绍兴市中医院信息安全等级保护测评服务采购合同

合同编号：

甲方（采购人：）绍兴市中医院　　签订地点：绍兴

乙方（供应商：）杭州安信检测技术有限公司

签订时间：2024.6.16

根据《中华人民共和国民法典》，经公开采购，绍兴市中医院三级等保测评服务项目（招标编号：TYJZ2024017），双方就中标物品买卖达成如下协议。

一、中标物品名称、型号、价格（可附清单）

标物名称	型号、规格	生产厂家	数量	单 价	总 价
基础支撑系统	等保三级	杭州安信	1	50000.00	180000.00
面向患者服务系统（包括互联网医院、医院集成平台）	等保三级	杭州安信	1	50000.00	
OA 办公系统	二级	杭州安信	1	30000.00	
商用密码应用安全性评估	三级	杭州安信	1	50000.00	
合计人民币（大写） 壹拾捌万圆整					

二、交货时间、地点

接甲方通知后 15 个工作日内，按采购文件要求，乙方测评师进驻到甲方指定地点，5 个工作日后出具问题清单供甲方参考整改。等甲方整改完成后再次复核。整改工作完成后 20 个工作日内出具测评报告。

三、质量要求及验收

乙方保证提供的中标物品，必须符合采购文件要求，必须符合现行的国家或行业技术规格和质量标准执行。

四、付款方式

1、乙方出具测评报告后，甲方应在 60 个工作日内支付合同总额的 90%，即壹拾陆万捌仟圆整（￥162000.00）。

2、配合甲方完成公安备案后，甲方应在60个工作日内支付合同总额的10%，即壹万捌仟圆整（￥18000.00）。

五、本合同解除条件

1、乙方提供的物品,如不符合采购文件要求或延迟交货,经催告后15个工作日内仍未履行，甲方可以无条件退货，造成的一切损失由乙方承担。

2、乙方不得将中标权转让给其他厂商，否则追究乙方的违约责任。

3、经双方协商一致。

六、违约责任

1、乙方如未按合同规定时间供货，每超过一天，扣合同价0.1‰的违约金给甲方，违约金额在合同款中扣除。

七、解决合同纠纷的方式

本合同未尽事项或履行时发生争议，双方将本着诚实信用的原则，协商解决。协商不成的，由管理部门先予调解，调解不成可向绍兴市越城区人民法院起诉。

八、其他约定事项

1、未尽事宜可另行签订补充合同（协议）。

2、本项目的招标文件、投标文件作为本合同的附件，招标文件与投标文件矛盾之处以招标文件为准。

九、采购文件作为合同的附件。本合同一式肆份，甲乙双方各执贰份。

甲方	乙方
单位名称（盖章）：绍兴市中医院	单位名称（盖章）：杭州安信检测技术有限公司
单位地址：绍兴市越城区人民中路641号	单位地址：杭州市滨江区长河路590号东忠科技园2号楼
法定代表人	法定代表人：
委托代理人	委托代理人：
邮政编码：312000	邮政编码：310009
电话:0575-89109951	电话:13588578696
传真	传真
开户银行：中信银行绍兴越城支行	开户银行：杭州联合银行科技支行
帐号：7334410182600041810	帐号：201000192837745

保密协议

甲方：绍兴市中医院

地址：浙江省绍兴市越城区人民中路 641 号

联系人：王宁

联系电话：0575-89102270

电子邮箱：

乙方：杭州安信检测技术有限公司

地址：浙江省杭州市滨江区长河路 590 号

联系人：章小涛

联系电话：13588578696

电子邮箱：zxt@axjc.net

鉴于甲乙双方将在等级保护测评项目中互相披露保密资料，为了促进协议双方的洽谈、合同的签订及履行，明确协议双方的保密责任，甲乙双方经平等、友好协商，签订本协议，以共同信守。其中，披露信息的一方简称为“披露方”，接收信息的一方简称为“接收方”。

一、保密信息

保密信息指不为公众所知，披露方接收方披露的所有信息、数据或技术，包括但不限于披露方的与研究、开发、生产、产品、服务、客户、市场有关的软件、程序、发明、工艺、设计、图纸、专有技术、工程、流程、方式、硬件配置信息、客户名单、合同、价格、成本、研究报告、预测和估计、报表、商业计划、商业秘密、商业模式、公司决议等任何的商业信息、财务信息、技术资料、生产资料以及会议资料和文件。保密信息既包括书面认定为保密或专有的，又包括口头披露，后经书面确认为保密或专有的。以口头形式披露的保密信息须在披露时表明其为“保密”信息，并在披露后 10 天内以书面形式另行提供给接收方并作出适当的保密标记。

保密信息不包括：（1）并非由于一方违约而已经是或者日后成为众所周知的或可通过公开途径得到的信息；(2)在披露方披露之前接收方已知晓或已拥有

的信息，接收方应出具相关的文档记载予以证明，或该等信息在披露方披露时已成为公众公知的信息；(3)由接收方从不承担保密义务的第三方处合法接收的信息；(4) 接收方未参照或使用保密信息独立开发所得的信息；(5)经披露方事先书面同意而披露的信息。

二、保密义务

接收方应以保护其本身保密信息的同等程度，并且在任何情况下不低于合理程度地保护披露方的保密信息免于未经授权的使用、传播、公布或接触。未经披露方的事先书面批准，接收方仅可于协议双方之预期交易或商业关系的评估范围内使用披露方的保密信息，不得直接或间接以任何形式或任何方式将保密信息和/或其中的任何部分，披露、透露给任何第三方或者公开。接收方亦不得依据披露方提供的任何保密信息，就任何问题，向任何第三方作出任何建议。但接收方披露给其关联方不受上述约束。

双方均须把对保密资料的接触范围严格限制在因本协议规定目的而必须接触保密资料的各自负责任的代表的范围内。因开展工作之需要，接收方有权向其委托的顾问、关联方透露或使其接触保密信息的全部或其中的任何部分，但前提必须要求相关机构或人员签订相应的保密协议或保密承诺书。双方在此同意，上述代表违反本协议的行为也同样构成对本协议的违约。

接收方一经发现对保密信息的任何未经授权的披露或接收方及其人员违反本协议时，接收方应立即通知披露方，并采取措施防止进一步未经授权而使用保密信息。

接收方应法院或其它法律、行政管理部门要求披露的信息（通过口头提问、询问、要求资料或文件、传唤、民事或刑事调查或其他程序）因而透露保密信息，在该种情况发生时，接收方仅能向有关部门披露必要的信息，且应提前 3 日向披露方发出通知作出必要说明。特殊情况无法提前 3 日的，应当在披露时立即向披露方发出通知。

三、归还与销毁

经披露方随时书面要求或本协议终止时，接收方或接收方的代表应向披露方归还披露方的所有保密信息、含有该等保密信息的所有文件或媒介，以及该等信息的所有复制件或摘要；或销毁包含该等保密信息的所有文件或媒介，以及该等信息的所有复制件或摘要，并向披露方提供一份由接收方授权代表签署的关于该

等销毁的书面证明。尽管返还或销毁了全部保密信息和记录，在本协议保密期限内，接收方及其代表仍受保密义务和下述其他义务的约束。

四、所有权和知识产权

披露方向接收方或接收方代表披露保密资料并不构成向接收方或接收方的代表的转让或授予接收方对其商业秘密、商标、专利、技术秘密或任何其它知识产权拥有的权益，也不构成向接收方或接收方代表转让或向接收方或接收方代表授予披露方受第三方许可使用的商业秘密、商标、专利、技术秘密或任何其他知识产权的有关权益。

接收方不得对披露方向其披露的保密信息实施逆向工程、反编译或反汇编，不得删除、套印或涂抹披露方所披露的保密信息的任何原件或复制件上的任何著作权、商标、标识、图例说明或其他所有权说明。

五、不保证

披露方按照原样提供所有保密信息，并未就其准确性或性能、特定目的的适用性、或未侵权作出任何明示、暗示或其他形式的任何担保。

六、保密期限

本协议的保密期限，即接收方对披露方保密资料负有保密义务的期限，为双方谈判期间、合同履行期间，至披露方书面通知解除保密义务，或双方书面另行约定为止，或保密信息进入公知领域、依照法律法规不再成为保密信息，以时间较早者为准。

七、违约责任

协议一方违反本协议约定的行为将被视为违约行为，违约方除应当立即停止违约行为之外，还应当赔偿非违约方因此所遭受的损失。其赔偿损失的范围包括但不限于：非违约方的直接损失、丧失商业机会的损失、丧失相关权利的损失、调查违约行为而支出的合理费用以及仲裁费、诉讼费、律师费等。

鉴于保密信息的唯一性和自身价值，双方认可接收方对本协议的任何违反将导致披露方不可挽回的损失，且该损失和后果是金钱不足以弥补的。因此，对于本协议的任何违反，除法律赋予的权利和救济外，披露方还有权获得禁令救济。

八、一般条款

本协议取代先前就本协议主题事宜作出的任何讨论或达成的任何书面协议，

且构成双方就本协议主题事宜达成的完整协议。对本协议的任何弃权或修改须以书面方式作出，并经每一方的授权代表正式签署方对双方具有约束力，未行使某一权利或延迟行使某一权利不得被视为放弃该等权利。

若本协议的某一条款根据现行法律或被法院认定为无效或者效力存疑，本协议其余条款的效力不受影响。本协议对协议各方的权利义务继受人和合法受让人均具有约束力。

本协议受中华人民共和国法律管辖并按中华人民共和国法律解释。对因本协议或本协议各方的权利和义务而发生的或与之有关的任何事项和争议、诉讼或程序，本协议双方不可撤销地接受中华人民共和国杭州市滨江区人民法院管辖。

本协议经协议双方法定代表人或授权代表签字并加盖公司公章或合同专用章后生效。本协议一式两份，具有同等法律效力，协议双方各执壹份。

甲方：
（盖章）
授权代表：
签订日期：2014年 6 月 16 日

乙方：
（盖章）
授权代表：
签订日期：2014年 6 月 16 日

基建工程和医药购销等廉洁合约（合同）

为加强卫生健康系统廉政建设，切实纠正各类招标和采购等经济活动的不正之风，杜绝商业贿赂，绍兴市各医疗卫生单位与各施工单位、生产经营企业及代表，在签定有关经济合同时，必须签定《建设工程廉洁合约》或《购销廉洁合约》。

甲方绍兴市中医院与乙方杭州安信检测技术有限公司签定如下廉洁合约（合同）：

1、甲乙双方在各种招标、采购等经济活动中，均要严格执行有关法律、上级有关部门及绍兴市卫健委的有关规定，规范操作程序，公平公正交易，践行合同承诺。

2、甲乙双方经办人员不准私下洽谈业务，不准组织可能影响公正执行公务的各类活动，不准违反规定私自向对方提供内部信息和个人承诺，不准在合同之外私定潜规则。

3、甲方在编制招标文件、提出资质要求、技术参数及规格型号、确定采购计划等工作环节中，要遵循有关法律法规和专项规定，做到公开透明，科学合理，公平准入，条件明确。

4、乙方在参与招标和实施合同规定过程中，做到身份明确，证件无误，良性竞争，有序操作。在制定标书和履行合同时，要体现企业诚信和责任心。

5、甲方不违反规定，增加不合理条件限制或排斥有正当权益的经济当事人或潜在投标人，不违反公开、公平、公正原则制定歧视性规定，不接受和索要乙方为个人提供的各种名目的红包、回扣等，不参加乙方组织的旅游、娱乐、宴请等非公务活动。

6、乙方不仿造资质，不弄虚作假，不串通作弊，不以红包、回扣等不正当经济手段向甲方人员进行促销活动。

7、甲方如有违反廉洁规定的行为，乙方可向甲方上级主管单位或有关部门举报投诉，并配合调查处理。

8、乙方如有违法违规促销和不按规定履约行为，甲方有权按有关规定作出处理，停止乙方1—2年的采购活动或中断与乙方的业务关系，直至建议取消在绍兴市卫生健康系统的招投标资格。

甲方：（盖章）

甲方代表人（签名）

2019 年 6 月 16 日

乙方：（盖章）

乙方代表人（签名）

2019 年 6 月 16 日

绍兴市中医院 应用信息技术服务人员
保密承诺书

绍兴市中医院：

为保障贵单位网络和数据安全，本人在从事信息系统开发、运维、管理过程中，将严格遵守以下承诺：

一、严格遵守《网络安全法》《数据安全法》《个人信息保护法》《保密法》等相关法律法规和贵单位有关规章制度。

二、妥善保管涉及项目相关的业务和技术资料，包括相关会议资料、业务系统的软硬件、技术文档、源代码、开发测试运维过程中产生的数据、使用的账号权限等，防止泄露、传播或转借他人。

三、严格执行数据调用审批流程，对重要敏感数据实行先审批后操作，针对数据库等核心设备进行操作时将通过安全防护设备或采取实时监控等有效措施，防止出现未经审批、未落实监管直接操作重要敏感数据。

四、严格执行安全运维有关规定，原则上采取现场驻点运维，绝不开展未落实安全保护措施的远程运维，绝不将真实公共数据部署在测试服务器等不可控环境。

五、严格按照授权范围使用相关数据，未经授权不以任何方 式将相关数据提供给第三方或用于其他目的，未经授权不对数据 进行任何增加、删除、修改等操作，防止相关数据被恶意篡改、破坏。

六、如发现数据安全隐患或其他不安全因素，第一时间上报，并密切配合主管部门做好数据安全事件的处置及调查工作，并采取相应措施，及时排除信息安全隐患，修复漏洞。

七、若违反本承诺书有关条款或国家相关法律法规，本人将承担相应的法律责任。

八、本承诺书一式两份，自签署之日起生效并遵行。

承诺人：

所属单位：杭州安信检测技术有限公司（盖章）

2024 年 6 月 16 日

绍兴市中医院 应用信息技术服务外包单位
网络安全承诺书

绍兴市中医院:

为确保我单位开发/运维的三个系统安全稳 定运行，我单位郑重承诺：认真落实等级保护测评部署的各项网络安全工作任务，采取包括增加人员和经费投入在内的一切必要手段，确保系统安全运行，确保不发生网络安全事件。

我单位明确： 何冠辉 为我单位项目负责人，全面负责信息 系统管理和网络安全工作，派出骨干技术力量负责项目的开发、运维 和保障工作。我单位将把应用系统安全运行情况纳入对上述人员的奖惩考核范围并充分征求贵单位意见。

我单位承诺：1.按照国家法律法规和技术标准加强网络安全技术 防护，确保自身和相关供应链的网络安全，积极配合贵单位和国家涉 网监管部门组织的检查、检测等工作。2.与贵单位官方网络安全服务 合作伙伴做好技术对接，确保重要网络安全态势信息互联互通。3.按 照最小化原则管理相关权限、信息和数据，对重要信息系统原则上采 用双因子认证进行身份认证和授权访问。4.对重要敏感数据实行先审批后操作，针对数据库等核心设备进行操作时将通过安全防护

设备或采取实时监控等有效措施，防止出现未经审批、未落实监　管直接操作重要敏感数据。5.严格执行安全运维有关规定，原则　上采取现场驻点运维，绝不开展未落实安全保护措施的远程运维，　绝不将真实公共数据部署在测试服务器等不可控环境。6.做好日　常监测、技术巡检等工作，及时修复高危漏洞、关闭高危端口，配备　防范页面篡改、黑客攻击、病毒入侵、系统故障、数据泄露等情况的　技术力量，确保系统安全稳定运行。7.制定应急预案，并定期开展应　急演练，当发生网络安全事件时，应于24 小时内向贵单位书面反馈　突发网络安全和数据安全事件处置情况。8. 留存系统日志、应用日志　和行为审计日志等直至项目结束，确保网络访问行为可记录、可追溯。 9.系统运行结束后按照贵单位的要求处置相关数据，确保系统安全关
停。

我单位确认：已对该项目暴露在互联网上的系统测试账号、配置 文件、系统数据、测试环境、试运行环境、密码记录、源代码(包括 github、gitlab等)、弱口令、技术方案等与项目安全运行无关的信息进
行了清理，后续也将对上述信息进行有效管理。

如我单位承建信息系统发生任何网络安全事件引发任何损失，我单位将采取一切可能的措施配合贵单位积极开展处置，承担相应损失，并追究相关人员责任。

单位名称(盖章)：

2024 年 6 月 26 日