政府采购合同（货物类）

项目编号：ZDCH-HW-2026845/02

合同编号：_____

项目名称：石景山区教育城域网核心机房基础设施升级改造（一期）和数据安全升级项目

分包名称：教育城域网数据安全升级项目

甲　　方：北京市石景山区教育委员会现代教育技术中心

乙　　方：北京紫翰科技有限公司

签署日期：2026年10月15日

合 同 书

北京市石景山区教育委员会现代教育技术中心（甲方）在石景山区教育城域网核心机房基础设施升级改造（一期）和数据安全升级项目中所需教育城域网数据安全升级项目（货物名称）经中鼎传鸿（北京）招标代理有限公司以 ZDCH-HW-2026845（项目编号）招标文件在国内公开招标。经评标委员会评定 北京紫翰科技有限公司（乙方）为中标人。甲、乙双方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本分，应该认为是一个整体，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. 中标通知书

c. 协议

d. 投标文件　　（含澄清文件）

e. 招标文件　　（含招标文件补充通知）

f. 货物清单　　（附合同后）

2. 货物内容和数量

本合同货物内容： 数据库审计 1 台、堡垒机 1 台、APT 1 台 、数据安全基础服务 1 项。

数　　量： /

详见附件 1 货物清单

3. 合同总价

本合同总价为人民币 738800.00 元（即人民币 柒拾叁万捌仟捌佰 元整，含税）

分项价格： 详见附件 1。

乙方在报价时已经充分考虑所报价格的合理性及市场价格波动对成本的影响，明确货物、人工、材料、施工机具使用费等的市场价格波动风险已经综合考虑并包含在投标报价中，本合同综合单价（或总价）不因乙方的任何原因及货物、人工、材料、机械等市场价格变化而进行调整。乙方不得以价格低为由拒不履行其合同义务，否则承担违约责任。

4. 付款方式

本合同的付款方式为：

（1）合同签署生效后，乙方向甲方交纳中标合同金额3%的履约保证金，即人民币22164.00元（人民币 贰万贰仟壹佰陆拾肆元整 ），并且提供首付款金额发票后，由甲方在10个工作日内向乙方支付合同总额40%的款项，即人民币295520.00元（人民币 贰拾玖万伍仟伍佰贰拾元整 ）。项目最终验收合格后，由乙方提出退还履约保证金申请，甲方于10个工作日内无息退还。如存在以下任一情形，甲方有权顺延退还，且不构成违约：

①乙方未提出书面申请；

②验收未通过；

③存在未解决争议。

（2）初步验收合格后10个工作日内，甲方向乙方支付合同总额30%的款项，即人民币221640.00元（人民币贰拾贰万壹仟陆佰肆拾元整）。

（3）初步验收合格后进入两个月试运行期，试运行期结束后开展项目最终验收，最终验收合格后10个工作日内，由甲方报送石景山区财政局或自行组织进行结算审计，甲方应以结算审定金额为准向乙方支付尾款。

双方同意，鉴于甲方付款依托于财政拨款，如遇财政拨款计划有变动，以款项实际到账时间和金额为准。如遇因财政拨款变动导致甲方实际付款时间迟于合同约定的情况和甲方实际支付金额不等于合同约定金额的情况（总支付金额等于合同金额），不构成甲方违约，甲方无需承担任何责任。甲方历次付款前，乙方应先开具等额有效发票，因乙方未及时开具发票导致甲方迟延付款的，该等责任由乙方自行承担。

5. 本合同货物交付时间及地点

交付时间：接采购人通知后 90 天内完成设备安装调试 。

交付地点：甲方指定地点

6. 合同的生效。

本合同经双方全权代表签署、加盖单位印章后生效。

7. 其他未约定事项见合同附件。

（本页无正文）

甲方：北京市石景山区教育委员会现代教育技术中心

名称：（印章）

日期：2026年10月15日

法定代表人或授权代表（签字或盖章）：

地址：北京市石景山区八角西街95号

邮政编码：100043

电话：010-68861221

开户银行：工行八角支行

账号：0200013429200006596

乙方：北京紫翰科技有限公司

名称：（印章）

日期：2026年10月15日

法定代表人或授权代表（签字或盖章）：

地址：北京市丰台区丰台总部基地17区18号楼10层

邮政编码：100070

电话：010-63788162

开户银行：交行北京丰台北路支行

账号：110060098015003650617

合同一般条款

1.定义

本合同中的下列术语应解释为：

1.1“合同”系指甲乙双方签署的、合同格式中载明的甲乙双方所达成的协议，包括所有的附件、附录和构成合同的其它文件。

1.2“合同价”系指根据合同约定，乙方在完全履行合同义务后甲方应付给乙方的价格。

1.3“货物”系指乙方根据合同约定须向甲方提供的一切设备、机械、仪表、备件，包括工具、手册等其它相关资料。

1.4“服务”系指根据合同约定乙方承担与供货有关的辅助服务，如运输、 保险及安装、调试、提供技术援助、培训和其他类似的服务。

1.5“甲方”系指与中标人签属供货合同的单位（含最终用户）。

1.6“乙方”系指根据合同约定提供货物及相关服务的中标人。

1.7“现场”系指合同约定货物将要运至和安装的地点。

1.8“验收”系指合同双方依据强制性的国家技术质量规范和合同约定，确认合同项下的货物符合合同规定的活动。

2.技术规范

2.1 提交货物的技术规范应与招标文件规定的技术规范和技术规范附件(如果有的话)及其投标文件的技术规范偏差表(如果被甲方接受的话)相一致。若技术规范中无相应说明，则以国家有关部门最新颁布的相应标准及规范为准。

3.知识产权

3.1 乙方应保证甲方在使用该货物或其任何一部分时不受第三方提出的侵犯专利权、著作权、商标权和工业设计权等的起诉。如果任何第三方提出侵权指控，乙方须与第三方交涉并承担由此发生的一切责任、费用和经济赔偿。

4.包装要求

4.1 除合同另有约定外，乙方提供的全部货物，均应采用本行业通用的方式进行包装，且该包装应符合国家有关包装的法律、法规的规定。包装应适应于远距离运输、防潮、防震、防锈和防粗暴装卸，确保货物安全无损，运抵现场。由于包装不善所引起的货物锈蚀、损坏和损失均由乙方承担。

4.2 每件包装箱内应附一份详细装箱单和质量合格证。

5. 装运标志

5.1 乙方应在每一包装箱的四侧用不褪色的油漆以醒目的中文字样做出下列标记：

收货人：

合同号：

装运标志：

收货人代号：

目的地：

货物名称、品目号和箱号：

毛重 / 净重：

尺寸(长×宽×高以厘米计)：

5.2 如果货物单件重量在 2 吨或 2 吨以上，乙方应在每件包装箱的两侧用中文和适当的运输标记，标明“重心”和“吊装点”，以便装卸和搬运。根据货物的特点和运输的不同要求，乙方应在包装箱上清楚地标有“小心轻放”、“防潮”“勿倒置”等字样和其他适当的标志。

6. 交货方式

6.1 乙方负责办理运输和保险，将货物运至甲方指定地点并安装调试。

6.2 甲方现场清点货物无误后，完成签收单据签字确认。

7. 装运通知

7.1 在现场交货和工厂交货条件下的货物，乙方通知甲方货物已备妥待运输后 24

小时之内，应将合同号、货名、数量、毛重、总体积（立方米）、发票金额、运输工具名称及装运日期，以电报或传真通知甲方。

7.2 如因乙方延误将上述内容用电报或传真通知甲方，由此引起的一切后果损失应由乙方负责。

8. 付款条件

8.1 付款条件见“付款方式”。

9. 技术资料

9.1 合同项下技术资料(除合同特殊条款规定外)将以下列方式交付：

合同生效后 10 日之内，乙方应将每台设备和仪器的中文技术资料一套，如目录索引、图纸、操作手册、使用指南、维修指南和/或服务手册和示意图寄给甲方。

9.2 另外一套完整的上述资料应包装好随同每批货物一起发运。

9.3 如果甲方确认乙方提供的技术资料不完整或在运输过程中丢失，乙方将在收到甲方通知后 3 日内将这些资料免费寄给甲方。

10. 质量保证

10.1 乙方须保证货物是全新、未使用过的，并完全符合强制性的国家技术质量规范和合同规定的质量、规格、性能和技术规范等的要求。

10.2 乙方须保证所提供的货物经正确安装、正常运转和保养，在其使用寿命期内须具有符合质量要求和产品说明书的性能。在货物质量保证期之内，乙方须对由于设计、工艺或材料的缺陷而发生的任何不足或故障负责。

10.3 根据甲方按检验标准自己检验结果或委托有资质的相关质检机构的检验结果，发现货物的数量、质量、规格与合同不符；或者在质量保证期内，证实货物存在缺陷，包括潜在的缺陷或使用不符合要求的材料等，甲方应尽快以书面形式通知乙方。乙方在收到通知后 1 日内应免费维修或更换有缺陷的货物或部件。

10.4 如果乙方在收到通知后 3 日内没有弥补缺陷，甲方可采取必要的补救措施，但由此引发的风险和费用将由乙方承担。

10.5 除“合同特殊条款”规定外，合同项下货物的质量保证期为自货物通过最终验收合格之日起 36 个月。

10.6 质保期满后免费维修硬件设施，只收取更换配件成本价。

11. 检验和验收

11.1 在交货前，中标人应对货物的质量、规格、性能、数量和重量等进行详细而全面的检验，并出具证明货物符合合同规定的文件。该文件将作为申请付款单据的一部分，但有关质量、规格、性能、数量或重量的检验不应视为最终检验。

11.2 货物运抵现场后，甲方应组织验收，并制作验收备忘录，签署验收意见。

11.3 甲方有在货物制造过程中派员监造的权利，乙方有义务为甲方监造人员行使该权利提供方便。

11.4 制造厂对所供货物进行机械运转试验和性能试验时，中标人必须提前通知甲方。

11.5 初步验收：所有产品到现场后，按采购文件要求对产品数量、规格、品牌、型号进行到货验收，完成所有设备安装调试，由乙方提出验收申请后可组织初步验收。初步验收需要提交文档包括但不限于：开工手续，支付手续、实施方案(含计划)、到货验收文件、隐蔽工程验收单、安装调试报告及记录、部署记录、系统联调测试报告、用户满意度调查表、初验总结报告，初验申请等文档，对系统整体及产品性能进行验收。初步验收通过后出具专家意见、初验报告。

11.6 初步验收合格并完成试运行期后，需要提交文档包括但不限于试运行方案、试运行记录、培训方案、培训记录、试运行总结报告（含记录）、用户使用意见表，终验总结报告，终验申请、项目运维方案等相关文档，进行最终验收，验收通过后出具专家意见、终验报告。

12. 索赔

12.1 如果货物的质量、规格、数量、重量等与合同不符，或在第 10.5 规定的质量保证期内证实货物存有缺陷，包括潜在的缺陷或使用不符合要求的材料等，甲方有权根据有资质的权威质检机构的检验结果向乙方提出索赔（但责任应由保险公司或运输部门

承担的除外）。

12.2 在根据合同第 10 条和第 11 条规定的检验期和质量保证期内，如果乙方对甲方提出的索赔负有责任，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

12.2.1 在法定的退货期内，乙方应按合同规定将货款退还给甲方，并承担由此发生的一切损失和费用，包括利息、银行手续费、运费、保险费、检验费、仓储费、装卸费以及为保护退回货物所需的其它必要费用。如已超过退货期，但乙方同意退货，可比照上述办法办理，或由双方协商处理。

12.2.2 根据货物低劣程度、损坏程度以及甲方所遭受损失的数额，经甲乙双方商定降低货物的价格，或由有权的部门评估，以降低后的价格或评估价格为准。

12.2.3 用符合规格、质量和性能要求的新零件、部件或货物来更换有缺陷的部分或/和修补缺陷部分，乙方应承担一切费用和风险并负担甲方所发生的一切直接费用。同时，乙方应按合同第 10 条规定，相应延长修补或更换件的质量保证期。

12.3 如果在甲方发出索赔通知后 10 日内，乙方未作答复，上述索赔应视为已被乙方接受。如乙方未能在甲方提出索赔通知后 10 日内或甲方同意的更长时间内，按照本合同第 12.2 条规定的任何一种方法解决索赔事宜，甲方将从合同款或从乙方的履约保证金中扣回索赔金额。如果这些金额不足以补偿索赔金额，甲方有权向乙方提出不足部分的补偿。

13. 迟延交货

13.1 乙方应按照“货物需求一览表及技术规格”中甲方规定的时间表交货和提供服务。

13.2 如果乙方无正当理由迟延交货，甲方有权提出违约损失赔偿或解除合同。

13.3 在履行合同过程中，如果乙方遇到不能按时交货和提供服务的情况，应及时以书面形式将不能按时交货的理由、预期延误时间通知甲方。甲方收到乙方通知后，认为其理由正当的，可酌情延长交货时间。

14. 违约赔偿

14.1 除合同第 15 条规定外，如果乙方没有按照合同规定的时间交货和提供服务，

甲方可要求乙方支付违约金。违约金按每周迟交货物或未提供服务交货价的0.5%计收。但违约金的最高限额为迟交货物或没有提供服务的合同价的5%。一周按7天计算，不足7天按一周计算。如果达到最高限额，甲方有权解除合同，同时要求乙方退还已支付款项并向甲方支付违约金。违约金不足以弥补甲方损失的，乙方应另行补足。

14.2 本协议项下所述“甲方损失”，包括但不限于甲方直接损失、第三方索赔损失以及甲方因维权支出的律师费、诉讼费、公证费等合理费用。

15. 不可抗力

15.1 如果双方中任何一方遭遇法律规定的不可抗力，致使合同履行受阻时，履行合同的期限应予延长，延长的期限应相当于不可抗力所影响的时间。

15.2 受事故影响的一方应在不可抗力的事故发生后尽快书面形式通知另一方，并在事故发生后7日内，将有关部门出具的证明文件送达另一方。

15.3 不可抗力使合同的某些内容有变更必要的，双方应通过协商在120日内达成进一步履行合同的协议，因不可抗力致使合同不能履行的，合同终止。

16. 税费

16.1 与本合同有关的一切税费均适用中华人民共和国法律的相关规定。

17. 合同争议的解决

17.1 因合同履行中发生的争议，合同当事人双方可通过协商解决。协商不成的，可向甲方所在地法院提起诉讼。

17.2 当事人一方在规定时间内不履行法院作出的生效判决的，另一方可以申请人民法院强制执行。

17.3 除本协议另有约定外，诉讼费应由败诉方负担。

18. 违约解除合同

18.1 在乙方违约的情况下，甲方可向乙方发出书面通知，部分或全部终止合同。同时保留向乙方追诉的权利。

18.1.1 乙方未能在合同规定的限期或甲方同意延长的限期内，提供全部或部分货物，

按合同第 14.1 的规定可以解除合同的；

18.1.2 乙方未能履行合同规定的其它主要义务的；

18.1.3 在本合同履行过程中有腐败和欺诈行为的。

18.1.3.1“腐败行为”和“欺诈行为”定义如下：

18.1.3.1.1“腐败行为”是指提供/给予/接受或索取任何有价值的东西来影响甲方在合同签定、履行过程中的行为。

18.1.3.1.2“欺诈行为”是指为了影响合同签定、履行过程，以谎报事实的方法，损害甲方的利益的行为。

18.2 在甲方根据上述第 18.1 条规定，全部或部分解除合同之后，应当遵循诚实信用原则，全部或部分购买与未交付的货物类似的货物或服务，乙方应承担甲方购买类似货物或服务而产生的额外支出。部分解除合同的，乙方应继续履行合同中未解除的部分。

19. 破产终止合同

19.1 如果乙方破产导致合同无法履行时，甲方可以书面的形式通知乙方，单方终止合同而不给乙方补偿。但甲方必须以书面形式告知同级政府采购监督管理部门。该合同的终止将不损害或不影响甲方已经采取或将要采取任何行动或补救措施的权利。

20. 转让和分包

20.1 政府采购合同不能转让。

20.2 经甲方书面同意，乙方可以将合同项下非主体、非关键性工作分包给他人完成。接受分包的人应当具备相应的资格条件，并不得再次分包。分包后不能解除乙方履行本合同的责任和义务，接受分包的人与乙方共同对甲方连带承担合同的责任和义务。乙方可以将合同项下非主体、非关键性工作分包给他人完成。但必须在投标文件中载明。

21. 合同修改

21.1 甲方和乙方都不得擅自变更本合同，但合同继续履行将损害国家和社会公共利益的除外。如必须对合同条款进行改动时，当事人双方须共同签署书面文件，作为合同的补充，并报同级政府采购监督管理部门备案。

22. 通知

22.1 本合同任何一方给另一方的通知，都应以书面形式发送，而另一方也应以书面形式确认并发送到对方明确的地址。

23. 计量单位

23.1 除技术规范中另有规定外，计量单位均使用国家法定计量单位。

24. 适用法律

24.1 本合同应按照中华人民共和国的法律进行解释。

25. 合同生效和其它

25.1 政府采购项目的采购合同内容的确定应以招标文件和投标文件为基础，不得违背其实质性内容。本合同一式肆份，具同等法律效力。甲方执贰份，乙方执贰份。合同将在双方签字盖章后开始生效。

附件 1 货物清单

序号	分项名称	制造商	品牌	规格、型号	单价（元）	数量	合价（元）
1	数据库审计	奇安信网神信息技术（北京）股份有限公司	奇安信网神	DAS3500-S3000-F60	120000	1 台	120000
2	堡垒机	奇安信网神信息技术（北京）股份有限公司	奇安信网神	BH3300-G-820Z-C57	100000	1 台	100000
3	APT	奇安信网神信息技术（北京）股份有限公司	奇安信网神	TY-TSS10000-S85-PF	278800	1 台	278800
4	数据安全基础服务	奇安信网神信息技术（北京）股份有限公司	奇安信网神	定制	240000	1 项	240000
总价（元）							738800

附件 2　售后服务方案

1. 方案总则

1.1. 编制目的

石景山区教育城域网是支撑全区教委机关、直属中小学、民办教育机构办公教学、学籍管理、师资运维、教育大数据统计的核心关键信息基础设施，承载海量教职工个人信息、学生学籍隐私数据及教育核心政务数据，具备 7×24 小时业务不间断、数据敏感度高、故障容忍度低、合规要求严苛、影响覆盖面广的核心特征，属于教育行业重点安全防护对象。

本项目部署 APT 深度安全检测设备、数据库安全审计设备、运维安全堡垒机三大核心安全设备，构建了内网威胁检测、全量数据审计、运维行为闭环管控的纵深安全防御体系，是保障全区教育网络安全、数据安全、运维合规的核心载体。设备长期稳定运行、安全策略持续有效、故障快速处置、风险闭环管控，直接决定教育业务连续性、师生数据安全性及行业合规达标有效性。

为规范项目全周期售后服务工作，建立标准化、体系化、闭环化的售后运维保障机制，明确团队配置、联络渠道、响应时效、处置流程、备件保障、应急值守、现场服务、质保到期过渡、考核改进等全维度工作标准，彻底解决售后响应滞后、故障处置拖沓、问题闭环不彻底、技术支撑断层等行业痛点，保障三大核心设备长期稳定、合规、高效运行，持续筑牢石景山区教育城域网安全防护屏障，特编制本专属售后服务保障方案。

1.2. 编制依据

本方案所有服务标准、流程机制、保障条款均严格对标国家法律法规、行业技术规范、教育行业专项要求及项目招投标文件、合同约定，核心编制依据如下：

① 《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》中关于信息化系统运维保障、故障应急、数据安全防护的相关条款；

② 《关键信息基础设施安全保护条例》中重点行业信息系统常态化运维、风险防控、应急处置的规范要求；

③ 国家标准《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）运维管理、日志留存、故障处置、持续安全保障合规条款；

④ 国家标准《信息安全技术 信息系统运维服务能力规范》（GB/T 33176-2016）

全流程运维服务管理标准；

⑤ 教育部《教育行业网络安全防护规范》《教育信息化运维服务管理规范》专项运维与安全保障要求；

⑥ 北京市教育行业网络安全运维、应急处置、安全督查相关管理规定；

⑦ 本项目招标文件、答疑文件、中标通知书、正式合同全部售后商务及技术服务条款；

⑧ 项目实施方案、试运行方案、应急处置方案、培训方案等配套技术文件；

⑨ 三大安全设备原厂售后服务标准、硬件维保规范、软件迭代体系及技术支撑机制；

⑩ 石景山区教育城域网业务架构、机房环境、运维模式及实际安全运维需求。

1.3. 服务总体目标

本项目售后服务以业务零中断、设备零宕机、风险零遗漏、问题零积压、合规零缺口、服务零短板为核心目标，构建“远程极速响应+现场快速处置+备件兜底保障+常态化巡检优化+持续迭代升级+全年应急值守”六位一体的长效售后保障体系，具体细化六大核心目标：

① 稳定性目标：质保期内三大核心设备整体运行稳定率≥99.99%，杜绝硬件宕机、系统崩溃、功能失效、策略异常等问题，全方位支撑教育城域网 7×24 小时不间断业务运行；

② 时效性目标：严格落实分级响应机制，对标合同最高时效标准，普通问题远程快速闭环，重大故障极速现场处置、备机兜底替换，杜绝故障长时间滞留、问题积压；

③ 合规性目标：通过常态化运维巡检、策略调优、日志留存、风险排查、报表输出，持续保障项目完全满足等级保护 2.0、数据安全法及教育行业安全督查合规要求，适配各类专项检查与合规测评；

④ 持续性目标：质保期内免费提供设备固件升级、威胁情报更新、检测规则迭代、功能优化升级，持续抵御新型网络威胁，适配教育业务迭代升级需求；

⑤ 能力赋能目标：通过常态化答疑、实操指导、专项复训、技术交底，持续提升采购人运维团队自主操作、故障排查、安全管控能力，实现设备稳定运行与人员能力提升双向赋能；

⑥ 风险闭环目标：建立故障、隐患、优化问题全台账闭环机制，实现问题有记录、

处置有过程、完成有核验、复盘有总结、长效有优化，彻底杜绝同类问题反复发生。

1.4. 服务适用范围

本方案适用于石景山区教育城域网数据安全升级项目全量建设内容，覆盖三年质保全周期及质保后增值服务周期，具体涵盖硬件设备、软件系统、授权服务、策略配置、交付成果、全服务场景六大维度：

① 硬件设备：APT 深度安全检测设备、数据库安全审计设备、运维安全堡垒机整机及冗余电源、硬盘、光模块、导轨、线材等全部原厂配套硬件；

② 软件系统：三台设备原厂操作系统、检测引擎、审计引擎、运维管控模块、态势感知模块、报表系统、权限管理系统等全部软件功能；

③ 授权服务：设备硬件维保授权、软件升级授权、威胁情报授权、规则库更新授权及各类资源并发授权；

④ 策略配置：项目建设期落地的镜像引流策略、告警白名单、风险检测规则、审计策略、运维权限体系、NTP 时间同步等全部定制化配置；

⑤ 交付成果：数据资产梳理台账、数据分级分类清单、安全管理制度、运维操作手册、培训资料等配套成果的答疑、优化与技术支撑；

⑥ 服务场景：日常运维答疑、设备故障处置、系统升级优化、安全策略调优、应急事件处置、常态化巡检、回访培训、合规支撑、问题闭环整改全场景售后工作。

1.5. 服务基本原则

为保障售后服务标准化、规范化、高质量落地，本项目全程遵循七大核心原则，所有售后工作严格对标执行：

① 业务优先、零影响原则：所有升级调试、策略变更、故障修复等高风险操作，一律避让教学、办公业务高峰，仅在夜间、周末、节假日低峰期实施，全程保障教育核心业务零中断、零卡顿、零风险；

② 极速响应、闭环处置原则：所有故障诉求、咨询疑问、优化需求分级响应、限时处置、全程跟踪、闭环核验，杜绝拖延处置、问题积压、无反馈、无结果；

③ 原厂标准、品质保障原则：所有硬件维保、软件升级、故障修复、功能优化均采用原厂配件、原厂技术、原厂标准，杜绝非正规配件、非标准化操作，保障设备原厂运行品质；

④ 预防为主、防治结合原则：依托常态化巡检、风险预判、策略优化，提前排查

化解潜在故障与安全风险，构建“事前预防、事中快速处置、事后复盘优化”全流程管控体系；

⑤ 透明公开、全程可溯原则：所有售后工作全程留痕，响应记录、处置过程、巡检报告、升级台账、问题闭环记录完整归档，实现全程可查询、可追溯、可核验；

⑥ 场景适配、按需服务原则：摒弃通用化模板服务，所有运维、优化、保障工作贴合教育行业业务特征、运维习惯与合规需求，定制化适配石景山区教育城域网实际场景；

⑦ 长效迭代、持续优化原则：依托原厂技术迭代能力，持续更新威胁情报与检测规则，结合业务升级、新型威胁、合规新政动态优化安全策略，保障防护能力长效有效。

2. 售后服务人员配置

2.1. 整体团队岗位配置

项目固定配置 7 名专职运维人员+3 名原厂技术专家，全员定岗不兼职、岗位不空缺，具体岗位配置如下：

① 项目售后总负责人（1 名）：高级项目经理，统筹全周期售后工作，对接采购人管理层，统筹应急处置与服务复盘；

② 运维工程师（1 名）：负责日常巡检、答疑、故障初步处置、台账整理；

③ APT 设备专项工程师（1 名）：专职负责 APT 设备运维、升级、策略调优、威胁分析、故障处置；

④ 数据库审计专项工程师（1 名）：专职负责审计设备运维、Caché/IRIS 数据库适配、数据审计策略优化；

⑤ 堡垒机专项工程师（1 名）：专职负责堡垒机权限管控、会话审计、运维策略优化、风险管控；

⑥ 售后质量管控专员（1 名）：负责服务监督、满意度回访、台账审核、问题整改复盘；

⑦ 7×24 小时应急值守专员（1 名）：全天候承接报修、咨询、工单流转，保障诉求零遗漏；

⑧ 原厂远程专家组（3 名）：三大设备原厂高级工程师，兜底解决疑难技术问题、底层故障、重大版本升级适配。

2.2. 各岗位资质与岗位职责

2.2.1. 项目售后总负责人

资质要求：本科及以上网络安全相关专业，持有 CISP 高级认证、信息系统项目管理师高级证书、原厂高级项目经理认证，5 年以上政企网络安全项目统筹经验。

项目经验：主导过 5 个及以上区县级教育行业网络安全项目售后运维，熟悉教育城域网架构、Caché/IRIS 数据库场景、教育合规要求及应急处置流程，具备重大安全事件统筹处置能力。

核心职责：统筹项目全周期售后服务规划、巡检计划、升级方案、应急预案；对接采购人管理部门，协调内外技术资源；审核所有售后台账与报告；组织季度、年度服务复盘；统筹重大故障与安全事件处置，保障整体服务质量达标。

2.2.2. 运维工程师

资质要求：大专及以上计算机相关专业，持有网络安全工程师、原厂设备运维认证，3 年以上网络安全设备现场运维经验。

项目经验：具备教育行业运维经验，熟悉教育机房管理制度、业务运行窗口期，熟练掌握三大设备日常操作、巡检排查、报表输出、基础答疑工作。

核心职责：常态化现场巡检、设备状态核查、基础告警梳理；承接日常操作咨询与实操指导；协助合规资料整理、安全自查支撑；记录日常问题并跟进闭环；配合设备升级、应急处置与专项培训工作。

2.2.3. APT设备专项售后工程师

资质要求：持有厂商 APT 设备高级运维认证，3 年以上 APT 设备实施、运维、优化经验，精通加密流量检测、WebShell 识别、隧道攻击研判、威胁情报迭代机制。

项目经验：参与过 3 个及以上教育行业 APT 运维项目，熟悉校园网攻击特征、师生终端异常外联行为，可独立完成设备故障排查、告警调优、态势分析、规则迭代工作。

核心职责：全权负责 APT 设备硬件维保、系统升级、情报库更新、检测规则优化、误报漏报调优、威胁态势分析、故障闭环处置及专项技术答疑。

2.2.4. 数据库审计设备专项售后工程师

资质要求：持有数据库审计设备原厂高级认证，精通主流及教育行业专用数据库审

计原理，3 年以上数据库审计设备运维经验。

项目经验：熟练掌握 Caché、IRIS 数据库运行机制与审计适配要点，具备教育行业数据库审计项目运维经验，可解决流量适配、敏感数据识别、异常访问研判等专项问题。

核心职责：负责审计设备硬件维保、系统迭代、审计策略优化、敏感数据扫描更新、合规报表定制、双向流量适配优化及故障专项处置。

2.2.5. 堡垒机专项售后工程师

资质要求：持有堡垒机原厂高级认证，精通运维权限管控、多因子认证、AD 域对接、会话审计、高危命令管控机制，3 年以上堡垒机运维经验。

项目经验：熟悉教育行业分级运维、多点管控场景，适配教育运维人员操作习惯，可针对性优化权限策略与风险管控规则。

核心职责：负责堡垒机硬件维保、系统升级、账号权限梳理、运维策略迭代、会话录像运维、高危操作管控、审计报表更新。

2.2.6. 售后质量管控专员

资质要求：3 年以上信息化项目服务质量管控经验，熟悉网络安全售后流程、台账规范、验收标准。

核心职责：全程监督售后响应时效、处置质量、服务规范；开展用户满意度回访；审核所有售后台账、巡检报告、整改记录；梳理服务短板，推动服务持续优化；归档全套售后资料。

2.2.7. 应急值守专员

核心职责：实行 7×24 小时无间断值守，全天候接听报修电话、监测服务群消息、接收线上工单；快速登记故障信息、分级流转工单、对接专项工程师；全程跟进处置进度、同步用户、归档值守台账，保障诉求零拖延、零遗漏。

2.2.8. 原厂远程技术专家组

由三大设备原厂总部高级研发工程师、技术架构师组成，不承接常规日常运维，专门兜底处置项目疑难故障、底层技术问题、重大版本升级适配、新型威胁规则定制，为项目提供原厂权威技术支撑。

2.3. 团队稳定性保障机制

为杜绝人员流动导致服务断层、服务质量下降，本项目建立严格的人员稳定管控体系：

① 人员备案固定机制：所有售后人员名单、资质、联系方式、岗位职责全部报备采购人备案，质保期内核心人员原则上不更换；确需调整的，提前 7 个工作日书面告知，完成全量项目交接与场景交底，经采购人确认后方可更替。

② 岗前专项交底机制：所有上岗人员必须完成本项目网络架构、业务场景、设备配置、运维规范、应急流程专项培训，考核合格后方可上岗。

③ AB 角双人备份机制：各专项岗位均设置主岗、备份岗，主岗人员离岗期间备份人员无缝接替，杜绝岗位空缺、服务停滞。

④ 常态化内部赋能机制：定期组织团队复盘新型网络威胁、设备新版本功能、教育行业合规新政，持续提升团队专业能力与项目适配能力。

3. 售后服务联络方式

3.1. 多维度专属联络渠道

(1) 7×24 小时专属售后热线

开通项目专属固定热线，全年 365 天无间断值守，专人接听、登记、流转、跟进，电话接通率 100%，无占线、无人接听、无故挂断问题，主要承接重大故障报修、紧急技术求助、应急事件上报等高频紧急诉求。

(2) 项目专属服务微信群

组建专属售后服务工作群，纳入采购人分管领导、运维人员、安全管理人员及我方全体售后团队、原厂专家，实行工作时间 1 分钟响应、非工作时间 5 分钟响应机制，承接日常答疑、进度同步、资料传输、问题反馈等常态化工作，群内沟通记录全程留存归档。

(3) 标准化线上工单系统

启用信息化工单管理系统，所有故障、咨询、优化需求、服务申请全部线上登记流转，实现“诉求录入-分级判定-人员分派-处置执行-进度跟进-结果核验-用户确认-闭环归档”全流程标准化管控，全程透明可溯、可查可评。

(4) 专属正式服务邮箱

开通项目专属售后邮箱，用于接收正式报修函、合规资料报送、巡检报告归档、升

级资料留存、书面整改通知等正式工作，专人每日查收、回复、归档，保障正式对接规范有据。

3.2. 分层级对接机制

为适配不同层级问题处置需求，避免资源浪费、处置层级不足，建立三级分层对接机制：

① 普通日常问题：由售后工程师、专项技术工程师直接对接、快速答疑、现场处置、即时闭环；

② 复杂技术与优化问题：由售后总负责人牵头，联合专项工程师、原厂专家协同研判、定制方案、落地优化；

③ 重大故障、应急事件、合规督查问题：我方高层负责人直接对接采购人分管领导，全程统筹处置、实时同步进度、落实保障措施。

3.3. 常态化沟通汇报机制

建立日通报、周周报、月月报、季度复盘的常态化汇报体系，确保服务透明化、进度可视化、问题可追踪：

① 每日值守通报：每日晚间在服务群同步当日设备运行状态、问题处置情况、运维工作小结及次日工作重点；

② 每周工作周报：每周输出售后周报，汇总本周故障台账、设备运行数据、策略优化内容、巡检情况及下周运维计划；

③ 每月服务月报：每月输出月度服务月报，全面复盘设备运行稳定性、问题闭环情况、升级优化成果、风险隐患整改情况；

④ 季度现场复盘会：每季度组织现场服务复盘会议，对接采购人梳理服务短板、优化运维方案、调整工作重点，持续提升服务质量。

4. 问题响应机制

4.1. 问题等级划分标准

(1) 一级重大问题（最高优先级 P0）

判定标准：设备整机宕机、核心功能失效、全网流量采集中断、审计服务瘫痪、运维管控失效、突发重大安全攻击、敏感数据异常泄露风险，直接影响整体安全防护体系与教育核心业务运行。

典型场景：APT 设备离线断流、数据库审计全量审计中断、堡垒机无法提供运维管控服务、设备硬件宕机、全网防护失效、内网大规模攻击爆发、批量敏感数据异常访问等。

(2) 二级一般故障（次高优先级 P1）

判定标准：设备局部功能异常、单条策略失效、模块运行异常、非核心告警异常、局部日志留存异常，不影响整体防护、审计、管控核心能力。

典型场景：单条检测规则误报、报表模板异常、个别运维账号权限异常、日志查询卡顿、设备偶发轻微告警、局部策略适配微调等。

(3) 三级普通咨询（常规优先级 P2）

判定标准：无故障、无风险的常规技术诉求，包含设备操作咨询、功能使用答疑、报表导出指导、运维流程咨询、制度解读等。

(4) 四级优化建议（长效优先级 P3）

判定标准：用户提出的策略优化、功能升级、运维流程完善、培训补充、台账迭代等优化类需求，无即时风险，可长效落地优化。

4.2. 分级响应时效标准

本项目响应时效优于行业标准、完全超额兑现招标文件及合同承诺，具体时效严格执行如下标准：

① 一级重大问题：7×24 小时即时响应，1 分钟工单登记，5 分钟工程师介入，2 小时抵达现场，12 小时无法修复立即启用备用整机替换；

② 二级一般故障：10 分钟响应对接，30 分钟远程排查，4 小时内完成修复闭环，复杂问题当日办结，需现场处置的 24 小时内到场；

③ 三级普通咨询：工作时间 1 分钟即时答疑，非工作时间 5 分钟响应、当场闭环；

④ 四级优化建议：24 小时对接确认需求，3 个工作日内完成方案落地与结果反馈。

4.3. 十步全流程闭环处置流程

所有等级问题统一执行“诉求接收→等级判定→工单分派→问题研判→处置执行→测试验证→用户确认→台账归档→复盘优化→长效整改”标准化闭环流程，确保问题处置无遗漏、无死角、可追溯。

① 诉求接收登记：多渠道接收用户诉求后，第一时间登记问题现象、发生时间、影响范围、对接人信息，录入工单台账；

② 等级快速判定：售后总负责人快速判定问题等级，匹配对应响应时效与处置资源；

③ 专人专项分派：根据问题类型精准分派对应专项工程师，明确处置时限与闭环要求；

④ 问题深度研判：工程师远程核查日志、设备状态、策略配置，精准定位根因，制定专属处置方案；

⑤ 限时处置执行：远程可解决的即时闭环，需现场处置的按时到场，硬件故障立即启动备件/备机保障机制；

⑥ 效果测试验证：处置完成后，核验设备功能、业务适配、策略有效性，杜绝次生故障；

⑦ 用户确认验收：同步用户核验处置效果，用户确认无误后完成工单初步闭环；

⑧ 台账完整归档：整理问题描述、根因、处置过程、验证结果、用户确认记录，完整归档；

⑨ 事后复盘优化：针对典型、反复性问题组织团队复盘，优化策略与运维流程；

⑩ 长效整改落地：针对共性短板完善巡检机制、策略规则，从源头规避同类问题复发。

4.4. 问题升级兜底机制

为杜绝复杂问题处置停滞、超时未闭环，建立三级升级兜底机制：

① 普通工程师无法处置的复杂问题，30 分钟内升级至售后总负责人统筹处置；

② 项目团队无法解决的底层技术问题，1 小时内升级至原厂专家组远程兜底；

③ 重大故障超时未修复，立即启动备机替换预案，优先恢复业务与防护能力；

④ 所有升级过程全程留痕，明确节点、人员、进度，确保问题全程有人跟进、有人负责。

5. 备品备件应急保障

5.1. 备件保障核心原则

① 业务优先恢复原则：硬件故障发生后，优先通过备件、备机恢复设备功能，再开展故障设备返修，最大限度缩短故障时长；

② 全覆盖保障原则：备件储备覆盖三大设备全部易损件、核心硬件、整机设备，无保障盲区；

③ 实时可用原则：所有储备备件、备机常态化通电检测、状态核验，确保随时可用、即插即用；

④ 零成本服务原则：质保期内所有备件更换、整机替换、硬件维修均为免费服务，无任何二次收费。

5.2. 四级备件储备体系

(1) 项目本地常备备件

项目常备三大设备高频易损硬件，实现小故障即时替换、快速修复，常备清单包含：设备冗余电源、千兆/万兆光模块、光纤跳线、备用硬盘、SSD 系统盘、原厂导轨、机房应急布线配件等。售后工程师每月盘点、定期通电检测，确保备件随时可用。

(2) 北京区域备件中心储备

依托我方北京区域备件库，储备同型号 APT、数据库审计、堡垒机核心硬件及半整机设备，距离石景山区机房通勤距离短、调度效率高，可实现当日备件送达、当日故障修复，覆盖中型硬件故障处置需求。

(3) 原厂全国备件调度中心

依托设备原厂全国统一仓储调度体系，全型号硬件配件现货储备，支持跨省极速调度、次日送达，彻底杜绝配件缺货、断供问题，兜底各类特殊硬件故障处置。

(4) 整机备机兜底保障（核心承诺）

我方郑重承诺：质保期内，若核心设备发生硬件故障，12 小时内无法彻底修复的，立即提供同规格、同性能、同功能全新备用整机替换上线，优先恢复设备防护、审计、管控全功能，故障设备返厂维修，维修完成后按需换回或留存备用，全程保障安全防护无空档、业务无中断。

5.3. 备件调用与替换标准化流程

① 故障判定：工程师排查确认故障为硬件问题，无法通过软件调试修复；

② 备件调度申请：根据故障硬件类型，启动对应层级备件/备机调度机制；

③ 现场替换部署：业务低峰期完成硬件替换、设备上线、配置恢复、策略同步；

④ 全功能核验：替换完成后核查流量采集、告警审计、运维管控等全功能状态，确保 100%恢复正常；

⑤ 故障硬件回收返修：故障硬件统一登记、回收、返厂维修，维修后纳入备用备件库；

⑥ 台账归档留存：完整记录备件替换时间、故障原因、替换内容、核验结果，形成专项台账。

5.4. 备件常态化管理机制

① 月度盘点机制：每月盘点本地及区域备件库存，及时补充短缺配件，保障库存充足；

② 状态核验机制：定期对备用硬件、备机通电测试、功能核验，避免闲置失效；

③ 专项资金保障：设立备件保障专项资金，保障质保期内备件补充、调度、替换零资金压力；

④ 闭环台账机制：所有备件取用、归还、替换、维修全程留痕，实现来源可溯、去向可查、状态可控。

6. 现场服务支持

6.1. 故障处置类现场服务

适用于硬件故障、远程无法定位的复杂异常问题。

① 到达现场之后，首先和采购人运维人员对接，确认故障现象、业务影响范围；

② 硬件层面：检查电源模块、硬盘、风扇、光模块、光纤链路，查看设备硬件告警灯；

③ 登录设备后台，核查系统日志、报错信息；核查双向镜像流量采集状态；核查审计报文捕获情况；

④ 定位故障根因：区分硬件故障 / 配置问题 / 外部网络环境问题；

⑤ 如果判定硬件故障，按照备件备机流程执行硬件更换或者整机备机替换；

⑥ 故障修复完成之后，开展全量功能验证：硬件状态、流量采集、告警功能、审计记录捕获、堡垒机会话录像；模拟教育业务访问，验证业务不受任何影响；

⑦ 向采购人现场同步故障根因、处置结果、后续注意事项；

⑧ 填写《现场服务记录表》，故障处置同步录入《售后工单登记表》《应急事件处置台账》。

一级重大故障：严格执行招标文件承诺，2 小时响应，4 小时抵达机房现场；12 小时无法修复，立即启动备机替换。

6.2. 预防性巡检类现场服务（月度、季度、年度巡检）

(1) 月度常规现场巡检

① 硬件健康检查：三台设备 CPU、内存、磁盘使用率、风扇、电源模块告警状态；

② 流量采集核查：APT 采集端口流量、数据库审计双向镜像流量，确认无断流，数据库审计可以捕获返回报文；

③ 授权与规则库检查：硬件维保授权有效期、APT 威胁情报库版本、情报条目数量；

④ 磁盘空间检查，预判磁盘满溢风险；

⑤ 查看近期高危告警，梳理真实威胁与业务误报；

⑥ 检查时间同步，三台设备时间偏差；

⑦ 检查物理布线、光纤、电源线连接是否牢固；

⑧ 现场和采购人运维人员简短沟通，收集运维疑问；

⑨ 输出《月度现场巡检报告》。

(2) 季度深度现场巡检

在月度巡检全部内容基础上增加深度核查：

① 逐条复核项目建设期全部安全策略基线：APT 检测规则、告警白名单；数据库审计规则、敏感数据扫描任务；堡垒机账号权限、高危命令黑名单、多因子认证配置；

② 对标数据安全法合规要求，核查日志留存时长≥6 个月，审计记录完整；

③ 复测全套客户端审计效果，重点校验查询返回结果捕获；

④ 排查内网潜在风险点，输出风险提示和优化建议；

⑤ 现场开展简短运维答疑，解答采购人运维人员实操疑问；

⑥ 输出《季度深度巡检报告》，发现问题全部纳入问题闭环台账。

(3) 年度全面现场巡检

① 硬件全维度体检，整机运行状态评估；

② 梳理一整年设备运行历史故障、告警趋势；

③ 全量核对全部授权有效期，预警即将到期的授权；

④ 全面复盘白名单、规则策略，结合全年业务变化做整体调优；

⑤ 配合采购人做年度安全自查支撑；

⑥ 输出《年度设备运行总报告》，给出下一年运维优化建议。

6.3. 硬件更换、备机替换现场服务

当设备电源、硬盘、光模块损坏，或者整机故障需要备机替换，现场执行如下工作：

① 进场前确认业务低峰窗口期，准备好备件 / 备用整机、配置备份文件、回滚方案；

② 现场硬件拆装，更换故障部件或者上架备用整机；

③ 备机场景：导入完整备份配置，核对 IP、NTP、镜像相关全部参数；

④ 设备上电，等待系统完全启动，硬件自检无告警；

⑤ 验证采集流量、告警、审计、堡垒机全部业务功能；重点验证数据库审计返回报文捕获；

⑥ 业务模拟访问验证，确认对原有七大教育业务系统无任何影响；

⑦ 故障硬件做好标签、登记回收，登记到备件备机调度处置记录表；

⑧ 现场向采购人演示确认设备恢复正常；填写现场服务记录。

6.4. 版本升级、重大配置变更现场服务

固件大版本升级等高风险操作，工程师现场值守执行：

① 严格使用采购人书面确认的时间窗口，夜间 / 周末业务低峰；

② 升级 / 变更前完整导出全部设备配置多重备份；

③ 现场执行升级或者配置变更，全程观察设备运行状态；

④ 升级完成逐项核验硬件、流量、告警、审计、堡垒机功能；重点验证 Caché、IRIS 审计功能不受版本升级影响；

⑤ 如果出现异常，现场立刻执行回滚方案，优先恢复业务；

⑥ 全部验证通过，记录版本信息，写入系统升级台账；

⑦ 现场向采购人运维人员同步升级结果。

6.5. 重大活动、安保专项现场值守服务

适用场景：开学季、中高考招生工作、网络安全保卫专项期、重大教育会议。

① 在关键保障周期内，按需工程师现场值守；

② 实时监控 APT 威胁告警、数据库审计高危访问告警、堡垒机高危运维告警；

③ 实时监控三台设备硬件状态、流量采集状态，一旦出现异常第一时间现场处置；

④ 配合采购人做安全态势研判，协助导出安全态势报表；

⑤ 保障周期结束输出专项值守小结。

6.6. 合规测评专项现场支撑

等保测评、数据安全专项督查、上级安全检查阶段，提供现场技术支持：

① 现场配合测评人员登录设备，演示功能；

② 按需导出审计报表、态势数据、日志记录，支撑合规测评；

③ 针对测评发现的问题，现场分析问题，制定整改措施；

④ 协助采购人完成整改落地，复核整改效果。

6.7. 人员变动补充现场培训交底

采购人运维岗位人员更替，提供现场补充实操培训：

① 现场机房结合设备实物开展讲解；

② 上机实操：告警查看、日志检索、报表导出、简单故障排查；

③ 交底本项目特殊点：审计注意事项、历史白名单基线、镜像链路关键点、应急回滚方案；

④ 发放操作手册，完成简易实操考核，留存培训记录。

6.8. 现场作业风险管控与操作流程

所有高风险现场作业，严格执行七步流程，规避业务误影响风险：

① 申请确认：提交现场服务申请，高风险操作同步脚本 + 回滚方案，采购人书面确认；

② 窗口确认：确认作业窗口期，避开教学、考试业务高峰；

③ 备份先行：操作前完整备份设备配置、交换机配置，本地多重保存；

④ 双人作业：硬件拆装、交换机配置修改等高风险操作，主操作 + 监护工程师双人在场；

⑤ 实施操作：严格按照确认过的脚本执行，不现场随意修改操作步骤；

⑥ 验证测试：操作完成后多维度验证硬件、流量、业务功能，重点验证审计捕获效果；

⑦ 确认闭环：采购人运维人员现场确认业务与设备运行正常，填写现场服务记录，归档全部资料。

现场作业一旦发生业务异常，第一优先级执行回滚恢复业务，再开展根因排查，禁止带着业务故障继续调试。

6.9. 现场服务输出交付物

每一次现场服务结束，根据服务类型输出对应书面交付物，电子 + 纸质归档，归入项目售后档案：

① 《现场服务记录表》

② 巡检类：《月度 / 季度 / 年度巡检报告》，附带硬件状态截图、告警统计、风险问题清单、整改建议；

③ 故障类：同步更新《售后工单登记表》《应急事件处置台账》，故障严重的输出故障处置简报；

④ 备件备机替换：填写《备件备机调度处置记录表》；

⑤ 版本升级：填写《系统版本升级台账》；

⑥ 专项值守：《专项保障值守小结》；

⑦ 现场培训交底：培训签到、实操记录。

7. 质保后服务

7.1. 质保到期预警机制

项目质保期到期前，我方正式出具《项目质保到期预警告知函》，以书面形式告知采购人剩余质保时长、设备硬件状态、软件授权有效期、威胁情报库到期时间，同步提供两套后续处置方案，预留充足采购决策周期，彻底杜绝授权过期、防护中断、技术支撑断层风险。

预警告知函同步附带：近一年设备运行健康报告、全设备授权到期清单、原厂维保参考报价、两套处置方案对比说明。

7.2. 质保到期两类可选处置方案

(1) 方案 A：续签原厂维保服务（推荐方案）

延续原厂全维度维保服务，完整继承质保期内所有服务权益，包含硬件维修更换、固件版本迭代、APT 威胁情报持续更新、7×24 远程+现场响应、备件备机保障、定期巡检、技术答疑等全套服务。我方提供原厂正式报价，协助采购人完成政府采购流程，保障新维保周期与原质保期无缝衔接，无任何服务真空期。

(2) 方案 B：不续签维保，提供有限免费咨询服务

若采购人暂不采购付费维保，我方承诺提供每年 12 次免费电话技术咨询服务，同

时明确服务限制与潜在风险：无硬件备件备机保障、无设备固件升级、无威胁情报与检测规则更新、无现场应急处置、无定期巡检服务，设备仅可保留基础日志查询功能，无法抵御新型网络攻击，安全防护能力持续弱化。我方将书面告知全部风险，由采购人评估决策并留存确认记录。

7.3. 到期平滑交接保障机制

质保到期前 30 天，我方无条件完成全套项目资料平滑交接，交付内容包含：全量设备配置备份文件、历年巡检报告与故障处置台账、全套操作与告警处置手册、原厂技术对接人信息、项目业务适配要点、安全策略基线资料。

若采购人更换新维保服务商，我方免费开展专项技术交底，完整移交项目场景、数据库适配要点、历史告警基线、运维注意事项，最大限度降低服务商更换带来的业务与安全风险。

7.4. 设备版本升级迭代管理

7.4.1. 升级工作总体原则

严格遵循业务优先、评估先行、备份先行、测试先行、回滚完备、窗口受控、升级后核验闭环七大原则。

① 业务优先：所有升级操作必须避让教学、考试、招生等核心业务高峰；重大版本升级仅允许夜间 22:00-次日 06:00 或者周末、节假日业务低峰窗口期执行；

② 评估先行：升级之前研读官方 Release Notes，梳理新增功能、修复漏洞、已知风险点、软硬件兼容约束，评估对现有教育业务、Caché/IRIS 审计策略、堡垒机运维权限体系的影响；

③ 备份先行：升级执行之前，完整导出设备全部配置，本地多重异地保存；

④ 测试先行：优先参考原厂测试报告，对变更点进行针对性功能验证；

⑤ 回滚完备：每一次升级操作必须具备完备回滚方案、回滚脚本、回滚操作步骤；

⑥ 窗口受控：升级窗口期提前向采购人书面提交升级申请，写明版本号、变更内容、风险点、执行时间窗口、回滚方案，获得采购人书面确认之后才启动升级；

⑦ 升级后核验闭环：升级完成逐项核验硬件状态、流量采集、审计、告警、运维管控全部核心业务功能，确认业务无异常，才算升级闭环。

区分两类升级：①情报库、攻击规则库增量小版本更新；②设备固件大版本升级。Beta 测试版本固件，严禁直接部署到生产业务环境。

7.4.2. 威胁情报库、攻击规则库增量更新（APT 设备）

威胁情报库、检测规则库属于增量更新，更新包体积小，主要新增新型 WebShell、远控木马、挖矿、加密攻击特征，不会改动设备底层业务配置。

① 默认开启自动每日增量更新模式；

② 如果教委运维人员希望人工管控，可以切换为手动模式，我方定期推送新版本情报库；

③ 更新完成，我方协助采购人简单验证设备 CPU、内存负载，确认不会出现告警风暴；

④ 如果更新之后出现大量业务误告警，立刻支持回退至上一版情报特征库；

⑤ 情报库更新操作记录，写入《系统升级台账》归档。

7.4.3. 固件大版本升级完整管控流程

步骤 1：原厂发布正式 Release 稳定版本，我方专项工程师完整研读 Release Notes 文档，梳理：版本主要变更、安全漏洞修复内容、新增功能、已知缺陷、硬件兼容约束、对现有策略的潜在影响，重点评估对 Caché/IRIS 数据库审计、堡垒机 AD-LDAP 对接、多因子认证配置的影响。 步骤 2：向采购人提交《版本升级书面申请报告》，写明：当前旧版本号、目标新版本号、升级主要变更内容、潜在风险、建议升级时间窗口、完整回滚操作方案。等待采购人书面确认。 步骤 3：升级执行之前，完整导出 APT、数据库审计、堡垒机三台设备全部配置文件，本地多重备份归档。 步骤 4：仅在采购人确认的夜间或者周末业务低峰窗口期开展升级。 步骤 5：执行升级操作，全程观察设备升级进度，不人为中断升级流程。 步骤 6：升级完成，登录后台逐项做全量功能核验： ① 硬件：CPU、内存、风扇、磁盘状态； ② 采集端口流量：APT 镜像流量、数据库审计双向 SPAN 镜像流量，确认报文采集正常； ③ 关键业务功能：APT 威胁告警、数据库审计 Caché/IRIS 操作捕获、堡垒机多因子认证、会话录像回放； ④ NTP 时间同步状态，三台设备时间偏差≤1s； ⑤ 选取教育真实业务访问样本，模拟访问，验证检测、审计、运维管控功能生效。 步骤 7：升级全部功能验证通过，将升级信息、版本号、时间窗口、回滚预案、核验结果完整写入《系统升级台账》。

如果升级之后出现业务异常，立刻严格按照回滚方案执行，退回旧固件版本，恢复备份配置，再开展根因分析，不允许带着故障继续运行生产环境。

7.4.4. 升级台账记录要求

每一次固件大版本升级，必须记录：升级日期、旧版本号、新版本号、申请报告编号、采购人确认情况、升级时间窗口、是否执行回滚、升级后功能核验要点、升级执行人。情报库重大版本更新同样简要登记。《系统升级台账》归入竣工交付文档。

7.4.5. 升级故障处置预案

① 升级过程设备断电、升级卡死：严格执行回滚流程，恢复上一稳定固件，导入升级之前备份配置；

② 升级完成后出现大量业务误告警：优先回退旧版本，再分析新版本规则变更带来的影响；

③ Caché / IRIS 数据库审计捕获返回结果失效：回滚，联系原厂分析新版本对后关系数据库解析模块改动；

④ 堡垒机多因子认证、AD 域对接异常：回滚，核查配置兼容性。 所有升级故障处置过程，完整记入售后问题闭环台账。

8. 应急处置措施

8.1. 事件分级标准

① 一级重大事件 P0（最高优先级）：设备整机宕机、核心功能失效、流量采集中断、审计中断、运维管控瘫痪、发生重大安全事件、业务存在重大数据泄露风险；响应：7×24 小时即时响应，1 分钟工单登记，5 分钟工程师介入，2 小时到达石景山区教育机房现场，12 小时无法修复提供备机。

② 二级一般事件 P1（次高优先级）：设备局部功能异常，不影响整体防护审计能力；响应：10 分钟响应对接，30 分钟远程介入排查，4 小时完成故障修复，需要现场处置的 24 小时抵达现场。

③ 三级普通事件 P2：普通咨询、配置微调需求，无业务风险；响应：工作时间 1 分钟响应，非工作时间 5 分钟响应。

④ 四级优化事件 P3：策略优化、体验提升类建议；响应：24 小时确认需求，3 个工作日落地优化。

8.2. 应急组织架构

① 应急总负责人：项目售后总负责人，统筹全部重大事件处置；

② 现场处置组：运维、专项技术工程师，负责现场排查、操作执行；

③ 原厂远程技术专家组：APT、数据库审计、堡垒机原厂高级工程师，疑难问题兜底；

④ 对外通报对象：采购人项目对接人、机房管理员。

处置核心原则：业务优先，回滚优先；备用资源前置；事件闭环复盘；重大故障优先恢复业务能力，再深度排查根因。

8.3. 分阶段各类场景处置流程

8.3.1. 供货物流阶段应急场景

场景编号	场景	处置流程	响应时限	备用资源 / 补救措施
YH- 01	原厂排产延期，整机生产发货滞后挤压 90 天总工期	1. 供应链专员第一时间获知延期；项目经理向采购人出具正式书面风险预警，写明预估滞后时长；2. 协调原厂优先调拨国内仓库现成整机；3. 启用原厂备用整机资源；4. 并行开展勘查、方案确认等不依赖硬件的工作；5. 每周书面同步供货状态	发现风险 1 个工作日书面预警采购人	原厂预留同型号备用整机，多仓库备选调度；并行非硬件类工作消化时间
YH- 02	物流运输货物严重损坏，包装箱撞击变形、进水	1. 现场停止开箱，保护现场，拍照录像留存证据；2. 向保险公司报险，同步采购人；3. 不等待保险理赔结案，直接调度原厂备用整机重新发货；4. 损坏设备后续走保险返修流程，理赔流程不作为工期滞后理由	现场发现 30 分钟上报项目经理	优先补发备用整机，保障工期不受理赔流程影响
YH- 03	恶劣天气、交通故障，物流到货推迟	1. 跟踪物流实时状态，评估预计延误时长；2. 书面告知采购人预计变更到货时间；3. 协调物流服务商优先转运；备选物流线路预案	识别延误 2 小时通报采购人	备选物流线路预案，并行开展文档编制工作

8.3.2. 到货开箱阶段应急场景

场景编号	场景	处置流程	响应时限	备用资源 / 补救措施
DH- 01	到货开箱发现硬件故障，硬盘、电源等硬件自检报错	1. 现场拍照记录，记录到货验收单；2. 启动原厂备用整机预案，协调备用整机发货；故障设备禁止进场施工，退回原厂返修；3. 向采购人同步现场情况	30 分钟上报项目经理	原厂备用整机，故障设备禁止进场施工，保障后续施工不受硬件故障拖累

8.3.3. 上架施工调试阶段网络业务故障应急

(1) 场景 1：配置 SPAN 镜像之后，交换机 CPU 负载飙升，业务受影响 处置流程：

① 立刻删除新增 SPAN 镜像配置，恢复交换机原始配置，优先保障业务；

② 根因定位：镜像源范围过大，把大量备份存储无效大流量报文全部镜像，造成交换机性能过载；

③ 优化镜像策略，配置过滤规则，剔除无效备份报文，只保留安全检测所需要业务流量；

④ 修改完成，小窗口测试，观察交换机 CPU 指标正常，再重新启用镜像；

⑤ 事件记入应急台账，向采购人同步情况。

(2) 场景 2：堡垒机 ACL 变更之后，运维人员全部无法登录业务资产 处置流程（回滚优先原则）：

① 立刻执行回滚脚本，删除新增 ACL 限制，恢复运维网段直连访问权限，保障运维通道可用；

② 排查 ACL 配置错误点，修正策略；

③ 再次选择夜间业务低峰窗口期，重新执行堡垒机切换；

④ 多名运维人员分别测试不同资产登录，验证全部运维功能正常；

⑤ 事件记入应急台账，内部复盘根因。

(3) 场景 3：Caché / IRIS 数据库审计解析异常，无法捕获返回结果报文 处置流程：

① 核查交换机是否配置双向 inbound+outbound 镜像，检查光纤链路；

② 联系数据库审计原厂工程师远程接入，抓取现场真实业务流量报文定位解析问题；

③ 开展固件调优、参数配置调整；

④ 使用真实业务客户端全套模拟操作，验证请求报文、返回报文都被完整审计捕获；

⑤ 疑难情况，启用备用整机替换测试；全部缺陷闭环之后，再进入下一阶段工作。

8.3.4. 设备硬件故障应急

招标文件商务：质保期 7×24 小时售后响应，2 小时内响应；4 小时内到达现场开展维修，12 小时不能修复的提供备机。本项目实施调试阶段同等执行备机保障，不只是质保期。 故障处置流程：

① 设备硬件告警上报，我方工程师 2 小时内响应；

② 评估硬件故障，如果条件满足，则 4 小时工程师抵达石景山区教育机房现场排查；

③ 经现场判定 12 小时之内现场无法修复故障设备，立刻启动备机调度，原厂调配备用整机运抵机房现场；

④ 备机上架，导入原有设备备份配置，恢复安全防护能力；

⑤ 故障硬件设备返厂维修；

⑥ 故障全过程向采购人同步进展；事件记入应急事件处置台账。

8.3.5. 告警误报、漏报应急处置

大量误告警风暴：试运行或者正式运行出现海量业务正常行为产生告警，运维无法开展运营。 处置：我方工程师远程登录设备，联合采购人梳理合法业务基线，配置告警白名单，调整告警阈值，区分高危中危低危告警；输出调优完成配置包以及《告警处置运维操作手册》。

发现存在漏报风险：模拟测试发现攻击行为没有被检测识别。 处置：第一时间提交原厂，抓取现场流量样本；原厂更新检测规则库或者固件版本；升级之后回归测试验证检测效果。

8.4. 应急上报、台账与复盘机制

① 上报机制：一级重大事件，15 分钟电话 + 书面简报同步采购人；二级一般事件 30 分钟通报；三级优化类事件纳入日常问题闭环台账。

② 应急事件处置台账：记录事件编号、发生时间、事件现象、事件等级、处置步骤、处置结束时间、业务是否恢复。

③ 复盘改进机制：每发生一级、二级应急事件，处置完成之后 3 个工作日开展内部复盘会议，分析根因，修改实施方案、操作脚本、预防措施，防止同类事件再次发生；复盘记录归入项目档案。

售后服务承诺：

承诺方提供制造商的新品、正品，能保证相应的制造商质保维修服务，在设备发生故障保修后30分钟内响应，2 小时内到达用户现场提供服务。质保期内保证所有设备均可正常使用，保障各系统稳定运行且功能正常，不能耽误用户方使用。质保期以项目通过最终验收之日起计算，质保期三年，质保期内所有硬件更换免费。提供制造商和承诺方的终身技术服务。

特此承诺！

承诺方名称（盖章）：北京紫翰科技有限公司

日期： 2026 **年** 10 **月** 15 **日**