合同编号：KSY20240516 0003
JDSHT2024014

2024年北京市卫生健康监督所
卫生监督信息化运维项目-政务云扩展服务项目合同

甲方：北京市卫生健康监督所

乙方：北京金山云网络技术有限公司

合 同 书

2024年卫生监督信息化运维项目硬件运维服务采购项目(项目名称)中所需政务云扩展服务(服务名称)经华诚博远工程咨询有限公司（代理机构）以11000024210200081439-XM001/06号招标文件，进行国内公开招标。经评标委员会评定北京金山云网络技术有限公司(乙方名称)为中标人。依据《民法典》、《中华人民共和国政府采购法》规定，甲方与乙方协商一致，同意按照下列条款，签订本合同书。

1、合同文件

下列文件构成本合同的组成部分，应当认为是一个整体，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：

a.本合同书

b.中标通知书（附件1）

c.合同条款

d.投标文件(含澄清文件)

e.招标文件其他内容（含招标文件补充通知）

2、服务内容

北京市卫生监督执法综合管理平台为等保三级系统，为达到网络安全等级保护三级的要求，需完成云端APT防护服务、网络防病毒服务、杀毒软件、漏洞扫描、

网页防篡改和安全加固等内容，具体如下：

基础软件支撑服务：商用操作系统套餐，Windows Server 套餐：Windows Server 租用、安装及维护；

基础软件支撑服务：开源操作系统套餐，提供开源操作系统安装和维护服务；

云端 APT 防护服务，对未知攻击威胁进行检测和防护，发现隐蔽威胁、木马后门等异常威胁；

网络防病毒服务，通过云平台网络内部部署网络防病毒服务，实现对网络边界病毒防护及网络内部流量监控，保障系统安全；

主机杀毒软件，需要采用云环境的专业防病毒软件，实现与云服务商使用的云平台对接，在不消耗虚拟机资源的情况下，对虚拟化环境进行有效的病毒防护和查杀；

主机漏洞扫描，在特殊时期（例如国庆、两会期间）提供 7*24 专人现场值守服务，提供网络信息系统安全运行监控、配置信息系统安全访问策略、及时响应信息系统故障并协助处置、排除网络信息系统安全隐患、重大信息安全事件的应急响应等服务内容，承担网络信息系统安全运行的现场技术保障；

主机安全加固，结合漏洞扫描检测结果和结论，根据安全基线要求，及时消除系统中所存在的技术性安全问题，降低恶意攻击者利用安全漏洞威胁系统安全运行的几率，从而有效控制因各种潜在安全威胁引发的业务中断及信息外泄等风险，将高风险漏洞和中风险漏洞降低至可接受的范围内，使得整个网络、应用系统的安全状况提升到一个较高的水平；

网页防篡改，通过统一网页防篡改资源池对各系统静态发布页面进行防护，防止页面被恶意篡改；

数据库审计服务，实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断；

主机日志分析，针对操作系统进行日志收集，用于了解主机安全情况及资源使用情况；

其他必要服务，按照网络安全等级保护要求、网络安全专项检查要求等，配合完成网络安全保护工作，确保各系统安全稳定运行，不发生网络安全案事件。

具体内容详见本合同附件（附件 2：服务内容及分项报价表）

3、合同总价

本合同总价：人民币（大写）陆拾柒万肆仟柒佰贰拾元整（￥674720.00）。

分项价格详见本合同附件（附件 2：服务内容及分项报价表）。

4、付款方式

1、自合同签订之日起 20 日内，甲方向乙方支付合同金额 50%首付款（人民币）叁拾叁万柒仟叁佰陆拾元整（￥337360.00）。甲方在 2024 年第三季度末前支付乙方合同金额 20%中期款（人民币）壹拾叁万肆仟玖佰肆拾肆元整（￥134944.00）。甲方在完成本单位 2025 年财政资金预算批复后 30 个工作日内支付合同金额 30%尾款（人民币）贰拾万贰仟肆佰壹拾陆元整（￥202416.00）。乙方应在甲方每次付款前给甲方开具符合国家规定的相应金额的正式发票。

2、甲方不应当支付除委托报酬以外的任何其它费用，乙方也不得要求改变报酬总额。

3、乙方应当对本项目的收支情况进行单独核算，以配合财政部门的延伸审计。

4、乙方指定帐户及联系方式情况如下：

账户名称： 北京金山云网络技术有限公司

账号：0110012830003054

行号：民生银行北京上地支行

纳税人识别号：9111010857121431XA

联系人： 王夏楠

联系电话：13811110522

5、乙方在收到甲方第一笔金额为合同总价 50%的资金 30 日内，需向甲方提供由乙方开户行开具的金额为合同总价 5%的不可撤销的履约保函；履约保函的有效期限至 2025 年 5 月 23 日，甲方在合同期结束并验收合格后 15 个工作日内退还乙方履约保函或履约保证金。

5、服务期限

服务期限：2024 年 05 月 24 日至 2025 年 05 月 23 日

6、合同的生效

本合同经双方各自的授权代表签署、加盖单位公章或合同专用章之日起生效。

甲方：北京市卫生健康监督所

名称：（印章）

法人代表授权人（签字）：

联系人：李志

电话：010-83366838

地址：北京市西城区赵登禹路 277 号

邮政编码：100034

签订日期：2024年 5 月20 日

签订地点：北京市

乙方：北京金山云网络技术有限公司

名称：（印章）

法人代表授权人（签字）：

联系人：王夏楠

电话：010-6292 7777

地址：北京市海淀区小米科技园 D 栋

邮政编码：100083

开户银行：民生银行北京上地支行

帐号：0110012830003054

开户银行：民生银行北京上地支行

帐号：0110012830003054

合同条款

委托人（甲方）：北京市卫生健康监督所

受托人（乙方）： 北京金山云网络技术有限公司

第一条 释义

甲方：指政务云使用单位，即签署本合同的北京市卫生健康监督所；

乙方：指北京市市级政务云平台的云租赁服务供应商，也称云租赁服务商,即签署本合同的北京金山云网络技术有限公司。

第二条 政务云租赁服务事项及内容

1.本合同有效期内，乙方为甲方单位提供如下政务云租赁服务：

1.1 具体内容详见本合同附件（附件 2）。

2.技术支持服务要求：

2.1 响应时间

乙方应提供 7*24 小时电话、邮件等方式解答、响应甲方的服务请求和故障申报，15 分钟内响应，并启动故障排查修复工作，故障处理完毕后提供相关故障报告。详见附件 5 故障处置应急预案。

2.2 乙方为甲方政务云机房提供 6 名技术人员 7*24 小时全天候运维值守服务。

第三条 政务云租赁服务质量要求及验收

1.乙方为甲方提供的政务云租赁服务质量应符合国家或相关行业的标准。

2.乙方提供的云平台整体可用性应不低于 99.9%，数据可靠性应不低于 99.9999%。

3. 在本合同有效期内，乙方保证提供的云平台层面的安全性。

4. 乙方应为甲方提供其云平台咨询服务，配合、协助甲方修订原有管理办法，并严格执行。

5. 乙方完成政务云租赁服务后应及时通知甲方进行验收，甲方应在收到通知后 10 个工作日内安排并完成验收，验收需在 2025 年 5 月 23 日之前完成。验收合格的，甲方项目负责人在验收合格单上签字，并对乙方政务云租赁服务质量进行评价。验收不合格的，乙方应当在 10 个工作日内进行返工或调整，并重新提交甲方验收。

第四条　项目小组及人员要求

1. 甲方指派一名代表作为本项目负责人，负责确定项目计划，监督项目执行，协调项目资源，确认项目成果。

甲方项目负责人：李志

2. 乙方指派一名代表作为本项目负责人，乙方项目负责人及联系方式：王夏楠 13811110522.

3. 项目主要人员要求

乙方须根据项目要求安排具备相应资质和经验的专业人员 6 名（单独提交甲方），从事本项目的调研和迁移工作，并确保项目实施队伍的稳定。项目实施过程中，乙方如因正当理由需要调整项目主要人员的，应当提前 10 个工作日通知甲方，获得甲方同意后方可更换。

第五条 政务云租赁服务期限

1. 乙方为甲方提供上述政务云租赁服务的期限为：2024 年 05 月 24 日至 2025 年 05 月 23 日。

第六条 政务云租赁服务费及支付方式

以《合同书》约定为准。

第七条 甲方的权利义务

1. 甲方有权要求乙方按照本合同约定提供各项政务云租赁服务。

2. 甲方有权对乙方提供各项政务云租赁服务的情况进行监督和检查和评价。

3. 甲方有权提出有关管理、技术需求和要求，协调云租赁服务商、业务系统服务商的关系，协调业务系统服务商配合调研、迁移、运维、安全和应急演练等过程的工作。

4. 甲方负责本单位业务系统的应用软件和系统软件的提供、日常维护、管理、安全和应急保障。

5. 甲方有权聘请第三方作为本项目的监理。监理方依甲方的授权，对项目的质量、进度和投资进行监督和管理，并协调有关单位间的工作关系。

6. 甲方有根据监理单位提出的惩罚措施对乙方进行处罚的权利。

第八条 乙方的权利义务

1. 乙方应按照本合同约定向甲方提供各项政务云租赁服务，确保政务云租赁服务质量符合本合同约定；如因乙方提供政务云租赁服务质量不合格给甲方造成损失的，乙方应予赔偿。

2. 乙方保证其向甲方提供的政务云租赁服务不存在任何侵犯第三方著作权、商标权、专利权等合法权益的情形，否则乙方应赔偿因此给甲方造成的全部损失。

3. 乙方有义务配合甲方根据工作需要，对其提供政务云租赁服务情况及项目政务云计算服务费支出、使用情况进行的监督和检查，出现问题的应及时整改。

4. 乙方应保证为甲方提供具备提供本合同项下政务云租赁服务所需的相应资质和许可，并保证乙方人员在为甲方提供服务的过程中，严格遵守甲方的各项规定、服

从甲方安排。

5 如因乙方原因，在从事提供本合同下政务云租赁服务中给甲方或第三方造成人员人身伤害或财产损失的，乙方应依法承担赔偿责任。

6. 乙方应协助甲方建立健全配套制度标准，包括：运维制度、应急预案、安全保障制度、监管办法等。

7. 乙方负责管理甲方申请的 IP 地址，为甲方提供 IP 地址分配和管理服务。

8. 乙方负责所建设政务云平台的具体管理、监控、安全防护等工作，按甲方需求定期向甲方提供监控报告。

9. 政务云租赁服务期满后，如乙方不再提供政务云租赁服务，乙方应配合各方完成迁移和切换工作，切换期及其费用由甲乙双方商议决定，但切换期最长不超过 6 个月，费用不超过本合同约定的费用标准。

10. 重大活动期间，乙方应配合甲方制定预案并提供云平台的现场值守等服务。

11. 未经甲方同意，乙方不得将本合同义务全部或者部分转委托第三方履行。

12. 乙方工作人员未经甲方授权，擅自篡改甲方业务数据，或利用甲方现有业务应用系统、网络平台或者冒用甲方身份获取非法利益，均属于乙方的重大违约行为，甲方有权根据违法行为及损失程度参照附件 3 要求乙方承担违约赔偿责任。

13. 乙方接受甲方聘请的监理单位的管理，按照监理单位的要求提供相应的资料与文档，配合监理单位的要求按时保质地完成工作。

第九条 甲乙方安全责任边界

1. 甲方安全责任

（1）甲方承担系统软件、应用系统、数据等方面的安全责任。

（2）甲方负责组织应用系统级别的应急演练，如有需要，甲方有权要求乙方配合

应急演练。

2.乙方安全责任

（1）乙方承担云平台层面（主要包括物理资源、计算资源 、存储资源、网络资源）以及数据防丢失的安全责任。

（2）乙方在取得甲方许可后，负责云平台应急演练；乙方有义务配合甲方完成业务系统的应急演练。

（3）乙方须按照《中央网络安全和信息化领导小组办公室关于加强党政部门云计算服务网络安全管理的意见》（中网办发文（2014）14号）的要求和有关网络安全标准，落实并通过所建设的云平台的第三方网络安全审查。

第十条 保密义务

1.乙方因承接本合同约定项目所知悉的本项目信息或甲方信息，以及在项目实施过程中所产生的与本项目有关的全部信息均为甲方的保密信息，乙方应按照《中华人民共和国保守国家秘密法》、《中华人民共和国保守国家秘密法实施条例》及甲方关于保密工作的相关要求，对上述保密信息承担保密义务，但此保密信息甲方告知以前乙方已经知道、或者保密信息已为公众所知的除外。未经甲方书面同意，乙方不得将甲方保密信息透露给任何第三方。

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

3.乙方保证将保密信息的披露范围严格控制在直接从事本项目工作且因工作需要有必要知悉保密信息的工作人员范围内，对乙方非从事本项目的人员一律严格保密。

4. 乙方应保证在向其工作人员披露甲方的保密信息前，认真做好员工的保密教育工作，明确告知其将知悉的为甲方的保密信息，并明确告知其需承担的保密义务及泄密所应承担的法律责任，并要求全体参与本项目的人员签署书面《保密协议》。

5. 经甲方提出要求，乙方应按照甲方指示在收到甲方书面通知后将甲方保密信息的所有文件或相关资料归还甲方，且不得擅自复制留存。

6. 非经甲方特别授权，甲方向乙方提供的任何保密信息并不包括授予乙方该保密信息包含的任何专利权、商标权、著作权、商业秘密或其它类型的知识产权。

7. 乙方承担上述保密义务的期限为长期，合同有效期间及合同终止或解除后，乙方均应履行上述保密义务，直至保密信息向社会公开。

8. 承担上述保密义务的责任主体为乙方（含乙方工作人员）。如乙方或乙方工作人员违反了上述保密义务，给甲方造成损失的，乙方均应向甲方承担全部责任，并赔偿因此给甲方造成的全部损失。

9. 未经过乙方事先书面同意，甲方不得使用乙方商标（包括但不限于文字、图形等）、logo、品牌标识等，双方不得就本协议的合作关系、未来可能或实际进行的合作及项目进行对外公开、宣传和发表公开言论（包括但不限于网站、新闻、报纸、微博、微信、公告、宣传单、海报等）。如果就特定事宜需要进行对外公开、宣传和发表公开言论，需要事先获得乙方书面确认对外公开、宣传和发表公开言论的内容。如果乙方发现或认为甲方的行为不符合要求，视为甲方违约，乙方有权要求甲方立即改正，因此造成乙方损失的，乙方有权要求甲方赔偿。本条款有效期追溯至甲乙双方初次建立合作之日。

第十一条　知识产权归属

1. 乙方为履行本合同义务所形成的服务数据的知识产权归甲方单独所有。

2. 乙方提供的相关软件应是自行开发的产品或具备合法、合规授权，满足知识产权方面的有关规定和要求。

3. 乙方保证向甲方提供的政务云租赁服务成果是其独立实施完成，不存在任何侵犯第三方专利权、商标权、著作权等合法权益。如因乙方提供的租赁服务成果侵犯任何第三方的合法权益，导致该第三方追究甲方责任的，乙方应负责解决并赔偿因此给甲方造成的全部损失。

4. 各方在对外宣传（如在各自官网、市场营销活动）时，如有涉及对方的内容，应提前通知对方，在取得对方同意后方可发布信息。

第十二条 违约责任及合同的解除

1. 甲乙双方均应全面履行本合同，任何一方不履行或不按约定履行均构成违约，违约方应赔偿因此给对方造成的全部损失。

2. 乙方提供政务云租赁服务不符合本合同约定标准的，乙方应当在甲方规定的期限内进行返工、修改，并重新提交甲方验收；如整改后仍不能达到甲方要求的，甲方有权单方解除本合同，乙方应返还甲方已经支付的全部款项，并约定向甲方支付违约金，不足以弥补甲方损失的应予以补足。

3. 乙方不接受甲方和相关审计部门对本项目进行监督检查的，或经检查发现存在违法违规情况的，按照附件 3、附件 4 的违约责任表处理。

4. 乙方提供政务云租赁服务过程中可能发生的违约行为及相应应承担的违约金详见附件 3 和附件 4，乙方发生违约行为应在甲方通知之日起按照附件 3 和附件 4 约定比例支付违约金，甲方亦可在应付款中扣除违约金，其他具体支付事宜由甲乙双方协商。系同一事件导致的事故，甲方不可就同一事件重复要求乙方承担违约责任，

经甲乙双方协商，择其重者确定乙方支付违约金的办法。

5.在政务云租赁服务期出现下列情况，甲方向乙方提出整改要求和期限，且乙方在规定期限内未能履行甲方正当要求的，甲方有权解除本合同：

（1）多次在云安全监管方已发出整改通知后未正确处置，出现问题并造成B级及以上事故；

（2）重大活动期间如甲方要求人员到场而乙方所承诺的骨干人员和管理人员未到场的；

（3）连续2个月所承诺的运维服务人员人数未达到合同要求；

6.甲方依法律规定或本条约定解除合同的，乙方应返还甲方已经支付的全部款项并按照附件3和附件4约定向甲方支付违约金，如不足以弥补甲方损失的应予以补足。

第十三条 退出机制

1.政务云租赁服务期内，如乙方提出退出要求，需至少提前6个月向甲方提出退出书面申请，并获得甲方的书面许可且配合各方完成迁移和切换工作后方可退出，对于由此给甲方带来的经济损失，由乙方承担。

2.政务云租赁服务期满或者甲方提前合同解除的，乙方应配合各方完成迁移和切换工作，切换期及其费用由甲乙双方商议决定，但切换期最长不超过【6】个月，费用不超过本合同约定的费用标准。乙方承诺在切换期内配合完成迁移和切换工作，如因乙方原因造成未在切换期内完成，对于由此给甲方带来的经济损失，由乙方承担。

第十四条 争议的解决

因履行合同所发生的一切争议，双方应友好协商解决，协商不成的，按下列方式解决：

应依法向甲方所在地人民法院起诉。

第十五条 不可抗力

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。

2. 由于不可抗力致使合同无法履行的，受不可抗力影响一方应立即将不能履行本合同的事实书页通知对方，并在不可抗力发生之日起 15 天内提供有关相关政府部门或公证机关出具的证明文件（如有）。

3. 由于不可抗力致使合同无法履行的，合同在不可抗力影响范围及其持续期间内将中止履行，本合同执行时间可根据中止的时间相应顺延，双方无需承担违约责任，但因延迟履行后遭遇不可抗力的除外。不可抗力事件消除后，双方应就合同的履行及后续问题进行协商，按照该事件对合同履行的影响程度，决定继续履行合同或终止合同。

第十六条 廉政承诺

1. 合同双方承诺共同加强廉洁自律、反对商业贿赂。

2. 甲方及其工作人员不得索要礼金、有价证券和贵重物品；不得在乙方报销应由本单位或个人支付的费用；不得以参与项目实施为名，接受乙方从该项目中支取的劳务报酬；不得参加乙方安排的超标准宴请和娱乐活动。

3. 乙方不得向甲方及其工作人员行贿或馈赠礼金、有价证券、贵重礼品；不得为其报销应由甲方单位或个人支付的费用；不得向甲方工作人员支付劳务报酬；不得安排甲方工作人员参加超标准宴请及娱乐活动。

第十七条 其他

1. 本合同自双方法定代表人签字/签章并加盖公章之日起生效。

2.未尽事宜，经双方协商一致，签订补充协议，补充协议与本合同不一致或相冲突的内容，以补充协议为准。

3.本合同一式柒份，甲方执肆份，乙方执叁份，具有同等法律效力。

4.附件内容作为本合同不可分割的一部分，与本合同具有同等法律效力。

（以下无正文）

附件：

附件 1 中标通知书

附件 2 服务内容及分项报价表

附件 3 重大安全事故表

附件 4 乙方一般违约行为和严重违约行为

附件 5 故障处置应急预案

附件 6 廉政建设共建协议书

附件 7 安全保密协议书

附件 1：中标通知书（需补充）

中 标 通 知 书

致：北京金山云网络技术有限公司

根据【项目编号：11000024210200081439-XM001】卫生监督信息化运维项目硬件运维服务采购项目的招标文件和你单位于 2024 年 5 月 11 日提交的 06 包投标文件，经评审小组综合评审，最终确定你单位为卫生监督信息化运维项目硬件运维服务采购项目 06 包的中标单位，中标金额：¥674,720.00（大写：陆拾柒万肆仟柒佰贰拾元整）。

请你单位自本通知书发出之日起 30 日内持本通知书，按照招标文件及投标文件确定的事项与采购人签订合同。

采购代理机构：华诚博远工程咨询有限公司

日期：2024 年 5 月 14 日

附件 2：服务内容及分项报价表

序号	分项名称	单价（元）	数量	合价（元）	备注/说明
1	扩展服务：基础软件支撑服务：商用操作系统套餐	￥120.00	16	￥23,040.00	无
2	扩展服务：基础软件支撑服务：开源操作系统套餐	￥50.00	4	￥2,400.00	无
3	扩展服务：安全服务：云端APT防护服务	￥1,000.00	2	￥24,000.00	无
4	扩展服务：安全服务：网络防病毒服务	￥800.00	2	￥19,200.00	无
5	扩展服务：安全服务：主机杀毒服务	￥12.00	20	￥2,880.00	无
6	扩展服务：安全服务：主机安全加固	￥3,000.00	20	￥240,000.00	无
7	扩展服务：安全服务：网页防篡服务	￥1,600.00	7	￥134,400.00	无
8	扩展服务：安全检测监测、审计服务：主机漏洞扫描	￥1,000.00	20	￥80,000.00	无
9	扩展服务：安全检测监测、审计服务：数据库审计	￥1,200.00	2	￥28,800.00	无
10	扩展服务：安全检测监测、审计服务：主机日志分析	￥3,000.00	20	￥120,000.00	无
总价（元）				￥674,720.00	

附件 3：重大安全事故表

云服务商服务期内的违约行为造成云平台整体故障（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）。

乙方触发该违约行为将被视为“政务云失信”、取消云服务商资格，同时云管理单位将向相关部门及单位通报处罚结果。

类别		范围	影响	影响时间	事件级别	次数
重大安全事故（云服务商主责）	服务中断	云平台整体	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，因云服务商的安全隐患原因造成的系统被恶意篡改事件。事件发生后云服务商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云平台超过 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云平台存在安全隐患，云服务商未在 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	云平台整体	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	因云服务商的安全隐患原因造成的系统被恶意篡改事件，事件发生后云服务商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、市级领导批示或关注的。	30 分钟以上		

类别		范围	影响	影响时间	事件级别	次数
	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云平台存在安全隐患，云服务商未在24小时内做有效处置或应急防护措施，造成业务系统被恶意篡改或敏感信息泄露事件。	——		

附件 4： 乙方一般违约行为及严重违约行为

云服务商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=业务系统云计算服务费/服务月数*惩罚系数

序号	问题描述	惩罚系数
1	所提供的云服务可用性低于 99.99%，或数据可用性低于 99.9999%，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，由于另一家云服务商服务中断，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	在云安全监管服务商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%
7	平均响应时间大于 15 分钟且小于 30 分钟，造成重大事故	200%
8	运维需求平均响应时间大于 30 分钟且小于 60 分钟，造成重大事故	200%
9	运维需求平均故障恢复时间大于 30 分钟且小于 60 分钟，造成重大影响	100%
10	运维需求平均故障恢复时间大于 60 分钟且小于 120 分钟，造成重大影响	200%
11	现场无人值守超过大于 1 小时且小于 2 小时，造成重大事故	100%

序号	问题描述	惩罚系数
12	现场无人值守超过大于 2 小时且小于 4 小时，造成重大事故	200%

云服务商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=业务系统云计算服务费/服务月数*惩罚系数

序号	问题描述	惩罚系数
1	所提供的云服务可用性达不到 99.99%，或数据可用性低于 99.9999%，出现问题但未造成重大损失的	50%
2	所提供的云服务可用性达不到 99.99%，或数据可用性低于 99.9999%，且在服务期内接到用户投诉此类情况 3 次以上的	20%
3	在运营期间，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	在运营期内，如乙方未能按照用户方的扩容需求，在 7 个自然日内完成云平台的资源扩容，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	在云安全监管服务商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%
8	运维需求平均响应时间大于 15 分钟且小于 30 分钟，出现问题但未造成重大影响	30%
9	运维需求平均响应时间大于 30 分钟且小于 60 分钟，出现问题但未造成重大影响	50%
10	运维需求平均故障恢复时间大于 30 分钟且小于 60 分钟，出现问题但未造成重大影响	30%
11	运维需求平均故障恢复时间大于 60 分钟且小于 120 分钟，出现问题但未造成重大影响	50%
12	现场无人值守超过大于 1 小时且小于 2 小时，出现问题但未造成重大影响	30%
13	现场无人值守超过大于 2 小时且小于 4 小时，出现问题但未造成重大影响	50%

附件 5 故障处置应急预案

安全事件定义

信息安全事件是指对计算机系统或网络系统的可用性、完整性、保密性、真实性、可核查性和可靠性造成危害的事件，或者是在计算机系统或网络系统中发生的对社会造成负面影响的其他事件。信息安全事件的主体是指信息安全事件的制造者或造成信息安全事件的最终原因。信息安全事件的客体是指受信息安全事件影响或发生信息安全事件的计算机系统或网络系统。依据计算机系统和网络系统的特点，信息安全事件的客体可分为信息系统、信息内容和网络基础设施三大类。

安全事件分类

信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件及其他信息安全事件等七个类别：

(1)、有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

(2)、网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

(3)、信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

(4)、信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

(5)、设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

(6)、灾害性事件是指由自然灾害等其他突发事件导致的信息安全事件。

(7)、其他信息安全事件：不能归为以上类别分类的信息安全事件。

安全事件分级

对信息安全事件分级是有效开展信息安全事件报告、应急处置、调查处理和评估备案等信息安全应急响应工作的必要条件。信息安全事件分级主要参考业务影响因素。即业务影响是衡量信息安全事件对事发单位正常业务开展所造成的负面影响程度的要素。

根据信息安全事件给业务所造成后果的严重影响程度，信息安全事件可划分为 4 个等级。应急事件可能造成的危害程度、波及范围、影响力大小、人员及财产损失等情况，由高

到低划分为特别重大（I 级）、重大（II 级）、较大（III 级）、一般（IV 级）四个级别：

I 级事件：规模大、范围广、影响持续时间长（比如发生不可预见的灾难性事故，如：火灾、水灾和地震等）；政务云平台整体网络发生大规模瘫痪，事态发展超出控制能力。

① 造成全网 2 小时以上网络中断，核心或汇聚机房建筑倒塌、破坏等事件；

② 造成北京市市级政务云平台核心和汇聚节点网络设备整机 、云平台管理系统和相关硬件以及云机房服务器和基础设施（如 UPS、空调等）停止运行的事件；

③ 面向公众服务（首都之窗、财政局系统、资源中心系统等）的重要业务系统被恶意劫持、篡改、拒绝攻击导致服务中断 30 分钟以上。

附表为 I 级事件明细：

编号	事件分类	事件	级别
1	攻击类事件	拒绝服务攻击，带宽已完全占用，网络访问缓慢或无法访问	I
2		漏洞扫描攻击，负载均衡无法提供服务	I
3	链路故障事件	核心链路故障，业务系统受影响，120 分钟内不能恢复	I
4		核心链路故障，云平台业务全部中断	I
5		安全防护类设备故障，所有链路网络中断	I
6	信息破坏事件	由云平台漏洞导致的云平台信息被篡改	I
7		由用户业务系统漏洞导致的云平台信息被篡改	I
8		由云平台漏洞导致的用户业务信息被篡改	I
9		由云平台运维人员问题导致的云平台信息被篡改	I
10		由云平台运维人员问题导致的用户信息被篡改	I
11		由云平台漏洞导致的用户业务系统信息泄露	I
12		由云平台运维人员问题导致的用户系统信息泄露	I
13		由云平台运维人员问题导致的云平台信息系统数据泄露	I
14		由云平台漏洞导致的用户业务系统信息丢失	I
15		由云平台运维人员问题导致的用户系统信息丢失	I
16		由云平台运维人员问题导致的云平台信息系统数据丢失	I
17	有害程序事件	云内网中主机感染蠕虫病毒，并且病毒感染情况正在蔓延	I
18		政务云内网主机感染病毒，并被安装了后门文件	I
19		由用户业务系统漏洞导致的云平台主机被完全控制	I

20		由用户业务系统漏洞导致的云平台超过 3 台以上主机瘫痪	I
21	服务器与应用	存储或磁盘阵列发生故障，用户业务系统受到影响	I

II 级事件：规模较大、范围较广；影响持续时间较长；本地无备用资源，需从设备供应商或设备维护商紧急调用备件。造成严重损害，需要跨部门、跨地区，在上级领导协调下，协同处置的突发公共事件。

① 核心节点非旁路的网络设备、安全设备以及具有阻断和防护功能组件或系统失效，且具备临时解决方案的（bypass）；

② 核心层网络光缆链路中断，但不会导致整个网络中断的；

③ 重要信息系统（信息安全等级三级及以上）故障或遭受攻击；

④ 面向公众服务系统（首都之窗、财政局系统、资源中心系统等）出现首页无法访问、首页格式错乱等异常现象或网站页面被篡改。

附表为 II 级事件明细：

编号	事件分类	事件	级别
1	攻击类事件	漏洞扫描攻击，负载均衡性能降低	II
2		由用户业务系统漏洞导致的云平台瘫痪	II
3		由用户业务系统漏洞导致的网络阻塞	II
4	链路故障事件	非核心链路故障，重要业务系统受影响	II
5		核心链路故障，业务系统受影响，120 分钟内能够恢复	II
6		审计类设备故障，流量数据无法正常记录和审计	II
7		安全防护类设备故障，自动 bypass，防护能力缺失	II
8		安全防护类设备性能低，防护能力下降	II
9		安全防护类设备故障，单条链路网络中断	II
10		云机房专线发生故障	II
11	有害程序事件	政务云用户门户系统网站被恶意篡改，网页内嵌恶意代码	II
12		政务云平台管理系统网站被恶意篡改，网页内嵌恶意代码	II
13		由用户业务系统漏洞导致的同一租户下所有主机瘫痪	II
14		由用户业务系统漏洞导致的云平台主机感染病毒	II
15		云平台运维终端感染特洛伊木马病毒，系统被控制	II

16	服务器与应用	2 台以上服务器发生故障，30 分钟内无备份服务器代替	II
17		主数据库服务器故障，导致云管理平台短时间内无法管理	II

III 级事件：范围较小、突然发生、影响持续时间较短；造成区域范围内（多个部门）无法正常使用网络和信息系统。但是可以采取临时措施恢复网络畅通。

① 云平台管理中心无法访问超过 15 分钟；

② 远程 VPN 接入服务无法使用超过 15 分钟；

③ 信息安全等级三级以下，非面向公众服务的系统出现故障或遭受攻击。

④ 跨部门区域范围内群体 pc 机中毒，或无法正常使用。

附表为 III 级事件明细：

编号	事件分类	事件	级别
1	攻击类事件	由用户业务系统漏洞导致的网络访问缓慢	III
2		拒绝服务攻击，带宽占用同比增长 50%以上	III
3	链路故障事件	非核心链路故障，部分业务系统受影响	III
4	有害程序事件	政务云用户门户系统网站页面被攻击，用户无法正常登陆	III
5		政务云平台管理系统网站页面被攻击，用户无法正常登陆	III
6		由用户业务系统漏洞导致的同一租户下主机感染病毒	III
7		由用户业务系统漏洞导致的同一租户下主机被完全控制	III
8	服务器与应用	2 台核心服务器发生故障，30 分钟内可以由备份服务器代替	III
9		数据库发生故障，云管理平台部分功能无法使用	III
10		1 台核心服务器发生故障，30 分钟内无备份服务器代替	III
11		管理中心页面访问延迟，页面打开延迟超过 30s 以上	III
12		其它应用系统操作系统故障	III

IV 级事件：范围小；影响信息系统或较少的网络用户；影响持续时间短；本地有备用资源，或虽无备用资源，但可以采取临时措施恢复网络畅通。不需要跨部门、跨地区协同处

置的突发事件。

附表为 IV 级事件明细：

编号	事件分类	事件	级别
1	攻击类事件	租户虚拟机内网漏扫攻击	IV
2		租户虚拟机内网嗅探类攻击	IV
3		由用户业务系统漏洞导致的操作系统瘫痪	IV
4		拒绝服务攻击，带宽占用同比增长 50%以下	IV
5	链路故障事件	非核心链路故障，业务系统不受影响	IV
6	信息破坏事件	由用户业务系统漏洞导致的用户自身系统信息泄露	IV
7		由用户业务系统漏洞导致的用户自身系统信息丢失	IV
8		由用户业务系统漏洞导致的业务被篡改	IV
9	服务器与应用	1 台核心服务器发生故障，30 分钟内可以由备份服务器代替	IV
10		存储或磁盘阵列发生故障，用户业务系统不受影响	IV
11		管理中心页面访问延迟，页面打开延迟超过 30s	IV
12	物理安全事件	未授权人员进出机房区域	IV
13		未经授权人员接入网管网络	IV

预警分级

可以预警的突发事件预警级别，按照突发事件发生的紧急程度、发展势态和可能造成的危害程度分为一级、二级、三级和四级，分别用红色、橙色、黄色和蓝色标示，一级为最高级别。

红色等级（一级）：预计将要发生特别重大以上突发事件，事件会随时发生，事态正在不断蔓延。

橙色等级（二级）：预计将要发生重大以上突发事件，事件即将发生，事态正在逐步扩大。

黄色等级（三级）：预计将要发生较大以上突发事件，事件已经临近，事态有扩大的趋势。

蓝色等级（四级）：预计将要发生一般以上突发事件，事件即将临近，事态可能会扩大。

预警响应

预警信息发布后，金山云运维团队应根据预警级别，启动相应的应急预案，组织部署所

属技术力量、应急队伍立即响应，进入应急状态，履行各方的责任。

蓝色预警响应

组织各部门相关人员实行 24 小时值班，保持通信网络畅通，管理小组密切关注事态发展，收集汇总监测信息，重要信息及时向客户汇报。

确保各应急队伍进入应急状态，60%应急技术人员处于待命状态。实时监控云平台硬件、软件状态，保证平台各个层面的可用性。

黄色预警响应

在蓝色预警响应的基础上，加强领导带班和 24 小时值班，保持通信网可以畅通；实行每日信息报送制度，每日发送事态进展至客户。应急小组联系相关专家，组织专家对预警信息和事态发展进行预判，制定防范措施，做好预防工作。

确保应急队伍进入应急状态，80%应急技术人员处于待命状态。实时监控云平台硬件、软件状态，保证平台各个层面的可用性。

橙色预警响应

在黄色预警响应的基础上，应急小组第一领导应全面掌握情况，部署预警响应措施；各部门分管领导加强监测和情报搜集工作，每天两次向客户报送相关信息，重要信息随时报告。

应急小组在展开应急处置的同事，制定预警防范措施，同时加强风险评估与控制工作，做好数据备份等技术防范工作。

红色预警响应

在橙色预警响应的基础上，应在公司领导的指挥下开展预警响应工作。各级领导应全面掌握情况，部署预警响应措施，并加强应急部门间的沟通、联系、协调，加强综合研判和情报共享，高度关注事态发展，联合公司内部和外援力量参与应急处置工作，全面做好应急准备。

先期处置

网络与信息安全事件发生后，必须在第一时间内实施先期处置，并按照职责和规定权限启动相关应急预案，控制事态发展并及时向上级主管部门汇报。

（1）控制事态发展，防控蔓延。需采取各种技术措施及时控制事态发展，最大限度地防止事件蔓延。

（2）快速判断事件性质和危害程度。尽快分析事件发生原因，根据网络与信息系统运行和承载业务情况，初步判断事件的影响、危害和可能波及的范围，提出应对措施建议。

（3）及时报告信息。在先期处置的同时要按照预案要求，及时向客户报告事件信息。

（4）做好事件发生、发展、处置的记录和证据留存。事发单位在先期处置过程中应尽量保留相关证据，采取手工记录、截屏、文件备份和影像设备记录等各种手段，对事件发生、发展、处置的过程、步骤、结果进行详细记录，尽可能保存原始证据，为事件处置、调查、处理提供客观证据。

Ⅰ级事件响应要求

由应急领导小组启动Ⅰ级响应，统一指挥、协调、组织应急处置工作，应急小组其他单位成员积极配合，集中技术力量解除故障。

（1） 启动指挥体系

应急领导组进入应急状态，各单位成员保持 24 小时联络畅通，相关负责人员需 24 小时在岗值班。

（2）掌握事件动态

跟踪事态发展。现场指挥及时将事态发展变化情况和处置进展情况上报至领导小组。检查影响范围。现场指挥小组及时了解事发单位主管范围内的信息系统是否受到事件的波及或影响，并将有关情况及时报领导小组。领导小组组织专家对事态进行研究，并根据需要组织对云平台的核查。

（3）处置实施

控制事态防止蔓延。现场指挥小组及时采取技术措施阻止事件蔓延，督促、指导相关运行单位有针对性地加强防范。

做好处置消除隐患。尽快分析事件发生原因，并根据原因有针对性地采取措施，恢复受破坏信息系统正常运行。

及时开展调查取证。现场指挥小组组织开展事件调查和责任评估工作，及时向市通信保障和信息安全应急指挥部办公室报告。

信息发布。现场指挥小组根据事件应急的实际情况，形成各阶段工作简报，报告至应急领导小组。

Ⅱ级事件响应要求

由应急领导小组启动Ⅱ级响应，统一指挥、协调、组织应急处置工作，应急小组其他单位成员积极配合，集中技术力量解除故障。

（1） 启动指挥体系

应急领导组进入应急状态，各单位成员保持 24 小时联络畅通，相关负责人员需 24 小时在岗值班。

（2）掌握事件动态

跟踪事态发展。现场指挥及时将事态发展变化情况和处置进展情况上报至领导小组。检查影响范围。现场指挥小组及时了解事发单位主管范围内的信息系统是否受到事件的波及或影响，并将有关情况及时报领导小组。领导小组组织专家对事态进行研究，并根据需要组织对云平台的核查。

（3）处置实施

控制事态防止蔓延。现场指挥小组及时采取技术措施阻止事件蔓延，督促、指导相关运行单位有针对性地加强防范。

做好处置消除隐患。尽快分析事件发生原因，并根据原因有针对性地采取措施，恢复受破坏信息系统正常运行。

及时开展调查取证。现场指挥小组组织开展事件调查和责任评估工作，及时向市通信保障和信息安全应急指挥部办公室报告。

信息发布。现场指挥小组根据事件应急的实际情况，形成各阶段工作简报，报告至应急领导小组。

III级事件响应要求

由应急领导小组启动III级响应，统一指挥、协调、组织应急处置工作，应急小组其他单位成员积极配合，集中技术力量解除故障。

（1） 启动指挥体系

应急领导组进入应急状态，各单位成员保持 24 小时联络畅通，相关负责人员需 24 小时在岗值班。

（2）掌握事件动态

跟踪事态发展。现场指挥及时将事态发展变化情况和处置进展情况上报至领导小组。检查影响范围。现场指挥小组及时了解事发单位主管范围内的信息系统是否受到事件的波及或影响，并将有关情况及时报领导小组。领导小组组织专家对事态进行研究，并根据需要组织对云平台的核查。

（3）处置实施

控制事态防止蔓延。现场指挥小组及时采取技术措施阻止事件蔓延，督促、指导相关运

行单位有针对性地加强防范。

做好处置消除隐患。尽快分析事件发生原因，并根据原因有针对性地采取措施，恢复受破坏信息系统正常运行。

及时开展调查取证。现场指挥小组组织开展事件调查和责任评估工作，及时向市通信保障和信息安全应急指挥部办公室报告。

信息发布。现场指挥小组根据事件应急的实际情况，形成各阶段工作简报，报告至应急领导小组。

Ⅳ级事件响应要求

按照相关预案进行应急处置，应急小组相关负责人及时赶赴现场，组织协调、指挥所属技术力量进行事件处置工作，必要时请求外援机构和队伍进行支援。应急团队负责将事件信息、处置进展情况及时向客户报告。

应急结束

在网络与信息安全事件处置已基本完成，次生、衍生灾害和事件危害基本消除，风险得到控制，应急处置工作即告结束。

附件 6 廉政建设共建协议书

北京市卫生健康监督所

廉政建设共建协议书

甲方：北京市卫生健康监督所

乙方：北京金山云网络技术有限公司

合同名称：2024 年生监督信息化运维项目硬件运维服务采购项目-政务云扩展服务项目合同书

为贯彻落实中央和市委关于加强行业作风建设的要求，进一步加强信息中心反腐倡廉建设，规范、约束甲乙双方的行为，维护双方合法利益，防止违纪违法和不廉洁问题发生，营造和谐的合作环境。经双方同意签订本协议。

甲乙双方单位项目建设实施负责人为项目廉政责任第一责任人（本协议书的第一责任人，如在项目执行期间调离负责人岗位，由其接任人承担协议书中的一切责任），须做到重要工作亲自部署、督办，重大问题亲自过问、重点环节亲自协调，切实加强项目建设中的廉政建设。

第一条 甲乙双方责任

（一）双方应自觉遵守党和政府的廉政建设规定，严格按照国家有关法律、法规和相关行业的标准开展政府采购、招投标、项目建设、项目运维等活动。

（二）双方应严格履行合同条款，业务活动必须坚持公开、公平、公正、诚信、透明的原则，不得损害国家、集体和对方利益。

（三）双方应接受审计监督。被审计单位和个人应如实反映情况，并提供真实、完整的资料和证据。

（四）双方应遵守《保密法》等相关制度，保证不泄露知悉的国家秘密、商业秘密等。做到不利用职权或知晓项目的秘密和内部信息，为自己和他人谋利。

第二条 甲方责任

甲方单位和项目管理等人员，应严格遵守以下规定：

（一）不准与乙方工作人员就项目管理等事项进行私下交易，不得弄虚作假。

（二）不准向乙方索要或变相收受回扣、礼金、有价证券、贵重物品等。

（三）不准在乙方单位报销任何应由甲方或个人支付的费用。

（四）不准要求、暗示和接受乙方为个人房屋装修、婚丧嫁娶、配偶子女的工作安排以及出国（境）、旅游等提供方便。

（五）不准参加有可能影响项目履行的乙方单位组织的宴请和健身、娱乐等活动。

（六）不准以任何理由向乙方推荐分包单位和要求乙方购买甲方个人推荐的材料、设备等。禁止配偶、子女、亲属、身边工作人员参与同乙方项目建设有关的经济活动。

（七）不准向乙方提出任何与项目建设管理工作无关的要求。

第三条 乙方责任

乙方应当与甲方保持正常的工作关系，按照有关法律、法规和程序开展业务工作，严格遵守以下规定：

（一）不准与甲方工作人员就项目管理等事项进行私下交易，不得弄虚作假，以次充好。

（二）不准以任何理由向甲方馈赠或变相转送礼金、有价证券、贵重物品和给予回扣等。

（三）不准以任何理由为甲方单位报销应由甲方或个人支付的费用。

（四）不准为甲方相关工作人员房屋装修、婚丧嫁娶、配偶子女的工作安排以及出国（境）、旅游等提供方便。

（五）不准以任何理由为甲方单位或个人，组织有可能影响项目履行的宴请、健身、娱乐等活动。

（六）不得接受甲方推荐的分包单位和购买甲方推荐的材料、设备等，不准为甲方配偶、子女、亲属提供乙方项目建设有关的经济活动。

（七）不准接受甲方提出的任何与项目建设管理工作无关的要求等。

第四条 违约责任

（一）若甲方工作人员违反本协议书的约定，依据有关法律、法规和规定给予党纪、政纪处分或组织处理；涉嫌犯罪的，移交司法机关追究刑事责任。

（二）若乙方违反本协议书的约定，给甲方造成经济损失的，乙方应予以赔偿；涉嫌犯罪的，移交司法机关追究刑事责任。

第五条 监督

甲乙双方若发现对方有违反上述廉政建设共建协议书中约定的行为，应向双方单位纪检监察部门或检察院举报。

第六条 本协议书作为项目商务合同的附件，与项目商务合同共同存档备查。

第七条 本协议书一式柒份，甲方执肆份，乙方执叁份。

甲方：北京市卫生健康监督所（公章）

法人：_____（签字）

项目负责人：_____（签字）

2024年5月20日

乙方：北京金山云网络技术有限公司（公章）

法人：_____（签字）

项目负责人：_____（签字）

2024年5月20日

附件 7 安全保密协议书

安全保密协议书

项目名称：22024 年生监督信息化运维项目硬件运维服务采购项目-政务云扩展服务项目合同书

甲　　方：北京市卫生健康监督所

乙　　方：北京金山云网络技术有限公司

为了保护项目合作中涉及的保密信息，明确双方的权利义务，甲、乙双方在平等自愿、协商一致的基础上达成以下协议：

第一条　安全要求

一、乙方必须遵守甲方的各项规章制定，严格按照工作规范组织进行项目工作，制定切实可行的措施保障人员安全，设备安全，生产安全，信息安全。

二、乙方必须制定合理的措施对项目人员进行管理和思想教育，加强保密意识，安全生产意识。

第二条 保密信息范围

本协议所称的“保密信息”是指，双方在合同履行过程中获得的下列信息，但不包括一方通过公众渠道可以获得的信息或经对方书面同意允许向第三方透露的信息：

一、工作秘密：一切与政府工作有关的信息资料或其他性质的资料，包括但不限于：政府业务数据、人员机构信息、财务资料等；

二、技术秘密：指甲方的计算机信息系统、网络架构、信息安全体系结构、软件、数据库系统、系统数据、文档及技术指标等；

三、其他保密信息：包括但不限于项目过程中获取的有关数据、流程、分析成果；甲方的内部管理资料、财务资料；甲方其他项目的信息及有关政府行政机关规划、调整等尚未公开的资料。

上述保密信息的表现形式不限，无论是书面的、口头的、图形的或其它任何形式的信息。

第三条 安全保密期限

本协议约定的保密责任期限为自合同生效之日起至可通过公众渠道获得或经甲方书面同意允许向第三方透露之日止。

第四条 保密义务人

本协议项下保密义务人为，双方单位及双方涉及保密信息的员工。

第五条 保密义务

一、甲、乙双方保证对所获悉的对方保密信息按照下列规定进行保密，并在缺少相关保密条款约定时，应至少采取适用于对自己的保密信息同样的保护措施和审慎程度进行保密：

1、仅将本协议项下保密信息使用于与项目工作有关的用途。

2、除直接参与项目工作的人员之外，不得将保密信息透露给其他无关人员或任何第三方。

3、不能将对方保密信息的全部或部分进行发布、传播、复制或仿造。

4、双方均应告知并以适当的方式要求其直接参与项目工作的人员，按照本协议规定保守保密信息。如一方工作人员违反本协议规定，泄露对方保密信息的，该方应承担违约责任。

5、任何一方不能利用获悉信息为自己或其他方开发信息、技术和产品，或与对方的产品进行竞争。

二、乙方保密义务

1、未经对方书面许可并采取加密措施，不得擅自将载有保密信息的任何文档、图纸、资料、磁盘、胶片等介质，带离对方工作场所。

2、对于用户数据和服务结果数据的保管、访问，乙方无关人员不能访问；必需访问的人员，乙方要进行严格的访问控制；管理用户数据的人员应由乙方严格筛选。

3、对于甲方提供给乙方使用的任何资源，如网络、NOTES 等，乙方都只能将其用于工作，而不能用于其他目的，特别是从事侵害甲方利益的活动。

第六条 保密信息的交回

一、项目工作终止后，双方应按照对方的要求对相关保密信息做相应处理，比如销毁或其他处理方式。

二、当一方以书面形式要求交回保密信息时，接受通知一方应当立即交回所有的书面或其它有形的保密信息以及所有描述和概括保密信息的文件。

三、未经对方书面许可，任何一方不得丢弃和自行处理保密信息。

第七条 违约责任

任何一方未履行本协议项下的任一条款均视为违约，违约方应按照守约方要求采取有效的补救措施，以防止泄密范围继续扩大，同时还应当根据违约情况向对方支付一定数额的违约金。

第八条 争议的解决

因履行本合同而发生的或与本合同有关的一切争议，双方应协商解决，协商不成的，双方同意提交北京仲裁委员会进行仲裁。

第九条 其他

一、本协议未尽事宜，甲、乙双方另行签订补充协议，补充协议与本协议具有同等法律效力。

二、本协议一式柒份，甲方执肆份，乙方执叁份。

三、本协议自甲、乙双方签字盖章之日起生效。

甲方：北京市卫生健康监督所　　乙方：北京金山云网络技术有限公司

法人（签字/签章）：　　法人（签字/签章）：

签订日期：2024年 5 月 20 日　　签订日期：2024年 5 月 20 日