浙江警察学院软硬件维保项目合同

项目编号： HSZB-2021-255

确认书号：

甲方（采购人）：浙江警察学院

乙方（中标单位）：浙江飞佛科技有限公司

采购代理机构：浙江豪圣建设项目管理有限公司

浙江豪圣建设项目管理有限公司受浙江警察学院委托公开招标浙江警察学院软硬件维保项目，经过招标，确定浙江飞佛科技有限公司为中标人。经协商双方就本采购事项达成以下条款：

第一条：维保服务期限

7 个月，2021 年 12 月 1 日至 2022 年 6 月 30 日

第二条：维保服务费用与支付方式

1. 维保服务费用（合同总价）为（大写）：陆拾柒万柒仟元（￥677000 元）。

2. 履行地点： 浙江警察学院滨江校区和临安校区；

3. 支付方式：合同签订后合同生效、甲方收到乙方履约保证金后支付 30%项目款（203100 元），合同全部履行完毕经甲方验收合格无任何服务问题后支付剩余 70%项目款（473900 元）。

第三条：维保服务内容、要求

1. 维保服务内容：具体详见合同附件 1

2. 维保服务具体要求：

（1）根据《中华人民共和国数据法》第二十七条规定，乙方在利用互联网等信息网络开展数据处理活动时，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

（2）乙方在服务过程中须留存维保记录、培训记录，并提交甲方，由甲方签章及项目负责人签字确认。

（3）甲方对中乙方提交的货物依据招标文件上的技术规格要求和国家有关质量标准进行现场验收。乙方交货前应对产品做出全面检查和验收文件进行整理，并列出清单，作为甲方验收和使用的技术条件依据，检验的结果应随货物交给甲

方。

（4）未经甲方事先书面同意，乙方不得将与本合同及有关的任何合同条文、规格、计划、图纸、样品或资料提供给任何第三方。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

（5）乙方应保证提供服务过程中不会侵犯任何第三方的知识产权，否则甲方有权解除本合同，拒绝支付合同价款，并要求乙方赔偿所有损失。

（6）乙方维保人员严格按照招投标文件配备，服从甲方各项工作安排，包括节假日加班等安排，维保人员如有变动需提前 1 个月告知甲方，经甲方同意后方可变更。

第四条：转包或分包

1. 本合同范围的服务，应由乙方直接完成，不得转让给任何第三方；

2. 乙方不得将本合同范围的服务全部或部分分包给他人提供；

3. 如有转让和分包行为，甲方有权解除合同，没收履约保证金并追究乙方的违约责任。

第五条：履约保证金

合同签订之日起 5 个工作日内，乙方向甲方缴纳合同总价 5%的履约保证金（33850 元），履约保证金在甲方服务期满后无服务和质量问题的无息退还。

第六条：质量保证及后续服务

1. 乙方应按招标文件规定向甲方提供服务。

2. 乙方提供的服务成果验收不合格的，或在服务期内出现问题，乙方应负责免费提供后续服务。对达不到服务要求的，根据实际情况，甲方有权自行选择以下办法处理：

（1）重做：由乙方承担所发生的全部费用，并承担所有损失。

（2）解除合同：甲方拒付（或要求乙方退还）合同价款。

3. 在服务期内，乙方应对出现的质量及安全问题负责处理解决并承担一切费用。

4. 提供网络和虚拟化技术培训：

培训时长：2 天

培训时间：合同签订后 1 周内

培训讲师：高级网络工程师

培训人数：4 人

培训内容：网络基础，路由、交换，无线网优等基础概念的培训，通过理论和实验结合的方式，使用户掌握相关的网络协议基础。

培训时长：4 天

培训时间：合同签订后 2 周内

培训讲师：高级虚拟化运维工程师

培训人数：4 人

培训内容：虚拟化系统的技术性能特点、使用方法、注意事项等内容，通过现场实验使用户掌握相关产品的使用和解决故障。

第七条：违约责任

1. 甲方无正当理由拒绝接受服务的，甲方应向乙方支付合同总价款百分之五的违约金。

2. 甲方无故逾期付款的，应按逾期付款金额的万分之五每日支付违约金。

3. 乙方逾期履行合同义务的，应按合同总价款的千分之六每日支付违约金。乙方逾期 10 个工作日及以上履行合同义务的，甲方有权解除本合同，并拒付（或要求乙方退还）合同价款，乙方应按合同总价款的 6%向甲方支付违约金，造成甲方损失的，乙方应承担赔偿责任。

4. 合同履行期内，任何一方因不可抗力事件不能履行合同的，合同履行期限可相应顺延。不可抗力事件发生后，应立即通知对方，并邮寄或送达有关权威机构出具的证明。

第八条：不可抗力事件处理

1. 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2. 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3. 不可抗力事件延续 120 天以上，双方应通过友好协商，确定是否继续履行合

同。

第九条：争议解决

本合同未尽事宜由双方协商解决，如协商不成，双方同意将本合同引起的争议提交甲方所在地法院起诉。

第十条：合同生效

1. 合同经三方法定代表人或授权代表签字并加盖单位公章后生效。

2. 合同执行中涉及采购资金和采购内容修改或补充的，须经甲方审批，并签书面补充协议报采购监督管理部门备案，方可作为主合同不可分割的一部分。

3. 本合同未尽事宜，遵照《民法典》有关条文执行。

4. 本合同一式七份，采购代理机构执一份，甲乙双方各执三份。

5. 本合同附件及甲方的招标文件、乙方的投标文件、书面澄清（承诺）等系本合同的组成部分。

甲方（需方）：浙江警察学院（公章）

甲方代表：

（签字）

地址：

邮编：

电话：

传真：

开户银行：

帐号：

签字日期：2021 年 12 月 8 日

乙方（供方）：（公章）

乙方代表：

（签字）

地址：杭州市西湖区翠柏路 6 号浙江电子研究所 3 幢 405 室

邮编：

电话：0571-56929076

传真：

开户银行：杭州联合银行骆家庄支行

帐号：201000258561897

签字日期：2021 年　　月　　日

合同鉴证方：

法定代表人或主要负责人：

（签字）

鉴证日期：2021 年　　月　　日

附件 1

维保服务内容

1、服务清单

项目	序号	服务名称	数量
基础设施维保服务	1	精密空调维保	1 项
	2	UPS 维保	1 项
	3	临安地下机房消防钢瓶检测服务	1 项
IT 全项服务	4	SSL 证书	1 项
	5	虚拟化平台维保	1 项
	6	数据库升级迁移及维保	1 项
	7	两校区网络维护服务	1 项
	8	两校区监控系统维护服务	1 项
	9	信息化项目全流程管理服务	1 项
安全服务	10	网络安全服务	1 项
	11	虚拟化防护授权	1 项
	12	玄武盾延保	1 项
	13	等保 2.0 服务备案及整改	1 项

2、服务详细

2.1、精密空调维保服务

（1）服务范围：

1、临安地下机房 2 台 英维克 30K 空调

2、临安地下机房 3 台 蓝代斯克 30K 空调

3、临安中心机房 2 台 英维克 12K 空调

4、滨江校网中心 1 台 英维克 30K 空调

5、滨江综合楼机房 2 台 艾默生 12K 空调

6、滨江综合楼机房 1 台 蓝代斯克 12K 空调

（2）服务要求：

1、对临安、滨江机房精密空调进行的 2 次精密空调巡检保养服务，主要是检测设备运行状况，检查历史运行记录有无异常情况，检查过滤网、皮带及加湿罐等易耗品，如需更换则尽快更换，完成后提交巡检报告单。365 天*24 小时电

话支持。维护保养人员应备专业知识和专业技能，自备专业设备工具及专业测量仪器检测设备。

2、设备发生故障后 2 小时内到达现场，检修设备，做好临时措施，保证机房温度。因配件原因无法短期内修复，应给出解决方案，如有特殊情况向校方提交书面报告说明情况。

3、本次维保为全包服务，维保中所有消耗品、配件更换及设备维修均由维保单位免费负责，不再产生额外费用。

4、提供巡检报告，巡检报告内容包括但不限于：服务人员出入记录、服务开始时间、服务结束时间、服务人员姓名、服务人数、服务地点、服务内容、服务结果。

（3）巡检内容：

1、控制系统:检查显示单元是否正常，各设置参数是否正确，查看历史报警记录对报警内容进行分析消除隐患。

2、空气过滤器:检查空气过滤器,如需检查或更换则检查或更换空气过滤器。

3、加湿器

1）检查蒸汽加湿盘是否结垢，如结垢需拆下进行清洗;

2）检查维护漏水报警系统

3）检查加湿器接线是否松动，按标准紧固。

4）检验供排水管和补水阀是否有损伤痕迹。

5）检查加湿器程控系统编程内容是否符合现场要求。

4、外部冷凝器和干冷器:

1)检查冷凝器是否清洁,如需清洁需用专用的清洗工具清洗室外冷凝器。风扇:检查风扇转动，有无异常噪声，运行电路是否正常。

2）检查室外冷凝器的电源开关，工作是否正常，绝缘是否可靠，电气接点是否紧固。

3）检查压力继电器，对室外风机的控制是否与设置的一-致并且根据当时的具体.工作环境调整压力断电器。

4）调速器(如果安装):检查调速器的工作状态，控制是否灵敏。

5、蒸发器:检查蒸发器是否清洁，如有污垢用药剂清洗，保证足够的热交换量。

6、风机组件:检查风机马达运转是否正常，有无异常噪音，并且轴承有无移动现象，如果移动超标，就要检查或更换轴承。对于由皮带传动的机 组，检查传动皮带，用手指拉紧时，是否可延长 2cm; 电机支架有无变形。分机叶轮有无异物，转动是否顺畅，与轴的连接是否紧固。

7、电加热器:检查三级电加热器的各级加热电流及各电气接点是否正常。电加热器的过热保护是否灵敏。

8、电路:

1)检查主电源及各支路的各相电压，电流。

2)检查所有的接触器，触点是否清洁，接触是否可靠、检测吸合的瞬间电流，对各接点进行紧固，确保安全。

3)对 24V 控制线路进行检测，确保控制的灵敏。

4)对各种的系统保护功能进行检测，(例如高压保护，低压保护，过热保护，相续保护等)保证设备的安全运转。

9、制冷系统:

1)检查制冷系统运行压力(高压，低压)是否正常，并根据当时的室外环境对压力进行适当的调节。

2)检查压缩机的三相绕组是否平衡，绕组的绝缘是否可靠。

3)进行过热度的测试，判断系统的运行效率是否能够达到指定的性能指标。

4)压缩机油位是否符合标准，工作时的声音是否异常，以判定系统的润滑程度。

5)制冷管道及膨胀阀的毛细管和平衡管是否异常。

6)检查压缩机部件是否有油渗漏痕，如发现必须查明原因,排除故障，使用 Sunisco3GS 制冷剂油恢复正常油位。

10、排水系统:检查排水系统是否畅通，如有水垢或异物堵塞管道，用药剂疏通管道，保证排水顺畅。

2.2、UPS 维保服务

（1）服务范围：

1、临安中心机房 1 台 科士达 15K

2、临安中心机房 1 台 科士达 40K

3、滨江综合楼机房 1 台 科士达 30K

4、滨江综合楼机房 1 台 艾默生 20K

5、临安地下机房 2 台 蓝代斯克 80

（2）服务要求：

1、对临安、滨江机房 UPS 进行的 2 次 UPS 巡检保养服务，主要是检测设备运行状况，检查历史运行记录有无异常情况，及时更换故障零部件，完成后提交巡检报告单。365 天*24 小时电话支持。维护保养人员应具备专业知识和专业技能，自备专业设备除尘和工具及专业测量仪器检测设备。

2、设备发生故障后 2 小时内到达现场，检修设备，做好临时措施，保证机房供电。因配件原因无法短期内修复，应给出解决方案，如有特殊情况向校方提交书面报告说明情况。

3、本次维保为全包服务，维保中所有消耗品、配件更换及设备维修均由维保单位免费负责，不再产生额外费用。

4、提供巡检报告，巡检报告内容包括但不限于：服务人员出入记录、服务开始时间、服务结束时间、服务人员姓名、服务人数、服务地点、服务内容、服务结果。

（3）巡检内容：

1、电池组的保养

1）检查电池组的物理状态

2）检查电池组的链接

3）检查电池外观情况（是否有漏液、鼓胀甚至开裂等情况）

4）进行链接 UPS 主机放电测试

5） 进行动态和静态测试

6） 检测后备时间测试

7） 检测浮充状态下电池电压测量

2、UPS 主机的保养

1）检查设备的运行状况及物理状态

2）检查设备易损单元(逆变器、整流器、静态开关、风扇)

3）检查设备的输入输出接线端是否牢固

4）检查功率连接的紧密程度(过热、氧化)

5）检查信号连接的紧密情况

6）进行充电电压测试

7）进行主、旁路切换测试

8）对需要清扫的机器进行除尘清扫

9）恢复设备运行，检查设备各项输入输出指标是否正常

2.3、临安地下机房七氟丙烷消防钢瓶检测服务

（1）服务范围：

临安地下机房 10 套七氟丙烷灭火剂瓶组

（2）服务要求：

1、根据我国消防法及中国质量监督检验检疫总局颁布的《压力容器技术监察规程》及《气瓶监察规程》中七氟丙烷消防钢瓶检验年限为 3 年强制检验的要求，对临安地下机房 10 套消防钢瓶进行检测。

2、七氟丙烷灭火设备灭火剂瓶组检测并提供第三方检验报告。

3、七氟丙烷灭火设备驱动气体瓶组检测并提供第三方检验报告。

4、补充钢瓶检测中损耗的七氟丙烷药剂。

5、七氟丙烷灭火设备灭火剂瓶组及驱动气体瓶组拆装。

6、包含来回运输费用。

7、灭火剂瓶组容量：22 公斤*10 瓶，共 220 公斤。

8、检测中发现钢瓶或药剂检测不合格的，2 瓶内（含）由中标方免费更换，以外的费用由甲方另外支付。

2.4、SSL 证书

（1）服务要求：

SSL 证书（SSL Certificates）为网站和移动应用提供数据 HTTPS 加密协议访问，保障数据的安全。装载 SSL 证书产品后自动激活浏览器中显示“锁”型安全标志，地址栏以“https”开头。提供的 SSL 证书（服务端和客户端），且均支持 ECC、RSA 或 SM（国密）三种加密方式。通配符域名证书 3 年。

2.5、虚拟化平台维保

（1）服务范围：

1、校园网及公安网 45 台 vmware 虚拟化物理主机

2、400 台虚拟服务器（维保期间数量如有增减，按实际增减后数量维保）

（2）服务要求：

1、7×24 电话服务和 7×24×4 现场技术支持保修服务。

2、提供 2 次/7 个月的 VCP 工程师现场系统性检查服务。针对客户各项配置(软件配置、核心参数配置、相关的数据配置)进行检查，针对不合理配置项提出调整建议，尽可能避免因配置不当造成的系统宕机及数据丢失风险。

3、将学校现有的虚拟化系统升级为稳定可靠的版本（包括补丁安装及软件版本升级），升级前需要提供完整的升级计划及方案，说明需要停机的时间等，升级完成后配合用户进行系统测试、提交系统升级实施报告和测试报告等。升级过程造成的一切损失，均由中标供应商承担。

4、对学校虚拟化平台进行整体分析，对占用资源较多的虚拟机进行优化；对长期不使用的虚拟机镜像资源重组再利用；对使用频繁的虚拟机进行合理化的调整；对单链路、单主机等情况的架构部署为冗余配置；对虚拟化后端存储配置不合理的，进行适当调整，提出建议及整改措施。

5、通过虚拟化专用备份软件对业务虚拟机进行异地备份，定期检查备份策略，保证数据正常备份。

6、滨江、临安校区所有服务器及虚拟化、超融合平台做一个资产整理，要求一个 VCP 的工程师在用户处驻点 2 个月时间。

7、配合第三方单位安装部署调试虚拟化平台。

8、虚拟化平台发生重大故障后 2 小时内到达现场，检修设备，做好临时措施，尽快恢复虚拟化系统。因配件原因无法短期内修复，应给出解决方案，如有特殊情况向校方提交书面报告说明情况。

9、提供巡检报告，巡检报告内容包括但不限于：服务人员出入记录、服务开始时间、服务结束时间、服务人员姓名、服务人数、服务地点、服务内容、服务结果。

2.6、数据库升级迁移及维保

（1）服务范围：

校园网、公安网 3 套核心业务数据库

（2）服务要求：

1、服务包括 7×24 电话服务和 7×24×4 现场技术支持保修服务。

2、提供 2 次/7 个月的 OCP 工程师现场检查服务。针对客户各项配置(软件配置、核心参数配置、相关的数据库系统配置、系统日志、系统软件性能)进行检查，针对不合理配置项提出调整建议，尽可能避免因配置不当造成的系统宕机及数据丢失风险。

3、将学校现有的数据库系统升级为稳定可靠的版本（包括补丁安装及软件版本升级），升级前需要提供完整的升级计划及方案，说明需要停机的时间等，并配合用户进行系统升级完成后的测试、提交系统升级实施报告和测试报告等。整个升级过程造成的一切损失，均由中标供应商提供。

4、中标供应商需立即对学校进行全面的信息收集和技术排查，提供给学校所有设备、数据库等的信息。

5、对数据库进行备份异地备份，定期检查备份策略，保证数据正常备份。

6、核心数据库发生重大故障后 2 小时内到达现场，检修设备，做好临时措施，尽快恢复虚拟化系统。因配件原因无法短期内修复，应给出解决方案，如有特殊情况向校方提交书面报告说明情况。

7、对非核心业务数据库提供技术支持（不纳入日常巡检维护范围）。

8、人员资质要求：OCP 工程师

9、提供巡检报告，巡检报告内容包括但不限于：服务人员出入记录、服务开始时间、服务结束时间、服务人员姓名、服务人数、服务地点、服务内容、服务结果。

2.7、两校区网络维护服务

（1）服务范围：

1、两校区校园网、公安网、医保、一卡通、政务网等网络

2、两校区 75 个井道、机房

（2）服务要求：

1、提供 2 名资深网络工程师 5*8 小时驻场服务，7×24 电话服务和 7×24×4 现场技术支持保修服务。

2、监控网络的日常运行情况，出现问题及时处理，保障网络系统可靠平稳运行。

3、巡检两校区 75 个井道，要求每两周对所有井道进行一次巡检，巡检内容

包括地面、水电门窗、机柜线路、设备运行、空调、温湿度、环境卫生、井道动环系统等，保证各井道运行安全稳定、环境干净整洁，线路整齐清晰，提供巡检记录。高温、雷雨季节部分重点井道需每天巡检。

4、对两校区4个大机房每天进行一次巡查，巡查内容包括地面、水电门窗、机柜线路、温湿度、UPS、空调、消防安全、设备运行状态、环境卫生等，保证机房运行安全稳定、环境干净整洁，提供巡检记录。

5、对两校区网络设备、安全设备的操作系统软件、配置文件每月进行备份、更新；对硬件物理工作状态进行检测与记录；对硬件技术工作性能进行检测与记录。时间均为每季度一次。对关键节点设备则依据使用与工作负荷情况，采取不定期实时检测。

6、配合第三方单位，调试网络配置。

7、建立健全各种技术文档资料，包括设备互联拓扑图、设备变更记录、IP地址分配、VLAN划分、路由配置、资产清单等。分析网络质量，优化网络配置，如有重要调整需保留调整记录。

8、遇招生体能测试、开学等重要敏感时期需加强值班，如有必要需加派人手，保证网络正常运行。

9、定期检查验证交换机、安全设备安全等设备策略是否生效；检查规则库、特征库是否按时升级；配合安全服务，进行简单的安全加固。

10、定期盘点资产，补贴资产标签，维护资产清单，及时更新新增报废资产信息。

11、监控校网、公安网核心业务系统，出现问题及时通知相关人员。

12、其他日常维护工作。

13、中标方需提供一套网络流量监控设备，要求包含应用识别、访问控制、应用负载均衡、应用路由、行为监控、带宽管理、行为审计、NPM应用时延监测、DNS管控、流量镜像等功能，实现上网应用可视化管理，通过对不同应用的流量监控，了解各种应用在网络流量中带宽占用情况，监控应用是否正常运行，监视服务器的运行状态并提供相应的统计报表。提供各种丰富的应用监控与分析功能，包括基于所有优先级的应用流量报表、所有基于配置策略的应用流量报表以及按照源IP地址、目的IP地址、源端口、目的端口、协议等生成各种格式的应用流量报表。可根据带宽大小、带宽百分比、总字节数、总包数、连接数等生成报表。

14、非工作时间网络发生重大故障或紧急情况，技术保障人员 2 小时内到达现场，检修设备，做好临时措施，尽快恢复业务。因配件原因无法短期内修复，应给出解决方案，如有特殊情况向校方提交书面报告说明情况。

15、提供工作日志及巡检记录，维护工作日志内容包括但不限于：维护时间、维护人员姓名、维护地点、维护内容、维护结果。

2.8、两校区监控系统维护服务

（1）服务范围：

1、两校区 1300 余路监控摄像头

2、监控相关业务系统

（2）服务要求：

1、提供 1 名资深网络工程师 5*8 小时驻场服务，7×24 电话服务和 7×24×4 现场技术支持保修服务。

2、每季度一次设备的除尘、清理，扫净监控设备显露的尘土，对摄像机、防护罩等部件要卸下彻底吹风除尘，之后用无水酒精棉将各个镜头擦干净，调整清晰度，防止由于机器运转、静电等因素将尘土吸入监控设备机体内，确保机器正常运行。同时检查监控机房通风、 散热、净尘、供电等设施。室外温度应在零下 20 C 与 60C 之间，相对湿度应在 10%与 100%之间;室内温度应控制在 5° C 与 35° C 之间，相对湿 度应控制在 10%~ 80%，留给机房监控设备一个良好的运行环境。

3、根据监控系统各部份设备的使用说明，每季度检测其各项技术参数及监控系统传输线路质量，处理故障隐患，协助监控主管设定使用级别等各种数据，确保各部份设备各项功能良好，能够正常运行。

4、对容易老化的监控设备部件每季度一次进行全面检查，一旦发现老化现象应及时更换、维修，如摄像头等;

5、对易吸尘部份每季度定期清理一次，如监视器暴露在空气中，由于屏幕的静电作用，会有许多灰尘被吸附在监视器表面，影响画面 的清晰度，要定期擦拭监视器，校对监视器的颜色及亮度;

6、对长时间工作的监控设备每月定期维护一次，如硬盘录像机长时间工作会产生较多的热量，一旦其电风扇有故障，会影响排热，以免硬盘录像机工作不正常;

7、对监控系统及设备的运行情况进行监控，分析运行情况，及时发现并排除故障。如:网络设备、服务器系统、监控终端及各种终端外设。桌面系统的运行检查，网络及桌面系统的病毒防御;

8、每季度定期对监控系统和设备进行优化:合理安排监控中心的 监控网络需求，如带宽、IP 地址等限制。提供每季度一次的监控系统网络性能检测，包括网络的连通性、稳定性及带宽的利用率等;实时检测所有可能影响监控网络设备的外来网络攻击，实时监控各服务器运行状态、流量及入侵监控等。对异常情况，进行核查，并进行相关的处理。根据用户需要进行监控网络的规划、优化;协助处理服务器软硬件故障及进行相关硬件软件的拆装等。

9、非工作时间监控系统发生重大故障，技术保障人员 2 小时内到达现场，，检修设备，做好临时措施，尽快恢复业务。因配件原因无法短期内修复，应给出解决方案，如有特殊情况向校方提交书面报告说明情况。

10、提供工作日志及巡检记录，维护工作日志内容包括但不限于：维护时间、维护人员姓名、维护地点、维护内容、维护结果。

2.9、信息化项目全流程管理服务

（1）服务范围：

所有信息化建设的日常维护工作

（2）服务要求：

1、通过专业人员统筹管理浙江警察院所有信息化建设的日常维护工作，与驻场运维工程师进行有效合作，有效开展校园网络等维护服务，同时对学校信息化建设提供有效建议，对学校信息化建设项目进行全流程管理，帮助校园网络中心减轻运维压力，帮助并支撑校园业务有效开展。

2、负责信息化建设过程中所有会议、论证、讨论的记录和文字整理工作，对各项目从申请立项到绩效考核全过程的材料进行收集、整理、编目、归档工作。

3、协助管理学校研发中心日常工作，收集各部门信息系统软件、硬件的需求，收集各项目申请立项书，配合各部门组织项目申报。

4、协助信息系统的日常维护和管理，确保应用系统的安全和稳定。

5、协助新建业务系统投入应用的实施工作，包括制订实施方案，安排实施进度，组织有关人员进行实施，对项目实施过程全程监督，确保信息系统的顺利

交付。

6、负责解决工作中涉及各应用系统技术性问题。

7、负责其他信息化日常工作。

8、提供工作日志，工作日志内容包括但不限于：时间、人员姓名、内容、结果。

9、人员资质要求：

1）计算机、信息科学技术、软件工程等相关专业本科以上学历。

2)从事软件开发与技术支持相关工作 10 年以上工作经验。

3）拥有有计算机程序设计员（三级）及计算机网络管理员（四级）证书。

4）有从事过高等院校软件研发或技术支持相关工作经历。

2.10、网络安全服务

（1）服务范围：

50 个 IP 地址的安全监控，核心业务服务器

（2）服务要求：

1、安全威胁分析：安全服务平台被动发现配合云端专家主动日志分析，识别服务范围内资产发现的病毒类事件、漏洞类事件、攻击类事件，并建立安全事件的进度监控机制。

2、对外服务威胁检查：针对对外的服务器，着重对 webshell、病毒进行重点排查，主动发现服务器风险隐患。

3、首次威胁处置：云端输出首次威胁分析报告，提供处置方法和工具给 T1；根据首次威胁分析报告，上门提供首次处置服务。

4、首次威胁汇报：处置完毕后，进行本次处置汇报，并进行报告解读。服务时效：服务组件上线 2 天后进行。

5、结合大数据分析、人工智能、云端专家提供安全事件发现服务：依托于安全防护组件、检测响应组件和安全平台，将海量安全数据脱敏，包括漏洞信息、共享威胁情报、异常流量、攻击日志、病毒日志等数据，经由大数据处理平台结合人工智能和云端安全专家使用多种数据分析算法模型进行数据归因关联分析，实时监测网络安全状态，发现各类安全事件，并自动生成工单。

6、安全威胁分析：安全服务平台被动发现配合云端专家主动日志分析，识别服务范围内资产发现的病毒类事件、漏洞类事件、攻击类事件，并建立安全事

件的进度监控机制。实时监测网络安全状态，对攻击事件自动化生成工单,及时进行分析与预警。攻击事件包含境外黑客攻击事件、高级黑客攻击事件、持续攻击事件。实时监测网络安全状态，对病毒事件自动化生成工单,及时进行分析与预警。病毒类型包含勒索型、流行病毒、挖矿型、蠕虫型、外发 DOS 型、C&C 访问型、文件感染型、木马型。云端专家针对每一类威胁，进行深度分析验证，分析判断是否存在其他可疑主机，将深度关联分析的结果通过邮件、微信等方式告知用户。结合最新威胁情报，及时对流行威胁进行评估、风险通告预警。安全专家排查是否对用户资产造成威胁，通知用户协助及时修复或调整安全策略。

7、策略调配：新增资产、业务变更策略调优服务，业务变更时策略随业务变化而同步更新。策略定期管理：安全专家每月对安全组件上的安全策略进行统一管理工作，确保安全组件上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。

8、策略调整：安全专家根据安全事件分析的结果以及处置方式，根据授权情况按需对安全组件上的安全策略进行调整工作。需提供用户授权界面截图。

9、针对病毒类的安全事件：安全专家提供病毒处置工具，并针对服务范围内的业务资产使用病毒处置工具进行病毒查杀，对于服务范围外的业务资产，安全专家协助用户查杀病毒。

10、针对攻击类的安全事件：通过攻击日志分析，发现持续性攻击，立即采取行动实时对抗，当用户无防御措施时，提供攻击类安全事件的处置建议。针对漏洞利用类的安全事件：安全专家验证该漏洞是否利用成功，提供工具协助处置。

11、针对失陷类的安全事件：安全专家协助用户处置，并提供溯源服务。基于主动响应和被动响应流程，对页面篡改、通报、断网、webshell、黑链等各类严重安全事件进行紧急响应和处置的解决方案。提供在服务平台申请主动响应的实际界面截图证明。根据事件发生的根因、影响范围，针对性给出安全加固方案。安全服务工程师通过现象深入分析安全事件的成因，发现用户网络中存在的薄弱点，通过技术手段和方法溯源攻击路径。针对勒索病毒、挖矿病毒、篡改事件、webshell、僵尸网络等安全事件，通过工具和方法对恶意文件、代码进行根除，快速恢复业务，消除或减轻影响。通过结合主动发现、主动处置、被动响应流程，对僵尸网络、病毒、后门、黑链等各类安全事件的处置服务。

12、提供安全态势简报。

13、人员资质要求：注册信息安全专业人员（CISP）

2.11、虚拟化防护

（1）服务范围：

1、31 台虚拟化物理主机

2、40 台物理主机

（2）服务要求：

1、原有 62 个物理 CPU 虚拟化防病毒模块续保，新增 62 个物理 CPU 虚拟化防火墙模块，20 个防病毒+防火墙（单客户端）续保，新增 20 个防病毒+防火墙（单客户端），提供 7 个月使用授权（含纸质授权书 1 份，电子授权码 1 份），包括：7X24 小时远程电话支持服务、病毒库升级服务、软件升级服务。

2、服务承诺函。

2.12、玄武盾延保

（1）服务范围：

20 个对外网站

（2）服务要求：

1、通过网站安全平台监测软件,为学校 20 个对外网站提供云防护和云监测功能。

2、服务承诺函。

2.13、等保 2.0 服务备案及整改

（1）服务范围：

2 套业务系统

（2）服务要求：

1、等保定级咨询：根据《GB/T 22240-2008 信息安全技术信息系统安全等级保护定级指南》的定级方法和指导意见，对两个系统进行定级对象分析、定级要素分析，初步确定系统保护等级，协助召开定级专家评审会议，确定系统保护等级，协助编制《等级保护定级报告》和《备案表》。协助联络公安机关，完成定级备案工作。等保测评实施：完成系统的基本情况调查、测评实施、工具扫描，对测评发现问题进行风险分析，编制测评报告，完成测评备案。

2、具体内容：依据等级保护 2.0 的相关标准《GB/T 22239-2019 信息安全

技术 网络安全等级保护基本要求》、《GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求》标准中的安全通用要求《云计算安全扩展要求》、《物联网安全扩展要求》等标准，对系统开展安全技术测评（包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等五个方面的安全测评）和安全管理测评（安全管理制度、安全管理机构、人员安全管理、安全建设管理和安全运维管理等五个方面的安全测评），出具符合信息安全等级保护主管部门要求的信息系统安全等级保护测评报告。提交的测评报告符合相应技术规范，并完成信息系统安全保护等级备案工作。

3、等保整改咨询：针对系统业务需求和部署环境，对等级测评发现的安全问题和漏洞隐患，提供安全整改咨询服务，形成测评问题汇总和整改建议。

4、等保整改：根据等保测评问题汇总和整改建议，针对系统业务需求和部署环境，对等级测评发现的安全问题和漏洞隐患，进行安全整改，形成整改建议报告。

附件2 合同清单：

序号	费用名称	数量	单位	单价	合价	备注
1	精密空调维保	1	项	¥42,000.00	¥42,000.00	/
2	UPS 维保	1	项	¥40,000.00	¥40,000.00	/
3	临安地下机房消防钢瓶检测服务	1	项	¥25,000.00	¥25,000.00	/
4	SSL 证书	1	项	¥15,000.00	¥15,000.00	/
5	虚拟化平台维保	1	项	¥26,000.00	¥26,000.00	/
6	数据库升级迁移及维保	1	项	¥26,000.00	¥26,000.00	/
7	两校区网络维护服务	1	项	¥134,000.00	¥134,000.00	/
8	两校区监控系统维护服务	1	项	¥67,000.00	¥67,000.00	/
9	信息化项目全流程管理服务	1	项	¥67,000.00	¥67,000.00	/
10	网络安全服务	1	项	¥47,000.00	¥47,000.00	/
11	虚拟化防护授权	1	项	¥98,000.00	¥98,000.00	/
12	玄武盾延保	1	项	¥20,000.00	¥20,000.00	/
13	等保 2.0 服务备案及整改	1	项	¥70,000.00	¥70,000.00	/
总报价					¥677,000.00	