版本号：v1.0

**移动终端安全管控**

**建设方案**

**北京惠讯时代企业科技有限公司**

**2018年8月**

# 目 录

[目 录 1](#_Toc527101996)

[1 需求分析 3](#_Toc527101997)

[1.1 设备管理需求 3](#_Toc527101998)

[1.1.1 设备绑定 3](#_Toc527101999)

[1.1.2 电子围栏 3](#_Toc527102000)

[1.1.3 丢失擦除 3](#_Toc527102001)

[1.2 应用管控需求 4](#_Toc527102002)

[1.2.1 应用限制访问 4](#_Toc527102003)

[1.2.2 私有应用商店 4](#_Toc527102004)

[1.2.3 关键字过滤 4](#_Toc527102005)

[1.2.4 陌生社交 4](#_Toc527102006)

[1.3 安全合规需求 5](#_Toc527102007)

[1.3.1 警示拍照定位 5](#_Toc527102008)

[1.3.2 数据加密 5](#_Toc527102009)

[1.3.3 网络加密 5](#_Toc527102010)

[2 方案设计 6](#_Toc527102011)

[2.1 总体架构 6](#_Toc527102012)

[2.2 功能架构 6](#_Toc527102013)

[2.2.1 功能设计 6](#_Toc527102014)

[2.3 部署方案 6](#_Toc527102015)

[2.4 管理方案 7](#_Toc527102016)

[3 方案优势 8](#_Toc527102017)

[4 软硬件清单 9](#_Toc527102018)

[4.1 软件清单 9](#_Toc527102019)

[4.2 硬件清单 9](#_Toc527102020)

[4.2.1 移动安全管理服务器 9](#_Toc527102021)

[4.2.2 安全生产力工具服务器 10](#_Toc527102022)

[4.2.3 移动终端 10](#_Toc527102023)

[4.3 网络配置清单 11](#_Toc527102024)

[5 建设工期 12](#_Toc527102025)

# 需求分析

## 设备管理需求

部队规模庞大，每个用户手中手机型号不一，这加大了部队对用户手机的管控难度，并且有些士兵带多部手机，逃脱部队管控措施。同时，在用户使用手机的过程中，难免出现违规操作移动设备的情况，或者遭遇设备丢失，可能导致设备中的文档、数据外泄。另外，在极端条件下，可能需要完全禁止用户手机的拍照、定位等功能，这时候就需要对设备进行严格管控。

### 设备绑定

海军总部下辖二级单位职工和用户多达数万人，为了做到总部对各分支机构以及各分支机构对下属用户的手机的有效管理，确保用户正确、合规的使用移动设备，需要对用户进行人、机、卡的自动绑定。管理员通过后台管理系统，分层、分级管控辖内的移动设备。用户需要更换手机或者电话号码时，需要向管理员申请变更关联数据，防止一人多机现象出现。

### 电子围栏

在特定的时间、地理范围内，根据部队管理需要和实际情况，可以限制移动终端的某些功能，例如禁止访问摄像头、禁用移动网络与Wi-Fi、禁止发送邮件等等。这就要求后台需要支持在特定环境下（例如指定地理位置范围内或者时间范围内）对手机进行高强度重管控。

### 丢失擦除

如果用户不慎遗失了手机，考虑到设备内部可能存储有用户的个人隐私数据以及部队的敏感数据，需要通过后台管理系统定位设备，并绘制设备运动轨迹，同时后台要支持远程擦除设备全部数据的功能，防止在无法找回的情况下导致的数据泄露。

## 应用管控需求

当前，手机软件市场缺乏有效监管，手机业务又逐步增多，大量恶意软件得以轻松混入软件市场。一旦下载、安装带有木马、后门的软件，个人信息、地理位置、隐私等将受到严重威胁。部分智能手机被用作非法信息传播平台，还有的智能手机采用非法加密压缩手段逃避监管部门的审查，并借助一些“翻墙”、“穿墙”软件访问境外非法内容。互联网的便利性与虚拟性也成为各种不和谐行为滋生的温床，孕育着网络恶搞、诽谤中伤、侵犯隐私、色情泛滥等问题。如果军人沉迷于智能手机无法自拔，使用智能手机严重占用休息时间，甚至影响到战友的休息，训练时出现心不在焉或者精力不足的情况。

### 应用限制访问

由于部队有部队特殊的纪律性要求，这就使得用户在使用智能设备进行休闲娱乐的时候，不能过度沉迷其中，在熄灯后、训练时、会议中等时间段应限制终端娱乐应用的启动。

### 私有应用商店

为了防止用户下载到恶意程序，进而威胁到设备中数据安全，应建立完善的私有应用商店机制，彻底隔绝恶意程序和病毒木马的威胁。

### 关键字过滤

用户频繁上网行为（如浏览不健康网站），对用户的身心健康、人生观、价值观等会产生不利影响。用户在浏览互联网内容时，极易接触到不良内容，或者在与家人、朋友进行网络聊天时，可能会泄露涉军信息。需要建立一套关键词屏蔽机制，对移动设备中的微信、QQ、浏览器等应用中出现的涉军敏感词、不良敏感词进行过滤，同时建立相应的审核机制。

### 陌生社交

在某些互联网应用中，会嵌入诸如“附近的人”、“摇一摇”、“漂流瓶”等社交功能，用户在使用这些功能时可能会泄露敏感位置信息，同时用户可能通过添加陌生好友，被不法分子盗取个人信息。我们需要在终端屏蔽这些功能项。

## 安全合规需求

1999年第二次车臣战争中，因俄军内务部队一名旅长使用手机指挥战斗时发生泄密，致使敌军掌握了行军路线并预先设伏重创俄军。韩国国防部公布的数字显示，2004年～2012年上半年期间共有3116名韩国军人因为使用互联网或手机泄密而受处分，而这其中智能手机是泄密的主要途径。

用户在使用移动终端时，很容易发生主动或者被动的泄密，而泄密过程甚至可以不被用户本身察觉。例如：用户通过拍照、摄像泄露敏感位置信息；用户通过不安全的网络环境进行网络通信导致数据泄露；用户将敏感文件对外发送导致数据泄露等等。

### 警示拍照定位

为了防止用户在使用手机时无意识的泄露军人身份信息和敏感军队数据，需要在系统开启定位功能和拍照功能时，弹出警示语，提醒用户注意周围环境。

### 数据加密

对所有通过内部推送下发的文档、数据、邮件等，需要在本地进行加密处理，另外可以对本地文件及应用生成水印，防止数据通过截屏形式泄露。

### 网络加密

对网络传输过程中的数据包进行加密处理，防止用户通过不安全的网络环境泄露敏感数据。

# 方案设计

## 总体架构

通过对移动安全实际需求的分析，我们为海军定制了一套移动安全解决方案。此方案由终端设备上的安全管控APP和移动安全管理平台两部分组成，可以满足系统对移动安全的实用性、安全性和高效性的要求。

方案整体架构图如下：

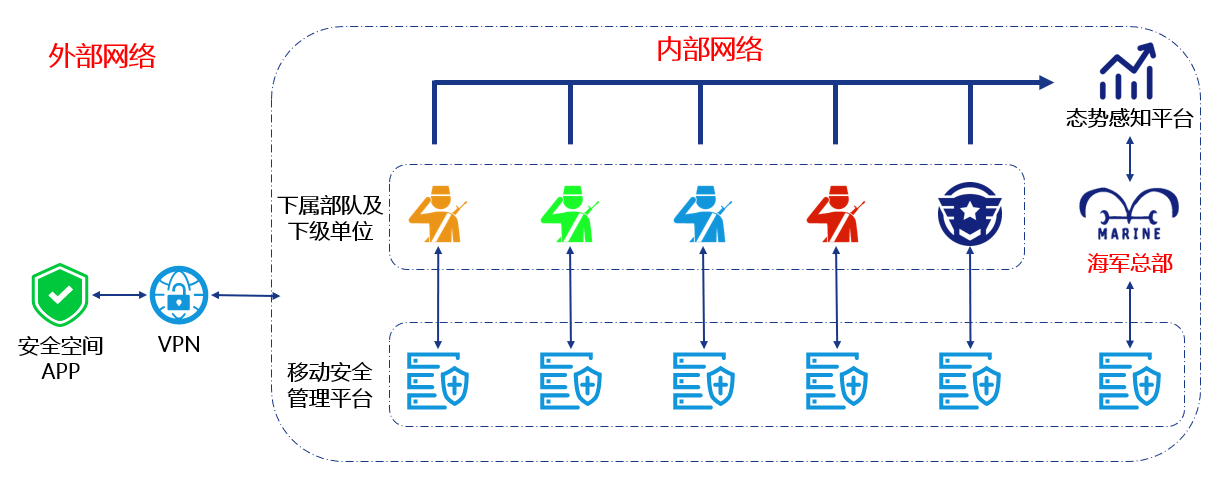


图 1移动安全办公系统整体架构图

本方案在海军总部、下属部队和下级单位各布置一套移动安全管理平台，分别管辖自己所属用户的移动设备，在海军总部额外部署一套态势感知平台，该平台会汇总收集各个移动安全管理平台的管理数据，总部管理人员可以在后台看到汇总分析后的管理数据，从而掌握整个海军用户的移动设备安全趋势。

## 功能架构



图 2功能架构图

在移动终端，我们提供了安全管控APP；在服务器端，我们提供移动安全管理平台，该平台可以采用私有云或者SaaS方式部署在指定服务器上，主要功能包含移动设备管控，移动应用管控、安全合规管控以及态势感知平台四部分。设备管控、应用管控、安全合规管控从不同维度对用户移动设备进行安全管理，管理数据由态势感知平台统一采集，分析后向后台管理人员以及领导呈现。

### 基础功能

### 拓展功能

### 后续功能

## 部署方案



## 管理方案

本系统从初始化到正常运作主要分为系统初始化和业务管理两个阶段，如下图所示。在系统初始化阶段，系统内置的超级管理员为唯一责任主体，负责完成系统初始化，包括管理员角色管理、机构管理、系统设置、客户端版本管理和License管理五项权责；在业务管理阶段，责任主体为超级管理员在机构数初始化时创建的业务管理员，业务管理员各自对权责内的机构负责，业务内容主要包括用户管理、设备管理、管理员角色管理、机构管理、策略管理、审计管理和应用管理。



本节将对两大阶段的各项管理业务作扼要说明。

### 系统初始化

系统初始化主要是系统的数据准备和系统配置，由系统内置的唯一超级管理员完成。操作流程如下图所示。超级管理员登录系统至平台管理界面，便可进入系统设置、管理员角色管理、机构管理、版本管理、Licence管理交互界面完成相应操作。下文将对这五项业务进行说明。



#### 系统设置

系统设置主要用于对整个系统的一些通用权限和特性做统一控制，包括但不限于服务端登录失败次数及冻结时间设置、客户端会话时间及密码特性设置、邮件服务器配置、系统管理员管理、认证方式配置、产品LOGO及名称等信息配置。

系统设置将这些权限和特性分为六大类，分别归于服务端设置、客户端设置、邮件服务器设置、管理员设置、认证方式设置和产品信息六个部分。

#### 管理员角色管理

超级管理员可以在管理员角色管理界面创建、编辑、删除、查询角色，每个角色对应一种具体业务的功能点集，可以视为一种业务管理员的权限，用于给机构的业务管理员快速配置权限。



#### 机构管理

机构管理的主要功能是通过导入机构树文件或者手动新建机构，初始化机构树。下图为机构树的结构示意图：



1. **机构树结构调整**

机构树支持移动、复制、删除操作，当进行此类操作时，对应机构及其所有子机构跟着移动、复制或删除。如上图，若移动一师到特战旅下面，则一师的加强团也会跟着移过去。

1. **管理员权限管控**

超级管理员可以为每个机构配置任意个数的业务管理员，配置的时候通过为每个管理员指定一个或多个角色，实现对每个机构不同业务管理员权限的定制式精准控制。

需要指出的是，超级管理员不具备直接管理机构内具体业务的权限。

#### 版本管理

版本管理用于管理客户端应用历史版本及当前版本，常用操作为查看、编辑所有版本信息及删除历史版本。

#### License管理

Licence管理用于激活、查看或者更新产品许可。该界面将清楚地呈现平台当前是否获得许可。如果已有授权许可，则会呈现许可的详细信息，包括上传时间、许可权限范围、许可剩余时间等。

### 业务管理

业务管理是各个业务管理员的日常，即处理机构内的具体事务。业务管理主要分为用户管理、设备管理、策略管理、管理员角色管理、机构管理、审计管理、应用管理。



#### 用户管理

业务管理员可以在用户管理界面，完成用户新建、批量导入、删除、编辑查找、分组管理、标签管理等操作。

1. **录入用户**

系统初始化新建的机构通常是没有用户的，业务管理员登入机构之后可以在用户管理界面手动添加用户或者批量导入用户。



1. **用户激活**

录入的用户还不能立即登录系统的，业务管理员还必须在用户管理界面激活这些用户，之后用户便能用手机登录安全管控APP。

#### 设备管理

业务管理员通过后台管理系统，对辖内的移动设备进行管控。用户的设备丢失或者更换设备时，需要通知业务管理员，业务管理员同步变更系统数据。

1. **设备注册**

在移动端，本系统提供安全管控APP，并提供安全管控APP下载地址。

用户使用移动设备扫描提供的二维码下载并安装安全管控APP，打开应用，输入用户名和初始密码(业务管理员提前录入系统)，并配置服务器地址和所属机构信息，开始登录系统(在首次登录系统时，系统会强制要求用户更改初始密码)。

移动端登录系统成功后，设备会自动注册至系统，实现对用户进行人和机的自动绑定。所属业务管理员可通过后台管理系统查看设备详情。



1. **设备丢失**

如果用户不慎遗失了手机，需要及时通知业务管理员，业务管理员在后台管理系统对丢失设备发送远程擦出设备的指令，可防止在设备无法找回的情况下导致的安全管控APP内数据泄露；对丢失设备执行淘汰设备指令，使人、机解除绑定，且从系统剔除此设备。



1. **设备更换**

如果用户需要更换设备，需要通知业务管理员，业务管理员在后台管理系统对旧设备对丢失设备执行淘汰设备指令，使人、机、卡解除绑定，且从系统剔除此设备。



1. **设备失联**

设备失联检测的功能需要合规策略(失联)的触发，如下图所示的合规策略(失联)的创建，业务管理员在后台管理系统添加合规策略，并设置失联的判断条件、限制功能，将策略下发给指定用户。

本系统有设备在线检测的机制，如果用户的账户被下发了合规策略(失联)，一旦用户的设备符合失联的条件，并以邮件向业务员管理员的进行通知。业务管理员在收到通知后，可以线下联系具体的用户进行确认和处理。



#### 管理员角色管理

业务管理员的管理员角色管理与超级管理员的管理员角色管理类似，都可以创建、编辑、删除、查询角色，每个角色对应一种具体业务的功能点集，是一种业务管理员的权限。



不同之处在于，每个机构的业务管理员管理的角色可以配置的所有功能点是有差异的。准确的说，就是其上级机构业务管理员为本机构配置的所有业务管理员角色所对应的功能点合集。

#### 机构管理

机构管理是以机构为最小管理单元，各机构业务管理员可以修改本级业务管理员的登录密码，可以创建和管控所有下级机构，并可指定所有下级机构的业务管理员和他们各自的角色，实现对下级机构业务管理员权限的控制。

业务管理员在登录界面输入自己的用户名以及密码，成功登入系统后，默认跳转至该业务管理员直接管辖的机构的业务管理界面，同时可以切换至其任意下级机构，管理其下级机构内具体业务。



#### 策略管理

策略管理涉及的具体业务除了策略的基本操作增删改查以外，还有下发、推送、推送并下发三种操作。

策略下发的主要功能是将当前机构业务管理员创建的策略下发至当前机构内指定的用户，策略效果最终在用户的手机上生效。

策略推送则是将当前机构业务管理员创建的策略推送至任意指定的下级机构，但不下发给机构内的用户。实际上可以视为将策略复制到指定的下级机构。如果需要将推送的策略下发到指定机构内特定的用户，则需要切换至相应机构下，选中其中的特定用户进行下发。

另外，接收推送策略的机构其业务管理员，可以查看、下发该策略，但是不能对策略进行修改和删除。

策略推送并下发即推送策略之后立即自动将策略下发至所选定的机构及其子机构，同时策略针对机构的用户和用户组即时生效。

对于本系统来说，策略分为设备策略、合规策略、围栏策略、应用策略、客户端策略五大类。围栏策略按围栏类型又分为时间围栏策略和地理围栏策略。

1. **设备策略**

业务管理员通过后台管理系统，对管控辖内的移动设备进行严格管控(如下图所示);

业务管理员通过后台管理系统配置设备策略，该设备策略可从四个方面对设备进行管控：1、锁屏策略(可设置锁屏密码最小长度、密码复杂度要求、最大尝试次数、密码有效期)， 2、限制策略(可管控相机、wifi、移动数据、蓝牙、GPS、短信、电话、安全管控应用) ，3、限制网络，4、限制WI-FI的使用；



1. **合规策略**

业务管理员通过后台管理系统，对管控辖内的移动设备进行违规监控(如下图所示);

业务管理员通过后台管理系统配置合规策略，该设备策略可从七个方面对设备进行监控：1、SIM卡变更 2、Rooted 3、失联(可设置失联天数) 等；针对每一种监控类型可设置不同的违规限制功能；并将合规策略下发至用户。

当用户使用的设备被发现SIM卡变更、被root、失联等情况，系统会通知业务管理员。



1. **地理围栏**

业务管理员通过后台管理系统，对管控辖内的移动设备进行地理位置的管控；

业务管理员通过后台管理系统配置地理围栏策略，该地理围栏策略通过设置指定的地理范围，并设置围栏内外的功能限制策略，对设备进行管控；并将地址围栏策略下发至用户。

用户的设备通过定位功能获取位置信息，并与设置的地理范围进行判定，动态的管控设备。



1. **时间围栏**

业务管理员通过后台管理系统，对管控辖内的移动设备进行时间区间的管控；

业务管理员通过后台管理系统配置时间围栏策略，该时间围栏策略通过设置日期区间、时间点区间、时间类型(工作日、每周、每日、特定时间)，并设置围栏内外的功能限制策略，对设备进行管控；并将时间围栏策略下发至用户。

用户的设备通过系统时间定时触发策略，动态的管控设备。



1. **应用策略**

应用策略用于管理安全管控APP外系统应用。应用策略分为黑名单策略和白名单策略。

配置应用策略之前，得先录入应用白名单和应用黑名单。应用白名单限制安全管控APP外除白名单应用外的应用启动，而应用黑名单限制安全管控APP外黑名单之内的应用启动。（如下图所示）

黑名单策略管控黑名单中的哪些黑名单应用不能访问，白名单策略则管控白名单中的哪些白名单应用可以访问。



1. **客户端策略**

客户端策略主要用于管理安全管控APP的各项功能，除了可以配置设备权限申请列表以外，还可以管控防卸载、保活、防截图、水印、剪切板等功能。



#### 审计管理

审计管理模块收集了整个系统所有管理员和用户的一切会改变数据库数据的操作日志。这些日志分为客户端日志、用户管理日志、设备管理日志、违规情况日志、策略管理日志、管理员日志等（如下图），每种类型日志的具体内容不尽相同，但基本都包含操作类型、操作时间、操作者、操作对象、操作结果这几种数据。

业务管理员可以通过查看这些日志，监控机构内所有成员、设备的行为。为了方便业务管理员查看日志，日志管理支持时间过滤、类型过滤、文本搜索等辅助功能。



# 方案特点

# 软硬件清单

## 软件清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **功能模块** | **子模块** | **描述** | **单位** | **备注** |
|  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | |  |  |  |
|  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  | |  |  |  |

## 硬件清单

### 移动安全管理服务器

|  |  |  |
| --- | --- | --- |
| 名称 | 参数 | 备注 |
| 移动安全管理服务器 | CPU：Intel(R) Xeon(R) CPU E5-2609 v4 @ 1.70GHz 16核  内存：32G  硬盘：500G  操作系统：CentOS 7.4 64位 |  |

### 移动终端

手机型号：华为、小米、OPPO、vivo、三星等；

手机操作系统：Android 4.4-8.0；

手机内存：建议可用内存在1G以上。

## 网络配置清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **服务** | **版本** | **提供功能** | **端口** | **备注** |
| SecSpace VPN | / | VPN服务 | 443 | 自带软件VPN |
| SSH | / | 远程访问 | 22 | 远程安装及调试时需要开启 |

注：需要开通网络防火墙策略，远程可访问443端口和22端口。

# 建设工期