陕西省教育考试院应用安全防护云服务合同

2025 年 12 月

合同签订地：陕西省教育考试院（西安市碑林区）

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：王飞

电话：029-85221724

乙方：北京万明众熠科技有限公司

地址：北京市丰台区菜户营 58 号 9 层 910

邮编：100054

开户银行： 招商银行北京丽泽商务区支行

帐号：110944445410401

联系人：韩艳艳

电话:13520261733

一、甲方委托服务内容

甲方购买服务内容

服务地点：陕西省教育考试院

服务时间：2025 年 12 月 19 日至 2026 年 12 月 18 日

具体服务内容见附件 1

二、购买价款和支付方式

1.购买价款

本维保服务合同的总金额为￥138,000.00（大写：人民币壹拾叁万捌仟元整税

率： ）

2. 支付方式

合同签订后，甲方在一个月内支付乙方合同总价的95%即人民币小写¥131，100.00元，大写：人民币壹拾叁万壹仟壹佰元整；待服务期满后无任何项目质量问题一次性付清剩余合同总价的5%。

乙方在合同签订后五个工作日内向甲方开具法定正规全额发票，其中涉及税务机关征税的，所缴税收乙方公司自行承担。

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。

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. 乙方出现下列情形之一的，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，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。严重错误是指导致整个系统无法运行的错误；主要错误是指影响系统正常运行的错误。

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，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，在合理时间内及时通知对方并采取可能的措施避免损失扩大的，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。

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：

北京万明众熠科技有限公司（签章）

委托代理人：

地址：北京市丰台区菜户营58号910

签订日期：2025.12.19

附件一：

服务内容要点：

产品名称	功能项	功能说明	功能内容
云防护	智能 DNS	可提供 DNS 域名解析	NS 和 cname
	web 防火墙	可防护 SQL 注入、命令注入、跨站脚本、文件包含、信息探测等常见攻击,防止网站因为漏洞导致被篡改，被拖库，被入侵。	支持
	防火墙策略集控制	支持子防护策略集打开关闭； 子防护策略集如下：政企专用防护策略集，扫描器/爬虫防御策略集，异常 HTTP 请求防御策略集，SQL 注入防护策略，POST 请求 SQL 注入防护策略，Webshell 防护策略，XSS 防护策略，POST 请求 XSS 防护策略，命令/代码执行防护策略，文件包含/注入防护策略，特殊/其他攻击防护策略。	支持
	防护策略屏蔽时间	可以设置防火墙策略拦截的 IP 的屏蔽时间	自定义
	防火墙策略白名单	对指定的 Web 防火墙策略不进行拦截	100 条
	智能攻击防御	可精准识别多种自动化扫描和攻击软件，深度解析编码过的、畸形的恶意代码，并阻断其请求，减少 90%以上的恶意攻击。	支持
	WebShell 防护	可防止黑客上传、访问 WebShell（网站后门）	支持
	协同防御	防护平台整体防御体系，全网拦截任何攻击过防护体系的攻击者 IP	支持
	境外访问控制	限制境外 IP 进行访问。由于攻击者大量使用国外跳板进行攻击，开启本功能可极大减少此类威胁	支持
	后台锁	禁止非授权 IP 访问网站后台管理地址或重要页面	60 条

	防黑锁	锁定页面关键资源（如 Banner 图片、LOGO 图片），避免关键资源受篡改而影响页面	10 条
	在线锁	确保网站永久在线，发现页面不可访问可立即恢复	支持
	裤带锁	防止黑客进行“撞库”攻击，保护网站敏感数据不被泄露	支持
	防盗链	保护网站图片、压缩包等资源文件不被其它站点盗用	50 条
	夜间模式	针对夜间网站更新频率较低、黑客攻击比较频繁的情况，设置夜间模式，可提高防护等级，大幅降低网站被黑可能性	支持
	URL 黑白名单	不经过防护的 URL 地址（URL 白名单）、不允许访问的 URL 地址（URL 黑名单）	各 100 条
	IP 地址黑白名单	可设置不进行防护的 IP 地址（IP 白名单）、不允许访问的 IP 地址（IP 黑名单）	各 100 条
	网站概况显示	提供网站访问情况信息展示，包括请求数、总流量、网站浏览人数，搜索引擎引导量，遭受攻击次数等，并能按照时间来统计的网站访问量	支持
	安全报告	查看网站安全状况，包括各种攻击发生次数，攻击 IP、来源（国家）等；可显示对网站的安全评级，如安全、危险等等，可显示历史攻击次数等； 可显示 CC 攻击详细情况； 可显示攻击情况，包括时间、攻击 URL，攻击者 IP 及归属地，攻击类型等 提供一年内自定义报表功能	支持
	实时攻击显示	提供实时攻击视图，在视图中实时显示攻击源 IP，国家，目标域名，目标所在地等	支持
	攻击预警	提供按照攻击阈值设定攻击预警功能	支持
	报表下载	默认支持当日、前一天、最近 30 天和最近一年的报表统计下载	支持

	日志下载	提供最近 7 天内的攻击和访问日志自助下载服务	支持
	一键关停	提供一键关停网站服务功能，用户需要事先在防护平台上认证手机	支持
	共享 SSL 证书节点	提供共享证书节点（sni 方式，低版本浏览器会有告警）SSL 证书自助上传功能（pem 格式，含证书和私钥）	支持
	子域名	支持子域名数量	10 个子域名

服务名	模块	服务说明	服务内容
加速乐	智能 DNS	DNS 负载均衡。	5 个源站 IP
		混合解析。	支持
		泛域名解析。	支持
	内容分发	自定义缓存设置。	60 条
		缓存黑白名单。	60 条
		缓存时间设置。	支持
		刷新缓存功能。	支持
	页面压缩	页面压缩功能。	支持

IPv6 安全改造服务内容		
模块	服务说明	服务内容
IPv6 DNS	IPv6 DNS 解析服务	支持
IPv6/IPv4 双向转换	将访客的 IPv6 请求转换为 IPv4 请求，将源站返回的 IPv4 内容转换为 IPv6 内容	支持
IPv6 访问加速	在 IPv6 网络环境下对网站资源进行缓存、压缩（CDN）。	支持
IPv6 安全防护	在 IPv6 网络环境下为网站提供 Web 应用防火墙，抵御常见 Web 漏洞攻击	支持
IPv6 天窗修复	无感知解决 IPv6 天窗问题	支持

服务对象

序号	域名	HTTPS 接入方式 (SNI/独享)	清洁流量
1	sneea.edu.cn	SNI	7200G/月

服务内容说明

1 如果被服务域名 DDoS 攻击峰值超出所服务的最大防护峰值且未使用 DDoS 攻击流量自动伸缩服务，乙方有权暂停服务并不承担相关责任；

2 如果超出了 DDoS 攻击流量自动伸缩最大峰值，乙方有权暂停服务并不承担相关责任；

3 DDoS 攻击流量出现以下任何一种情况时，须通过升级套餐或者进行超量计费的方式处理，超出的 DDoS 攻击防护每天以公式（当前 DDoS 攻击峰值-DDoS 攻击套餐防护峰值)/10*2000 元 来计费：

1）DDoS 攻击峰值超过约定的 DDoS 攻击流量自动伸缩最大峰值；

2）DDoS 攻击超量次数超出约定的 DDoS 攻击流量自动伸缩次数；

4 如果被服务域名 CC 峰值超出所服务的最大防护峰值，则每 10 个攻击 IP 扣除 1GB 网站正常请求流量；

5 如果被服务域下面的子域名中有多个 SSL 证书，乙方将采用 SNI（Server Name Indication）方式接入服务域名，SNI 方式接入的域名可支持的浏览器列表见附录 2。

附录 2. SNI 可支持的浏览器、服务器、库

SNI 可支持的浏览器、服务器、库	说明
Internet Explorer 7 or later, on Windows Vista or higher. Does not work on Windows XP, even Internet Explorer 8.	Windows Vista 及以上操作系统：只支持 IE7 及以上的 IE 浏览器。在 Windows XP 不支持 IE7，即使是 Windows XP 上的 IE8 也不行
Mozilla Firefox 2.0 or later	火狐浏览器 2.0 以后版本
Opera 8.0 or later (the TLS 1.1 protocol must be enabled)	Opera 8.0 以上版本（必须开启 TLS 1.1）
Opera Mobile at least version 10.1 beta on Android[citation needed]	安卓版的 Opera 移动版 10.1 beta 版以上
Google Chrome (Vista or higher. XP	Chrome 浏览器（Vista 或者更高版本都支持，XP

on Chrome 6 or newer. OS X 10.5.7 or higher on Chrome 5.0.342.1 or newer)	系统上的 chrome 必须是 6.0 版本以上的，OS X 10.5.7 以上系统上必须是 Chrome 5.0.342.1 以上的）
Safari 2.1 or later (Mac OS X 10.5.6 or higher and Windows Vista or higher)	Safari 2.1 或者更高版本（操作系统需要是 Mac OS X 10.5.6 或者更高，Windows 系统需要 Vista 以上）
Konqueror/KDE 4.7 or later MobileSafari in Apple iOS 4.0 or later Android default browser on Honeycomb or newer Windows Phone 7[citation needed] MicroB on Maemo	Konqueror/KDE 或者更高 苹果 iOS 4.0 中的 MobileSafari 或者更高 Android Honeycomb 系统默认浏览器更高版本 Windows 手机 7 Maemo 系统上的 MicroB

SLA 服务品质保障

1.SLA 计算方法：服务可用性（SLA）统计以分钟为单位，服务总时间为服务周期内的总分钟数，不可用时间为当某一分钟内，甲方所有正在访问甲方系统的客户试图与指定的乙方服务节点建立连接的连续尝试均失败，则视为该分钟内该服务不可用。在总服务周期内不可用分钟数之和即服务不可用总分钟数。

2.SLA 标准

产品或服务	服务等级目标	每年允许不可用时间
抗 D 保	99. 9%	(1-服务等级目标)*每年总时间=8.76(小时)
创宇盾	99. 9%	(1-服务等级目标)*每年总时间=8.76(小时)
加速乐	99. 9%	(1-服务等级目标)*每年总时间=8.76(小时)
深度反爬虫	99. 9%	(1-服务等级目标)*每年总时间=8.76(小时)
IPv6 安全改造	99%	(1-服务等级目标)*每年总时间=87.6(小时)
ScanV	99. 9%	(1-服务等级目标)*每年总时间=8.76（小时）

服务支持方式

- **电话支持：**7×24 小时提供电话或微信技术支持。