附表　主要工作内容

序号	主要工作	具体内容	成果要求
1	重要活动期间网络安全保障	1.根据行政主管部门和上级单位以及集团公司要求，在未来一年重要活动期间（国庆、春节、四中全会等，不少于 80 天）提供 7*24 小时的专业技术保障人员驻场服务，确保系统持续、稳定运行； 2.提供突发事件应急处置保障，当发生事件时，能快速做出研判，在 15 分钟内组织技术专家进行处置，并于事后出具处置报告。	1.编制重保期间每日网络安全日报； 2.在关键时间节点形成阶段性总结报告。
2	网络安全日常监测	1.利用流量监测工具或态势感知工具对集团总部机房、算力中心机房的日常网络流量进行采集，通过监测和分析，发现网络中存在的各种威胁和沦陷主机； 2.提供网站漏洞发现、网页篡改监测、网页挂马监测、黑词/暗链监测、可用性监测、仿冒/钓鱼网站监测等服务，对监测结果进行研判，及时推送可能造成影响的安全事件； 3.对攻击事件进行分析，还原攻击路径、攻击手法、攻击过程，并查找其他受影响设备，提出最佳的应对方案和措施。	1.按月出具流量检测分析报告和网站安全分析报告； 2.及时推送安全事件报告； 3.根据实际工作要求编制处置方案及改进建议。
3	信息系统安全检测	1.利用安全扫描评估工具每月对蜀道集团总部和蜀道智慧交通集团的核心服务器及重要的网络设备进行漏洞扫描，查找安全漏洞和系统隐患； 2.利用安全扫描评估工具每月对蜀道集团互联网侧的所有信息系统进行漏洞扫描（不少于 800 个）查找系统安全漏洞； 3.分 2 次对蜀道集团门户网站、财务、人资等重要信息系统以及新上线系统进行渗透测试(每次不少于 200 个系统），查找系统的脆弱性和风险点； 4.利用扫描工具每半年对蜀道集团总部和蜀道智慧交通集团的终端电脑进行保密文档扫描，防止涉密文件泄露； 5.建立风险跟踪台账，协助和跟进督促相关整改负责人完成风险整改。	1.按月出具漏洞扫描报告（分设备和系统）； 2.形成渗透测试报告； 3.形成保密文档扫描报告； 4.形成信息系统风险台账，按月记录全部系统的漏洞情况和漏洞整改情况。

4	网络安全检查和抽查	1.协助集团公司开展网络安全检查，提供人员和技术支持； 2.对蜀道集团开展 1 次“红队评估”服务（覆盖信息系统数量不少于 100 个），通过随机抽查及时发现存在问题，并协助系统责任单位进行整改。	1. 编制年度网络安全检查实施方案； 2. 形成红队评估报告。
5	攻防演练及应急演练	1.开展 1 次网络安全攻防演练，以系统提权、控制业务、获取数据为目的开展实战攻击，检验蜀道集团信息系统的网络安全防护能力（覆盖信息系统数量不少于 100 个）； 2.攻防演练结束后总结时挑选两个攻防演练成果作为模拟场景，设计攻击及应急环节，组织开展应急演练，检验和宣贯网络安全事件应急预案。 3.开展应急演练后根据演练时实际应急流程可优化程度对蜀道集团应急预案进行优化及修订。	1.制定攻防演练实施方案，形成攻防演练总结报告和整改建议书； 2.制定应急演练方案，编制应急演练脚本（如果需要），形成应急演练总结报告； 3.结合应急演练情况对应急预案进行优化和修订。
6	网络安全预警信息通报	收集和整理国家及行业发布的网络安全重大漏洞、安全风险、热点事件、安全态势、内外部威胁情报等，提供实时的网络安全预警信息通报和应急响应措施建议。	按月形成预警信息汇总报告。
7	网络安全制度建设	根据《蜀道集团网络安全管理办法》管理体系架构，编制蜀道集团数据安全相关的管理制度 2 份。	暂定为《数据安全管理办法》《数据安全事件应急响应实施指南》，根据具体工作情况进行调整。
8	网络安全教育培训	1.根据实际工作要求及日常工作内容，开展针对全员的安全意识培训课程，提升蜀道集团全员日常工作中网络安全意识风险； 2.针对蜀道集团网络安全相关管理人员开展安全政策解读及安全建设规划培训； 3.针对蜀道集团网络信息安全相关工作人员开展安全技能培训，包括但不限于：应急响应技术、安全测试技术、流量分析技术等。	1.制作培训教材，包括但不限于视频、PPT 等； 2.组织讲师进行授课； 3.提供一次面向网络安全产品操作的技术培训；

			4.提供2个CISP或同级别认证考试培训名额。
9	蜀道大厦机房安全运维驻场	提供蜀道大厦机房全年5*8小时的专业技术人员驻场服务，逐步完善网络安全管理制度和工作机制，规范日常管理工作和审批程序。	1.编制机房管理的相关工作规范； 2.开展日常管理工作，形成机房值守工作台账。
10	信息系统资产测绘	1.提供资产测绘工具对现有信息系统资产进行ICMP的方式进行存活探测，在网络禁PING时也能采用其他探测方式进行存活资产探测； 2.利用PDNS、大网测绘情报、域名备案情报等情报数据内容，发现企业暴露在互联网的影子资产； 3.对蜀道集团内网、外资产开展全面梳理，建立资产台账，定期对资产台账进行更新。	形成蜀道集团信息系统资产台账，并持续更新。
11	信息系统风险评估	1.参照《GB/T 31509-2015 信息安全技术 信息安全风险评估实施指南》、《GB/T 20984-2022 信息安全技术 信息安全风险评估方法》，对蜀道集团总部和蜀道智慧交通集团的信息系统资产、威胁、脆弱性、安全措施进行识别和分析，确定风险计算模型，从物理层、网络层、系统层和应用层等方面进行评估，全面分析系统面临的信息安全风险。 2.通过对集团总部、算力中心的网络架构，数据流向了解后根据核心数据库、数据存储点，逆向反推攻击链路，梳理链路后对链路上安全设备策略、安全能力等进行评估。	1.形成风险评估报告； 2.形成链路安全评估报告。