政府采购合同　　合同编号：

信息系统等级保护测评采购项目

采购人：陕西省交通运行监测中心

乙方：西安尚易安华信息科技有限责任公司

二〇二五年六月

合同主要条款

采购人（甲方）：陕西省交通运行监测中心

乙方（乙方）：西安尚易安华信息科技有限责任公司

根据《中华人民共和国民法典》及其他有关法律、法规，遵循平等、自愿、公平和诚信的原则，双方就下述项目范围与相关服务事项协商一致，订立本合同。

一、项目概况

1.项目名称：信息系统等级保护测评；

2.项目地点：陕西省西安市；

二、组成本合同的文件

1.中标通知书（成交通知书）、政府采购招投标文件、澄清函等文件；

2.本合同签订后，双方依法签订的补充协议。

三、合同金额

合同金额（大写）：叁拾伍万贰仟元整（￥352000）（含税，增值税税率6%）。

合同价格为含税价，乙方提供服务所发生的一切费用等都已包含于合同价款中。

四、付款方式

1.银行转账。

2.合同签订后乙方必须提供相应发票给甲方，收到乙方的发票后，达到付款条件起 14 个日历日内，支付合同总金额的100.00%。

乙方开户行：建设银行西安和平门支行

乙方户　名：西安尚易安华信息科技有限责任公司

乙方账　号：61050176370000001469

五、服务期限

合同签订后 1 年

六、内容及要求

1. 服务内容

序号	系统名称	级别	工作内容
1	陕西省交通运输云平台	三级	依据国家等级保护测评工作标准 GB/T22239-2019《信息安全技术 网络安全等级保护基本要求》、GB/T28448-2019《信息安全技术 网络安全等级保护测评要求》，完成物理安全环境、安全通信网络、安全区域边界、安全计算环境、安全管理制度等 10 个方面对信息系统实施等级保护测评服务，并出具系统测评报告。
2	陕西省交通运行监测调度平台	三级	
3	陕西省交通行业专网	二级	
4	陕西省公路水路建设与运输市场信用信息服务系统	二级	
5	陕西省交通运输统计分析监测和投资计划管理信息系统	二级	
6	陕西省交通地理信息共享服务平台	二级	

2. 服务要求

2.1 总体要求

根据国家《信息安全等级保护管理办法》(公通字[2007]43 号) 与《信息安全技术 网络安全等级保护基本要求》GB/T22239-2019 要求，等级测评工作须覆盖安全物理环境、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、安全运维管理等方面的内容，并根据现场实际情况完成风险分析工作，最终为完善等级保护安全防护体系提供指导依据。

2.2 测评备案

第一阶段：等级保护信息安全等级保护工作共分为五步，分别是："定级、备案、建设整改、等级测评、监督检查"。该项目主要完成系统的安全测评工作，依据安全技术和安全管理两个方面的测评要求，分别从安全物理环境、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、安全运维管理十个安全类别进行安全测评。

（1）定级要求：该项工作开展的主要依据是《网络安全等级保护定级指南》（GB/T 22240-2020）确定系统等级。

（2）备案：信息系统的安全保护等级确定后，二级以上（含二级）信息系统的运营使用单位或主管部门应到属地公安机关办理备案手续。按照国家政策要求，跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统，向当地设区的市级以上公安机关备案。该项目系统应向归属地网络安全监察支队申请重要信息系统备案。完成备案的信息系统，将获得公安机关颁发的《信息系统安全等级保护备案证明》。

（3）等级保护测评要求：乙方在测评过程中要求按照《计算机信息系统安全保护等级划分准则》（GB17859-1999）、《信息安全技术 网络安全等级保护实施指南》（GB/T25058-2019）、《信息安全技术 网

络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术 网络安 全等级保护测评要求》（GB/T28448-2019）、《信息安全技术 网络安全等级保护测评过程指南》（GB/T28449-2018）等相关的标准规范开展等级测评工作，对系统的安全物理环境、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、安全运维管理共10个层面进行安全等级保护测评。测评指标如下（二级）：

安全层面	安全控制点	测评指标
安全物理环境	物理位置选择	a）机房和办公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高层或地下室，否则应加强防水和防潮措施。
	物理访问控制	机房出入口应有专人值守，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记；
		b）应将通信线缆铺设在隐蔽安全处；
	防雷击	应将各类机柜、设施和设备等通过接地系统安全接地。
	防火	a）机房应设置火灾自动消防系统，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；
	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。
	防静电	应采用防静电地板或地面并采用必要的接地防静电措施。
	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，至少满足主要设备在断电情况下的正常运行要求。
	电磁防护	电源线和通信线缆应隔离铺设，避免互相干扰。
安全通信网络	网络架构	a）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；
		b）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。
	通信传输	应采用校验技术保证通信过程中数据的完整

		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	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。
	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检查，以允许／拒绝数据包进出；
		d） 应能根据会话状态信息对进出数据流提供明确的允许/拒绝访问的能力；
	入侵防范	应在关键网络节点处监视网络攻击行为。
	恶意代码防范	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。
	安全审计	a）应在网络边界、重要网络节点处进行安全审

		计，审计覆盖到每个甲方，对重要的甲方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、甲方、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。
	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)应对登录的甲方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。
	访问控制	a）应对登录的甲方分配账户和权限；

		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）应授予管理甲方所需的最小权限，实现管理甲方的权限分离。
	安全审计	a）应启用安全审计功能，审计覆盖到每个甲方，对重要的甲方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、甲方、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。
	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；
	恶意代码防范	应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。
	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	应采用校验技术保证重要数据在传输过程中的完整性。
	数据和备份恢复	a）应提供重要数据的本地数据备份与恢复功能；
		b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。
	剩余信息保护	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。
	个人信息保护	a）应仅采集和保存业务必需的甲方个人信息；
		b）应禁止未授权访问和非法使用甲方个人信

		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，包括甲方身份、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)应对要求管理人员或操作人员执行的日常管理操作建立操作规程。

	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；
		b)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	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。
	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执行审批过程。
	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、各类乙方、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。
	审核和检查	应定期进行常规安全检查,检查内容包括系统日常运行、系统漏洞和数据备份等情况。
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。
	人员离岗	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。
	安全意识教育和培训	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。
	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。
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进行安全方案设计；
		c)应组织相关部门和有关安全专家对安全方案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。
	自行软件	a）应将开发环境与实际运行环境物理分开，测

	开发	试数据和测试结果受到控制；
		b)应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。
	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。
	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。
	测试验收	a）应制定测试验收方案，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。
	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。
	服务乙方选择	a)应确保服务乙方的选择符合国家的有关规定； b)应与选定的服务乙方签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务。
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)应对机房的安全管理做出规定，包括物理访问、物品进出和环境安全等； 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	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。
安全运维管理	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)应对配套设施、软硬件维护管理做出规定，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。
	漏洞和风险管理	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。
	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。
	恶意代码防范管理	a)应提高所有甲方的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；
		b)应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；
安全运维管理	恶意代码防范管理	c)应定期检查恶意代码库的升级情况，对截获的恶意代码进行及时分析处理。
	配置管理	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。
	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	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。
	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。
	应急预案管理	a)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；
		b)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。
	外包运维管理	a)应确保外包运维服务商的选择符合国家的有关规定；
		b)应与选定的外包运维服务商签订相关的协

		议，明确约定外包运维的范围、工作内容。

第二阶段：渗透测试渗透测试是通过模拟恶意黑客的攻击方法，来对计算机网络的安全性进行检测评估的过程。对系统和网络进行非破坏性质的攻击性测试，尝试侵入系统，获取系统控制权并将入侵的过程和细节产生报告给甲方，由此证实甲方系统所存在的安全威胁和风险，及时提示开发人员修复安全漏洞，提醒安全管理员完善安全策略，提升系统安全防护能力。通过这种方法，可以发现系统面临和暴露的安全问题，同时渗透测试也是对安全措施有效性的重要验证。

第三阶段：建设整改咨询及安全加固（不涉及硬件）建设整改咨询工作以等级测评和渗透检测发现的安全问题为工作重点，编写《信息系统安全建设整改建议》；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。之后在甲方业务系统依据相关《信息系统安全建设整改建议》开展建设整改工作时，乙方将提供建设整改过程中的与建设整改相关的咨询服务。

对信息系统安全整改建议进行确认，并依照建议，协助甲方进行漏洞修复，补丁升级等非硬件层面的安全加固，制定可执行的安全整改方案和计划，然后协助甲方分步实施安全整改工作。

第四阶段：售后服务为期一年的售后服务工作中，乙方将向甲方业务系统提供包括应急响应、安全监测、配合检查、电话支持、安全咨询等服务在内的安全维保服务。

具体服务内容如下：

（1）应急响应服务：针对本次项目，乙方提供7*24的常规应急响应及灾难恢复专家服务。在接到甲方故障报修电话10分钟内响应。对客户信息网络应用系统突发的信息安全事件进行响应、处理、恢复、取证、跟踪、事后分析的方法及过程。

（2）配合检查服务：乙方协助甲方业务系统响应公安机关、单位内部以及第三方机构针对信息系统安全等级保护工作的检查工作。服务内容包括协助甲方业务系统准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。

（3）电话支持服务：每周7天/每天24小时不间断的电话支持服务，解答甲方业务系统在使用过程中遇到的问题，及时提出解决问题的建议和操作方法。电话响应时间不超过10分钟，到达现场时间不超过2小时，解决问题不超过24小时。

（4）安全咨询服务：乙方为甲方业务系统提供一年技术咨询服务，包括信息系统整改建设咨询服务以及其他相关安全咨询服务，一旦接到甲方的服务请求，技术服务工程师将立即开始提供服务，帮助甲方解决信息安全相关技术问题，全面配合甲方业务系统做好业务系统全保障工作。

2.3 主要交付物清单

在本次等级保护测评项目中，乙方须提交主要成果文档包含如下：

《信息系统安全等级保护定级备案证明》；

《信息系统安全等级保护项目计划书》

《信息系统安全等级保护测评方案》（每系统1份）

《信息系统整改建议书》；

《信息系统安全等级保护测评报告》（每系统1份）

《信息系统安全渗透测试报告》（1份）

七、项目实施地点

甲方指定地点

八、双方的责任义务

1.乙方服务内容应与政府采购招投标文件及本合同所指明的服务内容相一致，确保本项目正常交付使用，并负责后期服务。

2.甲方应按合同约定的付款方式向乙方支付相关费用。

3.如需乙方提供现场支持服务的，甲方应当尽合理努力为乙方提供办公场所、网络等便利条件。

4.乙方确认，甲乙双方不建立劳务派遣关系或类似关系，乙方应向其员工承担用人单位的全部责任。乙方应与其员工签署劳动合同，依法缴纳社会保险，对员工承担用人单位的全部法定责任。

乙方员工工作期间受到伤害或发生安全责任事故的，由乙方负责处理，并由乙方承担全部法律责任。

5.甲方不对乙方员工承担任何用人单位或劳务派遣用工单位的责任。无论因任何原因导致甲方向乙方员工或雇员承担任何责任的，甲方有权向乙方追偿。

6.甲乙双方不构成代理关系，乙方不得以甲方名义对外签署或发布任何文件、制度等。

7、乙方应勤勉敬业履行自身义务，及时、有预判性的处理好项目中的工作，不得因自身工作不到位影响设备正常运行，进而影响到

甲方工作。如遇到需要紧急处理事宜，乙方应无条件配合甲方予以处理。

九、验收

服务期满，经甲方验收合格后，确定项目完成。

十、保密

对工作中了解到的甲方的技术、机密等进行严格保密，不得向他人泄漏。本合同的解除或终止不免除乙方应承担的保密义务。

十一、知识产权

1.乙方应对所供产品具有或已取得合法知识产权，乙方应保证所供产品及服务不会出现因第三方提出侵犯其专利权、商标权或其它知识产权而引发法律或经济纠纷，否则由乙方负责解决并承担全部责任；如因此影响到甲方的正常使用，甲方有权单方解除本合同，乙方应无条件向甲方退回已收取的全部合同价款，给甲方造成损失的，由乙方一并赔偿。

2.本合同履行过程中，甲方向乙方及乙方人员提供的信息、材料、技术等知识产权仍归甲方所有；本合同的签订与履行不代表甲方对乙方的知识产权转让和许可，乙方仅可出于为甲方提供服务之目的而使用。

十二、合同争议的解决

合同执行中发生争议的，当事人双方应协商解决，协商达不成一致时，可向甲方所在地人民法院提请诉讼。

十三、不可抗力情况下的免责约定

双方约定在以下不可抗力情况下互不承担责任，共同协商解决。双方不可预见、不可避免、不可克服的客观情况，但不包括双方的违约或疏忽，这些事件包括但不限于：战争、严重火灾、洪水、台风、地震等。

十四、终止合同

除本合同约定，合同一经签订，不得擅自变更、中止或者终止合同。对确需变更、调整或者中止、终止合同的，应按规定履行相应的手续。

十五、违约责任

1.按《中华人民共和国民法典》中的相关条款和本合同的约定执行。

2.未按合同或政府采购招投标文件要求提供产品、服务，或供应的产品、服务质量不能满足甲方技术要求，经书面告知在合理期限内整改但仍不予调整的，甲方有权终止合同，并有权对乙方违约行为进行追究。

3.任何一方有其他违反本合同情形的，应赔偿守约方全部损失，该损失包括但不限于对守约方所造成的直接损失、可得利益损失、守约方支付给第三方的赔偿费用/违约金/罚款、调查取证费用/公证费、诉讼费用、律师费用以及因此而支付的其他合理费用。

4.甲方的违约责任

甲方因自身原因不按合同约定向乙方付款，每逾期一天，须按迟延付款额的 0.01% 向乙方支付延期付款的违约金。

甲方不按照合同约定提供相关资料及其它协作事项的，应提前7个日历天书面通知乙方，项目完成时间予以顺延。

5.乙方的违约责任

乙方未按照本合同约定保质保量提供产品或服务，经甲方催告后履行仍不符合合同约定的，甲方有权解除本合同，同时有权要求乙方按照合同价款的10%承担违约金。甲方维权支付的诉讼费、保全费、律师费等费用由乙方承担。

合同履行期限结束，乙方未能按期完成服务期限的内容，乙方应继续履行自身义务直至符合合同约定。同时从合同履行期限届满之日开始起算，每逾期一天按合同总金额的 0.03% 向甲方支付违约金。

若本项目经甲方验收不合格，甲方有权要求乙方在10日历天内整改完善，乙方必须予以整改完善。因此导致成果逾期提交的，履行期限不予顺延，每逾期一天，应按合同总金额的0.03%向甲方支付违约金；限期补充完善仍未达到甲方要求的，甲方有权单方解除合同，乙方除应承担上述逾期违约金外，还应赔偿因此给甲方造成的实际损失（例如：鉴定费、委托第三方为甲方提供完善项目所产生的费用、项目建设进度顺延给甲方造成的损失、诉讼费、律师费等），赔偿金额原则上不超过本合同总金额的30%，但甲方的实际损失超过合同总金额30%的，乙方应当承担补足责任。

甲乙双方任何一方违反保密义务的，违约方应向对方支付合同总金额10%的违约金，违约金不足以弥补对方损失的还应当承担补足责任。

乙方没有甲方的书面同意转让合同或将项目的全部或部分分包或转包出去，甲方可向乙方发出书面违约通知书，提出终止部分或全部合同。若甲方部分终止合同的，乙方应继续履行合同其他义务，并按照合同金额的10%支付违约金。若甲方全部终止合同的，乙方应按合同总金额30%的支付违约金。同时甲方的实际损失超过合同总金额30%的，乙方应当承担补足责任。

乙方违反合同约定的其它责任、义务视为违约，需向甲方支付合同总价款的30%违约金。同时甲方的实际损失超过合同总金额30%的，

乙方应当承担补足责任。

十六、反商业贿赂

双方均不得向对方或对方经办人、工作人员或其他相关人员索要、收受、提供、给予合同约定外的任何利益，包括但不限于明扣、暗扣、现金、购物卡、实物、有价证券、旅游或其他非物质性利益等，否则构成重大违约。如该等利益属于行业惯例或通常做法，则须在本合同中明示，否则亦为重大违约。

十七、其他

1.本合同签订时同步签订保密协议,详见附件。附件是本合同的一部分，具有与本合同同等的法律效力。

2.本合同一式四份，具有同等法律效力，双方各执一份，监管部门备案一份、采购代理机构存档一份。各方签字盖章后生效。

采购人（甲方）：_____（盖章）_____

地址：

法定代表人或
其授权的代理人
（签字或盖章）：李振兼

订立时间：2025年7月1日

乙方（乙方）：_____（盖章）_____

地址：西安市碑林区雁塔北路67号陕西红锋商务大厦4层西

法定代表人或
其授权的代理人
（签字或盖章）：

订立时间：2025年7月1日

附件：

信息系统等级保护测评项目保密协议

甲　方：陕西省交通运行监测中心

乙　方：西安尚易安华信息科技有限责任公司

甲方：**陕西省交通运行甲方**

地址：西安市唐延路 6 号

邮编：710075

电话：

乙方：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 号陕西红锋商务大厦 4 层西

邮编：710065

电话：029-89525570

依据《中华人民共和国民法典》的规定，就乙方履行合同《信息系统等级保护测评项目》期间，乙方所接触到的甲方各种技术内容、会议信息和其他秘密的保守事项，经协商一致，签订本协议。

一、保密范围和秘密定义

1. 本协议提及的技术秘密，包括但不限于：技术方案、设备配置、技术指标、技术报告、检测报告、试验结果、操作手册、技术文档、相关的函电，等等。

2. 本协议提及的其他秘密，包括但不限于：会议文件和开会内容、各办公室内纸质文件、资料，保存在计算机、应用服务器上数据库中的各种数据，保存于计算机上的各种文件、数据、资料、图片、声音、视频等以电子为介质保存的文件和数据，等等。

3. 保密期限：自合同签订之日起至乙方技术服务结束之日起五年。

二、甲方的权利和义务

甲方应指定专人定期督导和检查乙方关于秘密保守的执行情况。

三、乙方的权利和义务

1.乙方在甲方单位服务期间，必须遵守甲方规定的任何成文或不成文的保密规章、制度，履行与其工作相应的保密职责。

2.乙方承诺，甲方的保密规章、制度没有规定或者规定不明确之处，乙方亦应本着谨慎、诚实的态度，维护其于服务期间知悉的技术秘密或其他秘密信息，以保持其机密性。

3.除了履行服务职责的需要之外，乙方承诺，未经甲方同意，不得以任何方式向甲方指定人员以外的其他任何人或单位传递属于甲方的秘密。

4.乙方服务结束之后仍对其在甲方服务期间接触、知悉的属于甲方的技术秘密和其他秘密信息，承担如同服务期间一样的保密义务，而无论乙方因何种原因结束技术服务。

5.乙方承诺，在为甲方履行技术服务时，不得擅自使用任何属于他人的技术秘密或其他秘密信息。

6.乙方因工作上的需要所持有或保管的一切记录着甲方秘密信息的文件、资料、图表、笔记、报告、信件、磁带、磁盘、仪器以及其他任何形式的载体，均归甲方所有。

7.乙方应当于技术服务结束时，或者于甲方提出请求时，返还全部记载着甲方秘密信息的一切载体。

四、违约责任

1.双方因履行本协议而引起的争议或与本协议有关的争议，双方通过友好协商解决。如果无法达成一致意见，任何一方均有权限据本

协议向甲方所在地人民法院提起诉讼解决。

2.一方违反本协议时，另一方有权终止本协议，并有权向违约方主张合同总金额20%的违约金。

五、协议的变更和解除

1.在协议履行期内，甲乙双方均不得擅自变更或解除本协议。但经双方友好协商可对本协议条款进行变更或解除本协议。在技术服务合同期限内，甲乙双方不得终止本协议。

2.因客观原因，一方要求变更本协议时，须提前7天通知另一方，并征得的另一方的同意。

3.因一方严重违约使本协议不能履行，另一方可单方面解除本协议，同时由违约方应承担违约责任，并对因违约所造成的损失予以赔偿。

4.本协议未尽事宜由甲乙双方协商解决，并以书面备忘录形式加以补充规定，备忘录与本协议具有同等的法律效力。

六、其它

1.未尽事宜，双方本着友好精神，另行协商。

2.本协议一式肆份，甲方贰份，乙方贰份，具有同等效力。

3.本协议中所称的技术服务履约期间，以甲方和乙方签订的技术服务合同书为标志。本协议中所称的结束技术服务，以双方所签订的技术服务合同书相关条款所规定的解除合作关系的时间为准。

4.本协议自双方签字、盖章完成之日起生效。

甲方：陕西省交通运行甲方

（公章）

法定代表人

或授权代表人：

（签章）

乙方：（公章）

法定代表人

或授权代表人：

（签章）

订立时间：2025 年 7 月 7 日