网络基础设施：

一期，依据业务量级规划如下：

1. 本地IDC：
   1. 规划专线带宽100Mb，与混合云和办公区联通，用于混合云之间高速数据通讯；规划公网网络200M带宽，用于保障互联网业务服务。
   2. 规划机柜3个，核心接入设备10台，构建公网与内网、vpn网络等互为隔离的网络，采用堆叠方式部署，同时机柜之间互为冗余，用于接入服务器，存储设备，堡垒主机等网络设备。同时保障网络高可用。汇聚设备4台，采用堆叠模式，互为冗余，分别汇聚公网和内网到对应网络中。
   3. 构建防火墙设备，和流量分析设备，保障设备系统以及设备承载的业务安全。
   4. 构建堡垒主机，保障业务人员以及运维人员操作安全，同时应对审计要求。
   5. 规划盘柜1个，构建IDC高速存储中心。盘柜高效的读写效率以及严谨的权限和空间配额管理可以有效支持各个业务节点数据存储和使用要求。
   6. 规划服务器12台，用于构建基于容器的高可用资源弹性环境，保障资源利用率和业务稳定性。
2. 云服务：
   1. 业务需求基本要素，如域名，解析，防劫持，证书等，使用云服务。
   2. 业务加速CDN，包括静态加速和流媒体加速，使用云服务，一期规划静态流量1PB，规划媒体资源加速带宽5G。
   3. 使用SLB实现业务在云与机房的动态调度。规划300Mb。用户经CDN回源的访问经SLB动态在云与机房的动态调度。混合云跨节点之间的数据同步，通过数据专线和混合云高速通道实现对接。保障业务数据与内部数据的隔离，提高安全性和稳定性。
   4. 规划各类服务器180台，采用适配原则动态申请释放。
   5. 在存储方面规划300T存储，用于对云上各业务节点的存储支撑，同时与机房内存储构建双活数据中心，确保数据安全。
   6. 在三方服务方面，构建各类消息服务，如短信服务，消息推送服务，邮件服务等。保障业务需求。
   7. 安全层面，云安全引入代码渗透测试和系统漏洞扫描，每年1到两次，确保系统和代码健壮。同时引入安全服务，包括白盒测试，系统加固等。在业务内容安全层面，充分考虑言论敏感，引入对敏感图文，影音的规律，确保每一个发布出来的信息均足够健壮。
3. 监控和高可用：
   1. 部署监控服务，包括网络性能监控，移动端性能监控，监控报警系统等，实现对运行状态信息的及时感知和处理。

在二期，三期，四期的规划中，随着业务量的增加，各项资源的投入逐渐加大。基本依照一期的架构，按照业务量级，对机房和云各项资源做动态调整。