信息安全服务项目—第四包：商用密码应用服务

委托合同

甲方：北京市应急指挥保障中心

法定代表人：张鹏

地址：北京市通州区运河东大街 57 号院 4 号楼

联系电话：010-55573808

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 5 号楼 9 层 101 号

联系电话：010-62927777

本合同甲方委托乙方就信息安全服务项目—第四包：商用密码应用服务进行专项技术服务，并支付相应的技术服务费。双方经过平等协商，在真实、充分的表达各自意愿的基础上，根据《中华人民共和国民法典》的规定，达成如下协议，并由双方共同恪守。

一、服务内容

商用密码服务包括基于国密算法的远程安全接入、密钥管理服务、数据加密服务、签名验签服务、虚拟密码机（VSM)服务、密码 API 接口服务、国密 SSL 证书、USBkey。本次主要为安全生产监管综合信息平台（一期）——北京市安全生产检查和隐患治理信息子系统提供密码服务。

1.基于国密算法的远程安全接入

支持在终端与平台之间建立 SSL VPN 安全通道，支持对接入网络的终端设备进行安全认证，支持客户端与服务端之间数据加密传输，支持对终端设备的权限控制；支持与安全浏览器建立合规的 HTTPS 安全通道。

2. 密钥管理服务

提供密钥生成、密钥更新、密钥备份与恢复、密钥归档、密钥销毁等密钥全生命周期管理。

3. 数据加密服务

提供数据加解密和完整性保护服务，实现数据库加解密、文件加解密。支持

数据库字段级或表级加密与完整性保护；支持文件数据加密与完整性保护，支持细粒度数据加密控制，支持数据加密吞吐率 100Mbps。

4. 签名验签服务

提供数字签名与签名验证服务功能，用于身份认证时签名数据验证，基于数字签名技术实现数据的完整性保护，支持 SM2 签名速度不低于 700 次/秒。

5. 虚拟密码机（VSM)服务

基于符合国密要求的密码算法和密钥安全管理机制，提供密钥产生、使用以及基础密码运算服务功能，每实例 4C8G。

6. 密码 API 接口服务

把密码调用接口进行业务级封装形成统一密码服务 API 和 SDK，对云平台上所有业务应用提供统一的密码服务，提供多租户的密码服务能力。

7. 国密 SSL 证书

国密 SM2 服务器证书 SSL V3 型，支持通配，需要 IP 验证可以是 80/443 端口，域名验证可以选择邮箱或 DNS；根据浏览器识别地址栏显示绿标；证书主题显示：单位名称和所在省市；配套购买 RSA 算法的 SSL 证书。

8. USBkey

PC 终端密码支撑服务，PC 端用户身份认证。

业务系统每个用户配发一个。

具体采购名称、服务期、数量、功能描述如下：

序号	名称	服务期（月）	数量	功能描述
1	基于国密算法的远程安全接入	12	2	支持在终端与平台之间建立 SSL VPN 安全通道，支持对接入网络的终端设备进行安全认证，支持客户端与服务端之间数据加密传输，支持对终端设备的权限控制；支持与安全浏览器建立合规的 HTTPS 安全通道。
2	密钥管理服务	12	1	提供密钥生成、密钥更新、密钥备份与恢复、密钥归档、密钥销毁等密钥全生命周期管理。
3	数据加密服务	12	1	提供数据加解密和完整性保护服务，实现数据库加解密、文件加解密。支持数据库字段级或表级加密与完整性保护；支持文

				件数据加密与完整性保护，支持细粒度数据加密控制，支持数据加密吞吐率100Mbps。
4	签名验签服务	12	1	提供数字签名与签名验证服务功能，用于身份认证时签名数据验证，基于数字签名技术实现数据的完整性保护，支持SM2签名速度不低于700次/秒。
5	虚拟密码机（VSM）服务	12	1	基于符合国密要求的密码算法和密钥安全管理机制，提供密钥产生、使用以及基础密码运算服务功能，每实例4C8G。
6	密码API接口服务	12	1	把密码调用接口进行业务级封装形成统一密码服务API和SDK，对云平台上所有业务应用提供统一的密码服务，提供多租户的密码服务能力。
7	国密SSL证书	12	1	国密SM2服务器证书SSL V3型，支持通配，需要IP验证可以是80/443端口，域名验证可以选择邮箱或DNS；根据浏览器识别地址栏显示绿标；证书主题显示：单位名称和所在省市；配套购买RSA算法的SSL证书。
8	USBkey	12	1	PC终端密码支撑服务，PC端用户身份认证。 业务系统每个用户配发一个。

二、时间进度要求

本项目服务期为2026年12月1日至2027年11月30日，完成全部服务内容并通过验收。

三、双方的权利和义务

甲方权利义务

1.掌握委托工作进度，监督乙方完成委托工作的权利。

2.按照约定支付报酬的义务。

3.为乙方履行合同义务提供必要的协助或便利的义务。

4.甲方有权对乙方工作提出意见和建议，乙方应在甲方要求的时间内按照甲方的建议和意见进行整改。

5.甲方有权对乙方提交的服务成果进行验收，乙方应在甲方要求时间内按照甲方意见对服务成果进行修改、补充。

6.乙方人员的工作能力及表现不符合本合同约定和甲方要求的，甲方有权要求乙方在甲方指定的期限内更换。

7.甲方的联系人：陈利明，具体工作职责：项目全流程实施事宜。

乙方权利义务

1.根据委托权限和甲方需求处理受托事务的义务。

2.亲自处理受托事务的义务,未经甲方同意，不得将本合同项下全部或部分工作转包、分包给任何第三方。

3.处理委托事务应尽忠诚与勤勉义务。

4.按照甲方要求报告受托事务处理情况的义务。

5.处理委托事务时接受甲方监督的义务。乙方应按照甲方要求对工作成果进行补充、修改，直至通过甲方验收，工期不予顺延，否则，乙方应承担延期交付的违约责任。

6.乙方保证其人员具备完成本合同项下工作所需的相应资格和能力，并保证委托期限内乙方人员的稳定性，未经甲方事先同意，乙方不得更换本项目中的工作人员。甲方要求乙方更换服务人员的，乙方应在甲方指定的期限内完成更换。

7.在履行本合同义务时，乙方应采取相应措施保证双方人员的人身、财产安全。因乙方未采取适当保护措施而造成双方人员人身或财产损害的，由乙方承担相应责任和费用。

8.乙方保证在履行本合同过程中不侵犯任何第三方的合法权益，否则乙方应负责解决由此产生的一切纠纷，承担相应法律责任，并赔偿甲方因此遭受的所有损失。

9.如有需要，乙方应配合甲方进行项目费用审计等工作，接受甲方或其委托的第三方机构及有关部门的监督检查和绩效评价等工作。

10.根据甲方要求，乙方在委托期限期满后协助甲方处理受托事务的，经甲方确认后另行给予委托经费支持。

11.未经甲方事先书面同意，乙方不得将本合同项下的权利义务转让给其他任何第三方。

12.乙方在服务的全过程中，应始终坚持正确的政治导向、价值导向、舆论导向，不得违背国家方针政策。

13.乙方须遵守国家和北京市相关法律法规，做好在建、在用信息系统的网络和数据安全防护工作。按照甲方要求开展信息系统整改、漏洞修复和安全加固工作。

14.乙方的联系人：周一 18301662409，具体工作职责：负责合同及项目实施过程中的具体事宜。

四、服务费用及支付方式

1.本服务费金额（含税金额）：人民币：伍拾贰万肆仟捌佰贰拾元整（¥524,820元），该费用为乙方完成本合同所有义务，甲方应向乙方支付的全部费用，除此之外，甲方不再向乙方支付其他任何费用。

2.付款方式：

甲方应于本合同签订且本合同进入服务期后，财政经费下达后10个工作日内，向乙方支付合同总价款的60%，即人民币：叁拾壹万肆仟捌佰玖拾贰元（¥314892元）；在开展技术服务6个月后乙方申请第2笔支付款，甲方收到乙方的支付申请后10个工作日内向乙方支付合同总价款的30%，即人民币：壹拾伍万柒仟肆佰肆拾陆元（¥157446元）；项目验收合格后，乙方申请第3笔支付款，甲方收到乙方的支付申请后10个工作日内向乙方支付合同总价款的10%，即人民币：伍万贰仟肆佰捌拾贰元（¥52482元）。

当甲方收到项目批复单位批复的资金不足以支付应向乙方支付的费用时，甲方向乙方支付项目批复单位已拨付的相应全部资金，剩余资金根据项目批复单位的资金拨付进度向乙方补充支付，乙方不得因此原因暂停或中止履行本合同。甲方不因此原因承担违约责任。

甲方每次付款前，乙方应提供符合国家相关税务规定的等额发票，否则甲方有权延迟付款且不承担违约责任。乙方对发票的合规性负责，如因乙方所开具的发票不合规给甲方造成的任何损失，全部由乙方承担。

乙方指定开户银行信息如下：

开户名称：北京金山云网络技术有限公司

开户银行：民生银行北京上地支行

账　　号：0110012830003054

3.乙方应保证上述账户信息真实、准确。若乙方上述账户发生变化，应于变化前/后【15】个工作日内分别书面通知甲方，否则由此导致错付、无法支付，其全部法律后果均由乙方自行承担。

4.乙方确认并承诺，由于甲方资金为财政性资金，如因财政拨付不足或不及时所造成的延期付款，不视为甲方违约，甲方不因此承担任何违约责任。

五、项目验收

完成商用密码服务开发部署，通过第三方密评且结论合格，乙方提交完整资料，运行期间无重大故障、故障修复率100%。

乙方提交申请与资料，甲方组织专家审核，组织现场测试核查，形成相关资料，包括但不限于实施方案、部署配置清单、产品管理操作手册、服务集成规范、上线保障方案、运维服务方案、项目工作总结、日常巡检（每月至少1次，重要期间按甲方要求开展）、故障处置、突发事件处置等。不合格项需整改后重新验收。

序号	验收条目	验收内容
1	密码资质与算法合规	合规
2	核心密码功能达标	功能实现
3	性能与防护达标	性能安全
4	文档与配套报备完整	文档和服务完整

六、知识产权

1.乙方因履行本合同所产生的所有成果的所有权及全部知识产权，归甲方所有，乙方不得侵犯，否则需承担全部法律后果。

2.乙方保证其向甲方提供的服务属于自有合法权利，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，否则全部法律后果（包括但不限于向第三人承担侵权责任、赔偿甲方损失等）由乙方承担。

七、不可抗力

甲乙任何一方因受不可抗力的影响而不能执行本合同时，应及时向对方通报不能履行或不能完全履行的理由，在取得有关机构证明以后，按其对履行合同影响的程度，由双方协商决定是否解除协议，或部分免除履行协议的义务，或延期履行协议。双方对此互不承担违约责任。

受影响一方应在不可抗力情形发生之日起10日内，向合同相对方提供相应

的书面证明材料。合同相对方收到通知后，应尽可能采取适当措施减轻不可抗力事件对履行本合同的影响，没有采取适当措施致使损失扩大的，不得就扩大的损失要求赔偿。

受不可抗力影响而不能按期履行的一方，应在不可抗力终止或影响消除后尽快通知对方。

本合同中“不可抗力”，是指不能预见、不能避免且不能克服的客观情况，包括但不限于在本合同签署后发生的不可预见或可预见但不可避免且超越合同双方可以控制，阻碍该合同部分或全部履行的地震、风暴、火灾、洪水、战争及其它重大自然、人为灾害、公共卫生安全或政策变化、疫情、政府行为如征收、征用等，或社会异常事件如罢工、骚乱等。凡是发生了所罗列的事件即构成不可抗力，凡是发生协议中未列举的事件，不构成不可抗力事件。若双方对其含义发生争执，则由受理案件的仲裁机关或法院根据合同的含义解释发生的客观情况是否构成不可抗力。

八、保密事项

除本合同另有约定外，乙方因承接本合同约定项目所知悉的该项目信息或甲方信息，以及在项目实施过程中所产生的与该项目有关的全部信息、成果文件等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》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。未经甲方事先书面同意，乙方不得向任何第三方披露或供其使用，也不得在本合同约定事项范围之外自行使用。

乙方必须与甲方签订《安全保密协议》，详细内容参见附件 3。同时，项目团队全体成员应签订网络安全服务人员保密协议。

乙方（含乙方工作人员）因违反保密义务给甲方造成损失的，应当承担相应的法律责任，并赔偿甲方相应的经济损失。如损失数额无法确定的，乙方同意按照人民币【5】万元赔偿甲方的损失。

本条款长期有效，不因合同终止、解除或无效而失效。

如果发现以上保密内容被泄露或者因为过失泄露，乙应当采取有效措施防

止泄密进一步扩大，并及时向甲方报告。

九、合同的变更和解除

1.甲乙双方不得随意解除本合同，因解除合同给对方造成损失的，除不可归责于该当事人的事由外，应当赔偿损失。如乙方随意要求解除该合同，必须提前【5】日以书面形式通知甲方，在获得甲方书面同意后，退还甲方已支付的全部款项，同时应向甲方支付服务费总金额【5】%的违约金，还应赔偿因解约给甲方造成的全部损失。

2.甲方因特殊情况或其他合法正当原因要求乙方停止本合同约定的服务的，应提前【5】日书面通知乙方，乙方在收到甲方该书面通知后应立即停止提供服务，甲方不承担违约责任。对于乙方收到甲方该书面通知前已经完成的服务成果部分，甲方应根据乙方工作量参照本合同约定的费用标准向乙方支付对应的服务费用。

3.甲方依本合同约定发出了书面通知但乙方仍然继续提供服务的，后续有关费用由乙方承担。

4. 甲方行使单方解除权的，本合同自乙方收到书面解除通知之日起解除。合同解除后，除依约承担违约责任外，乙方有义务在甲方规定的交接期限内提交相关项目资料并配合甲方重新选择服务商，并与甲方选定的服务商进行工作交接。

十、违约责任

1.除不可抗力的自然及社会原因外，甲乙双方应严格遵守本合同的规定，否则，违约方需承担违约责任。

2. 除本合同另有约定外，执行双方若未经对方允许，单方面终止本合同的，则另一方可依法追究违约方责任。

3.乙方未按照本合同约定期限完成委托服务，每逾期一日，需承担服务费总金额【0.1】%的违约金。逾期达【10】日仍未完成的，甲方有权解除本合同，乙方应返还甲方已经支付的服务费，并要求乙方支付服务费总金额【5】%的违约金。

4.乙方提供的服务若侵犯第三方著作权、商标权、专利权等合法权益，给甲方造成损失的，乙方承担服务费总金额【5】%的违约金。同时甲方还有权视情况选择解除本合同，乙方应返还甲方已经支付的服务费，并要求乙方支付服务费总金额1%的违约金。

5.乙方未经甲方同意，擅自将本合同义务全部或部分转让给第三方的，甲方有权解除本合同，乙方应返还甲方已经支付的服务费，并向甲方支付服务费总金额【10】%的违约金。

6.乙方提供服务不符合本合同约定标准或甲方要求，或存在其他违约行为的，甲方有权要求乙方立即纠正，乙方纠正后仍不符合要求或未按时纠正的，甲方有权解除本合同，乙方应返还甲方已经支付的服务费，并要求乙方支付服务费总金额5%的违约金。

7.乙方未按照本合同约定提供专业项目组成人员或擅自更换人员，乙方应承担服务费总金额【5】%的违约金。

8. 乙方因违约而给甲方造成损失的，乙方还应赔偿损失。该损失包括但不限于实际损失、合同履行后可以获得的利益和诉讼费、仲裁费、合理的调查费、律师费、交通费、差旅费等有关费用。

9.对于乙方因违约而应向甲方支付的违约金及赔偿金等，甲方有权从应付合同价款中予以扣除，不足扣除的，乙方应予以补足。

10. 乙方未落实国家和北京市相关法律法规，做好网络和数据安全防护工作，以及未落实甲方要求，在规定时限内，完成信息系统整改、漏洞修复和安全加固工作的，乙方应当向甲方支付合同总额10%的违约金，违约金不足以弥补甲方损失的，乙方应承担赔偿责任。

11.如乙方发生违反本合同约定的其他义务的，每发生一次，乙方应向甲方支付服务费总金额【1】%的违约金；如发生【3】次以上或经甲方通知后【10】日内乙方仍然拒不整改的，甲方有权解除本合同，乙方应返还甲方已经支付的全部款项，并向甲方支付服务费总金额【5】%的违约金，如因此给甲方造成损失的，乙方还应承担全部赔偿责任。

十一、争议解决

甲、乙双方因本合同发生争议，应当友好协商解决；协商不成，双方均可向甲方住所地有管辖权的人民法院提起诉讼。

当产生任何争议及任何争议正在协商或诉讼时，除争议事项外，双方将继续执行本合同未涉争议的其他部分。

十二、合同生效及其他

1.本合同自甲乙双方法定代表人或授权代表签字并加盖双方单位公章后生效。本合同一式陆份，甲方执肆份，乙方执贰份，具有同等法律效力。

2. 组成合同的各项文件应互相解释，互为说明，解释合同的优先顺序如下：（1）合同及附件（安全保密协议（附件 2）、网络安全服务人员保密协议（附件 3）、供应商口令安全承诺书（附件 4））；（2）中标通知书；（3）招标文件；（4）投标文件；（5）其他合同文件。上述各项合同文件包括双方就该项合同文件作出的补充和修改，属于同一类内容的文件，应以最新签署的为准。

3.甲方需追加与本合同标的相同的工作的，在不改变本合同其他条款的前提下，可以与乙方协商签订补充协议，但所有补充协议的总金额不得超过本合同总金额的百分之十。

4.本合同附件及补充协议是本合同不可分割的组成部分，与本合同具有同等法律效力。

甲方（盖章）：北京市应急指挥保障中心

法定代表人或授权代表（签字）：

日期：2026年 8月 3 日

乙方（盖章）：北京金山云网络技术有限公司

法定代表人或授权代表（签字）：

日期：2026年 8 月 3 日

附件 1：采购需求、项目验收程序及标准
附件 2：团队人员表
附件 3：安全保密协议
附件 4：网络安全服务人员保密协议
附件 5：供应商口令安全承诺书

附件 1 采购需求、项目验收程序及标准

一、采购需求

商用密码服务包括基于国密算法的远程安全接入、密钥管理服务、数据加密服务、签名验签服务、虚拟密码机（VSM)服务、密码 API 接口服务、国密 SSL 证书、USBkey。本次主要为安全生产监管综合信息平台（一期）——北京市安全生产检查和隐患治理信息子系统提供密码服务。

1.基于国密算法的远程安全接入

支持在终端与平台之间建立 SSL VPN 安全通道，支持对接入网络的终端设备进行安全认证，支持客户端与服务端之间数据加密传输，支持对终端设备的权限控制；支持与安全浏览器建立合规的 HTTPS 安全通道。。

2. 密钥管理服务

提供密钥生成、密钥更新、密钥备份与恢复、密钥归档、密钥销毁等密钥全生命周期管理。。

3. 数据加密服务

提供数据加解密和完整性保护服务，实现数据库加解密、文件加解密。支持数据库字段级或表级加密与完整性保护；支持文件数据加密与完整性保护，支持细粒度数据加密控制，支持数据加密吞吐率 100Mbps。。

4. 签名验签服务

提供数字签名与签名验证服务功能，用于身份认证时签名数据验证，基于数字签名技术实现数据的完整性保护，支持 SM2 签名速度不低于 700 次/秒。。

5. 虚拟密码机（VSM)服务

基于符合国密要求的密码算法和密钥安全管理机制，提供密钥产生、使用以及基础密码运算服务功能，每实例 4C8G。。

6. 密码 API 接口服务

把密码调用接口进行业务级封装形成统一密码服务 API 和 SDK，对云平台上所有业务应用提供统一的密码服务，提供多租户的密码服务能力。

7. 国密 SSL 证书

国密 SM2 服务器证书 SSL V3 型，支持通配，需要 IP 验证可以是 80/443 端口，域名验证可以选择邮箱或 DNS；根据浏览器识别地址栏显示绿标；证书主题显示：单位名称和所在省市；配套购买 RSA 算法的 SSL 证书。

8. USBkey

PC 终端密码支撑服务，PC 端用户身份认证。

业务系统每个用户配发一个。

具体采购名称、服务期、数量、功能描述如下：

序号	名称	服务期（月）	数量	功能描述
1	基于国密算法的远程安全接入	12	2	支持在终端与平台之间建立 SSL VPN 安全通道，支持对接入网络的终端设备进行安全认证，支持客户端与服务端之间数据加密传输，支持对终端设备的权限控制；支持与安全浏览器建立合规的 HTTPS 安全通道。
2	密钥管理服务	12	1	提供密钥生成、密钥更新、密钥备份与恢复、密钥归档、密钥销毁等密钥全生命周期管理。
3	数据加密服务	12	1	提供数据加解密和完整性保护服务，实现数据库加解密、文件加解密。支持数据库字段级或表级加密与完整性保护；支持文件数据加密与完整性保护，支持细粒度数据加密控制，支持数据加密吞吐率 100Mbps。
4	签名验签服务	12	1	提供数字签名与签名验证服务功能，用于身份认证时签名数据验证，基于数字签名技术实现数据的完整性保护，支持 SM2 签名速度不低于 700 次/秒。
5	虚拟密码机（VSM）服务	12	1	基于符合国密要求的密码算法和密钥安全管理机制，提供密钥产生、使用以及基础密码运算服务功能，每实例 4C8G。
6	密码 API 接口服务	12	1	把密码调用接口进行业务级封装形成统一密码服务 API 和 SDK，对云平台上所有业务应用提供统一的密码服务，提供多租户的密码服务能力。
7	国密 SSL 证书	12	1	国密 SM2 服务器证书 SSL V3 型，支持通配，需要 IP 验证可以是 80/443 端口，域名验

				证可以选择邮箱或 DNS；根据浏览器识别地址栏显示绿标；证书主题显示：单位名称和所在省市；配套购买 RSA 算法的 SSL 证书。
8	USBkey	12	1	PC 终端密码支撑服务，PC 端用户身份认证。业务系统每个用户配发一个。

二、项目验收程序及标准

完成商用密码服务开发部署，通过第三方密评且结论合格，乙方提交完整资料，运行期间无重大故障、故障修复率 100%。

乙方提交申请与资料，甲方组织专家审核，组织现场测试核查，形成相关资料，包括但不限于实施方案、部署配置清单、产品管理操作手册、服务集成规范、上线保障方案、运维服务方案、项目工作总结、日常巡检（每月至少 1 次，重要期间按甲方要求开展）、故障处置、突发事件处置等。不合格项需整改后重新验收。

序号	验收条目	验收内容
1	密码资质与算法合规	合规
2	核心密码功能达标	功能实现
3	性能与防护达标	性能安全
4	文档与配套报备完整	文档和服务完整

附件 2 团队人员表

序号	姓名	职称	学历	专业	从业资格	相关工作年限	备注
1	朱鑫亨	/	本科	计算机科学与技术	高级/信息系统项目管理师	9	/
2	池增坤	/	本科	计算机科学与技术	系统架构设 计师（高级）	16	/
3	陈映桥	/	本科	信息安全	信息安全工程师(CISP)	5	/
4	魏志军	/	本科	计算机网络技术	中级/网络工程师	16	/

附件 3 安全保密协议

安全保密协议

甲 方：北京市应急指挥保障中心

乙 方：北京金山云网络技术有限公司

为了保护所属信息系统所涉及的保密信息，明确双方的权利义务，甲乙双方根据《网络安全法》《数据安全法》《网络数据安全管理条例》和《个人信息保护法》《互联网政务应用安全管理规定》等相关法律，在平等自愿、协商一致的基础上，就信息安全服务项目—第四包：商用密码应用服务技术服务过程中已经或将要知悉对方的相关保密信息达成以下协议：

第一条 安全要求

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

二、乙方必须制定合理的措施，对运维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

本协议称的“保密信息”是指，双方在订立和履行合同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：一切与政府工作相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、文档及技术指标等。

三、其他保密信息：包括但不限于技术服务中获取的有关数据、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、图形的或其他任何形式的信息。

第三条 协议的生效

本协议自双方法定代表人或授权代表签字并加盖单位合同章或者公章之日起

生效。

第四条　安全保密期限

本协议约定的保密责任期为伍年。

第五条　保密义务人

本协议项下保密义务人为乙方单位及乙方负责本项目的技术保障服务的员工。

第六条　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运维工作有关的用途。

2．除直接参与运维工作的人员之外，不得将保密信息透露给其他无关人员和任何第三方。

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运维工作的人员，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、U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；必须访问的人员，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。

第七条　保密信息的交回

一、信息安全服务项目—第四包：商用密码应用服务技术保障服务工作终止后，乙方应按照甲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、当甲方以书面形式要求交回保密信息时，乙方接到通知后应当立即交回

所有的书面或其他有形的保密信息以及所有的描述和概括保密信息的文件。

三、未经甲方书面许可，乙方不得丢弃和自行处理保密信息。

第八条　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的有效的补偿措施，以防止泄密范围继续扩大，同时还应向守约方支付合同总金额10%的违约金。

第九条　争议的解决

因履行本协议而发生的或与本协议有关的一切争议，双方应协商解决，协商不成的，向甲方住所地有管辖权的人民法院提起诉讼。

第十条　其他

本协议未尽事宜，甲、乙双方协商一致后另行签订补充协议。

甲方：北京市应急指挥保障中心　　乙方：北京金山云网络技术有限公司

法定代表人或授权代表：

日期：2026 年 8 月 3 日

法定代表人或授权代表：

日期：2026 年 8 月 3 日

附件 4 网络安全服务人员保密协议

网络安全服务人员保密协议

我单位承担了北京市应急指挥保障中心“信息安全服务项目—第四包：商用密码应用服务，本人在驻场服务、系统开发和维护等活动中，履行以下安全保密义务：

一、严格执行《中华人民共和国网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》《互联网政务应用安全管理规定》等相关法律法规，保守信息系统相关秘密，维护信息系统安全。杜绝篡改信息系统源代码、程序以及考生个人信息、成绩等操作和行为。

二、严格遵守《北京市应急管理局信息安全管理手册》、《北京市应急管理局第三方人员安全管理规定》、《北京市应急管理局介质安全管理制度》和《北京市应急管理局机房管理规范》等安全管理制度，在驻场服务、技术支持、系统维护等活动中，诚实守信，严于律己。

三、进出市应急管理局办公场所和机房，履行登记审批程序，严格按规范流程开展各项实施工作，禁止一切非正常用电和施工行为，杜绝引发触电、短路、火灾、伤害等安全事故。

四、授权接入市电子政务外网的终端设备禁止开启无线网络共享功能，禁止将无线路由器（含便携式无线设备）接入市电子政务外网。

五、服务过程中不随意探听市应急管理局内部信息或翻阅办公场所的文件资料。

六、采取内部措施，不得以任何方式直接或间接地向任何个人、企业、机关、或其他社会团体使用或泄露与市应急管理局有关的保密或专有信息。

我承诺履行上述义务和责任。如因我原因发生问题，将承担所引起的经济、法律等全部责任。

单位负责人签字：

（单位公章）

2026 年 8 月 3 日

承 诺 人 签 字：

2026 年 8 月 3 日

网络安全服务人员保密协议

我单位承担了北京市应急指挥保障中心“信息安全服务项目—第四包：商用密码应用服务，本人在驻场服务、系统开发和维护等活动中，履行以下安全保密义务：

一、严格执行《中华人民共和国网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》《互联网政务应用安全管理规定》等相关法律法规，保守信息系统相关秘密，维护信息系统安全。杜绝篡改信息系统源代码、程序以及考生个人信息、成绩等操作和行为。

二、严格遵守《北京市应急管理局信息安全管理手册》、《北京市应急管理局第三方人员安全管理规定》、《北京市应急管理局介质安全管理制度》和《北京市应急管理局机房管理规范》等安全管理制度，在驻场服务、技术支持、系统维护等活动中，诚实守信，严于律己。

三、进出市应急管理局办公场所和机房，履行登记审批程序，严格按规范流程开展各项实施工作，禁止一切非正常用电和施工行为，杜绝引发触电、短路、火灾、伤害等安全事故。

四、授权接入市电子政务外网的终端设备禁止开启无线网络共享功能，禁止将无线路由器（含便携式无线设备）接入市电子政务外网。

五、服务过程中不随意探听市应急管理局内部信息或翻阅办公场所的文件资料。

六、采取内部措施，不得以任何方式直接或间接地向任何个人、企业、机关、或其他社会团体使用或泄露与市应急管理局有关的保密或专有信息。

我承诺履行上述义务和责任。如因我原因发生问题，将承担所引起的经济、法律等全部责任。

单位负责人签字：

（单位公章）

2026年8月3日

承诺人签字：

2026年8月3日

网络安全服务人员保密协议

我单位承担了北京市应急指挥保障中心“信息安全服务项目—第四包：商用密码应用服务，本人在驻场服务、系统开发和维护等活动中，履行以下安全保密义务：

一、严格执行《中华人民共和国网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》《互联网政务应用安全管理规定》等相关法律法规，保守信息系统相关秘密，维护信息系统安全。杜绝篡改信息系统源代码、程序以及考生个人信息、成绩等操作和行为。

二、严格遵守《北京市应急管理局信息安全管理手册》、《北京市应急管理局第三方人员安全管理规定》、《北京市应急管理局介质安全管理制度》和《北京市应急管理局机房管理规范》等安全管理制度，在驻场服务、技术支持、系统维护等活动中，诚实守信，严于律己。

三、进出市应急管理局办公场所和机房，履行登记审批程序，严格按规范流程开展各项实施工作，禁止一切非正常用电和施工行为，杜绝引发触电、短路、火灾、伤害等安全事故。

四、授权接入市电子政务外网的终端设备禁止开启无线网络共享功能，禁止将无线路由器（含便携式无线设备）接入市电子政务外网。

五、服务过程中不随意探听市应急管理局内部信息或翻阅办公场所的文件资料。

六、采取内部措施，不得以任何方式直接或间接地向任何个人、企业、机关、或其他社会团体使用或泄露与市应急管理局有关的保密或专有信息。

我承诺履行上述义务和责任。如因我原因发生问题，将承担所引起的经济、法律等全部责任。

单位负责人签字：

（单位公章）

2026年 8月 3日

承 诺 人 签 字：

2026年 8月 3日

网络安全服务人员保密协议

我单位承担了北京市应急指挥保障中心“信息安全服务项目—第四包：商用密码应用服务，本人在驻场服务、系统开发和维护等活动中，履行以下安全保密义务：

一、严格执行《中华人民共和国网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》《互联网政务应用安全管理规定》等相关法律法规，保守信息系统相关秘密，维护信息系统安全。杜绝篡改信息系统源代码、程序以及考生个人信息、成绩等操作和行为。

二、严格遵守《北京市应急管理局信息安全管理手册》、《北京市应急管理局第三方人员安全管理规定》、《北京市应急管理局介质安全管理制度》和《北京市应急管理局机房管理规范》等安全管理制度，在驻场服务、技术支持、系统维护等活动中，诚实守信，严于律己。

三、进出市应急管理局办公场所和机房，履行登记审批程序，严格按规范流程开展各项实施工作，禁止一切非正常用电和施工行为，杜绝引发触电、短路、火灾、伤害等安全事故。

四、授权接入市电子政务外网的终端设备禁止开启无线网络共享功能，禁止将无线路由器（含便携式无线设备）接入市电子政务外网。

五、服务过程中不随意探听市应急管理局内部信息或翻阅办公场所的文件资料。

六、采取内部措施，不得以任何方式直接或间接地向任何个人、企业、机关、或其他社会团体使用或泄露与市应急管理局有关的保密或专有信息。

我承诺履行上述义务和责任。如因我原因发生问题，将承担所引起的经济、法律等全部责任。

单位负责人签字：

（单位公章）

2026 年 8 月 3 日

承 诺 人 签 字：

2026 年 8 月 3 日

附件 5 供应商口令安全承诺书

供应商口令安全承诺书

为加强北京市应管理局网络和数据安全管理，确保信息系统、数据安全稳定运行，本司（公司名称：北京金山云网络技术有限公司，代表人姓名：邹涛），在此郑重承诺严格遵守以下口令（密码）安全规定：

一、复杂性。本司承诺，对运维使用的各类账户口令（包括但不限于系统登录、数据库、中间件和软硬件设备、VPN运维账号、电子邮箱等）和系统中存在的用户设置密码复杂性强制要求，即包含大小写字母、数字及特殊字符，且长度不少于18位。本司将定期（至少每30天）更换口令，避免使用容易被猜测或破解的简单口令，如生日、电话号码、连续数字或字母等。

二、保密性。本司承诺，对系统相关的所有口令信息严格保密，不向任何未经授权的人员透露。同时，本司将采取必要措施防止口令信息被窃取或泄露，包括但不限于：将口令记录在不易被他人访问的地方，不使用公共设备或不安全网络环境进行运维操作。

三、单一用途。本司承诺，明确专人负责账号和密码管理，及时删除人员变动或者调整的账号。不在多个账户或系统上重复使用同一口令，以降低某个账户被攻破后，其他账户也面临风险的可能性。

四、合规性。本司承诺，遵守国家法律法规及公司关于网络安全、数据保护的所有规章制度，对于因违反本承诺书规定而造成的任何信息安全事故或损失，本司愿意承担相应的法律责任及公司内部责任。

五、应急响应。本司承诺，在发现账户口令可能泄露或被盗用的情况下，立即按照北京市应急管理局规定的应急响应流程进行报告和处理，竭尽全力将网络安全事件带来的影响降到最低。

本承诺书自盖章签字之日起生效，本司将始终遵守上述承诺。如因弱口令引发网络和数据安全问题，本公司将承担全部责任。

承诺公司（盖章）：北京金山云网络技术有限公司

代表人（签字）：邹涛

2026 年 3 月 3 日