**伦理审查与监管信息平台维保服务需求**

### **系统日常维护**

1. 7×24 小时监控系统运行状态，及时发现并处理系统故障，确保平台的稳

运行故障响应时间不超过10分钟，一般故障修复时间不超过 2 个工作日，重大故障修复时间不超过 3个工作日。

1. 定期对系统服务器、网络设备、存储设备等进行巡检，包括硬件状态检查、

性能指标监测、日志分析等，及时发现潜在问题并进行预警和处理。每月至少进行一次全面巡检，并提交详细的巡检报告。

1. 负责系统软件的安装、升级、补丁管理等工作，确保系统软件的安全性、稳

定性和兼容性。及时跟进操作系统、数据库管理系统、中间件等软件的官方更新，在测试环境验证后，按照既定的变更管理流程进行生产环境的升级和补丁部署。

### **安全保障服务**

1. 建立健全信息安全管理制度和流程，加强对平台的安全管理和监督。制定信

息安全策略、用户权限管理规定、数据安全管理制度等，明确信息安全责任，定期对制度的执行情况进行检查和评估。

1. 负责平台的安全防护工作，包括网络安全防护、应用安全防护、数据安全防

护等。部署防火墙、入侵检测系统、防病毒软件等安全设备，定期对系统进行安全漏洞扫描和修复，防范网络攻击、恶意软件感染和数据泄露等安全事件的发生。每季度至少进行一次全面的安全漏洞扫描，并及时修复发现的高危漏洞。

### **技术支持与培训服务**

1. 提供 7×24 小时的技术支持服务，解答用户在使用平台过程中遇到的技术问题。通过电话、邮件、在线客服等多种渠道接受用户咨询，确保用户问题得到及时有效的解决。对于用户反馈的问题，建立问题跟踪台账，记录问题处理过程和结果，定期对问题进行统计分析，总结常见问题及解决方案，提高技术支持服务效率。
2. 为平台用户提供系统操作培训和业务培训，帮助用户熟悉平台功能和业务流

程。根据用户角色和需求，在运维期内提供不超过5次远程培训服务。