项目编号：KY2023-3-253

合同编号：sxks20231008

陕西省教育考试院2023年技术服务类（第二批）采购项目（4包）：绿盟数据库审计、IPS及WAF设备维保服务及技术支持（安全运维）

合同书

甲方：陕西省教育考试院

乙方：陕西创秦科技信息技术有限公司

2023年5月

中国 西安

陕西省教育考试院2023年技术服务类（第二批）采购项目（4包）：绿盟数据库审计、IPS及WAF设备维保服务及技术支持（安全运维）合同

甲方：陕西省教育考试院

地址：西安市含光北路40号　　邮编：710068

联系人：　　电话：

乙方：陕西创秦科技信息技术有限责任公司

地址：陕西省西咸新区空港新城空港国际商务中心BDEF栋F区1层10107号房C-20号

邮编：710099

开户银行：交通银行西安太白路支行

开户帐号：611301015013000131224

联系人：陈双　　电话:15209188839

一、甲方购买产品情况和工程内容

1.甲方购买产品情况

序号	产品名称	服务内容	产品型号	数量	单位	单价(RMB)	合计(RMB)	备注
1	绿盟WEB应用防护系统	设备日常运维、信息资产核查、漏洞检查与分析、基线配置检查及整改、威胁监测分析、新系统上线检查、安全意识培训、漏洞分析校验与跟踪	WAFNX5-CH5330	2	台	43,500.00	87，000.00	

		处置。						
2	绿盟网络入侵防护系统	设备日常运维、信息资产核查、漏洞检查与分析、基线配置检查及整改、威胁监测分析、新系统上线检查、安全意识培训、漏洞分析校验与跟踪处置。	NIPSNX5-CH5330	1	台	31，000.00	31，000.00	
3	绿盟DAS日志审计	设备日常运维、信息资产核查、漏洞检查与分析、基线配置检查及整改、威胁监测分析、新系统上线检查、安全意识培训、漏洞分析校验与跟踪处置。	DASNX3-800C	1	台	31，500.00	31，500.00	
总计（大写）：人民币壹拾肆万玖仟伍佰元整							149,500.00	

2.甲方服务内容

服务地点：陕西省教育考试院

服务时间：12个月（2023.5.23-2024.5.22）

具体服务内容：见附件一

二、购买价款和支付方式

1.购买价款

本合同的总金额为¥149,500.00（大写：壹拾肆万玖仟伍佰元整）

2.支付方式

合同签订之日起10个工作日内，甲方支付合同总金额95%作为预付款即人民币小写：

¥142,025.00元，大写：壹拾肆万贰仟零贰拾伍元整；合同期满经甲方验收无误后在10个工作日内支付合同总金额的5%即人民币小写¥7,475.00元，大写：柒仟肆佰柒拾伍元整。

乙方在甲方付款前应向甲方开具法定正规全额增值税普通发票，其中涉及税务机关征税的，所缴税收由陕西创秦科技信息技术有限责任公司自行承担。乙方开具的增值税普通发票必须符合国家税收有关法律规定，不得使用虚假发票、或伪造、变造的发票，否则一切责任由乙方自行承担。

三、双方其它义务与责任

1.乙方根据本合同条款及时有效地提供服务内容中所描述的服务，并保证服务质量。

2.甲方应向乙方提供并允许乙方使用为履行本合同所需的信息、数据、文档等，并确保其向乙方提供的信息及数据的准确性和完整性。

3.服务期间，因乙方怠于履行合同义务给甲方造成损失的，甲方可以单方面解除本合同，乙方应退还甲方所支付所有价款，并承担合同金额30%的违约金，如违约金不足以弥补甲方损失的，甲方有权要求乙方赔偿违约金无法弥补部分的损失。

四、保密条款

1.合同双方保证由任何一方提供的并声明具有保密性质的所有信息均将被认同为保密信息，并由双方以对方要求的保密信息的保护方式，保证其安全性。

2.任一方不得出于除履行本合同以外的任何目的披露、传播、复制或使用来自另一方的所有或者部分保密信息；不得在未经另一方书面明确同意的前提下向任何第三方披露上述保密信息；任一方保证仅在必须知道的情况下，出于履行本合同的目的才许其员工接触保密信息并告知其本保密条款，本合同履行完毕后，任一方应当将所有涉及保密信息的载体交还另一方或者经另一方同意自行销毁。

3.乙方对在项目服务期间所获得的甲方的情报和资料有永久保密义务，泄漏秘密应承担法律的责任。不论本合同是否变更、解除、终止，本条款均长期有效。

五、法律责任

1.由于乙方原因出现下列情形之一给甲方造成损失的，甲方有权解除合同，乙方应当退还甲方所支付的所有价款，并承担合同金额30%的违约金，如违约金不足以弥补甲方损失的，乙方应当补足甲方的损失：

A、乙方提供的交付物和服务经甲方的验收，发现与合同约定不符或存在严重错误或主要错误的，乙方在甲方指定的合理时间内仍未能纠正该等严重错误或主要错误的。

B、乙方及其相关工作人员违反本合同项下的保密义务，而对甲方造成严重不利影响或重大

损失。

2. 对于非实质性违约的情况，包括由于乙方的原因导致系统局部受到影响等，除要求乙方除消除影响和赔偿实际损失外，甲方有权根据乙方违约对其造成的影响和损失，每次要求乙方按合同总额1%的标准支付违约金。连续出现5次以上的违约情形，甲方有权解除合同，乙方应当退还甲方支付的所有价款，并承担合同金额30%的违约金。

3. 不可抗力:在维护过程中由于地震、水灾、台风、战争以及其他双方都认可的不可抗力的因素造成一方违约的，可以免除其责任。

六、合同终止、生效及争议解决

1. 合同一方严重违反其在本协议项下的任何义务，并未能在对方发出书面通知指明该违约事项后10天内改正的，对方有权单方终止本合同。

2. 本合同一式陆份，甲方肆份，乙方贰份，自合同中规定的服务起始之日起生效。

3. 本合同根据中华人民共和国法律制定并予以解释，如双方因本合同发生任何争议，应首先协商解决，如协商不成，任何一方应向甲方所在地人民法院提起诉讼。

4. 附件与本合同具有同等法律效力。

甲方：陕西省教育考试院（签章）

委托代理人：

用户代表签字：

单位地址：西安市含光北路40号

签订日期：2023.10.23

乙方：陕西创秦科技信息技术有限责任公司（签章）

法定代表人（签章）：

委托代理人：

地址：陕西省西咸新区空港新城空港国际商务中心BDEF栋F区1层10107号房C-20号

签订日期：2023.10.18

附件一：

服务内容：

服务内容	系统及技术支持
服务覆盖范围	
硬件	保证
系统可用性	保证
系统升级	保证
服务响应	
电话覆盖时间	7*24 小时
电话响应时间	立即响应
到达现场时间	7*24 小时
到达甲方现场时间	4 小时
问题诊断时间	30 分钟
系统备件提供时间	24 小时
从备件到达现场起更换备件时间	2 小时
从人员到达现场起系统恢复时间	2 小时
定期巡检与预防性维护	
系统定期巡检维护	每半年一次
健康行检查	每半年一次
系统备份	提供
备份恢复	提供
系统巡检报告	提供
备件保证	
备件	提供
备件更换	现场更换
更换备件时限	2 小时
技术服务	

项目现场支持	提供
系统操作手册	提供
系统白皮书	提供
系统升级优化	提供
远程诊断	
远程故障解决	提供
远程系统性能监控	提供

系统故障响应现场服务：

乙方为甲方网络环境中所有用户提供安全、可靠、高效、智能的域名解析服务。保障系统在维护服务期间能够正常运行和顺利使用。

下列各项不属于服务的范畴：

- 服务器等硬件问题和故障。
- 网络、防火墙问题和故障。

维护期内乙方提供7×24小时响应服务（甲方通过电话、传真与乙方取得联系后，乙方保证在一小时内给出响应，二十四小时内恢复系统，一周内解决问题），具体响应方式根据故障级别而定，服务期内服务具体内容如下：

a. 服务响应

服务响应时间为即时响应，系统一般故障在2小时内排除，系统故障在24小时内提供备件或其他解决方案解决问题。

b. 定期巡检

根据系统服务特点及售后服务经验提出建议并与甲方协商，对系统进行定期上门巡检。

c. 现场排除故障或技术指导

系统服务期内应甲方要求，乙方负责派遣专业工程技术人员及时前往现场解决甲方的各种问题。如果甲方的网络管理人员有所变动，乙方负责进行相关培训。

1）紧急异常情况的及时处理

任何系统在运行过程都难免出现某些紧急异常情况，乙方应建立紧急异常情况的处理保障体系。服务期内在系统故障且无法修复时，24小时内提供备机或其他解决方案解决问题。

在系统服务期内，乙方需提供完整的产品白皮书及操作手册等技术资料，并帮助甲方建立

系统的运行、管理和维护文档，以便在发生故障时能及时提供资料，迅速找到并排除故障，将甲方损失减至最小。

2）故障解决方式

服务期内，甲方可以通过拨打公司相关人员电话或公司售后电话提出故障请求后，乙方安排技术工程师与甲方联系，共同解决甲方的故障。在甲方授权的情况下，通过电话、邮件、远程接入等方式解决甲方问题。如果远程无法解决甲方的故障，将立即升级到现场支持服务。

3）服务保障措施

➢ 日常维护

在项目服务过程中，乙方承诺将现场派驻经验丰富的技术工程师开展现场实施工作，项目试运行完成后，继续由专业技术支持人员进行日常维护巡检。

➢ 紧急技术支持

当系统在使用过程中出现故障时，一般问题在接到报告后30分钟内向技术人员提供明确的解决方法。若属重大故障，甲方无法解决时，技术人员保证在到场后一般故障4小时内解决问题，系统故障则提供备件或其他方案24小时内解决问题，重点确保恢复系统的正常运行。

➢ 现场巡检

在服务期内，向甲方提供现场巡检服务，一般每半年进行一次现场巡检。或者根据甲方的要求，协商安排现场巡检服务。主要对甲方的软硬件系统等进行例行检查，重点检查甲方的系统环境信息和状态。

服务支持方式

- **电话支持：**7×24小时客服热线；电话支持不限次数。
- **远程支持：**提供远程桌面技术服务，该方式需要甲方支持远程接入；远程支持不限次数。
- **现场支持：**如需现场服务，服务公司工程师将在第一时间赶赴甲方现场，现场响应时间将依照服务级别对应的服务承诺执行。
- **巡检服务：**每年定期安排熟悉用户系统的资深工程师上门进行系统全面健康巡检，及时消除故障隐患，保障系统健康稳定运行。

具体服务实施条款

1	设备日常	（1）日常巡检：对所有安全设备进行运行状态检查，查看设备引擎，接口，流量等信息是否正常。	每月

	运维	（2）设备升级：对所有存在更新升级包的设备进行一次设备升级，包括引擎升级，各类规则升级	每季度
2	信息资产核查	（1）提供信息资产的梳理、核查与变更管理；	每半年
		（2）协助进行主机、数据库、中间件、核心网络设备等全量资产的识别、梳理；	
		（3）统计分析资产规模，对新增、退出等情况进行确认、核实；	
		（4）出具资产清单，包括但不限于硬件配置信息、ip、操作系统版本、属主等；	
		（5）确认安全运维所需的主机所属、主机构成信息，维护资产基线；	
		（6）提供对互联网资产的核查与变更管理；	
3	漏洞检查与分析	（1）使用漏洞分析专业工具，在通用模板上定制适合甲方的检查模块；	每月
		（2）使用专业系统扫描工具检测网络设备、操作系统、数据库和应用服务中存在的安全漏洞，提供漏洞评估报告和修复建议；	
		（3）使用专业 web 扫描工具，检查 web 服务器漏洞，提供配置报告和修复建议；	
4	基线配置检查及整改	（1）使用专业工具，根据需求，在专业工具中配置适用于甲方的检查模板，对主机、数据库、中间件、核心网络设备全量资产进行基线配置核查；	每半年
		（2）出具配置核查报告；	
		（3）出具基线偏离跟踪表，全程跟踪基线整改过程；	
		（4）出具基线漏洞风险视图，以直观展示基线合规度；	
		（5）协助相关方进行偏离项整改及跟踪。	
5	威胁监测	（1）对 WAF、IPS、ISOP 等设备安全策略进行优化。	每季度
		（2）对 WAF、IPS、ISOP 等设备的安全告警进行分析；	每月

	分析	（3）提供专家服务，对安全威胁及事故进行调查取证，并提供处置建议。实现热点事件的预警与防护、高危访问源的监测与辅助封杀处置、可疑安全事件的发现与确认，（此项为 MDR 具有）	每季度
		（4）针对攻陷类事件进行通告，并对事件的处置情况进行追踪，定期对事件统计分析并反馈事件的处置结果。	每季度
6	新系统上线检查	（1）使用扫描系统、安全配置检查系统对新上线系统的主机、系统、中间件等进行安全扫描，对漏洞、用户名与口令、安全策略配置等方面进行评估；	有新系统申请上线时进行
		（2）对系统在上线前进行人工渗透测试。	
7	安全意识培训	根据信息安全技术的发展和不同层面的信息安全人才需求，围绕安全意识、安全技术方面，以理论和实操结合的方式开展安全培训。	1 次/年
8	漏洞分析校验与跟踪处置	（1）针对漏洞实例最多的前 20 种漏洞的原理及修复方式进行说明和介绍； （2） 对漏洞修复结果进行验证；通过对资产漏洞扫描的完成率、漏洞发现率、处置率、误报筛除率等指标对漏洞管理工作进行考核与度量。 （3）对漏洞修复与处置情况进行追踪，定期统计分析并反馈漏洞处置情况，并输出漏洞管理报告。 （4）对漏洞进行全生命周期管理完成从漏洞的发现、定级、验证、修复、复验、状态跟踪各个阶段管理，保障漏洞风险完整闭环，防止因管理上的问题导致漏洞风险被利用。	每半年