主要参数：

1.规范化要求：项目的架构和实施符合丽水市卫生健康网络信息安全管控平台建设方案（丽卫函〔2020〕635号）的要求。

2.平台接入及配套流量采集设备部署：接入丽水卫健委安全管控平台，并于平台联动。设备能发现已知和未知的高级网络攻击，基于威胁情报的上下文，可以为技术负责人员发现、研判和处置重大安全事件提供部分数据支持，还原和存储网络流量的元数据。

3.安全巡检：定期提供全方位的安全巡检服务，巡检内容包括授权状态检查、版本检查、网络流量检查、运行状态检查。系统资源占用检查、安全告警状态检查等。了解系统的整体工作状态，并为用户提供详细、专业的巡检服务报告。（4次/年）

4.漏洞扫描：SQL注入检测、跨站脚本攻击检测、文件包含漏洞检测等web漏洞检测，对各类操作系统进行漏洞扫描，对IIS、Apache、PHP等常用的软件进行漏洞扫描 对Windows主机、类Unix主机等目标对象进行漏洞扫描，统计漏洞数量、所有开放端口、列出每一个漏洞所存在的主机、详细描述与修补建议，提供扫描报告，并根据扫描报告给出整改建议。（ 4次/年）

5.应急响应：提供日常安全应急响应服务，服务期内，当业主发生病毒和蠕虫事件传播影响业务、黑客入侵事件等网络安全事件时，在接收业主的应急技术支持请求时，应在30分钟内响应；如需到现场进行技术支持的，根据路程在2-4小时内到达现场并协助用户进行处理。（1次/年）

6.信息安全通告：每月提供信息安全通告及不定期重要信息安全通告，通过实时和定期2种方式推送，包括威胁情报解读、高危漏洞预警、安全热点、漏洞统计分析、包括媒体关注通告、恶意IP地址攻击信息、安全资讯安全信息，旨在向用户提供有价值的安全预警和威胁情报资讯。不限次数 。

7.渗透测试：通过模拟黑客攻击的方法对系统进行非破坏性质的攻击性测试，根据检查结果制定针对性的加固方案，并协助进行安全加固处理和漏洞修复情况复测，以确保系统的安全性。渗透测试内容需覆盖OWASP TOP 10漏洞风险、业务安全风险、应用安全风险。（2次/年）对渗透测试结果及安全评估结果进行二次评估和测试，出具独立《回归测试报告》，并就加固前与加固后的效果进行对比分析，同时对未完全解决的问题进行列举，给出相关建议。