采 购 合 同

合同编号：

项目名称：　　戏曲学院信息化运维服务采购项目

分包名称：　　网络安全运维

采购方：　　北京戏曲艺术职业学院

中选供应商：　北京彗芯科技有限公司

签署日期：2026 年 1 月 19 日

合　同　书

北京戏曲艺术职业学院(采购方)戏曲学院信息化运维服务采购项目(项目名称)中所需 2026 年学院网络安全运维(服务名称)经 北京宏一工程管理咨询有限公司以 HYGC-2025-123（项目编号）的比选文件进行国内公开比选。经评审委员会评定北京彗芯科技有限公司(公司名称)为中选供应商。采购方、中选供应商同意按照下面的条款和条件，签署本合同。

1、合同文件

下列文件构成本合同的组成部分，应当认为是一个整体，彼此相互解释，相互补充。为便于解释，组成合同的多个文件的优先支配地位的次序如下：

a.本合同书

b.中选通知书

c.合同书条款

d.投标文件

2、合同范围和条件

本合同的范围和条件应与上述规定的合同文件内容一致。

3、服务内容

本合同要求提供的服务 2026 年学院网络安全运维

4、提供服务期限、地点

服务期限：自合同签订之日起至 2026 年 12 月 31 日止

服务地点： 北京戏曲艺术职业学院，北京市丰台区马家堡东里 8 号。

5、合同报价

序号	服务名称	单价（元）	数量	合价（元）	备注/说明
1	差距分析	20000	1	20000	详见附件：《戏曲学院信息化运维服务采购项目-02 包采购需求》
2	安全服务	700000	1	700000	
3	整改咨询	20000	1	20000	
4	最终测评	30000	1	30000	
5	云 WAF 服务	60000	1	60000	
6	虚拟化服务	50000	1	50000	
7	网络设备运维	50000	1	50000	
总价（元）				930000	

6、**合同金额及付款方式**

合同金额：人民币大写：玖拾叁万元整（人民币小写：930000）

付款方式：自同签订之日起 3 个月内，采购方向中选人支付合同总金额的 50%款项，待项目由采购方验收合格后 3 个月内，采购方向中选人支付合同总金额的剩余 50%款项。

7、合同的份数及生效

本合同一式 伍份，具有同等法律效力。采购方执叁份和中选供应商执贰份。

本合同经双方各自的授权代表签署、加盖单位公章或合同专用章之日起生效。

采购方：北京戏曲艺术职业学院

名称：(印章)

2026 年 1 月 19 日

授权代表(签字)：

地址：

邮政编码：

电话：

开户银行：

账号：

中选供应商：北京慧芯科技有限公司

名称：(印章)

2026 年 1 月 23 日

授权代表(签字)：

地址：北京市通州区潞邑街道疃里南区 5 号楼二层 A005-039

邮政编码：

电话：18510035819

开户银行：中国民生银行股份有限公司北京万柳支行

账号：654736122

合同书条款

第一章 验收时间和方式

1、 甲方在乙方服务完成后，应在及时进行验收；乙方服务内容不符合合同约定的，甲方应向乙方书面提出，乙方应及时予以解决。

2、 甲方验收合格后应在五个工作日内向出具验收报告，作为验收结果的书面材料；甲方逾期未提出验收报告的，视为甲方对乙方的服务内容验收合格。

3、 甲方指定 张鹏 （联系方式： 18600706896 ）为项目验收的授权代表，由该授权代表全权处理本合同项目验收阶段的全部事宜。

4、 本合同服务项目的保证期为 1 年，自项目通过甲方验收之日起计算。保证期间如发现服务质量有缺陷的，乙方应负责无偿修正、返工。

第二章 甲乙双方权利与义务

1、甲方权利与义务

（1） 甲方应向乙方提供本项目需提供的必要场地和现场提供服务的条件，具体为：

甲方协调人及联系电话：乐乐 13717680700

（2） 甲方应按时支付本合同约定金额的服务费。

（3） 按合同约定及时验收技术服务成果。甲方不验收或者逾期超过七个工作日未验收的，视为乙方提供的技术服务已严格按照本合同的约定提供完毕。

2、乙方权利与义务

（1） 乙方联系人及联系电话：李春霖 18511842870

（2） 乙方根据项目的要求，为甲方提供优质信息安全服务。

（3） 配合甲方做好安全工作培训、指导以及加固。

（4） 为甲方提供优质高效的安全运维服务：

a） 远程诊断：乙方电话技术支持中心将提供 7x24 小时响应，随时解决甲方产品技术问题与咨询。对于甲方反馈的技术问题，乙方电话客服中心应在 4 小时内予以口头或书面答复，48 小时内给出解决方法。

b） 现场服务：如通过电话等远程方式无法解决甲方遇到的故障问题，或遇到紧急故障情况，在甲方的要求下，乙方应派出工程师进行现场故障排除。在乙方分支机构所在地直径 20 公里范围内 2 小时之内到达(50 公里范围内 4 小时到达)，其它地区 24 小时内达到故障现场（不可抗力情况除外），72 小时解决问题或提出经甲方认可的解决方案。

第三章　不可抗力

1、合同签订后，任何一方，由于不可抗力事件而影响本合同履行时，则延长履行合同的期限，这一期限应相当于事件所影响的时间，并可根据情况部分或全部免予承担违约责任。不可抗力事件发生后，双方应尽可能减少损失，如一方未能履行此义务，则对因此扩大的损失承担责任。

2、受不可抗力影响方应尽快将所发生的情况以传真通知对方。

3、当不可抗力事件停止或消除后，受影响的一方应尽快以电传或电子邮件方式通知另一方。如不可抗力的影响连续或累计超过二十天以上时，双方应通过友好协商并尽快达成协议，解决本合同的履行问题。

第四章 保密条款

1、乙方同意，在任何时侯，不论是合同有效期内还是合同终止以后，对甲方提供的技术文件以及事务、业务或操作方法（下称秘密信息）实行严格保密。 乙方应就一切有意、无意泄露甲方秘密信息的行为向甲方承担赔偿责任。

2、乙方保证，其依本协议所知悉的秘密信息只用于本合同的目的，不用于其

他任何目的或向任何第三方（包括单位、个人，也包括甲、乙方的关联企业如子公司、参股公司、母公司等）披露。乙方承认并同意，甲方是秘密信息的独家拥有者，将不损害甲方对秘密信息的所有权。

3、乙方应只在下述情况下，方可使用甲方秘密信息：1)出于履行本合同的需要。2)不论如何，秘密信息均不得以任何方式用于对甲方不利、有损或相竞争的目的。秘密信息未经甲方事先书面同意，不得被复制、全部或部分与其他信息相编纂、透露给第三方。

4、乙方除经按本合同许可外，不得传播、透露秘密信息的全部或部分。秘密信息可向本方的代表和需获悉秘密信息以辅助本方履行其义务的的员工披露。乙方保证，在上述本方代表和员工知悉秘密信息之前，向其提示秘密信息的机密性与专有性，并保证上述代表与员工同意接受本合同条款的约束。

第五章　合同的变更、解除及违约处理

1、本合同所订一切条款，甲、乙任何一方不得擅自变更或修改，本合同如有未尽事宜或对本合同的任何修正、更改或增删需由甲、乙双方协商另订补充合同，补充合同经双方盖章后方可发生效力并与本合同有同等效力。

2、如一方违反本合同中所规定的义务，违约方在收到守约方要求纠正其违约行为的书面通知之日，应立即停止其违约行为，并在三十(30)日内赔偿守约方因此受到的所有损失。如违约方继续进行违约行为或不履行其义务，守约方除就其所有损失而获得违约方补偿外，亦有权提前终止本合同。

3、本合同期间，如甲方逾期未向乙方支付到期款项， 则每逾期一天，应向乙方承担逾期款项万分之四的违约金，同时乙方有权停止提供部分或全部服务。

第六章　争议解决

在本合同履行过程中发生争议时，甲、乙双方应及时协商解决。如协商不成，任何一方均有权向甲方所在地人民法院提起诉讼。

第七章　合同的生效、解除

1、本合同自甲、乙双方盖章之日起生效。

2、如果发生以下情况，可以视为合同解除：

（1） 双方共同同意提前解除合同；

（2） 按法院裁决，合同解除。

附件：《戏曲学院信息化运维服务采购项目-02包采购需求》

序号	名称	服务要求	备注
1	差距分析	根据国家信息安全等级保护政策和标准，并根据等级保护要求开展网络安全差距分析工作： 1、信息系统的安全等级要求：根据国家信息安全等级保护政策和标准，确定学院信息系统所属的安全等级要求。 2、安全防护差距分析：对学院信息系统在安全物理环境、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、安全运维管理等十个层面的安全防护措施进行详细分析，包括已经实施的措施和存在的漏洞或不足之处。 3、安全防护水平评估：根据现有的安全防护措施和相应保护等级的要求，评估学院信息系统的安全防护水平，确定与目标等级之间的差距。 4、整改意见和建议：根据评估结果，提供详细的整改意见和建议，包括针对不足之处的具体措施和优化方案，以提升学院信息系统的安全防护水平。	
2	安全服务	1、安全巡检：一年24次安全巡检服务，开展对现有网络系统中的安全设备、网络设备、业务系统进行安全巡检，包括对设备的可用性、性能、安全策略、业务系统可用性等进行检查，巡检完成后出具安全巡检报告，给出存在的安全漏洞及潜在的安全风险，并给出对应的整改建议，确保网络安全运行。主要包括： （1）基线核查：对校方指定的信息系统的服务器、数据库、中间件和重要网络设备等基础软硬件的配置开展信息安全基线检查，并协助对发现的问题进行整改，输出安全配置核查报告。 （2）日志巡检：对防火墙、IPS、WAF等安全设备的日志如应用日志、主机日志、网络安全设备日志进行安全检查，从记录的攻击日志进行分析，确认威胁，并输出日志巡检报告。 1.1、服务工具： （1）投标人在安全巡检过程中所使用的工具具备交互式风险识别能力，交互式安全检测系统需满足供应链安全检测证书工具类能力要求。 2、漏洞扫描：一年24次依据相关规范使用专业的漏洞扫描工具对目标信息系统进行全面漏洞扫描工作，并将扫描结果进行系统化管理，清晰掌握信息系统上的漏洞信息，让漏洞修复与管理工作有的放矢，闭环处理安全漏洞，通过及时预警与排查最新漏洞，专业	

		化的技术分析、评估是否影响，影响范围，并提供详细处置建议。 2.1、服务工具： #（1）服务过程中需供应商提供的商业检测设备，这些设备在服务期间，可对现网内各类资产进行自动发现，可检测在线资产的IP、MAC、操作系统、设备类型、设备厂商、设备型号、软件版本等，并支持基于 A/B/C 段的检测目标的任务创建，服务工具应具备CVE及CNNVD兼容性认证。**提供工具功能截图。** #（2）供应商服务工具能针对现网的非法外联主机进行有效检测和定位，可检测出目标设备连接智能手机热点、通过智能手机 USB 共享网络等违规双网卡共享外联行为。**提供工具功能截图。** #（3）供应商提供的服务工具具备漏洞验证能力，可对高危漏洞提供自动化验证功能。自动化验证不需要任何人进行参与，平台自动对漏洞进行验证、判断，并可在安全检测报表中体现。**提供工具功能截图。** 3、渗透测试：一年 24 次知名网络安全公司原厂服务：对目标进行渗透测试，提供专业服务人员配合工具，在校方授权范围内，针对指定的目标系统开展渗透测试工作，通过模拟黑客，使用业界可靠的攻击手段、攻击技术、攻击工具和自编脚本，对目标的安全漏洞、安全隐患进行全面检测，对发现的安全漏洞提供修复建议，并协助用户进行复测验证修复情况。 3.1、服务工具： （1）投标人在渗透服务过程中所使用的工具具备对代码安全风险进行识别，静态应用安全测试系统需满足供应链安全检测证书工具类能力要求。 （2）投标人在渗透服务过程中所使用的工具具备对系统组件风险进行识别，软件成分分析系统需满足供应链安全检测证书工具类能力要求。 4、网站安全监测：服务包含四个二级域名（www.bjxx.com.cn，portal.bjxx.com.cn，zs.bjxx.com.cn，sso.bjxx.com.cn）全年安全监测，对指定网站进行 7*24 小时安全监测，持续评估资产暴漏面、资产异动变化、漏洞脆弱性、紧急 0Day 漏洞等脆弱性问题，实时监测页面篡改、黑链、业务可用性、DNS 劫持、网页挂马等安全事件，在网站出现异常时自动进行告警，并根据需要导出监测日报、周报、月报。 5、网络安全应急响应服务：重要时期进行应急响应服务，当发生安全紧急事件时，根据学校要求进行安全应急响应。通过有效的技术手段、组织管理、预案流程、制度规范等综合措施，对已发生的网络安全事件进行响应处置，降低可能造成的风险和损失。全年不	

		少于 60 天网络安全应急响应服务。 应急响应服务具体包括： （1）元旦、春节、寒假、五一、十一、暑假等长假期间进行应急响应服务，通过现场支持的形式协助学校对遇到的突发性安全事件进行紧急分析和处理。 （2）重保期间，如国家级重要会议、国家级赛事、攻防演练、招生、特殊活动等学校或上级单位认为重要的时间点，委派至少 2 名高级信息系统安全工程师及 1 名高级网络安全工程师进行现场驻场支持。全程紧密监控信息系统与网络的运行状况，及时排查潜在的安全隐患。包括数据存储的安全性、系统软件的稳定性等。同时制定完善的应急响应预案，应对各类安全事件。高级网络安全工程师则在网络层面进行安全防护，加强网络边界的防护力度，防止外部网络攻击的入侵。实时监测网络流量，分析异常数据，及时发现并阻断恶意网络行为。 7、网站动态安全服务：对不少于十二个信息系统进行全年安全威胁分析服务，需提供专业web动态安全防御工具，配合高级威胁分析工程师。实现网站管理以及安全防护一站式服务，通过终端鉴真、终端密令、页面幻阵、数据混淆等创新技术实现全方位的动态安全防护，实现Web应用可视化； 7.1服务工具 #（1）支持自动识别网页中的URL地址、表单、JS代码等，并对这些内容进行动态混淆封装，同一页面内的相同内容（URL、表单、JS等）在每次请求封装后呈现结果应都不同。**提供工具功能截图。** #（2）支持自动为应用请求生成令牌，令牌随附请求至动态应用安全防护设备进行检查，无令牌、令牌已使用、令牌已过期的请求将无法访问应用系统。防止攻击者发出非法请求，抵御越权访问及重放攻击等恶意行为。**提供工具功能截图。** #（3）支持以动态的混淆算法与密钥自动对终端用户提交的数据内容和服务器cookie进行保护，提升中间人攻击的难度，防止中间人攻击、请求伪造、窃听或篡改请求数据包等行为，应具备自动识别并混淆用户提交数据，用户每次提交相同的内容经混淆后呈现都应不相同，以提升黑客反编译和猜解的难度。**提供工具功能截图。** 8、安全威胁分析服务：对不少于十二个信息系统进行全年安全威胁分析服务，需提供专业态势感知工具，配合高级威胁分析工程师。在用户侧开展网络安全威胁建模、威胁监测、分析研判、通报预警、协助处置等一系列的服务工作，实现全天候的网络与数据安全	

		态势监测，为安全管理者提供决策支撑，建立网络与数据威胁的持续闭环管理。	
3	整改咨询	1、根据等级保护标准，为目标系统提供专业的整改咨询服务，并依据学校具体需求定制相关安全培训课程。 2、在网络安全宣传周期间，为学校策划并实施安全宣传工作，并安排 1 名信息系统安全工程师知识普及等系列活动。 3、配合学校的其他宣传计划，开展相关的工作。根据学校的教学安排，将网络安全知识融入到相关课程中，让学生在日常学习中增强网络安全意识。与学校的社团组织合作，开展网络安全主题活动 4、定期对学校的网络安全状况进行评估和分析，为学校提供针对性的建议和解决方案，持续提升学校的网络安全防护水平。	
4	最终测评	对系统安全进行最终测评。	
5	云 WAF 服务	1、提供 DNS 域名解析。 2、通过 HTTPS 方式提供 Web 配置管理界面，保证自身安全性。 3、支持无限制带宽，不单独收费，可支持超大量访问请求。 4、支持无限制 QPS，不单独收费，多节点负载，有效提高访问效率。 5、支持弹性资源调配，特殊情况下可为网站动态分配节点及带宽资源，保障网站正常运行。 6、具有安全防护能力，能够抵御通用类型的 SQL 注入、文件包含、扫描器/爬虫、WebShell、XSS 跨站、代码执行、文件注入等攻击威胁，支持设置拦截模式、观察模式。 7、支持自定义开关策略，可以自定义的策略至少包括：扫描器/爬虫防御，异常 HTTP 请求防御，SQL 注入防护，POST 请求 SQL 注入防护，Webshell 防护，XSS 防护，POST 请求 XSS 防护，命令/代码执行防护，文件包含/注入防护等。 8、对指定的 Web 防火墙策略不进行拦截。 9、能够定义给定的 URL 作为网站后台管理页面，允许特定 IP 进行访问。 10、访问请求触发网站防火墙防御策略达到设置的阈值时，屏蔽该 IP 一定的时间，减少误拦截同时保障网站安全。 11、支持一键关停网站服务功能。 12、支持前置防御，支持浏览器安全检查，为首次访问您业务系统的客户端浏览器进行全方位安全检查。 13、支持 URL 黑白名单，对特定网址进行黑白名单设置，提高安全性，减少误报率。	

		14、支持 IP 黑白名单，对特定 IP（支持 IPv4、IPv6）进行黑白名单设置，提高安全性，降低误报率。 15、支持防盗链，开启后默认仅允许主站的所有子域名互相引用，支持设置白名单。 16、支持网站永久在线，当网站服务器宕机、配置故障、受攻击时，网站自动显示规范的 HTTP 状态码（503），避免百度等搜索引擎降权，同时向访客进行友好提示。 17、支持对 404 页面进行内容优化，提升用户体验、降低跳出率。 18、支持联动云蜜罐，自动同步云蜜罐捕获的高危 IP 到黑名单进行向前防御。 19、支持攻击态势可视化，应包括：。 20、实时获取网络攻击行为，实时发现、分析、报警；。 21、以地图形式实时显示网站遭受攻击的情况；。 22、展示内容包括攻击的具体来源、IP 地址、所属国家（地区）并标示攻击类型。。 23、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。 24、支持查看网站安全状况，包括各类攻击发生次数，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，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。 25、支持当日、前一天、最近 30 天和最近一年的报表统计下载。 26、支持报表自定义日期查询数据和日志下载功能，支持 7 天内访问/攻击日志的自主下载，支持操作日志查询、导出。 27、提供按照攻击阈值设定攻击预警功能。 28、已配置 HTTPS 证书的域名，支持自助开启 HTTP2.0 协议。 29、支持节点在 HTTPS 响应头中添加周期为一天的 HSTS 配置，支持该特性的浏览器在此周期内使用 HTTPS 访问。 30、节点请求源站时带上 SNI 信息，帮助正确选择证书。 31、支持强制将 HTTP 跳转到 HTTPS，仅支持配置了 HTTPS，并且 HTTPS 端口为 443 的网站。 32、支持根据不同域名的需求，灵活地配置 TLS 协议版本。 33、支持将部署到网站服务器的 HTTPS 证书上传至知	

		道创宇云安全防御平台、开启安全 HTTPS 访问，同时支持国际算法证书、国密算法证书。 34、支持配置端口转发策略。 35、支持多等级权限账号系统，可以设置超级管理账号，报表子账号，域名管理者子账号等类别，支持基于不同功能组合的账号角色自定义，支持自定义子账号权限。	
6	虚拟化服务	结合现有业务需求、应用系统需求、虚拟化平台需求综合进行网络规划及设计。 服务器、存储、网络设备安装及调试。 1)环境调研，规划设计，实施，文档交付。 2)根据环境调研结果设计出合理的规划方案，包含计算资源池规划，存储资源池规划，云平台网络规划，备份规划，数据库规划等。 3)实施包含：完成 1 个中心，N 个计算节点软件安装，完成新的服务器安装后，扩充用户的计算环境，从而能够运行更多的业务，支撑业务长远发展对资源的需求。 4、提供技术支持服务，要求响应时间≤10 分钟，故障处理时间≤1 小时，服务时间每日，服务人数≥1，并提供整个系统安装调试时所需的资料，包括：技术咨询、技术说明书、需求文档、系统设计文档、使用说明书、维护说明书等；	
7	网络设备运维	1、日常维护：包括 IP 地址维护管理、VLAN 划分、网络设备配置调整及网络优化、网络系统故障诊断、网络入侵监测、网络性能及资源使用情况检查、网络广播风暴监测、网络拓扑图的维护，以及网络运行日志、服务维护档案和网络运行状况报告的整理等。 2、设备硬件维护：定期检查网卡、网线、接口、交换机、路由器等设备的运行状态，对于使用年限较久、性能下降明显的硬件要及时更换，确保网络设备硬件的正常运行。 3、软件维护：包括服务器的软件维护，如检查服务器的 IP 地址、DNS 配置是否正确，网络服务、网络协议是否安装正确，应用程序运行是否正常，所提供的服务能否正常使用等；网络设备的软件维护，如检测路由器、交换机等网络设备的运行状态，以及设备的相关配置情况；以及网络安全性的维护，如及时更新系统补丁，升级维护杀毒软件和软件防火墙，定期进行病毒查杀，定期进行网络日志分析，检查是否有异常的登录或入侵行为。 4、提供技术支持服务，要求响应时间≤10分钟，故障处理时间≤1小时，服务时间每日，服务人数≥1	