信息网络安全责任承诺书

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》、《计算机信息网络国际联网安全保护管理规定》、《互联网安全保护技术措施规定》、《互联网信息服务管理办法》、《互联网域名管理办法》、《非经营性互联网信息服务备案管理办法》、《工业和信息化部关于进一步落实网站备案信息真实性核验工作方案》等法律法规，本单位做为网络运营者承诺承担以下安全主体责任：

1. 在国内注册和使用的域名，必须履行域名实名认证。
2. 经营性网站，应自行在当地通信管理部门办理经营性ICP许可证；非经营性网站应自行办理非经营性ICP备案手续；如涉及聊天室、BBS、新闻、游戏等栏目，除了办理一般的许可或备案手续外，也需根据相关法规政策要求获得批准或进行登记备案手续。并承诺提交的所有备案信息真实有效，当备案信息发生变化时请及时到备案系统中提交更新信息。并按照工信部要求在网站首页底部标注备案号并超链接到www.miibeian.gov.cn。
3. 获取工信部备案号后联入互联网的，应在30日内向属地公安网安部门备案登记，并按公安机关要求在网站首页底部标注公安备案号并超链接到www.beian.gov.cn。
4. 不通过互联网制作,复制,查阅和传播九不准法律法规禁止的内容。
5. 在公安机关的监督指导下，建立、完善计算机网络安全保护技术措施，指定专职部门开展网站安全保护工作，建立健全网络安全管理制度，制定网络安全事件应急预案，配备专职计算机安全员，协助接入服务商处置网络信息安全事故以及协助公安机关查处各类计算机违法犯罪案件。
6. 落实以下网络安全保护管理制度：
7. 网络安全等级保护制度；
8. 基本安全管理制度，包括主机安全管理、网络安全管理、系统运行维护管理、系统安全风险管理、资产和设备管理、数据及信息安全管理、用户管理、备份与恢复、密码管理等制度；
9. 网络人员岗位职责及管理制度；
10. 网络安全审计制度；
11. 网络信息收集、存储、备份、使用、清除管理制度；
12. 电子公告系统用户登记制度；
13. 信息发布审核、登记制度；
14. 网络安全事件应急预案；
15. 网络安全教育和培训制度；
16. 其他网络安全等级保护制度。
17. 健全完善以下信息网络安全保护技术措施：
18. 在计算机主机、网关和防火墙等网络边界设备上建立完备的日志审计记录。网络日志审计系统应使用经公安机关检测合格的产品，且审计系统必须保证日志记录的完整性，日志留存时间不少于6个月。日志审计重点考虑系统时间和操作系统日志，其技术指标主要包括：系统的启动时间、用户登录账号、登录时间、用户进行的操作、关机时间等。对每一次网络连接应记录连接的源IP地址、目的机器IP地址、连接的时间、使用的协议等信息。计算机主机登陆和访问日志记录功能，开启web网站日志记录功能，不仅限于URL、ID、注册IP、注册时间、最后的登录IP和时间、用户源IP、源端口号、上下线时间；
19. 具有安全审计或预警功能；
20. 有害信息封堵、过滤功能；
21. 开设邮件服务的，具有垃圾邮件清理功能；
22. 开设交互式信息栏目的，具有身份登记和识别确认功能；
23. 计算机病毒防护功能；
24. 网页被篡改、灌码的预警和防护技术；
25. 关键字过滤技术；
26. 互联网安全保护技术措施应当具有符合公共安全行业技术标准的联网接口；
27. 其他保护信息和系统网络安全的技术措施；
28. 切实加强本单位信息网络安全管理，积极履行安全保护职责，对发现的各类有害信息、网络安全事故以及其他违法行为，应在保留有关原始记录的同时，立即向公安机关网安部门报告，并依法停止传输。对不依法履行职责造成严重后果的，公安机关将依法严肃追究有关责任。

 网络运营者：（公章）

 单位负责人签名

 年 月 日