焦作市公共资源交易中心

焦作市公共资源交易中心
关于印发《焦作市公共资源交易平台网络安全防护制度汇编》的通知

中心各科室：

为确保中心电子交易平台安全性、稳定性，根据《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》等要求，现制定《焦作市公共资源交易中心网络安全防护制度汇编》，请认真执行。

附件：《焦作市公共资源交易平台网络安全防护制度汇编》

焦作市公共资源交易中心

2020年7月22日

明确了各项网络安全规定和措施

焦作市公共资源交易平台
网络安全防护制度汇编

1、网络安全管理办法
2、网站管理制度
3、网络机房管理制度
4、监控管理制度
5、密码、口令管理制度
6、网络设备管理制度
7、网站政务信息发布的管理规定
8、网络与系统安全维护管理制度
9、网络信息安全故障应急预案
10、技术服务外包、维护管理制度
11、人员离岗离职信息安全管理制度

网络安全管理办法

为确保焦作市公共资源交易中心网络系统的安全性，降低网络系统存在的安全风险，确保网络系统安全可靠地运行，特制订此办法。

维护管理：焦作浪潮云计算中心运维团队。

一、职责

负责对电子交易系统及网络设备、安全防护进行维护、监控等工作。

二、网络安全管理

（一）网络管理员应每年对网络进行漏洞扫描，并与系统管理员、安全管理员一起进行扫描结果的分析。如发现重大安全隐患，应立即上报。

（二）网络管理员应详细描述扫描的技术、范围、时间及可能的影响性，方可执行。

（三）对重要网段要进行重点保护，要使用防火墙等安全设备以及 VLAN 或其他访问控制方式与技术将重要网段与其它网段隔离开。

（四）网络结构要按照分层网络设计的原则来进行规划，合理清晰的层次划分和设计，可以保证网络系统骨干稳定可靠、接

入安全、便于扩充和管理、易于故障隔离和排除。

（五）网络管理员定期对网络进行性能分析，充分了解系统资源的运行情况及通信效率情况，出具网络运行报告。

（六）按照最小服务原则为每台基础网络设备进行安全配置

（七）网络连接管理过程中，需明确网络的外联种类，根据外联种类确定授权与批准程序，保证所有与外部系统的连接均得到授权和批准，并具备连接策略及对应的控制措施。

（八）一般情况禁止无线接入，特殊情况须经信息安全工作组批准方可接入。

（九）网络互连原则：

1. 与互联网的连接中，在互连点上的防火墙上应该进行 IP 地址转换，保护内部接口机或代理服务器真实的 IP 地址；

2. 互联网接入必须有防火墙等安全防范设备。

（十）办公网络中不同业务的网络之间互连原则：

1. 互连点上必须实施安全措施，如网络访问控制列表、安装防火墙等；

2. 网络之间互连点采取集中原则，并考虑安全冗余；

3. 网络互连点及安全设备必须纳入到网管体系的监控。

（十一）焦作市公共资源交易中心网站因系统维护或法定节假日等原因，原则上提前发布暂停交易服务通知。

三、用户和口令管理

（一）对网络设备及安全设备的登录帐号设置权限级别，授权要遵循最小授权原则。

（二）保证用户身份标志的唯一性，即不同的个人用户必须采用不同的用户名和口令登录，并且拥有不同的权限级别。不同用户的登录操作在设备日志文件上均有记录，便于追查问题。

（三）网络设备及安全设备的直接责任人拥有超级用户权限，其他管理员按照工作需求拥有相应的用户权限.网络管理员不得私开用户权限给其它人员。

（四）用户的口令尤其是超级用户的口令必须足够强壮难以被破译，这是保证设备安全性的基本条件，口令的设置应该满足密码标准。

四、配置文件管理

（一）网络设备及安全设备中的运行配置文件和启动配置文件应该保持一致。

（二）网络设备及安全设备的配置文件需要定期备份。

（三）网络设备及安全设备的拓扑结构、IP 地址等信息文档属于机密信息，应该在一定范围内予以保密。

（四）配置信息的修改要记录并存档。

（五）定期对网络设备及安全设备的配置信息是否符合当前网络状况进行检查和分析，并做详细记录。

五、日志管理

（一）网络设备及安全设备需存储日志信息。

（二）在日志文件中要求记录登录过该设备的用户名、时间和所作的命令操作等详细信息，为发现潜在攻击者的不良行为提供有力依据。

（三）定期查看所管设备的日志文件，发现异常情况要及时处理和报告上级主管，尽早消除网络安全隐患。

（四）定期对日志文件进行备份。日志文件保存时间应在3个月以上。

（五）对日志文件的访问要获得安全管理员的批准。

六、设备软件管理

对现有设备系统版本进行备份，并及时更新或升级网络设备及安全设备的软件版本。

七、设备登录管理

（一）网络设备及安全设备一般都具有允许远程登录的功能，应采取SSH等安全加密的接入方式实现远程登录。

（二）需限定可远程登录的主机的地址范围，拒绝潜在的攻击者，保证网络安全登录。

（三）对于关键设备，需采取双因子认证的方式实现安全登录。

中心网站管理制度

第一章 总 则

第一条 焦作市公共资源交易中心网站是我中心基于因特网的业务平台、是焦作市公共资源交易的对外信息窗口，同时也是中心对外的形象展示阵地。

第二条 为充分利用现有的网络基础设施，实现网络信息工作的规范化和制度化管理，保证中心网络的安全稳定运行，根据《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中华人民共和国计算机信息系统安全保护条例》和《中华人民共和国计算机信息网络国际联网安全保护管理办法》和其他有关法律、法规的规定，制定本管理制度。

第三条 网站信息工作以服务我市公共资源交易信息发布、业务协调开展、相关政策法规宣传以及公共资源交易业务研究为中心，实行统一领导、统筹规划、集中管理、分级负责的原则。

第四条 本制度适用于所有接入中心网络的科室和人员。

第二章 组 织 机 构

第五条 成立以中心主任为组长，各科室负责人为成员的领导小组负责组织、协调网站的管理工作。

第六条 信息科室中心网站的具体管理部门，负责中心网站

的综合管理、组织协调、网络安全、技术服务咨询、门户网站及业务办公平台的建设和维护等工作。

各科室有配合维护网站安全的义务。

第七条　网站日常维护和管理、网络设备和计算机硬件系统维护，由信息科网站管理员具体负责。网站内容上传、信息发布由信息科信息发布员负责。

第三章　信息发布管理

第八条　网站信息发布、转载新闻应当依据国家有关规定执行。不得发布和转载含有危害国家安全和社会稳定的不良信息，不得宣扬暴力、色情等内容，不得制作、复制和传播各类不健康信息。

第九条　网站发布信息的版块设置、字体、字号、颜色等具体规定详见附表《网站栏目信息发布分类》。

第十条　招标公告、中标结果公示等业务信息，按照各业务科室业务流程和审批程序发布。

第十一条　信息发布人员不得擅自在网站上发布信息，所有信息必须经审核同意后才能发布。

信息发布严格按照以下流程管理:

起草人拟文或收集---科室负责人审核---信息员发布

信息科信息发布员发布未经上述流程的信息，无论是否造成影响，均要承担全部责任。所有发布的信息，其内容由信息来源

科室负责，应标明拟发布栏目、版块。

信息发布员信息发布密码应严格保密，不得向其他人提供。

第十二条　各科室至少确定1名信息员，负责本科室信息的采集、整理和上报。每周每科室至少报送1篇工作信息。

上报信息情况作为科室考核依据。

第十三条　鼓励中心全体人员积极收集或撰写相关信息丰富网站内容。

第十四条　任何科室和个人不得利用中心网络制作、复制、查阅和传播下列信息：

（一）煽动抗拒、破坏宪法和法律、行政法规实施的言论；

（二）煽动颠覆国家政权、推翻社会主义制度的言论；

（三）煽动分裂国家、破坏国家统一的言论；

（四）煽动民族仇恨、民族歧视，破坏民族团结的言论；

（五）捏造或者歪曲事实，散布谣言，扰乱社会秩序；

（六）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪；

（七）公然侮辱他人或者捏造事实诽谤他人；

（八）损害中心形象和中心利益的言行；

（九）其他违反宪法、法律、行政法规的言行。

第四章　网站安全管理

第十五条　信息科负责按规定向公安部门、信息管理部门进

行网站备案;

第十六条　严禁使用来历不明或可能引发病毒传染的软件，不得使用黑客软件;

第十七条　严禁将外来计算机存储介质(软盘、光盘、优盘等)未经杀毒就在计算机上使用;

第十八条　网站管理员在工作时间内必须监视网站信息，防止有害信息的传播，发现有害信息应及时处理，发现恶意攻击行为，及时向信息科负责人汇报。紧急情况下应采取封锁端口、停止服务或关闭服务器等措施。

第十九条　任何科室和个人不得从事下列危害计算机信息网络安全的活动:

（一）未经允许，对计算机信息网络功能进行删除、修改或者增加的;

（二）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或增加的;

（三）未经允许，私自修改 IP 地址的;

（四）故意制作、传播计算机病毒等破坏性程序的;

（五）以端口扫描方式，破坏网络正常运行的;

（六）其他危害计算机信息网络安全的。

第五章　附　　则

第二十条　在网站运行管理与维护工作中，凡因人为造成网

站中断、信息传递延误、泄密、病毒感染和设备器材损坏等情节的，按其情节给予责任追究；

第二十一条　本制度对本中心全体人员以及以任何方式登录本网站或直接、间接使用本网站资料者，具有普遍约束力；

第二十二条　本制度自发布之日起实施。

附表

网站栏目信息发布分类

一级栏目	二级栏目	发布信息类型	信息来源	更新时限	版面要求
1. 政务公开		中心简介、职能、机构设置	综合科	实时更新	宋体4号黑色字体行间距固定值
2. 专题活动		中心重大专项活动报道、相关的实施方案、报道中心工作部署、工作动态即时报道	综合科、信息科	实时更新	
3. 中心动态	3.1 专题信息	中心的重要活动，工作开展情况、对外发文。	综合科、信息科	实时更新	

	3.2 中心简报	发布每期工作简报、工作信息	综合科、信息科		22磅
	3.3 图片新闻	中心重大活动、事项的照片	综合科、信息科		
	3.4 行业信息	四个交易行业的业界新闻、新政、新观点。建议发布时在标题首以中括号方式注明信息的行业类型：“[政府采购]”。	中国政府采购网、政府采购信息网、中央政府采购网、中国国土资源部网、中国土地市场网、国土资源报电	每天更新发布4篇	

			子版、中国产权交易所、北京产权交易所、江西产权交易所、住房建设部网站、中国建设工程招标网、中国招投标网		
4.重要通知		1、发布中心及有关监管部门的重要通知	综合科	实时更新	
		2、与中心有关的资格考试通知	业务相关科室		
5.交易信息		发布四个交易科室的公告、公示信息	各业务科室	审核无	宋体4

	5.1 建设工程	下设“招标公告”、“拦标、资格预审公示”、“中标公示”三个三级栏目，分别发布对应的公告、公示		误即时发布	号黑色字体行间距固定值22磅
	5.2 政府采购	下设“采购公告”、“变更公告”、“结果公告”三个三级栏目，分别发布对应的公告。			
	5.3 产权交易	下设“转让公告”、“成交公示”两个三级栏目，分别发布对应的公告			
	5.4 国土交易	下设“出让公告”、“结果公示”两个三级栏目，分别发布对应的公告			

6.办事指南	6.1服务指南	分别发布四个交易科室《进场项目交易需提交材料告知单》、四个业务科室服务手册	各业务科室	审核无误即时发布	
	6.2业务流程	分别发布四个交易科室《业务流程表》			
	6.3操作规程	分别发布四个交易科室《进场项目交易操作规程》			
7.政策法规		与中心工作有关的各项政策法规	各业务科室、行业网站，以及相应的主管部门网站	实时更新	宋体4号黑
	7.1国家级	按照国家级、省级、市级三个级别，分别在对应的栏目发布与中心			

	7.2 省级 7.3 市级	工作有关的各项政策法规			色字体行间距固定值22磅
8.理论研究		与中心工作相关的国内先进的理论探讨、调研文献或中心内部的研究性文章	中国政府采购网、政府采购信息网、中央政府采购网、中国国土资源部网、中国土地市场网、国土资源报电子版、中国产权交易所、北京产权交	每天更新发布4篇	

			易所、江西产权交易所、住房建设部网站、中国建设工程招标网、中国招投标网		
9.资料下载		中心业务表格、文件、资料	各业务科室	实时更新	宋体4号黑色字体行间距固
	9.1表格下载	四个交易科室进场项目办理需提交的表格、材料等资料下载			
	9.2文档下载				

10. 中心文化园地		中心文体活动、培训素材、学习成果展示	人民网、河南报业网、焦作市人民政府网站、焦作日报网		定值22磅
11. 图片展示		滚动展示有关工作、活动、会议、场所等图片	综合科、信息科	实时更新	

网络机房管理制度

一、管理员值班制度

（一）管理员应当具有认真负责的工作态度和科学、细致周到的工作作风。按时上、下班，坚守岗位，确保网络运行正常。

（二）模范遵守中心网络管理制度。检查各项规章执行情况，一旦发现用户违章使用网络，立即上报并予以纠正。

（三）值班时，要做好检查，并作如下记录:

1. 内外环境情况，天气状况，室内温度和湿度。

2. 供电系统是否正常，是否中断过。

3. 网络和服务器系统的运行情况，是否发生故障，如何排除和解决的。

4. 何人使用过何种设备，以及设备使用前后工作状况。

5. 进入机房的其他人数量和活动情况。

6. 对于用户的求助和投诉、事件内容、性质和处理结果。

（四）认真监测网站运行和发布的信息是否正常，如发现病毒或受到黑客攻击，应立即采取恢复和补救措施，并向主管部门汇报。

（五）未经允许和合法程序，不能擅自删改网站主页内容，不得擅自删改或修改网络中各种用户名及密码。

（六）认真执行安全消防保卫制度和网络中心安全消防制度。要有安全防范意识。值班人员不能擅离岗位；早进入、晚离开时要检查设备情况；离开时察看灯、门、窗、锁是否关闭好。

二、安全消防管理制度

（一）根据中心在安全消防工作中贯彻“谁主管，谁负责”的原则，网络机房安全消防工作具体由机房管理员全权负责。

（二）机房内应按规定配备灭火器，并定期更换。

（三）机房内严禁吸烟和使用电炉，不得随意用水。在夏季空调开放期间，应经常检查空调冷凝水管和窗户，以防止水流入机房。

（四）机房内不得堆放易燃物品，如纸箱和废纸等。

（五）机房内的电源和插座为机房设备专用，非机房设备不得使用机房电源。

（六）机房内严禁存放任何食品，要经常检查有无老鼠，一旦发现，应立即采取措施。

（七）机房内一旦发生火情，应立即采取措施灭火，同时报警。

（八）没有特殊情况并得到批准，机房内不准外人随意出入。

（九）各门钥匙由指定的专人保管，不能随意转借，丢

失要声明，出入请随手关门。

（十）安全消防关系网络机房人员的安全，必须严格遵守。对违反制度造成后果的要严加追查，予以处理。对于严格管理避免重大事故的，予以表扬和物资鼓励。

三、环境卫生管理制度

（一）机房内部卫生应每天进行清理，每周彻底清理一次。

（二）机房外室每周二、五各清理一次，网络中心办公室每周彻底做一次卫生。

（三）机房应配备专用工作服和拖鞋，并经常清洗。

（四）非网络中心人员，谢绝进入机房。

（五）无论是机房人员还是其他经允许进入机房的人员，必须更换专用拖鞋或使用鞋套。

（六）每周对服务器等设备进行内部清洗一次，每月彻底除尘一次。

（七）每周检查一次门、窗的密封性，发现问题及时解决。

（八）每年对环境卫生工作进行一次年终检查评估，找出问题，制定解决措施。

四、设备定期维护制度

季度维护

（一）彻底清扫机房内部和周围环境卫生。

（二）为机房内所有设备除尘。

（三）检查清洗空调系统。

（四）排除设备在使用中出现的故障和缺陷。

（五）检查、测试机房电源工作情况，并做好维护记录。

（六）UPS 系统的充放电操作。

（七）其他检查。

换季维护

（一）完成季度维护的内容。

（二）检查空调，保证无故障，检查排泄水管道。

（三）检查各种电缆和导线的固定、走向及通电后温升情况是否符合要求。

（四）检查各种安全设备、防火设备及报警设备。

（五）夏季来临之前，检查机房防水、防雷电措施情况。

（六）其他检查。

针对重大任务的设备维护

（一）完成季度维护内容。

（二）根据任务要求，重点检查相关设备的工作情况。

（三）需临时增设一些设备，事先安装并调试。

（四）其他有关设备维护。

定期大中修维护

（一）连续使用两年左右时间，根据实际使用情况对机房设备和机房进行中修。

（二）连续使用五年左右时间，对机房及其设备进行大修。

五、保密制度

（一）机房所有工作人员应遵守网络管理制度中的保密规定，勇于同违反规定的现象作斗争，堵塞各种不安全漏洞。

（二）机房负责人应承担机房安全和保密工作，检查保密措施的落实执行情况。

（三）上机资料及打印的各种报表必须在离开时带走，废弃的涉密资料及报表应统一销毁，不得乱丢乱放。

（四）处理涉密数据的计算机及软件程序要采取保密措施。

（五）涉密信息只能在加密通道传输，不加密不得上机。

（六）无线电通信系统必须按规定范围专用，不得随意进行其他工作，严禁用无线电通信系统交谈有关涉密内容。

（七）涉密计算机必须有严格的身份认证措施，严禁未授权者使用涉密计算机设备。

监控管理制度

为了加强监控系统操作室的管理，确保监控系统的正常使用和安全运作，充分发挥其作用，制定本制度：

一、监控室由交易监督科负责管理，信息科设置监控管理员负责监控系统的安全与维护。

二、监控管理员应具有高度的工作责任心，严格按照规定时间上下班，认真负责监控任务，不准随意脱离岗位。

三、监控管理员应熟练操作监控设施，严格操作流程，对交易过程做到全程监控，重点项目应按要求刻录光盘，贴好标签及时存档。每天对监控的情况进行登记。

四、监控录像、光盘资料要严格保密，相关监督执法部门需要调阅时，应按规定办理审批手续。未经批准，不得外借、删除、更改。

五、熟悉监控设备的操作原理，掌握操作技术，设备有故障及时进行维修，不得擅自拆卸、挪用或停用，保证设备正常运行。

六、无关人员未经许可不准进入监控室，不准在监控室聊天、会友。外来参观人员须有相关部门负责人带领。

七、监控室内严禁吸烟，保持室内的环境卫生。

八、监控管理员每日要检查监控服务器，维护好监控服务器，保证其正常工作。

九、监控管理员每个周末在确定没有业务情况下，都要巡查服务器，做好定期维护服务器工作。

十、监控室要做好下班检查所有电脑是否关闭，假日放假要关闭所有电源，检查窗户、门锁、光盘储存柜是否锁好。

密码、口令管理制度

为确保网络安全运行，保护数据安全，特制定此管理制度。

一、网络服务器密码口令的管理

（一）服务器的口令和密码，由部门负责人和网络管理员商议确定，必须两人同时在场设定。

（二）服务器的口令长度不得少于16位，且由数字、字母和特殊字符三种组合组成。

（三）密码及口令定期、不定期更换（视网络具体情况而定）。

（四）如发现密码及口令有泄密迹象，网络管理员要立刻报告部门负责人，由部门负责人指示后另行更换密码和口令。

二、办公系统工作人员密码及口令的管理

（一）办公系统密码由系统管理员设置，工作人员应在首次登陆时更改设置，长度不得少于6位。具有公开信息发布权限的工作人，密码不得少于12位，且至少包含数字、字母及特殊字符中2种。

（二）当忘记密码、口令时要及时向系统管理员申请重置密码。

（三）工作人员应定期更换密码及口令。

网络设备管理制度

为了加强招投标中心内部计算机网络及设备的管理，保障各项工作正常开展，特制定本制度。

第一条　中心工作人员在使用计算机网络及设备时必须遵守国家有关法律、法规的规定。

第二条　中心信息科负责计算机网络及相关设备的维护和管理。

第三条　网络管理人员应定期对计算机网络、服务器、电子屏等重要设施进行维护，发现问题及时处理。

第四条　机房等区域无关人员未经同意不得随意进入，专家管理、财务、监控等专用电脑和设备其他人员未经授权不得擅自使用。

第五条　中心工作人员在使用计算机及相关设备时应严格按照规程，合理操作，确保设备正常工作。

第六条　中心工作人员应妥善保管好自己使用的设备，不使用时及时关闭和切断电源，并且严禁在设备旁放置易燃、易爆、腐蚀性和强磁性等危险物品。

第七条　中心工作人员应注重网络及系统安全，专用电脑应与因特网物理隔离，密码等重要信息不得向无关人员泄露。

第八条　中心工作人员严禁私自乱设或修改统一分配的计

算机网络 IP 地址。

第九条　中心工作人员不得随意在中心网站、电子屏发布信息。

第十条　中心工作人员不得使用中心网络和设备制作、复制、发布、传播违法和不文明信息。

第十一条　中心工作人员不得使用来历不明的软盘、光盘等移动存储设备、不得随意安装可能影响计算机网络和设备正常使用的软件。

第十二条　中心工作人员不得在工作时间玩电脑游戏，不得利用计算机网络做与工作、学习无关的事情。

第十三条　中心工作人员和中心各科室应做好计算机日常业务数据和文档资料的整理，并及时做好备份工作。

第十四条　计算机应统一安装正版杀毒软件，并由使用人员定期升级和杀毒，以免计算机等设备中病毒造成网络瘫痪和系统崩溃。

第十五条　违反本制度而造成后果的将视情节轻重追究相关人员的责任。

第十六条　各单位派驻中心窗口工作人员参照此制度有关条款执行。

第十七条　本制度自发布之日起施行。

网站政务信息发布的管理规定

一、网站信息发布管理制度

为了促进信息资源的交流与共享，保障网站信息发布的及时、真实、安全、可靠、合法，根据《中华人民共和国计算机信息网络国际互联网管理暂行规定》、《中华人民共和国计算机信息系统安全保护条例》，按照统一领导、集中管理、分级负责的原则，制定本管理制度。

（一）凡在焦作市公共资源交易中心网站（以下简称中心网站）上生成及传递以文字、数据、表格、图片为载体等各种信息，必须遵守本管理制度。

（二）凡在中心网站上发布的信息应当属于可供社会公众查询的公开信息，应符合国家有关安全保密规定，凡涉及党和国家的机密以及不能公开的商业秘密和个人隐私一律不得在网上发布。

（三）有关涉密信息范围、密级按照国家保密局有关规定执行。

（四）凡有下列情形的信息不得发布：

1. 反对宪法所确定的基本原则的；

2. 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

3.损害国家荣誉和利益的;

4.煽动民族仇恨、民族歧视、破坏民族团结的;

5.破坏国家宗教政策，宣扬邪教和封建迷信的;

6.散步谣言，扰乱社会秩序，破坏社会稳定的;

7.散步淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的;

8.侮辱或诽谤他人，侵害他人合法权益的;

9.侵犯他人知识产权的;

10.法律、法规禁止的其他内容。

（五）建立网站信息提供审核制度。各科室提供信息实行领导负责制，对提供信息的真实性、可靠性、时效性、保密性、合法性负责。

（六）信息科指定专门的网站管理员信息发布，其他人员如需要发布信息，应先与管理员取得联系。各部门应负责信息的收集、整理、编辑和网上报送工作。

（七）网站信息实行审批发布制度。中心信息科为上网信息审核的主管部门。

（八）完善网站的信息发布程序。信息审批发布的程序为:各科室提供信息需经本部门负责人签字，交由信息科进行审核。审核程序完成后，上网发布。

（九）上网信息由资料来源部门按规范化要求提供。文字材料以WORD文档格式提供，表格以EXCEL格式提供，图片以JPG

等数据文件格式提供。

（十）信息发布人应建立信息发布日志，网站管理员负责记录每次信息发布的时间，做好信息发布审批表及原始资料的归档工作。

二、网站信息发布审核制度

中心网站是对外宣传的窗口和形象，为建立规范的信息采集、审核、发布、更新机制，做好网站对外信息发布，现对网站信息发布审核做以下规定：

（一）设立信息发布管理小组，用中心领导和相关管理人员组成，负责对信息的审核与管理。

（二）管理小组对上网内容要严格审核、管理，以确保网上信息的合法性、真实性、准确性、及时性，坚决禁止不健康的信息上网。

（三）各科室对所提供的信息内容负责。通过内网将电子版传信息科进行发布。

（四）各科室的信息经科室负责人校审并签字后交由信息发布管理小组审核，通过审核后方可提交网站上网发布。

（五）网站发布的各类信息必须严格遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》、《互联网信息服务管理办法》等有关国家政策、法规规定。

（六）加强对网站信息的更新。根据网站栏目内容设置，网站信息分随时更新与定期更新两大类，由各个栏目相关科室负责

采集、整理，信息科负责审核并发布。做到当天的重大活动、重要会议当天撰写稿件，当天发布，随时更新做到当天更新，定期更新按时间要求及时更新。

（七）加强信息发布审核制度。各科室负责的栏目内容，由各科室人员负责采集、整理后报科室负责人初审，初审合格后，报分管领导审核签发后方可对外发布。各科室负责的报送内容，本着“谁报送、谁负责，谁承诺、谁办理”的原则。

（八）信息科对网站发布的信息资料进行登记并汇总，每月对各科室报送信息量进行通报。

三、网站信息传送制度

为建立规范的信息发布、更新机制，搞好网站对外信息发布工作，特制定本制度如下:

（一）会议类、中心活动类信息由综合科负责采集、整理、审核并传送信息科管理员处，当天发布。

（二）交易活动的公告、公示等由业务科室项目负责人按中心规定时间整理、传送。电子版通过内网传送信息科管理员发布。

（三）各业务科室负责及时对行业动态、行业法律、法规的更新信息进行收集，电子版通过内网传送信息科管理员发布。

（四）各科室每周五向信息科传送一篇信息。信息科管理员负责登记汇总，每月对各科室信息发布情况进行通报。

（五）各科室负责报送信息超过规定的时间要求，一次警告，两次提出通报批评，三次取消文明科室评先资格。

网络与系统安全维护管理制度

一、硬件的安全与维护

（一）各科室使用的计算机硬件及配套设备统一由中心信息科负责管理。

（二）当设备出现故障时，须报告中心信息科统一处理，其他人不得随意卸载、处理。

（三）加强对计算机硬件设备、维修工具的管理，建立健全有关资产台账。

（四）硬件维护人员必须按操作规程操作、及时排除设备故障，保证设备安全高效运行。

（五）设备老化、性能落后、故障严重、不能应用于实际工作的计算机及附属设备，须经中心信息科进行技术鉴定并出具相应手续后，报有关部门批准，按固定资产报废程序处理。

（六）禁止已连接局域网的设备同时访问因特网，如相关部门必须访问因特网时，应将内网系统如财务系统等与因特网从物理上断开。

二、软件的使用与维护

（一）负责软件使用的操作人员应按照软件操作规程进行使用，在操作中出现的问题，要及时向中心信息科报告。

（二）软件的安装、系统维护和管理应由中心信息科负责，

其他人不得在单位机器上私自安装其他与工作、学习无关的软件。

（三）不经检测病毒的存储设备和软件不允许在机器上使用；机器感染病毒后在病毒未消除前，应停止机器上的一切软件的使用，以免其他软件遭到感染和破坏。

（四）操作人员必须严格执行密码管理制度，不得进行超越权限的操作，不得泄密。

网络信息安全故障应急预案

为建立健全我中心网络信息安全应急机制，科学应对信息安全与网络故障突发事件，提高处理突发信息安全与网络故障的能力，有效预防 及时控制和最大限度地消除信息安全与网络故障等各类突发事件的危害和影响，特制订本应急预案。

第一条　本预案坚持“统一领导、协调配合、明确责任、依法规范、条块结合、整合资源、防范为主、加强监控”的原则。

第二条　信息安全包括因设备故障造成的数据损失、因非法入侵或木马病毒软件造成的数据泄露等。网络故障包括因设备、线路等原因造成的网络不通等。

第三条　通信网络故障应急预案

（一）发生通信网络故障后，计算机操作员应及时将信息告知网络与信息安全领导小组。

（二）网络与信息安全领导小组及时查清通信网络故障位置，或告知相关通信网络运营商，请求协助查清原因，同时，隔离故障区域，切断故障区与服务器的网络联接。

（三）系统管理员会同电信技术人员或公司技术人员检测故障区域，逐步恢复故障区与服务器的网络联接，恢复通信网络，保证正常运转。

（四）相关责任人负责写出故障分析报告，上报网络与信息

安全领导小组备查。

第四条　不良信息和网络病毒事件应急预案

（一）当发现不良信息或网络病毒时，网络管理员应立即断开网线，终止不良信息或网络病毒传播，并告知网络与信息安全领导小组。

（二）接到报告后，网络与信息安全领导小组应立即通告局域网内所有计算机用户防病毒方法，隔离网络，指导各计算机操作人员进行杀毒处理，直至网络处于安全状态。

（三）对不良信息要进一步追查来源，对未经相关领导同意，擅自发布信息，造成不良影响且触犯法律者，移交执法部门追究法律责任。

（四）情况严重时，应立即向网络与信息安全应急领导小组报告，请求支援，作好应对措施。

第五条　计算机软件系统故障应急预案

（一）发生计算机软件系统故障后，计算机操作人员立即保存数据，并停止该计算机使用应用。

（二）由部门负责人将情况报告网络与信息安全领导小组，不得擅自进行处理。

（三）网络与信息安全领导小组迅速派出技术人员进行处理，必要情况下，应对硬盘进行备份。

（四）在保持原始数据安全的情况下，对计算机系统进行修复；修复系统成功，则检查数据丢失情况，利用备份数据恢复；

若修复失败，立即联系相关厂商请求技术支援。

第六条　黑客攻击事件应急预案

（一）当发现网络被非法入侵、网页内容被篡改，应用服务器上的数据被非法拷贝、修改、删除，或通过入侵检测系统发现有黑客正在进行攻击时，使用者或管理者应断开网络，并立即报告网络与信息安全领导小组。

（二）接到报告后，网络与信息安全领导小组应立即关闭网络，封锁或删除被攻破的登录账号，阻断可疑用户进入网络的通道。

（三）及时清理系统、恢复数据、程序，尽力将系统和网络恢复正常；情况严重时，应立即向网络信息安全应急领导小组报告，请求支援，作好应对措施。

第七条　机房设备硬件故障应急预案

（一）发生机房设备硬件故障后，网络与信息安全领导小组应立即确定故障设备及故障原因，并进行先期处置。

（二）若故障设备在短时间内无法修复，应启动备份设备，保持系统正常运行；将故障设备脱离网络，进行故障排除工作。

（三）故障排除后，在网络空闲时期，替换备用设备；若故障仍然存在，立即联系相关厂商与信息中心，并认真填写设备故障报告单备查。

第八条　应急处置

发生信息网络突发事件后，相关人员应在5分钟内向网络与

信息安全领导小组报告，应急小组组织人员开展先期处置。发生重大事件应向网络与信息安全应急领导小组报告。

第九条　善后处置

应急处置工作结束后，网络与信息安全领导小组组织有关人员及邀请信息中心技术专家组成事件调查组，对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估，总结经验教训，整改存在隐患组织，恢复正常工作秩序。

第十条　应急通讯保障

网络与信息安全领导小组全体人员保证全天 24 小时通讯畅通。

第十一条　装备保障

应预留一定数量的信息网络硬件与软件设备，指定专人保管和维护。

第十二条　数据保障

重要信息系统均应建立备份系统，保证重要数据在受到破坏后可紧急恢复。

第十三条　队伍保障

选择两个团队作为我中心的应急支援队伍：一是负责交易系统开发，运维的江苏国泰新点软件有限公司派驻两名技术人员做现场服务；二是与市政府信息中心、市联通公司作为突发信息网络突发事件的应急支援单位，提供技术支持与服务。

第十四条　宣传、培训和演习

网络与信息安全领导小组每年至少开展一次信息网络安全教育，提高信息安全防范意识和能力。

第十五条　培训

网络与信息安全领导小组每年至少开展一次信息网络安全培训，提高信息网络事件的应急能力。

第十六条　预案演习

网络与信息安全领导小组每年至少安排一次演练，通过演练发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处理能力。

技术服务外包、维护管理制度

为加强和规范单位业务的外包管理，规范和完善业务外包、降低成本、提高效率、保证单位信息化健康平稳的建设，特制定本制度。

业务外包是指：单位以合同或协议形式，与外部其他单位或个人签订契约，将单位负责的业务（工程、劳务、专业要求等）外包给专业、高效的服务提供商（简称承包商）的经营形式。

外包管理制度如下：

一、业务项目由单位主管部门提出申请，中心主任批准后，方可对外发包。

二、业务外包应考虑以下三个方面的因素：1.此项业务是否是利用单位没有的设备、专业人员及专门技术。2.此项业务外包可以降低成本。3.此项业务外包能够产生比自己运作更多的利益等。

三、针对外包商的管理，应本着有序竞争、择优选用，合约管理、制度规范，程序清晰、职责明确，考核有据、使用高效的原则。

四、按照“谁主管，谁负责”的原则，负责明确外包工作的项目和范围，外包工作的组织协调和检查指导，保证单位业务各项安全、质量方面的标准、规程和制度得到严格的执行。

五、单位是业务外包工作的服务主体，要对现场作业进行现场跟踪指导。同时负责外包工作现场作业环境安全措施的落实，严格监督外包业务承包商落实施工安全、技术、组织措施和施工方案及标准化作业指导书。

六、单位进行外包项目招标或竞争性谈判，确认外包承包商。最后单位与外包承包商签订外包合同。

七、单位对外包承包商建立考核制度，全面管理业务外包的工作中承包商的外包行为规范，有效监管承包商的履约情况。并定期派专人检查和评估外包项目实施进展情况。

八、外包承包商应严格执行合同或协议要求，规范工作内容，履行合同约定，服从业务管理部门的指挥调度，合理安排，确保外包业务工作能保质保量的完成。

九、外包技术服务、维护人员上门服务时，需携带单位介绍信及本人的身份证明，经网络管理员审核、信息科负责人批准后方可进入现场。

十、系统提供商自行进行的版本升级等内容，需将详细内容报信息科备案，由信息科请中心领导批准后方可操作。网络管理员需对现场及远程技术服务、维护记录存档。

人员离岗离职信息安全管理制度

为规范本单位计算机信息安全工作，保证内部计算机与网络信息安全，适应信息安全等方面的需要，防止计算机网络失密泄密事件发生，中心信息科特制定本规定：

第一条　本单位工作人员离岗离职时，有关部门应即时取消其计算机涉密信息系统访问授权。工作人员离岗离职之后，仍对其在任职期间接触、知悉的属于网络设备与各业务系统服务器机密，凡由本单位承诺负有保密义务的秘密信息，其必须承担如同任职期间一样的保密义务和不得擅自使用的义务，直至该秘密信息成为公开信息，而无论离岗离职人员因何种原因离岗离职。

第二条　本单位工作人员离岗离职时，应该把下列资料全部交给下一任工作人员，包括：

（一）网络管理的所有服务器，交换机，路由器的账号和密码口令。

（二）相关设备携带的说明书等设备与服务器系统资料。

（三）有关网络建设与信息化建设的各种合同，上级部门的各种批文、条例等文字材料，各种门钥匙与文件柜等钥匙要及时上交。

第三条　离岗离职人员应在离岗离职时，或者向本单位提出离职请求时，返还全部属于本单位的财物，应将工作时使用的电

脑、笔记本等贵重财物与设备交接给本科室领导，不得在离岗离职后带走单位的财物。