## 技术服务要求

## 1.云网络安全运维要求

统一协调包括IT运维专家团队在内的运维资源，实时监控采购人指定的信息系统运行状况，及时发现并排除网络运行中的不良因素消除安全隐患。安全服务厂商结合采购人系统现状，提供切实可行的项目服务方案（包括但不限于安全评估方案、安全整改方案和安全运维服务方案）。

### 1.1驻场人员要求

* 驻场人员持有CISP（注册信息安全专业人员）等证书。具有一定公文写作能力。
* 驻场人员从事不少于3年网络安全运维工作，掌握信息安全技术相关技能，包括:云平台网络安全技术、安全咨询、安全评估、等保服务、数据中心云化等方面;掌握等级保护标准、分级保护标准、安全风险评估规范和实施流程及方法，具备等级保护、风险评估、数据中心等信息安全领域咨询和建设的相关标准和测评实施的方法和经验。
* 熟悉信息网络安全相关基础产品特性，了解市场上现有常见的网络安全设备和产品。熟悉各领域的安全技术，包括：Web安全、系统网络安全、大数据平台安全、云平台安全、网络安全域的划分等，熟悉安全漏洞扫描等常用安全设备；
* 掌握主流操作系统、数据库、网络设备的配置及使用；掌握一种或多种编程或脚本语言，如Python、Perl等；
* 掌握维护设备的操作方法、故障排除方法、设备性能监测及注意事项。确保维护设备的安全运行，每日进行巡检，监测，根据业主需要进行相关配置。
* 所有涉及特征库、病毒库服务的设备或软件均应提供免费升级服务。

### 1.2维护服务清单

#### 1.2.1设备监控

驻场工程师将提供5\*8小时为基础的设备现场监控和7\*24小时的手机在线值班，以配合首讯科技的日常运营。 驻场工程师的现场监控任务不仅仅是简单的“告警监控”，而是参考警报和性能指标，通过不同的方式和性能数据进行诊断，以更有效地识别问题，挖掘故障根因，以确保可以快速、专业地处理可能发生的任何故障和告警。

#### 1.2.2预防性维护

驻场工程师通过现场或远程访问的方式对云安全设备进行每月一次的预防性维护，包括设备巡检，异常整改或调整，测试，设备内部和外部清洁，以及设备单元，板件，组件，模块的运行状态检查，异常部件的维修或更换。

预防性维护的目标是使设备保持稳定和正常的工作状态，预防缺陷和退化，从而减少设备故障发生频率和故障处理的时间。

#### 1.2.3故障管理

故障管理包括故障预测、故障诊断、故障处理、故障升级和故障进展跟踪、技术支持升级等子流程。

#### 1.2.4配置管理

驻场工程师将根据业主的业务需求对业务配置进行修改，包括监督或执行生成、修改和删除设备的业务数据配置。对于计划性的设备系统配置修改、软件更新，驻场工程师将负责分析此配置变更的影响，设计和优化所需的设备配置数据，协调资源完成配置变更。

配置变更操作结束后，驻场工程师将进行24小时业务监控，以业务系统的正常使用。

#### 1.2.5重点保障

在重要节日，重大会议或攻防演习期间，驻场工程师将与甲方工程师或第三方其他驻场人员一起准备并执行重大事件保障计划，主要动作包括：

提前准备额外的资源，备件和耗材；

提前设备巡检，负载检查，数据备份和清理；

制定值班计划，确保及时响应；

制定紧急和应急计划；

与甲方工程师或第三方其他驻场人员进行计划沟通，确保各方的准备；

至少保障2人同时驻场。

#### 1.2.6建立设备安全配置基线库

建立设备的安全配置基线库、定期对采购人现有系统进行脆弱性分析，对采购人开展行业网络信息安全监管工作、网络规划、信息安全建设和安全评审等信息系统相关活动提供技术支持。

## 2.网络安全咨询服务要求

根据《网络安全法》及GB/T 22239-2019《信息安全技术网络安全等级保护要求》（以下简称“等保2.0”）等要求，提供包括且不限于安全管理体系建设、培训及演练服务、应急响应服务、网络安全检查、安全咨询服务、专项通报服务等服务。

### 2.1驻场人员要求

驻场人员持有CISP（注册信息安全专业人员）等证书。具有一定公文写作能力。

驻场人员从事不少于5年网络安全咨询工作，掌握信息安全技术相关技能，包括:云平台网络安全技术、资产梳理、安全制度汇编、信息安全保障设计规划咨询、安全评估、等保服务、渗透测试、漏洞管理、威胁管理、新上线业务安全评估等。

熟悉信息网络安全相关基础产品特性，了解市场上现有常见的网络安全设备和产品。熟悉各领域的安全技术，包括：Web安全、系统网络安全、大数据平台安全、云平台安全、网络安全域的划分等，熟悉安全漏洞扫描等常用安全设备；

掌握主流操作系统、数据库、网络设备的配置及使用；掌握一种或多种编程或脚本语言，如Python、Perl等；

掌握安全设备的基本使用及策略配置。

### 2.2网络安全咨询服务清单

#### 2.2.1安全管理体系建设服务

参照国家及行业相关政策要求以及国内国际权威安全管理体系标准，结合工作实际，配合业主单位完善和修订网络安全制度、应急预案、个人信息管理办法等相关安全管理制度，完善安全管理体系，并对制度的可实施性、可操作性提出相关合理建议。

#### 2.2.2等保服务

根据等保2.0等相关文件要求，协助业主单位对需要备案的信息系统完成定级备案，协调和邀请专家对所有需要定级备案的信息系统进行定级报告评审；针对信息系统进行差距分析，出具可实施的《差距分析报告与整改方案》，协助业主开展整改工作，确保顺利通过等保；协助开展等保测评工作，根据等保测评结果，制订合理的整改方案，并提供多种形式的技术响应和支持协助落实。

#### 2.2.3培训及演练服务

根据业主安排，提供培训、演练服务；提供完善的培训实施计划、培训材料，由有网络安全相关资质的讲师承担；提供全面的演练实施方案，提供相关应急物资，提供演练技术服务，并形成完整的演练资料，根据演练情况完善或修改应急预案；根据业主单位完成保网/护网工作，提供全面的保网/护网方案，提供技术支撑，并形成完整的保网/护网材料，并在保网/护网期间安排驻场值守人员。

#### 2.2.4应急响应服务

提供重大时刻安全保障；对业主网站提供7\*24小时实时监测服务；当业主单位发生网络安全事件或事件预警时，应半小时响应，并根据情况派出安全专家团队开展事件响应工作，制订应急处置方案，现场排查处理安全事件，保障业务系统的连续性，阻止和减小安全事件带来的负面影响；专家团队必须第一时间通过电话进行远程指导，一小时内到达现场；事后完善相关过程资料。

#### 2.2.5专项安全检查

配合业主对业主及下属单位网络安全情况进行季度检查和不定期抽查，编制检查方案，形成检查记录，汇总分析，并提供可行整改方案；配合业主接受上级单位安全检查，编制迎检方案，协助准备迎检材料，做好前期迎检工作，现场协助检查，提供相关技术支持，对检查情况进行问题汇总分析，并提供可行整改方案；协助业主开展问题整改。

重大节假日、重要会议、重大活动、敏感时期等重要期间前期配合业主开展节前巡检、安全自查、检查与整改，期间安全值守，形成相关方案、记录等。无偿提供设备进行安全防护，至少保障2人同时驻场值守。

#### 2.2.6新建信息化项目安全检查

对所有在云平台上部署的新系统，上线或接入前进行安全漏洞扫描、渗透测试、代码审查等各项检查，并提供检测报告及整改建议与措施。。

#### 2.2.7巡检工作

提供资产梳理及日常巡检服务，包括7\*24小时网站实时安全监测、不定期对服务器、网络、终端关键设备开展日常巡检，并形成记录文档，并及时更新资产。

每季度开展不少于一次的季度巡检服务，内容包括且不限于渗透测试、风险评估、基线核查、WEB扫描、漏洞扫描、基线检查、弱口令、恶意代码检查、日志审计等。

#### 2.2.8加固服务

根据业主需求进行渗透测试、风险评估、基线核查、WEB扫描、漏洞扫描、基线检查、弱口令、恶意代码检查、日志审计等。提供安全漏洞修复、安全基线配置、网络及主机安全策略优化等服务，若需外单位协助整改，提供整改细则说明及相关配合工作。

#### 2.2.9安全咨询服务

包含且不限于按照路网公司要求落实网络安全整体建设规划、设计网络结构改造及优化方案、网络技术咨询、安全技术咨询、安全需求分析、建设期间安全咨询、相关政策文件及上级单位文件落实咨询等服务。

#### 2.2.10专项通报服务

根据上级单位要求及本单位通报规范，提供通报数据来源分析、通报信息汇总等服务；针对网监、网信办、交通部、交通局等上级单位及互联网安全漏洞预警通知、安全通报、安全风险排查等响应，提供技术解决方案并处理，提交处理反馈报告；制定重大时刻工作计划与工作方案等。