陕西省卫生健康信息安全系统运维合同

委　托　单　位：陕西省卫生健康信息中心

服　务　单　位：杭州安恒信息技术股份有限公司

日　　期：二〇二六年八月

委托单位(以下简称甲方)：陕西省卫生健康信息中心

服务单位（以下简称乙方)：杭州安恒信息技术股份有限公司

依据《中华人民共和国民法典》和《中华人民共和国政府采购法》之规定，经双方在平等、自愿、互利的基础上签订本合同，共同信守。

一、项目名称、项目内容

项目名称：陕西省卫生健康信息安全系统运维

项目内容：具体内容详见附件1、附件2

二、合同价款

(一)甲方通过竞争性磋商方式，接受了乙方以总金额大写贰拾玖万叁仟伍佰元整(￥小写293500.00)(以下简称“合同价”)提供合同条款附件所述服务。

(二)服务报酬中包括为完成服务内容可能发生的各项费用，包括但不限于人工费、车辆交通费、住宿费、管理费、办公、人员人身相关保险费、项目实施费用以及国家按现行税率征收的一切税费、不可抗力因素的可预见和不可预见费用等

(三)合同总价一次包死，不受市场价格、工作量变化等其它因素的影响。

三、款项结算

(一)合同签订后，甲方收到乙方开具的正式发票后10个工作日内支付合同总金额的80.0%(即人民币:贰拾叁万肆仟捌佰元整,¥ 234,800.00)给乙方。

(二)服务期满、项目验收合格后，甲方收到乙方开具的正式发票后10个工作日内支付合同总金额的20.0%(即人民币：伍万捌仟柒佰元整，¥ 58，700.00)给乙方。

(三)乙方须在甲方付款前出具合法有效的完税发票，甲方进行支付结算。

(四)结算方式：银行转账。

四、服务条件

(一)服务地点：甲方指定地点

(二)服务期：合同签署日期后一年。

(三)乙方需提供符合本合同及附件要求的原厂驻场运维人员服务，驻场工程师未经甲方书面同意不得更换。确需更换的，乙方应至少提前15日向甲方提交书面申请，并附替换人员的资质证明材料；替换人员经甲方审核确认具备不低于被更换人员的资质，并取得甲方书面同意后方可更换。乙方未经甲方书面同意擅自更换驻场工程师，或替换人员资质不符合本合同及附件要求的，构成违约，乙方应立即改正并承担因此给甲方造成的全部损失。

五、甲乙双方权利义务

(一)甲方的权利义务

1.甲方有权指派专门人员或者单位对乙方的工作进行全程监督检查、管理，明确员工职责范围。对工作中不负责任、违反管理规定的人员，甲方有权提出辞退要求，情况属实，乙方应无条件予以执行。

2.如果乙方不按甲方规定时限完成各阶段工作任务，或服务质效不符合约定，甲方有权要求乙方限期整改，整改期满仍不符合要求的，甲方有权单方终止合同，因此产生的全部损失由乙方承担。

3.为保证乙方顺利履行职责，甲方需向乙方提供履行本合同项下服务所必需的且不涉及甲方核心商业秘密及敏感个人信息的相关情况和资料；乙方获取前述资料仅限用于本次运维服务目的，不得擅自留存、复制或挪作他用。

4.按本合同约定向乙方支付合同价款。

（二)乙方的权利义务

1.按合同要求向甲方派出合格的服务人员，依据岗位职责结合甲方交予的任务执行服务工作；遵守甲方制定的各项规章制度，为甲方提供平台运维服务。

2.乙方应当严格按照国家有关法律法规政策及规定，为甲方提供服务，维护甲方的合法权益。乙方驻场工作人员如不履行职责、不履行甲乙双方的约定，甲方有权向乙方提出更换。

3.未经甲方事先书面同意，乙方不得将本项目全部或部分转包、分包给任何第三方，也不得委托无相应资质的人员提供本合同项下服务。

4.乙方定期征求甲方的意见，以便及时沟通并做好服务工作，及时报告工作进度，在规定时间内完成相应的项目建设工作。

5.乙方应在24小时内予以响应，并按照甲方要求的时限完成整改，整改完成后书面反馈甲方核查。

6.在未正式验收前，如政策发生变化，中标供应商须符合国家相应政策，完善服务项目。

六、保密要求

项目实施过程中收集、产生或形成的与本项目相关的全部文档、资料、数据及成果，包括但不限于文字、图片、表格、数字等，其所有权、知识产权及其他相关权益均归属甲方。未经甲方书面同意，乙方不得擅自使用、复制、修改、披露、转让或许可第三方使用前述内容。乙方及其服务人员必须对履行本项目过程中知悉的甲方商业秘密、项目资料、医疗健康数据、用户个人信息及其他未公开信息承担保密义务，并按照甲方要求签署保密协议。无论本合同是否终止或解除，乙方及其服务人员的保密义务持续有效。

七、违约责任

服务期间造成实际影响的，按以下条款处理:

(1)合同生效后，甲乙双方应按合同规定认真履约。合同履约责任只涉及合同甲乙双方，不考虑第三方因素。乙方须保证本项目使用的任何产品和服务（包括部分使用），不会产生第三方专利权、著作权、商标权或其他知识产权纠纷。如因乙方提供的产品和服务侵犯第三方知识产权引起法律和经济等纠纷，因侵权纠纷产生的全部费用(包括但不限于诉讼费、律师费、保全费、保全担保费、鉴定费、公证费、差旅费等)由乙方承担。乙方应赔偿甲方全部损失。

(2)乙方对服务过程中出现的问题推诿、拖延，未按时作出服务响应，应接受甲方的合理处罚。

(3)由于乙方原因不能履行合同服务项目，或履行合同质效达不到规定，甲方有权聘请第三方公司执行合同内所列项目，由此产生的全部费用，包括但不限于第三方服务费及甲方因此额外支出的管理成本等，均由乙方承担，甲方有权从应付乙方的服务费用中直接扣除；应付服务费用不足以抵扣的，乙方应在甲方

通知后3个工作日内补足差额，逾期未补足的，甲方有权追偿。甲方有权解除合同，并要求乙方承担相应违约责任。

(4)系统发生重大安全事件，将按照国家、部、省网络安全相关规定，根据造成的实际损失和影响，进行责任追究。

乙方有上述任一违约行为，甲方有权终止合同，并要求乙方支付合同金额的20%作为违约金，同时承担因此造成的所有损失。

八、凡涉及服务范围或工作量的调整，均须出具书面变更单，经甲方盖章确认后方可实施。其中，因国家法律、行政法规、部门规章及强制性国家标准(GB)明确要求而产生的系统改造工作，不另行收费。上述“强制性合规要求”是指由全国人大及其常委会、国务院、国家各部委正式发布的法律法规、行政规章及强制性国家标准中，对信息系统安全、数据保护、等级保护等方面提出的具有法律约束力的合规义务。因地方性法规、行业推荐性标准或甲方自行提升安全等级所产生的改造费用，不在本条款范围内。因甲方新增需求产生的工作，费用由双方另行协商确定。

九、合同争议解决的方式

本合同在履行过程中发生的争议，由甲、乙双方当事人协商解决，协商不成的按下列第 (二)种方式解决：

(一)提交仲裁委员会仲裁；

(二)依法向甲方所在地人民法院起诉。

十、合同生效

(一)本合同须经甲、乙双方的法定代表人(授权代表)在合同书上签字并加盖本单位公章后正式生效。

(二)本协议一经生效，双方均应严格遵守；如有违约，守约方可依照《中华人民共和国民法典》及有关法律法规规定，追究违约方的法律责任。

(三)本协议未尽事宜双方可另行协商，签订书面补充协议。与本协议具有同等效力。

十一、本协议一式四份，甲乙双方各执贰份，具有同等法律效力。

（下无正文）

甲　方：陕西省卫生健康信息中心

（盖章）

法定代表人：

被授权代表：李剑

电话：

日期：2026.8.31

乙方：杭州云恒信息技术股份有限公司

（盖章）

法定代表人：张小宝

被授权代表：任伟宁

电话：

日期：2026.8.31

附件一：服务清单表

项目名称：陕西省卫生健康信息安全系统运维

项 目 编 号： ZCBN- 省 本 级 -2026-06236

序号	服务名称	单位	单价（元）	服务期	备注
1	驻场运维服务	项	266500.00	自合同签订之日起一年	包含平台特征库升级服务
2	漏洞扫描服务	项	5000.00	自合同签订之日起一年	无
3	应急管理服务	项	9000.00	自合同签订之日起一年	无
4	安全培训服务	项	1000.00	自合同签订之日起一年	无
5	重要时期保障服务	项	12000.00	自合同签订之日起一年	无
总计：			大写：贰拾玖万叁仟伍佰元整 小写：293500.00		

日　　期：　　年　　月　　日

附件二：服务内容

序号	服务项	服务内容	备注
1	驻场运维服务	服务内容：派驻不少于1名信息安全驻场工程师，提供5*8小时驻场服务，为保证驻场工程师的服务能力，要求驻场人员具备3年以上工作经验并且具备CISP系列证书，协助卫健委开展日常信息安全服务的管理和分析工作。 驻场运维工作内容包括但不限于： 1)定期对安全设备实施升级维护，涵盖规则库与特征库更新、系统版本迭代等； 2)实时分析安全设备告警信息，主动识别攻击行为并及时响应处置； 3)配合甲方完成网络安全等级保护测评全流程工作，包括安全整改实施、漏洞闭环跟踪、定级备案材料编制等； 4)持续追踪安全漏洞整改进展，推动相关责任人按期完成修复； 5)每月基于承诺内容，对安全运行状况进行数据统计与分析，编制运维月报并按时提交。 6)安全日志采集、分析，收集现有安全设备如防火墙、IPS、网站防护系统、DDoS 防护等的日志信息，开展人工分析研判； 7)依据甲方网络安全管理制度，对各信息系统执行周期性安全抽查，并出具专项检查报告； 8)每日对安全设备执行运行状态巡检，驻场工程师直接登录设备核查，逐项填写巡检记录。巡检结束后输出《运维巡检日报》；巡检中如发现重大异常，需立即上报甲方主管人员，并协同推进问题处置； 9) 遭遇重大安全漏洞时，第一时间开展针对性专项检查；驻场工程师须每日跟踪安全设备的升级发布情况，及时完成同步升级，确保各安全设备系统版本始终保持最新且一致； 10)对态势感知平台、漏洞扫描及探针进行维护升级。定期对安全设备的系统版本、特征库、病毒库、威胁情报库和漏洞库等进行更新升级。 服务周期：服务期一年 服务交付物：包含不仅限于每日预警通报、月报、年报及其他报告，《运维巡检日报》、《安全加固建议》等。注：要求乙方提供二线专家支撑服务，按照标准的安全运营处置流程，二线专家对一线驻场工程师不能明确的安全事件进行综合研判，形成确认的安全事件报告。	

2	漏洞扫描服务	服务内容：采用专业的漏洞扫描工具及安全运营平台，通过定制的扫描规则，对服务器、网络设备、安全设备、web应用、数据库等进行自动化安全扫描，人工验证扫描结果并输出安全扫描报告及修复建议。漏洞扫描需全面覆盖甲方信息系统中的各类脆弱性风险，包括但不限于：信息探测类漏洞、后门程序类漏洞、域名服务类漏洞、Web安全类漏洞等；同时需识别安全配置缺陷、应用系统安全漏洞，排查系统弱口令，梳理非必要开放的账号、服务及端口。在此基础上，对发现的风险进行归类，明确风险类型、分布区域及严重等级，实现安全风险的可视化呈现。 服务周期：服务周期内对态势感知平台监管范围内的业务系统开展每年不少于 4 次漏洞扫描及复检服务。服务交付物： 《漏洞扫描报告》等	
3	应急管理服务	服务内容：当甲方信息系统遇到突发的安全问题如：发生网络入侵事件、大规模病毒暴发、遭受拒绝服务攻击等，无法及时对该事件进行处理或解决时，在收到甲方及相关单位的应急响应服务请求信息后，投标人应急专家需1小时抵达甲方现场，2小时完成应急处置、4小时完成溯源分析，8小时恢复系统上线运行。投标人应按照准备、检测、抑制、根除、恢复、跟踪标准化的流程，分析攻击路径、抑制事态发展、根除安全隐患、恢复系统重新上线运行，并对网络安全事件进行总结，编制《应急响应报告》。结合甲方信息系统现状及当前网络安全威胁态势，制定年度应急演练方案并组织实施。演练内容包括但不限于涵盖勒索病毒攻击、Web应用攻击、数据泄露、钓鱼邮件及供应链攻击等不少于六类典型安全事件场景。通过模拟真实攻击检验应急预案的可行性与安全防护体系的实际响应能力，提升安全运维团队的协同处置水平。每次演练结束后10个工作日内需提交演练计划、演练方案设计、演练动员与培训、应急演练实施、应急演练评估与总结等，并协助甲方完成问题整改，形成“演练—评估—改进—验证”的闭环管理。 服务周期：服务周期内应急响应按需提供，服务周期内应急演练开展不少于1次。 服务交付物： 《应急响应报告》《网络安全应急演练总结》等	
4	安全培训服务	服务内容：定期面向单位全体人员开展信息安全培训，内容涵盖个人隐私保护、钓鱼邮件防范、AI欺诈识别等安全意识提升，以及网络安全法规合规、APT攻击防御、大模型安全风险等专业知识培训，切实增强全员网络安全防护意识与日常风险识别能力，提升对AI驱动新型攻击的防范水平。 服务周期：服务期内需开展不少于2次。 服务交付物： 《安全培训课件》等。	

5	重要时期保障服 务	服务内容：在国家、省、市重要会议、重大活动及重大节假日期间，对态势感知平台监管范围内的业务系统提供7×24小时的安全保障服务，其间派遣安全服务人员进行现场值守，保障工程师利用人工结合工具等方式对单位信息系统、网站、服务器等资产进行实时监测，及时处理发现的系统安全事件。 1)服务前期的备战，包含服务计划、资源保障、人员安排等详细计划内容；根据服务目标制定详细计划并安排相应人员保障，例如攻击检查，则制定攻击检查计划，防守保障，则制定防守保障计划； 2)针对重要系统，应在开始前完成漏洞扫描、安全基线核查、安全加固等工作； 3)重大活动期间，完成安全监测、应急处理、追踪溯源等工作； 4)重保结束后，进行数据分析与报告总结，并对攻击进行复盘。 服务周期：服务周期内按需提供服务。 服务交付物： 《重要时期保障业务系统和资产列表》、 《脆弱性检查报告》《重要时期整改应急预案》、 《重要时期专题培训课件》《重大活动保障总结报告》《现场安全值守日报/巡检/监控报告》等。	