**智慧通行项目技术参数**

**第一部分项目需求**

**一、学生公寓门禁建设需求**

**1.学生公寓现状**

学校现有34栋公寓楼、22个出入口。各楼栋虽均配备门禁设备，但因建设时序不同，设备类型繁杂、新旧差异显著，老旧设备故障频发，且通行方式不统一；同时，各楼栋配备宿管人员实行24小时驻点值守。目前，学生公寓通行数据未得到有效挖掘应用，缺乏智能查寝及归寝异常预警系统，无法实时掌握学生在寝动态。

**2.建设需求**

2.1升级、改造学生公寓人脸识别门禁设备

在现有刷卡通道加装人脸识别终端，改造部分刷卡通道位置，新建人脸识别通道机；在各公寓楼出入口增加人脸识别专用摄像机，确保准确抓取学生出入数据；将现有刷脸闸机接入系统统一管理。

2.2部署智慧通行综合管理平台

（1）手机端定向推送预警：系统可实时或定时向辅导员推送晚归、未归、多日无出入记录学生的预警信息。

（2）手机端实时查寝及查看历史记录：系统支持通过手机端实时查看学生在寝情况、历史晚归等学生清单，可按宿舍楼或院系维度查看。

（3）黑名单、陌生人预警：系统自动识别黑名单或陌生人员，通过手机微信端向设置人员推送预警，也可通过宿管室语音或大屏预警。

（4）人员出入公寓报表查询、统计与分析：系统支持电脑端多维度查询，PC端和手机微信端均可查询，可按账号权限查询。

（5）建立人脸识别实时出入公寓可视化平台：可单独显示或与公寓楼大厅电视联动，实时显示学生出入情况，支持语音播报及弹窗预警，分类显示实时出入数据。

（6）与校园大门刷脸门禁系统联动：实现公寓楼与校园大门通行记录联动分析，分级预警，如未在寝室但在校园内触发二级预警，出校园触发一级预警。

2.3支持辅导员与未归学生的互动

辅导员可在手机端一键发起与未归学生互动，核实去向；学生收到消息后可上传自拍照片并描述，辅导员确认状态和位置后提交核实结果，也支持线下核实后手工填写。

2.4学生刷脸通行权限的联动

（1）初始化：与学生公寓管理平台联动批量初始化刷脸权限。

（2）入住：与异动信息联动自动下发对应宿舍楼刷脸权限。

（3）调宿：与调宿舍信息联动自动调整刷脸权限。

（4）退宿：与退宿舍信息联动自动取消刷脸权限。

（5）零星调整：支持管理人员后台零星调整。

**3.附各公寓出入口改造要求及主要设备配置表**

| **学生公寓智能门禁主要设备配置表** | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **宿舍楼号** | **现有通道数** | **是否利旧** | | | **新增设备数量** | | | | | | |
| **闸**机 | **人脸**设备 | **现有大屏** | **通道数** | **单机**芯数 | **双机**芯数 | **人脸识别**面板机 | **抓拍摄像机** | **可视化大屏** | **可视化显示安卓盒子** |
|
|
| 1号楼 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 |
| 2号楼 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 |
| 3号楼 | 三通道 | 利旧 | 利旧 | 利旧 | 0 | 0 | 0 | 0 | 2 | 0 | 1 |
| 4号楼 | 三通道 | 不利旧 | 0 | 利旧 | 0 | 0 | 0 | 0 | 2 | 2 | 2 |
| 0 | 0 | 不利旧 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 |
| 5号楼 | 三通道 | 不利旧 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 |
| 6号楼 | 三通道 | 不利旧 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 |
| 7号楼 | 三通道 | 利旧 | 0 | 0 | 0 | 0 | 0 | 6 | 2 | 1 | 1 |
| 8号楼 | 四通道 | 不利旧 | 0 | 利旧 | 三通道 | 2 | 2 | 6 | 2 | 0 | 1 |
| 9号楼 | 0 | 三通道 | 2 | 2 | 6 | 2 | 1 | 1 |
| 10号楼 | 四通道 | 不利旧 | 0 | 利旧 | 三通道 | 2 | 2 | 6 | 2 | 0 | 1 |
| 11号楼 | 0 | 三通道 | 2 | 2 | 6 | 2 | 1 | 1 |
| 12号楼 | 二通道 | 不利旧 | 0 | 0 | 二通道 | 2 | 1 | 4 | 2 | 1 | 1 |
| 13号楼 | 四通道 | 不利旧 | 0 | 利旧 | 三通道 | 2 | 2 | 6 | 2 | 0 | 1 |
| 14号楼 | 0 | 三通道 | 2 | 2 | 6 | 2 | 1 | 1 |
| 15号楼 | 四通道 | 不利旧 | 0 | 利旧 | 三通道 | 2 | 2 | 6 | 2 | 0 | 1 |
| 16号楼 | 0 | 三通道 | 2 | 2 | 6 | 2 | 1 | 1 |
| 17号楼 | 三通道 | 不利旧 | 0 | 利旧 | 三通道 | 2 | 2 | 6 | 3 | 0 | 1 |
| 18号楼 | 三通道 | 不利旧 | 0 | 利旧 | 三通道 | 2 | 2 | 6 | 3 | 0 | 1 |
| 19号楼 | 四通道 | 不利旧 | 0 | 0 | 三通道 | 2 | 2 | 6 | 2 | 1 | 1 |
| 20号楼 | 不利旧 | 0 | 0 | 三通道 | 2 | 2 | 6 | 2 | 1 | 1 |
| 21号楼 | 三通道 | 利旧 | 利旧 | 利旧 | 0 | 0 | 0 | 0 | 2 | 0 | 1 |
| 22号楼 | 三通道 | 利旧 | 利旧 | 利旧 | 0 | 0 | 0 | 0 | 2 | 0 | 1 |
| 23号楼 | 三通道 | 利旧 | 利旧 | 利旧 | 0 | 0 | 0 | 0 | 2 | 0 | 1 |
| 24号楼 | 三通道 | 利旧 | 利旧 | 利旧 | 0 | 0 | 0 | 0 | 2 | 0 | 1 |
| 25号楼 | 三通道 | 利旧 | 利旧 | 利旧 | 0 | 0 | 0 | 0 | 2 | 0 | 1 |
| 26号楼 | 三通道 | 利旧 | 利旧 | 利旧 | 0 | 0 | 0 | 0 | 2 | 0 | 1 |
| 27号楼 | 四通道 | 不利旧 | 0 | 0 | 四通道 | 2 | 3 | 8 | 4 | 1 | 1 |
| 28号楼 | 四通道 | 不利旧 | 0 | 0 | 四通道 | 2 | 3 | 8 | 4 | 1 | 1 |
| 29号楼 | 四通道 | 不利旧 | 0 | 0 | 四通道 | 2 | 3 | 8 | 4 | 1 | 1 |
| 30号楼 | 四通道 | 不利旧 | 0 | 0 | 四通道 | 2 | 3 | 8 | 4 | 1 | 1 |
| 31号楼 | 四通道 | 利旧 | 利旧 | 利旧 | 0 | 0 | 0 | 0 | 4 | 0 | 1 |
| 32号楼 |
| 33号楼 | 二通道 | 利旧 | 利旧 | 利旧 | 0 | 0 | 0 | 0 | 2 | 0 | 1 |
| 34号楼 | 二通道 | 利旧 | 利旧 | 利旧 | 0 | 0 | 0 | 0 | 2 | 0 | 1 |
| **汇总** | | | | | | **34** | **37** | **114** | **80** | **24** | **40** |

**二、校园大门门禁建设需求**

**1.建设现状**

学校目前有东、南、西、北四个大门，各有保安24小时驻点服务。学生凭纸质请假条进出，外来访客需提前在保卫部门报备。已对各大门进行现场勘测，东门左右出入口最大宽度分别为2.2米，南门2.9米，西门2.1米，北门左右出入口3.5米（以投标人现场勘测为准）。

**2.建设需求**

2.1新建设校园大门刷脸门禁闸机

各大门安装人脸识别智能通行闸机，兼顾行人与非机动车通行；加装专用摄像机，覆盖入口通道，识别并预警尾随及黑名单人员，准确抓取学生出入数据，提高归校数据分析准确性；通道空余部分用铝合金护栏围起，仅允许通过闸机通行；增加可伸缩、坚固耐用的棚子，用于挡雨遮阳；支持值班室一键开闸和遥控器现场开闸。

2.2部署访客预约系统

支持访客扫码填报预约申请，校外人员可手机预约并上传人脸照片，经校内管理人员审批后，可刷脸通过大门口闸机；访客预约信息与现有车辆道闸系统联动，审批后的车辆可直接通行；校外访客还可通过访客通道刷身份证或出示二维码，经识别后开闸。

2.3部署动态人脸识别专用摄像机

在各大门出入口增设动态无感知同时多人识别专用摄像机，预警尾随及黑名单人员，准确抓取学生出入数据，提升归校数据分析准确性；支持保卫处管理人员后台查询师生通行记录。

2.4实现以图搜人功能

上传照片可查询对应学生身份信息及通行记录。

2.5与学生公寓楼刷脸门禁系统联动

实现学生公寓楼与校园大门通行记录联动分析，分级预警。

**3.附各校门出入口改造要求及主要设备配置表**

| **校园大门智能门禁主要设备配置表** | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **位置（面向校外方向）** | | **人脸摆闸机通道数** | | | **人脸识别面板机** | **人脸识别抓拍摄像机** | **备注（宽度指的是净宽）** |
| **通道数** | **单机芯数** | **双机芯数** |
| 西门 | 右侧 | 双向五通道 | 2 | 4 | 10 | 4 | 安装一组双向五通道刷脸摆闸（双向刷脸通行），通道宽度均为60cm |
| 双向一通道 | 2 | 0 | 2 | 安装一组通道宽度为150cm的三轮车摆闸通道（也支持设置成仅两轮电瓶车车主、三轮车主刷脸通行） |
| 东门 | 左侧 | 单向三通道－进 | 2 | 2 | 3 | 2 | 两侧均安装三通道刷脸摆闸（单向刷脸通行），2个通道约60cm宽仅供行人刷脸通行，另外1个通道110cm宽，为非机动电瓶车道刷脸通行（也支持行人通行） |
| 右侧 | 单向三通道－出 | 2 | 2 | 3 | 2 |
| 南门 | 右侧 | 双向三通道 | 2 | 2 | 6 | 2 | 两个通道宽60cm，另一个通道宽110cm（支持行人和电瓶车通行）。 |
| 北门 | 左侧 | 单向二通道－进 | 2 | 1 | 2 | 2 | 2个通道60cm宽；另外1个通道110cm宽，支持行人和电瓶车通行。 |
| 单向一通道－进 | 2 | 0 | 1 |
| 右侧 | 单向二通道－出 | **2** | **1** | **2** | **2** |
| 单向一通道－出 | 2 | 0 | 1 |
| **合计** | | | **18** | **12** | **30** | **14** | 实际通道宽度以现场测量为准，通道设备需满足甲方要求。 |

**三、图书馆门禁建设需求**

**1.建设现状**

学校图书馆设有三个出入口，门禁设施建设情况如下：2019年完成二楼大厅左右通道双向6通道人行闸机建设，采用刷卡通行模式；同期建成一楼南门门禁；一楼北门未配备门禁设备。

**2.建设需求**

在现有刷卡通道机上加装人脸识别终端，实现刷脸通行；在一楼北门右侧新建一组双通道人脸识别闸机；支持管理人员后台查询师生通行记录；支持将学生刷脸进馆数据推送给自习室预约系统用于无感签到；与现有图书借阅系统对接实现刷脸还书。

**3.附各出入口改造要求及主要设备配置表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **位置（面向校园外方向）** | | **现有通道数** | **增加设备** | | | |
| **通道数** | **单机芯数** | **双机芯数** | **人脸识别面板机** |
| 二楼 | 北－左侧 | 现有3通道 | 0 | 0 | 0 | 6 |
| 北－右侧 | 现有3通道 | 0 | 0 | 0 | 6 |
| 一楼 | 南门 | 现有4通道 | 0 | 0 | 0 | 8 |
| 北门－右侧 | 0 | 双向两通道 | 2 | 1 | 4 |
| 刷脸还书 | |  |  |  |  | 5 |
| **合计** | | | | **2** | **1** | **29** |

**四、人脸识别数据安全保护系统及相关系统建设需求**

**1.建设现状**

随着人脸识别技术应用增多，国家重视人脸数据管理使用，相继出台《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《人脸识别技术应用安全管理办法》。目前学校照片多采用传统明文存储和U盘拷贝管理，易泄露，部分上传业务系统但缺乏整体安全架构，未体现个人信息保护合规要求，有信息安全隐患。我校拟建设多场景刷脸门禁，建成后存在多品牌设备统一管理、数据安全保障、数据使用合规三大问题，需建设人脸数据合规、安全和统一管理平台。

**2.建设需求**

本项目目标是实现师生底片一次采集，满足多品牌、多算法质量要求；手机端随时采集；数据加密安全保存、传输，防篡改校验；提供可视化报告，掌握人脸采集情况；个人数据全流程合规。

2.1核心内容包括：

（1）建设安全统一人像库，实现授权、采集、核验、存储、分发、销毁、溯源七大人脸数据处理活动全生命周期的管理，达到合规、安全和统一管理的目的。

（2）对第三方人脸业务系统加密和脱敏管理，实现人员基础信息的加密和脱敏，面板机内无法查询真实人员信息。提供溯源方案，恢复加密和脱敏后的数据。此功能降低面板机内人脸数据泄露的风险等级。

（3）建设人脸生物因子身份认证系统，提供人脸生物因子认证能力，通过提供安全的集成方法，嵌入到业务系统，在静态账号密码的基础上增加人脸因子认证保障，提升数据中心基础设施、网络及业务系统的认证安全。支持PC端和手机端的人脸认证。建设私有化部署的人脸识别算法软件，包含活体检测、人脸1:1算法、人脸1:N算法和照片质量检测等算法私有化部署。

2.2通过项目建设达成核心目标：

（1）管理上统一异质算法底片，合规、安全使用和管理数据，保障数据安全，满足合规要求。

（2）在用户体验上打消疑虑，一次采集满足多场景需求，提升满意度。

（3）提供创新的人脸生物因子身份认证系统，用于学校统一身份认证的激活、找回密码、修改手机号等场景，安全便捷实现身份认证。

（4）制定校级人脸识别技术应用规范，统一人脸识别接入要求，整体实现人脸数据可视化管理、合规遵守法律要求、安全保障人脸数据安全。

**3.技术要求**

（1）易用性要求：本项目建设着重服务于全校师生、集团单位、第三方人员等，因此要求系统建设要有较强的用户体验，满足易用性使用要求，可支持PC端、移动端样式呈现，且根据不同呈现载体的特点，能够灵活地设计出适合的呈现样式。

（2）扩展性要求：系统最大可支持50万张人脸底库，接入的人脸识别应用不限数量。

（3）兼容性：系统前端采用H5方式，兼容主流浏览器（Chrome、Firefox、Safari、Edge等），后端采用Java语言开发。支持主流的算法厂家集成（如海康、大华、宇视、旷视、商汤等），同时也承诺对小众品牌的对接支持。

（4）稳定性要求：系统运行后，将为全校提供服务，因此要求系统具备较强的稳定性，可保障业务7\*24小时的连续性。系统支持不低于5000人同时在线，不低于500用户的并发访问量，页面加载时间不超过4秒。

（5）平台须具有良好的开放性，提供数据开放API接口，能方便地兼容与其他应用系统的对接。

（6）人脸生物因子身份认证，支持所有B/S端业务直接调用，无需进行人脸识别认证流程开发，至少保证15QPS的认证并发。

**4.附系统建设清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **事项** | **单位** | **数量** |
| 1 | 人脸数据安全保护系统 | 套 | 1 |
| 2 | 人脸识别算法分析管理平台 | 套 | 1 |
| 3 | 智慧通行综合管理平台 | 套 | 1 |
| 4 | 访客预约系统 | 套 | 1 |
| 5 | 智能门禁可视化显示系统 | 套 | 1 |
| 6 | 网络安全等级保护测评（第二级） | 项 | 1 |

**第二部分设备清单及技术参数**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **技术功能参数要求** | **数量** |
| 1 | 智能翼闸 | **闸机数量（机芯类型）：单机芯36台；双机芯38台。**  1.机箱材料：国标SUS304不锈钢；材料厚度≥1.2mm（国标）。  2.外形尺寸：长1300mm（±100）\*宽300mm（±20mm）\*高1000mm（±10mm）；机身呈圆弧形（外形需经过校方最终确认）。  3.通道宽度：600mm(±50mm)；挡板材料：塑料亚克力、有灯带。  4.红外对数：≥4对。  5.正常使用寿命：≥1000万次。  6.自动复位功能：开闸后，在规定的时间内未通行系统将自动上锁，通行时间可调。  7.支持断电自动开闸、支持消防联动自动开闸，恢复正常信号后，门翼复位。  8.具有红外防夹功能；具有防尾随功能，能实现防尾随功能的设备应对尾随事件警示。  9.设备集成语音模块，可根据不同事件同时结合用户设定播放提醒语音，语音播放类型支持不少于20种/支持自定义。  10.应具备部件自检功能。  ▲如在内置液晶屏上显示故障类型，并可实现故障语音播报，故障检测类型包括电机故障、限位故障、红外故障等。  11.设备支持通过管理平台和终端设备对通道实现远程开门、关门、常开、常闭、解除常开、解除常闭等功能。终端设备应能实时监控设备的运行状态。（须提供真实系统的功能截图或产品厂商的官网截图或带有CMA标识的检测报告扫描件等相应的佐证材料，优先级为检测报告〉功能截图〉官网截图）。  12.支持通过终端设备（如人脸识别终端等）设置闸机开闸通行语音。  13.可实现通过终端设备（如人脸识别终端等）设置开闸方式：协议开闸/继电器开闸。  14.可实现通过终端设备（如人脸识别终端等）进行尾随/迂回/逗留设置。  15.可实现通过终端设备（如人脸识别终端等）设置通行方式：双向认证通行/双向自由通行/左向自由、右向认证通行/左向认证、右向自由通行。（须提供真实系统的功能截图或产品厂商的官网截图或带有CMA标识的检测报告扫描件等相应的佐证材料，优先级为检测报告〉功能截图〉官网截图）。  16.设备应支持异常开门、翻越、滞留、反向闯入、尾随、通行超时、误闯等行为检测，且会有报警提示（包括语音播报、指示灯等），同时上传报警事件。 | 74台 |
| 2 | 智能摆闸 | **闸机数量（机芯类别）：单机芯18台，双机芯12台。**   1. 外观尺寸：长（1400±200）\*宽（200±50）\*高（1020±200）（mm）。   2.通道宽度：600～1000mm（±50mm），支持定制；摆臂材质：不锈钢/亚克力。  3.板材规格：304不锈钢；板材厚度≥1.2mm（国标）。  4.红外对数：≥4对。  5.支持断电自动开闸、支持消防联动自动开闸，恢复正常信号后，门翼复位。  6.具有红外防夹功能；具有防尾随功能，能实现防尾随功能的设备应对尾随事件进行警示。  7.设备集成语音模块，可根据不同事件同时结合用户设定播放提醒语音，语音播放类型支持不少于20种可选/支持自定义。  8.应具备部件自检功能。  ▲如在内置液晶屏上显示故障类型，并可实现故障语音播报，故障检测类型包括电机故障、限位故障、红外故障等。  9.支持通过人脸识别终端设备重启闸机。  10.支持导出人脸识别终端的日志，包括：闸机尾随、逆向闯入、翻越、非法闯入等异常通行事件。  11.支持通过终端设备（如人脸识别终端等）设置闸机音量。（须提供真实系统的功能截图或产品厂商的官网截图或带有CMA标识的检测报告扫描件等相应的佐证材料，优先级为检测报告〉功能截图〉官网截图）。  12.支持通过终端设备（如人脸识别终端等）设置通道模式：人行模式/车行模式。（须提供真实系统的功能截图或产品厂商的官网截图或带有CMA标识的检测报告扫描件等相应的佐证材料，优先级为检测报告〉功能截图〉官网截图）。  13.可实现通过终端设备（如人脸识别终端等）设置闸机开关门力度。（须提供真实系统的功能截图或产品厂商的官网截图或带有CMA标识的检测报告扫描件等相应的佐证材料，优先级为检测报告〉功能截图〉官网截图）。  14.设备应支持异常开门、翻越、滞留、反向闯入、尾随、通行超时、误闯等行为检测，且会有报警提示（包括语音播报、指示灯等），同时上传报警事件。 | 30台 |
| 3 | 人脸识别面板机 | 1.显示屏：不低于8寸的触摸屏，分辨率不应低于1280\*800。  2.摄像头：设备应采用高清双目相机1路分辨率不低于1920\*1080的可见光摄像头，1路分辨率不低于1920\*1080的红外补光摄像头。  3.存储容量：支持至少100000张IC卡；支持至少100000张人脸，支持至少500000条事件。  4.出入认证方式：系统能对门的开启方式（卡、人脸、密码、二维码等）的使用权限进行组合设置，多重认证，实现不同安全级别场景的权限管理。1）人脸；2）人脸或刷卡；3）人脸+刷卡；4）人脸+密码；5）二维码。（须提供真实系统的功能截图或产品厂商的官网截图或带有CMA标识的检测报告扫描件等相应的佐证材料，优先级为检测报告〉功能截图〉官网截图）。  5.接口包含但不限于：  （1）网络接口：RJ45（LAN）接口\*1、WIFI模块\*1。  （2）串行通信接口：RS485接口\*1、韦根接口\*1、串口\*1。  （3）USB接口：USB接口\*1等。  （4）门控相关接口：门磁输入接口\*1、开门按钮输入接口\*1、继电器\*1。  （5）报警功能接口：报警输入接口\*2、报警输出接口\*1。  （6）音频接口：3.5mm音频输出接口\*1、扬声器\*1、麦克风\*1。  ▲（7）防护与控制接口：机械防拆开关（防拆按钮）\*1、Reset复位按钮\*1、状态指示灯\*1。  ▲6.防手机复制卡功能：应能对手机NFC复制IC卡进行检测，并不允许此类手机复制卡号后直接通行。   1. 支持单人和多人识别模式；支持远程/本地识别模式；具有1:N人脸比对模式；具有1:1人证核验模式。(▲具有1:1:1人脸抓拍图、身份证照片、人脸注册图三重比对功能模式。)识别模式支持设置和切换。（须提供真实系统的功能截图或产品厂商的官网截图或带有CMA标识的检测报告扫描件等相应的佐证材料，优先级为检测报告〉功能截图〉官网截图）。   8.人脸比对平均时间：人脸比对平均时间应<150ms。  9.刷卡类型：（1）支持能识读Mifare卡、CPU卡、IC卡、国密卡和身份证序列号；▲（2）具有超级SIM3.0卡识别功能。（须提供真实系统的功能截图或产品厂商的官网截图或带有CMA标识的检测报告扫描件等相应的佐证材料，优先级为检测报告〉功能截图〉官网截图）。  10.对A4纸打印照片、电子照片、视频图像中的人脸不能进行人脸识别；对3D头模、头套人脸不能进行人脸识别；对T型面具人脸不能进行人脸识别等。  11.刷卡：支持屏下NFC刷卡功能。  ▲12.当设备被拆除时，具有防拆报警功能；  13.含配套支架。 | 173个 |
| 4 | 人脸识别抓拍摄像机 | 1.视频分辨率&帧率：支持多码流同时输出访问，各码流应满足包含但不限于：2688×1520（25fps）、2560×1440（25fps）、1920×1080（25fps）、1280×720（25fps）。  2.具备至少4颗补光灯（红外不少于2颗）。红外开启条件下，在人脸比对模式下，支持最远可对10米处的人脸进行检出和识别。（须提供真实系统的功能截图或产品厂商的官网截图或带有CMA标识的检测报告扫描件等相应的佐证材料，优先级为检测报告〉功能截图〉官网截图）。  ▲3.支持对行进方向正对摄像机、平均行进速度不大于5m/s的人员进行人脸抓拍。（须提供真实系统的功能截图或产品厂商的官网截图或带有CMA标识的检测报告扫描件等相应的佐证材料，优先级为检测报告〉功能截图〉官网截图）。  4.接口应具备不少于：1个RJ45网口、2路报警输入/1路报警输出、1个复位按钮、内置MIC和扬声器，1个TF卡槽（最大支持256GB）、1个DC12V电源接口等。  5.支持最优抓拍模式，最快抓拍模式，支持人脸抓图跟背景大图，支持配置是否推送背景大图，支持配置背景大图的图片质量（高、中、低），抓拍分辨率（2688\*1520、2560\*1440、1920\*1080、1280\*720），支持配置智能应用识别区域。人脸最快抓拍模式下，支持同一画面内30个人脸并发检出功能。  6.支持对过曝、欠曝、阴阳脸、背光、光线较暗等光线条件下的人脸进行抓拍功能；  7.支持进行人脸比对时，对照片、离线视频中的人脸显示非活体，支持设置活体检测阈值。  8.支持对视频画面中的人员进行人脸识别比对，并显示人脸相似度。支持设置人脸识别区域，支持设置最优识别、快速识别模式，支持设置单次最大识别时间、两次识别间隔和识别阈值。人脸底库容量支持最多10万张，最大支持128个人员组。  9.采用多人依次循环通过进行测试，红外开启条件下，试验时被检测人脸完整无遮挡，正脸通过摄像机。在人脸比对模式下，人脸错误识别率≤1%，人脸正确识别率≥99%。  ▲10.报警管理：支持设置门禁应用事件的报警联动方式，包括上传服务器、上传FTP、报警录像、报警输出、韦根输出、语音播放。支持设置语音播放内容。  11.其他：学生公寓4、5、6三栋公寓楼将改造为教职工公寓，改造后门禁采用动态、无感、同时多人识别的刷脸模式：1）即在摄像机覆盖范围内，师生被同时识别，门的电磁锁弹开，师生拉开门通行后闭门器自动将门闭合，电磁锁再次锁上，陌生人无法开启；2）将人脸识别摄像机识别的结果在可视化大屏里进行即时展示，用于告知被识别人识别的结果；3）还应包含4、5、6三栋公寓楼实现以上功能所包含的闭门器、电磁锁等相关的辅材。 | 94个 |
| 5 | 身份证阅读器 | 1.供电：5V，1A。  2.工作温度：-20~60℃。  3.身份证阅读器模块性能：工作频率：13.56MHz±7kHz（fc）；阅读距离：0~3cm；读卡速度：＜1s。  4.二维码阅读器性能：识读包含但不限于以下类型的二维码：QR Code,Codeblock A、Codeblock F、PDF417、Micro PDF417、GS1 Composite Codes、Data Matrix、MaxiCode、Aztec、HANXIN.识读景深：Code39(13mil）：2～15cm；QR(15mil）：3.5～9cm。ENA-13(13mil):2～15cm.解码响应时间：0.5s以内。  ▲5.为确保系统的稳定，需与人脸识别面板机为同一品牌。 | 4个 |
| 6 | 人脸识别实时监控可视化大屏 | 屏幕尺寸：不低于65英寸 | 24台 |
| 7 | 人脸识别  实时监控  可视化主机盒子 | 用于配合楼宇级可视化大屏数据实时分析处理展示。  运行内存：不低于2GB。  CPU：不低于64位四核1.5GHz。  GPU：不低于750MHz。  存储内存：不低于8GB。 | 40台 |
| 8 | 监控磁盘存储阵列 | 1.处理器：1颗64位多核处理器。  2.系统内存：8GB（可扩展至64GB）。  3.系统盘：1×240GB SSD（后置）。  4.存储接口：48个SATA接口，支持硬盘热插拔。  5.接口不低于：2个千兆数据网口，1个千兆管理口，1×COM，2×USB2.0，2×USB3.0，1×VGA。  6.整机电源：1200W，1+1冗余电源。  8.视频性能：最大支持接入450路（最大接入带宽900Mbps）。  9.回放性能：最大支持45路2Mbps。  10.事件录像：最大支持200路2Mbps。  11.支持视频流直写。  12.支持ONVIF、GB/T 28181、RTSP等标准协议。  13.支持VRAID、RAID0、1、5、6、10等多种RAID模式。  15.支持RAID降级可读写（VRAID），支持全局热备（RAID0、1、5、6、10），多重保护数据安全。  16.支持RAID即建即用，支持存储空间扩展。  17.支持局部重构，原盘或其克隆盘拔出设备后再插回，未被覆盖数据可快速恢复。  18.支持定时录像、事件录像、手动录像等多种录像方式。  19.支持视频检索功能，按照监控点编号、录像类型、时间组合等条件查询。  20.支持视频回放功能：正序回放、定位回放、倍速回放等功能。  21.支持按需取流功能，未处于录像计划时间内的通道不占用网络带宽。  22.存储容量：内含硬盘，存储不低于3个月的视频流。 | 1套 |
| 9 | 校园大门护栏 | 材质为铝合金材质，颜色与学校建筑风格相协调，满足现场安装需求，达到验收状态。 | 6套 |
| 10 | 遮阳防雨罩 | 与人脸识别面板机配套使用，达到遮阳防雨效果， | 30个 |
| 11 | 人脸数据  安全保护  系统 | ★该系统需满足《人脸识别技术应用安全管理办法》中的所有要求。  ★1.移动端平台授权：用户需在移动端查看授权协议（《用户协议》《隐私政策》《人脸数据应用范围说明》），并同意授权协议后进行人脸数据采集。  2.移动端应用授权：支持用户在移动端根据人像应用场景进行独立的授权及取消授权操作，授权后在管理后台可查看此应用场景已获取此用户人脸数据；取消授权后可查看此应用场景已删除此用户人脸数据。  3.移动端通知：移动端展示最新公告信息，支持查看历史公告信息。协议到期系统发送通知。  ★4.人脸数据全生命周期流转履历：支持在移动端查看个人信息全生命流转履历，展示根据时间轴展示应用授权记录、采集平台授权记录、每个获取人脸信息的业务系统的最新获取时间记录、业务删除人脸的时间记录。  5.语言切换：支持移动端中英文系统语言切换功能。切换为英文时，页面文本字段都应为英文显示，切换为中文时，页面文本字段都应为中文显示。  6.采集端入口：采集页面支持以H5方式挂载到微信公众号、企业微信、钉钉、APP等载体内，支持调用摄像头进行拍照上传，拍照页面需展现虚线框来定位人脸位置。  7.照片编辑：支持对照片进行缩放、旋转、更换背景为纯色操作。  8.照片核验：支持移动端用户授权后自助拍照上传人像数据，经系统核验通过后，页面呈现算法核验结果；支持将核验结果失败原因返回到采集端告知用户。支持用户对没有核验通过的算法底片进行重新采集。  9.校外人员采集：可实现校外人员可通过扫描采集配置管理中的二维码或点击采集链接，进入采集界面，输入手机号并验证验证码。一旦手机号与数据库内信息比对成功，即可进行人像采集。  10.授权协议编写：支持授权协议（《用户协议》《隐私政策》《人脸数据应用范围说明》《隐私扩展协议》）的中英文协议编写、发布及更新，支持设置协议到期期限。  11.授权模式：用户同意系统授权协议后，所有第三方系统默认不直接获取人脸数据权限，需要获取数据授权的，需要用户自己对第三方系统进行独立授权后获取，亦支持取消授权。  12.公安可信身份核验：支持存储用户可信身份底片，底片数据获取应支持导入系统获取和用户上传照片与公安可信身份认证平台核验身份后获取。  13.系统具备与多品牌算法厂家的软件兼容能力，支持第三方人脸识别算法的注册和共享管理，可以适配主流厂家的算法。  ▲14.内置第三方算法对接配置项：系统内置第三方算法接口配置项不少于8个品牌，算法类型总数不少于16个。新增算法绑定时，可直接通过选择接口品牌和类型完成算法绑定，不需要额外开发。  15.支持对采集照片进行各项人脸质量检测，检测范围有真人人脸、是否佩戴眼镜、左右眼睛睁合、是否佩戴口罩、人脸倾斜角度、人脸在照片中占比、人脸面部光线、人脸面部是否被遮挡、人脸面部是否溢出照片检测。  16.算法核验：支持在人脸采集时同时用多个厂家的照片质量核验算法做照片质量核验。在核验前应根据算法厂商质量要求对照片进行二次处理，以提高核验通过率。  17.特征值采集：支持人脸算法厂家提供的特征值提取方法或专用接口，精确获取该厂家独有的人脸特征值，并进行加密存储。  18.数据结构及存储：支持将人员的个人信息和生物特征信息进行逻辑或物理方法隔离存储，实现信息库的独立部署及访问。  19.数据加密：支持对个人敏感信息、生物样本信息、生物特征值等个人隐私数据进行国密算法加密存储。  20.数据篡改告警：支持对非法篡改数据进行发现监控，包括但不限于篡改痕迹发现、篡改数据阻止流出、篡改告警实时通知安全管理员等。  21.支持对系统人员数量、系统授权人数、系统采集人像人数、接入算法健康监控、第三方业务系统（应用场景）当天接口情况、人像采集实时动态、接入第三方业务系统（应用场景）情况（接入系统数、应下发人数、实际下发人数）、人像实时核验动态。▲接入第三方业务系统数据销毁动态（应销毁人数、已销毁人数、未销毁人数、销毁率）进行统计。  ★22.人脸采集统计查看：可对人像的采集及人像核验状态进行统计。支持树形组织结构，可统计部门下的各个子部门按照条件的数据查询。  ★23.可查询结果包括但不限于：总人数、全系统通过人数、全系统通过率、未通过全系统核验人数、未核验人数、系统核验失败人数、无人像人数、全部授权人数、未授权人数、取消授权人数、可信身份核验通过人数、可信身份核验失败人数、其他算法系统核验通过及失败人数统计等。  24.人员采集管理：支持对人像底片、账号、姓名、部门/学院、人像来源、人员类型、授权状态、核验状态、核验失败原因、展示照状态、关联应用、时间、查看、下发人像（支持选择第三方应用系统将人像数据手动下发到第三方应用系统）进行管理。  25.人员批量核验：支持人像数据批量核验（可选择核验对象、1:1身份识别对比算法、质量比对算法进行人像数据批量核验）。  26.人员数据导出：支持人像数据按照组织机构、人员类型、核验状态、算法系统、人像类型、导出文件（支持人像压缩包及Excel表格导出）进行导出。导出的底片可以指定姓名、工号、身份证号作为命名，也可以根据姓名、工号、身份证号任意组合排序命名。  27.人员数据导入：支持人像数据按照jpg图片上传及zip压缩包导入。  28.第三方应用绑定：支持第三方应用绑定系统获取人像数据。  ▲绑定内容包括：应用名称、应用介绍、算法平台、数据类型、展示照（需要/不需要）、水印类型、权限范围（组织机构选择/用户群组选择）、组织机构、权限控制（启停第三方获取数据的接口）、保密协议签订情况（包含未签订和已签订）、传输加密类型选择。  29.支持对第三方系统获取数据的配置，可以可视化配置下发对应需要算法的Base64格式照片或特征值（Base64和特征值二选一）。  ★30.获取数据范围管理：支持第三方系统获取数据范围配置，数据范围可以选择组织机构和预先定义的用户群组，可查询第三方系统允许获取的人员数量和详细列表。  31.人像数据下发到第三方应用方式：支持自动下发：人像采集后，系统自动将人脸数据下发到第三方应用场景，并展示下发记录日志；支持手动下发：通过点击下发按钮将用户人脸数据下发到第三方应用场景，并展示下发记录日志。  32.加密管理：支持对用户及人脸数据传输进行加密及管理。支持国密算法加密。  ★33.防篡改管理：支持传输数据过程中加入防篡改信息进行篡改检测。  34.人脸数据分发API接口：支持提供数据异动接口、数据全量更新接口、时间段更新接口、增量更新接口、差异比对接口，实现对系统数据的分发管控。  35.第三方接入开发SDK：第三方接入开发SDK应提前封装好现成的API接口开发SDK，支持第三方直接引入SDK获取底片数据。并应提供SDK使用文档。  36.授权取消管理：支持用户在移动端一键取消授权，用户取消授权后系统会执行销毁任务，系统应在7个工作日内在人像库内对用户底片删除。支持对调用过此用户数据的第三方应用发送人像销毁指令，第三方应用删除数据后给到平台消息回执。支持按照约定触发销毁条件，自动触发销毁特定人员数据。  37.后台人脸全生命周期溯源：通过用户的账号或姓名，对该用户的人脸全生命周期进行溯源。按照时间轴模式，展示应用授权记录、授权记录、采集记录、核验记录、每个获取人脸信息的业务系统的最新获取时间记录、业务删除人脸的回执时间记录，清晰地看到人脸在各业务系统间的流动履历。  38.数据同步溯源：支持记录数据同步时间、同步数据量、同步成功/失败结果、原因等信息。  39.可信身份溯源：支持记录用户通过可信身份核验的信息。  ★40.应用授权溯源：支持记录用户每次同意应用授权、取消应用授权、删除应用授权的行为信息。  41.导出溯源：支持记录用户每次导出的行为信息，记录操作人账号、操作人姓名、操作端、操作系统、浏览器、操作IP、批次号、事件类型、数量、操作耗时（秒）、事件描述、操作结果、失败原因、操作时间  42.人像分发溯源：  （1）支持记录人像分发到第三方系统的操作事件，应支持按照批次下发及实时下发日志查询；  （2）支持批量下发日志按照数据获取方式、批次信息、获取数据量、获取数据时间、消耗时间查询；  （3）支持实时下发日志按照下发人员信息、批次号、部门、获取系统、获取时间查询。  43.人像回执溯源：支持以指令编号的方式记录发给第三方系统的人脸信息获取、删除通知指令详情及第三方系统执行该指令后的回执结果。每个指令编号都需要绑定展示其对应的通知和回执。支持按照账号、姓名、应用名称、事件类型、事件描述、操作结果、操作时间查询。  44.导出人脸数据溯源查询：导出的照片带有透明水印，使用水印解析功能提取出水印编号；通过该编号查询对应的人脸数据导出日志，日志信息应包含导出时间、导出操作人员账号、导出操作人员姓名、导出操作IP地址、被导出人员姓名、账号和部门信息等内容。  45.下发到第三方应用场景的人脸数据溯源查询：下发的照片带有透明水印，使用水印解析功能提取出水印编号；通过该编号查询对应的人脸数据下发日志，日志信息应包含获取数据的应用名称、获取时间、事件描述等内容。  46.导出任务中心：  （1）支持记录执行导出任务的信息有导出类型、文件名称、创建时间、导出数据量、导出进度、导出结果、下载次数、结果文件下载。  （2）支持人脸数据文件下载时发送短信验证码给安全管理员，输入安全管理员收到的验证码后下载文件。  47.审核任务中心：支持记录系统管理员导出人员数据的申请，系统安全员可以对申请进行审批，只有审批后，系统管理员才能导出审批流程内对应的人员的人脸数据。  48.组织机构管理：支持通过与学校数据平台集成自动同步更新、手动新增方式创建组织机构部门及多级子部门。  49.用户信息管理：支持组织机构人员信息管理；支持人员信息导入、导出；支持对本地用户账号进行密码重置；与学校数据平台的数据集成，实现组织机构、人员等相关信息的自动同步、更新。  50.角色管理：支持对角色的功能权限（系统菜单访问、管理权限）、数据权限（组织机构人员数据查看、管理权限）进行管理、对角色人员（将角色赋权于人员）进行配置。  51.用户群组管理：支持创建群组，支持在系统内需选择组织机构人员时快速选择使用（例如：支持在配置算法系统以及第三方应用权限时快速选择人员。）支持同步学校现有群组信息。  52.综合管理配置：  （1）支持配置采集端模糊、后台列表模糊、后台详情模糊管理  （2）支持账号登录超时、账号同时登录人数限制、账号登录踢人策略管理。  （3）支持短信平台配置、IP白名单管理、手机验证码登录、密码安全配置、钉钉参数配置及微信参数配置、IP黑名单管理、授权协议期限配置。  （4）支持数据脱敏配置，可实现对导出的手机号、身份证号等敏感信息数据脱敏。  ★53.账号黑名单管理：支持对账号连续登入错误次数进行设置，对账号进行禁止登录锁定时间设置，支持管理对账号进行加入及解除。  54.泄露提醒：支持实现当发生个人信息泄露时，导入人员名单，并编辑消息内容，提醒当事人。  55.日志记录：对第三方应用调用人脸库内置接口的日志信息（如应用名称、IP、调用接口名称、操作结果、操作时间等）进行记录；业务操作日志：支持对管理员用户业务操作日志信息（如系统模块、操作人员、操作类型、操作时间等）进行记录；对日志中的敏感信息进行前后端加密传输、加密存储，并对日志信息进行篡改检测，确保日志的完整性。  56.数据备份还原：支持可视化对系统的数据进行备份与还原。  ▲57.服务器管理：支持可视化对服务器或者人像系统进行重启。  58.主动推送数据第三方应用注册：支持主动推送数据给第三方应用。  ▲注册应用名称、应用介绍、数据源、数据类型、水印类型、权限范围（组织机构选择/用户群组选择）、人脸数据类型、权限控制（开启和停止主动推送数据）、是否签订保密协议（未签订/已签订）、传输加密类型，设置IP白名单，生成信息后AgentId、AgentSecret信息后，完成数据推送。  59.主动推送数据展示：支持人脸数据与人员组织机构推送结果展示。可展示待推送、已推送、推送失败、已删除的数据。支持差异下发、指定下发、单独重新推送等功能。  60.推送数据管理：支持对人像底片进行去标识命名，支持对人员敏感信息进行加密脱敏处理。对接算法厂家控制器，将人员数据、组织机构数据、底片数据、特征值数据主动推送第三方应用，实现对第三方应用的数据的增、删、改。实现第三方应用内人员信息的去标识化处理。  61.加密脱敏设置：支持加密策略设置，数据脱敏策略设置。数据脱敏策略可有如替换脱敏/随机化脱敏/假名化脱敏等方式。  62.第三方应用解密管理：应用注册：支持注册可获取脱敏前人员身份信息数据的应用，用于个人信息溯源查询使用。注册内容包括：应用名称、应用介绍、权限范围（组织机构选择/用户群组选择）、组织机构、防篡改、保密协议（未签订/已签订）、传输加密类型。  63.解密管理：可以通过解密接口，将获得加密的数据进行解密，获得真实数据。  64.应用解密溯源：支持记录解密应用调用获取脱敏前人员身份信息接口信息日志，记录内容有加密字符、用户信息、应用信息、事件描述、获取时间等。  65.人脸生物因子身份认证运行看板：支持对当前系统人员、已使用认证人数、认证总次数、接入应用场景、场景使用认证人数、场景使用认证人次、系统磁盘、CPU、内存使用资源统计、最新身份核验日志、认证人员类型占比、应用场景调用情况进行统计和展示。  66.支持认证辅助信息配置：可以用学/工号组合姓名、手机号、身份证号等字段进行联合认证。支持对最大同时认证人数限制，保证一段时间内的认证成功率，避免过多人员的认证，导致系统不稳定；支持设置人脸比对核验的QPS数量。  67.移动端身份认证：支持移动端进行随机左转头、右转头、点头、张嘴动作活体检测，通过活体检测后进行人脸识别认证。  68.PC端身份认证：支持手机端扫描PC端身份认证二维码，转到移动端进行随机左转头、右转头、点头、张嘴动作活体检测，通过活体检测后进行人脸识别认证。  69.前后端数据传输安全：支持前后端数据交互采用SM2双向身份验证、SM4传输数据加密、SM3完整性校验及时间戳的融合加密策略QPS数量。  ▲70.二维码刷新设置：支持PC端二维码定时刷新，支持不同第三方应用二维码刷新时间单独维护。  ▲71.人脸生物因子身份核验黑名单管理：支持查看身份核验超时锁定的用户信息，支持管理员对账号进行解除绑定管理。  72.登录日志：支持对系统的登录日志进行搜索、导出等操作，可查看用户的登录系统情况。  73.接口调用日志：对第三方应用调用人脸生物因子身份认证系统接口的应用名称、IP、调用接口名称、操作结果、操作时间日志信息进行记录。  ▲74.核验日志：支持记录用户使用系统进行人脸身份认证比对的所有记录，如记录包括身份认证成功、认证失败、认证中断、失败原因等。  75.支持与人脸识别算法分析管理平台对接，实现人脸数据的联动。可对人脸识别算法分析管理平台主动操作（增加、修改、删除）数据，包括组织机构、脱敏的姓名、加密后的学号和工号和人脸特征值，使平台内个人信息去标识化处理，保障平台内数据安全。 | 1套 |
| 12 | 人脸识别算法分析  管理平台 | 1.具有包含但不限于：数据看板、事件中心、人员管控、人数统计、智能分析、视频监控、门禁管理、资源管理、系统管理、运维管理等功能模块。  2.门禁设备管理：支持同时接入生物识别门禁设备和刷卡门禁设备。生物识别门禁设备包括但不限于人脸识别门禁机、人脸识别相机、人脸识别边缘盒、掌纹门禁机等。刷卡门禁设备包括但不限于门禁控制器、读卡器、发卡器等。支持将人脸、卡片、密码、二维码、掌纹等多模态认证因子作为门禁鉴权凭证。  3.不同角度的人脸识别比对要求：支持能对水平转动角度高达30°（即不超过±30°）、俯仰角角度高达35°（即不超过±35°），倾斜角角度高达35°（即不超过±35°）且无遮挡的人脸进行识别比对。  4.人脸抓拍性能试验：采用离线视频（由图片拼接而成）进行测试，1张合成图片、合成图片中具有160个人脸图片，合成图片停留时长为1秒。支持单张图片抓拍不少于150个人脸，人脸抓拍率>99%。（人脸抓拍摄像机实现该功能视为同等响应。）  5.以图搜人：支持上传人脸图片、设置相似度、选择分析源、开始时间和结束时间对基础人员、访客、关注人员、未知人员进行人脸1:N检索。1:N检索结果可展示高于相似度的人员档案，展示内容包括相似度、人员姓名、人员类型、采集次数。  6.人员轨迹功能：支持按人员信息检索基础人员、访客、关注人员，检索条件有姓名、身份证号、分析源、开始时间、结束时间。检索结果可展示实名人员档案，包含人员姓名、人员类型、采集次数；点击档案，可展示抓拍记录并查看人员通行轨迹。  7.人体检出尺寸：支持对视频流中分辨率低至30\*30像素的人脸进行抓拍。（人脸抓拍摄像机实现该功能视为同等响应。）  ▲8.支持设置人脸特征模型，可开启/关闭；支持设置人脸下发方式，包括图片下发、特征值下发；支持展示人脸特征模型适用的设备型号和固件版本号，可设置加密因子。  9.门禁报警功能：支持展示门禁报警记录，报警类型包括存储空间占用超过90%报警、存储空间占用超过90%20报警解除、防拆报警、防拆报警解除、密码破解报警、密码破解报警解除、门禁开放超时报警、门禁开放超时报警解除、门磁强开报警、门磁强开报警解除、门常开、取消门常开、门常闭、取消门常闭等。  10.最大可同时接入不低于256台人脸识别面板机。  11.接口具有包含但不限于：2个HDMI接口、2个RJ45千兆网口、1个VGA接口、1路音频输入接口，1路音频输出接口，1个RS485接口、1个RS232接口，2个USB 2.0接口，2个USB 3.0接口，16路报警输入接口，4路报警输出接口，8个SATA 3.0接口。  12.内存容量：不低于16GB；硬盘：支持接入不低于8块SATA硬盘，单块硬盘最大支持8TB。含一颗算力芯片。 | 1套 |
| 13 | 智慧通行  综合管理  平台 | 一、实时查寝及归寝异常预警功能  1.支持保存学生、宿舍管理人员和院系辅导员等人脸、院系、学号、宿舍号等信息，进行身份识别记录信息的收集和综合处理。  2.支持学生、教工、外来人员等基本信息管理功能。  3.支持对人脸信息进行添加、删除、修改、查询等管理。  4.支持提供信息批量导入功能，如身份信息批量导入、图片批量导入等。  5.支持显示公寓人脸识别总揽：支持展示内容，包括但不限于：学生总数、教职工总数、黑名单数量、今日陌生人数、今日通行总量、在寝数量、未归数量、晚归数量、多日无出入记录数量。  6.学生出入记录查询：可以按时间顺序查看，也可以按姓名、学院、专业、班级、楼号、宿舍号等查询。  7.支持对某个学生的详细信息查询，包括但不限于：抓拍时间、抓拍照片、出入方位、姓名、学院、专业、班级、楼号、宿舍号等信息，以及查看上条记录操作、查看下条记录操作、查看所有出入记录操作等。  8.支持归寝异常预警推送：通过手机端自动推送预警信息：系统支持对晚归、未归、多日无出入记录的学生，可以实时或定时通过手机微信端推送给对应的后台设定人员，如辅导员。  9.支持实时查寝及查看历史记录：系统支持通过手机端实时查看各公寓楼学生在寝情况，也支持通过手机端查看历史晚归、未归、多日无出入的学生清单；系统支持通过手机端按宿舍楼维度查看，也支持按院系维度查看等。  10.晚归记录查询  可查询学生晚归情况，内容包括出入时间、学生学号、姓名、性别、宿舍楼、通道及方向、通过状态、所属院系、所在班级、宿舍房间、个人照片等。  11.当前未归人员  可查询当前未归学生情况，内容包括宿舍楼、宿舍房间、学生学号、姓名、性别、状态、所属院系、所在班级、最后通行时间、最后通行位置、个人照片等。  12.未归汇总统计  可查询学生未归汇总统计情况，内容包括学生学号、姓名、性别、所属院系、所在班级、所在宿舍、在寝状态、未归天数、最后通行时间、个人照片等。  13.多天无记录人员  可查询多天无记录学生统计情况，内容包括学生学号、姓名、性别、所属院系、所在班级、所在宿舍、最后通行时间、无记录天数、个人照片等。  14.重点关注人员管理  可查询、编辑、删除重点关注人员信息，含编号、姓名、照片等；该生被人脸识别后，实时推送消息至后台设置人员手机端；可查询推送报警记录，含报警时间、地点、人员信息等。  15.陌生人记录查询  可查询陌生人出入记录，内容包括出入时间、宿舍楼、通道及方向、通过状态、通行方式、对比分析值、记录照片等。  ★16.归寝【晚报】推送：支持每日考勤晚报于晚上通过手机端定时推送《归寝晚报》，包含每日在寝室、校园、校外的人数。点击数字可查看该列学生清单，点击学生可查看其个人信息（含院系、住宿信息）、最近一次及近期通行记录（按时间展示刷脸通行时间、抓拍照片等）。  ★17.归寝【早报】推送：支持每日考勤早报通过手机端于早上定时推送《归寝早报》，包含每日在寝、在校、校外及早出寝、早出校、晚归寝、晚归校人数。点击对应数字，可查看该列学生清单；点击学生，可查看其个人信息（含院系、住宿信息）、最近一次通行记录及近期通行记录详情（含按时间先后展示的刷脸通行时间、抓拍照片等）。  ★18.手机端支持【实时查寝】功能：从主页点击实时查寝，可查看学生总数、不住宿人数及在寝、在校、校外三种在校状态，不同状态用不同颜色标注学生姓名。点击学生姓名，可查看其是否在寝、个人信息（含院系、住宿信息）、最近一次通行记录及近期通行记录（按时间展示刷脸通行时间、抓拍照片等）。  19.手机端【异常记录】功能：支持从主页点击异常记录，即可查看当日未归、2日未归、3日及以上未归、2日及以上未出寝、闭寝后早出晚归人数。点击对应数字，即可查看具体对应的学生信息。  二、实现辅导员与未归学生互动功能，完成对异常数据的闭环处理，如实现以下功能：  1.对于手机端推送的未归学生或辅导员通过手机端实时查寝时发现的未归学生，可在手机端一键操作，发起与该生的互动，核实该生的去向；  ▲2.学生手机端会实时收到辅导员的消息，支持该生在平台里上传自拍照片（同时系统自动获取该生的定位信息），并进行相关描述；  3.辅导员确认该生的状态以及位置信息后确保该生处于安全状态，然后提交去向核实的结果；  4.对于通过线上、线下均无法联系到的学生，辅导员可将其备注为“去向不明”标签；  5.系统也支持辅导员线下与学生核实去向后，手工填写去向情况。  三、校园大门通行查询与统计  1.系统支持通过手机移动端或电脑端多种维度的人员进出校园报表的查询与统计：  2.当日数据的手机端可视化展示：包括今日汇总人次、进校园人次、出校园人次、学生总人次、教职工总人次和其他人员总人次等统计（也支持电脑端）；  3.支持在手机上直接点击人次的数字可进入清单列表查看详情：支持按时间顺序排列展示明细（包括姓名、工号/学号、通行地点、通行方向、部门/院系信息、人脸识别时的抓拍照片等）（也支持电脑端）；  4.支持对历史通行人次数据的手机端可视化展示，包括：汇总人次、进校园人次、出校园人次、学生人次、教职工人次、其他人人次等，支持查看详情（也支持电脑端）。  5.系统支持对“学生”“教职工”“驻校服务企业人员”出入记录查询；  6.黑名单人员：可查询黑名单报警记录、内容包括报警时间、报警地点、黑名单人员信息、记录照片等。 | 1套 |
| 14 | 访客预约系统 | 一、访客自助预约功能  1.来访人员可通过学校的预约二维码或部署在学校微信公众号里的预约程序进行来访预约信息的填报。  2.预约信息支持填写姓名、身份证号码、手机号、车辆车牌号、选择拜访部门、填写被访人、来访日期、访客权限有效时长以及上传本人照片等。  3.访客信息提交后，系统支持向对应的被访人（或校方设定的审核人员）推送访客预约的审批消息。  4.访客预约审批后，照片信息下发至刷脸闸机，现场可刷脸开闸；车牌信息下发到车辆道闸系统，车辆到场可自动识别开闸。来访时限结束，刷脸权限或车辆信息自动失效。此外，还支持访客通过专门设置的访客通道，刷身份证或出示预约系统生成的二维码识别开闸。  二、校内人员邀约功能  1.校内人员可通过部署在手机端的程序代理访问人员提交相关预约信息。  2.预约信息支持填写姓名、身份证号码、手机号、车辆车牌号、选择拜访部门、填写被访人、来访日期、访客权限有效时长以及上传本人照片等。  3.访客信息提交后，系统支持向对应的被访人（或校方设定的审核人员）推送访客预约的审批消息，或支持自动审批功能。  4.访客预约审批后，访客的照片信息直接下发到刷脸闸机里，现场可刷脸开闸；车牌信息直接下发到车辆道闸系统，车辆到达现场可自动识别开闸通行；在来访的时限结束后，刷脸权限或车辆信息自动失效。  三、访客信息查询与管理  1.支持管理人员在手机端查看已审批、待审批、逾期未审批的分类的预约信息，并能在手机端直接审批。  2.支持管理人员在手机端查看各预约信息的详情。  3.支持管理人员在手机端查看访客的通行记录，并能查看通行刷脸时的抓拍照片。  4.支持按自定义时间段查看访客预约情况等统计数据。 | 1套 |
| 15 | 智能门禁可视化显示系统 | 一、楼宇级可视化展示内容：  1.本楼栋实时数据呈现：当前楼宇在寝人数、外出人数、总人数等；  2.本楼栋昨日归寝异常数据呈现：晚归人数、早出人数、1日未归、2日未归、多日未归、多日未出人数等；  3.本楼栋陌生人、黑名单人员抓拍预警：针对抓拍到的陌生人，在大屏上实时弹窗预警等相关信息；  4.本楼栋实时视频监控呈现：显示进入公寓的实时监控视频流。  5.本栋楼实时出入记录的列表：姓名、通行时间、当时的抓拍照片等。  二、校级可视化展示内容－－公寓场景  1.实时数据呈现：总床位数、空床位数、入住总人数、实时在寝人数等；  2.楼栋归寝预警信息呈现：涵盖楼栋号、入住人数、晚归人数、多日未归人数等。  3.学院归寝预警信息呈现：涵盖学院名称、总人数、晚归人数、多日未归人数等。  4.实时视频监控呈现：呈现进入公寓的实时监控视频流，可选择楼栋进行展示；  5.多日未归呈现：包含姓名、所在公寓楼栋、最后一次通行时间、未归天数；  6.实时通行记录呈现：包含姓名、所在公寓楼栋、通行时间、通行方向等；  三、支持人员进出校园大门数据的展示－－校大门场景  1.当日数据实时呈现：进校园数、出校园数据、进出汇总数等；  2.历史汇总数据呈现：进校园数、出校园数据、进出汇总数等  3.当日进出分类呈现：学生汇总、教职工汇总、其他人汇总等。  4.实时视频监控呈现：呈现各校门的实时监控视频流，可选择校门进行展示；  5.访客数据呈现：当日访客数、历史访客数；  四、屏显系统  1.支持手机、笔记本电脑等移动端通过自动搜索接收端设备和六位识别码两种方式无线连接到产品。  2.支持不少于6个投屏客户端图像画面对比展示，在产品上可以反向控制操作笔记本电脑上的内容，支持单击、双击、右键控制。  3.支持手机和大屏/电脑之间的文件互传，支持文件快传弹窗，用户可使用app扫码选择上传文件；也可选择电脑/大屏端文件进行下发，选择文件后刷新二维码弹窗，用户扫码带走文件，实现文件共享；支持查看下载的文件列表，可查看文件名称、类型、大小，也可打开、删除、取消下载的文件。  4.屏幕尺寸≥86英寸，分辨率≥3840×2160，采用OPS插拔式架构，内存：不低于16G；硬盘：不低于512G-SSD固态硬盘；配备可移动支架。  五、其他：可根据业务实际需求对大屏界面进行调整的。 | 1套 |
| 16 | 相关辅材 | 本项目设备安装所需的所有线材、辅材：（1）网线规格：不低于六类线；（2）电源线规格：纯铜，不低于RVV2\*1.0；（3）PVC线管规格：阻燃，壁厚不小于1.2mm，具体长度以现场施工需求为准；（4）27、28、29、30宿舍、图书馆新建通道闸机所需配套护栏及其他宿舍楼通道需加装护栏处所需护栏，护栏材质为不锈钢，宿舍楼护栏需带电磁吸力锁，宿管室有一键开关，满足现场闸机安装需求，达到验收状态；（5）各闸机处的配套刷脸指示提醒标贴、各处闸机配备遥控器、一键开门按钮，以及完成本项目所需要的其他辅材等。 | 1批 |
| 17 | 安装、调  试及系统  对接 | 1. 安装调试：   （1）原有闸机等设备拆除并运送至校方指定地点（校内）需中标厂商承担。  （2）完成本项目包含的所有设备安装、软件部署、相关辅材的供应以及软硬件调试等工作。  2.系统对接：  （1）与请销假系统对接：在推送未归等异常数据时，自动过滤掉已请假的学生；与现有车辆道闸系统对接：把访客预约系统里报备的车牌号信息，自动下发到现有车辆道闸系统里，进门时车辆闸杆自动识别并抬杆放行。与座位预约系统对接：将学生刷脸进馆数据推送给座位预约系统，用于无感签到；与现有图书借阅系统对接，实现刷脸还书功能；与现有一卡通系统进行对接；支持与校友系统对接。  （2）与现有人脸识别设备通过SDK接口形式（经与校方共同评估无法通过SDK接口形式对接的可通过软件对接）对接：把学校现有刷脸闸机的通行数据对接到本次建设的实时查寝及归寝异常预警系统里，做统一的归寝异常分析使用；同时也支持对现有人脸识别闸机进行管理，如对人脸权限的取消与增加等管控。在该项目的服务维护期内也支持其他品牌人脸识别面板机接入，开放接口。（现有品牌：商汤品牌、熵基品牌）。  （3）支持学校后建业务系统数据对接。  3.数据集成：  （1）对接学校数据中台，实时获取：学生院系基础数据、学生住宿基础数据、辅导员对应班级数据等；支持对接一卡通数据，通过刷一卡通实现人脸闸机通行。  （2）对接学校统一身份认证平台，完成认证集成，达成单点登录；与学校信息门户对接，实现页面集成；项目涉及系统移动端需支持集成至微信服务号、钉钉等平台的。  4.人脸识别数据安全保护系统还涉及的其他对接事项：  （1）移动门户对接：实现与移动门户的配置集成。（2）组织机构同步：实现系统组织机构及人员基础数据与学校数据源同步。（3）消息中心对接：实现对接学校现有的短信平台或消息中心，调用短信平台发送短信。（4）协助业务系统对接：协助学校使用人像数据与业务系统进行对接。  5.所有对接费用由中标单位承担。 | 1项 |
| 18 | 网络安全  等级保护测评 | 平台正式上线使用前，须完成网络安全等级保护（第二级）测评工作，并提供测评报告。 | 1项 |

**注：1.技术参数中标“★”项为重要指标项，参数响应要求：需提供功能截图或产品彩页或带有CMA标识的检测报告扫描件等相应的佐证材料，佐证材料的优先级为：检测报告〉真实系统的功能截图〉产品厂商的官网截图。**

**2.技术参数中标“▲”为加分项，不影响投标产品响应情况。**

**第三部分项目执行及要求**

**一、报价要求**

1.本项目报总价，包含产品、运输等完成所投任务的一切费用，采购人后期不追加费用，投标人勘查现场后充分考虑风险，中标后不得要求增费或拒服务。

2.与现有系统对接，投标人须无条件完成对接，不得要求采购人增加费用。

**二、供货安装及质保**

1.供货周期：合同签订后90个日历天完成供货、安装调试。

2.质保期限：2030年12月31日止。

1）质保期内:项目涉及软件须提供免费升级服务（含跨版本升级）。

2）质保期外：软件授权不影响使用。

**三、售后服务**

1.服务响应：质保期内提供7\*24小时技术服务热线，解答设备使用问题。

2.远程服务：7\*24小时支持，1小时内响应；现场支持：远程无法解决，2小时内到达，一般性故障24小时解决，复杂问题48小时解决，不能修复则提供同类型产品确保系统运行。

3.定期巡检及技术支持：合同货物投运后，中标人成立不少于2人的团队，根据采购人情况定期巡检、面访、回访，总结系统使用情况，提供培训等技术支持。

4.培训：中标人提供现场系统运维培训，讲解技术原理与注意事项，设计个性化巡检、运维内容，提供完整方案，直至采购人掌握操作，定期培训并解决问题、提供支持。

**四、其他要求**

1.项目采用本地化部署，学校分配虚拟机，中标供应商按要求部署。平台上线前，对软件系统进行等保二级测评，根据结果整改并提供合格报告。

2.项目实施过程中，涉及墙面、地面的施工需遵循“谁施工、谁恢复”原则，施工方需完成墙面、地面的修复工作；涉及地面瓷砖需更换新瓷砖，确保修复效果与周边环境保持一致，达到甲方要求。