

河南省科学技术馆网络安全设备及服务 采购项目合同



甲方： 河南省科学技术馆

乙方： 奇安信网神信息技术(北京)股份有限公司



2026 年 6 月



甲方：河南省科学技术馆

乙方：奇安信网络安全技术（北京）股份有限公司

根据《中华人民共和国政府采购法》《中华人民共和国民法典》等法律法规，依据河南省科学技术馆网络安全设备和服务采购项目磋商文件（项目编号：豫财磋商采购-2026-229），甲乙双方协商一致，就该项目具体事宜达成以下条款：



第一部分 服务内容

第一条 乙方应按照本项目磋商文件、响应文件及本合同的约定，向甲方提供以下完整的网络安全设备与安全服务，其来源应符合国家有关规定。具体内容如下：

1. 安全设备功能及要求

乙方提供的所有安全设备均须采用国产化 CPU 和国产化操作系统。具体设备清单、数量、主要功能及关键要求如下：

(1) 网络安全准入系统（1 台）：须具备对入网终端进行深度合规检查的能力，检查项至少包括桌面屏幕保护、安装软件、杀毒软件状态、操作系统补丁等。

(2) 流量探针（1 台）：须具备网络攻击（如 SQL 注入、命令执行等）检测、SSL 解密及机器学习模型检测能力。须提供三年威胁情报与检测引擎规则升级及标准维保服务。

(3) 互联网出口下一代防火墙（2 台）：须具备应用控制、入侵防御（IPS）、防病毒等安全功能。须提供三年硬件维保及所有特征库升级服务。

(4) 安全域下一代防火墙（2 台）：须具备应用控制、入侵防御（IPS）、防病毒等安全功能。须提供三年硬件维保及所有特征库升级服务。

(5) 漏洞扫描系统（1 台）：须支持系统扫描与 Web 扫描。须提供三年漏洞特征库升级与硬件维修服务。

(6) 态势感知与安全运营综合性分析平台（1 台）：须包含威胁检测、分析、响应、资产及态势感知等模块，并具备智能分诊、资产风险评估等能力。须提供三年软硬件维保、威胁情报与漏洞知识库更新服务。该平台须能与原有网络设备及本次采购的防火墙实现联动处置。

(7) 国密算法安全中间件（1 套）：须提供基于国密算法的数据加密服务，支持数据库字段级免改造加密，并需对接甲方现有票务管理系统、志愿者小程序及集成门户。须提供三年维保服务。

2. 安全服务内容及要求

乙方应提供为期一年的综合安全服务，具体内容与要求如下：

(1) 安全规划服务：协助甲方完善网络安全顶层设计与管理体系。

(2) 网站监测服务：对甲方官网平台进行持续监测，内容包括漏洞扫描（不低于每3天1次）、内容安全监测（不低于每2小时1次）、可用性监测（不低于每2分钟1次），并提供监测报告。

(3) 应用系统安全检测服务：对甲方新建、在用及在建的系统（含移动APP）进行渗透测试与代码检测，并出具报告。

(4) 渗透测试服务：每年进行4次渗透测试，模拟攻击发现系统脆弱性，并提供报告与修复建议。

(5) 重保服务：在春节、国庆等关键时期，安排技术人员现场值守，全年总服务时长不少于240小时。值守期间负责安全监控、事件分析与应急响应，并在发生信息安全突发事件时立即调配安全技术专家赶赴现场处置。

(6) 常态化安全服务：派遣具备信息安全保障人员认证(CISAW)的工程师提供“线上+线下”服务，每季度提交报告，服务内容包括但不限于：

①安全巡检；②互联网资产测绘与暴露面收敛；③风险评估与漏洞扫描（至少1次风险评估和4次漏洞扫描）；④安全基线检查；⑤安全加固；⑥威胁检测分析与响应；⑦软件升级；⑧安全策略优化。

(7) 应急响应服务：提供7*24小时的应急响应支持，制定专项应急预案。发生重大安全事件时，须在半小时内提供现场响应；一般安全事件时，须在一小时内提供现场响应。

(8) 网络安全培训服务：提供网络安全意识与设备使用专项培训。

(9) 总体服务要求：乙方须按季度提供汇总上述服务成果的总体安全服务报告，并履行保密义务。

第二部分 合同期限

第二条 河南省科学技术馆网络安全设备及服务采购项目，乙方应于本合同生效之日起30个日历天内，完成全部安全设备的交付、部署与初步调试工作。60个日历天内，完成系统加密对接工作。安全服务期自项目最终验收合格之日起计算为期一年。

第三部分 服务标准和售后要求

第三条 乙方应指派一名拥有三年以上网络安全项目管理经验，且至少持有信息系统项目管理师（高级）、项目管理专业人员资质（PMP）、注册信息安全工程师（CISP）中两项资质证书的人员担任项目经理。项目经理简历及相关资质证明文件（包括社保证明、证书复印件）应作为合同附件。

未经甲方书面同意，乙方不得擅自更换项目经理。若甲方有合理理由认为项目经理不称职的，有权书面要求乙方在7日内更换，新项目经理的资历不得低于原项目经理。乙方应提供7×24小时技术支持热线，并在工作时间内提供现场或远程技术支持。

甲方指定项目负责人为：杨光耀；联系方式：18790281567

乙方指定项目负责人为：王一普；联系方式：13070109303

第四条 乙方提交的设备应符合响应文件中所记载的详细配置、技术参数、参数及性能，并应附有此类设备完整、详细的技术资料和说明文件，应保证所供设备是全新的、未使用过的、用一流工艺生产的，并完全符合合同规定的质量、规格和性能的要求。乙方应保证其设备在正确安装、正常使用和保养条件下，在其使用寿命期内正常运行，乙方应对由于设计、工艺或材料的缺陷而产生的故障负责。

第五条 项目免费质保期自项目最终验收合格之日起计算，为期三年。其中，第一年为安全服务期（含设备质保），后两年为设备单独质保期。安全服务期内的设备质保由乙方负责，后两年质保期内仅对硬件设备提供质保服务（不含安全服务）。在质保期内，乙方提供“7×24小时”故障响应服务。收到甲方故障通知后，乙方需在30分钟内通过电话、邮件等远程方式予以响应，并在2小时内提供明确的解决方案或故障处理进展。

质保期内，因产品本身质量问题引起的维修、更换部件及软件升级费用由乙方承担；因甲方人为损坏、不可抗力或未按规范操作导致的故障，维修费用由甲方承担。

第四部分 合同价款及付款方式

第六条 甲乙双方约定，本合同项下甲方应向乙方支付的合同总价为（含税）：（人民币大写：）壹佰壹拾叁万元整（¥1130000）。本合同款项按照以下方式支付：

1. 预付款

合同签订后15个工作日内，乙方提交经甲方书面确认的项目《安全服务实施方案》，甲方向乙方支付合同总金额的20%，即226000元（大写：贰拾贰万陆仟元整）。

2. 设备验收款

乙方完成以下全部工作后，可向甲方书面申请设备验收：

(1) 合同生效之日起 30 个日历天内，完成全部安全设备的交付、部署与初步调试工作；

(2) 合同生效之日起 60 个日历天内，完成系统加密对接工作。

甲方在收到乙方书面申请后 15 个工作日内组织设备验收。验收合格的，双方签署《设备验收确认书》，甲方于签署后 15 个工作日内向乙方支付合同总金额 30%，即 339000 元（大写：叁拾叁万玖仟元整）。

设备验收标准：按照本合同第四条约定的设备部署要求、采购文件第五章技术需求中安全设备部分及乙方响应文件相应内容执行。设备验收仅针对硬件设备及系统加密对接，不涉及安全服务的考核。

如设备验收不合格，乙方应在甲方要求的期限内整改，整改后重新申请验收，因此产生的费用由乙方承担。整改超过 30 日仍不合格的，甲方有权解除合同，乙方应返还已支付的全部款项。

3. 第一次服务考核付款

自项目最终验收合格之日起计算安全服务期。安全服务期满六个月后，甲方依据本合同附件《网络安全服务考核表》对乙方安全服务进行第一次考核。考核合格（考核总分 \geq 80 分）的，甲方于考核结果确认后 15 个工作日内向乙方支付合同总金额的 30%，即 339000 元（大写：叁拾叁万玖仟元整）；考核不合格的，甲方有权暂缓支付，并要求乙方在 30 日内完成整改。

4. 一年安全服务期满后，甲方依据本合同附件《网络安全服务考核表》对乙方安全服务进行第二次考核，考核合格后，支付合同价的 20%，即 226000 元（大写：贰拾贰万陆仟元整）。

第七条 乙方收款账户信息如下：

户 名：奇安信网神信息技术（北京）股份有限公司

开户行：招商银行北京建国路支行

账 号：110902261210404

第八条 甲方每次付款前，乙方应向甲方开具相应金额足额、正规增值税发票，甲方自收到相应价款发票经查验无误后十五个工作日内支付对应金额，开票信息如下：

名称：河南省科学技术馆

税号：1241 0000 4158 0154 78

第五部分 检查验收

第九条 设备验收

1. 乙方应当根据合同约定的时间节点完成安全设备部署及系统加密对接工作，并以书面形式提交设备验收申请及相关材料，包括但不限于：

- (1) 设备移交单（含详细设备参数、功能、序列号、安装位置）；
- (2) 设备运行报告（含部署调试记录、性能测试数据）；
- (3) 系统加密对接完成确认文件。

2. 甲方在收到验收申请后 15 个工作日内组织设备验收。验收合格的，双方签署《设备验收确认书》。设备验收仅针对硬件设备及加密对接功能，不涉及安全服务质量评价。

3. 如设备验收不合格，乙方应在甲方要求的期限内完成整改，并承担因此产生的全部费用。整改后重新申请验收，直至合格为止。

4. 如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，直至完全符合验收标准。

第十条 安全服务考核与最终验收

1. 安全服务期内，甲方依据本合同附件《网络安全服务考核表》对乙方安全服务进行两次考核（分别在第 6 个月末和第 12 个月末）。

2. 一年服务期满后，乙方应完成所有安全服务相关工作，提交项目安全服务报告汇编，包括但不限于：安全服务实施方案、安全规划服务方案、网站检测报告、网络安全培训服务报告、应用系统安全检测服务报告、渗透测试服务报告、重保服务报告、风险评估报告、漏洞扫描报告、信息系统加固报告、威胁检测分析报告和应急响应服务报告等。

甲方依据本合同附件《网络安全服务考核表》对乙方安全服务进行第二次考核。

第十一条 乙方应当保证其交付给甲方的技术成果不侵犯任何第三人的合法权益。如发生第三人指控甲方实施的技术侵权，应由乙方承担全部责任。

第六部分 双方权利义务

第十二条 甲方权利义务

1. 提供必要的工作环境和乙方履行本合同必需的其他条件；
2. 协调甲方相关部门、人员配合乙方实施本合同有关工作；

3. 甲方对没有达到合同规定的服务质量或标准的服务事项，有权要求乙方在规定的时间内加急提供服务，直至符合要求为止；

4. 乙方为履行本合同所产生的所有工作成果，包括但不限于技术方案、设计文档、检测报告、分析数据、培训材料等（以下简称“工作成果”）的知识产权，自该成果产生之日起，全部归甲方所有。乙方享有署名权，但未经甲方书面许可，不得用于任何其他目的。乙方应保证其工作成果不侵犯任何第三方知识产权。

5. 按照本合同约定支付款项。

第十三条 乙方权利义务

1. 依据合同约定提供有关服务，依约保质保量完成本合同约定的内容。

2. 确保履行合同的人员有足够的必要能力，以保障实施合同规定的服务和任务，并确保遵守相关法律、法规。

3. 乙方应在签订合同的七天内向甲方提交项目的《安全服务实施方案》，经甲方同意后定稿，并按计划进行安全设备及安全服务的实施工作。

4. 乙方保证在服务中，未经甲方许可不得使用含有可以自动终止或妨碍系统运作的软件和硬件，否则，乙方应承担赔偿责任。

5. 乙方在履行服务时，发现存在潜在缺陷或故障时，有义务及时与甲方联系，共同落实防范措施，保证系统正常运行。

6. 乙方承诺按甲方要求配合甲方做好与项目相关的其他工作。

7. 未取得甲方书面同意，乙方不得转让合同的服务项目。

8. 如服务需要乙方人员驻场，人员应遵守甲方相关规章制度，并接受甲方的合理管理，乙方应对其派出人员的行为负责。

9. 乙方应保证项目实施期间核心技术团队的稳定性。未经甲方书面同意，不得随意更换本项目技术负责人及主要实施人员。如确需更换，应提前15个工作日书面通知甲方，且新派人员的资历和能力不得低于原人员。

10. 乙方应对在履行合同过程中知悉的甲方一切非公开信息（包括技术信息、经营信息、系统数据等）予以严格保密。

11. 乙方为履行本合同所产生的所有工作成果，包括但不限于技术方案、设计文档、配置文件、检测报告、分析数据、源代码（如有）、培训材料等（以下简称“工作成果”）的知识产权，自该成果产生之日起，全部归甲方所有。乙方享有署名权，但未经甲方书面许可，不得用于任何其他目的。

12. 乙方保证其工作成果不侵犯任何第三方知识产权。乙方应在本项目中使用任何第三方软件（包括开源软件）前，向甲方书面披露其名称、许可证类型及使用方式，确保不会导致甲方整体成果被约束需公开源代码或产生其他合规风险。

13. 基于本合同成果进行的任何后续改进所产生的技术成果，其知识产权均归甲方所有。

第十四条 安全事件与责任承担

1. 本合同所称“安全事件”，是指因乙方提供的设备、服务存在缺陷，或乙方人员违反操作规程、保密义务等，导致甲方信息系统发生数据泄露、数据丢失、系统瘫痪、被恶意篡改或遭受其他形式的网络攻击，对甲方业务或声誉造成负面影响的事件。

2. 应急响应：发生安全事件后，乙方应在收到甲方通知后30分钟内响应，并立即启动应急响应机制，派遣技术专家在2小时内到达甲方现场，与甲方共同处理事件。乙方应采取一切必要措施，防止损失扩大，并尽快恢复系统正常运行。

3. 事件调查与报告：乙方应无条件配合甲方及相关部门对安全事件进行溯源分析，并在事件处置后7个工作日内提交详尽的事件调查报告与整改方案。该报告应包括事件原因、影响范围、处置过程、责任认定及后续改进措施。

4. 责任与追偿：若发生经认定因乙方责任导致的安全事件，无论是否造成实际损失，乙方均构成违约，甲方有权根据事件严重程度，在当期应付服务费中扣除该期应付5%的款项作为违约金。若该安全事件给甲方造成实际经济损失，包括但不限于直接损失、处理事件的费用、为恢复系统支出的费用、向第三方支付赔偿金、行政罚款等，乙方应赔偿甲方的全部损失。前述违约金的支付不影响甲方就该实际损失向乙方主张赔偿的权利。

5. 本合同约定的各项违约金、扣款等责任承担方式，如因同一违约行为引发，应择其金额较高者适用，不重复计算。守约方有权主张因其违约行为所遭受的全部实际损失。

第十五条 网安部门通报处理

1. 本合同所称“网安部门通报”，是指国家、省、市各级网络安全主管部门，包括但不限于网信、公安、工信等部门，以书面形式（含通报文件、整改通知书、风险提示函等）向甲方通报的涉及甲方信息系统的网络安全漏洞、安全隐患、安全事件或其他合规性问题。

2. 服务期内，若因乙方提供的设备或服务存在缺陷、乙方人员操作失误、乙方未及时履行安全加固或漏洞修复义务等原因，导致甲方受到网安部门通报的，按以下标准进行处理：

(1) 受到地市级或县区级网安部门通报的，每次从当期网络安全服务考评总分中扣5分；

(2) 受到省级网安部门通报的，每次从当期网络安全服务考评总分中扣10分；

(3) 受到国家级网安部门通报的，每次从当期网络安全服务考评总分中扣15分。

同一事件受到多级通报的，按最高级别扣分，不重复计算。

3. 服务期内，乙方在接到甲方转发的通报文件后，应在甲方要求的时限内完成整改，并向甲方及通报部门提交整改报告。逾期未完成整改或整改不到位的，甲方有权在当期应付服务费中扣除5%的款项。

4. 服务期内，因乙方原因导致甲方受到网安部门通报，且情节严重的，甲方有权单方解除合同，乙方应返还已收取的全部费用，并按合同总价款的30%向甲方支付违约金；违约金不足以弥补甲方损失的，乙方还应赔偿甲方的全部损失。

第七部分 违约责任

第十六条 因乙方原因，未能按照合同约定或甲方要求提供服务，每延迟一日乙方应向甲方支付合同价款 0.5 % 的违约金，乙方承担违约金后不免除其继续履行合同的责任，甲方保留追究乙方的违约责任及赔偿损失请求权。乙方擅自解除本合同的，甲方有权不支付合同费用，并要求乙方支付相当于合同总价款 30% 违约金。如因乙方原因承担的违约金数额不足以弥补甲方损失的，甲方有权就损失部分要求乙方另行进行赔偿。

(如因特殊情况导致工期延迟，乙方可作出书面说明，经甲方同意后免于罚金。)

第八部分 不可抗力

第十七条 如果出现不可抗力，双方在本协议中的义务在不可抗力影响范围及其持续期间内将中止履行。合作期限可根据中止的期限而作相应延长，但须双方协商一致。

第十八条 声称遭受不可抗力的一方应在不可抗力发生后不迟于 7 日通知另一方，并提供经不可抗力书面证明，且应尽可能减少不可抗力的影响。

第十九条 如果不可抗力持续 30 日以上，且对本协议之履行产生重大不利影响，则任何一方均可解除本合同。因不可抗力导致的合同解除，甲方已支付的费用不予退还。

第二十条 任何一方违反本合同给对方造成损失的，应赔偿损失。在本合同其他条

款对违约有具体约定时，从其约定。

第九部分 附则

第二十一条 本合同一式捌份，甲乙双方各肆份，具备同等法律效力。

第十部分 索赔

第二十二条 违反合同约定给一方造成财产损失的，甲方、乙方均具有向对方提出索赔的权利。

第十一部分 合同的生效、解除与终止

第二十三条 合同生效

甲乙双方法定代表人在本合同书上签字、加盖单位公章或合同专用章之日起生效。如需修改或补充合同内容，双方应签署书面修改或补充协议，作为本合同的一个组成部分具有同等法律效力。合同生效时间不因修改或补充合同内容重新计算，若确需延长合同服务期限，须经甲方书面同意。

第二十四条 变更、解除与终止

1. 合同履行过程中，任何一方欲对合同期限、项目内容、工作进度、费用等合同内容或条款进行变更或补充的，应与对方协商一致并签订补充协议进行确定。

2. 合同履行过程中，如甲方因自身原因需提前解除合同的，应提前 30 日书面通知乙方。甲方应根据乙方已完成、且经甲方书面确认合格的工作量，按合同约定比例支付相应费用。乙方应在收到款项后 7 日内向甲方交付已完成的工作成果。

3. 如乙方因自身原因需提前解除合同的，应提前 30 日书面通知甲方，并返还甲方所支付的费用，并按本合同第十四条规定向甲方支付相关款项。

4. 除本合同另有约定外，任何一方违约导致合同解除的，守约方已支付的费用，违约方应予返还；守约方未支付的费用，不再支付。违约方还应赔偿给守约方造成的全部损失。

第十二部分 争议解决

第二十五条 双方当事人对本合同的订立、解释、履行、效力等发生争议的，应友好协商解决；协商不成的，双方同意向甲方所在地人民法院起诉；

第二十六条 本合同的终止、撤消、无效不应影响前款约定的效力。

第十三部分 履约保证金或履约保函

第二十七条 乙方按合同中标价的 5%，以银行转账或银行出具的履约保函方式向甲方缴纳履约保证金。乙方全面履行本合同项下全部义务(包括但不限于合同约定的服务内容及验收合格后三年后续服务责任，首年含安全服务及设备保障，后两年为设备专项服务保障全部服务责任等)，且无任何违约行为、无任何未了结的合同义务后，由乙方提出书面申请，甲方在收到申请后 30 日历天内全额无息返还履约保证金或解除履约保函。若乙方未按合同约定完成相应服务义务、存在违约情形或尚有未处理完毕的合同相关事项，甲方有权暂缓退还履约保证金，直至乙方按要求整改到位、全部义务履行完毕。

第十四部分 组成合同的文件

第二十八条 组成本合同的文件及优先解释顺序如下：

1. 本合同履行期间甲乙双方签订的补充合同（协议）或合同修正文件；
2. 本合同条款
3. 中标通知书
4. 磋商文件（含修改文件、澄清文件、答疑会议纪要等）
5. 响应文件及其附件
6. 甲方针对本项目建设管理的各项制度、规定、规范及有关技术文件
7. 关于本项目的谈判备忘录和会议纪要

双方有关项目的洽商、变更等书面协议或文件视为本合同的组成部分，并互为补充和解释，如各文件存在冲突之处，以上述排前的优先。当同一顺序上的文件内容出现不一致时，按时间在后者为准。

第十五部分 其他

第二十九条 一方变更联系人、通讯地址或者联系方式的，应于 3 日内将变更后的联系人、通讯地址或联系方式通知另一方，否则变更方应对此造成的一切后果承担责任；

第三十条 本合同的订立、解释、履行、效力和争议的解决等均适用中华人民共和国法律，对本合同的理解与解释应根据原意并结合本合同目的进行。

第三十一条 如果本合同任何条款根据现行法律被确定为无效或无法实施，本合同的其他所有条款将继续有效。此种情况下，双方将签订有效的约定替换该约定，且该有效约定应尽可能接近原约定和本合同相应的精神和宗旨；

第三十二条 本合同附件为本合同不可分割的一部分，与合同正文具有同等法律效力，如与本合同内容有不同之处，则以本合同的相关规定为准。

第十六部分 未尽事宜

第三十三条 其他未尽事宜，双方另行协商确定。

甲方：河南省科学技术馆（公章）

法定代表人：

日期：2026.6.10

法定地址：白沙园区金水大道北侧、锦绣路东侧

邮政编码：450000

电话：0371-65707501

开户银行：招商银行郑州分行营业部

账号：125915184310888

开户行地址：郑州市郑东新区农业东路96号
招商银行大厦1楼

乙方：奇安信网络安全技术（北京）股份有限公司（公章）

法定代表人：吴云坤

日期：2026.6.10

法定地址：北京市西城区西直门外南路26号院1号楼2层

邮政编码：100032

电话：010-62972893

开户银行：招商银行北京建国路支行

账号：110902261210404

开户行地址：北京市朝阳区建国路116号（招商局大厦一层）



附件 1

网络安全服务考评表

项目名称				
建设单位				
承建单位				
考评维度	考评内容	评分标准	分数	备注
服务完成度 (20分)	<ol style="list-style-type: none"> 1. 安全设备部署完成情况 (5分) 2. 安全服务方案提交与执行情况 (5分) 3. 各类安全服务报告提交完整性 (10分) 	<ol style="list-style-type: none"> 1. 按合同要求完成所有设备部署, 每缺 1 项扣 1 分, 扣完为止; 2. 按时提交《安全服务方案》并执行, 未提交扣 3 分, 未获确认扣 2 分, 执行不到位酌情扣分; 3. 按合同第九条要求提交全部报告每缺一项报告扣 1 分, 扣完为止。 		
服务质量 (35分)	<ol style="list-style-type: none"> 1. 安全设备响应及处理能力 (5分) 2. 漏洞修复时效 (5分) 3. 安全事件响应率 (5分) 4. 应急事件处置时效性 (5分) 5. 网安部门通报情况 (15分) 	<ol style="list-style-type: none"> 1. 安全设备无响应记录或无防护记录, 每缺 1 次扣 2 分, 扣完为止; 2. 漏洞未主动发现或未在甲方要求时限内修复, 每逾期 1 次扣 2 分, 扣完为止; 3. 对甲方通报的安全事件未达到 100%响应, 每漏报或未响应 1 次扣 2 分, 扣完为止。 4. 发生安全事件时, 未能在 30 分钟内响应或 2 小时内派遣人员到达现场, 每次扣 4 分; 未按规定提交事件调查报告, 扣 2 分, 扣完为止。 5. 未发生网安部门通报得满分; 发生通报按合同第十五条第 2 款执行扣分。 		

<p>服务规范性 (20分)</p>	<p>1. 服务内容及流程符合合同要求(10分) 2. 问题反馈及时性(5分) 3. 人员资质合规性符合合同要求(5分)</p>	<p>1. 服务内容、流程、交付物不符合合同或已确认实施方案,每发现1处不符合项扣2分,扣完为止; 2. 发现系统潜在缺陷、故障或风险未及时向甲方书面反馈,每发生1次扣2分,扣完为止; 3. 项目经理资质不符合合同第三条要求,扣4分;其他服务人员不具备相应能力,每发现1人次扣1分,扣完为止。</p>			
<p>服务效果 (25分)</p>	<p>1. 高危漏洞整改率(10分) 2. 安全事件发生率(5分) 3. 业务连续性保障(5分) 4. 服务满意度(5分)</p>	<p>1. 发现的高危漏洞整改率未达到100%,未完成1个扣2分,扣完为止; 2. 因乙方提供设备或服务缺陷导致可避免的安全事件,每发生1次扣1分;造成重大影响的本项不得分。 3. 因乙方责任导致甲方业务系统非计划中断,根据中断时长和影响范围,每次扣2分,扣完为止。 4. 根据甲方使用部门调研,满意度“一般”扣2分,“不满意”扣5分;出现有效投诉,每次扣1分,扣完为止。</p>			
<p>总分</p>		<p>监理单位意见</p>		<p>建设单位意见</p>	
<p>考核总分 ≥ 90 分: 全额支付当期应付服务费用; $80 \leq$ 考核总分 < 90 分, 按比例扣减, 每低1分扣减当期应付服务费的0.5%; $70 \leq$ 考核总分 < 80 分, 每低1分扣减当期应付服务费的0.5%, 并暂缓支付, 待乙方整改后再评估; 考核总分 < 70 分, 当期费用不予支付, 并视情况进行违约处理。</p>					

说明: 本考评表所列内容及评分标准仅供参考, 旨在明确服务考核的基本框架与核心要求。在项目具体实施过程中, 甲方可根据实际工作进度、阶段性重点及双方确认的服务内容变化, 对考评的具体项目、细项权重及评分细节进行合理调整与细化, 以确保考核的针对性与有效性。最终考核将以双方书面确认的考评方案或相关补充约定为准。

附件 2

保密协议

第一条 保密信息的范围

1. 保密信息是指由甲方通过文字、电子或数字方式或媒介向乙方提供的，在提供时明确标记有“保密”的，以及虽未标记为“保密”但属于甲方的生产经营数据、报表、图幅、报告及技术信息。口头传达并在传达同时认定为属于保密的信息应当视为保密信息。甲方相关的业务和技术方面有保密要求的资料信息。保密信息还包括本项目研发中形成的双方共有技术、产权、软件成果、研究思路。保密信息包括但不限于：

- (1) 数据库所有的数据；
- (2) 甲方或潜在甲方的身份及其他相关信息、甲方联系方式和甲方销售策略等；
- (3) 市场研究结果，市场渗透资料，及其他市场信息；
- (4) 网络架构、拓扑图、服务器信息、安全设备信息、安全防护策略、业务系统配置信息及关键系统管理员账号信息等；
- (5) 营业额、成本和其他财务数据；
- (6) 经营秘密、技术秘密、设计及专有的经营和技术信息，与本协议所涉及产品及其程序设计、源码等有关的方法、经验、程序、步骤；
- (7) 产品、零件及服务的供应源；
- (8) 任何其他秘密工艺、配方或方法；
- (9) 本项目研发形成的双方共有技术、产权、软件成果、研究思路在成果申报之前。

2. 保密信息不包括以下信息：

- (1) 甲方已经公布于众的资料，但不包括甲乙双方或其代表违反本协议规定未经授权所披露的；
- (2) 在双方签订本协议以后并非由于乙方的过错而被公众所知的信息；
- (3) 乙方在未违反其对甲方承担的任何义务的情况下从第三方获得的信息。

第二条 保密信息的使用

1. 乙方应使所有保密信息得到最严格的保密，本协议允许的用途外，不得使用该等

保密信息。

2. 除非事先取得甲方的书面同意，否则乙方不得复制、出版或向第三方披露任何保密信息。

3. 如果具有司法管辖权的法庭或政府主管部门要求乙方披露保密信息，乙方应事先通知甲方，使甲方能够查验需要披露的保密信息。

4. 本协议在终止后的 2 年内仍完全有效。期满后乙方如需对外披露保密信息，事先必须经过甲方书面同意。

第三条 保密信息的所有权

与本项目相关的全部工作成果的知识产权归属及使用，均以主合同第十三条的约定为准。

第四条 文件退还

如果双方同意终止项目合作，乙方应在双方同意终止后的 10 日内，向甲方退还全部保密信息及其全部副本（不论其是否是在计算机磁盘、光盘读取器、光盘、硬盘或软件中或在纸张载体上存储、保存或记录的）；如果乙方退还上述保密信息及其全部副本为不可行，则乙方应将其销毁，或者从计算机或其他电子系统中将其删除或抹掉。

（本页以下无正文）