合同编号：

北京市住房和城乡建设委员会综合事务中心

2026年度市级政务云租用采购项目

甲　　方：北京市住房和城乡建设委员会综合事务中心

乙　　方：北京金山云网络技术有限公司

签订时间：2026年9月18日

签订地点：北京

委托人（甲方）：北京市住房和城乡建设委员会综合事务中心

法定代表人：傅宗琛

地址： 北京市通州区达济街 9 号院

受托人（乙方）：北京金山云网络技术有限公司

法定代表人：邹涛

地址：北京市海淀区西二旗中路 33 号院

甲、乙双方根据《中华人民共和国民法典》及相关法律法规的规定，就北京市住房和城乡建设委员会综合事务中心（甲方）的政务云资源租用服务费事宜，经协商一致，同意按照下列条款，签订本合同。

第一条 释义

1.甲方：指政务云使用单位，即签署本合同的北京市住房和城乡建设委员会综合事务中心。

2.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）具体政务云租赁服务项目见附件 1：政务云租赁服务目录清单。

2.技术支持服务要求：

（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）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，同时甲方有权按照本合同约定追究乙方的违约责任。如甲方未在前述期限内完成验收或验收后未提出异议的，视为验收合格。

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：和玉栋

联系方式：010-55597710

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：

乙方项目负责人：陈俊燃

联系方式：13110032983

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12名从事本项目的日常运维，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：2026年度。

第六条 政务云租赁服务费及支付方式

1.本合同项下政务云租赁服务费总额为人民币16,946,304.00元，大写：壹仟陆佰玖拾肆万陆仟叁佰零肆元整。前述政务云租赁服务费已经包含乙方完成本合同项下政务云租赁服务的全部费用（含税），除前述款项外，甲方无需向乙方另行支付其他任何费用。

2.付款方式

（1）首付款：本合同生效且财政资金下达后，甲方自收到发票之日起10个工作日内向乙方支付合同总价款的50%，即人民币8,473,152.00元，大写：捌佰肆拾柒万叁仟壹佰伍拾贰元整。

（2）2026年10月30日前，且乙方已按合同约定完成阶段性服务并经甲方出具用户意见后，甲方自收到发票之日起10个工作日内向乙方支付合同总价款的30%，即人民币5,083,891.20元，大写：伍佰零捌万叁仟捌佰玖拾壹元贰角。

（3） 2026 年 12 月 20 日前，且乙方已按合同约定完成全部服务并经甲方最终验收合格后，甲方自收到发票之日起 10 个工作日内向乙方支付合同总价款的 20%，即人民币 3,389,260.80 元，大写：叁佰叁拾捌万玖仟贰佰陆拾元捌角。甲方应将上述款项以汇款方式支付给乙方在本合同中载明的账号。

（4）乙方均应在甲方付款前提供符合甲方要求的发票，否则甲方有权拒绝付款，且不视为甲方违约。如甲方遇到财政国库支付受限，支付期限顺延，不承担违约责任，但要及时通知乙方，待障碍消除后恢复支付。乙方不得因此延迟、暂停、终止、拒绝义务的履行。

（5）本合同一经签订，视为乙方已明确知晓财政付款的相关规定，并自愿承担财政预算执行对乙方影响的法律后果。如因乙方未按合同约定的进度完成，造成预算资金被财政收回，无法支付的，相关后果由乙方自行承担。

3. 上述费用应以电汇等银行转账方式结算。乙方指定账户信息如下：

（1）账户名：北京金山云网络技术有限公司

（2）开户银行：民生银行北京上地支行

（3）账号：0110012830003054

4. 2027 年招标工作的中标人确定前，乙方按本合同约定及甲方要求继续履行相应职责，费用标准以 2027 年预算批复金额为准，支付进度以财政拨款进度为准，支付方式由双方另行协商。

5. 乙方应在本合同生效后 15 个工作日内，向甲方提交金额为合同总价款 10%的履约保函（银行类机构出具），用以保证乙方全面地履行本合同项下的各项义务，在下一年度服务合同签订之日后 30 日内按相关规定退还保函。

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。

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租赁服务费支出、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. 如因乙方人员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；乙方人员在履行本合同过程中遭受的人身或财产损失，乙方亦自行承担相应责任。

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、支行监管办法等。

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.乙方不得将本合同义务全部或者部分转包或分包给第三方履行。

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。

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（2015）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 安全保密义务

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.乙方根据合同任务建立相对独立的管理技术团队并指定一名高管（公司副总及以上级别）作为网络安全责任人。

10.乙方需将政务数据存储在甲方指定地点，未经甲方同意，不得私自获取，变更用途、用法，不得公开、转让或向第三方提供；合同终止时按照甲方的要求处理政务数据。涉及个人信息的，严格按照法律法规和相关制度标准执行。

11.乙方应根据《北京市住房和城乡建设委员会信息系统巡检、故障处置管理规范》对其提供的产品或服务开展巡检，发现网络安全漏洞、缺陷或其它严重网络安全风险，应第一时间处置并报告甲方，不得公开或向第三方提供相关信息。

12.乙方处理政务的信息平台应当优先采用安全可信的硬件和软件产品，涉及密码的应符合国家密码管理规定。

13.乙方在发现可能影响政务网络安全的重大事项，包括责任人及其他重要人员变更、业务转型、合并重组、投资并购等，应提前向甲方报告。

14.乙方每年向甲方提交网络安全报告，报告至少包括数据安全管理情况、平台关键软件和核心硬件供应链安全情况、管理技术团队变化情况等内容。

15. 法律、行政法规明确的其他网络安全要求。

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新的服务成果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。

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，包括但不限于守约方为维护自身利益而发生的诉讼费、保全费、律师费、担保费、保险费等费用。

2. 除“第六条”和“第十五条”约定的情形外，甲方因自身原因造成支付逾期的，每逾期一日应向乙方支付应付但未付金额万分之五的违约金。

3. 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，并按照附件 2、3、4 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。

4. 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 2、附件 3、附件 4 的违约责任表处理。

5. 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 2、3、4，乙方发生违约行为应在甲方通知之日起按照附件 2、3、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，甲方有权依据本合同及附件约定要求乙方承担相应的违约责任；违约金不足以弥补甲方实际损失的，乙方仍应予以全额赔偿

6. 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；

7. 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 2、3、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。

8. 对于乙方按照本合同约定应支付的违约金，甲方有权自任一期支付给乙方的款项中直接扣除而不必事先通知或者征求乙方的同意。

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：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面通知对方，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。

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或授权代表签字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. 本合同一式四份，甲、乙双方各执两份，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　政务云租赁服务目录清单

附件 2　重大安全事故表

附件 3　乙方严重违约行为

附件 4　乙方一般违约行为

附件 5　故障处置应急预案

附件 6　人员名单及相应资质

甲方（盖章）：

法定代表人或授权代表（签章）：

签订日期：2026年 9 月 18 日

乙方（盖章）：

法定代表人或授权代表（签章）：

签订日期：2026年 9 月 18 日

附件1 政务云租赁服务目录清单

序号	服务类别	服务名称	服务描述	计费单位	数量	租用期限(月)
1	计算服务	平台云主机服务（包含X86、ARM、C86）	vCPU（主频不低于2.4GHz）	元/vCPU/月	9010	12
2			内存	元/GB/月	27566	12
3		物理服务器租用服务（包含X86、ARM、C86）	双路每CPU核数32核，主频 ≥2.0GHz，128G内存，2块600GSAS硬盘，2个HBA卡，2个万兆端口	元/台/月	13	12
4		物理服务器增配服务（包含X86、ARM、C86）	内存-32GB内存	元/条/月	24	12
5			硬盘配置1-480GB SSD	元/块/月	4	12
6			GPU显存（需同时租用算力资源、云主机或物理服务器资源，联合使用）	元/GB/月	384	12

7			半精度浮点运算能力（需同时租用 GPU 显存、云主机或物理服务器资源，联合使用）	元/1TFLOPS/月	5280	12
8	存储服务	普通性能存储	普通存储(单盘技术指标:单盘 IOPS 2000-5000))	元/100GB/月	9454.12	12
9		高性能存储	高性能存储(单盘技术指标：单盘 IOPS 10000-25000)	元/100GB/月	5493.14	12
10		静态存储	大容量、高可靠的数据存储服务，具备 PB 级线性扩展能力	元/TB/月	10	12
11	网络服务	互联网链路服务	互联网链路带宽	元/Mb/月	400	12
12		互联网 IP 地址租用服务	互联网 IP 地址租用服务、并提供备案服务	元/IP（互联网）/月	114	12
13		主机负载均衡服务	主机负载均衡服务	元/IP（内网）/	38	12

				月		
14		远程接入服务	远程接入服务	元/账号/月	58	12
15		SSL VPN 接入	SSL VPN 接入（每套 10 个账户）	元/套/月	4	12
16		WAF 防护	针对网站及 Web 应用系统提供应用层安全防护支持各类 SQL 注入、XSS 攻击、网页木马、WEBSHELL 等 Web 威胁防护(200Mbps)	元/IP（互联网）/月	70	12

附件2 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。	——		

类别		范围	影响	影响时间	事件级别	次数
	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		
	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3 乙方严重违约行为

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%
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%

附件4 乙方一般违约行为

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	30%

	影响	
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	III

		务器代替	
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，政务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时，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 人员名单及相应资质

序号	姓名	年龄	学历	职称	工作年限	拟在本项目担任岗位
1	赵学思	36	硕士	高级	12	项目经理
2	池增坤	47	本科	高级	19	技术负责人
3	彭思思	33	本科	高级	11	质量管理专员
3	许绍华	31	本科	工程师	8	技术工程师
4	郑宝利	40	本科	工程师	10	技术工程师
5	武江鹏	31	本科	工程师	9	技术工程师
6	魏志军	41	本科	工程师	16	技术工程师
7	朱鑫亨	30	本科	工程师	6	技术工程师
8	姚栋杰	36	本科	工程师	11	技术工程师
9	陈映桥	28	本科	工程师	6	技术工程师
10	徐长志	40	本科	工程师	11	技术工程师
11	辛小玲	39	本科	工程师	10	技术工程师
12	马千玉	29	本科	工程师	6	技术工程师