
信息安全管理制度

为维护公司信息安全，保证公司网络环境的稳定，特制定本制度。

第一条 信息安全是指通过各种计算机、网络（内部信息平台）和密码技术，保护信息在传输、交换和存储过程中的机密性、完整性和真实性。具体包括以下几个方面。

1、信息处理和传输系统的安全。系统管理员应对处理信息的系统进行详细的安全检查和定期维护，避免因系统崩溃和损坏而对系统内存储、处理和传输的信息造成破坏和损失。

2、信息内容的安全。侧重于保护信息的机密性、完整性和真实性。系统管理员应对所负责系统的安全性进行评测，采取技术措施对所发现的漏洞进行补救，防止窃取、冒充信息等。

3、信息传播安全。要加强对信息的审查，防止和控制非法、有害的信息通过本公司的信息网络（内部信息平台）系统传播，避免对公司利益、公共利益以及个人利益造成损害。

第二条 信息的内部管理

1、各部门在向网络（内部信息平台）系统提交信息前要作好查毒、杀毒工作，确保信息文件无毒上载；

2、根据情况，采取网络（内部信息平台）病毒监测、查毒、杀毒等技术措施，提高网络（内部信息平台）的整体搞病毒能力；

3、各信息应用部门对本部门所负责的信息必须作好备份；

4、各部门应对本部门的信息进行审查，网站各栏目信息的负责部门必须对发布信息制定审查制度，对信息来源的合法性，发布范围，信息栏目维护的负责人等作出明确的规定。信息发布后还要随时检查信息的完整性、合法性；如发现被删改，应及时向信息安全部门报告；

5、涉密文件不可放置个人计算机中，非涉密电子邮件的收发也要实行病毒查杀。

第四条 信息加密

-
- 1、涉及公司秘密的信息，其电子文档资料应当在涉密介质中加密单独存储；
 - 2、涉及公司和部门利益的敏感信息的电子文档资料应当在涉密介质中加密单独存储；

第五条 任何部门和个人不得从事以下活动：

- 1、利用信息网络系统制作、传播、复制有害信息；
- 2、入侵他人计算机；
- 3、未经允许使用他人在信息网络系统中未公开的信息；
- 4、未经授权对网络（内部信息平台）系统中存储、处理或传输的信息（包括系统文件和应用程序）进行增加、修改、复制和删除等；
- 5、未经授权查阅他人邮件；
- 6、盗用他人名义发送电子邮件；
- 7、故意干扰网络（内部信息平台）的畅通运行；
- 8、从事其他危害信息网络（内部信息平台）系统安全的活动。

第六条 本制度自发布之日起施行，凡与本制度有冲突的均以本制度为准。