# 网站安全保障措施

第一条 为加强网站安全管理，确保本网站的整体安全，根据《中华人民共和国计算机系统安全保护条例》等有关规定，制定本措施。

第二条 网站的建设应坚持“统一规划、统一标准，资源共享，安全保密”的原则。

第三条 公司网站管理小组负责组织指导、协调网站的统筹规划，建设管理工作及指导、检查网站的安全工作。由系统研发部具体承办网站的建设、运行维护和日常管理。

第四条 应急响应制度。网站管理人员应当充分估计各种突发事件的可能性，做好应急响应方案的及时实施，将损失降到最低。

第五条 网站服务器和其他计算机之间设置防火墙,做好安全策略,拒绝黑客攻击,保障网站正常运行。

第六条 在网站的服务器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，防止病毒攻击。

第七条 网站定期检测制度。网站应及时对网站管理及服务器系统漏洞进行定期检测，并根据检测结果采取相应措施。及时对操作系统、数据库漏洞进行修补和升级，防止黑客入侵。

第八条 做好访问日志的留存。网站具有保存三个月以上的系统运行日志和用户使用记录的功能，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。

第九条 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。

第十条 网站服务器存放于联通IDC机房，内有必备的独立UPS不间断电源、高灵敏度的烟雾探测系统和消防系统，管理员能定期进行电力、防火、防潮、防潮、防鼠检查。

# 信息安全保密管理制度

第一条 为处理网站信息资源发布过程中涉及的办公秘密信息和业务秘密信息，

特制定本制度。

第二条 网站应建立规范的信息采集、审核和发布机制，实行网站编辑制度。

第三条 公司信息部负责指导全公司各部门网站信息员的保密技术培训，落实技

术防范措施。

第四条 凡需要发布上网的信息资源必须遵循“谁发布，谁负责；谁主管，谁管理”的原则。

第五条 各部门要有一名领导主管此项工作。要指定专人负责上网信息的保密检

查，落实好保密防范措施，定期对本部门网站信息员进行保密教育和管理。网站信息员负责向网站编辑报送本部门需要公开发布的信息。

第六条 拟对外公开的信息，必须经本部门分管负责人审查同意并上传的内容进

行登记建档后方可发布上网，重要信息还需经公司网站管理小组审核确认。

第七条 对互动性栏目要加强监管，需要有IP地址、身份登记和识别确认功能，对非法评价或留言能做到及时删除并向相关部门汇报，确保信息的健康和安全。

以下有害信息不得在网上发布：

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. 散布谣言，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、恐怖或教唆犯罪的；
8. 侮辱或者诽谤他人，侵害他人的合法权益的；
9. 含有法律、行政法规禁止的其他内容的。
10. 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，严禁操作人员泄露自己的密码和口令。最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。
11. 定期备份制度。网站应当对重要文件、数据、操作系统及应用系统做定期备份，以便应急恢复。

第十条　不得利用网站从事危害国家安全，泄露国家机密的活动。

第十一条　发生重大突发事件期间，公示网站管理小组及各部门领导要加强网络监控，及时、果断地处置网上突发事件，维护公司内部稳定。

# 用户信息安全管理制度

第一条 遵守《中华人民共和国计算机信息系统安全保护条例》及其他有关的国家法律、法规和规定。

第二条　制定和严格执行安全管理制度。

第三条　保存会员登录记录30天以上。

第四条　尊重并保护用户的个人隐私，除了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，会员登记的私人信息资料，网站不得向外界散发、告知；未经许可，任何单位、团体、个人不得查阅、拷贝、抄录私人信息资料内容。

第五条　会员不得传播违反国家法律的言论，对传播淫秽资料的，网站负责人和管理员有责任阻止。

第六条　切实落实各项制度，做好各项管理制度的工作。

第七条　会员不得在网站进行个人攻击和任何违法活动。

第八条　信息安全内部人员保密管理制度：

1. 内部人员不得对外泄露需要保密的信息。
2. 内部人员不得发布、传播国家法律禁止的内容。
3. 信息发布之前应该经过相关人员审核。
4. 对相关管理人员设定网站管理权限，不得越权管理网站信息。
5. 一旦发生网站信息安全事故，应立即报告相关方并及时进行协调处理。
6. 对有毒有害的信息进行过滤、用户信息进行保密设置。

第九条　登陆用户信息安全管理制度：

1. 对登陆用户信息阅读与发布按需要设置权限，不得擅自进入系统，篡改他人信息。
2. 对有害的信息进行过滤，对用户的信息进行有效管理并保证其信息的安全保密。
3. 建立信息编辑、审核、发布责任制及流程，信息发布之前必须经过相关人员审核。
4. 对用户在网站上的行为进行有效监控，保证内部信息安全。
5. 固定用户不得传播、发布国家法律禁止的内容。
6. 一旦发生信息安全事故，就积极采取有效措施，并保存记录按规定报告有关部门。