网络安全等级保护测评
技术服务合同

项目名称　陕西省住房和城乡建设厅综合服务中心等保测评项目

甲　　方　陕西省住房和城乡建设厅综合服务中心

乙　　方　西安尚易安华信息科技有限责任公司

甲方通过竞争性磋商采购陕西省住房和城乡建设厅综合服务中心等保测评服务，并接受了乙方以价格(贰拾陆万陆仟元整)(以下简称“合同价”)提供的服务。

本合同在此声明如下：

1. 本合同中的词语和术语的含义与合同条款中定义的相同。

2. 下述文件是本合同的一部分，并与本合同一起阅读和解释：

2.1 合同条款

2.2 合同条款附件

附件 1—服务内容

附件 2—服务方案

附件 3—保密协议

2.3 成交通知书

2.4 竞争性磋商文件

2.5 竞争性磋商响应文件

3. 考虑到甲方将按照本合同向乙方支付款项，乙方在此保证全部按照合同的规定向甲方提供服务，并修补缺陷。

4. 考虑到乙方提供的服务并修补缺陷，甲方在此保证按照合同规定的时间和方式向乙方支付合同价或其他按合同规定应支付的金额。

5. 付款方式：（银行转帐）

合同签订后，乙方向甲方支付合同额的 5%作为项目履约金，乙方持成交通知书原件和等额发票在采购人处申请办理此项目成交金额 100%款项的支付手续，并由甲方支付项目成交金额 100%款项。乙方向甲方提交最终成果交付物且项目验收合格后 2 个工作日内，甲方向乙方退还 5%的项目履约金。

6. 服务期限：两个月。

7. 本合同一式陆份，其中，甲方叁份，乙方叁份。

8. 本合同由甲乙双方共同签字盖章，自最后一方签字盖章之日起生效。

甲方名称：陕西省住房和城乡建设厅综合服务中心

地　　址：西安市东新街240号平安银行大厦四楼

邮　　编：710000

电　　话：(029)87252990

传　　真：(029)87252990

开户银行：光大银行新城支行

账号：78700188000039564

法定代表人或授权代表签字：白波

盖章：

2024年12月3日

乙方名称：西安尚易安华信息科技有限责任公司

地　　址：西安市碑林区雁塔北路67号红锋商务大厦4层西

邮　　编：710000

电　　话：(029)89525570

传　　真：(029) 89536135

开户银行：建设银行西安和平门支行

帐　　号：61050176370000001469

法定代表人或授权代表签字：郝大永

盖章：

2024年12月3日

第一条 本着平等互惠、互相支持、共同发展的原则，就甲方针对本项目的事宜， 经甲乙双方友好协商， 共同签署本合同， 以资共同遵守。

第二条 服务定义：根据甲方需要，乙方为甲方提供该项目的服务等业务。

第三条 乙方服务人员：是指乙方派出的符合本合同资格条件的、在甲方从事本合同规定的服务项目范围以内工作的人员。乙方有义务在本合同有效期内维持其与服务人员合法的劳动合同关系，不得因与服务人员间就劳动法律关系或在其他方面的任何争议或瑕疵影响其履行在本合同项下的义务。

第四条 甲方的权利

1. 甲方有权享有乙方按照上述约定提供的服务。

2. 甲方有权要求乙方提供符合本项目服务要求的人员，且提供的服务质量达到前述约定标准。如乙方违反协议约定，未达到服务质量要求的，甲方有权要求乙方限期改正，逾期未改正的或改正后仍给甲方造成损失的，乙方应承担相应的法律责任；

3. 甲方有权根据服务要求和标准考评乙方服务质量，如乙方提供的服务考评不合格或不符合约定的，甲方有权按照一定比例减少支付服务费用，具体减付比例结合乙方提供服务未达到约定的范围，严重程度、给甲方造成的损失情况等确定。

4. 除本合同约定的服务费用外，乙方不得向甲方及其甲方人员收取其他任何费用，如甲方发现乙方有此类行为，甲方有权要求乙方清退所收费用，退还利息并支付违约金；

5. 对乙方相关服务资料的所有权、使用权的约定：归甲方所有。乙方不得以任何借口留存，否则承担由此产生的一切法律和经济责任。未经甲方允许，任何单位和个人不得转让和使用本项目的相关内容。

第五条 甲方的义务

1. 在服务实施过程中，甲方应为乙方提供必要的工作便利与指导，配合乙方履行职责。

2. 甲方不得将本合同的内容向甲乙双方以外的、与签订和履行本合同无关的任何第三方透露，不得泄露乙方的商业秘密（包括本合同及其附件和合同签订前的各项方案）。

第六条 任何一方违反或擅自变更本合同的约定，应当承担由此给对方造成的经济损失和相关责任。

第七条甲方违约责任

1. 由于甲方的原因或因不可抗力的自然因素影响，则服务时长顺延。

2. 对于乙方提供的资料以及属于乙方的内容，甲方有义务保密，不得向第三方提供或用于本合同以外的项目，否则乙方有权要求甲方按本合同项目款总额的 20%赔偿损失。

第八条乙方违约责任

1. 合同签订后，如乙方擅自中途停止或解除合同，乙方应向甲方双倍返还定金。没有约定定金的，乙方向甲方赔偿服务价款。

2. 在甲方提供了必要的工作、生活条件，并且保证了项目款按时到位，乙方未能按合同规定的日期提供服务时，应向甲方赔偿拖期损失费，每天的拖期损失费按合同约定的项目总价款。

3. 因天气、交通、政府行为、甲方提供的资料不准确等客观原因造成的时长拖期，乙方不承担赔偿责任。

4. 服务实施过程中，乙方未按竞争性磋商响应文件约定配备服务人员或乙方派驻服务力量无法胜任项目实施要求的，甲方有权提出增加人员和充实技术力量，乙方应立即安排实施，其费用被认为已含在合同价格之中。如乙方拒绝增加人员或充实技术力量，甲方有权利解除合同，乙方应承担由此给甲方造成的经济损失。

5. 乙方有责任按甲方要求提交项目资料。如乙方未能按规定的时间提供服务，每延误一天，应付逾期违约金人民币（但由于受天气等不可抗力的自然因素影响，则工期顺延），逾期 10 天以上的，甲方除有权终止履行合同外，乙方应

承担因延期造成的损失。同时，甲方有权根据乙方所承担服务的质量是否符合要求而对服务的内容进行调整。

6. 乙方提供的服务质量不合格的，乙方应负责无偿予以采取补救措施，以达到质量要求。因服务最终不符合合同要求（而又非甲方提供的资料原因所致）造成后果时，乙方应对因此造成的直接损失负赔偿责任，并承担相应的法律责任（由于甲方提供的资料原因产生的责任由甲方自己负责）。

7. 在合同期内和合同终止后，乙方应负责所有资料的保密，非经甲方书面认可，不得向任何人以任何方式提供任何资料。严格按甲方要求程序传递各种资料，否则甲方有权单方解除合同，并追回所付项目款。

8. 乙方不得将本项目的任何部分转包或分包给其他任何单位和个人。若擅自转包或分包本合同标的，甲方有权解除合同，并可要求乙方偿付预算 30%的违约金，同时追究其法律责任。

第九条 甲乙任何一方按照本合同规定索取违约金或赔偿金时，应书面通知违约方并说明违约金或赔偿金额；违约方应在收到对方发出的书面索赔通知的十个工作日内按索赔要求支付违约金或经济赔偿；如违约方对违约金或赔偿金额有异议，应在收到通知后七个工作日内通知对方，双方应在收到对方的通知或答复后尽快协商明确违约责任。

第十条 因执行本合同发生的一切争议，双方应首先友好协商解决。经协商不能解决，应向甲方所在地人民法院提起诉讼。在诉讼期间，除必须在诉讼过程中进行解决的问题外，合同其余部分应继续履行。

第十一条 甲、乙双方有一方有正当理由要求变更本合同，须提前一个月以书面形式通知对方并协商解决，双方应签署变更合同。

第十二条 本合同期满双方不再续约或者因一方违约导致本合同无法履行，则本合同终止。但合同的终止不得损害第三方的利益，双方应为此做出合理安排。

第十三条 未经对方同意，甲乙任何一方不得将本合同部分或全部权利和义务转让给第三方。

第十四条 本合同中涉及的所有“通知”、“同意”、“确认” 等事项均应以书面形式做出，并作为依据。

第十五条 本合同有关附件及补充合同是本合同不可分割的组成部分，与本合同具有同等法律效力；本合同未尽事宜，双方另行协商并签署补充合同，作为本合同的附件，具有同等法律效力。

附件 1—服务内容：根据采购需求填写

附件 2—服务方案：根据响应方案填写

附件 1—服务内容：

1. 建设目标

1.1项目总体定位

陕西省住房和城乡建设厅综合服务中心信息系统主要为 4 个业务系统，按照网络安全等级保护第三级要求进行备案及测评工作。

1.2项目总体目标

依据国家相关标准开展等级保护，通过开展等级保护推动安全工作的进一步落实，保障和促进陕西住房和城乡建设厅信息化建设健康发展。同时，也指导陕西省住房和城乡建设厅综合服务中心的信息安全保障建设，促进安全管理水平的提高，增强信息安全风险管理意识。

2. 服务内容

完成陕西省住房和城乡建设厅综合服务中心信息系统的本次等级保护测评工作。并出具测评报告、协助用户单位进行整改，整改后进行复测评工作。

本项目涉及系统范围如下：

序号	系统名称	定级
1	陕西省住建注册人员（二级）管理系统	第三级
2	陕西省住建执业人员资格考试管理系统	第三级
3	陕西省住房和城乡建设厅综合服务中心网站	第三级
4	陕西省住建行业电子证书系统	第三级

附件 2—服务方案：

1. 等级保护测评服务要求

依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）和《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）等国家关于信息系统安全等级保护的相关标准和规范要求，为 4 个系统提供等级保护测评实施工作，包括物理安全环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理 10 个方面。并出具 4 个系统的测评报告、整改建议书。

1.1等级保护测评技术要求

投标人应按照国家相关要求，从“定级-备案-等级测评-安全建设整改-配合监督检查”5 个环节配合采购单位做好等级保护工作。其中针对等级测评工作过程，依据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）和《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449-2018）等国家关于信息系统安全等级保护的相关标准和规范要求，要求参选人严格按照下列流程开展工作：

测评准备阶段：是开展等级测评工作的前提和基础，是整个等级测评过程有效性的保证。测评准备工作是否充分直接关系到后续工作能否顺利开展。本活动的主要任务是掌握被测系统的详细情况，准备测试工具，为编制测评方案做好准备。

方案编制阶段：是开展等级测评工作的关键活动，为现场测评提供最基本的文档和指导方案。本活动的主要任务是确定与被测信息系统相适应的测评对象、测评指标及测评内容等，并根据需要重用或开发测评指导书，形成测评方案。

现场测评阶段：是开展等级测评工作的核心活动。本活动的主要任务是按照测评方案的总体要求，严格按照测评指导书执行，分步实施所有测评项目，以了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。

分析与报告编制阶段：是给出等级测评工作结果的活动，是总结被测系统整体安全保护能力的综合评价活动。本活动的主要任务是根据现场测评结果和《信息安全技术 网络安全等级保护实施指南》的有关要求，通过单项测评结果判定、

单元测评结果判定、整体测评和风险分析等方法，找出整个系统的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距导致被测系统面临的风险，从而给出等级测评结论，形成《网络系统安全等级保护 XX 系统等级测评报告》文本。

建设整改咨询阶段：建设整改咨询工作以等级测评发现的安全问题为工作重点，以及测评报告中安全建设整改建议；将信息系统的安全建设整改需求落实到可操作的安全技术和管理上，提出能够实现的技术参数或制度及其具体规范。并依据测评报告中安全建设整改建议开展建设整改工作时，投标人将提供建设整改过程中的与建设整改相关的咨询服务。

1.2等级保护测评工作指标

三级要求指标

安全层面	安全控制点	测评指标（2.0）
安全物理环境	物理位置选择	a）机房场地应选择在具有防震、防风和防雨等能力的建筑内；
		b）机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员。
	防盗窃和防破坏	a）应将设备或主要部件进行固定，并设置明显的不易除去的标识；
		b）应将通信线缆铺设在隐蔽安全处；
		c）应设置机房防盗报警系统或设置有专人值守的视频监控系统。
	防雷击	a）应将各类机柜、设施和设备等通过接地系统安全接地；
		b）应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。
	防火	a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
		b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
		c）应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。
	防水和防潮	a）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
		b）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
		c）应安装对水敏感的检测仪表或元件，对机房进

		行防水检测和报警。
	防静电	a）应采用防静电地板或地面并采用必要的接地防静电措施；
		b）应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
	温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
	电力供应	a）应在机房供电线路上配置稳压器和过电压防护设备；
		b）应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；
		c）应设置冗余或并行的电力电缆线路为计算机系统供电。
	电磁防护	a）电源线和通信线缆应隔离铺设，避免互相干扰；
		b）应对关键设备实施电磁屏蔽。
安全通信网络	网络架构	a）应保证网络设备的业务处理能力满足业务高峰期需要；
		b）应保证网络各个部分的带宽满足业务高峰期需要；
		c）应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；
		d）应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；
		e）应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
	通信传输	a）应采用校验技术或密码技术保证通信过程中数据的完整性；
		b）应采用密码技术保证通信过程中数据的保密性。
	可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全区域边界	边界防护	a）应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；
		b）应能够对非授权设备私自联到内部网络的行为进行核查或限制；
		c）应能够对内部用户非授权联到外部网络的行为进行核查或限制；
		d）应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
	访问控制	a）应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接

		口拒绝所有通信；
		b）应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
		c）应对源地址、目的地址、源端口、目的端口和协议等进行核查，以允许/拒绝数据包进出；
		d）应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；
		e）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
	入侵防范	a）应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
		b）应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
		c）应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；
		d）当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。
	恶意代码和垃圾邮件防范	a）应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新；
		b）应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。
	安全审计	a）应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
		d）应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析。
	可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。
安全计算环境	身份鉴别	a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
		b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
		c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

		d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。
	访问控制	a）应对登录的用户分配账户和权限；
		b）应重命名或删除默认账户，修改默认账户的默认口令；
		c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；
		d）应授予管理用户所需的最小权限，实现管理用户的权限分离；
		e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
		f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
		g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。
	安全审计	a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
		b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
		c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
		d）应对审计进程进行保护，防止未经授权的中断。
	入侵防范	a）应遵循最小安装的原则，仅安装需要的组件和应用程序；
		b）应关闭不需要的系统服务、默认共享和高危端口；
		c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
		d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
		e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；
		f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

	数据完整性	a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等；
		b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
	数据保密性	a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
		b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
	数据备份恢复	a）应提供重要数据的本地数据备份与恢复功能；
		b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
		c）应提供重要数据处理系统的热冗余，保证系统的高可用性。
	剩余信息保护	a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
		b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。
	个人信息保护	a）应仅采集和保存业务必需的用户个人信息；
		b）应禁止未授权访问和非法使用用户个人信息。
安全管理中心	系统管理	a）应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；
		b）应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
	审计管理	a）应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
		b）应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
	安全管理	a）应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；
		b）应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

	集中管控	a）应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
		b）应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
		c）应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
		d）应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求；
		e）应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
		f）应能对网络中发生的各类安全事件进行识别、报警和分析。
安全管理制度	安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
	管理制度	a）应对安全管理活动中的各类管理内容建立安全管理制度；
		b）应对管理人员或操作人员执行的日常管理操作建立操作规程；
		c）应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。
	制定和发布	a）应指定或授权专门的部门或人员负责安全管理制度的制定；
		b）安全管理制度应通过正式、有效的方式发布，并进行版本控制。
	评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。
安全管理机构	岗位设置	a）应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权；
		b）应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；
		c）应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
	人员配备	a）应配备一定数量的系统管理员、审计管理员和安全管理员等；
		b）应配备专职安全管理员，不可兼任。
	授权和审批	a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
		b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；

		c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。
	沟通和合作	a）应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；
		b）应加强与网络安全职能部门、各类服务方、业界专家及安全组织的合作与沟通；
		c）应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
	审核和核查	a）应定期进行常规安全核查，核查内容包括系统日常运行、系统漏洞和数据备份等情况；
		b）应定期进行全面安全核查，核查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；
		c）应制定安全核查表格实施安全核查，汇总安全核查数据，形成安全核查报告，并对安全核查结果进行通报。
安全管理人员	人员录用	a）应指定或授权专门的部门或人员负责人员录用；
		b）应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；
		c）应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
	人员离岗	a）应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
		b）应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
	安全意识教育和培训	a）应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
		b）应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；
		c）应定期对不同岗位的人员进行技能考核。
	外部人员访问管理	a）应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案；
		b）应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
		c）外部人员离场后应及时清除其所有的访问权限；
		d）获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。
安全建设管理	定级和备案	a）应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；

		b）应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；
		c）应保证定级结果经过相关部门的批准；
		d）应将备案材料报主管部门和相应公安机关备案。
	安全方案设计	a）应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
		b）应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件；
		c）应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
	产品采购和使用	a）应确保网络安全产品采购和使用符合国家的有关规定；
		b）应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求；
		c）应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。
	自行软件开发	a）应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；
		b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；
		c）应制定代码编写安全规范，要求开发人员参照规范编写代码；
		d）应具备软件设计的相关文档和使用指南，并对文档使用进行控制；
		e）应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测；
		f）应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；
		g）应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。
	外包软件开发	a）应在软件交付前检测其中可能存在的恶意代码；
		b）应保证开发单位提供软件设计文档和使用指南；
		c）应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
	工程实施	a）应指定或授权专门的部门或人员负责工程实施过程的管理；
		b）应制定安全工程实施方案控制工程实施过程；
		c）应通过第三方工程监理控制项目的实施过程。
	测试验收	a）应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；

		b）应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。
	系统交付	a）应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；
		b）应对负责运行维护的技术人员进行相应的技能培训；
		c）应提供建设过程文档和运行维护文档。
	等级测评	a）应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
		b）应在发生重大变更或级别发生变化时进行等级测评；
		c）应确保测评机构的选择符合国家有关规定。
	服务供应商选择	a）应确保服务方的选择符合国家的有关规定；
		b）应与选定的服务方签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务；
		c）应定期监督、评审和审核服务方提供的服务，并对其变更服务内容加以控制。
安全运维管理	环境管理	a）应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；
		b）应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定；
		c）应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
	资产管理	a）应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；
		b）应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
		c）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。
	介质管理	a）应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点；
		b）应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
	设备维护管理	a）应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
		b）应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等；
		c）信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重

		要数据应加密；
		d）含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。
	漏洞和风险管理	a）应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；
		b）应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。
	网络和系统安全管理	a）应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限；
		b）应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
		c）应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
		d）应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等；
		e）应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；
		f）应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；
		g）应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；
		h）应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；
		i）应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道；
		j）应保证所有与外部的连接均得到授权和批准，应定期核查违反规定无线上网及其他违反网络安全策略的行为。
	恶意代码防范管理	a）应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码核查等；
		b）应定期验证防范恶意代码攻击的技术措施的有效性。
	配置管理	a）应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；
		b）应将基本配置信息改变纳入变更范畴，实施对

		配置信息改变的控制，并及时更新基本配置信息库。
	密码管理	a）应遵循密码相关国家标准和行业标准；
		b）应使用国家密码管理主管部门认证核准的密码技术和产品。
	变更管理	a）应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施；
		b）应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程；
		c）应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。
	备份与恢复管理	a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；
		b）应规定备份信息的备份方式、备份频度、存储介质、保存期等；
		c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。
	安全事件处置	a）应及时向安全管理部门报告所发现的安全弱点和可疑事件；
		b）应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；
		c）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；
		d）对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。
	应急预案管理	a）应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；
		b）应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；
		c）应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；
		d）应定期对原有的应急预案重新评估，修订完善。
	外包运维管理	a）应确保外包运维服务方的选择符合国家的有关规定；
		b）应与选定的外包运维服务方签订相关的协议，明确约定外包运维的范围、工作内容；
		c）应保证选择的外包运维服务方在技术和管理方面均应具有按照等级保护要求开展安全运维工作

		的能力，并将能力要求在签订的协议中明确； d）应在与外包运维服务方签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

1.3等级保护测评服务要求

（1）服务质量保证：测评机构应能根据质量体系要求建立科学的质量保证体系，从人员配备、工具保障以及科学的测评方法论、工作过程等多方面保证项目实施过程的质量。通过“项目调研-计划编制-方案编制-现场测评-编制测评报告”几个环节严格执行，并在重要环节进行文档评审，保证报告结论准确性。

（2）测评工具配备：要求测评过程使用专用测评设备，并配备国家权威机构认证的测评漏洞扫描工具，工具应具有相关采购证明材料。

（3）人员配备：为保证本项目测评工作质量及进度要求，项目组要求至少配备 5 名测评人员。项目经理要求至少为高级测评师，在本行业从事 5 年及以上，具备丰富的项目实施经验和技术能力；项目组成员至少 2 名中级测评师在本行业从事 2 年及以上，要求质量负责人具有中级测评师证书。

1.4测评服务原则

为保障项目的顺利实施，在项目实施过程须遵循以下原则：

（1）规范性原则

加强项目管理，在人员、质量和时间进度等方面进行严格管控。

（2）标准化原则

测评过程须严格遵守国家的相关法律、法规、规范、标准等相关要求。

（3）完整性原则

在测评过程中，必须确保测评数据、过程记录的完整性。评测内容要综合考虑所有评测对象的技术措施，并建立完整有效的评测流程，保证不存在影响评测结果的疏忽或遗漏。

（4）保密性原则

在测评过程中，切实加强对人员、技术等方面的组织管理；与采购人签署具有法律意义的保密协议，确保在项目实施过程中涉及的所有信息，不会泄露给第三方单位或个人，不得擅自利用这些信息。

（5）影响最小原则

在项目实施的过程中，须充分考虑到相关活动对系统正常运行的不利影响，采取必要的措施将相关风险降到最低。

2. 等保测评交付及期限

根据项目内容要求，以电子版或纸版形式按需求输出成果，并针对陕西省住房和城乡建设厅综合服务中心的咨询进行及时反馈，方式不限于现场支撑、邮件、电话或报告。主要产出物包括但不限于：

交付物：《网络安全ＸＸ系统等保测评方案》；

《网络安全等级保护ＸＸ系统整改方案》（每系统一份）；

《网络安全等级保护ＸＸ系统等级测评报告》（每系统一份）；

交付时限：中标人应在陕西省住房和城乡建设厅综合服务中心规定的时间内完成相关工作。

附件 3—保密协议

甲方：陕西省住房和城乡建设厅综合服务中心

乙方：西安尚易安华信息科技有限责任公司

一、总则

（一）为确保甲乙双方在陕西省住房和城乡建设厅综合服务中心网络安全等级保护测评服务采购中的信息安全合作事宜有序开展，杜绝项目实施过程中保密信息泄露事件的发生，经甲乙双方友好协商,签订本协议。

（二）本协议适用于甲乙双方本次合作开展的信息系统等级保护测评服务项目。

二、信息保密要求

乙方须遵守以下条款，对项目涉及的信息进行保密：

（一）乙方在为甲方提供本次服务中，应对来源于服务对象的所有信息进行涉密情况的征询，对于甲方的保密信息要做好保密管理。

（二）对来源于服务对象及甲方的所有信息（包括但不限于项目商务及技术资料、报告、摘要、纪要、文件、计划、报表、复印件、信息系统应用数据等），乙方负有保密责任，应采取有效保密措施确保网络安全。

（三）乙方人员须在甲方工作人员允许和在场的情况下对甲方内部信息数据进行操作，乙方不得擅自复制、传播服务对象及甲方的项目信息，不得外泄信息。

（四）乙方在使用完安全技术设备带离现场时，须在甲方监督下及时使用不可恢复的删除方式彻底删除设备内的甲方内部信息。未经甲方许可，不得带走甲方有关文件、资料和数据。

（五）乙方的项目实施工作计划需甲方确认后实施，且必须在甲方指定

的工作场所进行项目实施，未经甲方书面同意，乙方不得在该场所之外的其他任何场所进行。

（六）乙方在项目实施过程中，参与测评的乙方人员应遵守甲方有关规章制度。

（七）项目完成后，乙方应将项目信息完整交甲方，不得保留项目信息的副本，相关纸质及电子资料必须销毁，防止信息外流。

（八）乙方不得泄露服务对象项目应用系统及数据库的账号和密码。

（九）乙方工作人员调离乙方公司时，乙方公司应负责采取相关措施防止信息泄露；否则发生的项目信息泄露责任，由乙方负责。

（十）乙方违反本协议，甲方有权要求乙方及时采取补救措施，以防止损失的进一步扩大。如因乙方原因造成甲方任何资料泄露致使甲方遭受相关经济损失或不良后果，甲方可解除与乙方签订的本次项目合同，同时乙方须承担全部责任，性质严重的，由相关部门追究法律责任。

三、甲方须遵守以下条款，对项目涉及的乙方内部信息进行保密

（一）甲方提供涉密技术资料、数据、商务资料时应向乙方明示，并加盖“保密”鉴章。

（二）甲方不得向任何第三方披露乙方的工作程序，技术工具、设备、方法等。

（三）甲方不得向任何第三方披露乙方的技术资料或文档，包括但不限于项目过程文档、实施方案等。

四、保密期限

本保密协议有效期限为一年，自甲方信息系统网络安全等级保护测评服务采购项目生效之日起算。如果所涉及的保密信息依照国家有关法律、法规其保密期限超过上述规定的年限，则双方的保密责任在这些法律法规规定的

年限内继续有效。

五、其它

（一）本协议作为甲乙双方签订合同的附件，与合同具有同等法律效力，在甲乙双方合作期限内有效。

本协议一式陆份，甲方叁份乙方叁份，均具有同等法律效力。

（以下无正文内容）

本协议由以下双方签署，以资证明。

甲　　方：陕西省住房和城乡建设厅综合服务中心

法定代表人或授权代表：

乙　　方：西安尚易安华信息科技有限责任公司

法定代表人或授权代表：

合同专用章

签 署 日 ：2024 年 12 月