息：武汉市东西湖区行政审批局

地址： 武汉市东西湖区七雄路 111 号

电话：027-83893513

纳税人识别号：11420112MB1114851Q

开户银行： 中行东吴大道支行

账号：569072194709

第五条 甲方权利义务

5.1 甲方应协助乙方完成云平台资源初始化工作。

5.2 甲方应按照本合同约定使用云平台资源服务，遵守相关法律法规。

5.3 甲方负责其部署在云平台资源上的各项应用程序的运维及监控。若需乙方提供服务，甲方可以另行购买乙方提供的相应增值服务。

5.4 甲方将云平台环境与已有信息系统环境进行对接及连通时，应提前5个工作日向乙方提供对接及连通的相关信息（包括网络设备信息、配置、IP地址信息等）。

5.5 甲方利用云平台资源开展业务时，应确保具备相关法律法规所要求的执照、许可和授权，且遵守该执照、许可和授权相关的规定。

5.6 遵守相关法律法规（包括但不限于《网络安全法》、《互联网信息服务管理办法》）保留自己网站的访问日志记录，包括发布的信息内容及其发布时间、互联网地址（IP）、域名等，国家有关机关依法查询时应配合提供。甲方将承担未按规定保留相关记录而引起的相应法律责任，确保在云平台资源上进行的活动合法合规。

5.7 甲方应当确保：（1）甲方客户业务数据处理(包括但不限于获取、使用、处理与传输等，以下合称“处理”)的合法性。（2）甲方在处理客户业务数据时已取得合法、有效、充分且必要的授权，未侵犯任何第三方的合法权益。（3）甲方应当对客户业务数据以及甲方处理客户业务数据是否符合法律法规、部门规章和国家政策的规定进行必要审查，并由甲方承担所有责任，乙方不会因为客户业务数据或甲方处理客户业务数据违反上述约定，而需要承担任何责任。

5.8 甲方应对自身的客户业务数据的来源及内容负责，并谨慎判断数据来源及内容的合法性。甲方将承担因自身的业务数据内容违反法律法规、部门规章或国家政策而造成的相应结果及责任。

5.9 甲方除遵守国家有关规定外，还应理解并遵守乙方关于网络安全的有关规定，

详见附件三《中金云平台客户入网安全责任书》的相关内容。

第六条 乙方权利义务

6.1 乙方按本合同约定提供云平台资源服务，工作内容和服务水平按附件一《工作内容说明书SOW》和《服务水平协议SLA》执行。但甲方开展业务所需的应用程序及其运行所需的操作系统、中间件、数据库等软件授权由甲方负责。

6.2 当云平台环境发生紧急、异常情况，乙方依据附件一《工作内容说明书SOW》和《服务水平协议SLA》以邮件或电话等形式通知甲方并及时解决。

6.3 乙方按本合同约定安排工程师对甲方的服务需求和问题提供技术支持和及时响应。

第七条 网络安全

7.1 甲方需要根据国家有关法律、行政法规、行政规章以及监管指令，认真执行网络安全、数据安全与隐私保护的相关管理规定。甲方使用云主机服务所搭建的网络系统、应用程序由甲方进行管理和运营。乙方仅负责操作系统以下的底层部分（如基础设施及物理设备）及乙方提供的软件的运营维护，即服务的相关技术架构及乙方提供的操作系统等。操作系统之上部分（如甲方在系统上安装的应用程序）由甲方负责。此外，甲方自行升级操作系统可能会造成宕机等不良影响，请把握风险并谨慎操作。甲方理解并同意，甲方需要根据自身所处理数据和业务系统的安全要求选择、配置和使用所采购的云安全产品。乙方所提供的一系列的服务和能力，甲方可以通过乙方的安全服务实现不同程度的管控。

7.2 对于网络和数据安全风险（包括但不限于系统漏洞、计算机病毒、网络攻击、网络侵入、数据泄露等安全风险），甲方应当制定云上安全策略采购必要的安全服务，以实现上述风险的防范、监测和处置。

7.3 甲方可根据业务需要自行购买乙方提供的安全产品及服务，甲方知悉并确认，使用安全服务是提升计算机信息系统、设备安全性的必要措施，乙方将按照甲方所购买的安全产品向甲方提供安全保护服务，但甲方仍需要结合产品的使用

情况自行判断安全保护服务是否符合自身数据和业务系统安全性和合规性要求。

7.4 鉴于网络安全技术的局限性、相对性、不可预见性，甲方理解并充分认可，如因甲方服务器、业务系统或网站遭遇计算机病毒、网络入侵和攻击破坏（包括DDoS）等危害网络安全事项或行为而给乙方或者乙方的其他客户的网络或服务器（包括但不限于本地及外地和国际的网络、服务器等）带来危害，或影响乙方与国际互联网或者乙方与特定网络、服务器及乙方内部的通畅联系，乙方可决定暂停或终止服务。如果终止服务，乙方将按照实际提供服务月份计算（不足一个月的按天计）服务费，将剩余款项（如有）退还甲方。

第八条 合同解除与终止

8.1 有下列情形之一的，乙方有权解除与终止本服务合同：

8.1.1 依据法律法规或者政府机关的要求；

8.1.2 为甲方继续提供服务将会对乙方造成重大安全风险；

8.1.3 甲方服务费支付逾期超过30日；

8.1.4 甲方违反本合同的其他义务，经乙方要求后仍未在规定的（若未规定则为合理）期限内补救。

8.2 服务终止后，对于甲方使用的云主机等相关数据，乙方应保留30日，并通知甲方其数据将在服务终止后第30日被删除。

第九条 合同变更

9.1 在履行本合同期间内，双方均可以提出变更要求，项目变更须经过甲、乙双方的协调与审核，双方同意后方可执行，以免影响项目之价格、进度及合同内其它条款的变更。

9.2 双方均应以书面方式提出项目变更申请，变更申请一方应先填写变更申请表，描述变更内容、原因及对项目的可能的影响，甲、乙双方将负责审核及协调所提出的变更要求，并决定是否接受变更。若拒绝变更时，申请变更的书面资料将退回原申请方。

9.3 合同中描述的服务内容及服务期限若有任何增加或变更，均须经双方签署变更申请表之后方能生效执行；因此所产生的服务期及费用增加，甲方在签署并确认实施后第二个月首日开始计算服务期，并支付相关服务费。变更申请表视为原合同的修订文件。

第十条 违约责任

10.1 如乙方未按合同约定完成服务项目，甲方有权要求乙方支付违约金。具体可按以下条款执行：

（1）由于乙方原因导致服务交付延期 15 日以内的，每延期 1 日，应延长 5 日服务期；

（2）由于乙方原因导致服务交付延期超过 15 日及以上的，乙方应当向甲方支付合同价款总额万分之五的违约金，同时每延期 1 日，应延长 5 日服务期；

（3）由于乙方原因导致服务交付延期超过 30 日及以上的，甲方有权解除合同，并要求乙方按照逾期天数支付违约金。

10.2 甲方逾期付款的，乙方有权要求甲方支付违约金。具体可按以下条款执行：

（1）每逾期 1 日，甲方应当向乙方支付合同价款总额万分之五的违约金；

（2）如逾期超过 30 日，乙方有权解除合同，并要求甲方按照逾期天数支付违约金。

10.3 如因乙方原因造成甲方云主机中断，乙方应按中断时间的10倍延长服务期，不足一小时的按一小时计算。

10.4 因乙方重大违约行为(包括但不限于数据泄露、服务中断超过24小时等)导致甲方产生的业务损失、收益损失等间接损失，乙方应予以赔偿。

10.5 如甲方违反本合同 5.7、5.8 条款，则乙方有权立即停止提供服务，因此给乙方造成损失的，乙方有权要求甲方予以赔偿。

第十一条 责任限制

11.1 如甲方将云平台环境用于任何违法活动，甲方应承担全部法律责任，与乙方无关。乙方有权因此终止对甲方的服务，无需退还已收取的服务费。

11.2 除双方另有约定外，乙方不负责甲方使用的云主机中的操作系统、应用程序、甲方数据以及有关的系统配置数据等的管理和安全。

第十二条 知识产权及保密

12.1 乙方提供给甲方使用的云平台资源及相关技术资料等的知识产权属于乙方所有，涉及第三方资源的知识产权属于该第三方所有。甲方仅享有基于本合同目的的非独占、非排他、不得转许可的一般使用权，订单约定的服务期满后，乙方授权甲方的一般使用许可同时终止。

12.2 甲方不得删除、修改或掩藏乙方和任何第三方知识产权中包含的任何版权、商标或其他专有权标识、声明，或者进行其他侵权行为。

12.3 一方对在签订和履行本合同或订单过程中从对方获知的商业秘密，无论在本合同期限内还是合同终止后，均应遵守知识产权、反不正当竞争及其他方面的法律规定，尊重对方的知识产权和商业秘密，对所知悉的对方的商业秘密保密。

12.4 未经对方事先授权，任何一方不得以任何方式向任何第三方泄露、转让、许可使用、交换、赠与或与任何第三方共同使用或不正当使用对方的和/或知识产权。违反本款规定，给对方造成损失的，违约方应依法承担责任，但依据有关法律、法规应当提供的，或行政机关、司法机关依照职权要求该方必须提供的除外。

12.5 乙方不得未经甲方允许，以任何方式使用和利用（包括但不限于阅读、调取、分析、复制等方式）甲方在本合同项下之云平台上存储或者生成的数据和信息，同时乙方之员工或者其关联方、合作方通过乙方之便利条件实施以上行为的，也均由乙方承担责任。

12.6 本条规定在本合同终止后仍对双方具有约束力。

第十三条 法律适用和争议解决

13.1 本合同适用中华人民共和国法律、法规、电信管理部门的规定和计算机行业的国家强制性的规范。

13.2 有关本合同的任何争议应由双方友好协商解决。若协商不成，任何一方应向甲

方所在地人民法院提起诉讼。

第十四条 聘用禁止

14.1 在本合同服务期内和因任何原因终止合同后三年期间内，任何一方均不得拉拢或劝诱另一方的任何雇员（不论该雇员是否已经离职）接受其直接或间接聘用。任何一方违反本条规定，应向另一方支付违约金，违约金数额为该员工离职前12个月的工资总额。

第十五条 不可抗力

由于地震、台风、战争、罢工、政府行为、非因各方原因发生的火灾、基础电信网络、黑客攻击、尚无有效防御措施的计算机病毒的发作及其它各方不能预见并且对其发生和后果不能防止并避免的不可抗力原因，致使任何一方不能履行其在本合同项下的义务，该方不承担违约责任，但该方应及时通知对方不可抗力发生的情况。双方按不可抗力对本合同的影响程度，协商是否终止本合同、免除或部分免除本合同的义务。

第十六条 通知与送达

16.1 就本合同有关事项，双方应通过本合同约定的联系方式向对方发送相关通知，本合同约定的送达地址同时作为有效司法送达地址。

16.2 一方变更通知或通讯地址，应自变更之日起 5 日内，以书面形式通知对方，否则，由未通知方承担由此而引起的相关责任。

第十七条 其他

17.1 本合同一式四份，双方各持两份，每份具有相同法律效力。

17.2 本合同经双方盖章、授权代表签字后，自文首所述签订日期起生效，至服务期满日结束。在合同有效期届满前，一方可以通知另一方协商合同的续签事宜。

17.3 在合同有效期内签署的订单约定的服务期限长于合同有效期的，该订单继续适用本合同，直至该订单服务期届满。

17.4 本合同未尽事宜双方可签订补充协议或以附件的形式作出补充。补充协议或附件为本合同不可分割的一部分，与本合同具有同等的法律效力。

（本页为签署页，无正文）

甲方：武汉市东西湖区行政审批局

单位名称（盖章）：

单位地址：武汉市东西湖区七雄路111号码头潭综合楼

法定代表人或授权委托人(签字)：

联 系 人：王毅

电　　话：027-83256481

传　　真：027-83256481

开户银行：中行东吴大道支行

账　　号：569072194709

税　　号：11420112MB1114851Q

乙方：中金数据（武汉）超算技术有限公司

单位名称（盖章）：

单位地址：武汉市东西湖区临空港经济技术开发区网安大道9号

法定代表人或授权委托人(签字)：

联 系 人：周帆

电　　话：18942940259

传　　真：027-83053138

开户银行：交通银行武汉硚口支行

账　　号：421421031012002325089

税　　号：91420112MA4KMCG90J

附件一：

工作内容说明书(SOW)和服务水平协议(SLA)

目录

在合同主文及其附件约定的服务内容、服务时间内，在甲方接受并履行相应义务的前提下，乙方将依据下述服务内容和服务水平，为甲方提供中金云资源服务。

1. 定义

本文件中，下述词语具有以下含义：

1.1 云平台资源：指满足甲乙双方约定，提供承载甲方应用的可用资源包括虚拟服务器、存储、互联网和/或专线网络接入及其它增值服务。

1.2 云平台资源服务：指甲方向乙方订购云平台资源的交付和运维服务。

1.3 云平台环境：指由乙方提供、甲方虚拟服务器运行所必须的环境，包括云平台内网络与虚拟服务器的连通性及虚拟服务器的虚拟硬件资源，如处理器（CPU）、硬盘、内存、网卡等。

1.4 基础服务：指运行云平台资源所必须的服务，包括资源初始化、云平台资源交付。

1.5 增值服务：指乙方可提供、甲方可选择的需另外付费的服务。包括云平台的内部网络服务、报告服务、数据服务、定制服务、监控服务、网络安全服务等。

1.6 可用性：指云平台资源在单位时长内可正常使用的时间与约定服务单位时长的比值，可用性=（当月服务时间－当月非计划中断时间－计划中断时间）/当月服务时间×100%）。

1.7 主责：指在某事件、环节中承担该事件、环节的主要责任方，主责包括但不限于实施、操作、运行、管理、部署。

1.8 协助：指在某个事件、环节中承担事件、环节的协助义务方，协助包括但不限于配合、协助、确认、通知、提供的必要信息。

1.9 紧急/严重情况：指云平台资源或虚拟服务器部分或全部不可用事件计划维护时段除外。

1.10 工作时段：指国家法定节假日之外的、正常工作日的工作时间。工作时段为 5X8 小时（9:00-17：30）。

1.11 工作时段故障响应时间：指确认故障发生到乙方技术人员开始处理故障的时间段。

1.12 故障解决时间：指乙方技术人员开始解决故障到故障解决、服务恢复之间的时间段，但因第三方原因或不可抗力导致的故障除外。

1.13 紧急邮件：指客户邮件题目标注有“紧急”字样所报告故障或问题影响客户关键业务、该故障或问题容许持续的时间较短的邮件。

2 工作内容(SOW)

2.1 原则

2.1.1 工作内容：资源规划、业务导入、虚拟服务器状态管理、运维管理及流程、人工支持、主动监控、技术支持服务、日常维护、约定服务报告；

2.1.2 甲方负责：除乙方所提供的资源及服务外，甲方所使用的虚拟服务器操作系统、运行于操作系统上的应用、数据、系统配置及环境参数等甲方可直接控制的系统和资源；

2.1.3 乙方负责：甲方使用的云平台资源及运行该平台所需的双方约定的服务。

2.2 工作内容

2.2.1 业务导入

(1) 业务导入内容：根据甲方需求，乙方为甲方准备的、甲方业务所需的云平台资源，包括相关的物理环境、基础设施、硬件资源及线路连接、网络安全配置等；

(2) 业务导入时间及时长：甲乙双方在合同或订单中约定具体的业务导入时间、导入所需时长（所需时长与甲方所需云平台资源规模量相关）；

(3) 业务导入工作内容列表：

工作内容列表	乙方	甲方
提供详细云平台资源需求、数据信息	协助	主责
针对导入需求，对云平台资源规划、初始化部署、调试	主责	协助
互联网和/或专线网络连接及网络安全配置调试	主责	主责

2.2.2 虚拟服务器状态管理

(1) 该服务由乙方提供，并根据甲方需求（合同或订单中约定），对虚拟服务器状态进行操作。该服务请求，甲方需提前3个工作日以书面形式通知乙方；

(2) 乙方可提供的服务操作：创建、启动、停止、变更、重启虚拟服务器；

(3) 虚拟服务器状态管理工作内容及责任：

工作内容列表	乙方	甲方
提出虚拟服务器状态操作要求	协助	主责
确定虚拟服务器状态操作时间	主责	协助
进行虚拟服务器状态操作	主责	协助
虚拟服务器状态确认（创建/启动虚拟服务器时）	协助	主责

2.2.3 虚拟服务器系统初始化

(1) 甲方工作内容：甲方需提供与其自身环境相适应的配置要求及必要的操作系统介质和授权（如Windows操作系统授权），以便乙方初始化配置虚拟服务器；

(2) 乙方工作内容：乙方使用甲方提供的操作系统安装介质和授权，进行虚拟服务器操作系统初始化安装，并向甲方提供操作系统最高权限客户（如root、administrator）的登录信息，包括客户名及密码。以上服务请求，甲方需提前3个工作日以书面形式通知乙方；

(3) 虚拟服务器系统初始化工作内容及责任:

工作内容列表	乙方	甲方
提出操作系统初始化安装请求、提供合法操作系统安装软件和授权	协助	主责
操作系统初始化安装	主责	协助
虚拟服务器网络配置初始化（IP 地址设置等）	主责	协助
提供系统最高权限客户（如 root、administrator）登录信息	主责	协助
确认虚拟服务器符合合同/订单约定（登录虚服务器操作系统）	协助	主责

2.2.4 资源变更

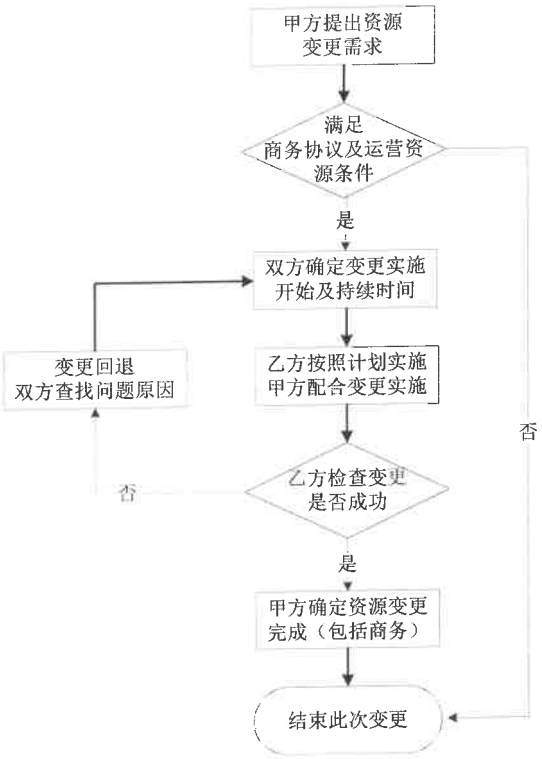
(1) 资源变更请求及确认步骤：

- 甲方需提前3个工作日提出书面的资源变更请求，并提供所需虚拟服务器的配置（包括IP地址，如需要）及变更时间等信息；
- 乙方在确认甲方的资源变更请求及变更时间后，以书面方式告知甲方变更风险；
- 获得甲方书面同意后，乙方按照甲方提供的虚拟服务器配置信息执行操作。

(2) 资源变更工作内容及责任:

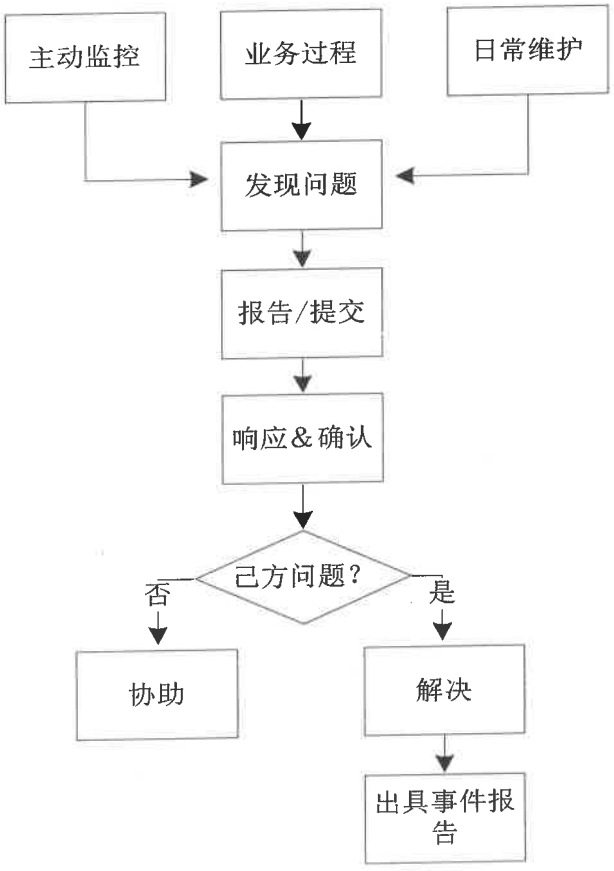
工作内容列表	乙方	甲方
提出虚拟服务器资源变更要求及相关信息	协助	主责
另行签订新的服务合同或订单（根据需要）	主责	主责
确定资源变更所需操作时间	主责	协助
进行资源变更操作	主责	协助
虚拟服务器操作	主责	协助
虚拟服务器变更确认	协助	主责

(3)资源变更流程



2.2.5 运维服务及流程

乙方为甲方提供的云平台资源及运维服务内容及流程如下图：



2.2.6 人工支持

(1) 人工支持服务内容：受理甲方使用云平台资源问题咨询、服务请求、甲方报告的事件及问题；

(2) 双方联络信息（信息如有变更，以书面方式通知对方）：

内容	甲方	乙方
服务交付经理电话		
服务邮箱		
交付经理工作时间		工作日 5x8 小时
24 小时服务电话		027-83383805

(3) 人工支持工作内容：

工作内容	乙方	甲方
配备客户服务人员，提供人工支持服务	主责	协助
开放服务邮箱用于受理邮件服务请求或问题咨询	主责	
建立常见问题列表	主责	
对客户来电咨询的相关业务功能及使用问题解答	主责	协助
接到故障报告或告警时转派事件工单至相应技术支持工程师解决	主责	
清晰描述相关的问题及服务请求	协助	主责
查看相关通知，获得云平台维护信息或其他提示信息	协助	主责

2.2.7 资源监控

(1) 监控的目的

- 预防故障：定期查看甲方使用资源的状态信息，根据告警或提醒信息，及时调整操作，减少故障发生几率，降低故障影响和损失；
- 发现故障：定期查看甲方使用资源的运行状况，及时发现异常，并进行第一时间的现场保护，如确认故障、启动故障处理流程；
- 甲方使用服务资源内容变更的跟踪与验证：跟踪内容变更计划，定时通知相关方有关变更进度与状态，变更完成后，进行变更验证。

(2) 监控方式、监控时段、故障预警及处理

- 乙方在独立、安全的监控室，对甲方使用的云平台资源及相关支撑环境进行集中监控；
- 当监控项目出现故障、异常时，乙方按照服务级别通知甲方，经甲方同意后，采取相关措施解决或配合甲方的协助要求。根据甲方需求，对所使用的虚拟服

务器进行重启，应提前通知乙方，提前通知的时间应该不少于一个小时。

(3)监控项目及指标

监控项目	指标	备注
监控对象	CPU、负载、节点状态、磁盘空间、网络流量	
监控范围	虚拟服务器及云平台资源	
监控信息刷新频率	每 5 分钟 1 次	
告警通知形式	电话、邮件	虚拟服务器节点状态为宕机状态时，监控人员以电话及邮件的形式通知系统相关的技术支持人员

(4)实现主动监控的技术要求

甲方需确保虚拟服务器操作系统中 SNMP 服务正常运行，且 161 端口可被正常监测。

(5)主动监控工作内容

工作内容	乙方	甲方
配备监控室场地及相应监控服务的设施资源	主责	
安排人员对甲方使用的云平台资源及虚拟服务器相关支撑环境进行监控	主责	
当监控系统报警时，在工单系统中创建事件、问题记录工单	主责	
通知相应的技术支持人员及甲方相关人员主责故障排查	主责	协助
确定故障原因，并解决事件及问题或提供协助	主责	主责
根据变更情况，适时调整监控的内容和范围	主责	协助
甲方因业务需要对使用的虚拟服务器执行操作，需提前通知乙方	协助	主责
甲方指定故障或异常通知的接口人、通知方式及处理方式		主责

2.2.8 技术支持服务

(1)目的

根据主动监控、日常维护或甲方报告等信息，乙方做出的排除影响甲方正常使用云平台资源的因素、处理甲方提出的服务要求。

(2)工作流程

当乙方接到甲方使用的云平台资源发生故障信息时，将安排相应的技术支持工程师解决故障问题，并于服务指标承诺的响应及解决时限内，解决故障、恢复服务。

(3)工作内容

工作内容	乙方	甲方

明确描述事件、问题、需要协助内容、功能故障、错误代码	协助	主责
明确客户的问题、需求及需要帮助内容，协调资源予以解决或满足	主责	协助
排除影响或可能影响虚拟服务器运行所需云平台资源可用性的因素，响应业务请求、排查故障、恢复业务	主责	协助
在故障解决及疑问解答过程中，提供必要的配合，如问题或故障的重现等	协助	主责
详细记录事件过程及解决方案，出具紧急严重事件报告（紧急及严重情况发生后的 3 个工作日内）	主责	协助

2.2.9 日常维护

(1) 目的

乙方根据甲方使用的云平台资源及相关支撑环境资源（用于支撑云平台资源）中各项指标和运行周期以及主动监控或甲方报告等信息，对甲方使用云平台资源及相关支撑环境资源进行周期性或事务性的检查调校，排除可能影响甲方使用云平台资源可用性的因素，包括根据甲方的服务要求进行的测试、验证、信息采集等事务型工作。

(2) 维护的原则

维护的时间段将选定在甲方非业务时间或业务量较小的时段进行，具体时间由乙方与甲方根据需求确定。

(3) 维护方式、类型、流程

- 计划性维护中断：在维护时段内，乙方将对中金云资源及支撑环境资源进行周期性维护，如预计进行的维护操作将影响甲方使用的虚拟服务器、中金云资源及支撑环境资源的正常运行并产生中断，即计划中断，则乙方将在维护具体时间确定后至少3个工作日前预先通知甲方；
- 云平台系统补丁或版本升级 ：针对云平台必须的系统补丁或版本升级，乙方应在保证甲方业务正常运行及数据安全的前提下进行；
- 其它计划中断：甲乙双方通过书面确定的，影响甲方使用的虚拟服务器云平台资源正常运行的中断，都属于计划中断。

日常维护服务根据确定的日常维护作业计划，定时收集资源及环境的各类信息，检查资源及环境运行状态，对发现或受理的问题进行预防性的维护作业，消除故障隐患；根据不同时期的不同要求，日常维护作业计划具体内容项目可以定期或不定期的调整；日常维护作业由乙方服务技术支持工程师按作业计划执行，并记录执行结果。对于日常维护作业中发现的故障将启动故障处理流程；日常系统维护记录及明细不作为是乙方工作流程、管理所需，不对甲方以交付物形式提交。如甲方有监管部门审计

需要，乙方会配合完成有关材料的出示。

(4)日常维护工作内容

工作内容	频率	甲方	乙方
机房巡检，查看云平台资源及相关支撑环境（物理服务器、物理环境及网络设备工作等）	每日 1 次		主责
云平台资源健康检查（人工）	每周 1 次		主责
制定维护作业计划	按需	协助	主责
按照维护作业计划进行相关维护性工作（维护时段）	按需	协助	主责
问题记录与处理，启动问题管理流程	按需	协助	主责

2.2.10 月度服务报告

(1) 月度服务报告的时限及要求

乙方在每月服务期满后，生成服务分析评估报告（以下简称服务报告），并于下一自然月前 5 个工作日内交付给甲方。服务报告中包含上一月度的资源及服务运行情况，受理的客户故障申报和服务请求数量等。

(2) 报告内容

针对甲方云主机及相关资源的运行情况，乙方每个自然月向甲方提供一份运行报告；运行报告的内容与格式，由甲方、乙方协商制定。

月度服务报告指标名称	指标	备注
客户联系信息	包含	
本月云平台资源可用率	包含	
本月事件工单数量	包含	
本月工单解决率	包含	
本月累积故障时间	包含	

(3) 工作内容

工作内容	乙方	甲方
统计故障次数、服务请求数量、中金武汉云运行状况	主责	
生成月度服务报告	主责	
指定联系人接收服务报告		主责
对上一服务周期进行服务质量确认并提出改进建议		主责

3. 服务水平级别（SLA）

3.1 原则

3.1.1 目的

为保证可持续的提供稳定优质的服务，乙方明确对甲方使用的云平台资源及支撑环境资源服务级别及服务承诺指标；

3.2.1 服务指标不超过乙方服务能力，同时满足甲方业务需求。

3.2 服务项目指标

乙方承诺为甲方提供的云平台资源服务将达到、且甲方接受以下所约定的服务水平：

服务项目	类别	方式	指标	备注
虚拟服务器云平台资源及服务运行时间			7×24 小时	
定期监控频率			5 分钟	
云平台资源可用性			99.95%/月	
紧急、严重情况响应时间	工作时段	电话	<15 分钟	遇忙线<30 分钟
		邮件	<30 分钟	紧急邮件
	非工作时段	电话	<60 分钟	
		邮件	<4 小时	
非紧急、严重情况响应时间	工作时段	电话	<2 小时	
		邮件	<4 小时	
	非工作时段	邮件	<24 小时	
紧急、严重情况解决时间	工作时段	电话	<3 小时	
		邮件		紧急邮件
	非工作时段	电话	<5 小时	
		邮件		紧急邮件
非紧急、严重情况解决时间（服务请求）		电话	<72 小时（工作日）	
		邮件		
月度服务报告			每月初前 5 个工作日内发送上一月度报告	

附：月度服务报告模板

客户基本信息	客户名称：					
	客户联系人：					
	联系电话：					
	邮件地址：					
主机信息	主机列表	IP	操作系统	备注	非计划 中断时间（min）	可用率
服务月						
当月服务天数						
服务统计周期						
服务时间						
服务请求	工单号	说明				
事件	工单号	说明				
		描述：		原因：		

4.信息安全保障

4.1 总体目标

中金云设计以高安全性、高可用性为基本原则，为客户提供安全、可靠、高效的云服务。

4.2 云安全保障

4.2.1 云计算物理区域安全保障

- 为客户提供服务的云计算机房按照国家A级机房等级建造，机房内部设有安全的保障系统，7×24小时专业技术人员监管，全年365天不间断闭路电视监控系统。采用智能UPS、双路市电，为机房提供不间断电源冗余设置，另外备有柴油发电机，确保机房的供电保障。
- 武汉超算中心园区周界通过围栏与外界安全隔离，整个安全防范体系采用分级别、分区域的整体纵深防范体系。
- 闭路电视监控系统
- 园区周界、楼宇的所有通道和出入口以及客户机房的重点部位，均布置有7×24小时闭路电视监控点，实现对现场人员活动情况的实时监控。
- 武汉城市云所在机房内布置有无死角的闭路电视监控系统，可全天候7×24小时实时监控并记录现场情况，视频数据可保留3个月以上。
- 门禁系统
- 武汉超算中心安全管制区域均设置门禁系统，所有授权人员均须凭IC卡和指纹出入。
- 集中式安全监控中心
- 闭路电视监控系统、门禁系统、入侵探测报警系统将集中连接到设施环境监控中心，由设施环境监控中心的7×24小时值班人员进行实时监控，可及时发现安全隐患并响应处理，保障客户生产环境机房的物理环境安全。

4.2.2 武汉城市云安全保障

- 采用独立的物理设备，并对环境进行了隔离及管理，与其他项目在物理上完全隔离。
- 系统权限分离，并保证相关人员的权限仅为工作需要的最小化权限。
- 独立的网络、运营支撑平台及工具，保证在逻辑上的独立与隔离。
- 严格的操作流程和访问控制，只有专门人员经过特殊的授权才可以进入中金高

等级数据中心进行环境初始化和系统部署的相关操作，且有物理监控记录及访问记录。

- 对主要设备进行监控，除对虚拟系统环境和物理系统环境进行监控外，也对主要的网络设备进行监控，设定相关的策略与阈值，并对相关的异常情况及时进行处理。
- 拒绝服务是另一种攻击形式。通过对网络带宽进行消耗、消耗服务器缓冲区、IP欺骗迫使合法客户连接复位等，都是拒绝服务攻击的常见形式。武汉城市云后台采用专线连接，屏蔽了非客户连接的可能性。
- 武汉城市云后台所有网络设备的日常维护及管理，都需通过本地操作终端设备进行连接，telnet及其他远程连接服务及端口均已关闭，防止非法接入。
- 定期对环境进行安全检查，主要针对物理环境、设备和网络配置情况。
- 统一的管理操作接口，并采用了堡垒机工具进行管理，对所有操作进行记录。

4.2.3 安全管理

- 武汉超算中心将负责中心机房的安全管理工作，确保武汉城市云所在机房的物理环境安全。
- 严格遵守双方约定的保密条款。
- 建立和维护相关安全管理制度，并定期对安全管理制度的执行情况进行检查审核，确认所有安全管理制度都得到了贯彻执行。
- 7×24小时人员、设备物品进出安全管理。
- 配备闭路电视监控系统，7×24小时实时监控机房内安全状况。
- 负责安保门禁系统的建设、日常运行管理和维护工作。
- 实行严格的人员、设备进出管理制度。

4.2.4 运行安全保障

- 双方将签订相关安全保密协议，并严格遵守，确保服务过程的信息安全。
- 乙方将严格执行安全保密制度，确保甲方在乙方的信息不会外泄。
- 乙方将对参与甲方信息系统运维服务（尤其是外包人员）的人员进行信息安全培训，增强相关人员的信息安全意识。

附件二：

中金云平台资源服务订单

项目名称：2026年武汉市东西湖区交易中心数据存储服务

项目编号：HBCZ-2503051708-254293　　所投包号：1

云存储服务明细表						
一、云资源服务						
1.云主机						
序号	服务项目	服务说明	计费单位	数量	单价（元）	合计（元）
1	云主机	2核vCPU、8GB内存、40G系统盘	台/年	2	3,990.00	7,980.00
2	云主机	8核vCPU、16GB内存、40G系统盘	台/年	8	13,300.00	106,400.00
合计（元/年）						114,380.00
2.云存储						
序号	服务项目	服务说明	计费单位	数量	单价（元）	合计（元）
1	云硬盘	每1GB高速云硬盘	GB/年	34,200	5.1	174,420.00
合计（元/年）						174,420.00
3.网络通信						

序号	服务项目	服务说明	计费单位	数量	单价（元）	合计（元）
1	电子政务外网带宽	100Mbps 单线电子政务外网带宽含 2 个政务外网 IP	1Mb/年	100	0.00	0.00
2	互联网带宽	独享单线互`联网带宽（最小开通带宽为 1Mb，计数单位为 1Mb）	1Mb/年	200	280.00	56,000.00
3	公网 IP 地址	公网 IP 地址（最小订购为 1 个，计数单位为 1 个）	每个/年	2	780.00	1,560.00
合计（元/年）						57,560.00

4. 云安全服务

序号	服务项目	服务说明	计费单位	数量	单价（元）	合计（元）
1	堡垒机	针对云上运维安全的管控，本服务提供： 1、运维账号集中管控服务，实现对所有被运维的 IT 资产账号的集中管理和监控；2、运维身份强制认证，支持双因素认证，对运维人员提供统一的访问入口及强制的身份验证机制；3、统一资源授权，提供运维人与设备对应关系，最大限度保护用户资源的安全；4、集中访问控制，支持命令集细粒度的权限控制，减少误操作导致系统受到破坏；5、集中操作审计，对运维人员操作集中审计，出现问题能快速定位并进行准确溯源；6、会话场景全程回放，提供视频回放的审计界面，以真实、直观、可视的方式重现操作过程；按管控的 IP 数量计费，每 5 个 IP 管控对象为 1 个计费单位，采用包年计费。	5 个 IP/年	2	9,500.00	19,000.00

2	入侵防御服务	通过建立主机和服务器的行为数据模型进行异常行为检测，支持对底层的ARP 攻击、网络攻击、20 多种常见协议的异常、病毒蠕虫木马、恶意 URL 等一系列入侵威胁进行检测及防御。按接入 IP 数量采用包年计费。	每 IP/年	2	4,750.00	9,500.00
3	网络防火墙	提供云平台基础防火墙，对云平台东西向、南北向网络进行防护。	每 IP/年	1	7,600.00	7,600.00
4	VPN 接入	10Mbps 专用 VPN 接入互联网带宽	条/年	1	11,400.00	11,400.00
5	漏洞扫描服务	全方位检测系统存在的脆弱性，包括：操作系统、数据库、中间件、Web 应用等，发现系统存在的安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，对系统中多个方面的安全脆弱性统一进行分析和风险评估，形成整体安全风险报告。按 IP 数量计费，每 5 个 IP 对象为 1 个计费单位，采用包年计费，每月提供一份安全评估报告（电子版）。	5 个 IP/年	2	7,125.00	14,250.00
6	日志审计	日志审计服务内容包括： 1、将安全系统、主机操作系统、数据库等系统的日志、事件、告警汇集起来，实现对安全信息（日志）进行统一监控。 2、基于安全监测、告警和响应技术的事件关联分析引擎。在关联规则的驱动下，事件关联分析引擎能够进行多种方式的事件关联。 3、对日志进行全面分析与审计，集成各种合规性关键控制点需求，为用户提供合规性审计报表报告	每主机/年	10	779.00	7,790.00
7	云主机防病毒服务	结合云查杀引擎、脚本查杀引擎、启发式查杀引擎、人工智能查杀引擎、系统修复引擎、主动防御技术，有效查杀已知和未知病毒	每主机/年	10	1,140.00	11,400.00

8	云主机系统安全防护	包含以下功能： 1、防病毒，通过云主机安全代理软件，有效查杀主机上的文件、内存、进程中的恶意程序； 2、WebShell 防护，包含了 40 万以上的网站后门样本和大量的后门特征码，双重机制保证对于样本的有效检测与查杀； 3、防暴力破解，可以有效防御远程桌面和 SSH 登录的暴力破解，保障主机的安全； 4、主机入侵防御，可实现主机的入侵防御功能，包括防御新型漏洞、病毒攻击，阻拦可疑的行为等； 5、网卡流量统计，可查看各个云主机网卡的流量情况，实现各主机流量的统一管理查看。	每主机/年	10	1,710.00	17,100.00
9	Web 应用防火墙	对 Web 的业务流量进行恶意特征识别及防护，提供 Web 服务器漏洞防护、Web 插件漏洞防护、爬虫防护、跨站脚本防护、SQL 注入防护、LDAP 注入防护、SSI 指令防护、XPATH 注入防护、命令行注入防护、路径穿越防护、远程文件包含防护等服务，将正常、安全的流量回源到服务器,避免网站服务器被恶意入侵，保障业务的核心数据安全。按实例数量采用包年计费。	每实例/年	2	15,200.00	30,400.00
10	网页篡改在线防护	实时过滤 HTTP 请求中混杂的网页篡改攻击流量（如 SQL 注入、XSS 等），监控网站所有需保护页面的完整性，采用文件级驱动保护技术，用户每次访问每个受保护网页时，Web 服务器在发送之前都进行完整性检查，保证网页的真实性，当检测到网页被篡改时，第一时间发出告警信息，对外仍显示篡改前的正常页面。按实例数量采用包年计费。	每实例/年	1	12,350.00	12,350.00

11	域名证书 ssl	网站安装 SSL 证书后，使用 https 加密协议访问网站，可激活客户端浏览器到网站服务器之间的"SSL 加密通道"(SSL 协议)，实现高强度双向加密传输，防止传输数据被泄露或篡改。	个/年	1	2,000.00	2,000.00
合计（元/年）						142,790.00
费用总计（元/年）：						489,150.00
服务地点：武汉市东西湖区公共资源交易中心						

附件三：

《中金云平台客户入网安全责任书》

通过中金数据（武汉）超算技术有限公司(以下简称“超算公司”)互联网数据中心接入互联网的客户必须认真阅读及签署《中金云平台客户入网安全责任书》(以下简称“责任书”)，并自觉遵守各项规定。

为了保证客户的合法利益，确保接入的业务不影响园区数据中心网络的运行安全，依据《中华人民共和国计算机信息系统安全保护条例》、《计算机信息系统国际互联网保密管理规定》、《计算机信息网络国际联网安全保护管理办法》、《最高人民法院、最高人民检察院关于办理利用互联网、移动通讯终端、声讯台制作、复制、出版、贩卖、传播淫秽电子信息刑事案件具体应用法律若干问题的解释（二)》等规定，特制定本责任书。

一、为了保证信息安全，客户应遵守国家有关法律、法规和行政规章：

1. 客户不得播放违反国家法律的政治性新闻（包括从 INTERNET 上下载的信息内容)；

2. 客户不得利用互联网从事危害国家安全、泄露国家秘密等犯罪活动；

3. 客户不得利用互联网查阅、复制和传播危害国家安全、妨碍社会治安和淫秽黄色的信息；

4. 在 INTERNET 上播放的信息内容是经当地宣传管理部门批准的内容；不得擅自下载境外 INTERNET 的信息在国内站址上发布；

5. 要对执行信息内容管理制度组织自查，发现问题立即处理，切实落实信息安全责任制，并加强从事信息管理工作人员的教育检查工作。

二、客户保证具备从事互联网服务的全部合法必要的资质条件，其中：

1. 客户如从事电子公告、新闻、出版、教育、医疗保健、药品和医疗器械、文化、广播电影电视节目等特殊互联网信息服务，应当根据法律、行政法规以及国家有关规定经有关主管部门审核同意，履行批准或备案手续，并取得相关通信管理部门批准或备案文件。

2. 客户如从事非经营性互联网信息服务，保证已首先登录工业和信息化部备案管理系统履行互联网备案手续，并按期履行年度审核手续。如当地通信管理部门要求履行非经营性互联网信息服务备案手续的，还应向其住所所在地通信管理部门履行非经营性互联网信息服务备案手续。

3. 客户如从事经营性互联网服务，必须取得相应的增值电信业务经营许可证。

4. 客户如从事经营性互联网服务，应当在其网站主页的显著位置标明其经营许可证编号；客户如从事非经营性互联网服务，客户网站开通时在主页底部的中央位置标明其备案编号，并在备案编号下方链接工业和信息化部备案管理系统网址，供公众查询核对，客户还需按照工业和信息化部备案管理系统的要求，将备案电子验证标识放置在其网站的指定目录下。

5. 客户保证已履行其他法律、法规及部门规章所规定的手续或已取得有关资质证明文件。

三、为了保证网络安全，维护所有数据中心客户的利益，保证系统运行正常， 数据中心客户须遵守以下规定：

1. 甲方有义务按照乙方的要求提供网络使用情况(如 IP 地址、域名等)，填写乙方要求提供的 资料，接受主管部门的检查；

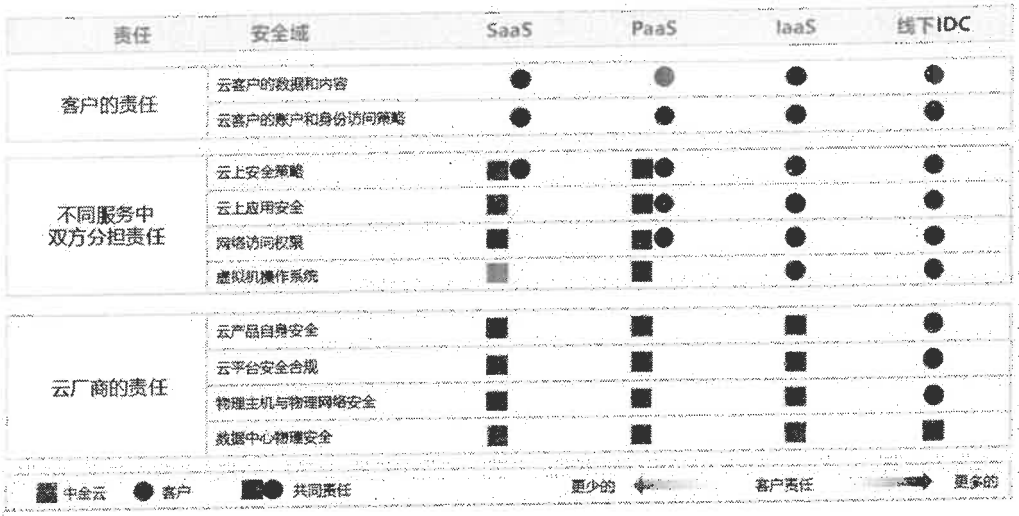
2. 对于由乙方分配的 IP 地址，甲方只有使用权，不可转让他人使用，业务终止时 IP 地址使用权自动取消。甲方有义务接受乙方对 IP 地址的监管及使用情况的调查，如果甲方提供虚假资料，乙方有权处理直至收回所分配的 IP 地址；严禁盗用他人 IP 地址；

3. 除提供正常服务外，严禁使用一切手段从事危害网络运行和侵犯其他客户利益的黑客行为。

4. 甲方在使用互联网业务时，应遵守互联网的国际惯例，不得向他人发送恶意的、挑衅性的文件和商业广告，包括垃圾邮件、垃圾信息等；不得向任何网络发动任何形式的攻击。 对于违反上述规定的客户，将接受相关部门规定处罚；同时，乙方将中断甲方的网络服务。甲方应积极配合国家主管部门和乙方进行网络安全事件的跟踪，并提供相关的、合法的资料。

四、云服务安全责任说明

基于超算公司客户的应用系统，其安全责任由双方共同承担：超算公司要保障云平台自身安全并提供安全产品和能力给云上客户，客户负责基于超算公司云服务构建的应用系统的安全。安全责任模型示意如下图所示：



超算公司负责物理基础设施（包括数据中心环境安全、数据中心运营安全、容灾）和物理设备（包括计算、存储和网络设备）的物理和硬件安全，并负责运行在超算公司城市云平台之上的云主机和云产品的安全。同时，超算公司负责平台侧的身份管理、访问控制、监控及运营，从而为客户提供安全可靠云主机和云产品服务。

客户负责以安全的方式配置和使用各种云上产品，并基于这些云产品的安全能力以安全可控的方式构建自己的云上应用和业务，确保云上安全。

五、如客户违反上述内容，超算公司有权拒绝或停止提供服务或设施，并要求客户在限期内改正。如客户在限期内未改正的，超算公司有权终止双方间服务合同，并不承担任何责任；客户存在前述情形给超算公司造成损失的，并应当予以赔偿。

六、以下所列内容是关于客户入网安全问题的基本建议，客户应根据实际使用情况，采取必要的安全防范措施，确保云上网络安全。

1、数据和内容的安全维护

客户应维护其存储在云服务平台上的所有数据和内容的安全。客户需采取必要的加密、备份、访问控制等措施，以防止数据泄露、篡改或丢失。

2、账户和身份访问策略

客户应为其云账户和访问身份实施严格的访问控制策略，包括但不限于设置强密码、多因素身份认证、定期更换密码等措施。

3、云主机的安全策略

客户应对其使用的云主机实施并维护必要的安全策略，包括但不限于安装防病毒软件，对每次下载文件、拷贝文件都进行病毒查杀；定期更新补丁、配置主机防火墙和入侵检测系统、关闭非必要端口及高危端口。

4、应用程序的安全维护

客户负责维护其在云服务中部署的应用程序的安全，包括代码漏洞修复、权限管理、漏洞扫描等。建议应用系统重要目录或文件非必要不对外开放、或增加鉴权。拥有写入权限的目录请增加检查过滤，以免恶意脚本或命令执行。

5、网络访问控制策略

客户应对其所使用的网络访问权限进行严格控制，确保仅有授权的人员和系统能够访问其云资源。

6、虚拟机操作系统的维护

客户应定期更新其云主机中的虚拟机操作系统，安装必要的安全补丁，并确保系统配置符合安全最佳实践。

7. 安全事件的相应和处理：

安全管理员发送的邮件告警事件请及时检查并修复漏洞。如出现主机失陷情况，请积极配合断网处置，以免影响扩大。

8. 数据库的安全维护：

客户应加强数据库的访问控制、身份验证、数据加密、定期审计、备份与恢复、及时更新补丁、防火墙和监控工具等，以确保数据的机密性、完整性和可用性

9. 客户必须同意遵守《中国人民共和国保密法》、《计算机信息系统国际联网保密管理规定》、《中华人民共和国计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》、《中华人民共和国计算机信息网络国际联网管理暂行规定》及其实施办法等相关法律法规的任何及所有的规定。

10. 根据公安局网监分局的要求，互联网客户应在入网后 5 个工作日内在网上提交备案信息，提交信息后 10 个工作日内到[所属地市]公安局网监分局办理备案业务，相关法律法规、备案流程、备案材料清单请查阅网站“常见问题”栏目或者向超算公司咨询。

七、客户的各级主管人员有责任教育、监督客户职工严格遵守上述条款。

我单位同意遵守《中金云平台客户入网安全责任书》中的各项规定，如违反规定，愿意依据相关法律规定以及本文件的有关规定承担相应责任。

单位名称（盖章）：

日期：2026 年 1 月 20 日

附件四：

服务质量综合评审表

项目名称：2026年武汉市东西湖区交易中心数据存储服务

项目编号：HBCZ-2503051708-254293　　所投包号：1

服务类别	考核条款	评审内容	分值	评审标准	评审得分	备注
维护能力（30分）	平台维护	虚拟化平台、云资源管理平台、运维管理平台、网管平台等管理。	15	1、虚拟化平台、云资源管理平台、运维管理平台、网管平台等部署合理、配置正确、运转正常（10分），每平台不能正常配置运转1次扣0.2分；		
				2、实现7*24小时监控，保证平台安全、防攻击、问题处理及时（5分），未做到7*24小时监控发现1次扣0.2分，问题处理不及时1次扣0.2分；		
	网络可用性	保证网络畅通可用。	15	1、因自身原因造成网络故障，4小时内修复的不扣分；超过4小时不到8小时修复的扣0.5分；以后每延后2小时修复的加扣		

				0.5 分；		
服务质量（30 分）	服务标准化、规范化	提供规范详实的服务目录、资源列表、流程。	3	1、服务期内供应商需提供服务目录、资源列表、流程（5 分），未提供扣 5 分。		
	资源虚拟化	按项目要求实现服务器虚拟化、存储虚拟化，并能动态调配资源。	15	1、按项目要求提供虚拟化资源，否则扣 1 分；		
				2、未实时监控并根据需要动态调配资源，造成服务中断后 3 小时之内修复的不扣分，超过 3 小时不到 5 小时修复的扣 0.5 分，每延后 2 小时加扣 0.5 分；出现资源报警 8 小时内未妥善处置，但未造成服务中断的 1 次扣 0.5 分。		
	故障管理	主要包括：故障时间、故障影响、故障上报、故障原因、恢复时间、处置方法、故障分析总结报告、报警管理等。	12	1、故障发生后 30 分钟内未上报采购人，1 次扣 0.2 分；		
				2、故障瞒报漏报未计入台帐的，1 次扣 0.5 分；		
				3、故障台帐记录不详细、故障分析总结报告不准确的，1 条扣 0.2 分。		
服务满意	业务开通	响应速度、技术咨	15	1、响应速度实现 6 小时内联系、3 日内开通的（8 分），未满足 1		

度(40分)		询、资源配置、服务态度等。		次扣0.2分；		
				2、技术咨询积极、专业（2分），否则酌情扣分；		
				3、资源配置合理符合要求(5分)，不符合的1次扣0.2分，但通过电话、邮件汇报并同意的除外。		
	投诉	考核期内投诉情况。	20	1、口头、电话等投诉1次扣0.5分，书面投诉1次扣1分；		
	事中服务	用户应用系统重要事件和故障第一时间通知用户并配合解决。	5	1、主动发现并告知客户系统问题（2分），未主动发现与告知1次扣0.1分；		
				2、配合解决问题（2分），未配合或不积极1次扣0.1分；		
				3、问题记录整理（1分），未记录1次扣0.1分。		
评审总分						
因乙方责任导致： 1、发生采购人的数据丢失事件； 2、发生采购人的数据被云中心或第三方获取外泄事件； **直接评为0分。**						

（以下无正文）