**技术安全保障措施**

 网络与信息的安全不仅关系到公司业务的开展，还将影响到国家的安全、社会的稳定。公司将认真开展网络与信息安全工作，通过检查进一步明确安全责任，建立健全的管理制度，落实技术防范措施，保证必要的经费和条件，对有毒有害的信息进行过滤、对用户信息进行保密，确保网络与信息安全。

**a、网站安全保障措施**

1、网站服务器和其他计算机之间设置防火墙,做好安全策略,拒绝外来的恶意攻击，保障网站正常运行。

2、在网站的服务器及工作站上均安装了相应的防病毒软件，对计算机病毒、有害电子邮件有整套的防范措施，防止有害信息对网站系统的干扰和破坏。

3、做好访问日志的留存。网站具有保存六个月以上的系统运行日志和用户使用日志记录功能，内容包括IP地址及使用情况，主页维护者、对应的IP地址情况等。

4、交互式栏目具备有IP地址、身份登记和识别确认功能，对非法贴子或留言能做到及时删除并进行重要信息向相关部门汇报。

5、网站信息服务系统建立多机备份机制，一旦主系统遇到故障或受到攻击导致不能正常运行，可以在最短的时间内替换主系统提供服务。

6、关闭网站系统中暂不使用的服务功能,及相关端口,并及时用补丁修复系统漏洞,定期查杀病毒。

7、服务器平时处于锁定状态,并保管好登录密码;后台管理界面设置超级用户名及密码,并绑定IP,以防他人登入。

8、网站提供集中式权限管理，针对不同的应用系统、终端、操作人员，由网站系统管理员设置共享数据库信息的访问权限，并设置相应的密码及口令。不同的操作人员设定不同的用户名，且定期更换，严禁操作人员泄漏自己的口令。对操作人员的权限严格按照岗位职责设定，并由网站系统管理员定期检查操作人员权限。

9、机房按照电信机房标准建设，内有必备的独立UPS不间断电源，能定期进行电力、防火、防潮、防磁和防鼠检查。

**b、信息安全保密管理制度**

1、严格按照“谁主管、谁负责”、“谁主办、谁负责”的原则，落实责任制，明确责任人和职责，细化工作措施和流程，建立完善管理制度和实施办法，确保使用网络和提供信息服务的安全。

2、网站信息内容更新全部由网站工作人员完成或管理,工作人员素质高、专业水平好,有强烈的责任心和责任感。网站相关信息发布之前有一定的审核程序。工作人员采集信息将严格遵守国家的有关法律、法规和相关规定。

3、遵守对网站服务信息监视，保存、清除和备份的制度。开展对网络有害信息的清理整治工作，对违法犯罪案件，报告并协助公安机关查处。

4、所有信息都及时做备份。按照国家有关规定，网站将保存6个月内系统运行日志和用户使用日志记录。

5、制定并遵守安全教育和培训制度。加大宣传教育力度，增强用户网络安全意识，自觉遵守互联网管理有关法律、法规，不泄密、不制作和传播有害信息，不链接有害信息或网页。

**c、用户信息安全管理制度**

1、尊重并保护用户的个人隐私，在与用户签署的隐私政策和网站服务条款以及其他公布的准则规定的情况下，未经用户授权不得公布与用户个人身份有关的资料，除非有法律或程序要求。

2、严格遵守网站用户帐号使用登记和操作权限管理制度，对用户信息专人管理，严格保密，未经允许不得向他人泄露。

公司定期对相关人员进行网络信息安全培训并进行考核，使相关人员能够充分认识到网络安全的重要性，严格遵守相应规章制度。

公司严格执行本规章制度，并形成规范化管理，建立健全信息网络安全小组。安全小组由单位领导负责，网络技术、客户服务等部门参加，并确定至少一名安全负责人作为突发事件处理的联系人。