**文件安全摆渡系统采购项目(2023年)需求**

# 项目名称

项目名称：文件安全摆渡系统采购项目(2023年)

# 建设内容

1. 需求内容如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 设备名称 | 数量 | 设备参数描述 |
| 1 | 文件安全摆渡系统 | 1台 | 冗余电源，不少于2个千兆网口，不少于2个万兆光口，并发用户数不少于200个、注册用户数不限，支持隔离网络数不少于4个、存储容量不少于960SSD+12TBHDD，提供三年企业级病毒特征库升级及软、硬件维保服务。  必须具备以下功能点：   1. 网路隔离区域文件摆渡； 2. 分级审批； 3. 操作记录审计功能； 4. 企业级防病毒功能； 5. 支持网络物理或逻辑隔离； 6. 数据防泄密DLP功能。 |

1. 文件安全摆渡系统的技术指标要求：

|  |  |
| --- | --- |
| 序号 | 指标要求 |
| 1 | 业务板端口：≥2个千兆以太网端口，≥2个万兆光口（含光模块），硬盘空间≥960GB SSD+12TB HDD。 |
| 2 | 数据摆渡吞吐量≥800Mbps，最大用户数：无限制。 |
| 3 | 支持≥4个不同等级域（隔离网络间），实现不同网络之间的数据摆渡。  支持基于SSL的加密传输，系统应具备加密存储能力，不以明文存储数据，防止后台恶意获取文件。 |
| 4 | 同一时间段内，系统支持≥200个用户的并发操作（登录、上传、下载等）请求。 |
| 5 | 内置企业级防病毒软件并可自动或手工更新病毒库，用户上传文件时，自动对文件进行防病毒扫描。 |
| 6 | 设备保留病毒检查的历史记录，管理员可通过控制台随时查询 |
| 7 | 支持不同用户间的文件分享，可控制分享方向，即分享者可将文件分享到有效等级域，支持外链分享。  用户可以对有权限的文档进行外链分享，用户在分享时可以设置分享有效期及访问密码，设置预览、下载等权限。 |
| 8 | 支持管理员可修改用户状态、管理员可设定用户过期时间、管理员可设定用户允许登录的范围。 |
| 9 | 支持各个隔离网络区域间进行文件摆渡，登录接口均可配置登录失败锁定策略，防止暴力破解。 |
| 10 | 支持用户认证信息、文件交换信息、文档追踪审计信息、敏感文件审计信息等日志查询及审计（提供产品界面截图证明）。 |
| 11 | 支持对用户上传的文件，可划分给多个管理员进行审批管理。 |
| 12 | 支持可设置一个或多个审批员。任意一人同意时，流转到下一环节；任意一人拒绝时，审批结束，逐级分级审批流程。 |
| 13 | 支持可一键重启宿主机，保证异常情况下的业务操作延续性。 |
| 14 | 支持在外网服务器下载补丁后，通过交换系统将补丁交换到内网的指定目录，系统获取补丁。 |
| 15 | 管理员可设置一个帐号，在多台终端上同时登录，实现同个账号同时多用的功能。 |
| 16 | 支持管理员管控用户上传文件的源网络和目标网络、应用范围、例外对象。 |
| 17 | 支持CS、BS客户端中文和英文版本的切换。支持windows/linux/masOS等操作系统 |
| 18 | CS客户端支持断点续传功能。 |
| 19 | BS客户端在线预览及编辑。 |
| 20 | 支持和现网的准入控制系统实现联动，通过准入客户端实现文件摆渡客户端的身份认证单点登录。 |
| 21 | 硬件现场质保及软件升级和内置病毒库免费升级三年。 |
| 22 | 支持对接企业微信或移动端进行审批操作。 |
| 23 | 根据用户需求，支持定制化开发 |
| 24 | 满足等保安全要求，根据院方安全扫描结果定期按需修复漏洞。 |
| 25 | 具有公安部颁发的《计算机信息系统安全专有产品销售许可证》（提供盖章版复印件） |
| 26 | 具有版权局《计算机软著著作权登记证书》（提供盖章版复印件） |

1. **日常维护**
2. 稳定运行保障：制定和调整系统检查和维护方案，根据实际使用需求适当开启文件安全摆渡系统的文件审批、文件病毒查杀等功能，保证系统能满足在三个以上的隔离网之间实现跨网文件传输与文件传输安全，承受日常办公中文件传输压力，保障系统高效、稳定地运行。
3. 系统错误修复：用户在使用过程中所产生的系统故障问题，需要在2个工作日完成系统故障修复。
4. 系统数据修复：系统使用过程中，因用户误操作等原因导致系统数据错误，需要查明问题原因和进行数据修复。在7个工作日完成修复。
5. 实施培训：负责因各种原因变化增加的项目实施和人员的系统培训工作。
6. **修改调整**

根据院方的要求修改文件安全摆渡系统的策略配置，使其更完善、适应环境的变化，将策略变更内容进行梳理，输出系统策略变更表，便于后续开展系统维护工作。

# 服务方式

1. 供应商成立专门的项目组开展工作，指派专人负责，按时完成工作内容。
2. 以现场服务为主，其它电话、邮件指导、远程维护、技术交流方式不限。

# 服务时间

文件安全摆渡系统的维保期为验收后36个月。

# 服务响应要求

1. **日常维护响应**
2. 售后服务需求发起后，供应商需要在1小时内响应；紧急情况下，2小时到达用户现场。
3. 供应商应提出故障解决方案，工作至故障完全修复且系统正常提供服务为止，修复时间不超过2个工作日。
4. **修改调整响应：**供应商应在院方提交修改调整内容后的2天内落实交付。

若供应商未能及时进行需求响应，院方有权终止维护合同。

1. **供应商应作出无推诿承诺：**即供应商在收到院方故障报修通知及要求后，须立即派技术人员到场，全力协助、使系统尽快恢复正常。
2. **提供详细的维护人员清单**

供应商应有专门的维护部门并指定固定技术力量用于信息系统维护，并向用户提供详细的维护人员清单及其联系方式。

1. **系统维护工作要求**
2. 供应商须有完整的维护记录管理，确保所有问题提出及处理有记录，有供双方共同记录反馈的简捷的操作方式，达到经双方确认真实可信，可跟踪问题解决情况，查询所有维护记录，并可作为验收依据。
3. 供应商需根据院方要求，安排维护人员使用院方项目管理平台系统中的需求管理模块和缺陷（报障）管理模块，接收院方相关报障及需求信息，并反馈相应处理信息，该维护记录可作为维保履约证明。
4. 定期每周进行系统巡检，对系统运行的软硬件情况、文件安全交换情况进行监控，并出具巡检报告，针对潜在的风险应提供解决方案并实施。