**招 标 文 件**

 **项目名称：北仑区校园智能安全防控系统**

 **项目编号：BLZFCG2020038**

 **采 购 人：****宁波市北仑区教育局**

 **采购机构：宁波市北仑区（开发区）公共资源交易中心**

**二〇二〇 年 九 月**

目 录

1、第一部分………………………………投标邀请

2、第二部分………………………………前附表

3、第三部分………………………………投标人须知

4、第四部分………………………………项目内容及要求

5、第五部分………………………………采购合同

6、第六部分………………………………投标文件组成及格式

7、第七部分………………………………评标办法及评分标准

**第一部分 投标邀请**

根据《中华人民共和国政府采购法》及有关办法，宁波市北仑区（开发区）公共资源交易中心受宁波市北仑区教育局委托，就北仑区校园智能安全防控系统项目进行公开招标，欢迎符合本项目资格要求的供应商参加投标。

一、项目编号：BLZFCG2020038

二、项目名称：北仑区校园智能安全防控系统

三、项目概况

1、预算金额：人民币1068.55万元

2、最高限价：人民币1068.55万元

3、采购需求：北仑区校园智能安全防控系统包括：1.校园智能安全防范信息平台建设；2.前端校园安防系统建设；3.支撑平台及安全系统建设；4.配套机房建设。

4、交付时间：合同签订后3个月内完成。

5、本项目不接受联合体投标。

四、投标人的资格要求

1、满足《中华人民共和国政府采购法》第二十二条规定；

2、本项目的特定资格要求：

（1）具备独立法人资格或是（银行、保险、电信行业）依法设立的分支机构。

（2）北仑区域内拥有有线网络的运营商(基础电信业务运营商或有线电视业务运营商)。

（3）若两家及以上投标人为同一单位的分支机构或子公司与同一单位具有隶属关系的，只允许一家参与投标，否则将都被取消投标资格。

五、招标文件获取时间及方式

1、时间：即日起至投标截止时间前。

2、地点：政府采购云平台（www.zcygov.cn）

3、方式：通过注册账号登录政府采购云平台在“项目采购”应用模块内获取采购文件。

4、售价：免费

六、提交投标文件截止时间、开标时间和地点

1、提交（上传）投标文件截止时间和开标时间：2020年10月21日09时30分（北京时间）

2、电子投标文件上传地点：政府采购云平台（www.zcygov.cn）

3、备份电子投标文件提交地点和开标会议地点：北仑区四明山路773号行政大楼B座三楼区公共资源交易中心交易厅（具体场所安排详见电子指示屏幕）。

七、投标注意事项

1、参加投标的供应商有义务在采购活动期间浏览宁波政府采购网（www.nbzfcg.cn）和宁波公共资源交易网北仑区分网（beilun.bidding.gov.cn），采购人（采购代理机构）在以上两个网站发布的与本次招标项目有关的信息视为已送达各供应商，不再采用其它方式传达相关信息。

2、本项目采用网上投标，不接受纸质投标文件，请投标供应商按照招标文件和政府采购云平台的要求编制、加密上传电子投标文件。

3、投标人上传电子投标文件后，还可以自行确定是否提交备份电子投标文件，如确定提交备份文件的，投标人应在投标截止时间前，将在“政采云投标客户端”上编制生成的后缀名为.bfbs的备份投标文件，以U盘为载体装袋密封后送达至开标地点，密封袋上需注明项目名称、项目编号、投标人名称并加盖公章。供应商仅提交备份电子投标文件的，投标响应无效。

3、采购代理机构解密指令发出后30分钟内，投标人应登录政采云平台，通过CA数字证书完成对电子投标文件的解密（开评标期间，投标供应商应关注政采云平台上的指令信息和手机短信并及时处理）。若投标人在规定时间内无法解密或解密失败，此时启用备份电子投标文件（如有），若备份投标文件仍无法使用，则视为无效投标。供应商制作电子投标文件和解密投标文件时必须使用同一把CA数字证书。

4、本项目有现场演示的环节，投标供应商应派代表到现场参加开评标会议。

5、本项目采用网上投标的方式进行，供应商投标前须办理CA数字证书和安装“政采云电子交易客户端（政采云投标客户端）”，并通过“政采云投标客户端”编制电子投标文件，供应商在使用系统进行投标的过程中遇到涉及平台使用的任何问题（包括不限于供应商注册、采购文件获取、CA数字证书办理、政采云投标客户端安装、投标响应文件制作加密上传等），可登录政府采购云平台网站（www.zcygov.cn）“服务中心”版块查阅相关的帮助文档和教学视频，也可致电政采云平台技术支持热线咨询，热线电话：400-881-7190。

6、疫情期间，请投标人代表全程佩戴口罩、一次性手套等防护工具，进入北仑区公共资源交易中心前，进行身份证实名登记，出示甬行码（健康码），自觉接受防疫期间有关要求，并如实报告情况，通过身份核验正常方可入场。出现发热症状等可疑情况，将予以劝离并登记上报。

八、联系方式

1、采购人

名 称：宁波市北仑区教育局

地 址：北仑区四明山路773号行政大楼B座四楼

项目联系人：吴剑斌 电话：0574-89383997

2、采购代理机构

名 称：宁波市北仑区（开发区）公共资源交易中心

地 址：北仑区四明山路773号行政大楼B座三楼

项目联系人：贝小明 电话：0574-89383942 传真：0574-89383949

3、同级政府采购监督管理部门

名 称：宁波市北仑区财政局

地 址：北仑区四明山路775号行政大楼A座六楼

联系人：阮老师

监督投诉电话：0574-89383756

**第二部分 前附表**

|  |  |
| --- | --- |
| **序号** | **内 容** |
| **1** | 项目名称：北仑区校园智能安全防控系统项目编号：BLZFCG2020038 |
| **2** | 采购人：宁波市北仑区教育局项目联系人：吴剑斌 电话：0574-89383997地址：北仑区四明山路773号行政大楼B座四楼采购代理机构：宁波市北仑区（开发区）公共资源交易中心项目联系人：贝小明 电话：0574-89383942 传真：0574-89383949地址：北仑区四明山路773号行政大楼B座315室业务二部邮编：315800 |
| **3** | 采购方式：公开招标  |
| **4** | 评标方法：综合评分法  |
| **5** | 采购预算（最高限价）：人民币1068.55万元。 |
| **6** | 是否接受进口产品投标：不接受 |
| **7** | 是否接受联合体投标：不接受 |
| **8** | 是否为专门面向小微企业的采购项目：否 |
| **9** | 是否允许投标人将项目非主体、非关键性工作交由他人完成：否 |
| **10** | 集中答疑会或现场踏勘：采购人不集中组织，供应商如有需要，请自行踏勘。 |
| **11** | 提交（上传）投标文件截止时间和开标时间：2020年10月21日09时30分开标会议地点：北仑区四明山路773号行政大楼B座三楼区公共资源交易中心交易厅注：本项目采用网上投标，不接受纸质投标文件，投标供应商须按照招标文件和政府采购云平台的要求编制、加密上传电子投标文件。 |
| **12** | 备份电子投标文件提交地点：北仑区四明山路773号行政大楼B座三楼区公共资源交易中心交易厅备份电子投标文件提交受理时间：2020年10月21日09时00分～09时30分注：投标人可自行决定是否提交备份电子投标文件。提交的备份电子投标文件应当袋装密封，密封袋上须注明项目名称、项目编号、投标人名称并加盖投标人公章。 |
| **13** | 投标有效期：开标之日起60日历天 |
| **14** | 投标保证金：本项目不收取投标保证金。 |
| **15** | 履约保证金：在收到第一笔款项前，中标供应商须按合同金额的5%以支票、银行转账、银行保函或保险保函等非现金方式向采购人交纳履约保证金；履约保证金在项目验收合格满四年后一周内无息退还。 |
| **16** | 投标人信用信息查询：资格审查时，通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）渠道查询投标人信用记录，经查询列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单，且在禁止参加采购期限内的，其投标将被拒绝。 |
| **17** | 其他说明：对于招标文件中提及的彩色扫描件要求，包括彩色照片件。扫描件的内容应当保证清晰可辨，否则由此产生的风险由投标人承担。 |

**第三部分 投标人须知**

**A、总则**

**1、适用范围**

1.1本招标文件适用于采购公告中所述项目的招标、投标、评标、定标、合同签订及履约、验收、付款等行为（法律、法规另有规定的，从其规定）。

**2、定义**

2.1“采购人”/“招标人”/“买方”系指前附表所指的采购人。

2.2“采购代理机构”/“采购机构” 系指前附表所指的组织本次政府采购的采购代理机构。

2.3“投标人”/“供应商”/“响应方”/“承包方”/“卖方”系指符合本招标文件规定并参加投标的供应商。

2.4“货物”指依据本招标文件中所述采购需求，投标人须向采购人提供的一切材料、设备、备品备件、工具、手册及其它有关技术资料和材料，以及实现货物功能价值所必须的配套技术和服务。

2.5“服务”指依据本招标文件中所述采购需求，投标人应该履行的承诺和义务。

2.6“法定代表人”本项目所指的法定代表人包含符合招标要求依法成立的分支机构的负责人。

**3、合格的投标人**

3.1符合2.2条件，并具备以下条件的供应商。

（1）符合《中华人民共和国政府采购法》规定。

（2）符合本项目采购公告中供应商应具备的资格条件，具有本项目生产、制造、供应或实施能力。

（3）符合、承认并承诺履行本招标文件各项规定。

3.2除联合体外，单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

3.3为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

**4、投标费用**

4.1本项目不收取招标代理服务费（中标服务费）。

4.2无论投标过程中的做法和结果如何，投标人自行承担所有与参加投标有关的全部费用。

**5、通知**

5.1参加投标的供应商有义务在采购活动期间浏览宁波政府采购网（www.nbzfcg.cn）和宁波公共资源交易网北仑区分网（beilun.bidding.gov.cn），采购人（采购代理机构）在以上两个网站发布的与本次招标项目有关的信息视为已送达各供应商，不再采用其它方式传达相关信息。

**B、招标文件说明**

**6、招标文件的构成**

6.1 招标文件由本文件目录所列内容组成。

**7、招标文件的澄清及修改**

7.1任何要求对招标文件进行澄清的潜在投标人，应在投标截止时间前以书面方式（包括信函、传真、电子文档等形式）通知采购人或采购代理机构。

7.2采购人或采购代理机构可主动地或依据投标人要求澄清的问题而修改招标文件，并以更正公告的方式在原公告发布网站通知所有获取招标文件的投标人。

7.3招标文件的修改内容将作为招标文件的一部分，对投标人有约束力。

**C、投标文件编制**

**8、要求**

8.1投标人应仔细阅读招标文件的所有内容，按招标文件要求格式认真细致地编制投标文件，以使其投标对招标文件作出实质性响应。未按要求提交全部资料或者投标文件没有对招标文件的要求做出实质性响应的，投标将被作为无效投标处理。

8.2投标人投标文件所提供的全部材料必须真实可靠，所述内容真实有效，不得弄虚作假。若投标文件填报的内容数据不详或提供了虚假数据或提供虚假材料的，其投标文件为无效投标文件，并按相关规定处理，由此引起的一切后果及法律责任由投标人承担。

**9、语言及计量单位**

9.1投标文件以及投标人与采购代理机构就有关投标的所有来往函电均应使用中文简体字。

9.2除在招标文件技术规格中另有规定外，计量单位使用中华人民共和国法定计量单位。

**10、投标文件组成**

10.1投标文件由资格证明文件、技术商务文件和报价文件三部分组成。

10.2资格证明文件

10.2.1资格证明文件用以证明投标人是否具备本项目的投标资格。

10.2.2投标人应按招标文件要求的内容和格式提供资格证明文件，具体详见本招标文件第六部分投标文件组成及格式。

10.2.3资格证明文件须逐页CA电子签章，否则资格审查不通过。

10.2.4资格证明文件中不得出现本项目的投标总价，否则投标无效。

10.3技术商务文件

10.3.1技术商务文件用于判断投标人提供的货物、服务是否满足招标需求，还用于包括不限于对投标人供货能力、实施能力、履约能力、项目经验等方面的评价。

10.3.2投标人应按招标文件要求的内容和格式提供技术商务文件，具体详见本招标文件第六部分投标文件组成及格式。

10.3.3技术商务文件中不得出现本项目的投标总价，否则投标无效。

10.4报价文件

10.4.1报价文件用于评价投标人的投标报价是否响应招标要求，是否符合相关的政府采购政策等。

10.4.2投标人应按招标文件要求的内容和格式提供报价文件，具体详见本招标文件第六部分投标文件组成及格式。

**11、投标文件制作**

11.1投标文件分为电子投标文件和备份电子投标文件。

11.2投标人应按照招标文件和政府采购云平台的要求编制、加密并上传电子投标文件。

11.3投标文件应根据招标要求做好关联定位，未进行关联定位而导致失分或无效投标处理的风险由投标人承担。

11.4投标人可自行选择是否提交备份电子投标文件，以便在上传的电子投标文件解密失败后启用备份投标文件。投标人仅提交备份电子投标文件的，投标响应无效。

**12、投标文件签署及密封**

12.1组成投标文件的各项资料均应遵守本条规定。

12.2投标人名称应填写全称，不能随意简称，要求加盖公章的应加盖公章（CA电子签章）。

12.3招标文件中规定的全权代表签名应由全权代表亲自签署，法定代表人可以签名或盖章。

12.4投标人选择提供备份电子投标文件的，备份文件应以U盘为载体并装袋密封，密封袋上需注明项目名称、项目编号、投标人名称并加盖公章。

**13、投标报价**

13.1投标报价是履行合同的最终价格，包含购买货物及服务需交纳的所有税费及其他一切相关费用，具体详见本招标文件第四部分项目内容及要求。

13.2投标人少报或漏报的工作量，采购人将视为已包含在投标总价中，并不予调整。

13.3所有投标均以人民币报价。投标人如需用外汇购入的设备，须折合人民币计入总报价中，总报价不受汇率变动影响。

13.4采购人不接受任何有选择的报价。

13.5超出采购人最高限价的投标为无效投标。

**14、投标有效期**

14.1本项目投标有效期见本招标文件前附表。投标文件应在投标有效期内保持有效，有效期短于这个规定期限的投标，将视为无效。

14.2特殊情况下，在原投标有效期期满之前，采购代理机构可征得投标人同意延长投标有效期，这种要求和答复都应以书面形式进行。投标人可以拒绝接受延期要求。同意延长有效期的投标人不能修改其投标文件。

**15、知识产权**

15.1供应商应保证在提供服务过程中或采购人在使用货物或货物的任何一部分时，不会侵犯任何第三方的知识产权，免受第三方提出侵犯其专利权、商标权或其它知识产权的起诉。

15.2投标报价应包括所有应支付的对专利权和版权、设计或其他知识产权而需要向其他方支付的版税等费用。

**D、投标文件提交**

**16、投标截止时间和投标地点**

16.1投标截止时间和投标地点见本项目采购公告和前附表。

16.2采购代理机构推迟投标截止时间或更改投标地点，将以更正公告的方式通知所有投标人。在这种情况下，采购人和投标人的权利和义务将受到新的截止时间和新的投标地点的约束。

**17、投标文件的提交、补充、修改和撤回**

17.1投标人必须在提交（上传）投标文件截止时间前，将加密的电子投标文件上传至政采云平台，逾期上传的投标无效。

17.2选择提交备份电子投标文件的投标人应在提交（上传）投标文件截止时间前，将密封的备份电子投标文件送达至开标现场，采购代理机构按要求进行签收登记。逾期送达或未按要求密封的备份电子投标文件采购代理机构拒绝接收。

17.3投标截止时间前，投标人可以对已上传的投标电子文件进行补充和修改。补充或者修改投标文件的，应先撤回原投标文件，再将补充、修改后的投标文件加密重新上传提交。投标截止时间前未完成上传的，视为投标文件撤回。不接受其他途径的补充和修改。

17.4投标截止时间前，投标人可以撤回已上传的电子投标文件。

17.5开标后，投标人不得撤回投标，否则报采购监督部门处理。

**E、开标和评标**

**18、开标**

18.1采购代理机构按招标文件规定的时间、地点进行开标。

18.2投标供应商法定代表人或其授权代表应准时通过政采云平台在线参加开标。

18.3投标供应商可以根据项目特点确定是否派代表出席现场开标会议，参加现场会议的供应商代表应遵守会场纪律。

18.4开标会议由采购代理机构主持，并按以下程序进行：

（1）主持人宣布开标会议开始及会场纪律，介绍到会人员。

（2）采购代理机构发出解密指令，投标供应商对加密电子投标文件进行在线解密。

（3）投标文件解密结束，开启投标文件，对“资格证明文件”进行审查。

（4）资格审查通过后，进行“技术商务文件”评审。

（5）公布技术商务评审情况，开启“报价文件”，投标人对投标报价进行在线确认。投标人对报价信息不予确认的不影响后续评标过程。

（6）对“报价文件”进行评审，计算价格分。

（7）汇总技术商务分、价格分，根据总得分排序推荐确定中标候选人，公布评审结果。

**注：如政采云平台对电子开标及评审程序有调整的，按调整后的程序操作。**

18.5开评标期间，投标供应商应关注政采云平台上的指令信息和手机短信并及时处理，否则由此产生的风险由投标人自行承担。

**19、投标文件解密**

19.1采购代理机构宣布开标后，将通过政采云平台发出解密指令，投标人登录政采云平台并使用CA数字证书对加密的电子投标文件进行在线解密。

19.2解密电子投标文件的时间为解密指令发出后30分钟内。解密成功的，备份电子投标文件自动失效。若在规定时间内无法解密或解密失败，此时启用备份电子投标文件（如有），若备份投标文件仍无法使用，则视为无效投标。

19.3电子投标文件在解密前处于保密状态。解密成功后，“资格证明文件”、“技术商务文件”、“报价文件”各自处于数据隔离状态，各部分信息只有在相关环节评审时可见，不受解密影响。

**20、评标委员会**

20.1采购人和采购代理机构根据采购项目的内容特点按照规定组建评标委员会。

**21、对投标文件的评审**

21.1开标后，采购人或者采购代理机构对投标人的资格进行审查。审查内容为投标人提供的资格证明文件是否齐全并满足招标文件的要求。

21.2评标委员会对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。

21.3评标委员会对具备实质性响应的投标文件进行评估和比较。

21.4评标委员会对投标文件的判定，只依据投标文件（包括样品、演示）的本身内容，不依据开标后的任何外来证明材料。

21.5评标办法及评分标准见本招标文件第七部分评标办法及评分标准。

**22、投标文件的澄清**

22.1对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会可以要求投标人作出必要的澄清、说明或者补正。

22.2评审期间，投标人应指派技术（商务）人员及法定代表人（或全权代表）在规定的时间内进行澄清和说明，否则将被视作自动放弃，由此造成的后果由投标人自行承担。

22.3对投标文件的澄清、说明或补正将通过政采云平台在线询标方式或线下书面形式进行。投标人的澄清、说明或补正须加盖公章（CA电子签章）或由法定代表人（或全权代表）签字。该澄清、说明或者补正将作为投标文件的一部分。

22.4投标人的澄清、说明或者补正不得超出投标文件的范围或者改变投标文件的实质性内容。不接受投标人提出的主动澄清。

**23、废标情形**

23.1 投标人不足3家未能开标的。

23.2经资格审查，合格投标人不足3家未能评标的。

23.3在评标过程中，评标委员会发现有下列情形之一的，应对采购项目予以废标：

（1）有效投标人不足3家的；

（2）出现影响采购公正的违法、违规行为的；

（3）因重大变故，采购任务取消的。

23.4废标后，采购代理机构通过公告的形式将废标结果通知所有投标人。

**24、采购方式变更**

24.1投标供应商不足3家或评审过程中有效投标供应商不足3家的，评标委员会应审查招标程序是否符合规定，供应商资格条件、采购需求和评审标准是否存在不合理条款，并出具审查意见和修改建议。

若存在不合理条款的，应按审查意见和建议修改招标文件后重新组织招标。

若没有不合理条款的，且参加投标供应商同意比照采用其他方式继续采购的，可以由采购人现场提出书面申请，经同级财政部门批准采取其他方式继续采购，否则按要求重新组织采购。

24.2比照竞争性谈判（磋商）方式继续采购的：

（1）招标项目的评标委员会转为竞争性谈判（磋商）的评审小组。

（2）评审小组确认原招标文件为竞争性谈判（磋商）文件。

（3）供应商的投标文件转为竞争性谈判（磋商）的首次响应文件。

（4）评审小组所有成员应当集中与单一供应商分别进行谈判（磋商），并给予所有参加谈判（磋商）的供应商平等的谈判（磋商）机会。

（5）谈判（磋商）结束后，评审小组应当要求所有继续参加谈判的供应商在规定时间内提交最终报价。

（6）竞争性谈判按照最低评标价法确定成交供应商，竞争性磋商按照综合评分法确定成交供应商。

24.3比照单一来源采购方式继续采购的：

（1）招标项目的评审委员会转为单一来源采购的评审小组。

（2）评审小组确认原招标文件为单一来源采购文件。

（3）供应商的投标文件转为单一来源采购的首次响应文件。

（4）评审小组与供应商协商确定合理的成交价格。

**25、评审监控及保密**

25.1本项目评标过程实行全程录音、录像监控，任何人在开标、评标过程中所进行的试图影响采购结果的任何不公正活动将受到监督，并承担相应的法律责任。

25.2凡是与本项目有关的审查、澄清、评审和比较的资料以及授予合同的建议，相关当事人均不得向投标人或其他无关的人员透露。

**26、中止电子交易的情形**

26.1采购过程中出现以下情形，导致电子交易平台无法正常运行，或者无法保证电子交易的公平、公正和安全时，采购代理机构可中止电子交易活动：

（1）电子交易平台发生故障而无法登录访问的；

（2）电子交易平台应用或数据库出现错误，不能进行正常操作的；

（3）电子交易平台发现严重安全漏洞，有潜在泄密危险的；

（4）病毒发作导致不能进行正常操作的；

（5）其他无法保证电子交易的公平、公正和安全的情况。

26.2出现上述情形的，采购代理机构可以待上述情形消除后继续组织电子交易活动，也可以决定某些环节以纸质形式进行；影响或可能影响采购公平、公正性的，应当重新采购。

**F、授予合同**

**27、授予合同标准**

27.1 采购人将依法把合同授予最佳投标者，具体方法见本招标文件第七部分评标办法及评分标准。

**28、中标通知**

28.1中标人确定之日起后2个工作日内，采购代理机构将在指定的政府采购信息发布媒体上公告中标结果，同时向中标人发出中标通知书。

28.2中标通知书对采购人和中标供应商具有同等法律效力。中标通知书发出以后，采购人改变中标结果或者中标供应商放弃中标，应当承担相应的法律责任，出现争议的，报财政部门处理。

28.3中标通知书是合同的组成部分。

**29、签订合同**

29.1中标人在收到中标通知书后，应按照规定的时间、地点，与采购人签订采购合同。

29.2招标文件、补充文件、投标文件及评标过程中的有关澄清、说明或者补正文件均为签订合同的依据。

29.3如果中标人不能按照招标文件要求及其投标文件的承诺签订合同或其投标文件与事实不符，影响采购合同的实施，损害采购人利益，采购人有权在签订合同前任何时候依照法定程序将合同取消，并宣布采购无效，对受影响的供应商不承担任何责任，也无义务给受影响的供应商解释采取这一行动的理由。

29.4自采购合同签订之日起2个工作日内，本项目政府采购合同将在财政部指定的媒体上公告，但政府采购合同中涉及国家秘密、商业秘密的内容除外。

29.5签约后即为招标结束。采购代理机构不退回任何文件资料。

**G、询问、质疑和投诉**

**30、询问**

30.1供应商对政府采购活动有疑问的，可以向采购人或采购代理机构提出询问。询问可以采用口头或书面方式提出，当采购人或采购代理机构要求采用书面形式时，应当采用书面形式。

30.2采购人或采购代理机构应当在3个工作日内对供应商依法提出的询问作出答复，但答复的内容不涉及商业秘密。

**31、质疑**

31.1供应商认为采购文件、采购过程、中标或成交结果使自己的合法权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、采购代理机构提出质疑。

供应商应知其权益受到损害之日，是指：

（1）对可以质疑的采购文件提出质疑的，为收到采购文件之日或者采购文件公告期限届满之日（公告期限届满后获取采购文件的，以公告期限届满之日为准）；

（2）对采购过程提出质疑的，为各采购程序环节结束之日；

（3）对中标或者成交结果提出质疑的，为中标或者成交结果公告期限届满之日。

供应商针对同一采购程序环节的质疑须一次性提出。

31.2质疑人应将质疑书原件送达被质疑人。质疑书应明确阐述采购文件、采购过程、中标或成交结果中使自己合法权益受到损害的实质性内容，提供相关事实、依据和证据及其来源或线索，便于有关单位调查、答复和处理。

31.3质疑书应当包括下列主要内容：

（1）供应商的名称、地址、邮编、联系人及联系电话；

（2）质疑项目的名称、编号；

（3）具体、明确的质疑事项和与质疑事项相关的请求；

（4）事实依据；

（5）必要的法律依据；

（6）提出质疑的日期。

31.4质疑书应当署名。供应商为自然人的，应当由本人签字；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或者盖章，并加盖公章。

31.5采购人、采购代理机构不得拒收质疑供应商在法定质疑期内发出的质疑函，应当在收到质疑函后7个工作日内作出答复，但答复的内容不涉及商业秘密。

**32、投诉**

32.1对采购人、采购代理机构的质疑答复不满意，或者采购人、采购代理机构未在规定期限内作出答复的，供应商可以在答复期满后15个工作日内向同级财政部门提起投诉。

**第四部分 项目内容及要求**

**1、采购内容**

项目名称：北仑区校园智能安全防控系统

项目编号：BLZFCG2020038

**2、项目范围**

详见本部分附件，供应商提供本项目采购范围内的货物和服务所需的一切费用均包含在报价中。

**3、项目说明**

3.1本招标文件所提出的项目技术标准是基本的技术标准和使用功能，并未规定所有的技术要求和适用标准，供应商应提供一套满足所列标准要求的高质量的产品及相应服务。

3.2本次招标项目应按国际标准或专业标准执行，最后按照国家有关规定及合同约定进行验收。

3.3本项目所有工作均由中标供应商负总责任。

3.4本项目要求使用的标准如与中标供应商所执行标准发生矛盾时，按较高标准执行。

3.5具体要求见本部分附件。

**4、▲交付地点与时间要求**

4.1本项目交付（实施）地点：北仑区，采购人指定地点。

4.2本项目交付（服务）期限：合同签订后3个月内完成，具体要求详见本部分附件。

4.3本项目质保期限：质保期为5年，质保期自项目正式验收合格之日起计算，具体要求详见本部分附件。

4.4本项目服务响应要求：在接到用户的故障维修电话后1小时内响应，简单故障能通过电话予以解决，如用户提出需要上门服务，维修人员应在4小时内赶到现场，并在12小时内解决问题。如在规定时间内不能解决问题，应提供同规格的替代设备给用户代用，直至设备故障修复，具体要求详见本部分附件。

**5、投标响应要求**

以下为投标人在投标文件中需要包含的最基本内容。若投标人提供的技术（服务）方案、设备（材料）性能参数与采购人要求不一致，必须在技术及服务条款偏离表中说明。

**5.1项目技术（服务）方案**

5.1.1项目技术方案包括项目需求分析、项目重难点及风险分析、设计方案等内容。

5.1.2项目需求分析。包括项目概述，系统描述，功能需求，性能需求，界面需求等内容。

5.1.3项目重难点及风险分析。包括项目建设目标及重难点分析，风险及控制方法等。

5.1.4设计方案。包括对总体框架、设计思路、采用的技术路线、系统功能设计、接口设计、开发平台、运行平台、维护工具等内容。

5.1.5货物技术性能。根据采购需求，详细列出符合要求的软件模块、设备配置情况及各项指标对应情况。参照第六部分格式：投标货物（服务）清单。

5.1.6品牌选择要求。为了便于维护，同类投标产品应尽量使用同一品牌。

5.1.7具体要求详见本部分附件。

**5.2项目实施方案**

5.2.1项目实施方案应包括总体实施方案、项目任务分解与控制、项目管理机构设置、实施团队人员配备、进度计划安排，系统测试和安装调试方案，主要测试设备清单等，内容应简洁实用。

5.2.2拟派本项目的主要实施人员未经采购人许可不得更换。

5.2.3具体要求详见本部分附件。

**5.3质量保证和服务承诺方案**

5.3.1包括服务质量保障措施、技术支持、服务响应及承诺等内容。

5.3.2质量标准的评定以国家或行业的质量检验评定标准为依据。因卖方原因产品质量达不到约定的质量标准，卖方承担违约责任。

5.3.3项目验收要求。项目安装、调试完成后，按约定进行试运行，试运行期满后，由采购人进行统一验收。

5.3.4在质保期内，须派专人定期或不定期参加日常维护工作；卖方须免费负责修理和替换任何由于产品自身的质量问题造成的损坏及故障。如果在短时内故障无法修复，则应提供同规格设备代用。卖方在质保期内的工作还应包括对货物的常规检查、调整。具体的操作程序和内容须在投标文件质量保证及服务承诺方案中说明。

5.3.5技术服务。供应商应对本项目提供长期有效的技术支持，投标文件中应提供技术服务和售后服务的内容及措施承诺，并列出售后服务机构设置情况，包括人员数量、人员技术资格情况、办公地址、联系方式及负责人等。

5.3.6具体要求详见本部分附件。

**5.4技术培训方案**

5.4.1包括负责培训的人员、培训内容、培训时间等内容。

5.4.2试运行开始时，供应商须对采购方的技术人员和操作人员进行培训，在试运行结束时完成全员培训。在质保期内，如采购人需要，供应商应免费提供技术指导和培训服务。

5.4.3具体要求详见本部分附件。

**5.5优惠承诺及合理化建议**

5.5.1提供针对本项目的具有可行性的合理化建议等内容。

5.5.2供应商可以根据项目实际情况和自己的实力及意愿在投标文件中作出优于招标要求的保证或承诺。

**6、付款方式**

（1）在收到第一笔款项前，中标供应商向采购人提交合同总价5%的履约保证金。

（2）中标供应商完成50%即52个学校后，向中标供应商支付合同总价的30%。

（3）试运行结束，项目验收合格，采购人（出资人）收到发票后15日内，向供应商付清剩余合同款。

（4）验收合格满四年后一周内采购人向供应商无息退还履约保证金。

**7、合同及履约**

7.1采购人和中标人应当自中标通知书发出之日起30 日内，根据招标文件和中标人的投标文件订立书面合同。中标人无正当理由拒签合同的，招标人取消其中标资格，并报采购监督部门处理，给招标人造成的损失的，中标人还应当予以赔偿。

7.2如果供应商提供的货物或服务与投标文件、相关澄清文件和合同等内容中承诺的不一致，则供应商必须接受无条件退货并赔偿采购人合同总金额100%的赔款。

7.3合同履行过程中，若发现投标人的投标文件中有投标价错误的，按不利于投标人的原则修正、调整相关价格，合同总价有变化的签订补充协议后作相应调整。

**附件：采购需求说明**

**附件：**

**采购需求说明**

**一、技术方案**

**第一章 项目概述**

**1.1.项目名称**

北仑区校园智能安全防控系统项目

**1.2.建设目标、规模、内容、建设工期**

**1.2.1.建设目标**

北仑区校园智能安全防控系统的建设目标是以校园安全数据为基础，构建统一的校园安全管理平台，通过大数据中心、前端安防设备系统、后台应用系统建设及安全保障体系等建设，利用大数据技术汇聚校园安全数据资源，实现校园安全隐患发现、整治、验收的全流程、可溯源闭环管理，实现业务管理的数字化、规范化、标准化、流程化。提升学校安全管理水平和应急处置能力，最大限度避免或减少安全事故发生，保障校园安全。

**1.2.2.建设规模**

本期项目覆盖北仑区9个街道104所中小学校及幼儿园，建设校园访客管理、人员通道管理、车辆出入管理等智能防控设施，接入校园重点部位监控，建设智能安全防控信息平台。具体建设规模及数量如下：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 校(园)名 | 所属镇(街道) | 学生教师数量 | 访客机 | 人脸道闸 | 车辆道闸 | 校园重点部位监控接入 |
| 通道数 | 抬杆数 | 大门 | 操场 | 厨房 |
| 1 | 宁波市北仑区白峰镇中心小学 | 白峰 | 859 |  | 2 | 1 | 1 | 9 | 9 |
| 2 | 宁波市北仑区白峰中学 | 白峰 | 380 | 1 | 1 | 1 | 1 | 19 | 12 |
| 3 | 宁波市北仑区三山学校 | 春晓 | 1090 | 1 | 2 | 3 | 2 | 8 | 14 |
| 4 | 宁波市北仑区泰河学校 | 春晓 | 2088 | 1 | 6 | 0 | 2 | 5 | 14 |
| 5 | 宁波滨海国际合作学校 | 春晓 | 1969 | 1 | 4 | 2 | 2 | 5 | 26 |
| 6 | 宁波市北仑区泰河中学 | 春晓 | 1480 | 1 | 2 | 2 | 2 | 4 | 20 |
| 7 | 北仑区春晓实验学校 | 春晓 | 1840 | 1 | 4 | 0 | 1 | 16 | 9 |
| 8 | 宁波市北仑区郭巨学校 | 郭巨 | 542 | 1 | 2 | 1 | 1 | 4 | 9 |
| 9 | 宁波市北仑区梅山学校 | 梅山 | 715 | 1 | 2 | 1 | 1 | 4 | 6 |
| 10 | 宁波市北仑区灵山书院 | 大碶 | 2031 | 1 | 4 | 0 | 2 | 5 | 13 |
| 11 | 宁波市北仑区大碶博平小学 | 大碶 | 1551 | 1 | 3 | 0 | 2 | 3 | 16 |
| 12 | 宁波市北仑区大碶小学 | 大碶 | 1591 | 1 | 3 | 1 | 2 | 7 | 8 |
| 13 | 宁波市北仑区实验小学 | 大碶 | 1285 | 1 | 3 | 1 | 2 | 4 | 6 |
| 14 | 宁波市北仑区大碶向阳小学 | 大碶 | 1343 | 1 | 2 | 1 | 1 | 6 |  |
| 15 | 宁波市北仑区大碶中学 | 大碶 | 1400 | 1 | 3 | 1 | 2 | 3 | 7 |
| 16 | 宁波北仑明港高级中学 | 大碶 | 2300 | 1 | 4 | 2 | 2 | 7 | 8 |
| 17 | 宁波市北仑区九峰小学 | 霞浦 | 1445 | 1 | 3 | 1 | 2 | 2 | 7 |
| 18 | 宁波市北仑区霞浦学校 | 霞浦 | 2314 |  | 4 | 1 | 2 | 12 | 11 |
| 19 | 宁波市北仑区柴桥小学 | 柴桥 | 991 | 1 | 2 | 1 | 1 | 4 | 8 |
| 20 | 宁波市北仑区柴桥实验小学 | 柴桥 | 1076 | 1 | 2 | 1 | 1 | 11 | 10 |
| 21 | 宁波市北仑区芦渎中学 | 柴桥 | 784 | 1 | 2 | 1 | 1 | 5 | 11 |
| 22 | 宁波市北仑区芦江书院 | 柴桥 | 176 | 1 | 1 | 0 | 1 | 4 | 8 |
| 23 | 宁波市北仑区柴桥中学 | 柴桥 | 1343 | 1 | 3 | 0 | 3 | 8 | 22 |
| 24 | 北仑区小港学达小学 | 小港 | 760 | 1 | 2 | 0 | 1 | 6 | 6 |
| 25 | 宁波市北仑区蔚斗小学 | 小港 | 1765 | 1 | 4 | 0 | 2 | 6 | 9 |
| 26 | 宁波市北仑区小港中心学校 | 小港 | 1873 |  | 5 | 0 | 2 | 8 | 12 |
| 27 | 宁波市北仑区小港实验学校 | 小港 | 1394 | 1 | 3 | 1 | 1 | 12 | 16 |
| 28 | 宁波市北仑区小浃江学校 | 小港 | 2300 | 1 | 1 | 0 | 1 | 3 | 25 |
| 29 | 宁波市北仑区江南中学 | 小港 | 1180 | 1 | 3 | 1 | 1 | 4 | 11 |
| 30 | 宁波联合实验中学 | 小港 | 1097 | 1 | 3 | 0 | 2 | 5 | 14 |
| 31 | 北仑职高 | 小港 | 3016 | 1 | 7 | 2 | 2 | 12 | 62 |
| 32 | 宁波市北仑区小浃江小学 | 小港 |  | 1 | 1 | 0 | 1 | 3 | 8 |
| 33 | 新棉校区 | 小港 | 495 | 1 | 1 | 0 | 1 | 3 | 5 |
| 34 | 宁波市北仑区淮河小学 | 新碶 | 1390 | 1 | 3 | 1 | 1 | 6 | 9 |
| 35 | 宁波市北仑区华山小学 | 新碶 | 1514 | 1 | 3 | 0 | 1 | 3 | 8 |
| 36 | 宁波市北仑区长江小学 | 新碶 | 1208 |  | 2 | 1 | 1 | 2 | 5 |
| 37 | 宁波市北仑区新碶小学 | 新碶 | 1574 | 1 | 3 | 1 | 2 | 3 | 9 |
| 38 | 宁波市北仑区绍成小学 | 新碶 | 2130 | 1 | 4 | 1 | 2 | 1 | 9 |
| 39 | 宁波市北仑区新碶东城小学 | 新碶 | 1252 | 1 | 3 | 0 | 1 | 6 | 4 |
| 40 | 宁波市北仑区庐山中学 | 新碶 | 1740 | 1 | 5 | 1 | 2 | 8 | 16 |
| 41 | 北仑区新碶中学 | 新碶 | 1480 |  | 2 | 0 | 2 | 8 | 9 |
| 42 | 宁波市北仑区岷山学校 | 新碶 | 2179 |  | 6 | 1 | 2 | 4 | 10 |
| 43 | 宁波市北仑区松花江中学 | 新碶 | 1264 | 1 | 3 | 1 | 1 | 3 | 8 |
| 44 | 宁波东海实验学校 | 新碶 | 2500 | 1 | 4 | 1 | 2 | 6 | 8 |
| 45 | 宁波市北仑区顾国和外国语学校 | 新碶 | 1080 | 1 | 2 | 2 |  |  |  |
| 46 | 宁波市北仑区长江中学 | 新碶 | 1387 |  | 3 | 1 | 2 | 24 | 9 |
| 47 | 宁波市北仑中学 | 新碶 | 1424 | 1 | 2 | 1 | 2 |  | 28 |
| 48 | 宁波市北仑区高塘学校 | 新碶 | 884 | 1 | 2 | 1 | 1 | 3 | 5 |
| 49 | 宁波市北仑区爱国学校 | 新碶 | 2960 | 1 | 6 | 2 |  |  |  |
| 50 | 高塘学校南校区 | 新碶 | 745 | 1 | 1 | 1 | 1 | 2 | 6 |
| 51 | 阳光学校 | 新碶 | 116 |  | 0 | 1 | 1 | 11 | 8 |
| 52 | 北仑区白峰幼儿园 | 白峰 | 212 | 1 | 1 | 1 | 1 | 3 | 5 |
| 53 | 北仑区白峰官庄幼儿园 | 白峰 | 211 | 1 | 1 | 1 | 1 | 8 | 5 |
| 54 | 上阳幼儿园 | 白峰 | 79 | 1 | 1 | 1 | 1 | 4 | 4 |
| 55 | 北仑区春晓幼儿园 | 春晓 | 440 | 1 | 1 | 1 | 1 | 6 | 11 |
| 56 | 北仑区春晓街道严玉德幼儿园 | 春晓 | 271 | 1 | 1 | 1 | 1 | 6 | 12 |
| 57 | 北仑春晓友飞幼儿园 | 春晓 | 210 | 1 | 1 | 0 | 1 | 7 | 6 |
| 58 | 宁波滨海国际幼儿园 | 春晓 | 260 | 1 | 1 | 1 | 1 | 3 | 8 |
| 59 | 昆亭幼儿园 | 春晓 | 95 | 1 | 1 | 0 | 1 | 4 | 7 |
| 60 | 北仑区郭巨幼儿园 | 郭巨 | 159 | 1 | 1 | 1 | 1 | 4 |  |
| 61 | 北仑区梅山幼儿园 | 梅山 | 319 | 1 | 1 | 0 | 1 | 9 | 9 |
| 62 | 北仑区大碶幼儿园 | 大碶 | 438 | 1 | 1 | 0 | 1 | 6 | 7 |
| 63 | 大碶街道幼儿园派舍提香分园 | 大碶 | 214 | 1 | 1 | 0 | 1 | 6 | 9 |
| 64 | 北仑区保税南区幼儿园 | 大碶 | 290 | 1 | 1 | 0 | 1 | 9 | 9 |
| 65 | 北仑区大碶街道惠琴幼儿园 | 大碶 | 427 | 1 | 2 | 0 | 1 | 9 | 9 |
| 66 | 大碶街道叶秋幼儿园 | 大碶 | 318 | 1 | 1 | 0 | 1 | 5 | 9 |
| 67 | 大碶街道育才幼儿园 | 大碶 | 125 | 1 | 1 | 0 | 1 | 3 | 6 |
| 68 | 大碶周翠玉幼儿园 | 大碶 | 120 | 1 | 1 | 0 | 1 | 3 | 6 |
| 69 | 北仑区九峰幼儿园 | 霞浦 | 273 | 1 | 1 | 0 | 1 | 3 | 7 |
| 70 | 霞浦街道黄鹂幼儿园 | 霞浦 | 302 | 1 | 1 | 0 | 1 | 2 | 7 |
| 71 | 霞浦街道陈华浦幼儿园 | 霞浦 | 195 | 1 | 1 | 0 | 1 | 5 | 7 |
| 72 | 霞浦中心幼儿园 | 霞浦 | 303 | 1 | 1 | 0 | 1 | 3 | 5 |
| 73 | 霞浦街道百灵幼儿园 | 霞浦 | 298 | 1 | 1 | 0 | 1 | 4 | 8 |
| 74 | 北仑区柴桥幼儿园 | 柴桥 | 244 | 1 | 1 | 0 | 1 | 2 | 4 |
| 75 | 柴桥街道中心幼儿园 | 柴桥 | 345 | 1 | 1 | 0 | 1 | 5 | 6 |
| 76 | 北仑区小港幼儿园 | 小港 | 419 | 1 | 1 | 0 | 1 | 10 | 6 |
| 77 | 小港长山幼儿园 | 小港 | 332 | 1 | 1 | 0 | 1 | 7 | 9 |
| 78 | 宁波市厚生幼儿园 | 小港 | 409 | 1 | 1 | 0 | 1 | 5 | 8 |
| 79 | 小港城区幼儿园 | 小港 | 371 | 1 | 1 | 0 | 1 | 2 | 6 |
| 80 | 小港江南幼儿园 | 小港 | 208 | 1 | 1 | 0 | 1 | 2 | 5 |
| 81 | 小港浃江幼儿园 | 小港 | 390 | 1 | 1 | 0 | 1 | 7 | 6 |
| 82 | 小港枫林幼儿园 | 小港 | 210 | 1 | 1 | 0 | 1 | 12 | 5 |
| 83 | 宁波经济技术开发区幼儿园 | 小港 | 617 | 1 | 0 | 0 | 1 | 11 | 13 |
| 84 | 宁波开发区幼儿园蔚斗分园 | 小港 | 200 | 1 | 1 | 0 | 1 | 7 | 8 |
| 85 | 北仑区戚家山中心幼儿园 | 小港 | 402 | 1 | 1 | 0 | 1 | 10 | 9 |
| 86 | 小港谢墅幼儿园 | 小港 | 227 | 1 | 1 | 0 | 1 | 8 | 4 |
| 87 | 下邵幼儿园 | 小港 | 208 | 1 | 1 | 0 | 1 | 5 | 6 |
| 88 | 北仑区中心幼儿园 | 新碶 | 616 | 1 | 1 | 1 | 1 | 8 | 11 |
| 89 | 北仑区中心幼儿园港务分园 | 新碶 | 203 | 1 | 1 | 0 | 1 | 5 | 11 |
| 90 | 北仑区实验幼儿园 | 新碶 | 882 | 1 | 1 | 0 | 2 | 3 | 9 |
| 91 | 北仑里仁童苑 | 新碶 | 342 | 1 | 1 | 0 | 1 | 11 | 6 |
| 92 | 北仑区新蕾幼儿园 | 新碶 | 410 | 1 | 1 | 0 | 1 | 4 | 7 |
| 93 | 北仑区新蕾四季幼儿园 | 新碶 | 439 | 1 | 1 | 0 | 1 | 7 | 7 |
| 94 | 北仑区新碶街道长来幼儿园 | 新碶 | 326 | 1 | 1 | 0 | 1 | 12 | 8 |
| 95 | 北仑区京华茗苑幼儿园 | 新碶 | 253 | 1 | 1 | 0 | 1 | 2 | 6 |
| 96 | 新碶世茂幼儿园 | 新碶 | 466 | 1 | 1 | 0 | 1 | 5 | 16 |
| 97 | 北仑区新碶街道辽河幼儿园  | 新碶 | 406 | 1 | 2 | 0 | 1 | 6 | 8 |
| 98 | 北仑区新蕾吉利幼儿园 | 新碶 | 203 | 1 | 1 | 0 | 1 | 7 | 6 |
| 99 | 北仑区新碶街道泰河幼儿园 | 新碶 | 543 | 1 | 2 | 0 | 1 | 5 | 6 |
| 100 | 新碶街道仙荷幼儿园 | 新碶 | 303 | 1 | 1 | 0 | 1 | 5 | 6 |
| 101 | 北仑区新碶街道岩河幼儿园 | 新碶 | 334 | 1 | 0 | 0 | 1 | 7 | 8 |
| 102 | 新碶街道松花江幼儿园 | 新碶 | 350 | 1 | 1 | 0 | 1 | 8 | 6 |
| 103 | 北仑区高塘幼儿园 | 新碶 | 326 | 1 | 2 | 1 | 1 | 7 | 8 |
| 104 | 小山幼儿园 | 新碶 | 250 | 1 | 1 | 0 | 1 | 5 | 8 |
| 合计 |  | 88093 | 96 | 203 | 52 | 129 | 619 | 961 |

**1.2.3.建设内容**

本次北仑区校园智能安全防控系统建设主要分为4大部分内容，具体为：

（一）校园智能安全防范信息平台建设

（1）校园安全风险防控大数据指挥中心

（2）安全防范信息平台

（3）校园体温实时监测管理系统

（二）前端校园安防系统建设

（1）访客登记查验信息管理系统

（2）人员通道管理系统

（3）车辆出入管理系统

（4）重点部位视频监控联网

（5）安防设备联网平台

（三）支撑平台及安全系统建设

（1）支撑平台

（2）网络安全系统

（3）运营商链路

（四）机房建设

**1.2.4.建设工期**

合同签订后3个月内完成。

**1.3.建设标准**

1)《浙江省人民政府办公厅关于加强中小学幼儿园安全风险防控体系建设的实施意见》(浙政办发[2018]110号)

2)《浙江省中小学幼儿园安全防范工作实施细则》(浙公通字[2015]85号)

3)宁波市教育局、宁波市委政法委、宁波市公安局《关于加强全市校园智能安全防控体系建设工作的通知》（甬教安体[2019]242号）

4)宁波市教育局《关于做好与宁波市校园智能安全防范信息平台数据对接工作的通知》甬教安体〔2020〕105号

5)《关于做好 2019 年“等级平安校园”评估工作的通知》（甬教安体〔2019〕301 号）

6)《公共安全视频监控联网系统信息传输、交换、控制技术要求》（GB/T 28181-2016）

7)《安全防范工程技术标准》（GB50348-2018）

8)《出入口控制系统工程设计规范》（GB50396-2007）

9)《视频安防监控系统工程设计规范》（GB50395-2007）

10)《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）

11)《计算机软件需求规格说明规范》（GB/T 9385-2008）

12)《信息技术开放系统互连网络层安全协议》（GB/T 17963）

13)《计算机软件开发规范》（GB8566-88）

14)《计算机软件可靠性和可维护性管理》（GB/T 14394-2008）

15)《政务信息资源交换体系》（GB/T 21062-2007）

16)《数据中心基础设施施工及验收规范》（GB50462-2015）

17)《综合布线系统工程验收规范》（GBT 50312-2016）

18)《建筑电气工程施工质量验收规范》（GB 50303-2015）

**1.4.系统功能和接口需求**

**1.4.1.功能需求**

1、访客登记查验信息管理系统的需求

全区中小学、幼儿园校园\*\*联络室需配置具有证件扫描、人脸识别、访单打印、短信提示（微信公众号）、回单注销及登记显示等功能的智能触摸访客机，安装访客登记查验管理平台软件，并通过县级教科网联入市、县两级公安机关校园智能防控平台，实现实时录入、实时比对、实时报警等功能，并预留接入市级校园智能安全防范信息平合接口。

2、校园主要出入口人车通行控制系统的需求

学校在主要出入口实行人车分离，在车辆通道安装车牌识别(抬杆)系统，对车辆出入实施智能控制。在人行通道安装人脸识别设施，对本校园人员实施智能识别通行。

3、校园重点部位视频监控联网的需求

结合“雪亮工程”建设(“雪亮工程”，即公共安全视频监控建设联网应用。根据“十三五”规划，到2020年，我国将基本实现“全域覆盖、全网共享、全时可用、全程可控”的公共安全视频监控建设联网应用)，将校园内重点部位或人员通行频繁区域的视频监控系统、紧急报警装置接入公安机关、教育部门平台，并与公共安全视频监控共享平台联网对接，建立校园安全网上巡查机制，及时掌握、快速处理学校相关安全问题。

4、校园智能安全防范信息平台的需求

平台需包括校园安全风险防控日常管理、校园安全风险防控专项应用、防控数据决策应用等功能。

校园安全风险防控日常管理包括安全管理系统、资源管理系统、安全检查系统、安全隐患治理、安全台账系统；校园安全风险防控专项应用包括校园智安系统、视频监控联网系统、交通及校车安全管理、防溺水安全管理系统、校园欺凌防范系统、安全应急处置系统、值班上报系统；针对性解决校园安全中涉及到的人的不安全因素、物的不安全状态、事务管理的缺陷。

防控数据决策应用主要包括总体态势大数据、在线督导评估系统、风险预警系统，通过该应用可实现区域校园全局安全工作动态化、数据化管理，通过采集预警数据、日常防范隐患排查治理数据、重点防范专项检查数据等汇聚成全方位校园安全风险画像，为安全管理决策提供依据。

**1.4.2.接口需求**

1、与区视频共享平台、区公安分局公共安全视频监控联网平台的接口

区教育局安防设备联网平台与区视频共享平台、区公安分局公共安全视频监控联网平台的对接接口应符合《安全防范视频监控联网系统信息传输、交换、控制技术要求》（GB/T 28181-2016）及《公安视频图像信息应用系统第4部分：接口协议要求》（GA/T1400.4－2017）的标准。

2、同级平台的对接接口

区教育局安防设备联网平台与本级的智能安全防范信息平台之间的对接，平台之间接口开放，并实现数据推送。

3、与上级平台的接口

提供符合相关标准的规范接口，统一满足外部的数据调取。支持与宁波市校园智能安全防范信息平台的数据对接，满足上下级之间实时推送安全基础数据、安全业务数据。参照甬教安体【2020】105号 关于做好与宁波市校园智能安全防范信息平台数据对接工作的通知。

4、与第三方平台的接口

支持与第三方平台（浙政钉、微信）的对接，开放系统接口，具备与第三方平台对接能力，实现实时安全基础数据、安全业务数据（包括PC端、移动端）的发送与接收。

**第二章 项目建设要求**

**2.1.总体要求**

项目通过对北仑区各中小学校、幼儿园校园智能安防系统的建设，获取访客、人员、车辆的实时数据，进行分类管控。通过安全防范信息平台，以校园安全基础数据为基础，将教育局现有校园安全管理业务进行梳理，建立统一的校园安全管理平台，并在其之上逐渐分模块实现各个应用。通过工作任务驱动的方式，对业务流程进行配置，实现业务管理的数字化、规范化、标准化、流程化。推进信息技术在校园日常安全检查和隐患排查整治工作中的应用。

北仑区校园安全防控系统应具有良好的开放性及兼容性，具备开放的事件接口，支持将相关的门禁事件、车辆抓拍事件、访客事件、视频流以及学校基础安全数据推送给市级安全平台。

**2.2.平台部署方案**

采用服务器（虚拟化）+SAN存储、网络传输、信息安全、数据库、虚拟化操作系统等软硬件组成，依托教育城域网部署。采用虚拟化技术，使平台的多种应用共享服务器、存储等硬件资源，可以帮助用户提供IT基础设施资源的利用效率，提升基础设施的应用和管理水平，实现计算资源的动态优化，使平台应用易维护、易扩充。

**2.3.系统拓扑结构**

本次北仑区校园智能安全防控系统拓扑结构如下图：



**2.4.数据标准规范**

本项目的基础数据包括视频监控数据、人脸数据、车辆数据、访客数据、学校基础安全数据以及等级平安校园管理数据。基础数据制定包括有关标准与规范，本项目数据标准遵循《宁波市校园智能安全防范信息平台数据接入管理办法（试行稿）》要求，按照数据接口及标准协议制定平台代码标准、字段标准、业务模型标准。为数据治理策略、数据质量管理提供唯一的数据格式依据。

数据来源：

（1）学校基础安全数据

学校基础安全数据主要包括：学校基础信息、学生数据（特异体质、心理测评预警）、教职工数据（安全干部、心理健康教师、卫技人员、医疗救护员）、“人防、技防、物防”建设等数据，学校基础安全数据的来源是各学校，通过录入或导入区级教育安全平台汇集后将数据接入至市级平台。

（2）校园四大系统数据

校园四大系统数据有访客登记查验信息管理数据、校园出入口智能抓拍预警数据、车辆进出数据、人员进出数据和校园重点部位视频监控，其中访客、车辆、人员、重点部位监控数据来源于本次项目建设的前端安防设备，通过安防设备联网平台汇聚后上传信息平台；校园出入口智能抓拍预警数据通过区公安分局视频专网接入。

**本项目数据接入规范标准：**

|  |  |  |  |
| --- | --- | --- | --- |
| 规范部分 | 接入类型 | 接入数据 | 备注 |
| 学校基础安全数据接入规范部分 | 学校基础信息 | \*学校编码，\*所属区域编码，\*学校办别，\*学校类别，\*学校地址，\*校长，\*学校电话，\*负责人电话，\*平台校园等级，\*评定时间，学校创办时间，学校 logo，建筑面积，\*教职工人数，\*学生人数，教学楼数量，图书馆数量，校大门数量，保安室数量，实验楼数量，\*是否有境外少数民族学生，\*是否有宿舍楼，\*是否有食堂，\*是否有校车，\*是否有卫生室，\*是否有心理咨询室，\*是否有在建工程，\*是否接入访客登记系统，\*是否建设智能抓拍报警系统，\*是否接入人员通行系统 |  |
| 学生特异体质 | \*姓名，\*性别，\*班级，\*出生日期，\*特异体质情况，\*目前情况，确诊时间，发病情况，\*班主任，\*班主任电话，\*家长姓名，\*家长电话，家庭住址，家长要求，学校要求，备注，\*是否履行告知义务情况 |
| 学生心理测评预警 | \*预警等级，\*学生编号，\*学生班级，测评名称，预警因子，测评报告，\*要求建档，\*测评时间，\*学生年级，\*学生性别 |
| 安全干部 | \*姓名，\*电话，\*单位职务，\*管理内容，备注 |
| 心理健康教师 | \*姓名，\*性别，\*持证类型，证件编号，证件照片，发证机关，发证日期 |
| 卫技人员 | \*姓名，\*电话，性别，出生日期，毕业学校及专业，单位职务，\*医师或护士执业证书号码， 医师或护士执业证书范围，\*医师或护士执业证 书照片，医师或护士执业证书注册日期，备注 |
| 医疗救护员 | \*姓名，\*性别，\*持证类型，证件编号，证件照片，发证机关，发证日期 |
| 保安信息 | \*姓名，\*联系电话，\*专兼职，\*身份证号，\*保安证号，\*聘用日期，年龄，保安证图片，培训 日期，培训级别，培训课时，培训内容，家庭 地址，保安公司 |
| 系统接入规范部分 | 访客登记查验信息管理数据 | \*登记方式，\*姓名，\*证件号，性别，住址，证件图，现场图，访问事由，来访，人数，车牌 号，\*进入时间，离开时间 |
| 校园出入口智能抓拍预警数据 | \*预警类型，预警图片，预警视频，\*预警位置 |
| 车辆进出数据 | \*方向，\*车牌号，\*进入时间，离开时间 |
| 人员出入数据 | \*用户编号，\*用户姓名，\*进出类型，抓拍图片 |
| 校园重点部位视频监控 | \*要求重点部位视频接入 5 路以上，包括：校门口及人员通行的主要出入口、财务室、实验室（危化品室）、实训室、配电机房、食堂、餐 厅、宿舍、体育场所、图书馆等学校重点区域。按照国标 GBT 28181-2016 标准接入。 |

**2.5.校园安全风险防控大数据指挥中心**

校园安全风险防控大数据指挥中心由总体态势大数据、重点环节大数据、风险预警大数据、在线督导大数据四大部分组成，大数据中心基于“自上而下关键指标为抓手、自下而上动态数据为监督、以5A等级评定为成效”的总体目标，可实现区域校园全局安全工作动态化、实时化管理。

**2.5.1.总体态势大数据**

通过总体态势大数据可统览下属各级各类学校校园安全日常防控管理大数据、等级平安校园在线化实时化评估。可实现对下属学校校园安全数据的采集、统计、分析、决策；实现对校园安全事前、事发、事中、事后管理中的规范化情况和安全成效情况清晰展示。

**2.5.2.重点环节大数据**

重点专项分为持续性重点专项和阶段性重点专项，如下二类管理重点：重点专项如智安数据建设、食品安全专项、防溺水专项、防欺凌专项、交通及校车专项、传染病防治、应急处置等规范性工作和执行情况工作监管；阶段专项如极端天气、维稳时段的值班安排、值班上报管理，突发事件的应急指挥，四个建设点、在线工程的合规性和进度管理。

**2.5.2.1.智安系统专项**

平台可通过统一化数据接口实现校园智能安全防范信息平台数据向上汇聚；通过接口开放对接服务应当与访客登记查验信息管理系统、重点部位视频监控联网系统、校园出入口智能抓拍报警系统、出入口人车通行管理系统等系统进行对接，实现全方位一体化的校园智能安全防范信息平台。

通过校园智安系统大数据可以对下属各级各类学校实现对访客管理系统建设、重点部位监控系统建设、可疑人员智能抓拍报警系统建设、以及人车通行系统建设情况汇总展示，还可以通过可视化地图点击实现对下属各级各类学校建设情况逐级查看。

1）学校访客管理模块可汇总显示下属学校访客管理系统建设完成情况、本周访客登记查验情况，同时可自动汇聚提醒消息，包括有未接入学校数量和本周访客查验可疑人员数量，点击提醒消息可查看、导出明细。

2）重点部位监控模块可汇总显示下属学校接入数量、下属学校重点部位监控接入建设数量，同时可自动汇聚提醒消息，包括有未接入学校数量和重点部位监控接入缺失学校，点击提醒消息可查看、导出明细。

3）可疑人员智能抓拍报警模块可汇总显示下属学校智能抓拍报警系统建设完成情况、本周可疑人员智能抓拍情况，同时可自动汇聚提醒消息，包括有未接入学校数量和本周可疑人员抓拍数量，点击提醒消息可查看、导出明细。

4）人车通行模块可汇总显示下属学校人车通行系统建设完成情况、本周车辆进出情况、本周人员进出情况，同时可自动汇聚未接入学校提醒消息，点击提醒消息可查看、导出明细。

**2.5.2.2.食品安全专项**

局端食品安全专项重点进行食堂规范化管理、从业人员规范化管理、食材供应规范化管理、食品品质管理（包括有食材验收、餐具消毒、操作人员规范和食品留样）、陪餐制度执行管理、学校开放日执行管理等。

通过食品安全专项大数据可以对下属各级各类学校食堂规范管理、从业人员规范管理、供应商规范管理、食品品质规范管理情况汇总展示，还可以通过可视化地图点击实现对下属各级各类学校建设情况逐级查看。

1）学校食堂规范管理模块可汇总显示下属学校食堂总数、建设阳光厨房的食堂总数、食堂A/B/C级总数、以及食品经营许可正常情况，同时可自动汇聚食品经营许可证过期、C级或未定级食堂提醒消息，点击提醒消息可查看、导出明细。

2）从业人员规范管理可汇总显示下属学校食堂从业人员总数、从业人员档案规范情况，同时可自动汇聚从业人员健康许可证过期提醒消息，点击提醒消息可查看、导出明细。

3）供应商规范管理可汇总显示下属学校食堂各类食材供应商总数和占比，同时可自动汇聚供应商食品经营许可证过期、供应食材检验有不合格情况的供应商提醒消息，点击提醒消息可查看、导出明细。

4）食品品质规范管理可汇总显示下属学校食材购买验收、餐具消毒、操作人员规范、食品留样、陪餐制度执行管理、学校开放日执行管理情况，同时可自动汇聚未进行食品留样、未进行陪餐或未执行开放日的提醒消息，点击提醒消息可查看、导出明细。

**2.5.2.3.防溺水专项**

通过学生防溺水大数据可以对下属各级各类学校校园学校防溺水八个一的执行情况、一封信回收率100%、防溺水学习平台完成率100%、水域警示巡检情况、区域内防溺水预警汇总展示，还可以通过可视化地图点击实现对下属各级各类学校建设情况逐级查看。

**2.5.2.4.防欺凌专项**

通过防欺凌专项大数据可以对下属各级各类学校校园学校防欺凌规范管理、学生行为规范管理、学生欺凌心理测评预警管理、重点问题学生档案管理和欺凌事件处置情况汇总展示，还可以通过可视化地图点击实现对下属各级各类学校建设情况逐级查看。

1）学校防欺凌规范管理可汇总显示下属学校欺凌防治委员会和反欺凌电话公示情况，同时可自动汇聚未按学校规范管理如未公示反欺凌电话的提醒消息，点击提醒消息可查看、导出明细。

2）学生行为规范管理可汇总显示下属学校学生出勤台帐、校门进出登记台帐、住宿生就寝查铺台帐、违禁刀具管理台帐、学生思想状况分析报告台帐、校园值班巡查台帐执行情况，同时可自动汇聚未按学校学生行为规范管理要求执行学校提醒消息，点击提醒消息可查看、导出明细。

3）学生欺凌心理测评预警管理可汇总显示下属学校学期欺凌心理测评一、二、三级预警情况，同时可自动汇聚学校学生级别学生的提醒消息，点击提醒消息可查看、导出明细。

4）重点问题学生档案管理可汇总显示下属各级各类学校/学校问题学生人数及档案完备情况，同时可自动汇聚未按要求管控的问题学生的提醒消息，点击提醒消息可查看、导出明细。

5）欺凌事件处置可汇总显示下属学校按一般欺凌、严重欺凌、涉嫌犯罪欺凌情况，以及下属各级各类学校/学校本学期上报事件和处理事件情况，同时可自动汇聚未处置事情的提醒消息，点击提醒消息可查看、导出明细。

**2.5.2.5.交通及校车专项**

通过交通及校车专项大数据可以对下属各级各类学校校园校车规范管理、司机规范管理、校车运行管理、月度学校交通巡检、交通及校车类风险预警信息情况汇总展示，还可以通过可视化地图点击实现对下属各级各类学校建设情况逐级查看。

**2.5.2.6.传染病防治专项**

按照教育系统落实学校防控责任，开展“晨午晚检”，实行“日报告”、“零报告”制度的要求。学校利用系统对到校学生、教职工进行出勤情况、体温情况按照晨检、午检、晚检要求进行上报管理，并对因病缺勤学生和教职员工实时及时追访和信息上报；局端可实时查看上报统计数据、到校体温异常人员及应急处理措施，并可依据上报问题进行监督与指导；学校端上报系统可兼容智能测温柱、智能蓝牙温枪数据自动上报等，可高效提高人工效率。从而保障科学有效防控、安全有序开学。

**2.5.2.7.应急处置**

通过局端应急处置专项大数据可以实现对下属学校应急预案完备情况、应急演练培训情况、突发事件管理情况汇总展示，还可以通过可视化地图点击实现对下属各级各类学校情况逐级查看。

应急预案管理可汇总显示下属学校应急预案完备情况，同时可自动汇聚未按类型、按要求完备应急预案学校的提醒消息，点击提醒消息可查看、导出明细。

应急演练管理，同时可自动汇聚未按时间要求执行应急预案演练学校的提醒消息，点击提醒消息可查看、导出明细。

突发事件管理可汇总显示下属学校突发事件上报情况和趋势，同时可自动汇聚本周突发事件发生学校的提醒消息，点击提醒消息可查看、导出明细。其中可展示非零损失安全事故学校情况。

突发事件处置，提供量化应急能力评估方式，按照时间轴汇总区域学校应急能力大数据。如本月应急演练较上月变化率、本月突发事件、零损失平稳处置事件较上月变化情况来反应处置能力。

**2.5.2.8.应急值班**

通过局端应急值班专项大数据可实时、动态、直观地查看下属学校的当日学校值班巡检情况。包括具体学校实时上报学校、上报状态和上报时间；可实时查看直属学校上报完成率和异常处理情况，以及各区域上报完成率；针对异常问题，可以查看异常上报内容，并进行处理；可生成汇总的值班报告供下载查看。

学校端可以以移动客户端进行值班上报，可以采用地图巡检轨迹、巡检拍照、以及巡检记录文字等方式记录应急巡查结果的方式上报。

**2.5.3.在线督导大数据**

可在线工作督导，在线下发安全文件、下发安全任务、统计安全干部、发起专项检查工作，并对以上任务执行情况实时可查。

在线督导大数据主要满足教育机构对安全任务文件管理、春季秋季专项检查、等级平安校园评估、安全干部管理。

1）安全干部管理模块可对管辖区域安全干部信息进行实时化、全面化管理。

2）安全任务文件管理模块一方面可管理上级/本级的安全文件，另一方面可将需要进行任务反馈的工作任务通知通过安全任务、安全文件发布给下辖机构，下辖机构可以根据任务性质进行执行、转发、反馈等操作，上级可实时查看下辖机构的反馈状态，并对收到反馈工作报告后可进行在线评价，同时实时展示未反馈单位，有效督促任务实施，提升实施效率。

3）春季秋季专项检查模块可用于春秋季开学安全大数据，其中检查内容可在线标准化制订，包括检查项、检查标准及扣分点，保证下辖机构可依据统一的标准全面开展检查工作，检查出的问题可自动生成逐校整改通知书、帮助针对性改进，同时自动生成区域共性问题报告，为下步整改要求和工作重点提供分析依据，提高工作效率、改善问题解决闭环。

**2.5.4.风险预警大数据**

通过风险预警可对校园中的人、物、事等高风险事件自动预警，便于上级部门组织应急处置；同时可自动生成区域风险预警信息，可由上级审核后发布，用于下属单位事前预防与实时督导。

风险预警的主要功能包括：

可通过可视化系统查看下属单位高风险事件预警，其中风险类型包括：人（外来访客黑名单、师生考勤低到校率等），物（重大隐患、超期隐患等），事（安全任务超期反馈、三防巡检未执行等），技（可疑人员抓拍报警、一键报警等）。

可以通过风险大数据自动统计生成风险预警排行，通过风险预警排行信息点击进入可查看到各预警详细内容，有：防溺水预警、学生非正常死亡预警、交通事故、食品与卫生风险预警、校园欺凌预警、校园周边风险预警和消防隐患预警。

**2.6.校园智能安全防范信息平台建设**

北仑区校园智能安全防范信息平台业务应用主要由校园安全风险防控大数据指挥中心、首页门户系统、数据直通系统、智安动态系统、安全教育系统、日常防范系统、重点防范系统、应急处置系统、智安物联系统以及基础支撑系统组成，各个子系统通过统一用户中心和统一认证系统进行业务关联为教育管理机构用户、学校用户以及家庭用户提供不同的业务和功能。用户可以通过手机、平板、电脑、多媒体教学机等多种途径、多种方式对平台提供业务进行操作与访问。

**2.6.1.基础支撑系统**

分级管理：以管理者、老师和家长为应用对象，不同的角色登录后展现不同的风格。通过集成用户中心系统、资源应用系统等为学校、管理部门提供个性的资源。

统一认证：系统负责对平台用户提供统一认证服务。系统功能包括系统配置、授权管理、修改密码、注销用户等。为学校管理者提供安全管理手机客户端软件。

用户中心：系统负责校园内教师及家长信息的管理。系统功能包括学校信息管理、教师信息管理、系统用户管理等。

**2.6.2.首页门户系统**

教育主管部门用户登录管理系统后，首页将展示出跟用户工作相关的最新信息，主要包括：安全数据、智安动态、突发事件预警、最新通知消息、安全文件（任务）的待办工作、隐患排查和巡更打卡，以及进去工作处理的快捷入口。用户登录后根据所属区域和角色自动跳转到教体局门户或学校门户，并可以处理个人相关工作和内容。

具体说明如下：

数据概况：提供展示管辖范围内教育机构和学校安全数据，包括学校数、教职工数、学生数、校车、监控数、保安数等宏观数据。

智安动态：展示上级或者本单位发布的安全新闻。

事件预警：展示下属学校预警的高风险事件，可进行点击安排相关负责人督办处理。

最新通知：展示接收到的上级或者本单位发布的最新通知信息，用户可以点击查看详细内容。

待办任务：展示当前用户需要做的工作，主要包括：安全文件（任务），并可以查看下属学校的整体完成情况和详细情况。

隐患排查：展示下属学校日常巡检完成率、隐患总数、隐患整治情况。

快捷入口：提供快捷操作入口，点击快捷入口后会直接进入对应的操作页面。方便用户一键到达。

**2.6.3.数据直通系统**

按照宁波校园安全风险防控体系框架要求，局端安全管理统一按照《关于做好与宁波市校园智能安全防范信息平台数据对接工作的通知（甬教安体〔2020〕105 号）》文件要求数据标准规范进行基础安全数据管理。

平台提供标准化接口汇聚各类安全子系统和报表子系统数据（包括学校基础信息、安全干部、学生特异体质、学生心理测评预警、心理健康教师、卫技人员、医疗救护员、保安信息等），生成大数据图表、报告等多种统计结果。个性化多维度安全数据统计表下发、填报和采集汇总，同时按月自动生成图表式安全台帐。上级教育部门可通过以上重点结果管控辅助达成对下属学校的安全监管工作。

（1）基础数据。数据上报要求见“数据标准规范”。

（2）校园安全评估大数据。学校是安全大数据的数据来源，通过管理学校进行学校基础信息填报、各项安全工作信息填报、在线化隐患巡检、在线化安全任务完成反馈等工作的完成，局端将自动进行数据向上汇聚、依据国标省标市标进行数据分析、数据统计，形成安全闭环管理。

**2.6.4.智安动态系统**

通过平台可以将安全信息、安全新闻、安全动态、安全知识等推送到用户终端，下属学校、教育局安全负责人可通过移动客户端实时接收、即时消息预警，让用户能够随时随地了解安全、学习安全技能、了解安全动态、增加安全防范意识与紧急自救能力。

**2.6.5.安全教育系统**

**2.6.5.1.安全教育平台**

通过标准化数据接口可链接至宁波市安全教育平台。

**2.6.5.2.安全教育资源**

系统管理：提供包括系统参数配置、资源服务器、存储路径配置等。

资源管理：提供包括资源仓库、资源分类、存储目录、资源信息等管理，以及校本安全教育资源存储库。

资源服务：提供资源服务调度，资源访问负载等功能。

资源分发：提供多资源服务器部署时，资源同步策略定义与资源同步分发功能。

安全教育课程体系：是依据《中小学公共安全教育指导纲要》、《中小学信息健康教育指导纲要》指导建设。主要包括预防和应对社会安全、公共卫生、意外伤害、网络信息安全、心理健康、自然灾害以及影响学生安全的其他事故或事件等模块。涵盖有幼儿园、中小学同步课程体系及专题资源体系。课程资源丰富多样，包含课件、动画、视频、教案等多种形式满足师生多样化学习需求；安全专题资源满足老师高效便捷备授课，多样化视频动画资源让学生秒懂安全知识。

**2.6.5.3.安全教育计划**

教育计划学校可在平台填写安全教育计划，主要包括教育内容、教育对象、教育方式、教育对象、使用教材等信息。上级教育机构可以查看管辖范围内学校的安全教育计划。并对比学校填写教育实施情况进行对比。对学校安全教育进行统一规范与监督。教育实施学校可以通过平台填写具体实施的安全教育情况，可以从计划直接实施，或者直接添加教育实施信息。具体实施时需要填写安全教育的具体时间、地点、参与人数、使用教材、授课方式、授课教师等信息。

**2.6.5.4.法制授课管理**

下级上报：可通过在线预览、下载方式查看下级上报的文件和管理上报的安全教育工作展示文件；可对上报文件内容进行在线评价。

我要上报：可向上级教育局上报文件；点击“上传文件”，选择想要上报的教育局，选择附件后，点击保存，即可成功上传；选择文件，点击“编辑文件”后，可修改文件；选择一个安全文件之后点击“删除”并确定即可删除上报的该文件。

**2.6.6.日常防范**

**2.6.6.1.通知消息**

公共信息发布：公共信息是基于公共服务账号的信息发送功能。安全部门、教育机构、学校管理用户可以通过平台在手机端、PC端发布通知公告、安全提醒、其他消息给目标用户。

点对点交流：点对点交流，包含教育机构用户、学校用户、家庭用户之间的点对点沟通和交流。在学校课外，老师也可以通过平台组织具体学生的心理辅导，老师可以和家长进行具体学生的情况分析和交流，老师间的信息互动有无等。

**2.6.6.2.安全文件（任务）**

教育局用户进入安全文件下发，点击文件管理，管理发布的本单位文件。点击上传按钮，选择接收单位，选择要通知的学校人员，上传本地文件，保存后即可发布成功。选中安全文件，可以进行修改和删除操作；点击选择职务，如选择职务则给所选机构或学校的职务发送文件，如不选择职务则所选机构或学校的所有职务人员均可见此文件。选中安全文件，点击“查看情况”查看文件被下级和学校查看的情况。

教育机构可以针对下属教育机构或者学校进行工作任务布置，工作任务发布时会以即时消息方式通知指定人群。并可以按照任务查看各个单位的任务执行和反馈情况。工作处理接收到任务的单位可以对任务进行反馈处理，反馈是按照需求可以上传附件、填写任务执行情况等。工作完成情况查看任务发布单位可以查看各个单位的执行完成情况和反馈信息。可以方便的查看已反馈单位和未反馈单位列表。以及查看任务完成情况与反馈内容。处理结果评分任务发布单位可以对已反馈单位的具体执行情况进行点评、批注与打分。评分结果任务执行单位可以在任务列表中进行查看。

**2.6.6.3.专项检查**

教育机构或者安全部门对下属学校进行专项检查评分的信息化实现（可根据权限设置检查内容）。

实现对检查单位的各类检查项目评分，以及发现问题的汇总。检查内容自定义、评分标准自定义，支持上级督查、学校自查、部门联查多种检查方式。检查过程中的多人协作检查方式，发现问题以拍照、录像、录音等方式记录与上报。检查结果统计与分析查看，包括：各个被检查单位的分数、问题报告查看，整体合格率分析，问题报告导出。

**2.6.6.4.隐患排查**

隐患发现：学校用户可以通过手机客户端方式或者管理系统进行隐患情况上报，并可以对本人上报的隐患信息进行管理。

隐患查看用户可以查看本单位其他人员上报的安全隐患信息和处理结果。教育机构或者安全部门用户可以按照学校查看管辖范围内所有安全隐患信息和具体处理情况，也可以看到下级上报上来的隐患项目。隐患处理学校管理人员接收到隐患信息后可以对隐患信息进行指派人员处理、上报上级处理等。指派处理人员时系统自动给被指派处理人员发送即时消息通知，用户点击后可以查看隐患具体信息并给予处理。

安全巡检：支持通过手机扫描二维码直接对安全关键点进行安全排查，并上报排查结果。主要包括校车安全巡查、消防设施安全巡查、应急通道巡查、食品安全巡查、交通安全巡查、校舍安全巡查、电器安全巡查等。

网格化管理：北仑区校园安全风险防控平台采用网格化管理模式，北仑区教育局平台实行三级架构：北仑区教育局领导—各组网格员—各学校，网格员直接负责对应学校的专项检查/在线督察以及日常巡检和隐患整改数据的检查并审核工作，初步审核后将数据反馈给（北仑区教育局领导）再进行最终审核。

**2.6.7.重点防范**

**2.6.7.1.交通及校车管理**

上级教育部门对交通及校车安全管理可重点放在学校每日校车运行管理、每月校内交通状况巡检自查情况和异常问题，通过以上重点结果管控辅助达成对下属学校此项安全工作监管。

**2.6.7.2.学生防溺水管理**

上级教育部门对学生防溺水安全管理重点放在学校防溺八个一完成记录，通过以上重点结果管控辅助达成对下属学校此项安全工作监管。

**2.6.7.3.学生防欺凌管理**

上级教育部门对学生防欺凌安全管理重点放在下属学校上报的欺凌事件、处置过程、处置结果，通过以上重点结果管控辅助达成对下属学校此项安全工作监管。

**2.6.7.4.外出活动管理**

上级教育部门对学生外出活动安全管理重点放在下属学校学校上报的外出活动，可在线审核办公，通过以上重点结果管控辅助达成对下属学校此项安全工作监管。

**2.6.7.5.传染病防治管理**

按照教育系统落实学校疫情防控责任、开展“晨午晚检”工作要求，学校可使用系统对到校学生、教职工进行出勤情况、体温情况按照晨检、午检、晚检要求进行上报管理，并对因病缺勤学生、未到岗教职工信息上报，同时支持学校智能测温柱、智能测温枪数据自动上报等。

局端可通过平台管理端“晨午检统计”功能可以进行统计、明细情况导出：（1）教师晨午检：可按区域、日期时段、体温、身份等导出上报和未上报明细；（2）学生晨午检上报统计：点击“上报统计”可查看所辖各学校晨午检的上报率、出勤率、考勤整体统计。（3）学生晨午检明细：点击“明细统计”可查看、导出所辖学校具体学生晨午检统计详情。

局端可通过“晨午检统计”模块查看各机构学生和教职工等人员的晨午检上报情况：（1）可以查看整体上报出勤率、看具体考勤统计、体温统计；（2）查看具体详情或下属学校统计历史；（3）点击到校发热人员详情，紧急联动家长或当事人老师。

**2.6.7.6.消防安全管理**

按照宁波市学校消防安全管理指导意见等文件要求，上级教育部门对学校消防安全工作管理情况进行定期监督管理，下属学校可定期按照安全管理项要求进行自查上报，消防安全管理项包括：组织建设、消防教育、防火巡查、用火用电、危险物品管理等方面进行消防类隐患自查自检上报。局端通过以上重点结果管控辅助达成对下属学校此项安全工作监管。

**2.6.7.7.周边治安管理**

按照宁波市学校周边治安管理指导意见等文件要求，上级教育部门对学校周边治安工作管理情况进行定期监督管理，下属学校可定期按照安全管理项要求进行自查上报，周边治安管理项包括：校园周边交通标识标线规范设置、上下学护导执行、校园周边不良店铺、校园周边无治安高危人员、校园周边无工地或变电站等高危场所地等方面进行周边安全类隐患自查自检上报。局端通过以上重点结果管控辅助达成对下属学校此项安全工作监管。

**2.6.8.应急处置系统**

**2.6.8.1.突发事件管理**

突发事件管理可汇总显示下属学校突发事件上报情况和趋势，同时可在大数据上自动汇聚本周突发事件发生学校的提醒消息，点击提醒消息可查看、导出明细。

**2.6.8.2.值班上报统计**

学校点击“值班上报”，可进行当日值班上报。上报完毕，可进行修改，如果已经被处理，则不能修改，非当日上报也不能修改。如果上报异常，则问题描述必须填写。上级教育部门未处理之前可以进行修改，处理后可以查看处理结果和处理人。

上级教育部门可安装大屏，通过大数据中心中的值班上报实时、动态、直观地查看下属学校、区域教育厅局的当日学校值班巡检情况。大屏可看到实时上报学校、上报状态和上报时间；查看上报完成率和异常处理情况，以及各区域上报完成率。

**2.6.8.3.风险预警发布**

系统可根据被高危突发事件自动生成区域类型风险预警，也支持教育部门人工发布区域类型风险预警。风险大数据可自动统计生成风险预警排行，通过风险预警排行信息点击进入可查看到各预警详细内容，例如有：防溺水预警、学生非正常死亡预警、交通事故、食品与卫生风险预警、校园欺凌预警、校园周边风险预警和消防隐患预警。

**2.6.9.智安物联系统**

物联数据管理

用于学校各类智安系统接入管理与数据汇聚管理。包括：访客记录、监控图像、车辆记录、人员出入记录、预警记录，并实现向市级安全平台推送。

支持视频分析闯入、拥挤、打架、密度、遗留、遗失等预警信息通过安防设备联网平台接入。用户可以点击查看预警采集摄像头现场，平台自动保存预警的所有信息，并提供预警历史记录的查看，包括采集时间、预警类型和内容、预警通知对象、预警通知时间、处理人处理方式、处理结果等。

**2.6.10.接口对接服务**

1.与浙政钉的页面整合，支持从浙政钉跳转至平台界面（包括PC端、移动端）。

2.实现与学校前端安全设备联网平台的数据对接。

3.与宁波市校园智能安全防控信息平台的数据对接，满足上下级之间实时推送安全基础数据、安全业务数据。同时，根据（甬教安体[2020]105号）文件要求，实现将学校基础安全数据、校园四大系统数据、等级平安校园管理数据等接入到宁波市校园智能安全防控信息平台。

**2.7.前端校园安防系统建设**

前端校园安防系统建设包括校园访客登记查验信息管理系统、人员通道管理、车辆出入管理等智能防控设施，接入校园重点部位监控，扩容建设安防设备联网平台等。前端建设覆盖北仑区9个街道104所中小学校及幼儿园，涉及新建访客机96台，利旧8台；新建人员通道203个，利旧23个；新建车辆出入口道闸52道，利旧22道；计划接入重点部位监控1700余处，新建透明厨房存储1152T；以及联网平台扩容、平台对接共享等内容。

**2.7.1.访客登记查验信息管理系统**

**2.7.1.1.系统设计**

访客系统包含完整的访客预约、访客登记、人证比对、访客签离、访客人脸授权等功能，可以对来访人员通过认证比对进行身份确定，并下发权限。具体流程如下：



一般在门卫放置桌面式访客一体机；已经预约过的来访人员使用自助访客一体机完成自助登记动作；未提前预约的来访人员则需要到前台或保安室处登记，由工作人员利用台式访客一体机完成访客登记。

**2.7.1.2.系统功能**

（1）短信、凭条配置

访客配置功能包括访客短信信息模板配置（支持自定义短信模板发给被访人）、访客打印单配置（可选择需要打印的访客信息）、访客单背景图片配置，访客刷卡最大次数配置。

（2）访客来访

临时访客直接来访时，由前台工作人员与被访者进行信息，并录入姓名、身份证号、联系方式等信息，当访客为系统的黑名单人员时，系统将不予接待。

（3）访客登记

采用人证访客机必须对来访人员进行人证比对通过后，才能自动完成访客登记动作，并抓拍访客人脸。访客登记完成后，可根据需要，支持对访客的人脸在人脸通道闸机、梯控、门禁系统选择进入区域和时间进行授权。

（4）访客签离

访客离开时在访客机上完成签离，平台删除访客权限。

**2.7.1.3.访客移动端预约**

为满足外来人员来访的预约需求，系统需实现通过钉钉侧进行来访预约，简化访客登记、核验手续，完成智能化的预约登记。

**2.7.2.人员通道管理系统**

人员通道子系统能够对受控区域进行有效管控，所有进出受控区域的人员均需经过认证后方可通行，可以有效防止未授权人员随意进入受控区域，提升内部安全系数。此外，该系统可有效控制人员通行秩序，使得出入口通行井然有序，方便人员出入管理。

**2.7.2.1.系统设计**

人员通道子系统由人员通道闸机、工作站和发卡器等组成，对于安保要求严格的场景，还可以配置使用人证比对技术的人证闸机。根据出入口通道管理需要，选用网络型门禁控制主机，通过TCP/IP通讯方式进行与上层管理层通讯方式，支持联机或脱机独立运行，并可联动附近视频监控设备进行抓拍存储，门禁控制主机接入综合管理平台可实现设备资源、人员权限与配置的统一管理。

1）人员通道闸机

人行通道闸机阻拦体受控制系统驱动，人员身份验证通过后，阻拦体自动打开，延时后闭合。闸机可辅以摄像头、身份证读卡器、CPU卡读卡器、二维码读卡器、指纹识别仪、显示屏、自动收卡器、恒温箱等配件，认证方式和逻辑灵活多样。

2）门禁控制主机

门禁控制主机可选择内置在闸机内，也可以选择外置，负责人员通道闸机输入、输出信息的处理和储存，用于闸机开关的控制。

3）人证比对组件

对于需要人证比对系统实时进行身份比对验证的场所，人员通道闸机可以配置人证比对组件，能够 确保实名实证，即时比对，一人一证，验证通过。人证比对设备抓拍人脸照片，进行人实时比对，比对通过后予以放行。

**2.7.2.2.系统功能**

1）系统能够实现刷卡、人脸等多种识别方式，对权限进行识别，对权限合格人员放行通过。

2）具备紧急逃生功能，在发生紧急情况如火灾时，人员通道能够自动打开放行，不会阻碍人员的紧急疏散。

3）上下学高峰期，为了保证人员快速通过，人员通道可保持常开，避免发生拥挤、滞留事件。

4）系统支持将人员通道闸机身份认证记录关联为考勤记录，自动完成考勤任务。

5）为满足家校互通的业务需求，本次新建的人员通道设备（含利旧接入通道）及平台，应实现将学生进出校园数据推送至家长手机钉钉端，让家长更清楚的了解学生的校园进出情况。

**2.7.2.3.师生权限管控**

平台支持针对校内的不同人脸身份，配置不同的通行权限。如：将校内人员分为老师组和学生组，教师可在白天任何时刻正常通过人员通道，学生只可在上学、放学期间进行通行，有效地对校内学生进行管控，防止学生偷偷溜出校园，减少安全事故的发生。

**2.7.2.4.师生人脸信息建设**

在北仑区教育局2020年3月已建健康码测温系统中，各学校已进行过学生基础信息的导入与人脸照片采集。针对于已建人脸信息，在本次项目人员通道系统中可直接使用。

系统支持针对不同学校，开放不同权限的子账号，进行自己学校的人员信息及人脸数据管控。对于原先未获取的人脸信息或人脸图片不符合要求的人员，可使用自助采集机或批量导入的方式进行人脸建库。

**2.7.2.5.人脸数据采集**

目前，人脸信息采集支持多种采集方式，分别是自助采集、人脸批量导入。

1) 自助采集

采集流程如下：

1、设备端加密保存学校师生身份证编号信息

2、师生刷身份证时设备采集照片，照片与身份证内保存的照片进行校验

3、校验完成后，将新采集的图片+身份证编号发送至平台

4、平台根据身份证编号更新对应的人脸库照片，并完成所有人脸识别设备的照片更新。

2）批量导入

学校端可自由采集学生人脸照片，通过姓名\_身份证号.jpg的形式进行批量导入。

**2.7.2.6.人脸数据建库**

在校学生进行人脸数据建库具体如下：

1）学生信息获取，从校园一卡通系统或现有校园管理系统中导出在校学生相关信息，以表格形式导出；

表格信息主要字段如下：



2）照片信息绑定，学生自行提供照片格式为背景单色的面部清晰的正脸照，JPG图片，单张200KB以内，建议尺寸110\*168，压缩包200M以内，若提供照片不合格，后期可能会导致刷脸时无法进行比对，采集到照片后会与之前导入信息进行关联建库，以学号进行绑定；

3）绑定后的学生数据信息库通过系统配置导入综合安防平台，在平台配置时选择人员信息导入，选中要导入的信息表，然后开始导入，系统提示提示结果时表示学生人脸库已经导入平台。

4）平台会根据学生具体住宿信息进行下发分配学生人脸库到前端人脸比对终端。

**2.7.3.车辆出入管理系统**

**2.7.3.1.系统设计**

车脸出入管理系统是通过采用电动挡车器+车牌识别模块设备的组合，并进行对设备进行整合联动的方式，来对车辆的进出进行管制。结合管制空余车位数量，计算或限制停车时间，加强了防盗/防弊的功能；使系统能够更有效的辩识和管理通过出入口的车辆。

**2.7.3.2.系统功能**

**2.7.3.2.1.信息查询**

信息查询功能包括过车记录查询、预约信息查询和固定车辆查询三大查询功能；实现通过单个或组合式条件来查询历史过车记录，实现按车牌，卡号，方向，车辆类型以及进出场时间等方式。记录按照以当前时间点为基准，向前查看（最新的记录显示在第一页）。同时可满足按列表查看和图片查看两种模式。查询新增预约车位数查询和固定车信息查询；车辆信息包括车辆通信信息和车辆图像信息两类。

在车辆通过出入口时，牌照识别系统能准确拍摄包含车辆前端、车牌的图像，并将图像和车辆通行信息传输给出入口控制终端，并可选择在图像中叠加车辆通行信息（如时间、地点等）。

按车牌，手机号，预约时间段条件来查询预约信息。

**2.7.3.2.2.黑名单管理**

支持在出入口管理单元进行黑名单管理（与管理平台数据一致），并提供黑名单添加和删除功能。

**2.7.3.2.3.车辆监控**

单个出入口管理单元支持最多四个抓拍窗口布局，展示所有车道的过车记录和车道关联道闸的相关信息。

实时图片抓拍：抓拍显示车辆入场图片，包括车身图片以及车牌图片；车身图片可放大和查看局部信息。

记录校对：支持车辆进出场信息的记录、查询，支持对识别异常的车牌进行手工校对；

根据中心平台配置的放行规则，出入口管理单元客户端对非自动放行的车辆进行人工确认，由人工来判断是否需要放行；

出入口管理单元客户端脱机模式：对于网络原因以及其他一些不可抗拒的因素导致的中心服务器不在线的情况下，客户端支持离线控制，网络恢复后支持同步离线过车记录到中心，保护数据完整性。

过车图片和信息实时显示，视频实时预览，进出车辆自动匹配，图片预览按车道轮询。

**2.7.3.2.4.系统余位统计**

系统可根据进出车辆的数量，根据预先输入的校内停车位数，自动统计园区车辆余位，有效辅助管理人员进行出入车辆的管控。当校内停车位数为0时，则停止抬杆，禁止外来车辆进入校内。

**2.7.3.2.5.LED信息显示**

控制主机包含语音提示系统、信息显示屏，车辆驶入、驶出可以根据客户需要提示语音，并显示相关信息。

通过在学校停车入口处放置led显示设备，可以实时展现园区车位空余数量。

通过在学校停车出口处放置led显示设备，可以展示车辆信息及收费情况。

**2.7.3.2.6.车辆管控**

自动抓拍并区分“固定车”，“临时车”，“布控车”三种车辆类型，实现车辆区分管理。

**2.7.4.重点部位监控联网**

**2.7.4.1.透明厨房监控联网**

在2014年，北仑区教育局已建设北仑区透明厨房联网平台，共涉及289路前端摄像机、6台硬盘录像机、4台中心IPSAN存储服务器，并通过4套管理服务器搭建1套视频管理软件进行全区透明厨房系统的管理。

因项目已建时间较久，距今已有6年时间，设备整体性能相较于现在不断发展的智能化需求存在一定不足，在存储稳定性、设备接入能力、数据安全性、预览回放速率等方面均存在一定差距。且设备距今已有6年，已经达到设备建议使用的年限，存在很大的硬盘损坏风险。同时原有设备备份机制可靠性较低，如果发生硬盘损坏，数据恢复难度较大。

故从系统稳定性、先进性及数据安全性等方面考虑，在利旧原有前端设备的基础上，进行中心存储设备的兼容升级，实现更高性能、高可靠性的视频联网需求。

**2.7.4.1.1.接入方案**

经前期调研，本次建设的104所学校透明厨房约961路，已接入教育局端的有608路，除289路在局端有存储外，其余均未存储。针对目前情况，本次学校透明厨房监控接入方案如下：

1、将已接入的608路透明厨房视频监控从透明厨房联网平台迁移至本次扩容建设的安防设备联网平台；

2、尚未接入区教育局端的学校透明厨房监控，本次通过教科网全部接入安防设备联网平台；

3、对本次所有接入区教育局端的透明厨房监控存储视频30天。

**2.7.4.1.2.存储系统**

视频存储功能要求

|  |  |
| --- | --- |
| 功能项 | 功能说明 |
| 视频录像 | 系统可以按照用户制定的计划保存前端设备采集的录像数据，录像类型、录像头由用户指定，存储开启相关的资源。 |
| 动态修订录像类型：前端采集视频数据过程中，按报警类型可以修改录像的类型，修改后采集的视频数据即时保存到系统中，并在数据保存类型上得到反映。 |
| 视频检索 | 用户可以按监控点编号、录像类型、时间组合、锁定、标注等条件查询录像数据。 |
| 视频回放 | 支持根据监控点编号以及时间段、录像类型对录像数据进行回放。 |
| 支持根据监控点编号以及时间段对录像数据进行回放时间定位。 |
| 支持快放、慢放、倒序回放、I 帧回放。 |
| 支持手动开启回放、暂停回放、停止回放。 |
| 视频下载 | 支持根据监控点编号以及时间段对录像数据进行下载。 |
| 支持断点续传。 |
| 视频锁定 | 支持指定的录像片段进行锁定，锁定后的数据不被循环覆盖掉。 |
| 支持已锁定的录像片段锁定时长到期自动解锁。 |
| 视频备份 | 支持根据监控点编号以及时间段对录像数据进行本云手动备份支持根据监控点编号以及时间段对录像数据进行异云手动备份支持录像写入时根据冗余份数进行自动备份 |
| 周期覆盖 | 按策略支持按周期、容量进行录像数据的周期覆盖式存储。 |
| 视频补录 | 当取流出现异常时，支持自动将丢失的录像补全 |
| 主/子码流存储 | 支持按照计划有选择的存储前端的主子码流 |
| 视频抽帧转存 | 支持按周期进行录像数据的抽帧存储 |

**2.7.4.2.校园重点部位监控联网**

根据市教育局文件要求，校园内重点部位或人员通行频繁区域的视频监控系统接入公安机关、教育部门平台，并与区公共安全视频监控共享平台联网，按照GB/T28181-2016《公共安全视频监控联网系统信息传输、交换、控制技术要求》标准接入。

因此，涉及校园重点部位监控约748路（校门、操场，不含透明厨房）本次要求通过教科网接入区教育局端的设备联网平台，同时通过联网平台将视频推送至北仑区视频资源共享平台，实现区视频资源共享平台对校园重点部位监控的调取。

**2.7.5.安防设备联网平台（原平台扩容）**

**2.7.5.1.系统概况**

2020年3月北仑区教育局针对新冠肺炎疫情防控要求，建设了校园人体测温系统，利用生物识别技术、热成像测温技术、视频智能分析等技术手段，实现有效预防、及时控制和消除突发公共卫生事件及其危害。为学校师生生命安全和身体健康构筑起一道安全可靠的健康防线。

北仑区教育局目前已建的测温管理平台具有良好的开放性与扩展性，可在现有的测温平台基础上进行模块扩容，即能实现本期项目校园安防设备联网平台的建设。

本次平台扩容后将整合现有的透明厨房监控、测温系统功能以及校园重点部位监控系统，对所有104所中小学、幼儿园的校园安防系统进行统一管理。

**2.7.5.2.平台现有功能**

**2.7.5.2.1.测温点管理**

配置接收事件测温设备，配置异常体温阈值和进出控制。

**2.7.5.2.2.事件查询**

将人员信息与体温数据关联，支持查询并导出体温、绿码事件。

**2.7.5.2.3.趋势分析**

形成体温、绿码数据趋势图，可以直观的了解各种类型码的人数及占比，体温正常、异常的人数及占比。

**2.7.5.2.4.体温异常告警**

热成像设备可设置测温阈值，当超过阈值时，则进行温度异常报警，并上传事件至管理软件，针对体温异常人员事件可联动配置弹框。

**2.7.5.3.扩容新增功能**

**2.7.5.3.1.视频监控**

视频监控应用依赖于前端编码设备，主要实现了实时监控、录像回放、图片查询及电视墙等应用。

1、实时预览

视频实时预览即为对监控实时画面的预览，包括基础视频预览、视频参数控制、视图模式的预览，平台与监控点所在的摄像机对讲通道的实时对讲、批量广播以及对具备云台能力的监控点的实时云台控制。

2、基础视频预览

支持WEB浏览器和CS客户端两种方式，通过视频控件的形式进行监控点实时画面预览；

支持视频监控点资源数上展示监控点在线/离线状态；

支持级联监控点的点位标识；

设备SDK协议接入的设备预览模式支持直连预览和非直连预览切换，直连预览为平台直连设备，非直连预览为平台过设备接入组件进行预览，预览时可配置默取流方式。其他类型的设备及级联设备只支持非直连预览；

支持预览时开启智能规则，包含警戒线、区域等；

支持视频播放窗口布局切换，包含1、4、9、16、25常规画面分割，1+2、1+5、1+7、1+8、1+9、1+12、1+16、4+9、3+4、1+1+12等个性化画面分割以及1x2、1x4的走廊分割模式；

支持辅屏预览；

支持双击区域节点查看该区域下的所有监控点，监控点的展示数量为当前窗口分割数；支持批量关闭预览窗口、窗口自适应和全屏播放等功能;

支持监控点预览画面进行抓图、打开/关闭声音、电子放大、主子码流切换、查看码流信息等操作。支持监控点预览工具栏定义配置，用户可根据需要在预览窗口对上述工能进行添加/隐藏;

支持对配置了抓图计划的监控点进行图片监控，用户可在视频预览界面进行视频预览和图片监控两种模式的切换；

支持监控点主子码流自适应，可根据窗口数量自动切换监控点码流类型，当窗口数量小于设定值时为主码流，大于设定值时自动切换为子码流；

支持在视频预览画面中进行紧急录像，用于异常问题的记录和举证；

支持在实时预览时进行即时回放，用于预览发现异常状况时快速确认；

支持限时预览，在开启限时预览后，到指定时长最后10秒开始倒计时，直至关闭。若选择继续预览，则重新开始倒计时。限时预览预览的指定时长在1-30分钟之内自定义；

支持监控点分组轮巡，用根据预先设定的轮巡时间间隔、轮巡分组中的监控点顺序、默认窗口布局等对监控点视频画面进行轮巡显示。支持轮巡分组管理，包括新增、删除轮巡分组、调整时间间隔、监控点轮巡顺序等。通过视频预览配置，可在轮巡过程中过滤离线监控点；

支持监控点预览记忆功能，是否开启预览记忆功能可配置；

3、视图预览

视频预览支持以视图的形式保存监控点和播放窗口的对应关系及窗口布局格式，用户可用视图进行监控点分组管理及快速预览。

支持以共有视图和和私有视图两种模式进行视图管理。对视图中的监控点有预览权限的任何用户都可对公有视图进行预览、视图配置；私有视图只对本用户开放权限，其他用户登录后无法看到该视图。

支持视图管理配置，包括视图组的管理，在视图组中进行视图的添加、删除、移动位置、修改视图的监控点、窗口布局等操作。

4、录像回放

录像回放用于对历史视频录像的查询、定位、播放、录像流控、片段下载等应用。

5、基础录像回放

支持WEB浏览器和CS客户端两种方式，通过视频控件的形式对监控点历史录像画面进行回放；

支持按录像类型进行查询，包括计划录像、报警录像、移动侦测三种类型，录像播放时，还可可查看这三种类型之外的其他类型录像；支持按录像存储类型进行查询，包括设备存储和中心存储；

支持录像回放窗口布局切换，包含1、4、9、16等4中回放窗口分割类型；

支持对录像回放画面进行抓图、打开/关闭声音、电子放大、查看码流信息等操作；

支持按时间段查找录像和按时间点定位录像两种方式搜索录像；

支持对录像回放画面进行流控操作包括正放、倒放、倍速播放、倍速倒放、慢放、慢速倒放、单帧步进、单帧步退等。倍速播放速率1、2、4、8倍速可选，慢速播放速率1/2、1/4、1/8可选。

支持对录像添加标签和描述信息，可按照标签的类型、描述信息和标记时刻范围查找录像片段。录像标签包括红、蓝、绿、黄4种类型；

支持对录像片段进行锁定和解锁，锁定的录像时间段和锁定时长可选，锁定后的录像片段将不能被覆盖或删除。锁定时长按照日、周、月、年的颗粒度可选；

支持录像进度条录像范围的缩放，进度条录像范围1小时到24小时可选，也可通过滚轮的方式进行缩放；

支持录像回放显示智能信息，包括警戒线、区域等。

6、录像下载与剪辑

支持录像下载，用户可自定义录像片段范围，下载地址。支持对录像下载任务进行查找、删除、暂停、继续操作。支持批量对下载任务进行开始下载和全部暂停操作。支持对根据下载任务状态进行过滤；

支持录像剪辑，用户可自定义剪辑录像片段大小，保存地址；

支持单个录像下载/剪辑片段大小设置，设置项包含256M、512M、1G、2G。

7、图片查询

支持对配置了抓图计划的监控点所抓历史图片的查询，并按照监控点排序和时间排序两种方式展示图片查询结果；

支持对图片查询结果进行自动播放和下载操作，图片播放速度在1秒/张至30秒/张可配置。

8、电视墙应用

电视墙应用于中心大屏幕，专注视频上墙，调度解码资源将前端编码设备的视频画面在电视墙上显示。电视墙提供了解码资源管理、视墙资源管理、电视墙/窗口的控制及内容上墙等功能。

* 解码资源管理

支持对电视墙进行增、删、改、查操作，电视墙类型包括LED和LCD两种类型；

 支持对解码资源进行增、删、改、查操作，解码资源接入协议包括海康网络SDK协议设备和GB协议；

支持电视墙关联解码器通道，一个解码器通道只能关联一个监视器，已关联的解码器通道无法拖动；

支持对解码器窗口设置视频制式及分辨率。

* 窗口操作

支持窗口漫游，可进行窗口拖动改变窗口位置和窗口大小；支持窗口放大和还原；

支持窗口分割，分割数量以设备能力集的形式获取；支持窗口拼接；

支持窗口名称的编辑和修改，窗口名称最长16个字符，设置为空则为删除窗口名称；

支持窗口自定义编号，编号数在1~2147483647之间；

支持窗口置顶置底操作，当有多个开窗窗口层叠时，可针对窗口置顶/底，该窗口会在最顶/底层显示；

支持虚拟LED设置，包括长度，内容，透明度，文字滚动速度等设置；

支持窗口上墙，包括本地桌面上墙、预览上墙和回放上墙，其中模拟信号源只能进行预览上墙，如果解码设备为开窗设备，且该通道上没有窗口，则拖动监控点上墙时会先执行开窗；

支持报警窗口设置，可将窗口按高、中、低等设为报警窗口，当有系统中有相应等级的报警上报时，在该窗口自动上墙；

支持查看解码设备的解码状态；

支持上墙时配置取流方式，取流方式包括直连设备取流上墙和非直连取流上墙（默认）；

支持显示智能规则信息

* 场景应用

支持场景的增、删、改及配置操作。电视墙场景就是电视墙的一组状态的集合，包括窗口的分割、拼接等布局，及窗口上的监控点、预览轮巡、告警窗口、是否自动启停及启停时间；

支持场景切换及场景切换计划的配置；场景切换计划支持按“天”和按“周”为周期切换；

支持在场景中配置监控点轮巡计划。在轮巡执行时，可对某轮巡进行启停及执行上下一页的操作，包括开始、暂停、结束等；

支持轮巡窗口配置，轮巡间隔配置，轮巡监控点顺序的调整。

* 其他业务应用

支持主子码流切换，键点击客户端上墙的窗口，可显示切换主子码流的菜单，点击菜单可实现对上墙码流类型的切换；

支持强制子码流设置，可配置当窗口分割大于一定数量时，上墙自动使用子码流；

支持声音控制，可操作打开窗口相应输出通道的声音输出；

支持本地监控点预览和回放；

支持显示监控点在线状态；

支持对接网络键盘，实现键盘控制上墙；

支持PAD客户端控制电视墙大屏上墙

支持客户单换肤功能，用户可根据续期切换黑、蓝皮肤；

支持设备场景和平台场景配置，针对现场业务场景比较复杂，开窗分割数量比较多的场景，客户端发起切换场景请求可能会因为切换超时导致提示切换失败，此种情况下可使用设备场景。

**2.7.5.3.2.访客管理**

访客管理组件主要用于访客的信息登记、操作记录与权限管理。访客来访，需要对访客信息做登记处理，采集访客照片抓拍，为访客指定接待人员、授予访客门禁点/电梯/出入口的通行权限、对访客在来访期间所做的操作进行记录。

1、访客预约

1）管理员预约

访客预约功能由管理端进行访客的预约、批量导入预约、取消预约、审批预约功能；支持查看预约记录。

2）内部人员预约

支持由内部人员进行访客的预约、批量导入预约、取消预约、查看预约审批进度功能；支持查看预约记录。

2、访客管理

1）来访记录

支持查询、导出所有来访记录；支持将来访人员添加到访客名单。

2）异常访客记录

支持查询异常来访记录；支持将来访人员添加到访客名单；

3）访客权限下载记录

支持查询授权记录；支持重新下发权限。

4）访客权限组

支持新增、编辑、删除访客权限组；访客权限组包含门禁权限、门口机权限、停车场权限的组合；支持搜索权限组；支持设置默认权限组。

3、访客登记

访客可通过二维码、身份证、验证码在人工访客校验操作，登记完成发放访客卡，打印访客单；

访客可进行未预约登记，登记完成发放访客卡，打印访客单；

若访客为名单管理中的人，则登记的时候给予提示；

可进行访客再授权和访客签离。

**2.7.5.3.3.车辆出入管理**

1、放行管理

支持配置群组车辆专属的放行方式；

支持车辆节假日免费放行；

支持特殊车辆免费放行；

2、信息查询

过车记录查询支持按停车库，出入口，过车方向，放行结果，车辆类型，是否黑名单，车辆分类等查询；

支持查询结果列表和图片方式展示，并支持过车图片导出功能;

库内车辆查询支持库内车辆查询、车牌矫正和在场记录删除；

支持按入场时间段和按停车时长进行查询；

停车记录查询支持车牌、车位号、楼层、停车库及开始时间、结束时间进行查询，查询结果支持列表和图片方式展示；

车辆包期退款记录支持车牌、卡号、包期时间和充值类型等进行查询，充值类型包括包期充值、和自定义充值等，查询结果支持列表和图片方式展示；

账户充值退款记录查询支持账户、收支方式、收支类型、时间段查询；收支方式包括支付宝、微信和现金，收支类型包括账户充值、账户退款；

缴费记录查询支持车牌、卡号、停车库、支付方式、车辆类型、缴费时间进行查询，查询结果支持列表和图片方式展示；

车位预约记录查询支持车牌号码、手机号、停车库、预约类型等进行查询；

优惠券记录查询支持关联商户、停车库、使用状态进行查询，并可查看所使用的优惠券详细信息；

**2.7.5.3.4.人员通道门禁管理**

1、门禁业务管理

1）权限配置；

支持按组织、人员分组、人员配置权限，其可根据人员组织架构、自定义人员分组、单个人员为人员主体，选择门禁计划模版，规划不同门禁分组和门禁点的权限；

支持权限配置按人员、门禁点重新生成；

支持权限下载到设备，分为下载卡片权限、下载指纹、下载人脸，并支持三种下载模式的初始化下载，初始化下载支持将原有设备上的权限清空再写入新的权限配置；

支持权限记录生成任务、权限下载任务跟踪、查看；

2）生物特征识别配置

支持根据区域、门禁点名称搜索门禁点；

支持查看每个门禁点的人脸权限介质配置容量；

3）分组管理

支持门禁分组管理，实现新增、修改、删除、查看功能；

支持门禁分组搜索，包含门禁分组、门禁点、描述；

支持人员分组管理，实现新增、修改、删除、查看功能；

支持人员分组搜索，包含人员分组、人员、描述；

2、门禁事件查询

1）人员出入事件

支持人员的门禁出入事件搜索，包含姓名、工号、所属组织、门禁点、控制器、门禁点区域、事件事件范围、事件类型查询条件的各组合查询；

支持人员出入事件手动从设备驱动进行数据同步；

支持人员的门禁出入事件数据导出，包含列表数据导出、一体机联动抓图图片导出；

2）设备事件

支持设备事件搜索，包含控制器、读卡器、控制区区域、事件类型、事件时间范围查询条件的各组合查询；

支持设备事件数据导出功能。

**2.7.5.3.5.事件告警信息接入应用**

在原有摄像机支持入侵告警、人员聚集、遗留物品、人员徘徊等SMART智能功能，可通过平台配置，进行事件的联动。

当前端相机识别到相应的画面时，进行事件报警，并在中心端进行事件统计，也可进行相关联动配置，实现弹窗、上墙等应用。

支持根据安保区域、事件进行筛选，支持通过客户端对前端子系统进行布放、撤防操作；

支持按照时间、事件源、事件类型查询和导出历史报警事件。

**2.7.5.3.6.网络管理**

1、运维概况

运维概况展现运维状态概览统计、区域资源运行情况、点位运行情况趋势图、视频异常情况统计。

支持按区域以统计图方式展示监控点总数、监控点在线率、图像正常率、录像完整率；

监控点总数统计图通过不同的颜色展现了监控点总数、高清数、标清数、未检测数；支持各项数据明细查看；

监控点在线率统计图通过不同的颜色展现了监控点在线数、离线数、未检测数，并计算出监控点在线率；支持各项数据明细查看；

注：监控点在线率 = 在线 / (在线 + 离线)

图像正常率统计图通过不同的颜色展现了图像正常数、图像异常数、诊断失败数、未检测数，并计算出图像正常率；支持各项数据明细查看；

注：图像正常率 = 图像正常 / (图像正常 + 图像异常 + 诊断失败)

录像完整率统计图通过不同的颜色展现了录像完整数、录像丢失数、巡检失败数、未检测数；支持各项数据明细查看；

注：录像完整率 = 录像完整 / (录像完整 + 录像丢失 + 巡检失败)

支持以柱状图方式对区域资源运行情况进行统计，支持各统计指标项明细查看；

支持以图形方式展示近24小时、近一周、近一月的点位运行情况趋势，统计指标项包括监控点在线率、图像正常率；

支持近24小时、近一周、近一月的视频异常问题统计，视频异常项包括取流异常、登陆失败、解码失败、图像异常、其他；图像异常项包括信号丢失、图像模糊、条纹干扰、视频遮挡、其他。支持视频/图像异常项明细查看。

2、一键运维

一键运维是从数据库中读取运维数据，进行数据展示。

支持对监控点数量、解码设备数量、编码设备数量、存储设备数量、录像巡检数、视频诊断数进行展现，支持以上各类型资源状态详情的查看和导出。

3、状态巡检

状态巡检包含对监控点、编码设备、解码设备、存储设备的在线状态巡检。

1）监控点状态巡检

系统通过统计图和列表方式分别展现了监控点在线率、高清率、监控明细信息。

在线率统计图通过不同的颜色展现了点位离线数、点位在线数、点位未检测数，并计算出监控点在线率。

注：监控点在线率 = 在线 / (在线 + 离线)

高清率统计图通过不同的颜色展现了高清点位数、标清点位数、未检测数，并计算出高清率。

注：高清率 = 高清 / (高清 + 标清)

列表展现项包括监控点名称、所属区域、IP地址、在线状态、录制状态、离线时长、巡检时间。

支持统计图收起操作，展现了监控点总数、在线数、离线数、未检测数、高清数、标清数、未检测数；

支持根据设备所属安保区域、是否包含下级区域、在线状态、录制状态、监控点名称、IP地址、巡检信息进行筛选；

支持将巡检结果导出到csv文件中；

支持对列表数据进行刷新；

通过查看详情可以查看该监控点的基本信息以及历史状态，基本信息包括监控点名称、所属区域、IP地址及端口号、在线状态、设备厂商、资源编码、通道编号、巡检时间；设备历史状态支持通过时间去查询。

2）编码设备状态巡检

支持以统计图、列表方式展现编码设备巡检结果；

统计图展现项包括设备总数、在线数、离线数、未检测数，并计算出设备在线率。

注：设备在线率=在线/ (在线+离线)

列表展现项包括设备名称、所属区域、IP地址、在线状态、离线时长、密码强度、硬盘状态、硬盘使用率、巡检时间。

支持统计图收起操作，收起之后展现设备总数、在线数、离线数、未检测数；

支持根据设备所属安保区域、是否包含下级区域、在线状态、密码强度、硬盘状态、设备名称、IP地址对巡检信息进行筛选；

支持将巡检结果导出到csv文件中；

支持对列表数据进行刷新；

通过查看详情可以查看该设备的基本信息、硬盘信息以及历史状态，基本信息包括设备名称、所属区域、IP地址及端口号、在线状态、密码强度、资源编码、设备型号、设备软件版本、接入协议、离线通道数、硬盘使用率、巡检时间；硬盘信息包括硬盘编号、硬盘状态；历史状态支持通过时间去查询。

3）解码设备状态巡检

支持以统计图、列表方式展现解码设备巡检结果；

统计图展现项包括设备总数、在线数、离线数、未检测数，并计算出设备在线率。

注：设备在线率=在线/ (在线+离线)

列表展现项包括解码器名称、所属区域、IP地址、在线状态、密码强度、离线时长、巡检时间；

支持统计图收起操作，收起之后展现设备总数、在线数、离线数、未检测数；

支持根据设备所属安保区域、是否包含下级区域、在线状态、密码强度、设备名称、IP地址对巡检信息进行筛选；

支持将巡检结果导出到csv文件中；

支持对列表数据进行刷新；

通过查看详情可以查看该设备的基本信息、历史状态，基本信息包括设备名称、所属区域、IP地址及端口号、在线状态、密码强度、设备厂商、资源编码、巡检时间；历史状态支持通过时间去查询。

4）存储设备状态巡检

支持以统计图、列表方式展现存储设备巡检结果；

统计图展现项包括设备总数、在线数、离线数、未检测数，并计算出设备在线率。

注：设备在线率 = 在线/ (在线+离线)

列表展现项包括设备名称、所属区域、IP地址、在线状态、密码强度、硬盘状态、离线时长、录像卷使用率、巡检时间；

支持统计图收起操作，收起之后展现设备总数、在线数、离线数、未检测数；

支持根据设备所属安保区域、是否包含下级区域、在线状态、密码强度、硬盘状态、设备名称、IP地址对巡检信息进行筛选；

支持将巡检结果导出到csv文件中；

支持对列表数据进行刷新；

通过查看详情可以查看该设备的基本信息、录像卷信息、硬盘信息以及历史状态，基本信息设备名称、在线状态、密码强度、录像卷使用率、CPU使用率、内存使用率、资源编码、设备厂商、巡检时间；硬盘信息包括硬盘编号、硬盘位置、硬盘状态；历史状态支持通过时间去查询。

4、告警查询

系统按巡检计划对监控点、编码设备、解码设备、存储设备进行巡检，记录告警。

支持以统计图、列表方式展现告警数据；

统计图页面展现了今日新增告警数、告警总量、状态告警数、录像告警数、视频质量告警数、其他告警数；

列表展现项包括告警源名称、告警源IP、告警源类型、等级、状态、触发时间、恢复时间、告警描述；

支持统计图收起操作，展现了进入新增告警数、状态告警数、录像告警数、视频质量告警数、其他告警数；

支持根据设备所属安保区域、是否包含下级区域、状态、告警等级、告警源类型、告警源名称、触发时间、恢复时间进行筛选；

支持对告警数据进行解决，告警状态从持续中变为已恢复；

支持将告警数据删除（数据库中也删除）；

支持将告警数据导出到csv文件中；

支持对列表数据进行刷新；

通过查看详情可以查看该告警的基本信息、历史状态，基本信息包括告警源名称、所属区域、告警源IP、告警源类型、告警等级、状态、触发时间、恢复时间、告警描述；告警历史状态支持选择触发时间去查询。

5、统计报表

系统支持对监控点在线率、视频质量、录像完整情况的巡检结果进行统计、打分，生成统计报表，分为区域运维统计、视频质量统计、录像情况统计、取流情况统计。

根据安保区域、时间筛选统计监控点在线率、图像正常率、录像完整率，并展示综合得分及排名；

支持按月统计和按时间段统计；

支持以统计图方式展示区域运维总分TOP10，X轴表示安保区域，Y轴表示监控点在线率、图像正常率、录像完整率，支持手动选择是否显示监控点在线率、图像正常率、录像完整率；

支持查看监控点在线率、图像完好率、录像完整率的计算公式，并支持配置计算总分的各项权重占比；

支持区域运维统计明细展示，展示项包括所属区域、总数、监控点在线率、图像正常率、录像完整率、总分、排名。

支持将区域运维统计明细导出到csv文件中。

**2.7.6.对接与共享**

**2.7.6.1.平台开放性**

扩容改造后的校园安防设备联网平台具有良好的兼容性与开放性，开放视频应用服务、门禁应用服务、车辆管控、访客管理、人脸应用等相关接口，能实现第三方厂商对接及二次开发的需求。能实现包括视频流推送、门禁点记录上传、车辆信息上传、访客事件上传等功能。

为满足第三方厂家的对接需要，开放平台api接口及SDK，第三方可根据开放接口进行对接。

相关能力概述如下图：











**2.7.6.2.对接与共享**

1、校园内部重点部位视频、访客登记、车辆进出、人员进出数据可与市内保平台进行数据对接，将相关信息同步至市内保平台。且平台具有开放的接口能力，第三方可根据开放接口进行视频取流、访客、车辆、人员通行事件的获取。

2、实现与区视频资源共享平台对接，实现重点部位视频监控向区视频资源共享平台推送；

3、实现与区公安分局公共安全视频联网平台对接，接入公安侧已建的校园门口智能抓拍设备。

**2.8.支撑平台及网络安全建设**

**2.8.1.超融合系统**

基于超融合架构（包括计算、网络、存储、安全等虚拟化）部署平台方式，使平台的多种应用共享服务器、存储等硬件资源，可以帮助用户提供IT基础设施资源的利用效率，提升基础设施的应用和管理水平，实现计算资源的动态优化，使平台应用易维护、易扩充。

本次项目备份主要有数据库备份和文件备份。

将数据库服务器上的数据备份到备份存储服务器上，当生产环境出现数据故障时，可从备份存储服务器上还原数据。备份策略：每天通过压缩方式进行全量备份，保留三个月备份数据。

文件备份策略：每天定时将新上传的文件备份到备份存储服务器上。

**2.8.1.1.技术架构**

本项目采用超融合架构构建数据中心。软硬件一体的超融合设备，每个节点都包含了计算和存储资源，替代了传统方案架构中的服务器和存储设备。

硬件超融合：通过软件定义的计算和存储资源，可以为核心的业务提供相关的业务和数据存储支撑，不需要分别采购服务器和存储设备。通过软件定义的形式，超融合提供统一的计算和存储资源池，可以灵活的被各种业务按需使用。

软件超融合:实现软件层面的超融合，使得存储和计算资源能够更加深度的整合，在管理层面实现所有资源的统一管理，并能够进行更加精细的软件定义。

管理超融合:对存储资源和计算资源在同一平台进行统一管理。

网络安全超融合：通过虚拟化安全保护软件，实现分布式逻辑路由，分布式防火墙保护，负载均衡，L2/L3 VPN功能等。

**2.8.1.2.超融合资源池设计**

本次北仑区校园智能安全防控系统建设通过5台X86服务器（CPU GOLD 2\*5118 2.3GHz，512G内存，12\*SATA/SAS盘位，默认128G系统盘，2\*960G SSD缓存盘，6\*4T SATA数据盘，6个GE接口，2个万兆光口），满足核心业务系统的需求。

虚拟资源池清单：

|  |  |  |  |
| --- | --- | --- | --- |
| 服务器名称 | 配置 | 单位 | 数量 |
| 联网平台 | CPU：2颗8核心 内存：32G 硬盘容量：2T | 台 | 2 |
| 视频接入服务 | CPU：2颗8核心 内存：32G 硬盘容量：2T | 台 | 2 |
| 访客接入服务 | CPU：2颗8核心 内存：16G 硬盘容量：1T | 台 | 1 |
| 通道接入服务 | CPU：2颗8核心 内存：16G 硬盘容量：1T | 台 | 2 |
| 通道事件服务 | CPU：2颗8核心 内存：16G 硬盘容量：1T | 台 | 2 |
| 人脸数据服务 | CPU：2颗8核心 内存：16G 硬盘容量：1T | 台 | 2 |
| 车辆接入服务 | CPU：2颗8核心 内存：16G 硬盘容量：1T | 台 | 1 |
| 车辆事件服务 | CPU：2颗8核心 内存：16G 硬盘容量：1T | 台 | 1 |
| 数据联网模块 | CPU：2颗8核心 内存：32G 硬盘容量：1T | 台 | 2 |
| 数据对接共享 | CPU：2颗8核心 内存：32G 硬盘容量：2T | 台 | 2 |
| 安全信息平台 | CPU：2颗8核心 内存：32G 硬盘容量：2T | 台 | 3 |

**2.8.1.3.主要功能**

超融合系统具备服务器虚拟化、存储虚拟化、网络虚拟化和高可用等功能。

**2.8.2.备份系统**

本项目通过配置备份一体机针对现有超融合环境，对于其中的关键性业务，此外还有数据库服务器以及其他物理服务器，采用安装一致性代理的有代理备份方式完成实时备份保护。同时按时间计划建立众多版本快照，当业务系统发生数据丢失，根据快照进行数据历史版本恢复。备份一体机可以恢复到原设备也可以通过本地应急功能将系统直接快速恢复到备份一体机自带的虚拟机上，实现业务的快速恢复。

**2.8.3.边界安全防护**

按照公安部《公安信息通信网边界接入平台安全规范（试行）--视频接入部分》的要求，建设视频安全接入与数据交换链路，满足其他部门接入到公安视频专网系统中调取公安视频专网视频资源的需求，同时又必须保证公安视频专网网络的安全性与保密性。前端接入区防护，包括前端接入的摄像头及其他设备，应建立前端安全防护机制，实现对前端资源访问的有效识别和安全管理。

网络安全边界确保公安视频专网与其他网络之间的安全隔离以及相互间的访问控制。视频安全交换接入系统包括视频认证服务器和视频安全隔离设备，视频认证服务器又分为视频用户认证服务器和视频接入认证服务器两类。视频用户认证服务器对使用视频资源的用户进行统一注册、身份认证及权限管理，仅允许认证通过的用户访问已授权的视频资源。视频接入认证服务器对接入对象进行设备认证，并对视频信令格式进行检查及内容过滤，只允许合法的协议和数据通过。视频安全隔离设备将视频控制信令和数据进行分别处理和传输，其中视频数据为单向传输，视频控制信令为双向传输。安全数据交换平台由专用的数据交换服务器组成，安全数据交换系统根据业务配置建立业务数据通道，并对业务数据通道上传输的数据进行过滤和审计，只允许符合安全策略的业务数据进行交换，不允许任何其它的数据传输。边界接入平台的外部接入链路使用专线。链路安全需求要做到如下几点：

1）接入平台内部为不同接入对象提供服务的链路必须根据接入对象安全级别和业务操作方式（数据交换或视频访问）加以区分。

2）教科网等网络接入到公安视频专网中需要对接入链路进行严格的访问控制，只允许视频、图片、控制信令等业务流量。

3）针对安全要求较高的边界数据交换，采用物理隔离设备连接的两个独立主机系统之间，使之不能存在通信的物理连接、逻辑连接、信息传输命令、信息传输协议，不存在依据协议的信息包转发，只有数据文件的无协议“摆渡”。

本次安全边界按照《公安信息通信网边界接入平台安全规范(试行)——视频接入安全部分》要求，采用三主机架构设计，包括视频专网前置服务器、教科网前置服务器和安全隔离设备（网闸）。

视频专网前置服务器部署在视频专网与专用安全隔离设备之间,实现了协议终止、接入设备认证、接入设备访问控制、流量管理等功能;

安全隔离设备（网闸）在安全隔离区内,实现协议终止、网络隔离、视频数据流与视频控制信令分离、视频控制信令与视频数据流的分析过滤、视频流单向传输等功能。

主要功能如下：

（1）安全数据交换平台只允许符合安全策略的业务数据进行交换，不允许任何其它的数据传输。

（2）能够实现对数据交换对象的身份认证；

（3）能够保证数据交换内容的机密性和完整性；

（4）能够区分连接内外网链路的接口；

（5）能够验证数据源和数据完整性；

（6）能够根据业务规则检查数据类型、格式、内容，过滤不符合安全策略的数据。

（7）视频接入认证服务器对接入对象（终端、视频服务器等）进行设备认证并与之交互，获取视频。视频用户认证服务器对公安视频专网上使用视频资源的终端用户进行统一注册、身份认证和访问控制，并提供视频服务。

（8）对视频数据与控制信令严格区分，分别处理后进行传输。支持视频数据的单向传输模式和控制信令双向传输模式。

（9）对视频信令格式检查及内容过滤：能够识别视频控制信令、视频传输协议，阻断未注册的协议和数据格式。

（10）支持集中监管，实时上报设备运行状态、数据流量、设备报警等信息。

**2.8.4.下一代防火墙**

本项目配置万兆下一代防火墙，用于对安全防控系统支撑平台的防护。

在硬件支撑平台服务器边界部署下一代防火墙，满足“访问控制”“入侵防范”和“恶意代码防范”等安全控制要求，防范网络病毒对于重要业务系统区域的侵袭。

**2.8.5.防病毒系统**

本次配备防病毒软件系统一套，20个节点授权。系统功能要求：

1、一体化管理

功能一体化：集终端防病毒和安全管控于一体的终端安全管理系统；

平台一体化：兼容Windows、Linux、国产操作系统、MacOS X；

数据一体化：结合云端大数据和威胁情报，有效感知本地安全态势。

2、病毒防御多维化

多引擎技术：拥有云查杀引擎、系统修复引擎、脚本查杀引擎、启发式引擎、人工智能引擎，有效查杀已知和未知病毒；

立体化主防：具备隔离防护、入口防护、系统防护及应用防护等主动防御技术；

智能自学习：通过海量病毒样本数据自学习，人工智能引擎无需频繁更新特征库、病毒检出率仍远超传统查杀引擎；

3、管控智能化

资产管理：自动识别全网终端资产信息，实时监控系统状态并告警，保障业务连续性；

安全策略管理：通过非法外联、外设管理、进程控制、主机防火墙、桌面安全加固等多元化方式，提升终端安全等级；

漏洞补丁管理：对全网终端漏洞进行扫描并关联，根据终端分组或操作系统类型错峰下发补丁。

**2.8.6.日志审计系统**

运维管理域部署日志审计系统，满足等保安全区域边界、安全计算环境、安全管理中心中所有对“安全审计”和“审计管理“的技术要求，同时满足《网络安全法》中“留存相关的网络日志不少于六个月”的法律要求。

日志审计系统通过监测及采集信息系统中的系统安全事件、用户访问行为、系统运行日志、系统运行状态等各类信息，经过规范化、过滤、归并和告警分析等处理后，以统一格式的日志形式进行集中存储和管理，结合丰富的日志统计汇总及综合分析功能，实现对信息系统整体安全状况的全面审计。

专注于对信息系统中各类主机、数据库、应用和设备的安全事件、用户行为、系统状态的实时采集、实时分析、异常报警、集中存储和事后分析，是支持分布式、跨平台的统一智能化日志管理及审计设备，可以对各类网络设备、安全设备、操作系统、WEB服务、中间件、数据库和其它应用进行全面的安全审计。

日志审计系统提供全面的日志采集功能，通过多种方式采集信息系统中众多类型系统日志、操作系统、应用系统等格式不一的日志数据。

基于对各类日志的理解和深入分析，并提供日志专家规则库，实时智能分析海量日志数据，呈现给用户可读性强、更易理解的日志信息。

**2.8.7.运维审计系统**

运维管理域部署运维审计（堡垒机）设备，堡垒机侧重于运维安全管理，集账号管理、身份认证、单点登录、资源授权、访问控制和操作审计，能够对用户IT资产（如服务器、网络设备、安全设备、数据库等）的操作过程进行有效的运维操作审计，使运维审计由事件审计提升为操作内容审计，通过内控管理平台的事前预防、事中控制和事后审计来全面解决政府和企业的运维安全问题，进而提高用户的IT运维管理水平。

**2.8.8.数据库监控与审计系统**

结合等级保护2.0相关标准和要求，从保障用户业务安全高效运行为根本出发点，进行网络安全体系方案设计。以安全能力模型支撑，为用户构建以技术、管理和运营三大安全体系为目标的可运营的智能化安全体系，使等级保护对象具备安全可视、持续检测、协同防御的能力。系统具备以下功能：

1、数据库发现与管理

2、数据采集

3、数据库对象统计

4、数据库入侵行为监测

5、数据库异常行为监测

6、数据库违规行为监测

7、数据库行为建模

8、敏感数据资产发现与审计

9、数据备份与恢复

10、系统权限控制

11、对外数据传输接口

12、集群管理

**2.9.机房建设**

**2.9.1.总体要求**

北仑区教育局目前没有独立的数据中心机房，主要依靠区信息中心机房和新碶中学机房来满足教育局信息化系统的整体运行。由于本项目规模较大，后端应用支撑平台服务器、存储、安全设备较多，而新碶中学机房仅为35平米，如果本项目建设完成后，新碶中学机房将无任何拓展空间。因此，本次暂定计划对新碶中学目前机房的西侧办公室进行改造（机房具体设置地点最终以教育局指定学校为准），做为北仑区教育局数据中心机房，并按B级机房标准进行设计，包括：装修系统、供配电系统、防雷接地系统、照明系统、环境监控系统、综合布线系统、UPS电源系统、精密空调系统、新风及排烟系统、气体灭火消系统等工程。

机房主体工程为框架结构，层高3.5米。本机房工程设计总面积约60平方米左右；整体中心机房标准参照GB50174-2017，按照B类机房标准建设设计。

具体要求如下：

1）机房规划应充分考虑系统的可靠性、实用性、先进性、可扩展性。

2）室内控制设备、电器设备、布线系统的选材应注重其可靠性，全部采用符合国家标准的优质产品，其特性和安装工艺符合或超过国家标准，以确保系统投入运行后故障率为最低。

3）采用机房专用精密空调和专用新风系统，机房环境的温度、湿度、洁净度与通风量满足国家B级标准机房需求。

4）采用UPS集中式供电设计，以充分保证机房电源供应的安全可靠性。

5）采用七氟丙烷自动灭火系统，以充分保证机房设备安全运行的可靠性。

**2.9.2.机房规划**

根据新碶中学机房目前的布局，本次新机房位于现有机房的西侧，整体设计满足B级机房要求，机房规划如下：：



在数据中心机房设计15套600\*1200\*2000mm服务器机柜,1套配电柜，1套UPS电源，1套30.5KW恒温恒湿精密空调，1套7.5KW精密空调；

数据中心机房是未来的数据处理中心，是整个网络系统的心脏，对安全性和环境温湿度及洁净度要求较严，需要采用机房专用精密空调、自动消防系统、新排风及自动排烟系统。结合中心机房结构和实际面积，本方案采用1台30.5KW精密空调做制冷处理，以满足机房制冷要求；配置二套70KG自动七氟丙烷气体灭火系统，以满足机房消防要求；配置一套1500m³/h的新风换气主机，以满足机房换气要求；配置一套4000m³/h的消防排气风机，以满足机房发生火灾后的排烟换气要求。

为减少机房信息泄露和外界对机房的干扰，需对机房做全屏蔽处理，屏蔽措施包括：墙体彩钢板饰面、地面屏蔽网及接地处理等。

**2.9.3.机房装修**

满足如下要求：

1）电子计算机机房组成按计算机运行的特点及设备具体要求确定；

2）计算机机房装修材料选用难燃材料和非燃材料，能防潮、吸音、不起尘、抗静电。

3）计算机机房的活动地板是难燃材料或非燃材料。

4）活动地板应有稳定的抗静电性能和承载能力，同时耐油、耐腐蚀、柔光、不起尘。

5）异型活动地板提供的各种规格的电线、电缆、进出口做得光滑，防止损伤电线、电缆。

6）活动地板下的建筑地面应平整、光洁、防潮、防尘。

7）在安装活动地板时，采取相应措施，防止地板支脚倾斜、移位、横梁、坠落。

8）主机房温度：温度23±1℃，相对湿度40%-55%，温度变化率＜5℃/h，不凝露 ，配电间温度15-25℃。

9）尘埃：颗粒≥0.5um ，个数≤18000粒/dm³。

10）噪音：操作间区间≤65dB。

11）电磁干扰：主机房内无线电干扰场强在频率为0.5-1000MHz时，无线电干扰场强不大于126dB，磁场干扰环境场强不大于800A/m。

12）对装饰工程中的隐蔽工程，严格按照国家标准，用材符合机房用材性能指标，做到不起尘、阻燃、绝燃、不会产生静电、牢固耐用并无病虫害发生；

13）本设计标高以楼层层面为基准±0.00mm，机房可用高度为2.8米，地板安装高度为0.35米，机柜高度为2.1米，上走线桥架高度0.15米，设备总高2.55米，剩余0.25米。

**2.9.3.1.机房地面**

对于本机房工程的结构和特点，采用在机房空调送风区域内房间的楼面采用铺设带防水面保温棉板来提高楼面的隔热功功能。在主机房精密空调区域的地面铺设30mm厚带防水、阻燃材料的橡塑保温棉板，在铺设保温棉之前先将地面清理干净及除尘。

本次机房防静电地板的安装高度为350mm。在安装地板之前对地表面以及安装面以下的墙面进行清洁处理。设计施工如下：

机房地面在施工之前，对放置精密空调位置处做空调挡水坝处理，高度为10cm，表面平整、密封、防漏水，挡水坝内做地漏；

机房地面铺设30mm厚塑胶材料保温层（包含墙面下立面）,塑胶保温材料防火等级B1级；

铺设完保温棉后，在地面上铺设钢质防静电活动地板，尺寸为600\*600\*35mm，防静电地板滚动载荷不小于3KN，集中载荷不小于4.5KN，均匀载荷不小于12KN/㎡；

铺设防静电地板时配套防静电地板紧固件做固定处理，防静电地板紧固件做有效的接地处理；

在走廊进入机房各门口处做台阶处理，台阶垫底材料使用水泥加细沙1:3混合砂浆找平一遍，厚度为20mm厚，粘结层材料使用环保型自带胶，面层材料使用150mm高定型支架支撑600\*600防静电活动地板，台阶设置两层。

**2.9.3.2.机房墙面**

本次工程的主要机房区内墙面选用复合彩钢板作为墙面装饰材料，施工时采取纵向整板安装。彩钢板为镀锌钢板成型，彩钢板的表面镀锌量为45g/单面m2，纸面石膏板满足与镀锌钢板粘结的剪切强度为0.15Mpa。

墙柱面采用彩钢板装饰，为了机房内设备的安全，所有机房与外界连接的墙体的缝隙区管线槽接口处均堵实，以防止虫、鼠进入机房。设计施工如下：

在原有墙面使用龙牌C75国标龙骨做内衬主支架，纵向600mm处设置一根主龙骨；

铺设好龙骨后延地面向墙面四周上来100mm及楼面向墙面下来100mm范围内使用石膏板做基层处理，基层外层使用30mm塑胶保温棉做保温处理；

所有龙骨做有效的接地连接处理；

彩钢板尺寸为：1200mm\*2960mm，厚度为：13mm，颜色：米白色彩钢板；彩钢板表面材料采用热熔镀锌钢板，厚度≥0.6mm，表面涂层厚度≥25UM，抗静电要求：表面电阻率106-108Ω/㎡，涂装色差≤1.5；

铺设完彩钢板后，延静电地板四周与墙面彩钢板间做贴脚线处理，贴脚线采用拉丝不锈钢材料，高度为10cm，厚度为13mm。

中心机房与操作间之间采用铯钾防火玻璃加钢基础做玻璃隔断，边框外包不锈钢包边。

**2.9.3.3.机房顶面**

机房顶面做铝合金微孔天花处理，施工设计如下：

顶面采用600\*600\*1.0铝合金微孔天花板做吊顶处理；

配置#75轻钢龙骨；

吊顶四周使用L型收边条做美饰处理。

**2.9.3.4.机房门窗**

从机房安全角度考虑，对机房砖墙隔断处安装钢制双开防火防盗门；从机房美观配套角度考虑，对机房玻璃隔断处安装双开玻璃门，所有的门材料必须符合防火规范要求。施工设计如下：

走廊进机房砖墙门口处，做1500\*2200mm双开防火防盗门，防火防盗门防火等级为甲级；配置门框美饰及地弹簧、闭门器、门锁等附件；机房区对外出入口防火门全部朝外开启。

原有窗户内侧贴深色膜后，进行封堵处理。

**2.9.3.5.机房隐蔽工程**

机房工程中的隐蔽工程，严格按照国建标准取材（环保、防火），安装时对隐蔽部分施工内容拍照留档，做好接地处理。

**2.9.3.6.机房承重**

对机房内机柜、空调等质量较大的设备放在静电地板上做散力架处理，配电箱散力架还左右出现进线导线功能；散力架的安装有助于设备的固定及楼面、静电地板的承重。设计施工如下：

支撑架采用Q235，5号槽钢做有效焊接，接点平整光滑，支撑架与地面做有效固定处理，支撑架除锈后，刷防锈漆两遍，防火漆两遍；

所有的支撑架固定时需在支点出安装防震动橡胶片；

所有的支撑架做有效的接地连接。

**2.9.4.机房照明系统**

**2.9.4.1.总体要求**

本方案设计采用LED灯盘。

正常照明：在正常情况下使用的室内外照明。

应急照明：当正常照明因故熄灭的情况下，供暂时继续工作、保障安全或疏散用的照明。

本工程在部分灯具中加入蓄电池，作为应急灯具的后备电源。

机房的平均照度大于500Lux，眩光控制等级为Ⅰ级，照度均匀度不低于0.7。

辅助房间的平均照度大于300 Lux。

应急照明的照度≥50 Lux。

疏散照明和安全出口标志灯的照度大于0.5 Lux。

**2.9.4.2.机房普通照明**

日常照明配电系统由机房配电柜供电，采用LED嵌入式灯盘。在机房内均匀分布安装规格为600\*600 LED灯盘，灯具采用墙面跷板开关控制，连接线缆使用BVR2.5m2电线；所有灯盘采用无启动电流干扰电子整流器，平均照度≥500Lx；照明均匀无眩光无死角、各作业面无方向性限制；控制采用分区、分片控制方式，维修方便，外观与铝合金天花板相匹配。

**2.9.4.3.机房应急照明**

应急照明配电系统由机房配电柜供电，采用LED嵌入式灯盘。在机房内均匀分布安装规格为600\*600LED灯盘，灯具采用墙面跷板开关控制，连接线缆使用BVR2.5 m2电线；所有灯盘采用无启动电流干扰电子整流器，平均照度≥500Lx；照明均匀无眩光无死角、各作业面无方向性限制；控制采用分区、分片控制方式，维修方便，外观与铝合金天花板相匹配。

**2.9.4.4.机房应急指示灯**

疏散照明和安全出口标志灯的照度大于0.5 Lux，安全出口标志灯自带蓄电池，配电系统由机房配电柜供电，使用市电插头方式供电。

**2.9.5.机房防雷接地系统**

**2.9.5.1.总体要求**

本机房要求三级防雷：（防雷产品反应时间<2.5ns）

第一级防雷器：在大楼总进线的低压配电房后的机房市电接入端进行第一级避雷保护(大楼负责)。

第二级防雷器：在机房配电柜的输入端进行第二级避雷保护。

第三级防雷器：在机房UPS输出端加装第三级避雷保护。

根据实际情况，本方案防雷做2+3级防雷；

机房接地：

计算机直流工作地：采用铜排在活动地板下敷设，依据计算机设备布局，纵横组成网格状，配有专用接地端子，用编织软铜线以最短的长度与计算机设备相连。计算机直流地需用接地干线引下至接地端子箱。接地电阻≤1Ω。

配电系统交流工作地：取自大楼的交流保护地，接地电阻≤4Ω。

安全保护地：采用接地干线引下至接地端子箱，接地电阻≤4Ω。

防雷保护地：建筑的结构防雷接地由其他有关部门完成，电源防雷为在电源配电柜电源进线处安装浪涌防雷器。

本次工程接地系统利用大楼原有接地极，做联合接地处理，接地电阻≤1Ω。

**2.9.5.2.机房防雷**

电源系统做2+3级防雷处理；

2级防雷单模块最大放电电流40KA，响应时间＜2.5ns；

3级防雷单模块最大放电电流20KA，响应时间＜2.5ns；

所有防雷产品都做有效接地连接。

**2.9.5.3.机房接地**

在机房区的静电地板下设置等电位地排，采用40\*4mm紫铜排构成等电位均压环，铜排通过高强度绝缘子固定在地面上；

通过50 mm2专用接地线连接紫铜排与接地汇接箱，作为交流接地和安全保护接地；

机柜部分采用两根不同长度的6mm2接地专用线与等电位连结网络连接；

所有金属顶棚、龙骨、防静电地板、墙面及设备的金属外壳、金属管线等都与等电位地网连接；

等电位联接网络采用M型结构；

接地地租≤1Ω，零地电压小于2V。

**2.9.6.机房综合布线系统**

1、配线架

选择模块化的线架以灵活配置端接数量，减少端口浪费便于日后的维护变更。使用高密度配线架，来提高机柜的使用密度，节省空间。

2、跳线

用颜色来区分不同网络的跳线；跳线性能指标满足相应标准的要求；采用高密度的铜缆和光纤跳线，提高高密度环境的插拔准确性和安全性。

3、线缆

选择具有长久的使用寿命的线缆，减少占用空间，具有更好的传输容量，具有安全阻燃性，提供多种颜色区分；选择的传输介质为6A 类双绞线、多模光缆、单模光缆。

4、机柜

选择开放式的机架，来安装配线设备；选择封闭式的机柜，来安装网络设备、服务器和存储设备等；统一采用标准的19英寸的机架和机柜。预留足够的布线空间、线缆管理器、电源插座和电源线以确保充足的气流。

本项目水平分配区共划分为1个分区，有15个机柜组成，水平分区每个机柜区布置24 根6 类双绞线至列头柜，每个列头柜至核心区布置1根6对多模光纤。水平分配区主要包括水平跳接、SAN 网络交换机、服务器和KVM 交换机。

每个机柜配置一个24 口快接式配线架至列头柜，为一些应用考虑的线缆也要规划并在此端接好，配线架之间的水平布线采用6类低烟无卤线缆。

**2.9.7.机房新风排烟系统**

新风系统：

采用1500m³/h的一进一出新风换气主机，吊顶式安装，配置高静压/低噪音两种形式，具有正压送风功能及根据新风温度自动控制功能，具有高效过滤和降噪功能；过滤效率达到亚高效，满足数据中心设计规范要求的洁净度，新风排量配比能够保持微正压；可设置定时自动开启和关闭，具备化霜功能，具备来电自恢复功能。

消防排烟系统：

根据气体灭火要求，机房气体灭火区设置消防排气系统。选用风量为4000m3/h以上的轴流风机，消防排气下弯管沿墙面返至地板上下方200mm处设单层百叶风口。同时配置有消防自动泄压作为气体灭火的泄压装置。为保持机房内的新风循环，须在靠近墙的位置（最好是在空调送风的末端）安装排风机及排风管道，用低噪音轴流风机作为排风机组，通过排风管道把多余的废空气排到室外。一旦发生火灾，气体灭火后房间存在大量的气体，就要启动排风机组排到室外。

**2.9.8.机房精密空调系统**

本次机房采用32KW精密空调1台，采用地板下送风上回风方式。配电间采用7.5KW精密空调1台，采用上送风下回风方式。达到数据中心内有效制冷，空气循环。

机房内主要热量的来源如下：

设备负荷（计算机及机柜热负荷）；

机房照明负荷；

建筑维护结构负荷；

补充的新风负荷；

人员的散热负荷等；

其他。

**2.9.9.机柜及UPS系统**

**2.9.9.1.总体要求**

项目规划15个服务器机柜，1套配电柜，1套模块化100KVAUPS主机。

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 数量 | 单位 | 说明 |
| UPS模块 | 1 | 套 | 模块化UPS |
| 机柜 | 15 | 台 | 双供电回路设计，每个机柜内配置2条PDU |
| 配电列头柜 | 1 | 台 | 供模块内所有供电需求 |
| 监控 | 1 | 套 | 温湿度、烟感、水浸、报警、管理 |

**2.9.9.2.低压配电系统**

本项目机房的供电采用380/220V电压、50HZ频率和三相五线制(即TN-S系统)的配线方式供电。

配电总体设计方案为：提供1路专用市电，1路市电-输入配电-UPS-输出配电-PDU-负载组成。

在保证电源运行时满足三相基本平衡，设计时将单相负荷均匀分配在各相上。计算机机房内的插座应分两种，它们是：不间断电源（UPS）供电的设备用标准插座和市电直接供电的设备用标准插座。为防止闪电雷击及操作过电压对设备造成的危害，机房专用动力配电柜进线处装设过压保护装置，以消除线路上产生的瞬时高压尖峰脉冲。保证计算机设备稳定运行，不受损坏。

机房的动力设备如精密空调、新风换气机由市电供电，其它计算机设备如服务器、交换机等由UPS进行供电。

配电柜中设有电流表、电压表，供检查电源电压、电流及三相间平衡的关系，三相电分别设有电源指标灯，以监控三相电的供电情况，并且备有断电自动切换开关，完全满足机房的需要。

**2.9.9.3.UPS电源**

依据GB50174规范B级机房要求，本着机房建设安全、经济、节能的原则，本项目UPS方案采用模块间并机冗余，模块间并机工作。

UPS配套电池组承担在市电断电的情况下为UPS提供电源的工作，保障在市电断电的情况下机房内的计算机系统仍能在一定时间内正常工作，可见电池组在UPS系统中充当着非常重要的角色。考虑到成本及使用性能，作为后备电源使用，电池多采用阀控式密封蓄电池，循环充放电次数达300次以上，使用寿命5年以上。

**2.9.9.4.机柜系统**

机柜系统主要为服务器、网络设备、存储设备等设备提供物理空间，标准机柜尺寸为19英寸42U。机柜整体结构由机架、前后门、侧板、底板、层板、U立柱、走线孔、底座组成，标准尺寸为宽x深x高=600x 1200x2000mm。

**2.9.9.5.动力环境监控系统**

动力环境监控主要针对微模块内部的配电、空调、温湿度、消防、视频、门禁、漏水等设备的实时数据、设备状态、实时告警进行管理。

1）系统结构

整个系统主要由以下三部分组成：现场设备采集层、监控主机、浏览终端。各部分的主要作用如下：

现场设备/信号采集层:由各种设备、传感器组成，如UPS、空调、温湿度、漏水，烟感等的现场信号，将采集的现场信号通过RS485/RS232方式上传到监控主机。

监控主机：可脱网工作并具有独立数据处理及数据存储能力，用于将现场设备采集层传输来的的各种信息进行存储、实时处理、分析和输出，处理所有的报警信息，记录报警事件，并负责将控制命令发往前端设备，实现对现场设备的远程控制。

2）UPS监控

对UPS内部整流器、逆变器、旁路、负载、电池等各部件的运行状态进行实时监视，一旦有部件发生故障，系统会自动报警。并且实时监视UPS的各种电压、电流、频率、功率、电池后备时间等参数。监控可全面诊断UPS状况，监视UPS的各种参数。一旦UPS报警，应自动切换到相关画面。越限参数将变色，并伴随有报警声音，有相应的处理提示。对于重要的参数，可作曲线记录，并可显示选定某天的最大值，最小值，使管理人员对UPS的状况有全面的了解。

3）空调监控

机房监控系统能实时监视空调各部件（压缩机、风机、加热器、加湿器等）的运行状态与参数，并可远程修改设置与开关空调。（根据生产厂提供的全部监控功能）此系统所实现功能如下：压缩机状态、风机状态、加湿器状态、去湿器状态、加热器状态、空调的温度、湿度值。

4）配电柜监控

监测馈线回路和电源进线的电气参数，提供主电源进线及每条分支回路运行的电流、电能及谐波等完整信息。精密配电柜可配合漏电采集单元实现在线漏电监测功能，同时配合温度传感器附件对列头柜内温度进行实时监视，完善了微模块机房供电系统的安全性。

5）温湿度监控

根据机房实际面积，加装温湿度传感器，实时监测机房和机柜的温度和湿度数值，在监控界面上以电子地图的方式直观地显示现场的温湿度，并可对温湿度进行实时和历史查询。

并且当机房的温湿度超过预定值时，系统将对管理人员电话短信报警；管理人员则可通过远程监控系统对机房内的空调进行调节，以完成对机房的控制。

6）漏水检测

系统本身包括：漏水控制器、漏水感应绳及其他辅助设备，系统可检测感应线上任何点的漏水位置并有语音报警。系统还可检测机房洁净度，当感应上的尘埃集结到一定厚度，系统会报警提示管理人员派人清洗感应线。

7）消防检测

设计对机房内由消防控制箱提供的干接点信号（在机房内安装烟感探测器）进行实时火警监测，一旦发生报警通过监控平台发出对外报警。

实时监测机房内的消防火警信号，一旦发生报警，系统自动切换到相应的监控界面，且火警状态图标变红闪烁显示，同时产生报警事件进行记录存储及有相应的处理提示，并第一时间发出手机短信、声光等对外报警。

**2.9.10.机房安防系统**

**2.9.10.1.视频监控**

设计在机房出入口、机柜间的通道、走廊等重要区域安装彩色半球摄像机、硬盘录像机，进行全天候的视频图像监视。

彩色半球摄像机通过视频线直接接入到监控主机的视频输入接口（硬盘录像机，同时将硬盘录像机接入与监控主机相同的内部网络中），通过监控平台软件进行图像监控。

**2.9.10.2.门禁系统**

出于对机房安全的考虑，设计对机房门进行门禁管理，采用进门刷卡、出门按按钮的进出验证方式，由监控平台软件进行机房出入的门禁管理。

通过网络门禁控制器设备提供的TCP/IP接口及通讯协议，采用网络的方式将门禁信号接入监控主机，由监控平台软件进行门禁的实时监测。

**2.9.11.机房消防系统**

机房的自动消防灭火系统主要由探测器、控制器、执行装置和灭火容器组成。工作原理大致为：由装在机房内的烟感探测器感应到物质燃烧时生成的烟雾或由温感探测器感应到周围空气温度升高而发出声光报警，同时将信号送到执行装置。执行装置收到信号后，开始切断电源、关闭风门，并通过延时器延长一短暂时间，以便人员在灭火器启动前撤离。然后以此电信号启动电磁阀（或电磁撞针）打开氮气施放筒，由氮气气体来打开灭火剂药瓶的气动阀门，灭火剂顺着预先设置的管道至喷口喷出，直到喷完为止。

系统设备选用七氟丙烷自动灭火系统。

系统构成：本系统由火灾自动报警系统、灭火控制系统等系统组成。

**2.10.安全体系建设**

本项目按照《信息安全技术网络安全等级保护基本要求》二级的标准建设。要求结合等级保护2.0相关标准和要求，从保障用户业务安全高效运行为根本出发点，进行网络安全体系方案设计。以安全能力模型支撑，为用户构建以技术、管理和运营三大安全体系为目标的可运营的智能化安全体系，让等级保护对象具备安全可视、持续检测、协同防御的能力。

**2.11.本项目利旧设备**

为保护政府投资，整合现有系统和设备，本项目将充分利用旧有设备，达到节约投资的目的。本次拟利旧设备如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **品牌** | **数量** | **备注** |
| 1 | 人脸识别一体机 | 海康DS-K1T671M | 78 | 测温系统，做为人员通道的人脸识别 |
| 2 | 流媒体服务器 | 海康DS-VM11S-B/ISC | 1 | 测温系统，做为本次安防设备联网平台的流媒体转发 |
| 3 | 测温管理平台 | 海康iSecure Center-Education | 1 | 测温系统，扩容改造后做为本次安防设备联网平台 |
| 4 | 访客机 | 海康 1台灵峰 6台易天 1台 | 8 | 校方安装，本次接入 |
| 5 | 人员通道闸机 | 海康、掌通家园、麦兴 | 23 | 校方安装，本次接入 |
| 6 | 车辆抓拍机 | 海康、捷顺、创通、龙联、红门 | 8 | 校方安装，车辆抬杆利旧 |
| 7 | 校园出入口智能抓拍机 | 海康 | 按需 | 公安建设，做为资源共享接入区教育局平台 |
| 8 | 校园内部监控 |  | 按需 | 设备联网接入区教育局平台，同时推送至区视频资源共享平台 |

**二、采购清单及参数**

**一、校园智能安全防范信息平台采购清单**

**1.1采购清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **分项名称** | **技术要求** | **数量** | **单位** |
| **（一）校园安全风险防控大数据指挥中心** |
| 1 | 总体态势大数据 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 2 | 重点防范大数据 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 3 | 风险预警大数据 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 4 | 在线督导大数据 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| **（二）校园智能安全防范信息平台建设** |
| 1 | 首页门户系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 2 | 数据直通系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 3 | 智安动态系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 4 | 安全教育系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 5 | 日常防范 | 通知消息系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 6 | 安全文件（任务）系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 7 | 隐患排查系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 8 | 专项检查系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 9 | 重点防范 | 交通及校车管理系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 10 | 学生防溺水管理系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 11 | 学生防欺凌管理系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 12 | 外出活动管理系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 13 | 传染病防治管理系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 14 | 消防安全管理系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 15 | 周边治安管理系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 16 | 应急处置系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 17 | 智安物联系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 18 | 基础支撑系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 19 | 接口对接服务 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 项 |
| **（三）校园体温实时监测管理系统模块** |
| 20 | 体温实时监测管理系统 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 套 |
| 21 | 体温设备管理平台 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 项 |
| 22 | 体温实时监测家长端 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 项 |
| 23 | 体温实时监测教师端 | 详见“校园智能安全防范信息平台技术参数要求” | 1 | 项 |
| ★其他技术要求：依据《关于做好与宁波市校园智能安全防范信息平台数据对接工作的通知》（甬教安体〔2020〕105号）的相关要求，为保证平台的兼容性与整体性，投标人所投系统应该完全响应招标技术参数需求，并承诺按照文件要求将数据接入至宁波市校园智能安全防控信息平台。若投标人无法实现对接的，业主有权更改平台服务商。承诺5年平台免费升级优化服务，提供承诺函。 |

**1.2校园智能安全防范信息平台技术参数要求**

|  |  |  |
| --- | --- | --- |
| **序号** | **分项名称** | **采购技术参数要求** |
| **一、校园安全风险防控大数据指挥中心** |
| 1 | 总体态势大数据 | 安全态势大数据能够对下属学校校园安全事前、事发、事中、事后管理中的规范化情况和安全成效情况清晰展示，还可以通过可视化地图实现对下属学校安全态势的逐级查看，能够按月的方式自动计算学校评估得分，能够查看分项得分明细，并生成学校评估排行。一、安全态势大数据1.按照等级平安校园关键指标为应用，能够对教育局、学校等日常关键安全工作监督监管，最终可依据安全平台相应应用积分进行积分排名；2.事前预防能够通过采集的安全大数据、对比安全工作标准规范等方式，自动生成区域学校主动防御建设达标雷达图、食品安全工作学校达标统计、卫生与心理健康工作学校达标统计、学生防溺水工作达标统计、学校欺凌防范工作达标统计、校车管理工作达标统计等，统计结果能够自动生成。支持查看未达标学校及指标详情，并发送整改通知。3.事发风险预警支持汇总显示区域内的学校、教师、学生总数量；可根据区域实时上报的预警风险数量，自动统计汇总生成风险分布状态，能够通过风险四色图清晰的看出各区域安全风险程度；支持通过点击地图相应区域进入下级单位实现逐级管理的功能。4.事中应急处置A.支持通过线上和线下应急预案的一键启动、执行过程录制视频、执行过程记录和执行评分等方式，提供量化应急能力评估的功能。B.支持按照时间轴的形式分析汇总学校应急能力大数据。支持查看下属学校的应急演练现场监控、现场直播等；5.事后安全事故管理支持学校安全事故的上报，支持学校安全事件的汇总；支持按照时间轴的形式分析汇总学校安全事故。 |
| 2 | 重点防范大数据 | 重点防范包括持续性重点专项和阶段性重点专项。持续性重点专项应包括智安系统建设、食品安全专项、防溺水专项、防欺凌专项、交通及校车专项、传染病防治、应急处置等规范性工作和执行情况工作监管；阶段性重点专项应包括极端天气、维稳时段的值班安排、值班上报管理，突发事件的应急指挥等情况监管。 |
| 3 | 风险预警大数据 | 1.应具备通过可视化系统查看各学校高风险事件预警的功能，其中风险的类型应包括：人（外来访客黑名单、师生考勤低到校率等），物（重大隐患、超期隐患等），事（安全任务超期反馈、三防巡检未执行等），技（可疑人员抓拍报警、一键报警等）。2.可以通过风险大数据自动统计生成风险预警排名，同时通过风险预警排行信息查看到各预警详细内容，例如有：防溺水预警、学生非正常死亡预警、交通事故、食品与卫生风险预警、校园欺凌预警、校园周边风险预警和消防隐患预警。 |
| 4 | 在线督导大数据 | 在线督导大数据应满足局端对安全任务文件管理、开学时间段（春季秋季）专项检查、等级平安校园评估、安全干部管理。1.安全任务管理应有效督促任务实施，提升实施效率，一方面可管理上级/本级的安全文件，另外一方面可将进行任务反馈的工作任务通知通过安全任务、安全文件发布给学校，学校可以根据任务性质进行执行、转发、反馈等操作，同时教育局能实时查看学校的反馈状态，并对收到反馈工作报告后能够进行在线评价，同时要实时展示未反馈学校。2.开学时间段（春季秋季）专项检查模块可用于春秋季开学安全大数据。检查内容能够在线标准化制订，包括检查项、检查标准及扣分点，保证学校能够依据统一的标准全面开展检查工作，检查出的问题自动生成各学校的整改通知书，帮助针对性改进，同时自动生成所有学校共性问题报告，为下步整改要求和工作重点提供分析依据，提高工作效率、改善问题解决闭环。3.等级平安校园评估模块，依据等级平安校园评估量化标准从多个方面指导学校开展安全工作，同时利用专项检查方式用于年度等级平安校园评定。4.安全干部管理模块具备安全干部信息进行实时化、全面化管理的功能。 |
| **二、校园智能安全防范信息平台** |
| 1 | 首页门户系统 | 支持为教育局提供二级域名安全门户，用户直接输入域名可以浏览对应地市的教体局发布的信息内容；为学校提供统一的学校门户展示，并支持与手机客户端信息同步；1.基础信息：安全门户展示教育局基本信息，包括：机构LOGO、下属机构数量、学校数量、教职工数量、学生数量、监控点、安全干部、保安、平台使用数量等。2.最新动态：展示展示到的上级或者本单位发布的最新通知信息，用户可以点击查看详细内容。3.待办工作：展示当前用户需要做的工作，主要包括：隐患处理、安全巡更、安全任务等，并可以查看下属单位的整体完成情况和详细情况。4.快捷入口：提供快捷操作入口，主要包括安全教育、重点防范、智安物联、数据直通、日常防范、应急处置等。点击快捷入口后会直接进入对应的操作页面，方便用户一键到达。 |
| 2 | 数据直通系统 | 1.数据直通管理数据内容包括：安全干部、安全制度、人防建设、物防建设、技防建设、重点设备、食品安全、校车安全、学生防欺凌、卫生健康、心理健康、危化品、以及在建工程管理共13大类学校基础安全数据。2.支持上级教育部门通过平台可对下属单位13大类学校基础安全数据按区域、按明细实时查看统计，其中按区域可以实时查看统计柱状图和统计表格，可以导出统计表格。3.支持学校端在线按照13大类学校基础安全数据进行文本、图片、附件等数据格式进行学校基础信息填报，并自动进行数据向上级汇聚。4.支持学校端按照等级平安校园评估表进行引导填报，等级平安校园评估表自动依据本地教育系统进行自动评分、自动生成总分，支持按月进行动态评估评分。 |
| 3 | 智安动态系统 | 1.支持将安全信息、安全新闻、安全动态、安全知识等推送到用户终端。2.下属学校、教育局安全负责人可通过移动客户端实时接收，让用户能够随时随地了解安全、学习安全技能、了解安全动态、增加安全防范意识与紧急自救能力。 |
| 4 | 安全教育系统 | 结合安全教育平台的优质安全资源，建设校本安全资源库，实现知识的推送、信息发布、活动发布、安全教育广播和安全授课等功能。1.安全知识库：提供安全知识题库，能支撑学校各类安全点专题检测、随堂检测、知识竞赛、安全广播联动习题检测，安全点涵盖中学应掌握的安全点，题目设计符合中学生知识接受特点，贴近生活，题量不低于4000条。2.安全知识推送：具备通知消息推送功能，实现管理人员对指定的人员进行公共消息发送，包括安全知识、安全提醒、通知公告等。3.安全信息发布：能够将安全信息、安全新闻、安全动态、安全知识等推送到学校，让学校能够随时随地了解安全、学习安全技能、了解安全动态、增加防范意识与紧急自救能力。4.安全活动发布：可以通过通知消息的方式通知用户参加活动。活动方式包括：文档上传、问卷调查、问题讨论、问题辩论等，满足不同组织的不同活动需求。5.安全知识评测：以安全知识题库为基础，提供测评试卷生成功能，支持用户手工组卷、自动组卷、试卷生成策略定义等。用户可以通过手机、PAD、PC等多种方式进行安全知识在线测评，支持顺序做题、随机做题、章节做题等多种方式，测试提交后可以立即获得测评分数，并可以对错误的试题进行查看与纠正。可以满足在线考试、知识竞赛等多种场景使用。6.安全教育管理：应当具备安全教育计划管理、安全教育计划实施等功能。7.安全授课管理：应当具备安全授课计划、安全教材资源浏览、安全授课记录、安全备课等功能，同时需具备pc、移动端的应用。8.安全教育广播：支持安全教育广播任务管理，包括即时广播、定时广播、作息广播、查看广播历史等功能。具备广播资源库、广播模块进行个性化选择。9.安全素养评估：应当具备对教师和学生安全知识、安全技能和安全能力等维度的评估，形成素养评估。10. 能够与宁波市学校安全教育平台对接，能够建立科学化、常态化、信息化的学校安全教育资源共享体系。 |
| 5 | 日常防范 | 通知消息系统 | 1.公共信息发布：教育局、学校管理用户可以通过平台在手机端、PC端下达安全活动通知、安全督导等，支持红头文件及附件、文本、图片、动画、网页等。2.即时通讯交流：支持教育机构用户、学校用户、家庭用户之间的点对点沟通和交流。 |
| 6 | 安全文件（任务）系统 | 1.教育局可以针对下属学校进行工作任务布置，工作任务发布时会以通知消息方式通知指定人群。并可以按照任务查看各个单位的任务执行和反馈情况。2.工作处理接收到任务的单位可以对任务进行反馈处理，反馈时按照需求可以上传附件、填写任务执行情况等。3.工作完成情况查看任务发布单位可以查看各个单位的执行完成情况和反馈信息，可以方便的查看已反馈单位和未反馈单位列表。以及查看任务完成情况与反馈内容。4.处理结果评分任务发布单位可以对已反馈单位的具体执行情况进行点评、批注与打分；评分结果任务执行单位可以在任务列表中进行查看。 |
| 7 | 隐患排查系统 | 1.隐患排查治理应具备安全隐患分级分类、安全隐患治理等功能内容的数据采集、分析；能够按月生成安全巡检、隐患治理等各类台账。2.隐患排查：支持手机扫描二维码直接对安全关键点进行安全排查，并上报排查结果；学校安全负责人能够实时查看排查上报问题，确认是否存在隐患、隐患类型、隐患级别。3.上报隐患：支持以图片、小视频形式上报隐患，指定负责人处理并自动记录；支持分级权限管理，授权用户可通过PC端、手机端查看本校安全隐患记录。4.隐患整改：管理员收到隐患上报信息，审核后可转派到相应的责任人进行处理（支持自动转派），隐患处理人收到提醒后，可在线查看隐患详情并做及时整改。5.隐患验收：隐患整改完成后，支持以图片、文字、视频等形式汇报整改情况，管理员可实时查看，合格可验收通过，不合格可要求重新整改。 |
| 8 | 专项检查系统 | 1.支持局端对下属学校进行专项检查评分的信息化管理。2.支持对下属学校的各类检查项目评分，以及发现问题的汇总。3.支持检查内容自定义、评分标准自定义，支持上级督查、学校自查、部门联查多种检查方式。4.支持检查过程中的多人协作检查方式。5.支持发现问题以拍照、录像、录音等方式记录与上报。6.支持检查结果统计与分析查看，包括：各个被检查单位的分数、问题报告查看，整体合格率分析，问题报告导出。 |
| 9 | 重点防范 | 交通及校车管理系统 | 1.能够对校园校车规范管理、司机规范管理、校车运行管理、月度学校交通巡检、交通及校车类风险预警信息情况汇总展示，能够通过可视化地图查看下属学校情况。2.能够汇总显示下属学校校车总数、校车具体信息（包括车牌号、使用单位、核载人数、承运人责任保险合同期限、使用许可有效期、检验有效期、标配有效期、是否具有卫星定位等），能够自动汇聚未完成校车规范的提醒消息，支持查看、导出明细提醒消息。3.能够汇总显示合法营运从业司机、司机具体信息（包括单位名称、人员名称、驾驶证号、手机号码、校车驾驶资格截止日期等），能够自动汇聚未完成司机规范的提醒消息，支持查看、导出明细提醒消息。4.能够汇总显示校车运行的状态，能够显示校车运行开始时间、结束时间、司机、随车老师等。5.能够汇总显示月度校园交通巡检情况，显示检查时间、检查学校数量、问题数量、风险点及待整改的详细内容，支持查看、导出明细提醒消息。 |
| 10 | 学生防溺水管理系统 | 能够汇总展示下属学校的防溺水执行情况、防溺水学习平台完成率、水域警示巡检情况、区域内防溺水预警等，能够通过可视化地图查看下属学校的情况。 |
| 11 | 学生防欺凌管理系统 | 能够汇总展示下属学校的防欺凌规范管理、学生行为规范管理、学生欺凌心理测评预警管理、重点问题学生档案管理和欺凌事件处置情况，能够通过可视化地图查看下属学校的情况。1.学校防欺凌规范管理需汇总显示下属学校欺凌防治委员会和反欺凌电话公示情况，同时可自动汇聚未按学校规范管理如未公示反欺凌电话的提醒消息，支持查看、导出明细提醒消息。2.学生行为规范管理需汇总显示下属学校学生出勤台帐、校门进出登记台帐、住宿生就寝查铺台帐、违禁刀具管理台帐、学生思想状况分析报告台帐、校园值班巡查台帐执行情况，同时可自动汇聚未按学校学生行为规范管理要求执行学校提醒消息，支持查看、导出明细提醒消息。3.学生欺凌心理测评预警管理需汇总显示下属学校学期欺凌心理测评一、二、三级预警情况，同时可自动汇聚学校学生级别学生的提醒消息，支持查看、导出明细提醒消息。4.重点问题学生档案管理需汇总显示下属区县/学校问题学生人数及档案完备情况，同时可自动汇聚未按要求管控的问题学生的提醒消息，支持查看、导出明细提醒消息。5.欺凌事件处置需汇总显示下属学校按一般欺凌、严重欺凌、涉嫌犯罪欺凌情况，以及下属学校本学期上报事件和处理事件情况，同时可自动汇聚未处置事情的提醒消息，支持查看、导出明细提醒消息。 |
| 12 | 外出活动管理系统 | 支持上级教育部门对学校学校上报的外出活动情况，可在线审核办公，通过以上重点结果管控辅助达成对下属学校对此项安全工作的动态监管。 |
| 13 | 传染病防治管理系统 | 学校能够利用系统对到校学生、教职工进行出勤情况、体温情况按照晨检、午检、晚检要求进行上报管理，并对因病缺勤学生和教职员工实时及时追访和信息上报；局端应能够实时查看上报统计数据、到校体温异常人员及应急处理措施，并可依据上报问题进行监督与指导；学校端上报系统可兼容智能测温柱、智能蓝牙温枪数据自动上报等，可高效提高人工效率。 |
| 14 | 消防安全管理系统 | 1.支持上级教育部门对学校消防安全工作管理情况进行定期监督管理，下属学校可定期按照安全管理项要求进行自查上报。2.消防安全管理项包括：组织建设、消防教育、防火巡查、用火用电、危险物品管理等方面进行消防类隐患自查自检上报。局端通过以上重点结果管控辅助达成对下属学校此项安全工作监管。 |
| 15 | 周边治安管理系统 | 1.支持上级教育部门对学校周边治安工作管理情况进行定期监督管理，下属学校可定期按照安全管理项要求进行自查上报。2.周边治安管理项包括：影响学校安全的工程建设、影响学校安全的易燃易爆等危化品场所、环保不达标污染源、治安复杂区域设有治安岗亭和报警点、上下学时段安排值班校领导值日教师、上下学时段“见警灯、见警力、见警车”、对周边治安高危人群进行摸排、周边有无网吧等游艺娱乐场所、周边餐饮门店有无违法经营行为等方面进行周边安全类隐患自查自检上报。3.局端通过以上重点结果管控辅助达成对下属学校此项安全工作监管。 |
| 16 | 应急处置系统 | 1.安全应急通过将预警、分工引导过程进行任务分解，使用手机端进行实时执行与管控、辅助的应急通讯录、应急线路图、应急现场直播等多种技术手段，为学校安全应急演练及实战提供有力的技术支持。2.应急处置应涵盖应急预案、演练培训、突发事件管理，包括校园内人员伤害突发事件、台风灾害应急处置、暴雨灾害应急处置、低温冰雪灾害天气应急处置、校园涉稳事件应急处置、校园食品与卫生应急处置、校园其它突发事件。3. 值班上报需应用于极端天气、维稳时段的应急值班管理。可实时、动态、直观地查看下属学校的当日学校值班巡检情况；可以采用地图巡检轨迹、巡检拍照、以及巡检记录文字等方式记录应急巡查结果。 |
| 17 | 智安物联系统 | 1.通过统一化数据接口实现校园四大系统（访客登记查验系统、智能抓拍报警系统、人脸识别通道、车辆通行系统）的接入，实现全方位一体化的校园智能安全防范信息平台。2.支持汇总显示下属学校访客管理系统情况，当月访客登记查验情况，同时可自动汇聚提醒消息，包括有未接入学校数量和本周访客查验可疑人员数量，点击提醒消息可查看、导出明细。3.支持汇总显示下属学校接入人脸识别通道情况，当月师生出入数量情况，同时可自动汇聚提醒消息，包括有未接入学校数量和本周一键报警联动处置数量，点击提醒消息可查看、导出明细。4.支持汇总显示下属学校智能抓拍报警系统情况，当月可疑人员智能抓拍情况，同时可自动汇聚提醒消息，包括有未接入学校数量和本周可疑人员抓拍数量，点击提醒消息可查看、导出明细。5.支持汇总显示下属学校车辆通行系统情况，当月车辆进出情况等，同时可自动汇聚未接入学校提醒消息，点击提醒消息可查看、导出明细。6.支持通过统一化数据接口实现校园智能安全防范信息平台数据向上汇聚，支持与110、应急管理中心横向联动。 |
| 18 | 基础支撑系统 | 基础支撑包括安全门基础数据、权限管理、组织架构、统一认证等功能；1.基础数据：支持自定义填写教育局及下属学校组织结构、安全领导小组、教职工和学生信息，为安全防控管理提供数据支撑。2.权限管理：支持教育系统的多级管理，以不同层级教育管理机构、学校管理者、教师、家长为应用对象；支持自定义角色权限分配；不同角色登录后提供不同的功能模块；通过用户中心系统、安全工作事项、待办工作等为教育系统工作者开展安全工作提供个性化工具与服务。3.组织架构：支持教育部门管理、学校的管理、以及学校信息管理、学校部门分类管理、学生信息管理、系统用户管理，支持部门及部门成员分权限的查看。4.统一认证：系统负责对平台用户提供统一认证服务，包括系统配置、授权管理、修改密码、注销用户等。 |
| 19 | 接口对接服务 | 1.具备与市级平台数据对接接口，完成本级安全平台对辖区内下属学校基础安全数据汇总工作并接入市级安全平台。2.数据接入内容应包括学校基础安全数据的接入、校园四大系统数据的接入、等级平安校园管理数据的接入。3.与钉钉的页面整合，支持从钉钉跳转至平台界面（包括PC端、移动端）。 |
| **三、校园体温实时监测管理系统模块** |
| 20 | 体温实时监测管理系统 | 系统架构：必须本地私部署平台功能：平台集班级管理、一卡通、校园教职工体温云监测、家校互动、安全防控、大数据监管为一体，具有查看超温报警通知、24小时实时云监测、体温查看和统计、校园人员体温大数据看板、学生安全定位轨迹查询与紧急求助等功能。为保证平台功能的安全性、及时性、可扩展性，并可作为校园疫情防控综合管理平台，具体模块及要求如下：1、客户端软件支持在安卓手机及IOS手机安装使用，并支持通过微信公众号实现与客户端相同的功能或服务。 2、教师端要求在安卓与IOS手机基础上同时实现PC端WEB登录管理。 3、微信公众号支持校园安全模块，功能包含：实时定位（支持三维二维地图上查看定位信息，支持通话，轨迹查询，远程监护）、电子围栏，远程监护、设备消息、亲情号码、SOS号码设置、低电量提醒、体温监测、计步、心率等。 4、体温24小时实时云监测4.1体温记录 : 支持按照年级、班级、学生、时间、状态查询学生体温，并可导出，支持查看无体温数据及体温异常的学生。4.2发热统计：支持查看实时、每日、每月的发热数据统计及发热人员明细。4.3发热预警：设置学校、班级的大范围发热预警值，设置对应的短信通知校方人员。一旦发生大范围发热，校方人员实时收到短信通知。5、硬件管理5.1上课禁用设置：支持对全校、具体年段进行穿戴式设备的上课禁用设置。5.2人脸上传下发：支持按照班级单个、批量上传学生人脸，并在线完成人脸规范监测，同时自动下发到考勤设备。5.3穿戴式设备状态：查询学校已绑设备的状态，包括设备号、绑定学生、最后连接时间、电量、定位轨迹。5.4设备离线设置：设置学校设备离线的短信告警接收人员。6、学生信息管理：平台可输入或导入学生信息，包括班级、姓名、监管人等信息，方便学校管理。7、学生安全功能：7.1实时定位：可查看孩子的当前实时位置，支持每日历史轨迹查询。7.2电子围栏：可设置多个安全围栏，孩子进入危险区域或离开安全区域，家长接收微信报警推送。7.3远程监护：通过软件发送指令给设备，设备将回拨家长手机号。7.4设备消息：查询设备的围栏报警记录、SOS报警记录、低电量提醒等记录。7.5亲情号码： 支持设置多个亲情家人手机号，设置后自动同步设备端，方便孩子快速联系家长。7.6SOS号码： 支持设置多个一键报警手机号，设置后自动同步设备端，孩子求助后可以自动循环拨打SOS号码，且家长需要收到微信求助提醒。7.7低电量提醒：设置设备的低电量预警值，低于预警值家长需要收到微信提醒。7.8体温监测： 查看孩子的实时体温、每日体温波动情况及发热预警记录，同时孩子发热，家长需要收到微信、短信提醒。7.9计步：查看历史7天内的步数统计。7.10心率监测：查看当日心率监测数据。8、微信消息推送通过微信公众号实现校方重要信息、学生安全信息的消息自动推送服务，包括进出校打卡、班级通知、学校通知、作业通知、成绩通知、请假结果通知、校园待缴费通知、一卡通充值、一卡通补助、一卡通消费、一卡通退款、电子围栏通知、SOS报警通知、低电量通知、异常体温通知。 |
| 21 | 体温设备管理平台软件 | 数据上传 | 已经实现与国内主要业务平台通讯对接；支持socket、web service、Http Post等多种方式上传数据到业务平台。 |
| 多平台分发 | 可以将进出数据同时分发到多个不同的应用平台（无限制） |
| 设备统一实时监控 | 能够对设备进行实时统一的监控;所有设备状态可由后台平台实时监控，和报警;可以实时检测设备连接情况;如果设备发生异常（如：可穿戴设备、信息机故障、网络连接终端），平台都可以获知，并产生报警;能够同时查看所有设备的运行情况，可以查看设备实时的运行状态和数据; |
| 设备管理 | 设备管理平台可以通过Internet实时监控设备运行状态，包括读感器和信息网关。能够实现远程升级 、自动报警、远程参数配置、故障报表。 |
| 设备预警 | 系统有监控、预警机制，能够实现主动反馈。如某学校某天的刷卡率突然出现大幅度增/减的情况（节假日休假除外）。 |
| 异常处理 | 系统能够自动处理业务系统认为有错误的数据，并进行相应的记录。 |
| 22 | 体温实时监测家长端 | 1、登录注册、退出1.1登录注册：手机号快速登录微信公众号，支持学校后台添加的家长直接登录，同时支持未添加的家长自行注册。1.2退出：允许家长自行退出微信公众号。2、孩子管理2.1添加孩子： 学校后台添加的家长无需添加孩子，支持自行注册的家长通过“班级码”或“班主任手机号”添加多个孩子。2.2 解绑孩子：允许家长解除孩子的绑定关系。2.3切换孩子：多个孩子，支持快速选择切换。2.4孩子人脸拍摄：支持家长为孩子拍摄人脸，自动上传。3、设备管理3.1绑定设备：通过扫码、输入设备号等方式快速添加孩子的穿戴式设备。3.2解绑设备：允许家长解除设备的绑定关系。4、通讯录班级通讯录，方便家长查看老师的联系方式，并实现快速拨打功能。5、学生安全5.1实时定位：可查看孩子的当前实时位置，支持每日历史轨迹查询。5.2电子围栏：可设置多个安全围栏，孩子进入危险区域或离开安全区域，家长接收微信报警推送。5.3远程监护：通过软件发送指令给设备，设备将回拨家长手机号。5.4设备消息：查询设备的围栏报警记录、SOS报警记录、低电量提醒等记录。5.5亲情号码： 支持设置多个亲情家人手机号，设置后自动同步设备端，方便孩子快速联系家长。5.6SOS号码： 支持设置多个一键报警手机号，设置后自动同步设备端，孩子求助后可以自动循环拨打SOS号码，且家长需要收到微信求助提醒。5.7低电量提醒：设置设备的低电量预警值，低于预警值家长需要收到微信提醒。5.8体温监测： 查看孩子的实时体温、每日体温波动情况及发热预警记录，同时孩子发热，家长需要收到微信、短信提醒。5.9计步：查看历史7天内的步数统计。5.10心率监测：查看当日心率监测数据。**6.家长端功能通过第三方自愿购买学生端服务才能实现；** |
| 23 | 体温实时监测教师端 | 1、登录、退出1.1登录：老师由学校后台导入后，通过手机号快速登录微信公众号。1.2退出：允许老师自行退出微信公众号。2、个人信息管理2.1教师人脸拍摄：支持自行拍摄人脸，自动上传。2.2身份切换：支持以老师身份登录后切换家长身份使用。3、通讯录3.1班级通讯录：方便老师查找家长的联系方式，并实现快速拨打功能。3.2学校通讯录:：查看学校内所有教职工的联系方式，并实现快速拨打功能。4、教学教务4.1家庭作业：老师快速发布作业，且可查询家长的阅读情况，了解已读未读人员。4.2班级通知：老师快速发布通知，且可查询家长的阅读情况，了解已读未读人员。4.3学生成绩：查看考试的数据统计，包括单科考试、多科考试的最高分、平均分、最低分，优良中差的占比统计、人数统计，学生成绩分数及班级排名。4.4课堂点名：老师上课点名旷课学生，短信通知班主任及家长。4.5教职工通知：支持按照年级、教研组、班主任、部门等分组对全校老师发送通知，并可查看未读、已读人员明细。4.6学校通知：接收、查看学校发布的学校通知。班级管理5.1学生人脸拍摄：支持班主任为本班学生拍摄人脸，自动上传。5.2班级相册：班主任可发布上传班级照片。5.3校园缴费：班主任快速发布班级缴费项目信息，包括缴费金额、缴费时间等，支持查看缴费统计及人员明细。5.4班级考勤：查看学生的打卡时间，了解异常考勤学生名单（迟到、早退、请假、旷课）5.5请假审批：班主任接收家长的请假微信提醒，并在线审批，审批结果实时通知家长。5.6体温监测：查看本班学生的实时体温数据及无体温数据的学生，学生出现发热，班主任收到短信、微信提醒。6、微信消息推送通过微信公众号实现校方重要信息、学生安全信息、家长反馈的消息自动推送服务，包括学生成绩、课堂点名、教职工通知、学校通知、请假待审批通知、学生异常体温通知。 |

**二、前端校园安防系统采购清单**

**2.1采购清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **参考品牌****及型号** | **参数** | **数量** | **单位** |
| **2.1访客登记查验信息管理系统** |
| 1 | 人证访客机 | 海康威视DS-K5022QN-BL、悉点I130G、中控ZKVD01 | 1、高清双屏显示，带有≥15寸电容触摸显示屏和≥10寸液晶显示屏；2、内置≥200万高清摄像头、居民身份证阅读器，支持1：1人证比对功能；3、双网口设计，支持TCP/IP有线网络通讯；4、内置二维码扫描仪，可识别访客单的二维码；5、高速热敏打印机，登记完成后自动打印访客信息凭条； 须包含推送对接模块★设备支持访客黑名单管理功能。★设备具有双网口设计。★设备支持接入教育局原有平台，实现访客信息记录、访客预约、访客黑名单管控等功能。▲访客机需能与人员通道进行联动，将访客人脸下发至人员通道进行刷脸通行。须包含推送对接模块 | 96 | 台 |
| 2 | 人证访客机接入 | 定制开发 | 8台已建访客机的接入，包括对接软件开发等工作。 | 8 | 台 |
| **2.2人员通道管理系统** |
| 1 | 人脸识别终端 | 海康威视DS-K56JQN-BL、正元YT-RS606RL、德亚SA-56RL | 1、设备外观：采用≥7英寸LCD触摸显示屏；≥200万像素双目宽动态摄像头，采用星光级图像传感器，可适应夜间低照度环境；人脸识别距离大于2m，支持照片视频防假；2、设备容量：支持50000张人脸白名单，1：N人脸比对时间≤0.2s/人；支持100000笔事件记录存储；3、认证方式：支持人脸；支持通过RS485或韦根外接读卡器，实现刷卡开闸；支持人证比对（需外接身份证阅读器）；基线支持标准韦根26/34；4、通讯方式：上行通讯为TCP/IP；支持Wifi；5、视频对讲：支持视频语音对讲功能；可接NVR，支持视频预览；6、设备接口： LAN\*1；RS485\*1；韦根\*1；USB \*1；门磁\*1、开门按钮\*1、报警输入\*2；电锁\*1、报警输出\*1；7、使用环境：室内外（防护等级IP65），要求配置遮阳罩；8、安装方式：通道安装；★设备≥7英寸LCD触摸显示屏，屏幕分辨率不小于1024\*600，屏幕防冲击防护等级IK04，除后壳盖板外的外壳防冲击防护等级IK07，支持IP65防水等级。★设备的人脸识别距离：0.2~3m；人脸识别误识率≤0.01%，准确率≥99.8%，人脸识别速度≤0.2s；支持在0.001lux低照度无补光环境下正常实现人脸识别。▲设备支持黑名单功能，本地50000个人脸黑名单比对，支持本地黑名单事件信息上传平台，有授权人员和未授权陌生人刷脸时，设备支持抓拍图片并实时上传平台。★需能与访客机进行联动，接受访客机录入的访客人脸，进行快速的刷脸通行。 ▲设备支持接入教育局扩容后的安防联网平台进行综合管控。 | 234 | 台 |
| 2 | 人脸识别终端（利旧安装） | 利旧 | 现有的78套测温系统人脸识别一体机利旧使用，做为人员通道识别终端；包含安装支架、遮阳罩及调试。 | 78 | 台 |
| 3 | 已建人员通道数据接入 | 定制开发 | 对已建人员通道闸机的6所学校进行设备对接，包括对接软件开发工作。 | 6 | 所 |
| 4 | 左边通道闸 | 海康威视DS-K3B411QN-L、正元YT-RY6288L、德亚SA-805L | 单机芯边道箱，1200\*1020\*200mm /20-60人每分钟，实际通行速率受人员情况和通行模式影响/通道宽度550mm—1400mm，超过1100mm，仅支持金属门翼，另外门翼打开后，门翼超出箱体外/6对红外检测/门翼亚克力、不锈钢可选/室内外/工作电压220V/工作温度范围-20℃~+70℃/标配超级电容，断电开门/翻越报警/分时段管控，最多支持8个时段常开、常闭模式设定/反潜回功能，单通道反潜回，多通道跨主机反潜回/防夹功能/防冲撞★闸机通道采用厚度不低于1.2mm的不锈钢板材；通道应至少采用6对红外对红外对射，能在晴天、雨天等环境下稳定运行，不产生误报 ▲闸机通道应具备防水浸功能，通道在底部积水情况下可正常运行，最大水浸高度不小于150mm★闸机通道门翼开/关速度至少支持10档可调，开门速度＜0.5 s，每分钟最大通达通行人数不低于50人★闸机通道应满足防冲要求，满足机芯保护要求；当门翼受到外力冲撞后，可以迅速恢复到正常状态，恢复时间不超过3s★闸机通道主机可扩展读卡器、二维码、人脸识别组件、指静脉、显示屏等设备集成，可实现多种认证方式组合应用，支持不少于6.3万卡片管理和18万事件记录存储  | 64 | 台 |
| 5 | 中间通道闸 | 海康威视DS-K3B411QN-M、正元YT-RY6288M、德亚SA-805M | 双机芯中间道，1200\*1020\*200mm /20-60人每分钟，实际通行速率受人员情况和通行模式影响/通道宽度550mm—1400mm，超过1100mm，仅支持金属门翼，另外门翼打开后，门翼超出箱体外/6对红外检测/门翼亚克力、不锈钢可选/室内外/工作电压220V/工作温度范围-20℃~+70℃/标配超级电容，断电开门/翻越报警/分时段管控，最多支持8个时段常开、常闭模式设定/反潜回功能，单通道反潜回，多通道跨主机反潜回/防夹功能/防冲撞★闸机通道采用厚度不低于1.2mm的不锈钢板材；通道应至少采用6对红外对红外对射，能在晴天、雨天等环境下稳定运行，不产生误报 ★闸机通道应具备防水浸功能，通道在底部积水情况下可正常运行，最大水浸高度不小于150mm▲闸机通道门翼开/关速度至少支持10档可调，开门速度＜0.5 s，每分钟最大通达通行人数不低于50人 ★闸机通道应满足防冲要求，满足机芯保护要求；当门翼受到外力冲撞后，可以迅速恢复到正常状态，恢复时间不超过3s★闸机通道主机可扩展读卡器、二维码、人脸识别组件、指静脉、显示屏等设备集成，可实现多种认证方式组合应用，支持不少于6.3万卡片管理和18万事件记录存储 | 84 | 台 |
| 6 | 右边通道闸 | 海康威视DS-K3B411QN-R、正元YT-RY6288R、德亚SA-805R | 单机芯边道箱，1200\*1020\*200mm /20-60人每分钟，实际通行速率受人员情况和通行模式影响/通道宽度550mm—1400mm，超过1100mm，仅支持金属门翼，另外门翼打开后，门翼超出箱体外/6对红外检测/门翼亚克力、不锈钢可选/室内外/工作电压220V/工作温度范围-20℃~+70℃/标配超级电容，断电开门/翻越报警/分时段管控，最多支持8个时段常开、常闭模式设定/反潜回功能，单通道反潜回，多通道跨主机反潜回/防夹功能/防冲撞★闸机通道采用厚度不低于1.2mm的不锈钢板材；通道应至少采用6对红外对红外对射，能在晴天、雨天等环境下稳定运行，不产生误报▲闸机通道应具备防水浸功能，通道在底部积水情况下可正常运行，最大水浸高度不小于150mm★闸机通道门翼开/关速度至少支持10档可调，开门速度＜0.5 s，每分钟最大通达通行人数不低于50人★闸机通道应满足防冲要求，满足机芯保护要求；当门翼受到外力冲撞后，可以迅速恢复到正常状态，恢复时间不超过3s★闸机通道主机可扩展读卡器、二维码、人脸识别组件、指静脉、显示屏等设备集成，可实现多种认证方式组合应用，支持不少于6.3万卡片管理和18万事件记录存储  | 64 | 台 |
| 7 | 幼儿园专用人员通道左边道 | 海康威视DS-K3BK4101QN-L、正元YT-RR5243L、德亚SA-803L | 智能安全儿童摆闸，单机芯边道，采用直流无刷电机、4对红外检测传感器，高寿命和高稳定性，支持IC卡、人脸识别终端等认证核验方式扩展，适用于幼儿园出入口使用。 | 53 | 台 |
| 8 | 幼儿园专用人员通道中间道 | 海康威视DS-K3BK4101QN-M、正元YT-RR5243M、德亚SA-803M | 智能安全儿童摆闸，双机芯中间道，采用直流无刷电机、4对红外检测传感器，高寿命和高稳定性，支持IC卡、人脸识别终端等认证核验方式扩展，适用于用于幼儿园出入口使用。进方向含有人脸识别终端，支持幼儿园学生通过人脸进出校园。 | 2 | 台 |
| 9 | 幼儿园专用人员通道右边道 | 海康威视DS-K3BK4101QN-R、正元YT-RR5243R、德亚SA-801R | 智能安全儿童摆闸，单机芯边道，采用直流无刷电机、4对红外检测传感器，高寿命和高稳定性，支持IC卡、人脸识别终端等认证核验方式扩展，适用于幼儿园出入口使用。进方向含有人脸识别终端，支持幼儿园学生通过人脸进出校园 | 53 | 台 |
| 10 | 家长人脸组件 | 海康威视DS-K56JQN-BL、正元YT-RS606RL、德亚SA-56RL | 1、设备外观：采用≥7英寸LCD触摸显示屏；≥200万像素双目宽动态摄像头，采用星光级图像传感器，可适应夜间低照度环境；人脸识别距离大于2m，支持照片视频防假；2、设备容量：支持50000张人脸白名单，1：N人脸比对时间≤0.2s/人；支持100000笔事件记录存储；3、认证方式：支持人脸；支持通过RS485或韦根外接读卡器，实现刷卡开闸；支持人证比对（需外接身份证阅读器）；基线支持标准韦根26/34；4、通讯方式：上行通讯为TCP/IP；支持Wifi；5、视频对讲：支持视频语音对讲功能；可接NVR，支持视频预览；6、设备接口： LAN\*1；RS485\*1；韦根\*1；USB \*1；门磁\*1、开门按钮\*1、报警输入\*2；电锁\*1、报警输出\*1；7、使用环境：室内外（防护等级IP65），要求配置遮阳罩；8、安装方式：通道安装；★设备≥7英寸LCD触摸显示屏，屏幕分辨率不小于1024\*600，屏幕防冲击防护等级IK04，除后壳盖板外的外壳防冲击防护等级IK07，支持IP65防水等级。▲设备的人脸识别距离：0.2~3m；人脸识别误识率≤0.01%，准确率≥99.8%，人脸识别速度≤0.2s；支持在0.001lux低照度无补光环境下正常实现人脸识别。★设备支持黑名单功能，本地50000个人脸黑名单比对，支持本地黑名单事件信息上传平台，有授权人员和未授权陌生人刷脸时，设备支持抓拍图片并实时上传平台。▲需能与访客机进行联动，接受访客机录入的访客人脸，进行快速的刷脸通行。 | 114 | 台 |
| 11 | 配套管线及辅材 | 配套 | 所有强弱电管线配套施工及一切辅材 | 104 | 套 |
| **2.3车辆出入管理系统** |
| 1 | 出入口控制终端 | 海康威视DS-TPEJQN-BLS、德亚TLC-520C，日电CR-300 | CPU：4核CPU处理器 ；内存：4GB，硬盘：2T；其他接口：≥4个1000Mbps自适应网口（支持双网隔离）、2个RS232、2个RS485、4个USB3.0；4个开关量输入，4个继电器开关量输出、1个VGA输出接口，1路内置预留SATA接口、1路音频输入/输出接口、1个HDMI输出接口支持接入的牌识设备数量：4路高清出入口视频单元；存储功能：支持对车辆出入记录的本地存储；平台功能：支持上传至校园安全设备联网平台；远程管理：支持远程进行权限设置或维护管理；★网络接入功能：可直接接入网络。同时支持6路10M/100M/1000M网口、1路4G全网无线通信功能★双IP地址检查：可设置两个独立的IP地址。 ★级联功能：能够支持5个终端同时运行管理独立停车场，无需平台。★固定车过期提醒功能：支持声、光、软件三重报警功能，使管理人员和车主都能及时了解包期规则。▲设备支持接入教育局扩容后的安防联网平台进行综合管控。 | 56 | 台 |
| 2 | 道闸 | 海康威视NP-TMG4B3、德亚TPR-T9，日电Ww-80 | 1个防砸雷达包含：2个遥控器道闸类型：栅栏杆、广告道闸、直杆（根据学校实际需求三选一安装）道闸杆长：4米运行速度：3秒、6秒、1.5-2秒机箱材质：冷轧钢机箱颜色：黑色遥控距离：≥30m输入电压：220VAC+10%电机驱动：交流电机电机功率：90W功能特性：支持外接红绿灯警示、外接红外保护、外接地感功能，支持强冷天气★具有遇阻返回功能：当闸杆下落时，遇到物体阻挡，将立即开闸；★应有自锁手动解除装置，停电时能解脱自锁，实现手动控制功能；★应有自动限位功能，档杆开关到位后，将自动停机限位；★应装有热过载保护装置。 | 48 | 台 |
| 3 | 道闸 | 海康威视NP-TMG4B3、德亚TPR-T9，日电Ww-80 | 1个防砸雷达包含：2个遥控器道闸类型：栅栏杆、广告道闸、直杆（根据学校实际需求三选一安装）道闸杆长：3米运行速度：3秒、6秒、1.5-2秒机箱材质：冷轧钢机箱颜色：黑色遥控距离：≥30m输入电压：220VAC+10%电机驱动：交流电机电机功率：90W功能特性：支持外接红绿灯警示、外接红外保护、外接地感功能，支持强冷天气★具有遇阻返回功能：当闸杆下落时，遇到物体阻挡，将立即开闸；★应有自锁手动解除装置，停电时能解脱自锁，实现手动控制功能；★应有自动限位功能，档杆开关到位后，将自动停机限位；★应装有热过载保护装置。 | 4 | 台 |
| 4 | 车检器 | 海康威视DS-TMG03A、德亚HVD112，日电RB-160H | 独立式,支持接入的最大线圈数2,继电器输出★具有485接口、2路继电器开关量输出接口；★支持接入2路线圈；★支持灵敏度可调：有4级可设（高、中高、中低、低）； | 104 | 台 |
| 5 | 地感线圈 | 海康威视DS-TMG023、德亚HVD110，日电RB101 | 0.75mm²，绞合导体，镀锡铜，绝缘蓝色PVC外被，1捆线圈50米。 | 208 | 捆 |
| 6 | 立柱 | 海康威视DS-PMC142-B、德亚KB17，日电CB17 | 立柱高度：1.3米立柱直径：60mm1.3米处可安装一体机0.5米处可安装LED显示屏 | 124 | 根 |
| 7 | 出入口视频单元 | 海康威视DS-PMC142、德亚TPR-500D，日电TD-116 | 高清晰：200万像素高清摄像机，分辨率：1920\*1080，帧率：25fps；低照度效果：1/1.8""逐行扫描CMOS，成像效果好，0.002Lux星光级监控效果，夜间看的更清；集成度高：内置2颗LED补光灯，集摄像机、护罩、LED补光灯、镜头、电源适配器于一体调试方便：采用5.2-13mm电动变焦镜头，支持软件自动调焦，调试更加方便，场景适应性强；接口丰富：可直接控制道闸开/关，支持外接报警设备；智能识别算法：丰富的智能识别算法，支持车牌、车型、车标、车身颜色识别；黑白名单控制：支持黑、白名单的导入及对比，可直接联动道闸开闸，支持脱机运行；多种触发模式：支持线圈触发、视频触发、雷达触发、线圈结合视频触发等多种触发模式；可显示信息：置于停车场出入口显示欢迎信息、发布中心下发信息等显示字体：显示标准的中文和数字字符。显示内容：可以是整个车库的空余车位余数，车牌号码，收费金额。可根据上位计算机发出的指令显示不同内容内置语音模块：可通过抓拍机支持预录语音播报，车牌号码和收费金额等。 | 124 | 台 |
| 8 | 出入口显示屏 | 海康威视DS-PMC142、德亚HMD601 ，日电TD-05 | 室外显示屏LED亮度:1200cdLED角度:110°外框材料:铁框喷塑，显示部分要求深色钢化玻璃安装方式:背面抱箍喇叭规格:4Ω10W防护等级:IP65点距:P4.75基色:1红1绿下行通讯方式:RJ45显示方式:即显、左移、上移、上展开、下展开等显示方式字符显示:支持GB2312字符集，支持16×16点阵常用汉字通讯距离:RJ45 120米功能特性：四行，四字，双色，带语音模块及音箱，出入口室外显示屏 | 124 | 块 |
| 9 | 配套管线及辅材 | 配套 | 所有强弱电管线配套施工及一切辅材 | 1 | 项 |
| **2.4重点部位监控联网** |
| 1 | 校园内部重点部位监控接入 | 定制 | 1、所有学校透明厨房监控接入区教育局的设备联网平台2、校园内部重点部位监控接入区教育局设备联网平台，校门口及人员通行的主要出入口、食堂（配菜间、厨房等）、实验室（危化品室）、.配电机房、财务室、餐厅（学生、教职工就餐区域）、宿舍、体育场所、图书馆等学校重点区域；3、原有视频按GB28181或Onvif协议接入4、含接入设备及施工管线。 | 104 | 所 |
| 2 | 中心存储设备（透明厨房） | 海康威视DS-A71048R、戴尔ME4012、浪潮NF5468M5 | 机架式/8U48盘位/48块6T企业级SATA磁盘/可接扩展柜/≥1500Mbps接入带宽/64位多核处理器、4GB（标配，可扩展至32G）2个千兆数据网口（可扩展至4千兆或2万兆网口），1个千兆管理网口/冗余电源/支持流媒体1:1:1接入存储转发/视频流、图片、SMART、视频文件混合直写/智能事件检索、精确定位、浓缩播放/RAID 0、1、3、5、6、10、50，60/网络协议：RTSP/ONVIF/PSIA/SIP（GB/T28181）▲单设备应标配≥2个千兆网口，可增扩≥4个万兆口或≥8个光纤接口或增配≥4个HDMI接口或≥2个SAS3.0接口，可扩展2个SSD固态硬盘★提供多设备同步升级功能，可以通过一键式操作对整个局域网内的所有设备同步升级。★设备可同时支持视频、图片、智能流和文件直写存储。★可对指定的录像段或指定事件的1个或多个前端的不同时间段的录像段添加标签，并自动备份到存档卷中，使之不会被覆盖删除。★可通过IE浏览器对一台、多台样机或扩展柜中的磁盘进行定位，使对应的磁盘指示灯闪烁，闪烁的时长可设。▲设备满足教育局扩容后的安防联网平台对存储进行调用和管理。 | 4 | 台 |
| 3 | 24口交换机 | 锐捷RG-S1930-24T4SFP、华三LS-3600V2-28TP-EI、华为S3700-28TP-SI-AC | 1、支持固化百兆电口≥24个，固化千兆光口≥4个，标准1U设备;2、交换缓存≥4.1Mbit3、★内存≥256MB，交换容量≥64Gbps，包转发率≥9.6Mpps4、支持 MAC地址容量≥8K；支持ACL条目≥12005、支持生成树 STP / RSTP ; 提高容错能力，保证网络的稳定运行和链路的负载均衡，合理使用网络通道，提供冗余链路利用率。6、★ 支持防环路检测，自动解决环路问题7、支持静态链路聚合8、支持端口镜像，一对一镜像，多对一镜像9、★支持DHCP Snooping；很好的避免了上网终端从非法DHCP服务器分配的IP地址，引起的网络异常或安全隐患10、支持VLAN划分，最大支持4094个VLAN11、★支持高效节能以太网（EEE），端口如果在连续一段时间之内空闲，系统会将该端口设置为节能模式，当有报文收发时再通过定时发送的监听码流唤醒端口恢复业务，达到节能的效果12、★支持防雷等级≥6KV13、支持QOS，支持端口流量限速；14、★支持和云管理，远程管理和维护设备,支持极速智能配置15、支持多种管理方式，中文WEB界面；16、支持标准的ACL、支持基于IP/MAC扩展的ACL；17、支持CPU安全保护策略(硬件CPP)18、★支持自组网，支持云端管理。19、提供电信设备进网许可证证书复印件；20、提供国家强制认证CCC认证书复印件；21、★工作温度范围-0ºC ~ 50ºC，提供官网截图22、每台配置2块千兆单模光模块。 | 93 | 台 |
| 4 | 24口交换机（无教科网幼儿园） | 锐捷RG-S5310-24GT4XS、华三LS-5130-30C-HI、华为S5720S-28X-SI-AC | ★1、交换容量≥330Gbps，转发性能≥126Mpps，若官网有大小两个指标以小的为准★2、固化10/100/1000M以太网端口≥24，固化10G/1G SFP+光接口≥4个★3、支持可拔插双模块化电源，配置一块电源模块。4、支持静态路由、RIP/RIPng、OSPFv2/OSPFv3等三层路由协议5、要求所投产品端口浪涌抗扰度≥10KV（即具备10KV的防雷能力）6、支持SAVI功能，可防止地址解析欺骗，7、要求所投设备支持1对1、1对多、多对1和基于流的镜像；且支持RSPAN和ERSPAN8、支持专门针对CPU保护机制的CPP功能，可将送CPU的报文，如ARP报文的速率进行限制，使CPU的使用率降低到15%以内，保障了CPU安全9、支持专门基础网络保护机制，支持多种类型的防护，如ARP防护，当ARP速率超过攻击水线，对有攻击行为的用户进行隔离，保证设备和整网的安全稳定运行10、要求所投产品支持sFlow网络监测技术11、支持虚拟化功能，最多可将9台物理设备虚拟化为一台逻辑设备统一管理，并且链路故障的收敛时间≤30ms12、要求所投产品支持ITU-TG.8032国际公有环网协议ERPS,并且链路故障的收敛时间≤50ms，13、符合国家低碳环保等政策要求，支持IEEE 802.3az标准的EEE节能技术14、具有工信部三层交换机进网许可证15、要求所投产品具备节能环保设计，具有中国质量中心颁发的节能证书，16、要求所投设备支持IPv6 Ready第二阶段认证证书17、支持SNMP、CLI(Telnet/Console)、RMON、SSH、Syslog、NTP/SNTP、FTP、TFTP、Web | 11 | 台 |
| 5 | 机柜 | 国产 | 9U挂墙机柜；19英寸标准；最大沉重量为200公斤，前门为5MM的钢化玻璃 | 104 | 个 |
| **2.5安防设备联网平台（原平台扩容）** |
| 1 | 联网平台 | 原平台扩容 | 支持系统内的组织、人员、车辆、用户、角色、认证、区域等的配置和管理；包含图上监控、事件联动、视频网管、门禁网管、紧急报警、违停球接入等功能。支持前端编码设备的集中管理；支持视频预览、录像回放、图片查看、解码上墙等功能；用于平台对外标准化互联互通（跨网、异构）的组件。支持通用视频联网标准协（GB/T28181）,提供支持其他联网标准的扩展能力为校园安防区域提供门禁服务，支持以人脸为身份识别的核心，对进出人员进行集中管控；支持准确记录识别诸如卡号、车牌号等验证凭据，确保车辆的进出有据可查、可控，保障车辆快速通过道闸，支撑停车场的高效和安全运转支持车辆分组管理；支持放行规则的配置；支持信息记录的查询和统计分析；支持访客认证、来访记录查询、访客权限管理 | 1 | 套 |
| 2 | 访客模块 | 原平台扩容 | 支持访客通过身份证在自助访客机和人工访客机进行认证比对并登记，打印访客单，访客单可自定义设置；支持访客人脸采集，下发设备后进行人脸通行；支持设置门禁点、楼层、门口机、停车场作为门禁、梯控、门口机、停车场权限的权限项，设置的权限项作为访客管理人员设置访客权限组的基础；支持访客在访客机上进行签离；支持查看访客来访记录，可导出来访记录；支持自定义配置短信模板；支持设置访客来访记录保存时长；来访人员可通过钉钉，提前进行来访预约登记；预约后可由对应学校老师进行审批，审批后完成来访预约。 | 1 | 套 |
| 3 | 门禁模块 | 原平台扩容 | 支持对学校人员通道系统进行集中统一管理，支持批量录入、下发人脸权限，对师生进出进行权限管控；支持按组织、按人员分组、按人员配置权限，支持权限配置综合查询功能，可按姓名、工号、所属组织、门禁点、区域配置时间、下载时间等查询人员已配置权限；支持对门禁点分组，便于批量配置权限；支持设定计划模板、假日组，使门禁权限按预先设定的计划、假日组生效；支持查询人员出入事件，可按姓名、工号、所属组织、门禁点、控制器、门禁点区域、事件时间、事件类型、抓拍图片进行查询；支持人员出入事件的导出和同步功能；门禁事件查询按照部门查询可以查询当前部门以及下级部门的数据支持对门进行开、关、常开、常闭的反控操作，并在客户端界面上反映门当前状态；支持按事件类型进行筛选查询；支持查看监控人员的进出记录事件，可全屏显示；事件内容包含以下信息：A、时间：人员在门禁点的进出认证时间；B、门禁点：发生该事件的门禁点位；C、持卡人信息：包括姓名、证件号码、所属部门、照片；E、进出方向：出/入；▲实现将学生每日进出人脸通道的事件信息推送至钉钉，对应学生家长可通过钉钉进行查看。 | 1 | 套 |
| 4 | 车辆模块 | 原平台扩容 | 支持展示已添加在平台的车辆信息；支持添加车辆信息，批量导入车辆信息、批量导出车辆信息；支持通过车牌号码、车主姓名、车辆类型、车牌类型、是否关联车主选项查询车辆信息； 支持配置停车库总车位数量，剩余空车位数量，固定车位和预约车位的数量；车辆信息及查询条件增加所属组织、停车库、有效期状态支持对空余总车位数、空余固定车位数进行手动矫正；支持按照车牌、卡号、停车库、出入口、开始时间、结束时间、过车方向、放行结果、车辆类型、黑名单、车辆分类、放行原因这些选项查询过车记录；支持按照车牌号码、卡号、停车库、放行方式、识别准确度、车辆类型、停车时段、停车超过多少时间这些选项查询停车场内停车信息；支持反控道闸开、关、常开； | 1 | 套 |
| 5 | 数据联网模块 | 原平台扩容 | 支持采集门禁的资源和事件(设备事件、人员出入事件)支持将门禁的事件、资源通过CSV、开放接口、中间数据库等方式发布给第三方平台支持采集访客来访记录信息和访客门禁事件支持将访客来访记录信息、访客门禁事件通过CSV、开放接口、中间数据库等方式发布给第三方平台支持采集停车场的资源(停车库、出入口、车道）、余位、过车数据、固定车有效期支持把停车场的事件、资源通过CSV、开放接口、中间数据库等方式发布给第三方平台 | 1 | 套 |
| 6 | 视频模块 | 原平台扩容 | 支持GB28181、Onvif等通用协议支持预览窗口布局切换，包括1、2、3、4、6、8、9、10、13、14、16、17、24、25布局模式，可实现预览画面自适应和全屏切换设置；支持监控画面中紧急录像、即时回放、主子码流切换、声音开启/关闭；支持监控画面显示码流信息（帧率，分辨率，编码格式分装格式、主子码流类型）；支持辅屏预览（1个辅屏）；支持预览画面中显示热成像设备温度信息；支持视频轮巡分组增加，删除，修改及搜索；支持轮巡分组设置（轮巡时间间隔，轮巡窗口个数设置，轮巡监控点添加、删除和轮巡顺序设置）；支持轮巡暂停、开始、切换操作；支持监控点计划模块设置（全天候模式、工作日模式、周末模式及自定义模式）；支持监控点录像计划设置和存储模式设置（设备存储、中心存储）；支持按存储模式（设备存储、中心存储）进行取流切换；支持录像流控操作（正放、倒放、快进、慢放、单帧播放，拖动进度条）；支持多画面播放时同步回放和异步回放切换；支持录像下载、录像剪辑、录像标签、录像锁定设置；支持录像播放时声音开关闭，录像抓图，录像画面关闭，全屏播放操作； | 1 | 套 |
| 7 | 事件接收联动模块 | 原平台扩容 | 支持实时展示平台各子系统视频监控、一卡通、车辆管理、报警检测、网络管理触发的事件信息；支持对报警事件做已处理标记；支持对报警事件进行批量处理；支持对历史事件进行查询，并且可以按照以下条件事件类型、规则名称、所属区域、位置、事件源、事件等级、开始时间、结束时间、处理意见、处理状态进行筛选查询；支持将查询出的历史事件信息导出成文件；支持查看历史事件联动详情，包括联动预览、联动录像回放、联动抓图；支持事件详情页面同时查看预览和回放画面；支持在默认模板或者自定义模板基础上配置事件规则；支持指定事件触发条件：区域、位置、事件源；支持事件规则计划模板按全天候模式、工作日模式、周末模式及自定义模式配置；支持指定事件发生的类型：视频事件、热成像报警事件、入侵报警事件、IO事件、门禁事件、停车场事件、人脸识别事件； | 1 | 套 |
| 8 | 数据对接共享 | 原平台扩容 | 1、支持重点部位视频、访客登记、车辆进出、人员进出数据可与治安内保平台进行数据对接，将相关信息同步至治安内保平台。且平台具有开放的接口能力，第三方可根据开放接口进行视频取流、访客、车辆、人员通行事件的获取。2、与本次信息平台对接，根据市教育局《安全防范信息平台数据接入管理办法》要求提供接口、共享数据；3、实现与区视频资源共享平台对接，实现重点部位视频监控向区视频资源共享平台推送，根据设备一机一档管理要求，须包含平台对接网关；4、实现与区公安分局公共安全视频联网平台对接，接入公安侧已建的校园门口智能抓拍设备。5、实现访客预约、学生进出学校的事件信息在钉钉端的业务应用。 | 1 | 项 |

**三、支撑平台及网络安全采购清单**

**3.1采购清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **参考品牌****及型号** | **参数** | **数量** | **单位** |
| **3.1支撑平台** |
| 1 | 平台管理服务器 | 海康威视DS-VM21S-B、戴尔PowerEdge R940xa、浪潮NF5270M5 | HG7169(24核2.2GHz)×1/64G DDR4/600G 10K SAS×4(RAID\_10)/SAS\_HBA/1GbE×2/550W(1+1)/2U/16DIMM2U单路标准机架式服务器CPU：1颗 HG7169(24核，2.2GHz)内存2\*32G DDR4，16根内存插槽，最大支持扩展至2TB内存硬盘：4块600G 10K 2.5英寸SAS盘可选支持12块3.5寸(兼容2.5寸)热插拔SAS/SATA硬盘可选支持2块后置2.5寸热插拔SAS/SATA硬盘可选支持4块NVME U.2热插拔硬盘支持1个M.2插槽支持1个TF插槽阵列卡：标配SAS\_HBA卡，支持RAID0/1/10可选RAID\_2G卡，支持0/1/5/6/10/50/60，可选支持断电保护PCIE扩展：最大可支持6个PCIe扩展插槽网口：2个千兆电口其他接口：1个千兆RJ-45管理接口，4个USB 3.0接口，2个位于机箱后部，2个位于机箱前部1个VGA口，位于机箱后部电源：标配550W（1+1）白金冗余电源支持200-240V 50/60Hz AC/HVDC | 2 | 台 |
| 2 | 超融合一体机 | 深信服aServer-P-2205、华为RH2288V5、华三UIS-Cell 3000 G3 | 详见“支撑平台技术参数要求” | 5 | 台 |
| 3 | 统一管理软件 | 深信服aCloud、华为FusionCube Center、华三UIS-Manager | 详见“支撑平台技术参数要求” | 10 | CPU |
| 4 | 计算服务器虚拟化软件 | 深信服aSV、华为FusionSphere、华三CAS | 详见“支撑平台技术参数要求” |
| 5 | 网络虚拟化软件 | 深信服aNET、华为物理网络、华三UIS-Net | 详见“支撑平台技术参数要求” |
| 6 | 虚拟存储软件 | 深信服aSAN、华为FusionCube、华三UIS-OneStor | 详见“支撑平台技术参数要求” |
| 7 | 管理电脑 | 华为、联想、HP | [第十代i5 CPU 13.9英寸全面屏笔记本电脑轻薄商务3K触屏超极本](https://detail.tmall.com/item.htm?id=591863083175&standard=1) | 1 | 台 |
| **3.2网络安全系统** |
| 8 | 下一代防火墙 | 深信服AF-2000-B2150、锐捷RG-WALL 1600、华三H3C SecPath F1080 | 详见“下一代防火墙技术参数要求” | 1 | 台 |
| 9 | 防火墙 | 深信服AF-1000-B1300、锐捷RG-WALL 1600-E、华三H3C SecPath F1050 | 详见“防火墙技术参数要求” | 1 | 台 |
| 10 | 网闸 | 深信服GAP-1000-C640、华三H3C SecPath GAP2000-B、绿盟SIES 3000A | 详见“网闸技术参数要求” | 1 | 台 |
| 11 | 日志审计系统 | 深信服LAS-1000-A600、绿盟LASNX3-L3000、华三H3C SecPath AK640 | 详见“日志审计技术参数要求” | 1 | 台 |
| 12 | 运维审计系统 | 深信服OSM-1000-A600、华三A2020-G、绿盟NSFOCUS OSMS NX3 600C | 详见“运维审计技术参数要求” | 1 | 台 |
| 13 | 数据库监控与审计系统 | 深信服DAS-1000-A620S、华三D2020-G、绿盟NSFOCUS DAS NX5-E6000C | 详见“数据库监控与审计技术参数要求” | 1 | 台 |
| 14 | 防病毒软件 | 深信服 终端检测响应平台EDR、江民 杀毒软件网络版 V16.0、360天擎终端安全管理系统 | 详见“防病毒软件技术参数要求” | 20 | 点 |
| 15 | 备份一体机 | 杭州美创 备份一体机B-B5000、北京合力极易 数据宝备DB1000、杭州容错 ENAS-288 | 详见“备份一体机技术参数要求” | 1 | 台 |
| 16 | 汇聚交换机 | 锐捷RG-S5750C-48GT4XS-H、华三LS-5560-54C-EI、华为S5730-60C-HI | ★1、固化端口：≥48个10/100/1000Mbps电口，≥4个SFP+光口，最大支持万兆光口≥8个。★2、设备可提供2个电源模块插槽、2个扩展槽，要求提供官网截图。配置4万兆光口板卡，配置双电源。★3、交换容量≥736Gbps，包转发率≥252Mpps（以官网最小值为准，要求提供官网截图）4、工作温度0-50°，要求提供官网截图。5、整机采用绿色环保设计，满负荷情况下电源功率≤50W，要求提供官网截图。6、为提升设备适应环境的能力，保证寿命更长，要求所投产品必须涂装三防漆，充分提升设备防腐蚀能力，符合GB-T2423.51标准；7、要求所投设备MAC地址≥64K，ARP表项≥20K，FIB表项≥12K。8、支持RIP，OSPF，BGP，RIPng，OSPFv3，BGP4+9、支持IGMP v1/v2/v3，IGMP v1/v2/v3 Snooping，支持PIM-DM，PIM-SM，PIM-SSM，PIM for IPv610、支持专门基础网络保护机制，增强设备防攻击能力，即使在受到攻击的情况下，也能保护系统各种服务的正常运行，保持较低的CPU负载，从而保障整个网络的稳定运行。11、要求所投产品支持sFlow网络监测技术，可提供完整的第二层到第四层信息，可以适应超大网络流量环境下的流量分析，让用户详细、实时地分析网络传输流的性能、趋势和存在的问题。12、支持虚拟化功能，最多可将9台物理设备虚拟化为一台逻辑设备统一管理，并且链路故障的收敛时间≤50ms（最快8ms）。13、要求所投产品支持ITU-TG.8032国际公有环网协议ERPS,并且链路故障的收敛时间≤50ms。14、符合国家低碳环保等政策要求，支持IEEE 802.3az标准的EEE节能技术。15、支持SNMPv1/v2C/v3、CLI(Telnet/Console)、RMON(1,2,3,9)、SSH、Syslog、NTP/SNTP、FTP、TFTP、Web16、具有工信部IPv4/IPv6 三层设备进网许可证复印件17、要求所投产品支持openflow 1.3协议，具有全球SDN测试认证中心出具的证书18、要求所投设备支持IPv6 Ready第二阶段认证证书 | 2 | 台 |
| 17 | 汇聚交换机（无教科网学校） | 锐捷RG-S6120-20XS4VS2QXS、华三LS-6520-26C-EI、华为S6730-S24X6Q | 1、★整机交换容量≥2.5Tbps、包转发≥570Mpps；2、★配置20个1G/10G SFP+光口，4个1G/10G/25G SFP28光口，2个40G QSFP+端口，2个模块化风扇，2个模块化冗余电源；电源及风扇支持热拔插恢复。3、支持多虚一技术，可将多台物理设备虚拟化为一台逻辑设备统一管理，支持跨设备链路聚合及最快50ms 级故障链路收敛4、支持专门针对CPU的保护机制，能够针对发往CPU处理的各种报文进行流量控制和优先级处理，保护交换机在各种环境下稳定工作。5、支持RIP，OSPF，支持IPv66、★支持静态路由、支持RIP，RIPng、支持OSPFv2，OSPFv3，IS-ISv4，IS-ISv6、支持BGP4，BGP4+、支持等价路由7、支持标准IP ACL（基于IP地址的硬件ACL）、支持扩展IP ACL（基于IP地址、TCP/UDP端口号的硬件ACL）、支持MAC扩展ACL（基于源MAC地址、目的MAC地址和可选的以太网类型的硬件ACL）、支持基于时间ACL、支持专家级ACL （可同时基于VLAN号、以太网类型、MAC地址、IP地址、TCP/UDP端口号、协议类型、时间等灵活组合的硬件ACL）、支持ACL80、支持IPv6 ACL8、支持LACP(802.3ad)9、支持专门基础网络保护机制，能够限制用户向网络中发送数据包的速率，对有攻击行为的用户进行隔离，保证设备和整网的安全稳定运行10、支持同时开启802.1X或WEB认证，CPP、ACL、防ARP欺骗等功能不会相互冲突、制约。11、具有工信部IPv4/IPv6三层设备进网许可证复印件 | 1 | 台 |
| 18 | 万兆多模模块 | 锐捷XG-SR-MM850、华三SFP-XG-SX-MM850-A、华为OMXD30000 | 万兆多模与交换机同一品牌 | 28 | 块 |
| 19 | 万兆单模模块 | 锐捷XG-LR-SM1310、华三SFP-XG-LX-SM1310、华为OSX010000 | SFP+-10G-单模模块(1310nm,10km,LC) ，与交换机同一品牌 | 24 | 块 |
| 20 | 万兆单模模块 | 锐捷XG-SFP-ER-SM1550、华三SFP-XG-LH40-SM1550、华为OSX040N01 | SFP+-10G-单模模块(1550nm,40km,LC) ，与交换机同一品牌 | 6 | 块 |
| 21 | 配套辅材 | 配套 | 光纤跳线、六类跳线、理线架、机打标签、PDU电源等辅材 | 1 | 批 |
| 22 | 等保2.0测评 | 有资质的第三方 | 通过等保2.0二级评测 | 1 | 项 |
| **3.3运营商链路** |
| 23 | 运营商专线 | 运营商 | 1、与区视频资源共享平台对接链路1条；2、与区公安分局公共安全视频监控共享平台对接链路1条；3、与大数据信息中心专线2条；共4条裸光纤，每条裸光纤不少于2芯； | 5 | 年 |
| 24 | 幼儿园教科网专线 | 运营商 | 11所幼儿园教科网链路11条；共11条裸光纤，每条裸光纤不少于2芯； | 5 | 年 |

**3.2支撑平台技术参数要求**

|  |
| --- |
| **超融合硬件要求参数（5台）** |
| **指标项** | **技术指标和要求** |
| ★机箱高度 | ≥2U |
| ★CPU型号 | CPU INTEL Xeon Gold，核数≥12，线程≥24，主频≥2.3GHz |
| ★CPU个数 | ≥2  |
| ★内存 | DDR4，容量≥512G |
| 系统盘要求 | ≥1\*128G SSD |
| ★缓存盘要求 | ≥2\*960G SSD |
| ★数据盘要求 | ≥6\*4T SATA，≥7.2K |
| Raid卡要求 | 支持直通模式  |
| ★标配网口 | 6个GE电口，2个10GE光口 |
| 电源 | 冗余电源 |
| USB接口数量 | ≥2 |
| 质保要求 | ▲5年免费质保。提供7\*24小时技术支持，2小时内快速到现场响应服务。 |
| **云计算管理平台技术要求** |
| **产品** | **指标要求** |
| 云计算管理平台技术要求 | ★本次项目提供10个物理CPU数量的云平台管理授权  |
| 支持定义可用区、跨地域的多集群管理，支持不低于8000台云主机的管理规模 |
| 支持工单功能，用户通过工单可以向云管理员反馈云资源使用所遇到的问题； |
| 支持多租户划分，平台管理员能够为不同的租户分配CPU、内存、存储等资源配额； |
| 提供统一的镜像管理功能，实现各个可用区上镜像的统一创建和管理，  |
| 云资源的申请需要通过管理员审批方可使用，云操作系统支持多级审批流程，可以根据用户实际组织进行自定义 |
| ▲云平台具备对资源池中CPU、网络、磁盘使用率等指标进行实时的数据统计功能，并提供报表功能（需提供产品功能截图）  |
| ▲云计算管理平台，和底层资源池部分的（计算虚拟化、存储虚拟化、网络虚拟化）均为同一厂商品牌提供，并可以支持扩展同一品牌的网络功能虚拟化、虚拟应用防火墙、虚拟应用负载均衡等功能组件，以保障平台的扩展性和兼容性（需提供通过序列号方式扩展产品功能的截图） |
| 支持租户自定义虚拟网络拓扑，并可以在租户网络环境中，配置虚拟分布式防火墙策略。 |
| 支持业务整体可靠性指标的集中展示，包括业务可靠性、平台可靠性和硬件可靠性，方便管理员能直观地掌握整个数据中心的可靠性状态。 |
| 提供符合Openstack的API，满足集成或者二次开发的需求。 |
| ★投标方所提供的软件产品和硬件产品必须为国产品牌；具备解决方案级研发和交付能力，具备自主品牌的全系列硬件产品、软件产品以及原厂服务能力。 |
| ▲5年免费质保。提供7\*24小时技术支持，2小时内快速到现场响应服务。 |
| **超融合技术要求参数** |
| **产品** | **指标要求** |
| 服务器虚拟化及管理 | 要求服务器虚拟化按照物理服务器CPU颗数进行授权，本次提供10颗正版CPU的服务器虚拟化授权 |
| 虚拟机可以实现物理机的全部功能，如具有自己的资源（内存、CPU、网卡、存储），可以指定单独的MAC地址等 |
| ▲支持配置动态资源扩展功能，系统支持自动评估虚拟机的性能，当虚拟机性能不足时自动为虚拟机添加CPU和内存资源，确保业务持续高效运行。 |
| 虚拟化内核基于开源软件KVM底层开发，可维护性好，部署时无需绑定安装OpenStack相关组件 |
| 支持虚拟机的无代理备份，能提供至少100个虚拟机的高性能备份功能，支持至少8T的备份数据容量的许可，可将直接将虚拟机备份到磁盘，并支持生成全新虚拟机的方式进行恢复（需提供产品功能截图） |
| 支持IO重试，当存储出现故障，导致虚拟机无法读取存储数据时，自动挂起虚拟机，避免业务故障。 |
| ▲每个虚拟机都可以安装独立的操作系统，为获得良好的兼容性操作系统支持需要包括Windows、 Linux，并且支持国产操作系统包括：红旗linux、中标麒麟、中标普华、深度linux等（需提供功能截图） |
| 支持在线的带存储的虚拟机迁移功能，保障业务连续性。 |
| 支持虚拟机跨集群的虚拟机迁移，支持在不停机的状态下跨集群迁移。 |
| 支持虚拟机的HA功能，保障业务连续性。 |
| 支持无代理跨物理主机的虚拟机USB映射，对于业务的自适应能力、使用便捷性更佳（需提供产品功能截图） |
| ▲采用分布式管理架构，去中心化，管理平台不依赖于某一个虚拟机或物理机部署，采用分布式架构保障平台更可靠（需提供相关证明材料） |
| 支持平台中的集群资源环境一键检测，对硬件健康、平台底层的虚拟化的运行状态和配置，进行多个维度进行检查，提供快速定位问题功能，确保系统最佳状态。（需提供产品功能截图）  |
| ▲虚拟化的管理平台、可以支持扩展同一品牌的存储虚拟化、网络功能虚拟化、虚拟应用防火墙、虚拟应用交付、SSL VPN软件、数据库审计软件等功能组件的，并支持统一管理，以保障平台的扩展性和兼容性（需提供产品功能的截图） |
| 存储虚拟化 | ★要求存储虚拟化按照物理服务器CPU颗数进行授权，本次提供10颗正版CPU的存储虚拟化授权，不受硬盘容量限制 |
| ▲支持存储虚拟化功能，无需安装额外的软件，在一个统一的管理平台上使用License激活的方式即可开通使用，存储虚拟化与计算虚拟化为紧耦合架构，减少底层开销，提升性能（需提供产品功能截图） |
| 采用分布式架构设计，由多台物理服务器组成分布式存储集群，通过新增物理服务器可以实现存储容量和性能的横向扩展（Scale-Out架构），扩容过程保证业务零中断。 |
| 支持多副本冗余功能，支持2个或以上副本，副本互斥地保存在集群的不同节点，当1个或多个主机或者磁盘故障，确保数据依旧正常访问。 |
| ▲支持数据重建优先级调整，在故障数据重新恢复时，可由用户指定优先重建的虚拟机，保证重要的业务优先恢复数据的安全性。（需提供产品功能截图） |
| ▲支持数据分层，提供好的读写性能，并支持对重要虚拟机提供性能保护。（提供虚拟机重要标记的功能截图证明） |
| ▲支持内存读缓存功能，可以利用物理节点的内存作为读缓存，以提高读性能，实现内存、SSD、HDD三级存储分层（需提供产品功能截图） |
| ▲支持条带化功能，实现分布式raid0的性能提升效果，并且支持以虚拟磁盘为单位设置不同的条带数（需提供产品功能截图，） |
| ▲支持坏道扫描功能，由用户设置扫描的时间段定期对集群的硬盘进行扫描，及时发现潜藏的坏道。（需提供产品功能截图） |
| 支持磁盘亚健康监测，包括PCIE SSD寿命告警、硬盘卡、慢的检测和告警、IO错误告警、RAID卡错误告警等，并支持短信告警。 |
| ▲分布式存储能够提供超高性能，能够提供百万级IOPS和12GB/s以上的带宽能力。（需提供产品功能截图） |
| ▲3台超融合即可支持存储分卷功能，以物理主机为单位划分为不同的存储卷，如高性能卷，大容量卷，全闪存卷等（需提供产品功能截图）  |
| 支持一键清除磁盘功能，实现快速进行数据清理 |
| 支持一键导出虚拟机功能，实现资源一键导出 |
| 支持一键还原已删除的虚拟机功能，可恢复30天内已删除的虚拟机 |
| 为了便于部署关键业务系统，虚拟存储可支持Oracle RAC，支持共享盘，及共享块设备，支持向导式安装，降低部署复杂度。（需提供产品功能截图） |
| 网络虚拟化 | ★要求网络虚拟化按照物理服务器CPU颗数进行授权，本次提供10颗正版CPU的网络虚拟化授权。支持部署虚拟分布式交换机、虚拟路由器、分布式防火墙 |
| ▲通过License激活的方式，实现网络虚拟化功能（分布式虚拟交换机、虚拟路由器、虚拟应用防火墙、虚拟应用负载均衡），支持Vxlan网络和现有的Vlan网络对接，实现虚拟化平台与原有网络的兼容性。（需提供产品功能截图） |
| 可以支持手动指定路由器运行在固定的物理主机上，可以自动将路由器规划到高性能和高网络吞吐的物理主机上 |
| ▲在管理平台上可以通过拖拽虚拟设备图标和连线就能完成网络拓扑的构建，提升运维管理的工作效率。（需提供产品功能截图） |
| 提供虚拟路由器、虚拟交换机等设备的连通性探测功能，（需提供产品功能截图）  |
| 应用性能监控 | 提供大屏展示功能，可直观看到当前整个数据中心业务状态 |
| ▲支持对oracle、sqlserver、Weblogic数据库及中间件监控，实现对数据库的语句的故障定位排错，执行时延分析（需提供相应的产品功能截图） |
| 分布式防护墙 | ▲分布式防火墙能够基于虚拟机进行3-4层安全防护，以虚拟机为单位的安全策略部署，即使改变虚拟机的IP地址信息，安全策略依然生效。（需提供产品功能截图） |
| 维保服务 | ▲5年免费质保。提供7\*24小时技术支持，2小时内快速到现场响应服务。 |
| ★资质要求 | 云厂商拥有ITSS私有云服务能力符合性评估二级认证 |
| 厂商提供的软件或者系统都是厂商自研，非OEM或者采用第三方的产品，要求服务器虚拟化、存储虚拟化、网络功能虚拟化、云计算管理平台为同一品牌，具有相应组件软件著作权 |
| 投标方所提供的软件产品和硬件产品必须具备解决方案级研发和交付能力，具备自主品牌的全系列硬件产品、软件产品以及原厂服务能力。 |
| ▲售后服务要求 | 省内有厂家直属的服务办事机构，提供7\*24小时400电话支持，快速上门服务和2小时内快速响应服务； |
| 提供产品相关的使用和技术培训 |

**3.3下一代防火墙技术参数要求**

|  |  |  |
| --- | --- | --- |
| **项目** | **功能项** | **功能要求说明** |
| 硬件要求 | 硬件平台 | ★产品采用多核并行处理架构。 |
| 性能配置 | 性能要求 | ★网络层吞吐量≥25G，应用层吞吐量≥3G，并发连接数≥2200000，新建连接数（CPS）≥200000，SSL VPN最大接入数≥1000，SSL最大加密流量≥350M，IPSec VPN最大接入数≥1000，IPSec VPN加密速度≥650M。硬件参数：2U，8G内存，64G SSD+1T SATA硬盘，双电源，≥6个千兆电口+2个万兆光口，默认支持2个扩展槽； |
| 基础网络特性 | 部署方式 | 支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。 |
| 链路探测 | ★具备链路故障检测功能，通过ARP、DNS、PING协议等方式检测目标主机的可达性，确认接口链路是否有效，并可自定义检测频率。（需提供产品功能截图证明） |
| 链路聚合 | 具备链路聚合功能，将2个或者更多物理链路组合成一个更高带宽的逻辑链路接口，提高链路带宽和链路可靠性。 |
| 路由功能 | 具备静态路由和多播路由，支持RIP、OSPF、BGP等动态路由协议。 |
| ★支持基于IP地址、端口、地域、协议、应用等维度配置策略路由策略，支持多种负载均衡算法，包括加权、带宽比例、轮询、线路排序等。（需提供产品功能截图证明） |
| 网络服务 | 具备ARP代理功能，对指定地址的ARP请求使用指定接口的MAC地址应答，实现保护内网主机。 |
| 具备标准DHCP服务功能，可为终端统一分配IP地址。 |
| 具备DNS透明代理功能，可将DNS请求重定向至指定的DNS服务器。 |
| 地址转换 | 支持IPv4／IPv6下NAT地址转换，包括支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT， 支持一对一、一对多、多对一等多种转换方式。 |
| 支持NAT64、NAT46 地址转换。 |
| IPv6 | 支持IPv4/IPv6双栈工作模式。 |
| 支持IPv6环境的应用控制策略设置，能针对IPv6的IP地址、服务端口、区域、服务/应用、时间等条件进行应用访问规则的设置。 |
| 支持IPv6环境的安全策略设置，实现入侵防御、防病毒、Web应用防护等等安全功能。 |
| VPN | 支持IPsec VPN、SSL VPN和GRE VPN。 |
| IPSec VPN支持DES、3DES、AES、AES192、AES256等标准加密算法，支持MD5、SHA1、SHA2-256、SHA2-384、SHA2-512等标准HASH算法。 |
| ★IPSec VPN支持智能选路功能，保障业务的高可靠性。（需提供产品功能截图证明） |
| 具备专线备份功能，可在专线策略路由异常情况下，主动切换至IPSec VPN线路，保证网络数据传输的连续性。 |
| 访问控制 | 应用控制策略 | 支持基于区域、IP地址、域名、端口、用户、应用、服务、时间等多个维度设置应用控制策略。 |
| 地域访问控制 | ★支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。（需提供产品功能截图证明） |
| 应用控制 | 应用识别 | 产品内置应用特征识别库，支持不少于3000种应用规则，支持对游戏、P2P下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等类型应用进行检测与控制。 |
| 流量控制 | ★具备基于国家/地区的流量管理功能。 |
| 连接控制 | 支持基于区域和IP地址配置连接控制策略，对特定IP地址设置最大并发连接数，实现内部资源保护和系统资源合理分配。 |
| 用户认证 | 单点登陆认证 | 支持密码、单点登陆等用户认证方式，同时支持自定义例外名单。 |
| 外部服务器认证 | 支持LDAP、RADIUS、POP3等多种外部认证服务器认证。 |
| 安全防护 | DDoS防御 | 支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。 |
| 支持TearDrop 攻击、IP数据块分片传输、Land攻击、Smurf攻击、WinNuke攻击、超大ICMP数据攻击等异常报文攻击防护，支持IP协议异常报文和TCP协议异常报文攻击防护。 |
| 支持ARP欺骗类攻击防护。 |
| URL过滤 | 内置海量互联网URL分类库，支持过滤上千万条恶意URL。 |
| 文件过滤 | 具备文件过滤功能，可对视频文件、音频文件、图片文件、文本文件、可执行文件、驱动文件等类型文件进行安全过滤。 |
| SSL解密 | 支持对HTTPS协议加密会话进行解密分析，支持基于区域、对象、业务类型、服务器IP/端口设置解密策略。 |
| 防病毒 | ★支持对HTTP、HTTPS、FTP、SMB、SMTP、POP3、IMAP协议进行病毒检测和查杀，支持最大16层的压缩文件查杀。（需提供产品功能截图证明） |
| ★支持与云端联动对未知文件进行检测，在设备界面显示云端检测结果。（需提供产品功能截图证明） |
| 具备勒索软件通信防护功能。 |
| 入侵防御 | 产品内置IPS检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过7000种特征规则。（需提供产品功能截图证明） |
| ★具备僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。（需提供产品功能截图证明） |
| Web应用防御 | ▲产品内置Web应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含SQL注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL后门攻击、跨站请求伪造、目录遍历攻击、WEB整站系统漏洞等应用层攻击行为，支持超过3000种Web服务器漏洞特征规则。（需提供产品功能截图证明） |
| 支持对HTTP异常请求协议检测和防护攻击，检测内容包含HTTP请求信息的方法及参数长度等。（需提供产品功能截图证明） |
| 支持基于源IP、Referer、URL等多种组合条件对CC攻击进行检测，检测指标为检测时间和触发阀值。 |
| 具备识别与阻断外部扫描器发起的服务器恶意扫描行为，可对扫描器地址进行自定义封堵。（需提供产品功能截图证明） |
| ★支持服务漏洞检测功能，基于服务器请求和响应内容识别服务器存在的系统安全漏洞和应用安全漏洞。（需提供产品功能截图证明） |
| 支持内容敏感数据防泄露功能，对传输的文件和内容进行检测,支持对银行卡号、手机号码等类型数据防护。 |
| 支持网站防篡改功能，可防止攻击者非授权修改网站目录文件。（需提供产品功能截图证明） |
| ★支持网页恶意链接检测功能，有效识别网页盗链/黑链的行为，避免用户网页资源被滥用。（需提供产品功能截图证明） |
| 产品联动 | 网端云联动 | 具备网端云协同联动功能。 |
| 安全策略管理 | 策略快速部署 | 支持在单条安全策略中可同时启用入侵防御、防病毒、URL过滤、文件过滤、Web应用防护等安全功能。 |
| 策略有效性检测 | 支持应用控制策略有效性检测，保障策略持续优化。 |
| 策略生命周期管理 | ★支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。（需提供产品功能截图证明） |
| 策略优化 | 支持对当前应用控制策略异常分析，包括策略风险访问、策略冗余、策略冲突、策略重合、端口放通过大等问题，并提供相关解决方案便于用户快速调优。 |
| 高可用性 | 双机部署 | 支持主主、主备两种双机模式部署。 |
| 会话同步 | 支持产品配置、会话、用户认证等多种信息同步。 |
| 安全运维管理 | 资产识别 | ▲支持Web服务器自动侦测功能，根据Web服务器在线状态、端口使用状态、Web服务器之间的互访关系生成业务资产列表，同时展示内网资产访问的风险等级。（需提供产品功能截图证明） |
| 终端安全风险分析 | 支持对终端安全风险汇总展示，按照不同风险等级展示终端整体安全状况，并给出解决建议实现风险快速处置。 |
| 服务器安全风险分析 | 支持对Web服务器安全的风险汇总展示，按照业务重要性、风险等级、攻击事件统计等维度展示Web服务器的整体安全状况，并给出解决建议实现风险快速处置。 |
| 攻击事件风险分析 | 支持针对业务攻击事件汇总，展示攻击事件类型TOP5及当前业务命中的全网实时热点事件，支持通过地图区域颜色深浅展示攻击者的分布与数量。 |
| 安全报表 | 产品内置安全报表模板，可定义报表内容，包括网络整体安全状况、服务器安全风险分析、终端主机安全分析等。 |
| 双因素认证 | 支持管理员双因素认证，包含用户名/密码和指纹校验等不同方式。 |
| 网管协议 | 支持标准网管协议SNMP V1、SNMP V2、SNMP V3、SNMP Trap。 |
| 集中管理 | 产品支持接入集中管理平台实现多设备的统一管理，集中管理平台支持硬件和云端两种部署方式。 |
| 支持通过集中管理平台统一配置产品的安全策略，包括但不限于访问控制、入侵防御、防病毒、Web应用防护等安全策略。 |
| 资质要求 | 产品资质 | 要求所投产品具备计算机信息系统安全专用产品销售许可证。要求所投产品具备中国国家信息安全产品认证证书。要求所投产品具备国家信息安全漏洞库兼容性资质证书。要求所投产品具备公安部安全与警用电子产品质量检测中心出具符合《GB/T 28181-2016 公共安全视频监控联网系统新型传输、交换、控制技术要求》的证书或者检测报告。要求所投产品具备中华人民共和国工业和信息化部颁发的《电信设备进网许可证》。要求所投产品具备IPv6 Ready Phase-2认证。 |
| 厂商资质 | 要求所投产品的生产厂商具有中国信息安全测评中心、公安部信息安全产品检测中心、国家版权局、中国软件评测中心之中任意一家机构出具关于“未知威胁检测”的证书或测试报告要求所投产品的生产厂商具备中国信息安全测评中心信息安全服务-安全工程类一级资质。要求所投产品的生产厂商具备中国网络安全审查技术与认证中心的信息安全应急处理一级服务资质。要求所投产品的生产厂商具备中国网络安全审查技术与认证中心的信息安全风险评估一级服务资质。 |
| 其他 | ▲5年免费质保。 |

**3.4防火墙技术参数要求**

|  |  |  |
| --- | --- | --- |
| **项目** | **功能项** | **功能要求说明** |
| 硬件要求 | 硬件平台 | ★产品采用多核并行处理架构。 |
| 性能配置 | 性能要求 | ★网络层吞吐量≥5G，应用层吞吐量≥600M，并发连接数≥1800000，新建连接数（CPS）≥40000，SSL VPN最大接入数≥1000，SSL最大加密流量≥200M，IPSec VPN最大接入数≥1000，IPSec VPN加密速度≥140M。 硬件参数：1U，4G内存，硬件64G SSD，单电源，≥4个千兆电口+4个千兆光口； |
| 基础网络特性 | 部署方式 | 支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。 |
| 链路探测 | ★具备链路故障检测功能，通过ARP、DNS、PING协议等方式检测目标主机的可达性，确认接口链路是否有效，并可自定义检测频率。（需提供产品功能截图证明） |
| 链路聚合 | 具备链路聚合功能，将2个或者更多物理链路组合成一个更高带宽的逻辑链路接口，提高链路带宽和链路可靠性。 |
| 路由功能 | 具备静态路由和多播路由，支持RIP、OSPF、BGP等动态路由协议。 |
| ★支持基于IP地址、端口、地域、协议、应用等维度配置策略路由策略，支持多种负载均衡算法，包括加权、带宽比例、轮询、线路排序等。（需提供产品功能截图证明） |
| 网络服务 | 具备ARP代理功能，对指定地址的ARP请求使用指定接口的MAC地址应答，实现保护内网主机。 |
| 具备标准DHCP服务功能，可为终端统一分配IP地址。 |
| 具备DNS透明代理功能，可将DNS请求重定向至指定的DNS服务器。 |
| 地址转换 | 支持IPv4／IPv6下NAT地址转换，包括支持源地址转换SNAT，目的地址转换DNAT和双向地址转换双向NAT， 支持一对一、一对多、多对一等多种转换方式。 |
| 支持NAT64、NAT46 地址转换。 |
| IPv6 | 支持IPv4/IPv6双栈工作模式。 |
| 支持IPv6环境的应用控制策略设置，能针对IPv6的IP地址、服务端口、区域、服务/应用、时间等条件进行应用访问规则的设置。 |
| 支持IPv6环境的安全策略设置，实现入侵防御、防病毒、Web应用防护等等安全功能。 |
| VPN | 支持IPsec VPN、SSL VPN和GRE VPN。 |
| IPSec VPN支持DES、3DES、AES、AES192、AES256等标准加密算法，支持MD5、SHA1、SHA2-256、SHA2-384、SHA2-512等标准HASH算法。 |
| ★IPSec VPN支持智能选路功能，保障业务的高可靠性。（需提供产品功能截图证明） |
| 具备专线备份功能，可在专线策略路由异常情况下，主动切换至IPSec VPN线路，保证网络数据传输的连续性。 |
| 访问控制 | 应用控制策略 | 支持基于区域、IP地址、域名、端口、用户、应用、服务、时间等多个维度设置应用控制策略。 |
| 地域访问控制 | ★支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。（需提供产品功能截图证明） |
| 应用控制 | 应用识别 | 产品内置应用特征识别库，支持不少于3000种应用规则，支持对游戏、P2P下载工具、聊天工具、网上银行、视频软件、股票软件、木马控制软件等类型应用进行检测与控制。 |
| 流量控制 | ★具备基于国家/地区的流量管理功能。 |
| 连接控制 | 支持基于区域和IP地址配置连接控制策略，对特定IP地址设置最大并发连接数，实现内部资源保护和系统资源合理分配。 |
| 用户认证 | 单点登陆认证 | 支持密码、单点登陆等用户认证方式，同时支持自定义例外名单。 |
| 外部服务器认证 | 支持LDAP、RADIUS、POP3等多种外部认证服务器认证。 |
| 安全防护 | DDoS防御 | 支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood等泛洪类攻击防护，支持IP地址扫描和端口扫描攻击防护。 |
| 支持TearDrop 攻击、IP数据块分片传输、Land攻击、Smurf攻击、WinNuke攻击、超大ICMP数据攻击等异常报文攻击防护，支持IP协议异常报文和TCP协议异常报文攻击防护。 |
| 支持ARP欺骗类攻击防护。 |
| URL过滤 | 内置海量互联网URL分类库，支持过滤上千万条恶意URL。 |
| 文件过滤 | 具备文件过滤功能，可对视频文件、音频文件、图片文件、文本文件、可执行文件、驱动文件等类型文件进行安全过滤。 |
| SSL解密 | 支持对HTTPS协议加密会话进行解密分析，支持基于区域、对象、业务类型、服务器IP/端口设置解密策略。 |
| 防病毒 | ★支持对HTTP、HTTPS、FTP、SMB、SMTP、POP3、IMAP协议进行病毒检测和查杀，支持最大16层的压缩文件查杀。（需提供产品功能截图证明） |
| ★支持与云端联动对未知文件进行检测，在设备界面显示云端检测结果。（需提供产品功能截图证明） |
| 具备勒索软件通信防护功能。 |
| 入侵防御 | 产品内置IPS检测引擎，支持口令暴力破解、僵尸网络、恶意软件、服务器与终端漏洞攻击等检测和防护，支持超过7000种特征规则。（需提供产品功能截图证明） |
| ★具备僵尸网络检测功能，可基于僵尸网络检测引擎发现主机的异常外联行为，并提供威胁等级和非法外联次数作为举证。（需提供产品功能截图证明） |
| Web应用防御 | ★产品内置Web应用攻击检测引擎，支持文件包含攻击、抵御注入式攻击（包含SQL注入、系统命令注入）、信息泄露攻击、跨站脚本（XSS）、网站扫描、WEBSHELL后门攻击、跨站请求伪造、目录遍历攻击、WEB整站系统漏洞等应用层攻击行为，支持超过3000种Web服务器漏洞特征规则。（需提供产品功能截图证明） |
| 支持对HTTP异常请求协议检测和防护攻击，检测内容包含HTTP请求信息的方法及参数长度等。（需提供产品功能截图证明） |
| 支持基于源IP、Referer、URL等多种组合条件对CC攻击进行检测，检测指标为检测时间和触发阀值。 |
| 具备识别与阻断外部扫描器发起的服务器恶意扫描行为，可对扫描器地址进行自定义封堵。（需提供产品功能截图证明） |
| ★支持服务漏洞检测功能，基于服务器请求和响应内容识别服务器存在的系统安全漏洞和应用安全漏洞。（需提供产品功能截图证明） |
| 支持内容敏感数据防泄露功能，对传输的文件和内容进行检测,支持对银行卡号、手机号码等类型数据防护。 |
| 支持网站防篡改功能，可防止攻击者非授权修改网站目录文件。（需提供产品功能截图证明） |
| ▲支持网页恶意链接检测功能，有效识别网页盗链/黑链的行为，避免用户网页资源被滥用。（需提供产品功能截图证明） |
| 产品联动 | 网端云联动 | 具备网端云协同联动功能。 |
| 安全策略管理 | 策略快速部署 | 支持在单条安全策略中可同时启用入侵防御、防病毒、URL过滤、文件过滤、Web应用防护等安全功能。 |
| 策略有效性检测 | 支持应用控制策略有效性检测，保障策略持续优化。 |
| 策略生命周期管理 | ★支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。（需提供产品功能截图证明） |
| 策略优化 | 支持对当前应用控制策略异常分析，包括策略风险访问、策略冗余、策略冲突、策略重合、端口放通过大等问题，并提供相关解决方案便于用户快速调优。 |
| 高可用性 | 双机部署 | 支持主主、主备两种双机模式部署。 |
| 会话同步 | 支持产品配置、会话、用户认证等多种信息同步。 |
| 安全运维管理 | 资产识别 | ★支持Web服务器自动侦测功能，根据Web服务器在线状态、端口使用状态、Web服务器之间的互访关系生成业务资产列表，同时展示内网资产访问的风险等级。（需提供产品功能截图证明） |
| 终端安全风险分析 | 支持对终端安全风险汇总展示，按照不同风险等级展示终端整体安全状况，并给出解决建议实现风险快速处置。 |
| 服务器安全风险分析 | 支持对Web服务器安全的风险汇总展示，按照业务重要性、风险等级、攻击事件统计等维度展示Web服务器的整体安全状况，并给出解决建议实现风险快速处置。 |
| 攻击事件风险分析 | 支持针对业务攻击事件汇总，展示攻击事件类型TOP5及当前业务命中的全网实时热点事件，支持通过地图区域颜色深浅展示攻击者的分布与数量。 |
| 安全报表 | 产品内置安全报表模板，可定义报表内容，包括网络整体安全状况、服务器安全风险分析、终端主机安全分析等。 |
| 双因素认证 | 支持管理员双因素认证，包含用户名/密码和指纹校验等不同方式。 |
| 网管协议 | 支持标准网管协议SNMP V1、SNMP V2、SNMP V3、SNMP Trap。 |
| 集中管理 | 产品支持接入集中管理平台实现多设备的统一管理，集中管理平台支持硬件和云端两种部署方式。 |
| 支持通过集中管理平台统一配置产品的安全策略，包括但不限于访问控制、入侵防御、防病毒、Web应用防护等安全策略。 |
| 资质要求 | 产品资质 | 要求所投产品具备计算机信息系统安全专用产品销售许可证。要求所投产品具备中国国家信息安全产品认证证书。要求所投产品具备国家信息安全漏洞库兼容性资质证书。要求所投产品具备公安部安全与警用电子产品质量检测中心出具符合《GB/T 28181-2016 公共安全视频监控联网系统新型传输、交换、控制技术要求》的证书或者检测报告。要求所投产品具备中华人民共和国工业和信息化部颁发的《电信设备进网许可证》。要求所投产品具备IPv6 Ready Phase-2认证。 |
| 厂商资质 | 要求所投产品的生产厂商具有中国信息安全测评中心、公安部信息安全产品检测中心、国家版权局、中国软件评测中心之中任意一家机构出具关于“未知威胁检测”的证书或测试报告要求所投产品的生产厂商具备中国信息安全测评中心信息安全服务-安全工程类一级资质。要求所投产品的生产厂商具备中国网络安全审查技术与认证中心的信息安全应急处理一级服务资质。要求所投产品的生产厂商具备中国网络安全审查技术与认证中心的信息安全风险评估一级服务资质。 |
| 其他 | ▲5年免费质保。 |

**3.5网闸技术参数要求**

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 系统架构 | 1、采用2+1系统架构即内网单元+外网单元+FPGA专用隔离硬件。不能采用网线等形式直通。2、采用基于linux内核的多核多线程专用SUOS安全操作系统，加固内核。 |
| 产品配置 | 吞吐量1Gbps，最大并发连接数50万。标配提供文件交换、数据库访问和同步、视频交换、组播代理、访问交换等功能模块。2U设备，“双主机+隔离卡”架构，单主机硬件信息：6电4光，内存4GB，硬盘64G SSD，冗余电源 500W。 |
| 管理接口 | 外网端不允许配置任何形式的管理接口，所有管理配置操作均通过专用的网闸内网可信端管理接口进行配置。 |
| 部署模式 | ★设备支持透明、代理及路由三种工作模式，管理员可依据实际网络状况进行相应的部署。（提供功能截图） |
| IPV6、IPV4 | ★支持IPV6、IPV4双协议栈接入  |
| 内置应用 | ▲产品内置各类应用支持模块，无须用户增加投资，功能模块至少包含：邮件模块、安全浏览模块、视频交换模块、数据库访问模块、数据库同步模块、文件交换模块、OPC模块、MODBUS模块、WINCC模块、组播代理模块、用户自定义应用模块等各类应用模块,并可控制相应应用协议的的动作、参数、内容。 |
| 文件交换 | 支持Samba、FTP等多种文件协议，可以实现内网到外网、外网到内网、双向的文件传送。 |
| 支持病毒检测 |
| 支持对文件类型的黑白名单控制，根据文件格式特征进行过滤，并且不依赖于文件扩展名；支持文件内容深度检测，对包含关键字内容的文件进行过滤 |
| 支持增量传输、传输后删除等传输策略；支持目录内子目录同步，子目录级别不受限制； |
| ★支持文件交换容错和告警功能，交换出错能够自动重传，出现异常能够告警提示并记录日志； |
| 可通过专用客户端或共享方式提供安全的文件同步功能 |
| 视频交换 | 支持视频会议 |
| ★支持平台级联和视频点播功能 |
| 支持RTP/RTCP、H.323、H.264等协议。 |
| ★符合GB/T 28181国家标准，支持相关厂商协议规范（提供功能截图） |
| 支持SIP信令控制，可控制云台 |
| 支持海康、大华、华为、华三、公安一所、天地伟业、天视达、宇视、科达、数码视讯、藏愚、合众、汉邦等视频厂商。 |
| 数据库同步 | ★支持Oracle、SQLServer、Mysql、Sybase、DB2、Postgresql等多种主流国外数据库的同步和国产达梦数据库、人大金仓数据库的同步（提供截图） |
| ★支持同构、异构数据库之间的同步，如Mysql同步至Oracle。 |
| 支持字段级数据同步，仅同步表中某几个字段。 |
| ★支持BLOB、CLOB等大字段的同步。 |
| 同步功能由网闸主动发起并完成，无需在数据库安装方软件，支持Windows、Linux、Unix 等多种数据库操作系统，且网闸无需开放端口以杜绝安全隐患； |
| 同时支持客户端方式，提供更高性能的数据库同步。 |
| 支持数据库同步实时日志记录，提供日志审计、查询 |
| 数据库访问 | 支持Oracle、DB2、SyBase、SQL Server、MySql等主流数据库的安全访问，实现内外网之间数据库及表内容安全传输。 |
| ★支持SQL语句控制，如只允许查询，不允许删除等。（提供截图） |
| ★支持任务单独启停管理，不影响数据库同步的其他任务运行。 |
| 支持对访问源地址、目的地址、本机地址和端口的自定义访问控制。 |
| 安全浏览 | ★支持应用层指令控制，如GET、POST、PUT、HEAD、CONNECT等。 |
| 可限制用户行为，如只允许浏览不允许登陆等 |
| 支持代理模式 |
| 支持URL地址过滤，并可限制网页中的Script脚本、ActiveX脚本、java applet等 |
| 支持关键字网页过滤； |
| 支持对下载文件的大小、类型过滤； |
| 邮件交换 | 支持SMTP、POP3协议 |
| 支持病毒检测功能。 |
| 支持邮件地址、附件、主题、内容等进行过滤。 |
| 支持附件大小、附件格式控制；支持发件人、收件人过滤。 |
| TCP应用传输 | 支持TCP应用层数据单向传输的控制，保证TCP应用数据的0反馈，以满足二次防护对数据传输的安全性需求。 |
| 组播代理 | ★系统支持多任务的组播代理功能，可穿透三层交换机网络进行部署，支持PIM协议（提供截图） |
| 工业控制应用 | ★支持OPC协议。支持同步、异步监测数据的传输，只需绑定固定的一个起始端口即可满足动态端口的数据传输。可控制功能代码，比如只允许读取，不能写入等（提供截图） |
| ★支持MODBUS协议，可按照用户需求控制具体功能代码，比如控制线圈、值域范围等（提供截图） |
| 产品资质 | 产品具有公安部《计算机信息系统安全专用产品销售许可证》； |
| 产品具有国家版权局《计算机软件著作权登记证书》 |
| 厂商资质要求 | 厂商具有国家信息安全漏洞库（CNNVD）技术支撑单位等级证书（二级）厂商具有中国信息安全测评中心颁发的信息安全服务资质（安全工程类一级）厂商具有国家计算机网络应急技术处理协调中心颁发的网络安全应急服务支撑单位证书（国家级）厂商具有中国信息安全认证中心颁发的信息安全服务资质，风险评估（一级）厂商具有中国信息安全认证中心颁发的信息安全服务资质，应急处理（一级） |
| 维保要求 | ▲5年免费质保。 |

**3.6日志审计技术参数要求**

|  |  |
| --- | --- |
| **功能指标** | **指标要求** |
| 产品性能 | 内置50个主机审计许可证书；最大可扩展审计主机许可数150 |
| 硬件配置 | 内存大小8GB；硬盘容量64GB minisata+1TB SATA\*2；电源:单电源;尺寸:2U;接口:6个千兆电口; |
| 系统安全 | 支持通过SSL加密对数据传输等进行处理、采用B/S架构，HTTPS访问 |
| 支持对象 | 支持各类设备的日志采集要求，主要包括：安全设备：国内主流防火墙； 操作系统：Linux、Windows、Windows Server、Unix等操作系统；数据库：Oracle、MySQL、SQLServer等；应用系统：如Apache、Tomcat、IIS、Weblogic等；网络设备：主流的路由器、交换机、负载均衡等网络设备等主流网络设备 |
| 采集方式 | 支持Syslog、Syslog-ng、SNMP Trap、文件、WMI、FTP、数据库、镜像流量等方式采集日志，审计中心可以支持多个日志采集器 |
| 标准化 | 支持对日志格式进行标准化操作时，不破坏原始日志内容。从不同设备或系统的日志中抽取相关片段准确和完整地映射至日志的标准字段中，统一格式。 |
| 支持对安全事件重新定级，能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义 |
| 过滤 | 支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件 |
| 归并 | 支持归并技术，一段时间内对重复日志进行归并 |
| 日志查询 | 支持根据设备类型，按日期展示日志的接入情况，包含不同级别日志数量统计；支持精确的专家模式查询，根据页面的指导提示，通过组合查询表达式完成精确查询 |
| ★支持全球地理位置库，支持不同设备相同IP的日志识别。（提供截图） |
| 关联分析 | ▲支持挖掘不同类型、来源于不同设备或系统的日志或安全事件之间可能存在的关联关系，需支持GUI方式的关联规则设置功能，关联的类型包括基于规则和基于统计的。（提供截图） |
| 告警响应 | 支持关联、审计策略命中后定义告警，响应方式包括：SYSLOG、邮件、自定义命令联动第三方设备。 |
| ★支持列表的方式展示告警；告警声音设置；告警过滤策略；支持实时监控，滚动显示实时的日志接入信息。（提供截图） |
| 人员审计 | ★支持定义部门和人员的对应关系，支持定义人员与账号的对应关系。（提供截图） |
| 流量审计 | 支持会话数据解码和分析，支持普通以太头解析、支持PPPoE、VLAN、VLAN QinQ、支持TCP、UDP、ICMP、ICMPv6、SCTP、IGMP等，支持HTTP、DNS、邮件等、支持IPv4、IPv6 |
| ★支持HTTP网页标题、BBS、威胁情报、DGA、搜索关键词的网络会话分类展现（提供截图） |
| ★支持DNS、DGA、解码错误、解码失败、解码超时的网络会话分类展现（提供截图） |
| ★支持TLS会话、数据库会话、工控会话、邮件会话、FTP会话、Telnet会话，即时通讯会话的展现（提供截图） |
| 全文检索 | 支持全文检索功能，能对系统内的对象提供全文检索功能  |
| 用户管理 | 支持根据三权分立的原则和要求进行职、权分离，对系统本身进行分角色定义，如系统管理员只负责完成设备的初始配置，规则配置员只负责审计规则的建立，安全审计员只负责查看相关的审计结果及告警内容；安全管理员只负责完成对系统本身的用户操作日志管理 |
| 厂商资质 | 厂商具有国家信息安全漏洞库（CNNVD）技术支撑单位等级证书（二级） |
| 厂商具有中国信息安全测评中心颁发的信息安全服务资质（安全工程类一级） |
| 厂商具有国家计算机网络应急技术处理协调中心颁发的网络安全应急服务支撑单位证书（国家级） |
| 厂商具有中国信息安全认证中心颁发的信息安全服务资质，风险评估（一级） |
| 厂商具有中国信息安全认证中心颁发的信息安全服务资质，应急处理（一级） |
| 产品资质 | 产品具有公安部《计算机信息系统专用产品销售许可证》 |
| 产品具有国家版权局《计算机软件著作权登记证书》 |
| 维保要求 | ▲5年免费质保。 |

**3.7运维审计技术参数要求**

|  |  |
| --- | --- |
| **功能指标** | **指标要求** |
| 系统部署 | 软硬一体化机架式设备，至少提供6个1000M电口 |
| 可管理资源数≥50个，支持licence扩容 |
| 物理旁路单臂部署，以逻辑网关方式工作；不改变现有网络结构 |
| 系统各模块支持以B/S方式管理，采用https加密方式访问 |
| 支持协议 | 字符协议：SSHv1、SSHv2、TELNET |
| 图形协议：RDP、VNC |
| 文件传输协议：FTP、SFTP、RDP磁盘映射、RDP剪切板 |
| 支持通过协议前置机进行协议扩展，至少支持扩展KVM、Vmware、数据库、http/https、CS应用等 |
| 动作流 | ▲支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入（提供截图） |
| 用户管理 | 支持批量导入、导出用户信息；支持用户手动添加、删除、编辑、设定角色、单独指定登陆认证方式、设定用户有效期 |
| ★用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD域认证、Radius认证等认证方式；并支持各种认证方式和静态口令组合认证（提供截图） |
| 支持从windows AD域抽取用户账号作为主账号，支持一次性抽取和周期性抽取两种方式 |
| ★支持Windows AD域账号与堡垒主机账号周期比对，自动或手动删除或锁定失效的域账号（提供截图） |
| ★内置三员角色的同时支持角色灵活自定义，可根据用户实际的管理特性或特殊的安全管理组织架构，划分管理角色的管理范畴（提供截图） |
| 支持对用户指定限制登录IP、登录时间段（可循环，如每周一到周五9：00-17：00时）等规则，以确保可信用户登陆系统 |
| 支持口令有效期设置，用户账号口令到期强制用户修改自身口令，口令强度必须符合密码策略要求 |
| 支持登陆控制台会话超时时间设置，用户在指定时间内无操作自动注销当前会话 |
| 支持设定访问锁定策略，达到限制主帐号密码输入错误次数和锁定时间的目的 |
| 支持以图形方式查看用户占比、在线用户数量、以及活跃用户 |
| 资源管理 | 支持unix资源、windows资源、网络设备资源、数据库资源、C/S资源、B/S资源 |
| 支持批量导入、导出资源信息；支持手动添加、删除、编辑、查询资源，支持变更默认运维端口 |
| ★支持RDP安全模式（RDP、NLA、TLS、ANY）设置，以适应RDP-Tcp属性中的所有功能配置，包括加密级别为客户端兼容、低、高、符合FIPS标准等加密级别（提供截图） |
| 支持网络设备enable和unix主机su等身份切换的单点登录功能 |
| 支持以柱形图方式查看系统中不同资源所占比例 |
| 运维授权 | 支持一对一、一对多、多对多授权，如将单个资产授权多个用户，一个用户授予多个资产，用户组向资产组授权 |
| ★支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问（提供截图） |
| 支持按授权名称、用户名称、用户账号、资源名称、资源地址、资源账号查询已授权信息 |
| 支持在授权基础上设定双人复核登陆，登录时必须经过第二人授权后才能登录，第二人可通过远程授权或同终端授权两种方式实现授权 |
| ★支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作（提供截图） |
| ▲支持自定义紧急运维流程开启或关闭，紧急运维开启时，运维人员可通过紧急运维流程直接访问目标设备，系统记录为紧急运维工单，审批人员可在事后查看或审批（提供截图） |
| 支持按加密格式导入、导出运维授权数据，方便授权关系备份以及授权数据迁移 |
| 支持生成授权报表和可访问外部资源报表，报表详细展示用户和资源的授权关系，并提供EXCEL、WORD、PDF、HTML等格式导出 |
| 口令策略 | 可以配置口令长度，是否包含字母及字母的长度，是否包含数字及数字的长度，是否包含符号及符号的长度，口令时效性；口令策略还可以配置禁止包含的关键字 |
| 改密计划 | ★支持定期变更目标设备真实口令，支持自定义口令变更周期和口令强度。口令变更方式至少支持手动指定固定口令、通过密码表生成口令、依照设备挂载的口令策略生成随机口令、依照密码策略生成同一口令等方式（提供截图） |
| 支持密码策略设置，可自定义密码复杂程度，可设置密码中包含数字、字母、符号及禁用关键字等内容 |
| ★支持密码文件备份功能，密码文件需密文保存，密码包及解密密钥分别发送给不同管理员保存，并使用专用的解密器才可打开（提供截图） |
| 口令变更至少支持windows系统、网络设备、linux/unix系统、数据库等 |
| 访问控制 | 支持命令黑命单，对字符型设备（如linux/unix/网络设备）的高危命令执行进行阻断，如rm、shutdown、reboot等 |
| ★支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人（提供截图） |
| 支持配置资源访问时间规则，即使授权范围内的资源，需在指定时间范围内才可发起访问，确保运维在可信时间范围 |
| 支持对文件传输类协议进行传输控制，如RDP剪切板、mstsc磁盘映射、FTP/SFTP等的上行、下行控制 |
| ★支持RDP协议的控制台登录控制（提供截图） |
| 运维方式 | ★支持web页面直接发起运维，无需安装任何控件，并同时支持调用SecureCRT、Xshell、Putty、WinSCP、FileZilla、RDP等客户端工具实现单点登陆，不改变运维人员操作习惯（提供截图） |
| 审计日志 | 支持监控正在运维的会话，信息包括运维用户、运维客户端地址、资源地址、协议、开始时间等，并可以实时阻断 |
| 对字符命令方式的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出，并支持通过搜索操作语句或执行结果中关键字定位审计回放 |
| ★图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放（提供截图） |
| 支持运维审计自查询功能，用户可查看自身的运维审计历史 |
| ★支持对FTP/SFTP传输的原始文件进行完整记录，并提供下载取证（提供截图） |
| 支持提供系统内部操作审计，包括管理员和运维用户的登录、登出、对系统的配置操作、账号属性修改等系统管理操作 |
| ★支持运维审计日志在线播放，并且支持离线下载后使用专用离线播放器播放（提供截图） |
| 支持倍速播放、拖动、暂停、停止、重新播放等播放控制操作，并可以指定时间点定位播放位置 |
| 支持自定义报表，可记录审计报表模板，可生成图形报表，并提供EXCEL、WORD、PDF、HTML等格式导出 |
| ★支持标准SNMP v1、v2、v3管理协议，支持syslog等标准日志格式外发（提供截图） |
| IPV6 | ★全面支持IPV6，设备自身可以配置IPV6地址供客户端访问，并且支持目标设备配置IPV6地址实现单点登陆和审计（提供截图） |
| 备份与维护 | 支持手动和自动定期备份配置信息，支持配置信息本地备份及异地FTP备份 |
| 支持系统配置还原，可以还原至任一备份点 |
| 具有日志防溢出功能，当磁盘空间达到阈值时，可设置停止记录审计日志或日志回滚 |
| 管理能力 | 支持NTP系统时间同步配置，保证系统拥有可靠的时间戳 |
| 支持日志数据的外置存储，支持NFS、ISCSI和Windows文件共享协议 |
| cpu工作情况，内存使用情况，磁盘使用情况，网卡使用情况，系统数据库工作情况， WEB服务工作情况，其他关键组件工作情况等 |
| 支持从 WEB管理界面重启、关闭设备 |
| 支持通过WEB界面进行系统升级 |
| ★支持从WEB页面设置多端口绑定，防止单网卡或单网线故障发生（提供截图） |
| 支持WEB页面配置双机热备（HA），保证系统可靠运行 |
| 虚拟化部署 | ★支持云端快速部署，实现远程运维管理的规范化；可按照运维人员数量，调整云端服务器配置，即可实现性能优化（提供截图） |
| 客户端兼容 | ★全面支持Windows、linux、国产麒麟系统、Android、IOS、Mac OS等客户端，实现跨终端适应性BYOD（Bring Your Own Device）（提供截图） |
| 产品资质 | 产品具有公安部《计算机信息系统安全专用产品销售许可证》； |
| 产品具有国家版权局《计算机软件著作权登记证书》 |
| 产品具有中国网络安全审查技术与认证中心《IT产品信息安全认证证书》 |
| 厂商资质要求 | 厂商具有国家信息安全漏洞库（CNNVD）技术支撑单位等级证书（二级） |
| 厂商具有中国信息安全测评中心颁发的信息安全服务资质（安全工程类一级） |
| 厂商具有国家计算机网络应急技术处理协调中心颁发的网络安全应急服务支撑单位证书（国家级） |
| 厂商具有中国信息安全认证中心颁发的信息安全服务资质，风险评估（一级） |
| 厂商具有中国信息安全认证中心颁发的信息安全服务资质，应急处理（一级） |
| 维保要求 | ▲5年免费质保。 |

**3.8数据库监控与审计技术参数要求**

|  |  |
| --- | --- |
| **功能指标** | **指标要求** |
| 性能配置 | 性能参数：吞吐量：3Gbps，SQL处理性能：30000条SQL/s，日志检索性能：1亿条日志，查询时间30秒以内，日志检索：100000条/秒。硬件参数：规格：1U，内存大小：8G，硬盘容量：2TB SATA，电源：单电源，接口：6千兆电口+2千兆光口SFP。 |
| 数据库类型 | ★1、支持主流数据库：Oracle、MSSQL、MySQL、DB2、Sybase、Informix、PostgreSQL、Teradata、Cache2、支持国产数据库：达梦DM、人大金仓Kingbase、南大通用Gbase、神通Oscar3、支持非关系型数据库：MongoDB、Redis |
| 防护手段 | 支持记录日志、不记录日志、日志的风险等级自定义。 |
| 规则条件 | ▲访问的时间、次数、访问客户端IP、客户端操作系统主机名、客户端操作系统用户名、客户端连接工具名、数据库用户名、数据库IP、数据库实例、表、列等、操作类型、执行成功、执行失败、执行时长、返回行数、登录成功、登录失败、SQL异常、SQL模式、SQL关键字等。（提供截图） |
| 全局参数 | 支持全局参数配置，方便不同策略引用，可以配置的参数有：IP集、源应用程序集、数据库用户集、操作系统用户集、操作系统主机名集、表组集、存储过程集、数据库列集、数据库Schema集、敏感数据组集、查询组集。 |
| 策略管理 | 支持策略的添加、删除、导入、导出。 |
| 内置规则 | ★支持内置高风险规则，防范维护人员执行no where 删除、truncate table等合法的授权的高危操作检测。（提供截图） |
| 默认全记录 | 支持默认情况下全部记录的规则。 |
| 超级白名单 | ★支持数据库连接工具白名单功能，自动忽略数据库连接工具访问数据库的默认操作。 |
| 默认高风险规则 | ★支持内置高风险操作特征规则，包含：清表（delete no where 、truncate table）、删表（drop table）、提权（alter、grant）。 |
| 数据库自动发现 | ★支持通过监控网络流量自动发现未审计数据库。 |
| SQL注入 | ★支持基于CVE的SQL注入漏洞检测。 |
| 缓冲区溢出检测防护 | 支持特征方式的缓冲区溢出检测规则。 |
| 日志内容 | ▲日志内容能够详尽的显示访问行为发生的具体特征，具体信息包括：访问的时间、访问客户端IP、客户端MAC、客户端操作系统主机名、客户端操作系统用户名、客户端端口号、客户端连接工具名、数据库用户名、数据库IP、数据库MAC、数据库实例、表、列、操作类型、SQL内容、SQL结果内容、执行时间（毫秒）、响应状态、影响行数、查询返回行、匹配的策略、风险等级。（提供截图） |
| 解析能力 | ★支持双向审计、Oracle变量绑定。 |
| 日志模糊化 | ★支持日志模糊化处理，保护访问数据安全。 |
| 日志查询 | 按访问的时间查询； |
| 按访问源查询：访问客户端IP、客户端MAC、客户端操作系统主机名、客户端操作系统用户名、客户端连接工具名、数据库用户名； |
| 按访问的目标查询：数据库IP、数据库MAC、数据库实例、表、列等； |
| 按操作类型查询； |
| 按SQL内容查询； |
| 按匹配的策略查询； |
| 按风险等级查询。 |
| 日志检索 | ★支持检索条件保存功能； |
| 支持检索结果导出，导出文件格式PDF、EXCEL、WORD。 |
| 会话回放 | 支持会话回放功能，还原用户的访问行为。 |
| 用户行为轨迹分析 | ★以曲线连接多点的形式展示用户的访问来源、目标、操作的轨迹；支持轨迹定位到具体日志信息。（提供截图） |
| 流量监控 | 支持实时的网络流量监控；支持实时/历史的入库日志流量监控。 |
| 告警查询 | 支持以相同的规则进行告警日志汇总显示；支持以引擎的方式对进行告警日志汇总显示； |
| 支持以风险等级、匹配的策略、时间、其他操作条件对告警日志进行查询。 |
| 告警方式 | 支持告警日志外发至第三方日志平台，外发格式有SYSLOG、SNMP、FTP、EMAIL。 |
| 告警策略 | 支持自定义告警的等险等级，包括低风险、中风险、高风险、致命四个等级。 |
| 告警处理 | 支持对误报的告警日志进行处理，包括加入SQL攻击例外、禁用SQL注入规则。 |
| 攻击趋势 | 支持以柱状图的形式显示风险趋势。 |
| 访问来源趋势 | 支持以柱状图的形式显示访问来源趋势。 |
| 事件排名 | 支持以柱状图的形式显示事件（策略命中计数）排名。 |
| 实时报表 | 支持系统内置报表模板形式的实时统计分析。 |
| 支持可以根据需要再使用内置模板的情况下，设置检索条件进行实时统计分析。 |
| 支持的检索条件与日志检索相同细颗粒度的检索条件。 |
| 支持的内置报表模板不少于30个，可以从来源分析、执行时长分析、操作类型分析、特权操作、登录情况等维度展示数据库的访问情况。 |
| 定时报表 | 支持系统内置模板的定时报表； |
| 支持定时报表可以通过邮件形式外发； |
| 支持定时报表可以按照周期时间生成后发送； |
| 自定义报表 | 支持自定义（数据来源、数据分析条件、展示效果等）报表； |
| 旁路模式 | 支持以交换机镜像方式对数据库进行审计分析。 |
| 软件探针 | 支持以旁路情况下，在数据库服务器上部署探针的方式对数据库进行审计。 |
| IPv6 | 支持IPv6环境下审计系统的部署、配置和使用，支持对IPv6环境下数据库进行审计。 |
| 角色管理 | 支持三权分立的内置用户设置，不同用户负责产品不同模块的配置与使用；默认管理员可以根据自身的权限对新增用户进行授权；授权范围包括自身角色下的所有功能页面；可以针对某些功能页面进行授权。 |
| 备份还原 | 支持系统配置+审计日志的全量备份； |
| 支持的备份方式有：手工备份、定时自动备份、自动远程备份； |
| 支持手工方式还原； |
| 支持备份文件手工、自动方式清理。 |
| 配置管理 | 支持系统时间手工、自动与NTP服务器同步，保证审计日志时间准确性； |
| 支持接口配置、用户登录安全管理等。 |
| 升级 | 支持页面方式进行升级； |
| 支持不丢失配置情况下升级。 |
| 系统诊断 | 支持系统能够自动对审计进程、解析进程、存储进程、检索进程进行诊断分析，方便用户排除故障。 |
| 磁盘使用率监控 | 支持磁盘使用率监控，当磁盘使用率达到预定的阈值时，页面弹框提示管理员； |
| 系统状态监控 | 支持系统CPU、内存、网络吞吐率、交换分区、磁盘的使用率监控，支持磁盘的读写速率监控。 |
| 系统告警 | 支持系统CPU、磁盘使用率超限告警。 |
| 系统磁盘清理 | 当磁盘使用率达到预定的阈值时，系统停止记录日志或者覆盖以前的记录。 |
| 产品资质 | 产品具有公安部《计算机信息系统专用产品销售许可证》；产品具有国家版权局《计算机软件著作权登记证书》；产品具有中国信息安全认证中心《中国国家信息安全产品认证证书》。 |
| 厂商资质要求 | 厂商具有国家信息安全漏洞库（CNNVD）技术支撑单位等级证书（二级）；厂商具有中国信息安全测评中心颁发的信息安全服务资质（安全工程类一级）；厂商具有国家计算机网络应急技术处理协调中心颁发的网络安全应急服务支撑单位证书（国家级）；厂商具有中国信息安全认证中心颁发的信息安全服务资质，风险评估（一级）；厂商具有中国信息安全认证中心颁发的信息安全服务资质，应急处理（一级）。 |
| 维保要求 | ▲5年免费质保。 |

**3.9防病毒软件技术参数要求**

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| ▲系统架构 | 控制中心：采用B/S架构管理端，能够设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能。 |
| 客户端：与安全控制中心通信，提供控制中心管理所需的相关数据信息；执行最终的木马病毒查杀、漏洞修复等安全操作。 |
| 服务器端客户端支持WIN2003/WIN2008/WIN2012/WIN2016 |
| 本次采购20个Windows服务器操作系统授权 |
| 本次采购的功能授权必须具备防病毒与补丁管理 |
| 病毒、恶意代码、木马防护 | 内存防护 | 支持内存实时监控查毒，能够自动隔离感染而暂时无法修复的文件； |
| 网络安全防护 | 拦截下载器自动下载木马程序、恶意推广程序、盗号木马； |
| 拦截黑客远程控制本机； |
| 嵌入式防御 | 支持用户添加嵌入杀毒的应用程序；支持FlashGet、NetAnts、WinZip、WellGet、WinRAR等工具的嵌入式杀毒功能； |
| 移动设备病毒防护 | 要求提供U盘等移动设备接入电脑自动检测功能，全面拦截和清除在移动设备接入系统可能带来的病毒木马； |
| 聊天安全防护 | 检测QQ、MSN、阿里旺旺等常用聊天软件传输文件的安全性，确保传输文件不中毒； |
| 检测QQ、YY、飞信等聊天软件中对方发来网址的安全性 |
| ▲聊天软件传输某些文件会添加“.重命名”，如果文件安全，将自动去除“.重命名”（提供功能截图） |
| 攻击防护 | 能够实时检测和拦截攻击行为，包括改写系统关键文件、修改注册表关键键值、感染移动存储介质、创建系统账号 |
| ▲云修复 | 支持扫描发现文件遭破坏或被感染时触发修复流程，修复通过公有云下载正常文件替换遭破坏的文件；（提供功能截图） |
| 黑白名单例外 | 支持文件、目录和数字签名自定义黑白名单的方式来管理全网终端的文件； |
| ▲支持手工导入MD5+SHA1的黑白名单方式，支持txt批量导入方式；（提供功能截图） |
| ▲支持对windows/Linux/国产操作系统终端的文件黑白名单和信任区在服务端统一管理；（提供功能截图） |
| 压缩包杀毒 | 要求支持文件解压缩病毒查杀，支持对zip、rar、7z等多种格式的压缩文件查杀能力； |
| ▲可对压缩包层级设置以节省终端计算资源；（提供功能截图） |
| 敲诈者病毒防御 | ▲对敲诈者病毒提供专有的防护功能；（提供功能截图） |
| 多杀毒引擎 | 要求产品具备本地多引擎查杀能力，且引擎可配置；（提供功能截图） |
| Linux、国产操作系统杀毒 | ▲支持linux、国产操作系统杀毒（提供至少4个厂商认证证书） |
| 样本库数量 | 要求产品具备公有云检测能力，并且公有云特征储备超过145亿； |
| 支持私有云查杀，预置至少8亿黑名单及2亿白名单，终端威胁统一到控制中心查询黑白并进行查杀。 |
| ▲补丁分发与漏洞修复 | 终端支持智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁；（提供功能截图） |
| 产品具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能（提供功能截图） |
| 产品具备漏洞集中修复过程中的流量控制和保证带宽,补丁分发支持服务端带宽限流与客户端P2P补丁分发加速，有效节省外网带宽资源（提供功能截图） |
| 相关资质 | 具有公安部颁发的《计算机信息系统安全专用产品销售许可证》具有国家保密科技测评中心颁发的《涉密信息系统产品检测证书》安全监控与审计资质证书。 |
| 其他要求 | ▲5年免费质保。 |

**3.10备份一体机技术参数要求**

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 基本要求 | 要求自主研发，拥有完整知识产权，非OEM，国内品牌产品。 |
| 硬件要求 | 2U一体机设备，550W冗余电源 |
| 64位六核处理器，支持升级至两路八核处理器 |
| 本次配置64G内存，支持升级至256G |
| ★本次配置1\*240G SSD系统盘，6\*4TB SATA硬盘；存储裸容量最大支持96TB； |
| 配置4个千兆网口，支持光纤卡、万兆网卡扩展 |
| 配置许可 | 配置≥24 TB容量的备份许可数据库备份许可无上限；LINUX/WINDOWS虚拟服务器备份许可无上限；LINUX/WINDOWS物理服务器备份许可无上限； |
| 管理要求 | 要求提供WEB中文管理界面，通过同一个界面即可集中管理所有功能，包括存储资源、备份计划、恢复操作等。 |
| 提供WEB向导式操作，备份策略和恢复策略设置简单，在WEB端即可完成所有操作。 |
| ★集中管理 | 支持直接纳管其他的备份节点，统一配置备份和恢复策略，无需单独配置集中备份管理软件或者界面。 |
| 备份及瞬间恢复功能 | 备份系统要求支持WINDOWS/LINUX/UNIX操作系统，满足对32/64位平台及应用支持，以充分考虑以后计算机网络系统建设的兼容性。应用系统保护，支持Oracle、SQL Server、Exchange Server、Lotus Domino、MySQL、SharePoint、Active Directory等数据库的增量备份和热备份。 |
| 支持文件、数据库、邮件的快速恢复。 |
| 支持双机和集群的服务器持续性接管备份，主服务器中断后，从服务器可以接替主服务器进行增量备份，以减少数据重复备份和管理的复杂性。 |
| 数据库备份 | 支持Unix平台下Oracle、Oracle RAC等大型数据库在线备份。 |
| 可同时备份Linux, Windows等服务器中的两个数据库，如Oracle和Mysql同时部署在一台服务器中的情况。 |
| 备份数据库重建功能 | 备份软件的内部数据库崩溃后，可以直接利用备份介质上的自描述信息重建日志数据库，完成灾难条件下的数据恢复。 |
| 虚拟化备份 | 支持Vmware vSphere ESX/ESXi、Microsoft Hyper-V、KVM、XEN、CAS等主流虚拟化应用保护。 |
| 支持备份任务并发，能够同时备份多个ESXI上的各自的虚拟机，或单台ESXi上的多个虚拟机，在单个任务下实现多个ESXI或多个虚拟机同时发起备份。 |
| 支持对Vmware虚拟化平台的备份恢复，通过vSphere API进行虚拟机的完全和增量备份恢复。 |
| 对虚拟化平台进行备份后，当虚拟化平台中增加新的虚拟机，备份任务能自动发现新增的虚拟机，并自动纳入备份管理的数据源，而无需手动添加。 |
| ★云备份支持 | 备份软件能够支持云备份环境，支持备份到云、云平台备份、备份云的建设 |
| 支持将本地备份数据直接备份到云平台提供的存储接口，支持阿里云、S3标准等标准协议的对象存储接口；支持将云上的数据备份到本地备份设备上的存储空间。 |
| 支持将公有云平台的云主机和对象存储中的数据备份到本地数据中心或第三方云平台。 |
| 客户端管理 | 厂家自主研发，拥有完整知识产权，非OEM，国内品牌产品。 |
| 管理服务器平台支持 | 备份管理服务器和客户端可以支持任何主流平台，如WINDOWS、UNIX（AIX、HP-UX、Linux）等，采用LAN-FREE备份方式。 |
| 客户端管理 | 支持将客户端根据不同的目标和需求进行分组分类。 |
| 支持多种备份策略 | 在支持全量、增量和差量备份的基础上。支持对全备份和多次的增量、差分备份进行逻辑合并的备份功能。减少全备份对生产系统的影响。 |
| ★跨域复制 | 要求能在多个备份站点（独立的备份域）间能实现备份数据远程复制，以实现数据级异地灾备。备份数据复制可在两个或更多的站点间进行，整个过程自动完成，无需人工干预，即使在生产站点完全瘫痪的情况下，在容灾站点也可以独立的直接恢复数据。 |
| 复制的对象可根据需要选择，即可仅选择对生产站点部分客户端的备份数据进行复制。 |
| 支持一对一、一对多、多对一、双向复制及瀑布型等多种复制架构。复制作业的时间窗口和带宽占用可独立于备份作业控制。 |
| 重复数据删除 | 集成重复数据删除： 实现功能强大且灵活的重复数据删除功能，能根据所备份对象和备份策略进行智能消重，节省存储空间，并且可自定义重删数据块大小。 |
| ★备份安全 | 提供数据校验功能，以确保备份数据与生产数据的一致性，并可选是否启用该功能。 |
| 提供传输加密功能，以确保备份数据在传输过程中的保密性。非全局开启，可根据策略的不同选择否启用该功能。 |
| ★产品资质 | 具备计算机软件著作权登记证书。具备国家保密科技测评中心颁发的涉密信息系统产品检测证书。 |
| 原厂商资质 | 原厂商具有信息安全管理体系认证证书ISO27001原厂商具有信息技术服务管理体系认证证书ISO20000原厂商具备Oracle OPN认证证书原厂商具备省级及以上高新技术企业研究开发中心证书 |
| ★售后服务 | 本次项目实施由原厂工程师实施；要求实施项目经理同时具备项目经理证书和OCM认证证书，实施工程师同时具备OCP和CISP工程师证书。要求原厂培训讲师具有ACE认证证书。 |
| 提供5年7×24小时上门质保维护服务，提供2小时以内的上门服务。 |

**四、机房建设采购清单**

**4.1采购清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **参考品牌****及型号** | **参数** | **数量** | **单位** |
| **4.1机房装修工程** |  |  |
| **4.1.1天花吊顶工程** |  |  |
| 1 | 顶面防静电漆 | 立邦/环保型、多乐士/环保型、三棵树/环保型 | 二遍成活，底漆加面漆，水溶性，环保型 | 60 | ㎡ |
| 2 | 顶面保温棉（含胶水） | 华美/30mm、神州/30mm、金威/30mm | 30mm，塑胶保温棉，B1级，环保型 | 60 | ㎡ |
| 3 | 天棚龙骨 | 龙牌/U50-38、可耐福/U50-38、杰科/U50-38 | U50/U38，国标 | 60 | ㎡ |
| 4 | 铝合金微孔吊顶天棚 | 佳美600\*600\*1.0、安乔600\*600\*1.0、宝兰600\*600\*1.0 | 1、规格：600\*600\*1.0；2、厚度：铝板1.0mm；3、冲孔类型：g2516/Rd1522； 4、噪音系数NSMOT:0.75； 5、防潮：一级； 6、反光度：25度；  7、防火等级：A级（GB8624-2006）；  8、隔音等级：冲孔板-CAC24db | 60 | ㎡ |
| 5 | 吊杆 | 国产/现场制作 | 10mm | 60 | ㎡ |
| 6 | 收边条 | 国产/现场制作 | 铝制0.8，带弹簧片 | 54 | 米 |
| **4.1.2地面工程** |  |  |
| 7 | 地面防静电漆 | 立邦/环保型、多乐士/环保型、三棵树/环保型 | 二遍成活，底漆加面漆，水溶性，环保型 | 60 | ㎡ |
| 8 | 地面保温棉（含胶水） | 华美/30mm、神州/30mm、金威/30mm | 30mm，塑胶保温棉，B1级，环保型 | 60 | ㎡ |
| 9 | 铝箔纸保护层 | 国产/现场制作 | 1.0mm | 60 | ㎡ |
| 10 | 无边钢制静电地板 | 创星/600\*600\*35、沈阳沈飞/600\*600\*35、汇丽/600\*600\*35 | 600×600×35mm  | 60 | ㎡ |
| 11 | 踢脚线（不锈钢） | 国产/现场制作 | 304，100mm，基层 | 54 | 米 |
| 12 | 地板四周支撑 | 国产/现场制作 | 40\*40mm | 135 | 米 |
| **4.1.3墙柱面工程** |  |  |
| 13 | 轻钢龙骨 | 龙牌/C75、可耐福/C75、杰科/C75 | C75 | 110 | ㎡ |
| 14 | 隔音防火棉 | 华美/70mm、神州/70mm、金威/70mm | 隔音防火棉，厚度70mm | 110 | ㎡ |
| 15 | 彩钢板贴面 | 汉姆拜克/1200\*3000、格满林/1200\*2.961、穹明/1200\*3000 | 金属夹芯彩钢板基层为厚度12mm左右防火石膏板+厚度大于0.6镀锌烤漆抗静电钢板彩钢板 | 110 | ㎡ |
| **4.1.4隔断工程** |  |  |
| 16 | 防火玻璃隔断 | 耀强特玻/12mm、福耀/12mm、北玻/12mm | 12mm铯钾防火玻璃，防火时间大于120分钟 | 21 | ㎡ |
| 17 | 镀锌方钢支架（基层，防护） | 国产/现场制作 | 8mm方钢定制 | 14 | 米 |
| 18 | 不锈钢包边 | 国产/现场制作 | 304拉丝不锈钢板饰面，120mm,1.5mm | 14 | ㎡ |
| 19 | 辅材 | 国产/现场制作 | 配套 | 1 | 套 |
| **4.1.5门窗工程** |  |  |
| 20 | 甲级钢质防火门 | 璐璐红/1500\*2200、万达/1500\*2200、群升/1500\*2200 | 双开、1500\*2200mm | 1 | 套 |
| 21 | 防火玻璃门 | 耀强特玻/12mm、福耀/12mm、北玻/12mm | 单开、900\*2200mm | 1 | 套 |
| 22 | 闭门器 | 国产 | 与钢制防火门配套 | 1 | 付 |
| **4.1.6基础工程** |  |  |
| 23 | 地面找平 | 国产/现场制作 | 3：1水泥细沙，厚度大于30mm | 60 | ㎡ |
| 24 | 机房踏步 | 国产/现场制作 | 混凝土浇筑，大理石饰面，定制 | 1 | 项 |
| 25 | 地漏工程 | 国产/现场制作 | 做S弯下水口处理 | 1 | 项 |
| 26 | 空调进水出水管铺设 | 国产/现场制作 | 含进水和出水 | 1 | 套 |
| 27 | 挡水堰 | 国产/现场制作 | 80\*100，内刷防水涂料 ，环氧地平，钢材料 | 1 | 项 |
| 28 | 垃圾清理 | - | 垃圾清理、运输 | 1 | 项 |
| 29 | 机柜承重支架 | 国产/现场制作 | 槽钢5# | 16 | 套 |
| 30 | 电池架承重支架 | 国产/现场制作 | 槽钢5# | 2 | 套 |
| 31 | 门洞拓展 | 国产/现场制作 | 1580\*2280 | 1 | 套 |
| 32 | 通道口制作 | 国产/现场制作 | 200\*200通道口制作，含外立面修复 | 3 | 套 |
| **4.2供配电系统** |  |  |
| 33 | 机房输入电缆 | 浙上/WZD YJV 4\*70+1\*50、人民/WZD YJV 4\*70+1\*50、东方/WZD YJV 4\*70+1\*50 | WZD YJV 4\*70+1\*50 ATS后端引出，国标 | 120 | 米 |
| 34 | UPS输入输出电缆 | 浙上/WZD YJV 4\*50+1\*35 、人民/WZD YJV 4\*50+1\*35 、东方/WZD YJV 4\*50+1\*35 | WZD YJV 4\*50+1\*35，国标 | 20 | 米 |
| 35 | AP配电柜 | KSTAR成套、施耐德成套、ABB成套 | 定制 | 1 | 套 |
| 36 | 列头柜输入电缆 | 浙上/WZD YJV 4\*35+1\*16 、人民/WZD YJV 4\*35+1\*16 、东方/WZD YJV 4\*35+1\*16 | WZD YJV 4\*35+1\*16，国标 | 40 | 米 |
| 37 | 精密空调输入电缆 | 浙上/ZR YJV 5\*10 、人民/ZR YJV 5\*10 、东方/ZR YJV 5\*10 | ZR YJV 5\*10，国标 | 20 | 米 |
| 38 | 柜式空调输入电缆 | 浙上/ZR YJV 5\*4 、人民/ZR YJV 5\*4、东方/ZR YJV 5\*4 | ZR YJV 5\*4，国标 | 12 | 米 |
| 39 | 机柜电源输入线 | 浙上/ZR YJV 3\*6 、人民/ZR YJV 3\*6、东方/ZR YJV 3\*6 | ZR YJV 3\*6，国标 | 500 | 米 |
| 40 | 新风、排风机输入电线 | 浙上/ZR VV 3\*4 、人民/ZR VV 3\*4 、东方/ZR VV 3\*4 | ZR VV 3\*4，国标 | 40 | 米 |
| 41 | 强电桥架 | 华强/200\*100\*1.2、玮诚/200\*100\*1.2、尚品/200\*100\*1.2 | 200\*100\*1.2mm强电桥架，地板下安装，含支架 | 20 | 米 |
| 42 | 插座电缆 | 浙上/ZR YJV3\*2.5、人民/ZR YJV3\*2.5、东方/ZR YJV3\*2.5 | ZR YJV3\*2.5，国标 | 200 | 米 |
| 43 | 地面插座（含底盒） | 鸿雁/三插、德力西/三插、西门子/三插 | 二、三级插座 | 8 | 个 |
| 44 | 工业连接器 | 国产 | 32A含公母头 | 26 | 套 |
| 45 | 金属软管 | 国产 | 外有塑套 | 200 | 米 |
| 46 | KBG25管 | 国产 | 25MM | 200 | 米 |
| 47 | 配件 | 国产 | 标签、扎带、管接等 | 1 | 批 |
| **4.3机房照明系统** |  |  |
| 48 | 照明、维修插座电线 | 浙上/ZR-BVR 3\*2.5、人民/ZR-BVR 3\*2.5、东方/ZR-BVR 3\*2.5 | ZR-BVR 3\*2.5 | 500 | 米 |
| 49 | LED灯盘 | 雷士/600\*600、飞利浦/600\*600、三雄极光/600\*600 | 600\*600嵌入式LED灯盘 | 7 | 套 |
| 50 | LED灯盘（应急） | 雷士/600\*600、飞利浦/600\*600、三雄极光/600\*600 | 600\*600嵌入式LED应急灯盘 | 7 | 套 |
| 51 | 电线管明配DG25 | 国产 | 镀锌 | 200 | 米 |
| 52 | 安全出口指示灯 | 国产 | LED灯 | 2 | 套 |
| 53 | 86型单联双控开关 | 鸿雁/86、德力西/86、西门子/86 | 86型单联双控开关 | 2 | 个 |
| 54 | 86型底盒 | 国产 | 86型底盒 | 2 | 个 |
| **4.4机房接地系统** |  |  |
| 55 | 铜排 | 国产 | 40\*4mm等电位接地铜排 | 24 | 米 |
| 56 | 铜带 | 国产 | 60\*0.6接地紫铜带 | 86 | 米 |
| 57 | 绝缘端子 | 国产 | 定制 | 24 | 付 |
| 58 | 等电位箱 | 国产 | 定制 | 1 | 套 |
| 59 | 接地电缆 | 国产 | BVR50mm2/BVR10mm2/BVR6mm2接地线缆 | 1 | 项 |
| 60 | 附件 | 国产 | 固定螺丝/线耳/焊条/固定码/支架等 | 1 | 批 |
| **4.5机房空调系统** |  |  |
| 61 | 精密空调 | 艾特网能/CS007HA0TI1、科士达/ST007FAAAAONT、DENE/DKT05KW | 1.采用风冷式上送风，下回风，单冷精密空调机组；2.制冷量＞7.5KW；3.显冷量≥6.9KW；★4.投标产品应高效节能，整机能效比≥3.1★5.要求投标产品制造商具备国家压缩机制冷设备质量监督检验中心以及CNAS审核通过的实验室合格证书，其中制冷量覆盖1.5~120KW；6.风量≥3200m3/h；7.噪音≤61dB(A)；8.整机模块化设计：功能模块独立，隔离干扰；结构模块化，减少加工成本且易拆卸；部件模块化，备件最少维护成本低；9. 运行寿命要求：24小时365天不间断运行设计，设计寿命≥15年；★10.空调应具备高显热，要求显热比（显冷量/总冷量）>0.91；11.空调须满足电压适应范围380±15%，具备缺相保护、提示和告警功能；12.空调应在-20/-35℃～45℃的室外环境温度范围内保证正常制冷；13.空调须100%全正面维护；主要部件可拆卸维护，满足机房搬运通道要求，搬运、安装新空调和折除旧空调时不得对机房现有门窗、墙体结构进行改动和破坏性施工。14.空调须采用高效后倾离心直联风机，具备风压调整范围宽的特点，且不需皮带传动，无需例行维护及更换皮带；15.蒸发器表面须采用亲水膜涂层工艺，提高换热效率，减少绝热损失；16.采用V型大面积蒸发器，换热面积最大，换热效率高，采用铜管套冲缝型亲水铝翘片式蒸发器盘管；★17.空气过滤器复合EU4标准，效率≥30%，符合Ashrae 52/76， Eurovent 4/5规范；★18.空调机组应配备滤网压差开关和气流丢失压差开关两个气压差开关；19.空调标准配置RS485监控接口，RJ45监控接口，支持Modbus和YD/T1363.3双通讯协议，可现场选择协议类型；▲20.不接受OEM或ODM产品，必须为原厂生产，《全国工业产品生产许可证》获证单位名称与制造商名称完全一致。21.空调机组EMC电磁兼容性应符合IEC61000-4，IEC61000-3-2-2000，IEC61000-3-4-1998标准；22.空调机组需满足8、9级烈度抗震考核，以确保机组在特殊情况下的正常使用。★23.精密空调产品具备CRAA产品认证证书、CE产品认证证书；▲24.提供5年免费质保。 | 1 | 套 |
| 62 | 精密空调 | 艾特网能/CM030DA、科士达/ MT030DAACAOBT、DENE/DKT030KW | ★1.下送风上回风，空调总冷量≥32KW，显冷量≥30KW，风量≥8500m3/h，，投标机房专用空调标准配置制冷剂型号应为R410A环保制冷剂。★2.投标产品应高效节能，整机能效比≥3.0。要求投标产品制造商具备国家压缩机制冷设备质量监督检验中心以及CNAS审核通过的实验室合格证书，其中风冷空调的制冷量覆盖1.5~120KW。★3.整机模块化设计：功能模块独立，隔离干扰；结构模块化，减少加工成本且易拆卸；部件模块化，备件最少维护成本低。4. 运行寿命要求：24小时365天不间断运行设计，设计寿命≥15年；5. 空调须满足电压适应范围380±15%，具备缺相保护、提示和告警功能。6. 空调须100%全正面维护；主要部件可拆卸维护，满足机房搬运通道要求，搬运、安装新空调和折除旧空调时不得对机房现有门窗、墙体结构进行改动和破坏性施工。7. 空调须采用高效后倾离心直联风机，具备风压调整范围宽的特点，且不需皮带传动，无需例行维护及更换皮带。8. 空调须采用可拆卸电极加湿器，易封装，封闭加湿，效率最高，自动冲洗且可拆卸维护，维护费用低。9. 蒸发器表面须采用亲水膜涂层工艺，提高换热效率，减少绝热损失。10. M型大面积蒸发器，换热面积最大，换热效率高。★11.空调须采用G4级大面积贴附式过滤器。12. 分布式冷凝水收集系统：冷凝水积水盘根据模块化结构分布收集冷凝水，确保冷凝水排水畅通无阻。13. 空调需配备滤网压差开关和气流丢失压差开关，实时检测过滤网脏堵状况和风机运行状态。★14.空调须配置7英寸彩色触摸显示屏，操作菜单专为中国市场用户设计，操作简单明了。15. 空调标准配置RS485监控接口，支持Modbus和YD/T1363.3双通讯协议，可现场选择协议类型。▲16.不接受OEM或ODM产品，必须为原厂生产。《全国工业产品生产许可证》获证单位名称与制造商名称完全一致。★17.具有CRAA产品认证证书、CE产品认证证书。★18.投标产品具有节能认证。▲19.提供5年免费质保。 | 1 | 套 |
| 63 | 铜管 | 国产 | #16、#19铜管 | 40 | 米 |
| 64 | 辅材 | 国产 | 现场制作 | 2 | 套 |
| **4.6新风及排风系统** |  |  |
| 65 | 新风换气机 | 天方/HR16D、松下/FY-150ZJP3C、远大/SD1500 | 1500m3/h | 1 | 台 |
| 66 | 排烟机 | 天方/PY4.0、九阳/YDT100L2-2/4、越舜/XGF3.5 | PY4.0 4000m3/h | 1 | 台 |
| 67 | 新风风管 | 国产/现场制作 | 200\*200（0.8白铁皮/20mm厚橡塑保温板） | 35 | 米 |
| 68 | 送风风口 | 国产/现场制作 | 定制 | 2 | 只 |
| 69 | 排风风口 | 国产/现场制作 | 定制 | 4 | 只 |
| 70 | 防火阀（新风） | 国产 | 平时常开，接24V消防电源，给信号关闭 | 1 | 只 |
| 71 | 防火阀（排风） | 国产 | 平时常闭，接24V消防电源，手动开启 | 1 | 只 |
| 72 | 辅材 | 国产 | 电工电料；封堵、管道辅料、其他辅材等； | 1 | 项 |
| **4.7综合布线系统** |  |  |
| 73 | 六类非屏蔽4对室内线缆带十字隔离 | 万马/WM/WX-C6-UTP-LSZH、爱谱华顿/AP-6-01-WD、罗格朗/632720 | 内部须采用十字骨架分隔结构；标准：TIA/EIA568B，带宽：≥250MHz；阻抗：100±15Ω | 15 | 箱 |
| 74 | 六类非屏蔽RJ45跳线（3米） | 万马/WM/TX-C6-UTP-PVC、爱谱华顿/AP-6-02-3、罗格朗/632753 | 标准：TIA/EIA-568B.2-1和ISO11801 2nd；传输带宽≥250MHz，阻抗: 100 ohms±15%。 | 150 | 根 |
| 75 | 24口六类非屏蔽模块式配线架（含模块） | 万马/WM/PXJ-C6-FTP-24K、爱谱华顿/AP-24-KS、罗格朗/632781 | 规格： 24口RJ45模块化结构，后面带背面理线盘。标准：ISO/IEC 11801:2002 Ed2.0，TIA/EIA-568-B.2-1； | 28 | 套 |
| 76 | 1U水平理线器（19"机柜用） | 万马/WM/LXQ-12D、爱谱华顿/AP-J-01-LG-12、罗格朗/632787 | 采用优质冷轧钢板材料，确保产品的坚固耐用。大容量设计，有助于布线的条理性；标准19英寸机架安装 | 60 | 个 |
| **4.8安防系统** |  |  |
| **4.8.1视频监控系统** |  |  |
| 77 | 红外半球网络摄像机 | 海康/DS-IPC-B12-I、大华/DH-IPC-HDW2233C-A、天地伟业/TC-NC9201S3E-2MP-E-I3A | 200万1/2.7”CMOS ICR日夜型半球型网络摄像机；最小照度 0.01Lux @(F1.2,AGC ON) ,0 Lux with IR；0.028 Lux @(F2.0,AGC ON), 0 Lux with IR；快门 1/3秒至1/100,000秒；镜头 2.8mm, 水平视场角:114°(4mm可选)；支持三轴调节 ：水平:0°~355°,垂直:0°~75°,旋转0°~355°；宽动态范围 120dB；帧率 50Hz: 25fps (1920 × 1080,1280 × 960,1280 × 720)；支持智能后检索，配合NVR支持事件的二次检索分析；ROI支持三码流分别设置1个固定区域；存储功能 支持Micro SD/SDHC /SDXC卡(128G)断网本地存储,NAS(NFS,SMB/CIFS均支持)；智能报警：越界侦测,区域入侵侦测,场景变更侦测,人脸侦测,虚焦侦测,物品遗留侦测,物品拾取侦测,非法停车侦测,人员聚集侦测,徘徊侦测,快速移动侦测,进入区域侦测,离开区域侦测，音频异常侦测；具有1对音频输入（Line in）/输出接口（插线式）、1对报警输入/输出（三极管：超过30毫安建议加继电器）接口；工作温度和湿度 -30℃~60℃,湿度小于95%(无凝结)；电源供应 DC12V±25% ；功耗 5W MAX（ICR切换瞬间7W MAX）；红外照射距离 10-30米；防护等级 IP67；防暴等级 IK08 | 4 | 个 |
| 78 | 电源箱 | 国产 | 国产 | 1 | 只 |
| 79 | 开关电源 | 国产 | DC12V/6A | 1 | 个 |
| 80 | 硬盘 | 希捷/ST4000DM004、西部数据/WD40EZRZ、东芝/DT02ABA400 | 4TB/64MB(6Gb/秒 NCQ)/5900RPM/SATA3 | 2 | 个 |
| 81 | 8路NVR硬盘录像机 | 海康/DS-7808NB-K1/8P、大华/DH-NVR4832-4KS2、天地伟业/TC-R5820 | 机架式IP存储，嵌入式处理器，嵌入式软硬件设计；支持32路高清，320M带宽网络视频接入，256M网络带宽输出；支持8个SATA盘位；支持RAID 0、1、5、6、10多种RAID模式及全局热备，多重保护数据安全；支持关键视频添加标签和加锁保护、整机热备、断网续传、SMART 2.0等功能；2个千兆以太网口，充分满足网络预览、回放以及备份应用。 | 1 | 台 |
| 82 | 交换机 | H3C/Mini S24G-U、华为/S1724G-AC、锐捷/RG-NBS1824GC | 24口非管理型 | 1 | 台 |
| 83 | 线缆 | 国产 | 六类网线、电源线等 | 1 | 批 |
| 84 | KBG管 | 国产 | 25DN | 100 | 米 |
| **4.8.2门禁系统** |  |  |
| 85 | 四门网络型门禁控制器（带安装箱） | 海康威视/DS-K260ZFW-F4、大华/DH-ASC1204C-D、中控/IFACE702 | 通信接口 RJ45，支持脱机运行读卡器输入格式 Wiegand 26/ Wiegand 34开门延时时间 1-600 秒可调（软件）工作电压 12VDC，＜100mA（不含电锁、读卡器等配件）多种发卡方式 支持手工输入卡号发卡、指定读卡器刷卡发卡、USB发卡器发卡可接读卡器数量 4个可控制门输出 4组，支持单向识别+开门按钮注册卡片数量 2万张记录脱机存储数量 10万条，支持以堆栈的方式保存最新的信息掉电保护 高速闪存读卡器到控制器距离最大100米扩展功能 远程开门、首卡开门、定时开门、胁迫报警、互锁功能、反潜回、防尾随、多卡验证、超级密码、消防联动等外置电源 支持外置蓄电池（7AH 12V蓄电池） | 1 | 个 |
| 86 | 单门电磁锁（270KG带门磁） | 海康威视/270KG、大华270KG、中控/270KG | 270KG | 1 | 个 |
| 87 | 双门电磁锁（270KG带门磁） | 海康威视/270KG、大华270KG、中控/270KG | 270KG | 1 | 个 |
| 88 | 出门按钮 | 国产 | 86型 | 2 | 个 |
| 89 | 读卡器 | 海康威视/配套、大华/配套、中控/配套 | 读卡器 | 2 | 套 |
| 90 | 平台软件 | 海康威视/配套、大华/配套、中控/配套 | 使用网络型门禁控制器，通过门禁控制器设备提供的网络智能接口及通讯协议，采用网络的方式将门禁信号接入到现场管理服务器，由监控平台软件进行门禁的实时监测。 | 1 | 个 |
| 91 | 感应卡 | 海康威视/配套、大华/配套、中控/配套 | IC卡 | 50 | 张 |
| 92 | 线缆 | 国产 | 网线、控制线、电源线等 | 1 | 批 |
| 93 | KBG管 | 国产 | ¢25 | 100 | 米 |
| **4.8.3报警系统** |  |  |
| 94 | 防盗报警主机 | 国产 | 2防区报警主机 | 1 | 套 |
| 95 | 双肩探测器 | 国产 | 红外探测 | 2 | 套 |
| 96 | 线缆辅材 | 国产 | 配套 | 1 | 套 |
| **4.9机柜及UPS系统** |  |  |
| 97 | 机柜系统 | 科士达/ SP-61242B、DENE/DX612、艾特网能/BSRSX-061220 | 600\*1200\*2000mm网络机柜 | 15 | 套 |
| 98 | 监控主机 | 科士达/PE-HP20D、DENE/DJX01、艾特网能/BSM-M | Intel1.8GHZ双核处理器，4G内存，固态硬盘120G，1路VGA接口，6路DI，2路DO,2个232串口，6个485串口，工作温度-10℃~50℃。 | 1 | 套 |
| 99 | 采集主机 | 科士达/PE-NDC、DENE/DCJ101、艾特网能/Modbus-S | 用于采集各智能设备数据 | 1 | 套 |
| 100 | 专业版软件 | 科士达/PE-DZT、DENE\D01、艾特网能/BSM-L | 用于各智能设备数据分析 | 1 | 套 |
| 101 | 温湿度传感器 | 科士达/PE-STHL、DENE/THL2600、艾特网能/BSSTH-11RS | 专用于机房环境的高精度数字式温湿度传感器，-20C~+80C的精度在±0.5C，高亮度LCD显示，用于模块通道内温湿度检测 | 2 | 套 |
| 102 | 烟雾传感器 | 科士达/ JTY-GD-S833、DENE/JTY-GD-L832、艾特网能/JTY-GD-S832 | 带磁铁，监控机房烟雾状况 | 2 | 套 |
| 103 | 声光告警模块 | 科士达/PE-ALP、DENE/DSL05、艾特网能/BSSB2-RJ | 本地声光报警，配置12V直流电源 | 1 | 套 |
| 104 | 模块化配电机柜 | 科士达/YMK3300-100-F-20、DENE/DM3000-100KVA、艾特网能/UM-1200TEL-FF/2 | ★1、≥100KVA模块化热插拔UPS电源系统，≥5个支持热插拔功率模块，兼容上下进线；单机柜不更换功率模块可扩展至100KVA；本次配置模块≥4个。★2、纯在线机柜式模块化支持热插拔式UPS，本项目杜绝塔式支持热插拔式UPS；3、中文触摸液晶面板，显示输入输出参数电压、频率，并可直接在液晶面板上设置输入、输出参数，液晶面板上有直观的输入、输出曲线图，历史纪录、整流模块温度显示、逆变模块温度显示、系统温度显示、电池电池电压显示，输出电压、电流及功率，机器故障代码等.面板上嵌入EPO按键，在紧急情况下按下EPO按键就可紧急关机，并且具有远程紧急关机（REPO)功能；4、可直接进行集中监控，监控模块支持热插拔功能，拔出监控模块时，系统仍能正常运行；5、标配维修旁路，紧急情况下可在线维修；6、主机柜自带配电模块，与主机一体，配电模块功率为满配；▲7、提供5年免费质保，7\*24小时上门服务。 | 1 | 套 |
| 105 | 模块化UPS | 科士达/YMK3300-RM-20、DENE/DM3000-2OKVA、艾特网能/UM-0200TEL-M | 1、主机自带:干接点\RS232\RS485\SNMP通讯界面及2个智能插槽；2、输入电压范围208vac～478vac，UPS输入频率范围40HZ～70HZ,能与任意发电机兼容；3、充电电流最大可设置60Amax；4、每个功率模块≥20KVA；每个功率模块有独立的控制系统，故障功能模块能自动退出运行；5、单个功率模块抽出能单独使用，直流电压与主机柜能通用；6、每个模块有独立LCD+LED显示系统；7、32/34/36/38/40节电池灵活配置。系统在运行使用中有电池故障，可直接在线下架故障的电池。最低可在线设置成不少于32节电池供电。8、输入功率因数≥0.99，输出功率因数≥0.9，电源效率≥95%；★9、具有UPS模块的热插拔结构；★10、具有UPS模块拆装感应结构技术；★11、具有监控电路技术；▲12、提供5年免费质保，7\*24小时上门服务。 | 4 | 台 |
| 106 | 开放式电池箱 | 国产 | 600\*1600\*1600，开放式电池箱，可方式32节12V-100AH蓄电池，含直流控制箱 | 2 | 套 |
| 107 | 蓄电池 | 科士达/6-FM-100、DENE/12V-100AH、艾特网能/121200 | 1、12V-100AH免维护长寿命铅酸蓄电池；2、长寿命电池，浮充寿命≥10年；★3、蓄电池具有防漏液托盘技术；▲4、提供5年免费质保，7\*24小时上门服务；▲5、承诺保修期内一组电池组中有电池损坏更换整组电池。 | 64 | 节 |
| 108 | 智能接入模块 | 科士达/PE-DSM、DENE/DZ302、艾特网能/Modbus-C | 智能设备接入软件，每台设备提供1个接入模块 | 4 | 套 |
| 109 | 侧门 | 科士达/ SP-OD1242I、DENE/DX612-1、艾特网能/BSRAS-D12H20 | 1、机柜单侧内嵌式侧门；2、每块侧门含上下两段式门板；3、卡扣式安装。 | 4 | 套 |
| **4.10消防系统** |  |  |
| 110 | 七氟丙烷柜式装置 | 湖南金鼎/GQQ70/2.5、海湾/GQQ70/2.5、泰和安/GQQ70/2.5 | GQQ70/2.5七氟丙烷柜式装置，含罐体及柜体 | 2 | 瓶组 |
| 111 | 灭火剂 | 湖南金鼎/HFC-227ea、海湾/HFC-227ea、泰和安/HFC-227ea | 七氟丙烷气体灭火药剂，纯度:＞99.6%酸度(以HF计)(mg/Kg):＜1，水含量(mg/Kg):＜10，蒸发残留物:＜0.01%悬浮或沉淀物:不可见， | 130 | KG |
| 112 | 气体灭火控制器 | 国泰怡安/GK652B、北大青鸟/JB-QB-21S-VFC3010A/CE2、久远/JF999-QM2 | 1、壁挂式模块化设计；2、液晶显示，全中文菜单操作；3、控制器软关机功能；4、按消防设备分类启动技术；5、具有黑匣子功能，报警联动一体化。6、一个主机管理4个分区。 | 1 | 套 |
| 113 | 控制模块 | 国泰怡安/GM613W、北大青鸟/JF-M22、久远/VM3365A | 采用脉冲隔直探测技术，接线方便牢靠。 | 2 | 个 |
| 114 | 声光报警器 | 国泰怡安/GM633W、北大青鸟/JBF-VM1372B、久远/JF-SG41 | 工作电压：信号总线电压：24V允许范围：16V～28V，电源总线电压：DC24V允许范围：DC20V～DC28V工作电流：总线监视电流≤0.8mA，总线启动电流≤6.0mA，电源监视电流≤10mA ，电源动作电流≤160mA线制：四线制，与控制器采用无极性信号二总线连接，与电源线采用无极性二线制连接声压级≥85dB（正前方3m水平处（A计权）） | 2 | 个 |
| 115 | 放气指示灯 | 国泰怡安/GT1521-PA、北大青鸟/LW5606、久远/LR566 | 工作电压：信号总线电压：24V允许范围：16V～28V电源总线电压：DC24V允许范围：DC20V～DC28V工作电流：信号总线监视电流≤3mA电源总线监视电流≤2mA，信号总线动作电流≤4mA ，电源总线动作电流≤25mA闪光频率：每分钟闪亮60±6次编码方式：电子编码方式，编码范围可在11～20之间任意设定线制：与气体灭火控制器采用四线连接。其中两线接总线，无极性；另外两线接电源DC24V，无极性 | 2 | 个 |
| 116 | 泄压口 | 国泰怡安/XY02、北大青鸟/200\*200、久远/200\*200 | 200\*200 | 2 | 个 |
| 117 | 烟感探测器 | 国泰怡安/GY601W、北大青鸟/JTY-GDJBF-3100、久远/JTY-GD/JF-D21 | 编码型 | 4 | 个 |
| 118 | 温感探测器 | 国泰怡安/GW601W、北大青鸟/JTW-ZD-LN2110、久远/JTY-GD/JF-D22 | 编码型 | 4 | 只 |
| 119 | 通讯电缆 | 国产 | 配套 | 1 | 批 |
| 120 | 辅材 | 国产 | 配套 | 1 | 批 |

**三、其他要求**

**（一）项目验收要求**

1、验收标准

完成建设合同所约定的建设内容、工期和其他要求，满足招标文件的技术需求，并一次性验收合格。建设标准须符合1.3建设标准规范及相关文件要求。

2、项目验收

项目的验收包括初步验收、试运行和终验。

1）项目初验

项目初验前，中标方应首先对系统进行自测，并将系统自测报告提交业主方和监理方审查。中标方依本合同约定向业主方提交成果及相关文档，并向业主方提出初验申请。业主方接到中标方初验申请后，组织专家和相关单位对项目进行初验，初验合格后业主方、中标方、监理方共同签署初验报告。

2）试运行

初验合格后，系统进入试运行，试运行时间1个月。

3）终验

系统通过试运行后，中标方向业主方提出终验申请，业主方组织专家和相关单位进行系统的终验。系统终验收合格的条件必须至少满足以下三个要求：已提供了合同要求的合格产品和资料；试运行稳定并满足使用要求；项目初验和试运行出现的问题已解决。

3、设备检测

验收过程中，采购人有权对项目内的产品及设备对照招标参数要求及投标文件设备技术响应参数进行检测。由双方共同认可的有资质的第三方检测机构（或政府采购监管部门指定的检测机构）进行检测，检测合格的，检测费用由采购人支付。如检测结果不符合国家相关标准或投标文件中的技术性能承诺的，检测费用由供应商支付，按本招标文件第五部分采购合同的相关条款处理，另外采购人将报政府采购监管部门进行处理。

**（二）质保期及运维期要求**

1、项目的质保和运维范围包括本次所有中小学、幼儿园的前端设备、传输网络和局端后台设备。2、中标单位在系统建成通过竣工验收后需提供如下服务：

1）本项目所有设备质保期为5年以及提供5年的运行维护，在设备质保期内中标单位应提供快速技术服务，在接到用户的故障维修电话后1小时内响应，简单故障能通过电话予以解决，如用户提出需要上门服务，维修人员应在4小时内赶到现场，并在12小时内解决问题。如在规定时间内不能解决问题，应提供同规格的替代设备给用户代用，直至设备故障修复。

2）每周7×24小时技术支持，需落实具体的技术服务人员，负责日常视频监控平台专用软件的升级和维护。

3）中标单位必须保证在维护期间除去地震、洪水、战争因素外每天重点部位监控接入完好率在98%以上，保证所有中小学、幼儿园前端设备完好率100%，保证局端中心设备完好率100%。必须安排专用车辆和人员作为日常维护力量。

4）配合业主单位的重大活动的技术保障工作。

**四、特别说明**

1、采购需求中，带“▲”（如有）的为实质性条款，不得出现负偏离，否则做无效标处理。技术指标中带“★”（如有）为重要指标，不满足将被酌情扣分。

2、采购需求中的品牌、型号（如有）仅供投标人参考，没有任何限制性，投标人可选择同等或更优档次的产品，但必须满足相应（实质性）技术要求、规格及安装条件。

3、投标人应自行组织现场踏勘（如有需要），自行确定货物的安装方法和安装费用，并将安装费用列入报价，安装费用中标后不予调整。

**4、采购需求中，采购人提供的参考品牌型号，都是完全满足技术参数要求的，如投标供应商提供的投标产品是采购人提供的参考品牌型号的，视为满足采购技术要求，不存在技术偏离。**

**第五部分 采购合同**

**北仑区校园智能安全防控系统采购合同**

甲方：（买方）

乙方：（卖方）

丙方：（支付方）宁波市北仑教育发展有限公司

各方根据 项目（项目编号： ）公开招标的结果，签署本合同。

**一、货物清单**

1. 货物名称：

2. 型号规格：

3. 技术参数：

4. 数量（单位）：

**二、合同金额**

本合同金额为（大写）： 元（￥ 元）人民币。

**三、技术资料**

1. 乙方应按招标文件规定的时间向甲方提供使用货物的有关技术资料。

2. 没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。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。

**四、知识产权**

乙方应保证所提供的货物或其任何一部分均不会侵犯任何第三方的知识产权。

**五、产权担保**

乙方保证所交付的货物的所有权完全属于乙方且无任何抵押、查封等产权瑕疵。

**六、履约保证金**

乙方交纳人民币 元作为本合同的履约保证金。

**七、转包或分包**

1. 本合同范围的货物，应由乙方直接供应，不得转让他人供应；

2. 除非得到甲方的书面同意，乙方不得将本合同范围的货物全部或部分分包给他人供应；

3. 如有转让和未经甲方同意的分包行为，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。

**八、质保期**

1. 质保期 年。（自交货验收合格之日起计）

**九、交货期、交货方式及交货地点**

1. 交货期：

2. 交货方式：

3. 交货地点：

**十、货款支付**

1. 付款方式：

2. 当采购数量与实际使用数量不一致时，乙方应根据实际使用量供货，合同的最终结算金额按实际使用量乘以成交单价进行计算。

**十一、税费**

本合同执行中相关的一切税费均由乙方负担。

**十二、质量保证及售后服务**

1. 乙方应按投标文件承诺的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品。

2. 乙方提供的货物在质保期内因货物本身的质量问题发生故障，乙方应负责免费更换。对达不到技术要求者，根据实际情况，经双方协商，可按以下办法处理：

⑴ 更换：由乙方承担所发生的全部费用。

⑵ 贬值处理：由甲乙双方合议定价。

⑶ 退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

3. 如在使用过程中发生质量问题，乙方在接到甲方通知后在 小时内到达甲方现场。

4. 在质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切费用。

5. 上述的货物免费保修期为 年，因人为因素出现的故障不在免费保修范围内。超过保修期的机器设备，终生维修，维修时只收部件成本费。

**十三、调试和验收**

1. 甲方对乙方提交的货物依据招标文件上的技术规格要求、乙方投标时的技术响应承诺和国家有关质量标准进行现场初步验收，外观、说明书符合招标文件技术要求和投标技术响应的，给予签收，初步验收不合格的不予签收。货到后，甲方需在五个工作日内验收。

2. 乙方交货前应对产品作出全面检查和对验收文件进行整理，并列出清单，作为甲方收货验收和使用的技术条件依据，检验的结果应随货物交甲方。

3. 甲方对乙方提供的货物在使用前进行调试时，乙方需负责安装并培训甲方的使用操作人员，并协助甲方一起调试，直到符合技术要求，甲方才做最终验收。

4. 对技术复杂的货物，甲方应请国家认可的专业检测机构参与初步验收及最终验收，并由其出具质量检测报告。

5. 验收时乙方必须在现场，验收完毕后作出验收结果报告；验收费用由乙方负责。

**十四、货物包装、发运及运输**

1. 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

2. 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

3. 乙方在货物发运手续办理完毕后24小时内或货到甲方48小时前通知甲方，以准备接货。

4. 货物在交付甲方前发生的风险均由乙方负责。

5. 货物在规定的交付期限内由乙方送达甲方指定的地点视为交付，乙方同时需通知甲方货物已送达。

**十五、违约责任**

1. 甲方无正当理由拒收货物的，甲方向乙方偿付拒收货款总值的百分之五违约金。

2. 甲方或丙方无故逾期验收和办理货款支付手续的，甲方或丙方应按逾期付款总额每日万分之五向乙方支付违约金。

3. 乙方逾期交付货物的，乙方应按逾期交货总额每日千分之六向甲方支付违约金，由甲方从待付货款中扣除。逾期超过约定日期10个工作日不能交货的，甲方可解除本合同。乙方因逾期交货或因其他违约行为导致甲方解除合同的，乙方应向甲方支付合同总值5%的违约金，如造成甲方损失超过违约金的，超出部分由乙方继续承担赔偿责任。

4. 乙方所交的货物品种、型号、规格、技术参数、质量不符合合同规定及招标文件规定标准和投标响应承诺的，甲方有权拒收该货物，乙方愿意更换货物但逾期交货的，按乙方逾期交货处理。乙方拒绝更换货物的，甲方可单方面解除合同。

**十六、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，各方应通过友好协商，确定是否继续履行合同。

**十七、诉讼**

各方在执行合同中所发生的一切争议，应通过协商解决。如协商不成，可向甲方所在地法院起诉。

**十八、合同生效及其它**

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，须经财政部门审批，并签书面补充协议报政府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《合同法》有关条文执行。

4. 本合同正本一式 份，具有同等法律效力，三方各执 份，区招投标中心一份。

甲方：(公章) 乙方：(公章)

地址： 地址：

法定代表人或授权代表（签字）： 法定代表人或授权代表（签字）：

联系方式：（电话） 联系方式：（电话）

签字日期： 年 月 日 签字日期： 年 月 日

丙方：(公章)

地址：

法定代表人或授权代表（签字）：

联系方式：（电话）

签字日期： 年 月 日

**第六部分 投标文件组成及格式**

**说明**

1、投标文件由资格证明文件、技术商务文件和报价文件三部分组成。

2、投标人应按照招标文件要求的内容和提供的格式编写投标文件。

3、投标人如果是依法成立的分支机构的，在制作投标文件时应将参考格式中的“法定代表人”修改为：分支机构负责人。

**资格证明文件组成：**

1、投标人声明（见格式1）（提供原件彩色扫描件）

2、法定代表人身份证明书 或 法定代表人授权委托书（见格式2）（提供原件彩色扫描件）

3、法定代表人身份证（正反面） 或 全权代表身份证（正反面）（提供原件彩色扫描件）

4、投标人营业执照（提供原件彩色扫描件）

5、近一年内投标人基本开户银行出具的资信证明 或 投标人近一年度（投标截止时间为上半年的，提供近两年度任一年度）经审计的财务报告（提供原件彩色扫描件）

6、投标人税务登记证（多证合一的投标人提供营业执照）（提供原件彩色扫描件）

7、投标人社会保险登记证（多证合一的投标人提供营业执照）（提供原件彩色扫描件）

8、投标人具有独立法人资格或是（银行、保险、电信行业）依法设立的分支机构的证明材料（提供投标人营业执照原件彩色扫描件）

9、北仑区域内拥有有线网络的运营商(基础电信业务运营商或有线电视业务运营商)的证明材料（提供投标人营业执照原件彩色扫描件）

**说明**

1、投标人应按照资格证明文件组成所列内容提供资格证明材料。

2、资格证明材料须逐页CA电子签章，否则资格审查不通过。

3、资格证明文件中不得出现本项目的投标总价，否则为无效投标。

格式1：

投标人声明

**宁波市北仑区（开发区）公共资源交易中心：**

 （投标人名称） 系中华人民共和国合法企业，经营地址 。我 （法定代表人姓名） 系 （投标人名称） 的法定代表人，我方愿意参加你中心组织的 北仑区校园智能安全防控系统（项目编号：BLZFCG2020038）项目的投标，我方就本次投标有关事项郑重声明如下：

1、我方提交的所有投标文件、资料都是准确的和真实的。

2、我方不是采购人的附属机构；与采购人聘请的为此项目进行设计、编制规范、提供咨询服务的公司及其附属机构没有任何直接或间接的关联。

3、我方已具备履行本项目所必需的设备和专业技术能力。

4、我方在参加本次政府采购活动前三年内，在经营活动中没有重大违法记录。

5、以上事项如有虚假或隐瞒，我方愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

投标人名称（加盖公章）：

法定代表人（签字或盖章）：

日 期：

**说明：**

**1、本声明须由法定代表人签署，否则声明无效。**

**2、盖章签字后，提供彩色扫描件。**

格式2-1：

法定代表人身份证明书

**宁波市北仑区（开发区）公共资源交易中心：**

本人系 （投标人名称） 的法定代表人，现为你中心组织的项目编号为BLZFCG2020038 的 北仑区校园智能安全防控系统 政府采购项目，代表本单位签署上述项目的投标文件并处理与之有关的一切事务。

特此证明。

法定代表人姓名：

身份证号码：

联系电话：

法定代表人签字：

投标人名称（加盖公章）：

日 期：

**说明：**

**1、投标单位安排法定代表人参加本项目投标的，只须提供本证明书即可。**

**2、盖章签字后，提供彩色扫描件。**

格式2-2：

法定代表人授权委托书

**宁波市北仑区（开发区）公共资源交易中心：**

我 （法定代表人姓名） 系 （投标人名称） 的法定代表人，现授权委托本单位在职职工 （姓名、职务） 作为全权代表以我方的名义参加你中心组织的 北仑区校园智能安全防控系统（项目编号：BLZFCG2020038） 项目的采购活动，并代表我方全权办理一切与之有关的事务。

本授权书于 年 月 日签字生效，全权代表无转委托权，特此声明。

全权代表姓名：

身份证号码：

联系电话：

全权代表签字：

投标人名称（加盖公章）：

法定代表人（签字或盖章）：

日 期：

**说明：**

**1、投标单位安排全权代表参加本项目投标的，只须提供本授权书即可。**

**2、盖章签字后，提供彩色扫描件。**

**技术商务文件组成：**

1、封面（见技术商务文件封面格式）

2、目录

3、评标索引表（见格式3）

4、投标函（见格式4）

5、技术及服务条款偏离表（见格式5）

6、商务条款偏离表（见格式6）

7、投标货物（服务）清单（见格式7）

8、项目技术（服务）方案（内容格式自拟，要求见招标文件第四部分）

9、项目实施方案（内容格式自拟，要求见招标文件第四部分）

10、拟派本项目主要实施人员情况表（见格式8）

11、质量保证和服务承诺方案（内容格式自拟，要求见招标文件第四部分）

12、技术培训方案（内容格式自拟，要求见招标文件第四部分）

13、优惠承诺及合理化建议（内容格式自拟，要求见招标文件第四部分）

14、投标人取得的证书及荣誉情况表（见格式9）

15、投标人认为需要提供的其他材料

**说明**

1、投标人应按照技术商务文件组成所列内容和顺序编制技术商务文件。

2、技术商务文件应按照招标文件格式要求进行CA电子签章，未有规定的投标人视情况签章。

3、技术商务文件可以在招标文件格式的基础上适当调整，以使内容更加完备。

4、技术商务文件中不得出现本项目的投标总价，否则为无效投标。

技术商务文件封面格式：

技术商务文件

项目名称：北仑区校园智能安全防控系统

项目编号：BLZFCG2020038

投标人名称（CA签章）：

日 期：

格式3：

评标索引表

项目名称：北仑区校园智能安全防控系统

项目编号：BLZFCG2020038

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **评分项目** | **投标文件****对应页码** | **简要说明** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**说明：**

1、根据评分标准表技术商务部分逐条填写。

投标人名称（CA签章）：

日 期：

格式4：

投 标 函

**宁波市北仑区（开发区）公共资源交易中心：**

 （投标人名称） 委派 （全权代表姓名、职务） 参加你中心组织的 （项目名称、项目编号） 项目公开招标的有关活动，并对此项目进行投标。为此：

1、我方同意在本项目招标文件中规定的投标有效期内，遵守本投标文件中的承诺且在此期限期满之前均具有约束力。

2、我方保证遵守招标文件的全部规定，并提供招标文件规定的全部投标文件。

3、本项目投标总价见我方的报价文件。

4、如果我方中标，保证忠实地执行双方所签订的政府采购合同，并承担政府采购合同规定的责任和义务。

5、我方保证尊重评标委员会的评标结果，完全理解本项目不一定接受最低报价的投标。

6、我方愿意向你中心提供任何与本项目投标有关的数据，并根据需要提供一切承诺的证明材料。

7、我方已详细审查全部招标文件，在投标之前已经与招标方进行了充分的沟通，完全理解并接受招标文件的各项规定和要求，对招标文件的合理性、合法性不再有异议。

8、与本项目投标活动有关的一切正式往来信函请寄：

地址：

联系电话： 传真：

投标人名称（CA签章）：

日 期：

格式5：

技术及服务条款偏离表

项目名称：北仑区校园智能安全防控系统

项目编号：BLZFCG2020038

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **招标文件技术、服务要求** | **投标文件响应情况** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**说明：**

1、技术、服务条款内容主要是针对招标文件有关的技术规格、服务要求等内容。

2、无偏离应在本表“投标文件响应情况”栏注明“无技术及服务条款偏离”的字样。

投标人名称（CA签章）：

日 期：

格式6：

商务条款偏离表

项目名称：北仑区校园智能安全防控系统

项目编号：BLZFCG2020038

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **名称** | **招标文件商务要求** | **投标文件响应情况** |
| 1 | 交付时间 |  |  |
| 2 | 质保期 |  |  |
| 3 | 付款方式 |  |  |
| 4 | 合同主要条款 |  |  |
| … | … |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**说明：**

1、商务条款内容主要是针对招标文件有关的付款条件、交付期、质保期、合同主要条款等内容。

2、无偏离应在本表“投标文件响应情况”栏注明“无商务条款偏离”的字样。

投标人名称（CA签章）：

日 期：

格式7：

投标货物（服务）清单

项目名称：北仑区校园智能安全防控系统

项目编号：BLZFCG2020038

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **规格、型号** | **主要性能参数** | **单位** | **数量** | **产地、品牌** |
| **一、软件部分** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **二、硬件部分** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**说明：**

1、本表产品名称填写的顺序应与本招标文件第四部分中的采购清单相一致。

2、此表在不改变表式的情况下，可自行制作。

投标人名称（CA签章）：

日 期：

格式8：

拟派本项目主要实施人员情况表

项目名称：北仑区校园智能安全防控系统

项目编号：BLZFCG2020038

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **拟在本项目中担任职务** | **姓名** | **身份证号码** | **获得的相关证书名称、主要项目实施经历、工作经验（或另附简历）** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 声明：一旦我单位中标，将实行项目经理负责制，并配备上述项目实施人员。我方保证上述填报内容真实，若不真实，愿按有关规定接受处理。 |

**说明：**

1、拟派人员须是投标单位正式职工，以社保证明为准，如为符合法律规定的离退休返聘人员的，须提供退休证明及单位聘用证明。

2、表后附拟派人员的社保证明（或返聘人员证明）、业绩证明、相关证书的原件彩色扫描件。

3、拟派主要人员未经许可不得更换，否则取消中标资格，并赔偿采购人损失。

投标人名称（CA签章）：

日 期：

格式9：

投标人取得的证书及荣誉情况表

项目名称：北仑区校园智能安全防控系统

项目编号：BLZFCG2020038

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名 称** | **发证单位** | **发证时间** | **备注** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**说明：**

1、对照评分标准表，表后附相关证书及荣誉的原件彩色扫描件，未提供的，相关项目不得分。

2、以上内容必须是真实的，否则一经查实，按相关规定处理。

投标人名称（CA签章）：

日 期：

**报价文件组成：**

1、封面（见报价文件封面格式）

2、目录

3、开标一览表（见格式10）

4、投标分项报价表（见格式11）

5、政府采购统计基础信息表（见格式12）

6、投标人认为需要提供的其他材料

**说明**

1、投标人应按照报价文件组成所列内容和顺序编制报价文件。

2、报价文件应按照招标文件格式要求进行CA电子签章，未有规定的投标人视情况签章。

3、报价文件可以在招标文件格式的基础上适当调整，以使内容更加完备。

报价文件封面格式：

报价文件

项目名称：北仑区校园智能安全防控系统

项目编号：BLZFCG2020038

投标人名称（CA签章）：

日 期：

格式10：

开标一览表

项目名称：北仑区校园智能安全防控系统

项目编号：BLZFCG2020038

|  |  |  |
| --- | --- | --- |
| **项目名称** | **投标总价（元）** | **完成时间** |
| 北仑区校园智能安全防控系统 | 小写： | 满足采购人要求 |
| 大写： |

**说明：**

1、投标总价应为供应商提供本项目采购范围内的货物和服务所需的一切费用。

2、本表格的“投标总价”应与投标分项报价表的“投标总价”一致。

3、投标人在投标客户端填写的最终报价应当与加密上传的报价文件中“开标一览表”的投标总价一致，否则以上传文件开标一览表中的报价为准，并对客户端报价进行修正。

投标人名称（CA签章）：

日 期：

格式11：

投标分项报价表

项目名称：北仑区校园智能安全防控系统

项目编号：BLZFCG2020038

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **主要功能、参数 &****品牌、规格及型号** | **单位** | **数量** | **单价****(元/单位)** | **总价****（元）** |
| **一、软件部分** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **小计** | / | / | / | / |  |
| 二、**硬件部分** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **小计** | / | / | / | / |  |
| **投标总价（元）** | **小写：** |
| **大写：** |

**说明：**

1、本表产品名称填写的顺序应与本招标文件第四部分中的采购清单相一致。

2、本表格的“投标总价”应与开标一览表的“投标总价”一致。

3、此表在不改变表式的情况下，可自行制作。

投标人名称（CA签章）：

日 期：

格式12：

政府采购统计基础信息表

项目名称：北仑区校园智能安全防控系统

项目编号：BLZFCG2020038

|  |  |
| --- | --- |
| 投标单位名称 |  |
| 是否国内企业 |  |
| 是否宁波企业 |  |
| 企业划分标准类型（大型、中型、小型、微型） |  |
| 提供的货物是否本企业制造 | 由本单位制造的货物金额为 万元，提供其他大型企业制造的货物金额为 万元、其他中型企业制造的货物金额为 万元、其他小型企业制造的货物金额为 万元、其他微型企业制造的货物金额为 万元。 |
| 货物原产地是否是中国境内 | 原产地为中国境内货物金额为 万元 |
| 货物原产地是否是宁波 | 原产地为宁波货物金额为 万元 |
| 提供的货物是否是认证的节能产品 | 认证的节能产品货物金额为 万元 |
| 提供的货物是否是认证的环境标志产品 | 认证的环境标志产品货物金额为 万元 |
| 承担的服务是否本企业提供 |  |

**说明：**

1、小型、微型企业提供大、中型企业制造的货物的，视同为大、中型企业。

2、企业划分标准，按照（工信部联企业[2011]300号）文件的规定。

投标人名称（CA签章）：

日 期：

**第七部分 评标办法及评分标准**

**1、评标原则**

评标活动遵循公平、公正、客观的原则，按招标文件中规定的评标方法和标准进行。

**2、评标办法**

本次招标采用综合评分法。

**3、评标委员会**

采购人和采购代理机构根据采购项目的内容特点按照规定组建评标委员会。

评标委员会由采购人代表和评审专家组成，成员人数为5人以上单数，其中评审专家不少于成员总数的三分之二。

**4、评标**

**4.1资格文件审查**

开标后，采购人、采购代理机构按照招标文件的规定对投标人的资格证明文件进行审查，以确定投标供应商是否具备投标资格。

审查内容包括投标人提供的资格证明材料是否齐全规范，投标人资格、信用信息等是否满足招标文件的要求。审查不合格的投标人，不进入技术商务文件评审。（具体见本部分无效投标的认定）

**4.2技术商务文件评审**

4.2.1技术商务文件符合性审查

资格审查通过后，开启合格投标人的技术商务文件。

评标委员会依据招标文件的规定，对投标人的技术商务文件的有效性、完整性和对招标文件的响应程度进行审查，以确定是否对招标文件的实质性要求作出响应。

审查内容包括技术商务文件是否完整、文件签署是否齐全等，还包括投标文件是否对招标文件提出的所有实质性要求和条件作出响应，有无重大偏差；如有重大偏差者，作无效投标处理，不予进入详细评审。（具体见本部分无效投标的认定）

4.2.2技术商务文件详细评审

评标委员会对具备实质性响应的技术商务文件进行进一步评估和比较。

评标委员会成员根据投标人的技术商务文件及相关澄清文件，按照评分标准表（具体见本部分评分标准表）对各投标人技术商务文件进行打分。

评标委员会成员打分采用记名方式，统计时汇总每一细项每位评标委员会成员的评分，取算术平均分（小数点后保留二位小数，四舍五入）。

**4.3报价文件评审**

4.3.1报价文件符合性审查

技术商务文件评审结束后，开启有效投标人的报价文件。

评标委员会对投标人的报价文件的有效性、完整性和对招标文件的响应程度进行审查，以确定是否对招标文件的实质性要求作出响应。

审查内容包括报价文件是否完整、文件签署是否齐全，报价是否超出采购预算或最高限价，投标文件是否对招标文件提出的实质性要求作出响应，有无重大偏差；如有重大偏差者，作无效投标处理，不予进入详细评审。（具体见本部分无效投标的认定）

4.3.2报价文件详细评审

评标委员会对具备实质性响应的报价文件进行进一步评审。

评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标期间合理的时间内提供书面说明，必要时提交相关证明材料，投标人不能证明其报价合理性的，作无效投标处理。

4.3.3报价修正规则

在评审中，对投标报价出现前后不一致的，除招标文件另有规定外，按照下列规定修正：

（1）投标文件中开标一览表内容与投标文件中明细表内容不一致的，以开标一览表为准。

（2）投标文件的大写金额和小写金额不一致的，以大写金额为准。

（3）单价金额小数点或者百分比有明显错位的，以开标一览表的总价为准，并修改单价。

（4）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。

按上述方法调整后的投标报价经投标人确认后产生约束力，投标人不确认的，其投标无效。

4.3.4计算报价得分

报价评审结束后，评标委员会按评分标准表规定计算各投标人的报价得分（小数点后保留二位小数，四舍五入）。

**4.5评审结果**

评标委员会对各投标人技术商务得分和报价得分进行汇总并排序。

评标委员会根据全体评标成员签字的原始评标记录和评标结果编写评标报告。按得分由高到低顺序推荐中标候选人。

**5、询标澄清**

5.1对于投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会可以要求投标人作出必要的澄清、说明或者补正。

5.2除依法进行的澄清、说明、补正外，投标人不得通过对投标文件修正、撤销不符合要求的条款或通过投标文件以外的补充、纠正、佐证等，使其投标成为实质上响应的投标。

**6、无效投标的认定**

实质上没有响应招标文件要求的投标被视为无效投标，投标响应文件有下列情形之一的作无效投标处理：

6.1未按采购公告规定方式获取招标文件的。

6.2仅提交备份电子投标文件的。

6.3不具备招标文件规定的资格要求的或者未按招标文件要求提供资格证明文件的。

6.4单位负责人为同一人或者存在直接控股、管理关系的不同供应商，参加同一合同项下的政府采购活动的（相关投标人均作无效投标处理）。

6.5为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，再参加该采购项目的其他采购活动的。

6.6经查询，投标人被“信用中国”、“中国政府采购网”列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单，且在禁止参加采购期限内的。

6.7投标文件未按招标文件文件要求密封、签署、盖章的。

6.8投标文件项目不齐全，经评审委员会认定为无法评审的。

6.9投标有效期、付款方式、交货（服务）期限、质保期等条款不能满足招标文件要求的。

6.10不符合招标文件中有关分包、转包规定的。

6.11“资格证明文件”或“技术商务文件”中出现本项目的投标总价的。

6.12投标文件的实质性内容未使用中文表述、意思表述不明确、前后矛盾或者使用计量单位不符合招标文件要求的（经评标委员会认定并允许其当场更正的笔误除外）。

6.13投标文件标明的响应或偏离与事实不符或提供虚假材料投标的。

6.14标“▲”的条款不能满足招标文件要求的。

6.15在报价评审时，如发现下列情形之一的，投标文件将被视为无效：

（1）未采用人民币报价或者未按照招标文件标明的币种报价的；

（2）报价超过招标文件中规定的预算金额或者最高限价的；

（3）未按照招标文件规定报价的；

（4）投标报价具有选择性的；

（5）不接受按修正错误的原则修正后的报价的；

（6）评标委员会认为投标人报价明显低于其他通过符合性审查投标人报价的，且在合理的时间内不能提供其报价合理性书面说明的。

6.16有下列情形之一的，视为投标人串通投标，其投标无效，并书面报告财政部门：

（1）不同投标人的投标文件由同一单位或者个人编制；

（2）不同投标人委托同一单位或者个人办理投标事宜；

（3）不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；

（4）不同投标人的投标文件异常一致或者投标报价呈规律性差异；

（5）不同投标人的投标文件相互混装。

6.17投标文件有重大偏差或未实质性响应招标文件要求的或者投标文件含有采购人不能接受的附加条件的。

6.18违反法律、法规及本招标文件规定的其他无效投标情形。

**7、中标原则**

7.1评标委员会根据投标人的技术商务文件和报价文件的总得分高低排定顺序，推荐中标候选人，得分最高者即为中标候选人。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的，按技术方案优劣顺序排列。如出现其它情况，由评标委员会决定。

7.2采购人根据评审报告推荐的中标候选人确定中标供应商。

**8、中标结果**

采购代理机构将中标结果在政府采购指定媒体上公告，并同时向中标供应商发出中标通知书。

**9、评分标准**

9.1评分标准

详见后附评分标准表。

**附：评分标准表**

附：

**评分标准表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **评分项目** | **评分内容及标准** | **分值** |
| **技术商务部分 60分** |
| 1 | 技术方案 | 总体设计：根据学校实际情况，对系统整体设计架构、软硬件环境以及系统整体部署的合理性、完整性、可操作性进行综合评议，对项目建设需求有详细、充分和客观的分析，对重难点分析准确，内容完整。 | **8** |
| 2 | 采购需求响应情况 | 投标人针对招标文件中各项技术指标的规定，进行点对点技术应答，根据投标文件响应程度，对应性、完整性、偏离程度进行评分。完全响应招标文件技术和规格要求表中各项指标的，得20分。标▲的指标（如有）不得负偏离，否则投标无效，标★的指标（如有）每有1项负偏离扣0.02分，一般指标每有1项负偏离扣0.01分，扣完为止。 | **20** |
| 3 | 设备选型 | 根据核心产品选型的品牌、规格及对于本项目的适用性进行综合评议。核心产品包括：智能安全防范信息平台、前端校园安防系统、支撑平台。 | **8** |
| 4 | 实施方案 | 针对本次项目的具体组织实施方案（包括实施组织方案、实施进度计划、风险与缓解措施、质量控制管理、验收等）情况。 | **3** |
| 5 | 人员配置 | 1、拟派项目负责人具有项目管理专业人员（PMP）资格证书、CCIE工程师证书、注册信息安全专业人员（CISP）证书的，每个证书得1分，最高得3分。2、拟派人员中（项目负责人除外），具有大数据分析师CPDA、信息系统项目管理师证书、IT基础架构库认证ITIL Foundation的，每提供1个得0.5分，1人多证可按证书数量得分，本项最多得3分。**在投标文件中提供拟派人员资质证书和社保证明的原件彩色扫描件，未提供的不得分。** | **6** |
| 6 | 质量保证及售后服务 | 根据提供的售后服务方案、备品备件配备情况、升级方案，售后响应能力、响应时效以及其他服务质量与承诺情况进行评议。 | **3** |
| 7 | 培训方案 | 根据培训人员、时间、内容的合理性、可操作性进行评议。 | **2** |
| 8 | 优惠承诺及合理化建议 | 根据供应商提供的合理化建议和优惠承诺进行评议。 | **1** |
| 9 | 投标人证书 | 具有有效质量管理体系认证证书的，得1分；具有有效环境管理体系认证证书的，得1分；具有有效职业健康安全管理体系认证证书的，得1分。具有有效ITSS信息技术服务运行维护证书的的，得1分。**在投标文件中提供证书的原件彩色扫描件，否则不得分。** | **4** |
| 10 | 现场演示 | 根据演示功能点实现情况进行综合打分。投标人自行选择下列任一功能点进行演示。 功能点1：总体态势：校园安全事前预防工作包含浙江等级平安校园要求的食品、卫生、心理健康、学生防溺水、校园欺凌防范和校车等安全指标，辖区内学校达标情况，点击其中一项可查看下属学校达标与未达标明细。功能点2：通过手机客户端演示值班上报功能，在值班巡视的过程中可以产生巡查轨迹，在平台和手机端可查看轨迹图片，可查看统计情况。功能点3：风险预警：风险预警可依据风险矩阵自动统计生成按类型的风险预警排名、按区域的风险预警排名，实时汇聚下属学校高风险事件，包括外来访客黑名单报警、可疑人员抓拍报警、一键报警等，局端可进行现场监控查看，可进行安排督办。评审专家根据操作界面是否友好、系统操作是否简便以及演示功能是否满足采购要求等情况进行评议。优得4.5-5分，良得3.5-4.5分，一般得0-3.5分。**现场演示所需设备请各供应商自备，参加现场演示人员不得超过3人，其中现场陈述者必须为拟派本项目的项目经理或技术负责人，参加演示时需出示本人身份证。****演示时间不超过10分钟，不进行现场演示的投标无效。** | **5** |
| **报价部分 40分** |
| 11 | 评标基准价：参与评审的价格中最低的为评标基准价基准价得分：40分其他供应商的价格分按照下列公式计算：报价得分＝（评标基准价/参与评审的价格）×40注：投标人的报价超过最高限价（不含最高限价）的作为无效报价。 |