甘肃省公共资源交易网络信息安全管理办法

第一条 为加强公共资源交易信息系统和交易数据安全保护，保障信息系统稳定正常运行，根据《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》《中华人民共和国计算机信息网络国际联网管理暂行规定》等有关法律、法规、规章的规定，结合实际，制定本办法。

第二条 本省行政区域内公共资源交易局（中心）的网络信息系统安全保护管理工作适用本办法。

第三条 本办法所称网络信息系统，是指与公共资源交易相关的软件系统（电子服务系统、电子交易系统、电子监管系统等），网络系统（交换设备、传输设备、网络安全设备等），硬件设施（计算机、监控系统、询标系统、门禁系统等），支撑平台（服务器、数据库、存储、云平台资源等），数据资源（各类公共资源交易数据、设备配置信息、系统日志等）。

第四条 公共资源交易局（中心）负责本平台网络信息安全保护管理工作。

第五条 网络信息系统的安全保护，应当涵盖公共资源交易相关软件系统、网络系统、硬件设施和支撑平台。应保障所有相关系统、设施的功能正常发挥，应保障所有数据资源的安全性、合法性和有效性。

第六条 公共资源交易局（中心）应当构建公共资源交易网络信息安全防护体系，保障信息系统及其相关的设备、设施、

网络安全，保障公共资源交易平台运行安全和数据安全。

第七条 公共资源交易局（中心）应当履行信息安全主体责任，按要求对本平台信息系统进行安全等级保护测评，制定本平台的网络信息安全应急响应预案，定期开展网络安全应急演练，提高网络安全意识。

第八条 任何单位和个人不得利用公共资源交易网络信息系统危害国家安全、泄露国家秘密，不得侵犯国家、社会、企业利益和公民的合法权益，不得泄露应该保密的信息，不得将重要敏感数据擅自公开及用于商业用途，不得从事违法犯罪活动。

第九条 公共资源交易局（中心）及其工作人员不得通过任何非法手段接入和使用互联网。

第十条 严格管理连接到互联网的设备设施；对涉及国家秘密及商业秘密的设备，必须做到专机专用，严禁接入互联网。

第十一条 所有需要连接互联网或允许通过互联网访问的设备设施，要统一规范设置 IP 地址和访问端口，要通过白名单控制其访问权限。

第十二条 通过互联网下载的文件，必须经过计算机病毒和木马扫描后方可使用。

第十三条 公共资源交易局（中心）须做好接入互联网的网络系统及支撑平台系统日志的存储和分析工作，并做好日志备份工作。

第十四条 公共资源交易局（中心）要定期对内部局域网进行安全扫描，对发现的漏洞及时修补、并统一提供修补程序及

修补办法。

第十五条 公共资源交易局（中心）负责对内部局域网上的设备设施的网络配置信息进行登记管理，对所有设备的 IP 地址进行统筹分配和登记，局域网内部所有设备必须使用单位统筹分配的 IP 地址，不得私自修改。

涉及全省远程异地评标系统的所有设备，应当使用由省公共资源交易局统筹分配的 IP 地址。

局域网内的所有计算机、服务器的工作组名、域名和计算机名等配置信息不得随意修改，防止影响网络通讯。

第十六条 任何单位和个人不得从事下列危害内部局域网网络信息安全的活动：

（一）未经允许访问、修改和删除任何设备设施的配置信息；

（二）未经允许，对公共资源交易相关的软件系统、数据资源进行查阅、删除、修改；

（三）故意制作、传播计算机病毒或木马等破坏性程序；

（四）其他危害计算机信息网络安全的行为。

第十七条 局域网中的计算机应专人专用，并设置独立的系统账号和密码；对多人共用一台计算机的，应分别设置每个人的系统账号及密码，保存在该计算机上的涉密资料应设置密码进行保护；系统登录密码要定期更改；关键计算机应当设置定时屏保及密码。

第十八条 任何部门或个人未经允许，不得擅自安装、拆卸或改变软件系统、网络系统、硬件设施和支撑平台，不得擅自

访问和修改数据资源。对获准允许安装、拆卸或改变的，进行记录留痕。

第十九条 公共资源交易局（中心）要统一部署国产正版防病毒软件，所有计算机、服务器都必须安装防病毒软件客户端，并接受服务端的集中统一管理，未安装防病毒软件的计算机、服务器严禁接入内部局域网。

第二十条 公共资源交易局（中心）负责管理防病毒软件服务器，承担病毒防御策略制定和病毒特征库的分发工作。

第二十一条 公共资源交易局（中心）要确定专人负责管理防病毒服务器，确保防病毒服务器的正常运行和病毒特征库的及时更新。防病毒管理员应每天定时对所有计算机、服务器进行病毒扫描，发现病毒的应立即查杀。

第二十二条 任何单位和个人不得擅自停用或删除计算机、服务器中的防病毒软件；使用计算机、服务器时要关注防病毒软件的状态，确保防病毒软件正常工作；发现问题及时与防病毒管理员联系。

第二十三条 发现计算机、服务器感染病毒，应立即启用防病毒软件进行杀毒处理。如发现无法清除病毒，应立即采取如下措施:

（一）迅速断开本机的网络连接，做好病毒查杀工作;

（二）工作人员应作好相关记录，并立即报告本单位负责人;

（三）情况严重的，应立即启动应急预案，并做好取证工作。

第二十四条 公共资源交易局（中心）统一管理本平台信息网络系统的账号和密码；密码要定期更换，长度不少于10位，要采用数字、字母和符号组合进行设置；软件系统、网络系统和支撑平台管理账号必须设置密码，不得使用系统默认密码；密码必须采用分段管理方式，有条件的要使用数字证书进行用户身份认证。

第二十五条 公共资源交易局（中心）对来自各种渠道的信息网络服务请求、告警和故障，按照运行维护事件的范围、影响和紧急程度进行处置并做好记录工作。

第二十六条 软件系统、支撑平台及数据资源相关的运行维护服务工作包括以下内容:

（一）负责软件系统支撑平台的用户账号、密码和权限的分配与管理;

（二）负责软件系统支撑平台的运行状态检查、资源配置和日志分析;

（三）负责软件系统的安装、测试、升级、培训、技术支持等服务，并做好相应记录，要做到处处留痕、可溯可查;

（四）负责软件系统支撑平台的安全防护;

（五）负责软件系统用户的增加、删除和修改工作，对系统使用权限进行分配;

（六）负责软件系统和数据资源备份，并制定相关的备份和恢复策略;

（七）负责完成与各类第三方软件系统的对接和数据交换共享工作;

（八）负责对数据资源的完整性、有效性、合法性进行校验，及时处理发现的数据问题。

第二十七条 软件系统及支撑平台要满足以下安全要求:

（一）软件系统代码或数据资源的任何修改，必须经公共资源交易局（中心）负责人审批后进行修改并记录;

（二）软件系统中的数据传输要采用安全套接层（SSL）实现加密;

（三)软件系统要具备防结构化查询语言(SQL)注入功能;

（四）支撑平台应具备入侵监测、病毒查杀、漏洞修复、网页防篡改等功能;

（五）支撑平台应具备维护服务审计功能，可以全程记录运行维护服务人员对支撑平台的使用过程，做到可溯可查;

（六）在公共资源交易活动中需要提供电子文档的，应当使用数字证书进行签名和加密。

第二十八条 网络安全运行维护服务工作包括以下内容:

（一）对网络安全情况进行分析，对系统运行过程中出现的网络安全问题进行监控并及时解决;

（二)全面规划和指导系统升级、网络病毒的控制等工作，及时消除网络安全隐患;

（三）负责网络系统、硬件设施和支撑平台的配置，关闭网络系统、硬件设施和支撑平台上非必要的服务和端口，减少安全隐患；对所有设备设施的配置信息和运行日志进行规范管理;

（四）发生网络入侵或攻击事件时，要具备必须的应对手

段，能及时定位到相关入侵来源，同时启动应急预案，并配合信息管理部门做好取证工作;

（五）对信息网络系统的故障和性能进行监控，发现问题及时解决，并及时报告;

（六）负责对信息网络系统运行过程中发生的其他各类问题进行及时处理。

第二十九条 公共资源交易局（中心）工作人员和运行维护单位违反本办法有关规定的，依规处理；构成犯罪的，移送司法机关处理。

第三十条 法律、法规、规章对网络信息安全另有规定的，从其规定。

第三十一条 公共资源交易局（中心）应与系统运行维护服务单位签订保密协议。

第三十二条 公共资源交易局（中心）应加强安全意识，定期开展网络信息系统安全培训和教育，强化工作人员对信息网络安全的认识，引导工作人员遵守保密制度，同时不定期对运行维护服务单位及相关工作人员进行安全制度和技术知识考核。

第三十三条 本办法自发布之日起施行，有效期 5 年。