

采购需求

一、移动办公办案服务采购项目概述

1. 项目建设目标

移动办公移动办案服务为打破政务工作受地域空间的限制，法官干警可通过使用安装在移动终端上的移动办公办案 APP 软件随时随地获知院内资讯、业务提醒、办案审限预警、院内通讯录、案件办理等信息。能够及时、便捷地完成移动审批、移动信息查询等工作。

结合法院专网内外数据的安全合规交换场景，解决移动专网和法院专网之间的数据安全交互，以安全、可信、合规为目标，实现接入应用系统和设备的身份可信，保护数据安全共享，抵御网络恶意攻击，满足机密性、完整性和可用性要求，确保跨网数据共享和业务协同的网络安全、主机安全、应用安全和数据安全。

1.1 移动办公办案

省高院干警以及采购了该项服务的中基层法院干警在国内可使用配发的智能办公办案终端，使用移动专网在线办理政务系统上大部分业务，以及一部分审判执行业务，为了保障顺利办公办案，本次采购的通信套餐至少包含 80G 流量，500 分钟通话。智能终端用满 3 年可更换，采用满足安全要求的国产双系统智能终端。

1.2 居家办公通信

满足干警居家办公的需要，保障干警居家和在外出差时能够通过移动办公办案系统处理各种事务，在线办理审判执行业务。

1.3 建成移动专网

采用购买服务的方式建设全省法院移动专网，建设费用包含在本次总费用中，实现陕西法院专网向移动无线端延伸，并通过可靠的安全措施保障专网安全。

1.4 实现专网短号码功能

省高院干警以及采购了服务的中基层法院干警，可使用本次配发的流量卡号码免费互打，并开通短号码功能，呼叫对方只需要呼叫相应的 5 位或 6 位短号码，方便法院干警快捷的进行日常通信及内部沟通。

2. 移动办公办案系统须遵循的文件规定和相关规范

法〔2022〕136 号《人民法院信息化建设五年发展规划（2021-2025）》

法办发〔2017〕10号《全国法院办公专网跨网信息交换安全保密管理规定》

法办发〔2015〕11号《最高人民法院办公专网移动办公安全保密管理办法》

法办发〔2015〕21号《最高人民法院手机使用保密管理规定》

FYB_T_53001-2017 安全隔离与信息交换平台建设要求

FYB_T_54008.1-2020-法院专网技术规范

FYB_T_54009-2020-法院统一 DNS 系统建设技术规范

FYB_T_53006-2020-法院专网网络准入和主机防护技术规范

FYB_T_53005-2020-法院专网安全域划分和边界防护技术规范

3. 建设原则

3.1 标准化原则

结合专网/内网业务系统实际需求，应用大数据、人工智能、移动互联等先进技术，采用成熟的产品，充分考虑“标准和开放”的原则，支持各种相应的软硬件接口，使之具有灵活性和延展性，具备与多种系统互连互通的特性，在结构上实现真正开放，便于与其它系统的互联和扩展，平台具有可移植性、互操作性、系统独立性和集成性。

3.2 自主可控原则

移动办公平台基于国密密码算法，利用现有资源，实现可信身份管理、网络传输安全、数据使用与存储安全等方面进行综合防护。

3.3 安全保密原则

在数据库设计、应用操作权限和身份认证方面均严格遵守国家有关安全、保密标准，全面加强安全措施，所有应用项目采用符合国家标准的基础软硬件。

3.4 可靠性原则

系统能够有效的传输数据，确保数据的有效性和完整性。

3.5 经济适用原则

以需求为基础，充分考虑发展的需求来确定系统规模，功能模块子系统以插件方式扩展。系统突出实用，和当前法院的实际需求及后期规划相结合。

3.6 可管理性原则

系统设备易于管理、维护，操作简单，便于配置，在安全性、数据流量、性能等方面能够得到很好的监控和控制，易于进行管理和故障诊断。

3.7 先进性原则

系统的结构设计、配置、管理方式，应采用成熟的先进技术，延长系统的生命周期。

3.8 开放兼容原则

系统要求开放性好、标准化程度高，系统建设应与现有的内网系统平台兼容。系统建设符合国家有关标准。

3.9 技术成熟性原则

在系统软硬件方面，充分考虑采用国内通用的，成熟的软硬件产品进行开发，保证系统功能的高稳定性。

二、移动办公办案服务采购的主要内容

根据最高人民法院加强系统整合、坚持统建优先的原则，结合我省高院信息化建设和应用的实际，陕西法院采购的移动办公办案系统服务应包含以下内容：

1. 移动专网安全接入服务

采购移动专网安全接入服务，供应商提供从移动终端到移动办公办案系统的4G/5G+VPN安全接入服务，采用VPN技术保障智能终端的安全接入和双因子认证，实现与法院移动办公平台的安全对接。

2. APP应用和移动办公办案平台支撑服务

供应商应提供成熟易用的APP，结合现有政务系统在用功能，实现在智能终端上通过APP对专网新闻、通知公告、公文管理、后勤管理、会议管理、请假管理、接待管理、会议管理、行政装备、邮件管理、考勤查询、签到签退等功能进行实时操作。

供应商应提供支撑APP所需的后台服务，后台所需基础硬件、应用软件、安全硬件和软件应部署于移动专网内，实现法院专网和移动专网数据实时、安全同步。

3. 移动应用安全管理服务

供应商应提供移动应用安全管理服务，能严格控制智能终端上的移动应用下载安装行为，保障办公应用与生活应用的数据隔离，并实现针对移动应用的数据级防泄漏能力，在办公办案APP退出后，清除工作域缓存，系统不残留敏感数据，

确保移动办公办案应用和法院工作数据安全。

4. 安全智能终端和安全管控服务

供应商需提供干警移动办公办案所需的安全智能终端，安全智能终端应具备双域安全能力，国内一线品牌，国产操作系统。

供应商需提供针对移动办公终端的安全管控平台，实现对移动办公办案智能终端的安全管控，能够防止非法用户获取超级权限，在智能终端不慎丢失时能远程擦除终端设备上的敏感工作数据，取消流量卡对移动专网的接入权限，以及能远程采取其它的必要措施，确保移动专网不被非法用户入侵，安全终端上的敏感数据不失控。

5. 移动互联网安全访问服务

供应商提供的 4G/5G 接入套餐，要保障配套的智能终端在不接入法院移动专网时，要能够安全访问移动互联网，满足法院干警在智能终端上检索信息、查阅司法资料、参加学习强国、陕西干部网络学院的学习培训等需求。

6. 虚拟专网服务

供应商应提供虚拟专网服务，组建全省法院流量卡号码虚拟专网，网内用户互打免费。开通短号码功能，方便法院干警快捷的进行日常通信及内部沟通。

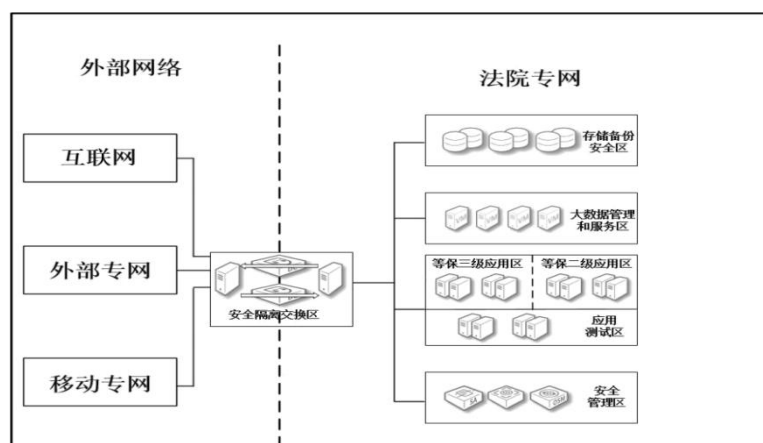
三、移动办公办案服务技术要求

1. 移动专网安全接入服务技术要求

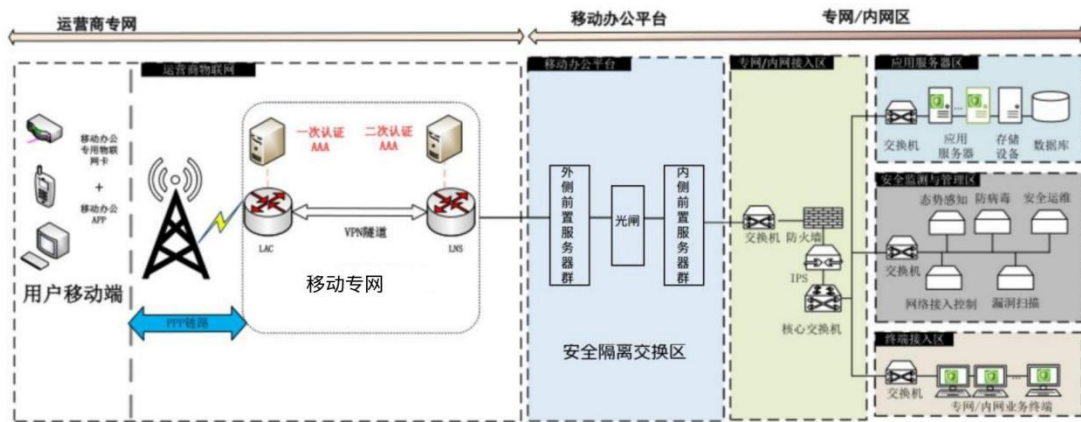
移动专网作为人民法院“五网三云”的重要组成部分，和法院专网通过安全隔离交换平台相连接，和法院专网进行数据交互，必须满足最高人民法院相关通知要求和技术规范。

1.1 安全隔离交换

最高人民法院对移动专网和法院专网间的隔离连接和数据交换有明确要求，其基本连接结构如下图：



本次移动专网由移动终端、无线链路、物联网平台（VPN 平台）、安全隔离交换区组成，和法院专网进行数据交换，通过 VPN 链路向移动终端提供服务。



单个智能终端通过 VPN/VPDN 的方式访问外侧前置服务器，达到访问内网办公系统完全相同的效果，实现安全的移动办公办案。该模式通过 VPN/VPDN 虚拟隧道提供内网访问能力，供应商要能够提供独立、高速、安全的数据通道、电信级的安全保障。通过外网前置服务器、外网光闸和内网光闸、内网前置服务器之间的数据交换及安全防护，形成安全可控控制网络区域。确保办公办案数据不泄露。该模式可以通过移动终端安全+VPDN 安全+安全接入控制区等方式形成一个多层次的安全防护。

1.2 数据传输加密

在智能终端上，办公办案等敏感数据支持存储加密，并对客户端数据库进行整体加密，确保数据不泄露。可以由管理员设置终端数据不落地，文件只能在线预览。也可以个人在发文件的时候自行选择，或限制传输的文件仅可在同一类型客户端中下载。

1.3 安全接入服务

提供移动安全接入服务，实现全省移动办公终端安全接入，并与移动办公办案服务器连接。提供基于 4G/5G +VPN 的虚拟专网安全接入通道；安全接入需具备安全认证，认证成功才可接入安全区。

1.4 流量和通话服务

为每个接入的智能终端提供每月 80G 流量、500 分钟通话时长。

2. 智能终端要求

2.1 国产化要求

本次移动办公办案服务提供的终端须为国产一流品牌智能终端，采用国产智能终端操作系统，满足开机界面定制等要求。

2.2 数据安全隔离要求

智能终端应该具备双操作系统，连接互联网的系统和移动专网的系统应相互独立，并按照办公专网等级保护要求进行隔离。数据存储区应相互独立，两个系统内的 APP 软件只能在本系统内读写数据，不能对另一个系统的存储进行读写。实现双域服务，进入工作域时网络会自动切换到虚拟专用拨号网的接入点并建立好虚拟专用拨号网连接。退出工作域时网络会自动切换回 4G/5G 移动数据的接入点并还原为 4G/5G 的互联网数据网络。

2.3 部分技术参数要求

终端实行 1 年保修。

国产主流终端：5G 芯片，八核 CPU，主频 $\geq 2.8\text{GHz}$ ，支持 NM 存储卡。

网络制式：双卡双待全网通，支持联通/电信/移动 5G/4G/2G。

屏幕尺寸： ≥ 6.5 英寸；

运行内存（RAM）： $\geq 8\text{GB}$ ；

机身内存（ROM）： $\geq 256\text{GB}$ ；

分辨率： $\geq 2700 \times 1224$ 像素；

后置摄像头：摄像头 1 ≥ 5000 万像素，5 倍光学变焦。摄像头 2 ≥ 1300 万像素；

前置摄像头： ≥ 1300 万像素；

电池容量： $\geq 4100\text{mAh}$ ；

支持 IP68 及以上防水；

支持北斗定位功能，支持蓝牙、WIFI、指纹、红外传感器、陀螺仪，内置 NFC 模块；

双系统：终端两个操作系统运行在不同 ROM 空间，两个系统独立运行，完全隔离。两个系统的蓝牙、WIFI、NFC 等外设独立配置；任何一个系统不能删除、创建或控制另外一个系统；一个系统恢复出厂设置不影响另外一个系统；支持公共 APN 和专属 APN 同时接入、同时在线；当前系统能接收到另外一个系统的通知栏消息，但看不到数据；

支持基于芯片集成安全模块的警务通加解密服务，并实现证书远程管理功能；
工作区蓝牙与 wifi 热点由 MDM 远程控制，不能随意开启，可通过蓝牙设备类型或 Mac 地址白名单机制限制蓝牙仅可连接指定设备；

系统需防 Root，须定制双系统 ROM 包，禁止刷成普通消费者版本；

支持系统级全局水印功能，防止偷拍屏幕造成信息泄露，同时支持防截屏、防录屏；

系统预置运营商定制 APN 接入点，只能通过 VPDN 接入专网做数据业务；

支持通过互联网系统进行在线 OTA 升级服务；

所投产品具备电信设备进网许可证、无线电发射设备型号核准证、中国国家强制性产品（3C）认证证书、SGS 绿色环保认证

所投产品制造商具有质量管理体系认证（ISO 90001）、环境管理体系认证（ISO 14001）、职业健康安全管理体系认证（ISO 45001）、业务连续性管理体系认证证书（ISO 22301）、知识产权管理体系认证证书；

支持对终端在不拆机的情况下，擦除终端敏感数据，将定制系统版本回退成普通消费者版本，并提供具有的由权威检测机构出具的敏感数据擦除安全性检测报告；

投标产品生产厂家具备售后服务能力，具有国家标准《商品售后服务评价体系》五星级认证证书；提供证书复印件加盖投标人公章，若投标人为代理商须加盖原生产厂商和代理商公章；

提供的终端自合同签订之日起质保 1 年。

3. 移动终端安全管控服务

该系统需具备自主知识产权，且满足一定的安全保密认证。以此实现对所有办案终端及移动应用的安全管理，防范办案终端及移动应用安全风险，移动终端管理系统的功能需求说明如下：

3.1 资产管理

在系统首页可显示系统信息概况，展现用户总数、设备总数等基本信息，具备资产统计、分类、状态显示等功能。

3.2 组织机构管理

组织机构管理：根据客户实际情况创建、编辑组织结构，从而使人员、智能

终端在等可以按照组织结构进行管理。

3.3 用户管理

可以对用户信息进行增删改查，移动用户到另外组织结构等操作，支持批量按模板添加用户。用户信息包括姓名、流量卡号码、归属组织、邮箱等信息。

3.4 设备激活

为用户生成设备激活码，该激活码用于移动设备激活。该激活码通过短信的方式下发到用户的移动设备上，用户通过在客户端中输入收到的激活码来完成移动设备的激活。

3.5 设备管理

管理员可以通过设备管理简洁清晰地了解移动设备的硬件信息，硬件信息包括手机型号、软件版本号、运行内存、存储内存、设备串号等信息。同时可以通过用户的手机号码、姓名等进行设备的检索查询。

3.6 设备控制

可以通过远程控制命令的方式对移动设备进行远程锁屏/解锁，远程擦除等操作。

3.7 应用发布管理

平台提供专用办公应用商店，可以通过平台对客户的办公应用进行添加、更新、下架应用等操作。

3.8 应用分类

平台支持对发布的应用进行分类管理，客户可以按照应用名称、分类筛选应用。

3.9 外设策略

平台通过设置外设策略可以对通用的手机外设，例如摄像头、蓝牙、WIFI、VPN、移动热点、位置等进行启用或者禁用的限制。

3.10 日志管理

记录管理员操作内容、终端 IP、时间。支持按时间筛选查询。记录设备安装应用历史。

3.11 系统设置

系统设置中包含管理员角色管理、管理员管理等创建、修改、删除等操作，

从而实现管理员的权限分配和可管范围。

4. 虚拟专网服务要求

对接入本次移动专网的移动电话号码组建虚拟专网。网内用户互打免费。每个号码赋予一个 5 位或 6 位短号码，方便干警之间联系沟通。短号码前冠字号应按地市划分，同一个地市用相同的前冠字号，不同地市用不同的前冠字号。

5. APP 应用服务要求

客户端包括新闻中心、通知公告、工作台、我的邮箱、个人中心，法官干警可通过 APP 随时随地获知院内资讯、业务提醒、案件信息、电子卷宗、庭审排期、案件审限、院内通讯录等信息，搭建工作台方便法官干警及时处理办公办案事项，法官干警可在工作台进行公文管理、后勤管理、请假管理、会议管理、接待管理、用车管理、超审限提醒、办案信息、办案审批等工作，可及时、便捷地完成各类办公办案审批事项的移动审批等工作，满足法院干警随时随地远程跨网系办理各类办公办案需求。

5.1 总体业务流程

移动办公通过与内网门户系统、办公系统和办案系统、执行系统进行对接，可获取内网门户系统的新闻资讯通知公告信息，以及办公系统、办案系统的相关业务数据，并将移动端数据与内网系统进行同步，方便进行跨网远程处理办公办案事项。

移动办公总体业务流程：干警通过账号登录移动办公办案系统，可查询、浏览内网系统的新闻资讯、通知公告等信息，可进行收发邮件管理，同时支持考勤管理，干警可进行考勤签到签退，查看个人待办事项、已办事项、历史通知信息等。工作台提供办公办案业务办理，干警可在此处理公文、接待、用车、会议、后勤、行政装备、请假等业务的申请及审批。干警可查看办案信息、超审限信息，办理办案过程中的审批业务。

5.2 数据流程

移动端至内网：移动端发起请求，调用外网服务器应用程序接口，应用程序根据请求类型进行处理。

查询请求：查询外网数据库，直接返回结果。

数据提交请求：封装数据，将数据包通过 FGAP 发送至内网服务器指定位置，

内网监听程序解析数据包，调用内网接口进行处理，将处理结果返回至外网，外网处理程序接收结果对待办数据进行更新。

外网程序提供监听磁盘数据包功能。

内网至移动端：

内网数据发生变更，将数据打包调用内网监听程序发送至外网指定位置，外网监听程序解析数据包进行数据更新。内网推送数据包需要保存推送记录。

5.3 数据安全

从智能终端到数据处理服务器全程加密传输和存储，使用国密算法，满足《数据安全法》相关规定。

5.4 功能要求

5.4.1 下载安装与更新

移动办公下载，进入内网门户扫码下载，自动安装。

系统更新采用热更新模式，用户只需打开应用，系统检测到有版本更新会自动更新；同时也提供用户手动更新的方式。

5.4.2 登录与验证

系统提供用户登录与验证功能。系统通过法院内网门户系统的用户信息为法院司法工作人员提供账户信息，设置用户名和密码，法院司法工作人员可通过用户名和密码进入移动办公办案首页，系统支持指纹登录，用户可通过录入指纹信息使用指纹验证登录。

系统支持与法院内网门户系统对接，可获取法院内网门户系统的用户信息，并支持与法院内网门户系统同步用户信息，移动办公办案平台不单独存储用户信息。

用户输入用户名密码认证环节，系统首先会对终端进行授权认证，认证通过后再对用户信息进行身份认证，通过后可进入移动办公。

5.4.3 新闻中心

系统提供新闻中心功能，通过与法院内网信息门户对接，可接收和查阅法院内网门户网站新闻中心栏目下的新闻内容，可实时同步到移动端进行展示。

新闻中心支持对新闻进行分类，可对法院内网门户网站新闻中心栏目下的新闻内容进行分类布局，方便用户查阅相关类别的新闻信息。

系统提供滚动新闻功能。支持将每日的热点新闻以滚动新闻的形式展示在新闻中心页首，方便用户快速了解今日热点信息。

系统提供新闻查看和新闻查询功能，用户在新闻中心可查看法院内网门户网站新闻中心栏目下的新闻内容；可使用全文检索检索新闻条目查询新闻。

新闻详情页提供新闻收藏功能。

5.4.4 通知公告

系统公告消息功能，通过与法院内网政务系统、信息门户系统对接，获取内网政务系统、信息门户系统的公告、通知、消息内容，可供法院司法工作人员在移动端查阅内网政务系统、信息门户系统的公告、通知、消息内容。

公告消息管理具体功能点包括已读消息、未读消息和消息查询功能。

5.4.5 个人工作台功能

●系统更新通知

在工作台可查看系统的通知信息，例如系统更新的内容、系统维护升级等信息。

●公文管理

主要的功能包括内部发文管理、外部发文管理、收文管理、收文传阅管理。系统能够按预先定义的流程实现自动传递，运转全过程的流程自动跟踪和监控，并通过日志来记录每个环节的具体办理过程。用户可查看的公文信息包括公文标题、内容、正文、审批意见、历史处理轨迹等。

●干部管理

主要的功能包括离退休干部管理、婚丧嫁娶报备/登记、派遣人员入职审批、派遣人员离职审批。系统能够按预先定义的流程实现自动传递，运转全过程的流程自动跟踪和监控，并通过日志来记录每个环节的具体办理过程。

●考勤管理

系统提供考勤管理功能，可实现加班、公出、请假、考勤说明各流程的申请、审批以及历史记录查阅，主要功能包括加班申请管理、公出申请管理、请假申请管理、考勤说明、部门负责人外出报备。

●资产管理

系统提供资产管理功能，可实现资产申领、资产维修和资产处置的线上申请

审批，以及历史记录查阅。具体功能包括设备领用管理、设备报废管理、设备维修管理。

●后勤管理

系统提供后勤管理功能，包括物品领用管理，可实现各流程的申请、审批以及历史记录查阅。系统提供物品领用管理，用户可进行领用物品的申请，实现物品领用申请单的审核。

●会议管理

系统提供会议管理功能，实现会议发起、会议议题、会议议程、党组决议等的申请审批全流程化管理。主要功能包括：党组会议议题申报、办公会议议题申报、议程审批、党组决议事项督办等。

●接待管理

系统提供接待管理功能，可实现对外接待的全流程管理，具体功能包括接待申请管理、接待审批管理、接待记录查看。

●门禁人员管理

系统提供法院门禁人员的在线申请功能，由各部门发起，填写部门名称、姓名、身份证号码、手机号码、开始日期、结束日期，经过逐级审批后，通知各业务庭室进行手续办理。

●我的邮箱

系统提供我的邮箱功能，我的邮箱功能与法院内网政务办公系统的邮件系统进行对接，同步我的邮箱数据。支持向法院内网政务办公系统的邮件接口推送数据，实现在移动办公系统内进行接收、发送、回复内网邮件，方便院内人员及时的处理邮件。保证内外网数据的统一性。

●个人中心

系统提供个人中心功能，可实现历史通知查看、我的待办、我的已办、我的收藏、签到、签退、考勤查询、我的名片、系统设置功能。

6. 移动办公办案平台支撑服务要求

6.1 自主可控

移动办公平台基于国密密码算法，实现可信身份管理、网络传输安全、数据使用与存储安全等方面进行综合防护。

●应用安全

6.1.1 身份鉴别

系统用户的身份标识应具有唯一性；

应对登录的用户进行身份标识和鉴别；

系统用户的身份鉴别信息具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；

同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

具有登录失败处理功能，如：结束会话、限制非法登录次数，当登录连接超时，自动退出；

系统及时清除存储空间中动态使用的鉴别信息。

6.1.2 访问控制

依据安全策略控制用户对客体的访问；

自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表级；

由授权主体设置用户对系统功能操作和对数据访问的权限；

应用系统特权用户的权限分离，例如将管理与审计的权限分配给不同的应用系统用户；

权限分离应采用最小授权原则，分别授予不同用户各自为完成自己承担任务所需的最小权限，并在它们之间形成相互制约的关系；

严格限制默认用户的访问权限；

用户在访问移动端时，采用拍照、截屏等方式，在每个页面上会留下用户的唯一性信息，后续可进行溯源。

6.1.3 资源控制

同一用户只允许在移动端一端登录，发现其他设备登录时，其他终端强制下线；

应用系统设置最大并发会话连接数；

用户终端访问系统严格记录 IP、设备编号等信息。

6.1.4 代码安全

应用程序代码编写安全规范，要求开发人员参照规范编写代码；

应用程序代码进行代码复审，识别可能存在的恶意代码；

应用程序代码进行安全脆弱性分析；

应用程序代码进行穿透性测试；

程序加固，对抗反编译逆向工具，防止 APP 被破解剽窃；

6.1.5 通信安全

当移动应用进入后台时，系统自动断开登录，下次进入需要重新登录；

在通信过程中，应对整个报文或会话过程进行采用 RSA 算法加密；

在通信过程中，存在文件传输的，文件落地后进行加密存储，查看文件时进行解密。

6.1.6 安全审计

安全审计会覆盖到每一个用户；

用户每一次操作信息都会进行日志记录，包含时间、类型、功能、设备编号、时间结果等；

后台服务会有审计结果查询。

6.2 数据安全

6.2.1 数据完整性

应用系统在数据传输过程中，对数据进行加密传输，解密时校验数据完整性。

6.2.2 数据保密性

数据传输过程所有参数及报文采用 Base64 加密方式进行加密。

6.3 数据传输

6.3.1 结构化数据：内网数据一经变更，内网数据监听系统会将变动的数据通过数据解析程序进行业务整理，形成数据包，然后进行 RSA 文件加密，传输至内网光闸指定文件目录；外网前置机即接收到加密文件，数据解析程序进行解密获取到数据，对数据进行存储，将加密数据包删除。

6.3.2 非结构化数据：非结构化数据通过指定的文件传输通道进行传输，传输成功后外网文件监听系统对文件进行加密存储，移动端的数据展示需要对文件进行解密；对于有时效性的文件，系统会在文件过期后进行物理删除处理。