**用户需求书**

**1.项目背景**

中山大学孙逸仙纪念医院（中山大学附属第二医院）为国家卫生健康委属（管）医院，创建于1835年，是我国第一家西医医院，中国西医学和西医教育的发源地，至今已有189年历史。医院作为国家卫健委直管三级甲等综合医院，需要满足国家等级保护标准、个人信息保护法、网络安全法、数据安全法等安全要求。网络安全防御体系是一项复杂的系统工程，除了网络安全产品建设以外，更重要的是持续的安全运营。2024年度全院信息安全保障服务项目合同即将到期，为加强医院网络和数据安全日常管理，提升信息安全风险感知、分析、处置能力，医院拟继续采购全院信息安全保障服务，选择安全工作经验丰富、技术实力较强、符合资质要求的企事业单位参与医院安全建设，以增强应对重大事件和应急响应的信息安全保障力量。

**2.项目主要内容**

|  |  |  |
| --- | --- | --- |
| **序号** | **服务名称** | **服务内容** |
| 1 | 互联网侧资产盘查服务 | 通过调研的方式确定互联网资产范围，基于IP或域名，采用WEB扫描技术、操作系统探测技术、端口的探测技术、服务探测技术等各类探测技术，对互联网侧的主机/服务器、安全设备、网络设备、工控设备、WEB应用、中间件、数据库、邮件系统和DNS系统等进行主动盘查，形成互联网侧资产及应用清单列表，列表中不仅包括设备类型、域名、I P、端口（需要识别是否为高危端口），更可深入识别运行在资产上的中间件、应用、技术架构的详细情况（类型、版本、服务名称等）。通过对比发现潜在的未知互联网资产，避免医院管理人员遗漏相关资产信息，造成信息孤岛。  **服务频率：提供1年2次互联网资产发现服务。**  **交付物：《互联网资产发现报告》** |
| 2 | 网站安全监测服务 | 针对中山大学孙逸仙纪念医院10个网站，提供专用SAAS平台进行7\*24小时监测服务，主要包括漏洞扫描、木马分析、黑链监测、篡改监测、敏感内容监测、网站可用性监测，提供全面的事前、事中的安全监测。网站安全监测服务活动包括网站状态安全监测、安全事件报警与响应、网站漏洞检测及网站监测报告编制等四项主要任务。  ▲网站安全监测服务应具备以下能力：  （1）对网站主要页面提供挂马监测能力，检测网页中嵌入的恶意代码，例如JS挂马，恶意加密挂马，框架隐藏，挖矿脚本，搜索引擎劫持等。根据不同页面的重要等级提供不同频率监测，提供事件验证能力，排除误报。  （2）对网站主要页面提供黑链监测能力，检测网页中嵌入的恶意链接（黄赌毒广告钓鱼等）。根据不同页面的重要等级提供不同频率监测，提供事件验证能力，排除误报。链接范围包括暗链。  （3）对网站主要页面提供篡改监测能力，根据不同页面的重要等级提供不同频率监测，提供事件验证能力，排除误报。  （4）支持识别判定自动扫描行为，在设定周期内采集发送端向网站服务器发送的访问请求消息和网站服务器向发送端返回的响应消息，将设定周期等分为至少两个子周期，依次统计每个子周期内访问请求消息个数，确定发送端请求可信度，判定发送端是否发生了自动扫描的行为。须提供国家权威机构（如工业和信息化部、经济和信息化委员会或国家知识产权局）证明材料。  服务范围：中山大学孙逸仙纪念医院指定的10个网站  **交付物：《网站安全监测报告》** |
| 3 | 重要web系统渗透测试服务 | 对中山大学孙逸仙纪念医院10个重要web应用系统及15个对外业务系统进行非破坏性质的模拟入侵者攻击测试，使用渗透测试结合人工渗透分析开展。同时针对其他应用系统（约50个）进行渗透测试扫描，以期掌握系统的安全状况，对发现的安全风险提出针对性的安全整改建议，修补漏洞，为抵御安全风险提供技术支持。渗透过程中涉及对目标系统进行主动分析，以发现可能由于系统配置不当而导致的潜在漏洞，并协助医院进行修复，修复后进行复测，以确认漏洞被完全修复。服务过程中供应商需自带漏洞检测工具，并满足以下功能要求。  ▲漏洞扫描工具要求：  （1）支持对漏洞进行单个或批量复测，且支持查看复测结果。（提供功能截图并加盖投标人公章）  （2）内置扫描任务报表、基线检查报表、资产报表、漏洞报表、对比报表和自定义报表模板；自定义的维度包括且不限于资产（主机存活性、主机指纹、端口、web指纹等）、漏洞（修复方案、CVSS评分、漏洞细节、漏洞描述、漏洞危害、影响范围等）进行筛选。（提供功能截图并加盖投标人公章）  （3）支持自定义漏洞POC检测插件，包括漏洞名称、漏洞类型、漏洞危害、CVSS信息、检测脚本等，用于日常突发漏洞应急。（提供功能截图并加盖投标人公章）  **服务范围：中山大学孙逸仙纪念医院指定的约10个应用系统**  **交付物：《渗透测试报告》** |
| 4 | 敏感信息情报服务 | 以蓝队（攻击队）视角，对中山大学孙逸仙纪念医院聚焦于敏感信息泄露情况的分析，探测范围覆盖互联网的各类公开应用，如搜索引擎、代码托管平台、网盘、暗网情报、Telegram情报等。核心关注代码或文档泄漏、医疗数据泄露、Telegram情报，需在各类代码托管平台进行分析（包括但不限于Github、Bitbucket、Gitee、Gitlab等）。具体服务要求如下：  （1）根据医院提供及服务方提炼院方相关敏感关键字，利用网络爬虫、代码托管平台、网盘、API接口、暗网论坛等多渠道搜集医院相关的敏感情况，如应用系统代码泄露、非公开技术文档泄露、医护数据泄露、敏感数据非法传播与地下交易等情报，及时发现和处置敏感信息泄露事件，降低客户损失；  （2）▲支持通过暗网、Telegram等加密渠道搜索用户相关敏感情报，如泄露的数据样本、情报泄露渠道、情报发布时间等关键信息，搜索的暗网通道覆盖中文及英文，数量不少于20个。（提供暗网渠道功能截图及以往敏感情报样本证明并加盖投标人公章）  **服务频次：在服务期内提供2次敏感信息情报服务。**  交付物：《敏感信息泄露情报分析报告》 |
| 5 | 钓鱼邮件演练测试服务 | 基于社会工程学的原理，根据中山大学孙逸仙纪念医院网络环境、邮件使用习惯和特征，结合内部的热点事件，精心构造具有欺骗性、迷惑性、含有钓鱼链接的钓鱼邮件，模仿院内部门向目标群体定向发送钓鱼邮件，进行钓鱼演练测试。  **服务频次：在服务期内提供1次钓鱼邮件测试服务。**  **交付物：《钓鱼邮件测试服务报告》** |
| 6 | 病毒监控防治服务 | 提供防病毒系统巡检、病毒查杀服务、防病毒管理软件的安装管理和协助安装服务。旨在保障防病毒软件的全面覆盖，持续提升防病毒系统的使用效果，实现防病毒安全预警，提升病毒安全事件应对能力。针对防病毒系统提供防病毒运维工具进行病毒日志深度分析，结合人工研判，通过人机共治方式，对周期性病毒数据进行自动化分析，保障病毒巡检报告的准确性与可靠性。具体要求如下：  （1）▲防病毒运维工具支持病毒传播及感染方向智能分析，可展示数据包括本机内横向扩散病毒数、通过移动存储感染病毒数、通过互联网感染病毒数、引导区病毒数、局域网横向传播病毒数，辅助安全管理人员直观判断病毒传播渠道风险。（需提供工具界面截图及病毒分析报告证明并加盖投标人公章）  （2）防病毒运维工具支持前十病毒全网扩散情况分析，可展示数据包括病毒扩散情况排名前十的病毒名称、被感染计算机数量与具体被感染的计算机名称。（需提供工具界面截图及病毒分析报告证明并加盖投标人公章）  （3）▲防病毒运维工具支持勒索病毒感染情况、挖矿病毒感染情况分析，可展示数据包括病毒名、受感染文件路径、感染计算机名称、感染计算机数量，帮助安全管理人员梳理勒索病毒、挖矿病毒感染情况，有效闭环病毒处置工作。（需提供工具界面截图及病毒分析报告证明并加盖投标人公章）  （4）防病毒运维工具支持全网感染黑客工具的计算机分析，可展示数据包括黑客工具名称、感染计算机名称和感染计算机数量。基于全网感染黑客工具的计算机分析数据，可以直观发现网内是否存在黑客入侵风险与被入侵的计算机名称及数量。（需提供工具界面截图及病毒分析报告证明并加盖投标人公章）  （5）▲防病毒运维工具支持自定义防病毒运维考核KPI指标包括病毒码更新率、客户端部署率、病毒感染率、病毒接触率。通过防病毒日志分析周期内运维考核KPI指标完成情况，直观呈现出单位当前防病毒运维效率。（需提供工具界面截图及病毒分析报告证明并加盖投标人公章）  （6）支持病毒扫描方式数量及占比情况分析，可展示数据包括病毒扫描方式如实时扫描、预设扫描、手动扫描、其它扫描类型以及扫描数量占比情况，帮助用户了解单位工作周期内的防病毒运维工作情况。  **服务频次：在服务期内提供12次病毒监控防治服务。**  **交付物：《病毒监控防治服务报告》** |
| 7 | 安全培训服务 | 提供安全培训服务，包括政策法律法规解读、日常安全防范等，提升全员安全意识，提高运维人员信息安全技能和安全管理水平。投标人需提供专业讲师开展2次安全培训，包括：1次针对采购人普通员工的信息安全意识培训和1次针对采购人运维人员的专业技能培训。  **服务频次：在服务期内提供2次安全意识培训**  交付物：培训记录表、培训课程内容等。 |
| 8 | 安全通告服务 | 定期为采购人提供安全事件通告服务。定期提供最新的安全资讯。内容包括但不限于新闻、流行病毒提示、新病毒列表、系统漏洞提示、安全防护技巧等。服务周期为每周1次。  **交付物：《安全通告周报》** |
| 9 | 常见安全场景的应急演练（桌面推演）服务 | 协助采购人组织策划和开展应急演练，包括制定演练计划、编制演练工作方案、设计演练脚本、动员与培训、演练过程记录和总结等工作。  根据应急预案，对钓鱼邮件、社会工程学攻击、病毒传播等常见安全场景，配合医院编写信息安全应急演练方案，确保该应急预案可以适应现时信息技术发展趋势和国内外互联网安全威胁态势，强化应急相关工作人员的应急操作水平。  **服务要求：在服务期内提供3个场景安全应急演练服务。**  **交付物：《安全演练报告》** |
| 10 | 等级保护测评服务 | 投标人需按照网络安全等级保护2.0标准对采购人8个三级系统进行等保测评服务，服务要求如下：  完成信息系统相关资产梳理；  完成信息系统等级备案与专家评审；  采用具有网络安全等级保护测评与检测评估资质的测评机构进行等保测评服务，等保测评需包括差距测评及验收测评服务；  对测评机构发现的安全问题单按网络、主机、应用（应用系统、中间件、数据库）进行分类，按院方时间表相关制定整改计划，推动各相关责任方落实整改，跟踪整改进度并定期反馈整改进展；漏洞整改过程提供漏洞降级服务工具，可实现以下效果：  （1）漏洞安全隐藏服务工具支持对导入的高危漏洞信息进行智能分析，生成漏洞分析结果和屏蔽建议。（需提供工具界面截图并加盖厂家公章）  （2）漏洞安全隐藏服务工具支持一键开启漏洞屏蔽策略，支持针对不同主机范围应用不同的屏蔽策略，并支持灵活调整屏蔽的策略，设置是否拦截漏洞攻击，也可对应设置屏蔽白名单，放行正常业务。（需提供工具界面截图并加盖厂家公章）  完成信息系统等保验收测试评估，输出等保2.0验收测评报告，并协助通过公安机关的备案与检查。  **交付物：等保2.0测评标准的《等级保护安全测评报告》、《公安部等保备案回执证明》** |
| 11 | 攻击队评估服务 | 采用最大限度模拟APT（高级持续性威胁）攻击手法，不限定攻击路径和手段，以不采用破坏性攻击为底线，以系统提权、控制业务、获取数据为目标，深入评估医院安全防护短板，检验安全监测与响应体系的有效性。攻击队评估服务需具备安全防护有效性进行评估，具体要求如下：  安全防护有效性进行评估工具要求：  （1）支持对纵深防御体系做整体验证，支持对各类攻击向量、攻击场景和攻击过程的编排，验证范围覆盖边界突破、权限提升、权限维持、横向移动完整过程。（提供功能截图并加盖投标人公章）  ▲（2）支持对黑客工具进行模拟仿真，包括但不限于MSF、哥斯拉、冰蝎、Empire、Cobalt Strike、frp等，数量不少于30种。（提供功能截图并加盖投标人公章）  ▲（3）支持模拟涉及2台以上服务器的完整攻击路径模拟，可模拟横向移动过程。（提供功能截图并加盖投标人公章）  （4）网络安全防护能力检测服务工具支持以攻击方视角展示样本对应的请求包、响应包、攻击工具等信息；支持以防守方视角展示验证样本所属的攻击阶段、技术点、涉及安全设备等信息。  **服务频次：一次**  **交付物：《攻击队评估报告》** |
| 12 | 重保值守服务 | 在重大会议、上级的安全大检查、省级或以上攻防演练等特殊时期内，为采购人提供网络安全专家临时性驻点值守服务，协助采购人找出本地化安全威胁和隐患，并对可能已经造成的安全事件进行日志取证和溯源。  对安全事件影响范围、后果进行分析，找出安全防御体系和策略的实战缺陷，并配合进行紧急整改。对重保过程中发现的新漏洞进行验证，并协助进行紧急处置。  **服务要求：在服务期内，根据采购人通知按需提供20人/天的重保值守服务。**  **交付物：《重保值守报告》** |
| 13 | 应急响应及处置服务 | 本服务的目标是确保在发生安全事件时，能够及时响应并有效地排除风险隐患，提供关键时期的紧急保障措施，从而降低潜在的安全风险并减少因安全事件可能造成的损失。具体服务要求如下：  （1）即时响应与风险缓解：在安全事件发生时，迅速采取行动，系统地响应并采取适当的步骤，以最小化安全事件带来的负面影响。  （2）数据与服务保护：采取措施帮助采购人从安全事件中迅速有效地恢复，确保信息丢失、数据被盗和服务中断的风险降至最低。  （3）漏洞与安全预警：持续关注零日漏洞和行业内新发现的高危安全漏洞，针对采购人的网络设备、网站和信息系统进行风险评估，为其信息安全管理团队提供预警和建议，制定遏制和缓解策略。  （4）专业应急处置：在发生黑客入侵、系统崩溃或其他严重影响业务正常运行的安全事件时，驻场服务人员应立即进行应急响应处理。若事件风险等级较高或影响范围较大，超出驻场人员解决能力时，须提供专业的应急响应服务团队协助处理。  （5）应急保障支持：在关键时期或面对重大安全威胁时，提供加强的应急保障支持，确保业务连续性和数据安全。  （6）事后复盘与改进：安全事件处理结束后，进行详细的事后分析，总结经验教训，提出改进措施，防止类似事件再次发生。  ★（7）中标人须提供7\*24小时的应急响应服务，接到采购人应急响应支持请求，半小时内选派资深安全工程师（包括但不限于一线及二线人员）赶赴采购人现场，根据事件类别和应急预案，协助采购人对遇到的突发性安全事件进行紧急分析和处理。 |
| 14 | 安全驻场运维服务 | 提供网络安全驻场运维服务，按照实际需要提供具有网络安全相关资质证书的驻场一线信息安全工程师，服务内容包含但不限于资产梳理、策略优化、弱口令检查、基线配置检查、全网信息系统漏洞扫描、web系统漏洞扫描、安全迎检、全网日志安全数据分析等内容。协助医院开展日常网络安全运维工作，常态化安全管理，基础网络设备（采购人主要品牌为思科、华为）状态巡检，保障网络信息业务稳定运行。  交付物：《日常巡检报告周报》、《日常巡检报告月报》。 |
| 15 | ★医院原有安全产品和工具授权（维保）续保服务 | 为保障医院安全防御工具的可持续性，需提供医院原有安全方面产品的授权（维保）续保服务。 |

★**其中医院原有安全产品和工具授权（维保）续保明细见下。**

为保障医院安全防御工具的可持续性，投标人需提供采购人原有以下安全方面产品的授权（维保）续保：

①深信服防火墙安全特征库和URL库订阅一年，具体设备清单见下：

|  |
| --- |
| **设备型号** |
| NGAF-1560 |
| NGAF-1230 |
| NGAF-1750 |
| NGAF-2050 |
| NGAF-2050 |
| NGAF-1560 |

②终端安全软件一年服务：

|  |  |  |
| --- | --- | --- |
| 产品名称 | 产品 | 数量 |
| 服务器安全管理系统维护服务 | （1）医院现有亚信服务器防病毒功能（Windows 服务器）维护服务（1年） | 200 |
| （2）新增服务器防病毒功能（Windows 服务器）使用授权点数服务（1年）  （3）▲新增授权可兼容导入医院现有防病毒管理平台，实现全网服务器防病毒软件特征库统一更新、病毒统一查杀、病毒日志集中留存等。（提供原厂兼容性承诺函并加盖投标人公章） | 300 |
| 终端安全管理系统维护服务 | （1）医院现有亚信终端防病毒软件维护服务（1年） | 3780 |
| （2）新增服务器防病毒功能（Windows 服务器）使用授权服务（1年）  （3）▲新增授权可兼容导入医院现有防病毒管理平台，实现全网服务器防病毒软件特征库统一更新、病毒统一查杀、病毒日志集中留存等。（提供原厂兼容性承诺函并加盖投标人公章） | 2220 |

②主机安全保护软件一年服务：

|  |  |  |
| --- | --- | --- |
| 产品名称 | 产品 | 数量 |
| 主机安全保护软件 | 新增主机安全保护软件，实现内网数据中心主机漏洞检查、主机基线检查、主机弱口令检查、主机命令执行跟踪、C&C回连进程定位、入侵轨迹记录、进程调用监控及高危行为阻止、WebShell后门检测查杀等功能，1年软件升级及规则库更新服务。功能要求如下：  （1）主机安全保护软件支持部署在 RedHat、CentOS、Ubuntu、Suse、Windows Server等操作系统，支持中标麒麟、银河麒麟、统信 UOS 等国产化操作系统中部署。支持在ARM架构、X86架构系统部署，支持在非 root 权限下运行和正常使用，减少对系统运行的影响。  （2）支持自动清点和梳理主机信息，包含主机名称、主机IP地址、主机状态、操作系统、主机关联威胁事件、主机关联漏洞风险、最近一次发现时间等。可设置主机分组信息和备注信息，按照多维度进行主机信息筛选过滤。  （3）支持清点主机上的进程信息，内容至少包括：进程名，父进程，PID，进程启动参数，进程状态，启动时间，工作目录，启动用户，可执行文件等  （4）支持自动清点和梳理主机端口和开放进程信息，包含主机名称、主机IP地址、协议、监听地址、端口对应的进程名、进程PID，可对端口进行多维度筛选过滤操作  （5）支持清点的软件应用类型包括 java 依赖、系统库、系统工具、编译器、解释器、web 服务、web 框架、数据库、消息队列、web 应用、操作系统内核、其他网络服务、第三方工具、虚拟化工具。  （6）支持自动清点和梳理主机上运行的web站点信息，包含主机名称、主机IP地址、服务类型、对应端口、端口协议类型、域名、web路径信息。服务类型包含Nginx、Apache、Tomcat，端口协议类型包含http和https 。可对web站点进行多维度筛选过滤操作。  （7）支持检测 Linux 与 Windows 系统弱口令。  ▲（8）支持检测 MySQL、PostgreSQL、Redis、Oracle、InfluxDB、GBase 8a、KingbaseES、HighgoDB、openGauss等主流数据库弱口令。（提供功能截图并加盖投标人公章）  （9）支持检测 Tomcat、Jenkins、WebLogic、SVN中间件弱口令。  （10）支持检测 vsftpd、Rsync 、OpenLdap网络服务弱口令。  （11）支持检测 Radmin Server、TigerVNC、TightVNC、向日葵等远控软件弱口令。  （12）支持检测容器内应用的弱口令。  （13）支持对操作系统、应用程序的等级保护、CIS合规基线和重保基线的快速核查与结果报告导出。  ▲（14）支持webshell拟态防护功能，能够有效诱导黑客webshell攻击并进行攻击溯源。（提供功能截图并加盖投标人公章）  （15）实时监控主机上发生的异常登录事件，检测的异常登录事件类型包括异常时间登录、异常IP登录、异常登陆地点、异常用户名登录四种。 | 400 |

**3.实施人员要求**

为确保服务质量，中标人应成立由具备相应资质的专业技术人员组成的项目实施小组。小组由一线、二线人员（含项目经理）组成。具体见下。

★**3.1一线人员要求**

提供3名具有下文列举的网络安全相关资质认证中一份或多份证书的安全技术人员工作日5x8小时驻场服务。分别驻场在北院区及南院区。驻场周期一年。驻场具体地址见下：

|  |  |
| --- | --- |
| 院区 | 服务地址 |
| 北院区 | 广州市越秀区沿江西路107号 |
| 南院区 | 广州市海珠区盈丰路33号 |
| 花都院区 | 广东省广州市花都区新华街迎宾大道163号 |

网络安全相关资质证书包括但不限于：注册信息安全专业人员认证（CISP）、信息安全工程师、网络工程师的一种或几种。

备注: 提供承诺函加盖投标人公章。承诺在本项目成交后合同签订之前提以上资质证书供给采购人审核确认。如内容有虚假，采购人有权上报监管部门，采购人、评审委员会及有关行政监督部门保留追究其虚假响应的权利，由此引发的所有损失由中标人负责。

**3.2二线人员要求**

提供由7名及以上专家组成的服务团队为采购人提供二线服务，即由包括项目经理在内的7名及以上专家提供的远程支持服务，根据项目需要为一线驻场人员提供相关技术支撑。项目经理应具有本科或以上学历，3年或以上信息安全维护相关工作经验，以及CISP证书。其他技术人员应至少具备以下证书：注册信息安全专业人员认证（CISP）、信息安全工程师、网络工程师证书中的一种或几种。

**3.3人员变更要求**

在合同期内，如因个人原因离职或其他原因需发生人员更换，中标人需告知采购人；必须保证至少一个月的工作交接时间，确保中标人派遣的接任驻场人员完全掌握服务内容后方可更换人选，其人员资质要求与启动时一致。

**4.安全服务工具要求**

4.1服务期内，需提供支撑用户需求书中提及的所有服务的必要工具，包括但不限于资产发现工具、自动化渗透测试工具、漏洞扫描工具、代码检测工具、开源代码检测工具、网络流量采集与分析工具，应提供工具的著作权证书（如投标人非服务工具制造商，需同时提供工具制造商与投标人合作关系的证明文件）。

★4.2医院自有网络安全设备及安全服务工具发生故障时中标人须在自故障发生起8小时内（含）提供同等档次的备用设备，直至原设备修复完成。（提供承诺函并加盖投标人公章）

★4.3在服务期内，中标人负责对以上提供的服务支撑工具进行维护及升级，期间产生费用由中标人负责。（提供承诺函并加盖投标人公章）

**5.质量保障措施**

5.1投标人应提供针对本项目的服务方案（内容至少包含①项目理解和分析②安全政策与标准遵循③安全架构设计④项目人员安排⑤安全操作和维护⑥服务流程和方法）、服务质量控制方案（内容至少包含工作安排与时间规划、项目建设过程管理、质量控制、风险控制等）

5.2为保证项目质量，投标人应具有良好的体系管理能力，具备相关管理体系认证证书。

5.3工作质量及表现考核

考核过程：

（1）采购人每季度根据系统安全运行情况填写《系统安全运行季度考核评分表》

《系统安全运行季度考核评分表》——暂略

（2）中标人驻场服务人员表现发生如下情况，需进行扣罚款。

罚款情形——暂略

（3）每季度经采购人确定《系统安全运行季度考核评分表》、《服务表现季度扣罚金额统计表》后，如服务表现考核合格，采购人所需支付之服务费用按“该季度得分/100 \*原每季度支付款-服务表现扣罚金额”确定。如服务表现考核不合格，则本季度采购人不予付款。

**6.保密原则**

项目中所涉及的双方的内部资料、数据和其他商业信息，未经信息拥有方的许可，信息获得方不得以任何形式用于合同之外的目的，不得以任何形式向第三方泄露。中标人不得以在软件系统中留有任何可能导致采购人数据泄密的软件“后门”。发生泄密事件，信息拥有方有权追究泄密方的经济和法律责任，但因采购人及其授权的任何工作人员自身过错导致其该项目发生泄密而产生损失的，中标人不承担任何法律责任。

**7.商务要求**

1.服务期：自合同生效之日起1年。

2.报价要求：完成本项目全部内容所需费用的含税价，不高于本公司目前的报价水平，且符合国家有关的价格规定（如有）。

3.付款方式：合同签订后，每经历壹个季度，双方协商确定《系统安全运行季度考核评分表》、《服务表现季度扣罚金额统计表》后，中标人向采购人开具金额为“合同总金额\*25%\*该季度得分/100 -服务表现扣罚金额”的合法有效发票，采购人收到发票，在具备支付条件后10个工作日支付相应金额。如该季度服务表现考核不合格，则采购人不予付款。