中共北京市委网络安全和信息化委员会办公室2026年

网络安全运维合同书

甲方：中共北京市委网络安全和信息化委员会办公室

乙方：北京安信天行科技有限公司

签订时间：2026.5.9

地点：北京

网络安全运维及保障合同

中共北京市委网络安全和信息化委员会办公室(甲方) 2026年**信息化运维及安全保障项目经费**经北京中城建华工程咨询有限公司(招标机构)以2026ZCZB00013/01号招标文件组织招标，经评标委员会评定，北京安信天行科技有限公司为中标商（乙方）。双方同意按照下面的条款和条件，签署本合同。

1、合同文件

下列文件构成本合同的组成部分，应该认为是一个整体，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

c. 投标文件 (含澄清文件)

d. 招标文件 (含招标文件补充通知)

e. 2026年网络安全运维及保障-保密协议

2、合同总价

本合同总价为：¥1,900,000.00元人民币， 大写：壹佰玖拾万元整，此价格含税。

3、本合同的服务期限和实施地点

服务周期：服务周期为生效之日起一年

实施地点：北京

4、付款方式

甲方在合同签订后一个月内向乙方支付合同首款（大写：壹佰壹拾捌万元整 ¥1,180,000.00），甲方待项目结束后完成本项目考评验收，并根据考评结果于验收通过后一个月内向乙方支付尾款(大写：柒拾贰万元整 ¥720,000.00)。甲方具体支付进度以财政拨付为准，因财政原因导致甲方延迟支付的，甲方不承担违约责任。乙方应向甲方提供符合甲方要求的相应金额的税务发票。

甲方发票抬头信息如下：

单位名称：中共北京市委网络安全和信息化委员会办公室

纳税人识别号：11110000MB03598814

地　　址：北京市通州区留庄路4号院1号楼

5、服务内容

乙方须统筹甲方总体网络安全，负责整体网络安全运维及保障，持续开展监测、预警、处置等安全保障工作，指导各系统运维服务商实施系统安全加固等。

乙方须针对甲方云主机、云上系统和应用，近400台办公电脑，有线网络和无线网络，提供网络安全运维及保障服务（具体数量以甲方实际提供为准）。全面加强甲方网络安全、系统安全、信息安全、应用安全、终端安全，保障网络、系统和服务器安全，加强系统和应用软件安全管理和升级维护，实施系统上线前安全检查等，按照等保三级要求全面提高甲方网络和信息安全保障水平。详见《附件：服务内容及要求》

6、绩效考评

为进一步提高安全服务工作成效，双方同意对安全服务工作进行考评，考评结果与服务费挂钩，具体考评办法和考评结果运用方式见《北京市委网信办信息化项目运维服务验收管理办法》。

7、双方的权利和义务

7.1 甲方的权利和义务

1、本合同期内，甲方应向乙方提供完成服务所需的资料、文件及工作条件。

2、甲方应根据合同性质，承担乙方完成服务所需的经费。

3、除本合同另有约定外，在乙方按约定完成服务时并经甲方验收合格时，甲方应按约定时间、方式支付报酬，并及时结算费用。

4、本合同期内，甲方有权要求乙方按照甲方要求对运维工作进行调整，乙方应积极配合。

5、甲方有权要求乙方随时向甲方汇报服务过程中出现的问题，有权要求乙方配合甲方工作，提供与服务内容有关的相关信息。

7.2 乙方的义务

1、乙方保证所有服务项目符合国家标准以及行业标准。

2、乙方严格遵守中华人民共和国法律、法规及合同对有关技术资料及技术的要求。

3、乙方确保其提供的本合同项下的所有服务所涉及的产品、技术、资料不会侵

犯第三方的知识产权、所有权及其他任何权利，否则经甲方书面告知并同意乙方全权处理且予以配合后，乙方将承担由此造成的一切经济损失和法律责任。

4、乙方派出人员在甲方服务期间，因故意或过失给甲方造成相应损失的，乙方应承担全部的赔偿责任。

5、乙方有权要求甲方提供完成本项目服务必要的帮助和工作环境。

6、乙方在按合同约定完成服务的情况下，有权要求甲方支付相应的服务费用。

8、知识产权

乙方保证乙方提供的服务不存在任何侵犯第三方知识产权的情形。如果第三方声称乙方向甲方提供的服务侵犯其知识产权，并已就此对甲方或乙方提起（包括威胁提起或很可能提起)法律诉讼程序或知识产权行政执法程序(以下简称“侵权诉讼”），则知悉上述事项的一方应立即通知合同对方，甲方有权：

(1)暂停履行对侵权诉讼所涉服务的采购或支付义务直至侵权诉讼完全解决，并要求乙方自担费用向甲方提供与该第三方协商、诉讼、和解所需的一切协助(包括但不限于向甲方提供证明侵权不存在的各类证据、派出人员参加协商、诉讼或会谈等）；

(2) 甲方有权选择与该第三方达成和解，并由乙方支付和解协议所约定的全部费用以及甲方因侵权诉讼而遭受的全部损失和费用（包括但不限于诉讼/仲裁费、律师费、交通费、通讯费、差旅费、对第三方的损害赔偿金、行政处罚罚款、获取该服务相应使用许可的费用、因停止使用或修改、替换侵权威胁所涉及的服务而遭受的损失等）。如果甲方选择继续参加侵权诉讼法律程序，乙方应当赔偿甲方因侵权诉讼及履行生效法律裁判而需支付的费用和遭受的损失，但生效法律裁判认定乙方服务不存在侵犯第三方知识产权情形的除外。

(3) 甲方在乙方提供的服务基础上开发、研制形成的技术成果（包括但不限于程序、文件、资料等）的知识产权归甲方所有。

(4) 不论本合同是否解除或终止，本条款独立适用。

9、保密义务

（1）乙方应对其知晓的甲方的商业、技术、市场、管理、人事、财务等任何方面的信息和资料予以保密，未经甲方事先书面同意，乙方不得披露、使用或以任何方式处置上述信息、资料，并应促使其员工、关联方承担相同保密义务，如

果乙方员工、关联方违反上述保密义务，视为乙方违反保密义务，并适用本条第2点的约定。

（2）乙方同意，保密义务为永久期限，违反保密义务的，应当对甲方因此所遭受的损失承担全部赔偿责任。如果乙方在本合同有效期内违反保密义务，甲方有权单方提前终止本合同。

（3）不论本合同是否解除或终止，本条款独立适用。

（4）具体保密要求详见《附件2：保密协议》。

10、不可抗力

（1）由于发生不可抗力事件（如战争、暴动、严重火灾、水灾、台风、地震、政府行为和禁令等事件），致使合同任一方不能履行合同义务时，遭受不可抗力事件影响的一方负有自不可抗力事件发生之日起15日内尽快通知合同对方以减轻可能给对方造成的损失，并应当在合理期限内提供证明。

（2）遭受不可抗力事件影响的一方在履行前述义务后免除违约责任。但其合同义务不因此免除。经合同双方协商同意，合同履行时间可合理延长，延长时间相当于因事件发生受到影响的时间。

11、违约责任

（1）乙方违反本合同约定义务的，甲方有权要求乙方在指定期限内采取弥补措施，乙方未能弥补的，视为乙方违约，乙方应向甲方支付相当于合同总金额百分之三的违约金。乙方延期履行的，每延期一日，还应按合同总金额千分之三的比例向甲方支付延期履行违约金。

（2）因乙方过错造成甲方或第三方损失的，乙方应赔偿甲方和第三方全部损失。

（3）甲方有权直接在未支付的合同总金额中扣除本条约定的违约金及赔偿金。

12、争议管辖

本合同项下发生的争议，由双方当事人协商解决；协商不成的，任何一方有权向甲方住所地人民法院提起诉讼。

13、通知与送达

任何一方根据本合同规定向另一方发出的通知应以书面形式作出，并以邮寄/快递、传真、专人送达方式发送。如以邮寄/快递方式发送，以邮寄/快递回执

上注明的收件日期为送达日期。如以传真方式发送，收到传真机发出的确认信息后，视为送达。如专人送达，被送达人签署后，视为送达。各方联系信息以本合同文末所列为准，一方联系信息变化后，该方应在联系信息变化之前将变化情况书面通知对方，否则该方应自行承担相应的风险、责任和后果。

14、合同生效

本合同自双方负责人/法定代表人或授权代表签字并加盖公章之日起生效。本合同一式柒份，甲方执肆份，乙方执三份，具有同等法律效力。本合同的任何变更、补充或修改，应由双方协商一致并签署书面补充协议，与本合同具有同等法律效力。

15、其他

本合同附件作为本合同内容的一部分，与本合同具有同等法律效力。（以下无正文）

（本页无正文，为《中共北京市委网络安全和信息化委员会办公室2026年网络安全运维合同书》签署页）

甲方（盖章）：中共北京市委网络安全和信息化委员会办公室

负责人或授权代表(签字)：

时　　间：2026年5月9日

地　　址：北京市通州区留庄路4号院1号楼

邮政编码：100010

电　　话：67093980

开户银行：北京银行景山支行

账号：01090314200120112002746

乙方（盖章）：北京安信天行科技有限公司

法定代表人或授权代表(签字)：

时　　间：2026年5月9日

地　　址：北京市海淀区北四环西路68号

邮政编码：100080

电　　话：58045643

开户银行：**北京银行双清苑支行**

账　　号：01090327800120102315974

附件 1：服务内容及要求

服务类别	服务内容
虚拟化安全服务要求	**云主机安全威胁动态监测服务：** 对办内云主机开展安全威胁动态监测服务，通过对云主机上的各类安全事件进行实时监测、分析、预警和响应，以确保云主机的安全性和稳定性。定期提供安全报告和合规性评估，详细记录云主机的安全状况、威胁事件以及采取的应对措施等信息，帮助了解整体云主机安全态势并持续优化安全策略。 **云主机脆弱性安全检测服务：** 每季度对办内云上系统主机开展1次全面的安全漏洞检测与评估，旨在及时发现并修复潜在的安全隐患，提升云主机的整体安全防护能力。在检测过程中，应基于漏洞数据库和最新的安全威胁情报，对云主机可能存在的安全漏洞进行精准识别，包括但不限于常见的Web 漏洞、系统漏洞、应用漏洞以及配置不当等安全风险。
业务系统安全服务要求	**Web 安全漏洞检测分析服务：** 对办内 Web 应用进行全面的安全检测与评估，发现潜在的应用层安全隐患，提供及时、准确、有效的安全建议和改进措施。 **系统渗透测试服务：** 对办内信息系统开展渗透测试服务，利用安全扫描工具对系统进行非破坏性质的模拟入侵者攻击，挖掘其中安全风险，协助修补漏洞，增强抵御黑客攻击的能力。
	实战攻防演练服务： 为办内组织开展 1 次通实战化红蓝对抗，检测是否存在系统漏洞、安全设备策略是否有缺陷、监测手段是否有效等，针对性提出整改计划和方案，协助进行整改，同时对对抗过程中发现的问题进行总结和完善安全自查和整改，为后续工作积累经验。
	重要应用安全监控服务； 通过远程监控系统为办内互联网重要应用提供远程安全监控和实时告警服务，一旦系统遇到风险状况后，及时通知相关人员，并提供专业的解决方案建议，整体掌握互联网系统的风险状况及安全趋势。

	应用日志分析服务： 对办内应用运行日志等进行统一采集和存储，并且通过互联网大数据方法对日志进行关联分析和统计汇总，实现对信息系统日志/事件的全面管理。
数据安全服务要求	**数据安全评估及分析服务：** 对办内信息系统数据资产进行全面的梳理和分类，在此基础上，利用专业的安全评估工具和方法，对系统和应用程序进行全面的风险评估，发现可能存在的安全弱点和安全隐患。同时，对系统等访问控制和权限管理进行严格的审查，确保只有经授权的人员能够访问敏感数据和资源。
	办公网数据安全防泄漏监测服务： 依托第三方监控系统为办内办公网提供终端防泄露监测服务，对终端侧数据拷贝、网络侧数据外发、办公应用侧数据分享及物理输出等关键场景的实时监测，一旦发现违规操作或敏感数据泄漏风险，立即触发分级告警，完整留存数据流转日志、操作轨迹等审计信息，为事后追溯、风险排查及合规审计提供可靠依据，全面防范内部人员无意泄露、违规外传等数据安全风险，保障办公网核心数据资产的保密性与安全性。需提供原厂授权产品。
	云上系统数据安全防泄漏监测服务： 为办内云上业务系统提供数据防泄露监测分析服务，重点针对云上系统数据跨网传输、数据外发等网络流量进行实时监测，及时识别敏感数据违规外发、批量数据外泄等风险行为，触发分级预警提醒；完整留存数据外发敏感字段、传输时间、操作主体等关键审计信息，保障云上数据资产的保密性与安全性。需提供原厂授权产品。
安全运营服务要求	**一体化安全运营服务：** 通过对办内提供综合性的安全运营管理服务，构建一套统一的安全管理体系，将安全监测、预警、响应、处置等各个环节紧密衔接起来，形成闭环的安全运营流程。利用先进的安全监测工具和技术手段，对本地及云上业务系统进行全天候、全方位的监测和分析，实时捕捉和识别潜在的安全威胁和异常行为。
	重点时期安全保障服务： 在节假日期间（如：春节、五一、国庆等期间）及重要活动时期（如全国两会、HW 等），为办内提供 7x24 小时现场值守服务和重点检查等服务，以保障网络信息系统稳定、安全为主要目标，加强人员及技术力量投入，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，确保办内基础设施、业务系统等正常运行。

	应急响应服务 根据上一年监测发现的安全事件，结合国家、地区和行业等信息安全政策和标准，协助办内修订网络安全应急预案，明确应急响应组织以及预防、预警机制，针对可能的安全事件编制规范的应急处理流程。 根据修订的应急预案，协助开展模拟应急演练，使得相关人员了解安全事件应急流程和自己的责任，在安全事件发生时，能够有条不紊开展工作，最大程度降低安全事件带来的负面影响和损失。 提供全年 7x24 小时安全事件应急响应服务，排查攻击痕迹，进行取证及修复。
	安全培训服务： 为办内相关人员提供基础安全意识培训，有利于提升人员的信息安全意识，使得更多人员参与到信息安全建设和维护工作中，确保办内信息安全工作得到良好的推广，信息防护整体水平得到提升。
授权更新服务要求	**瑞星防病毒授权服务（一年）** 对近 400 台办公电脑杀毒以及病毒监控服务。需提供原厂授权及专业人员现场服务。
采购标的需满足的服务标准、期限、效率等要求	1. 在合同签订之日起提供为期 1 年的持续的网络安全运维服务； 2. 在 1 个自然月内完成驻场和其他工作交接和实施。驻场人员不少于 5 人，实行项目经理负责制，选派专人担任项目经理，服务期内原则上不允许更换项目经理，更换其他驻场人员应经采购人同意。 3. 工作时间要求：提供每周 7*24 小时服务支持。工作日提供 5 人 5 天*8 小时驻场服务。工作日 8 小时外及周末根据需要随时提供工程师开展驻场服务，节假日及重大活动时期按照采购人要求提供相应数量值班工程师提供驻场服务。需要加班和值班时按照采购人的时间安排执行。 4. 响应时间要求：重要业务安全保证 10 分钟内响应，其它业务安全提供 30 分钟内响应，非工作时间 1 小时内到达现场； 5. 安全事件响应：发生安全事件时，须立即向采购人报告并采取紧急措施。 6. 安全保密要求 按照国家《保密法》等有关保密的法律法规的规定，合同约定及办内要求，加强项目人员管理，承担相应保密责任，并签订《保密承诺书》。