信息系统安全管理制度

第一章 总则

第一条 为了保护有限公司计算机信息系统安全，规范信息系统管理，合理利用系统资源，推进公司信息化建设，促进计算机的应用和发展，保障公司信息系统的正常运行，充分发挥信息系统在企业管理中的作用，更好地为公司生产经营服务。依据相关监管机构的监管规定以及自律机构的自律指引，结合公司实际，制定本办法。

第二条 本制度所称的信息系统，包括计算机硬件、软件、打印机、电子邮件、办公应用系统、局域网和广域网的访问等，及按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

第三条 信息系统的安全保护，应当保障计算机及其相关的和配套的设备、设施的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，保障应用系统的正常运行，以维护计算机信息系统的安全运行。

第四条 信息网络系统安全的含义是通过各种计算机、网络、密码技术和信息安全技术，在实现网络系统安全的基础上，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。

第五条 本制度适用于公司员工使用的信息系统。

第二章 计算机使用管理

第六条 按照谁使用谁负责的原则，落实责任人，负责保管所用的计算机，打印机等设备的完好。做到谁使用谁领用，且由部门经理进行确认。

第七条 公司员工应服从公司对计算机分配，不得私自调换计算机及外围设备。

第八条 计算机领用人严禁使用公司计算机玩游戏、看影碟及进行其他与工作无关的操作。

第九条 计算机领用人应对外来软盘，光盘，优盘，移动硬盘及其他便携式

存储设备进行严格的病毒监测，方可使用。

第十条 计算机领用人不得擅自修改计算机设置，杜绝一切影响网络正常运行的行为发生。

第十一条 计算机产生异常情况，计算机领用人应暂停计算机的使用，并将计算机出现的异常情况及时告知公司网络管理人员。

第十二条 计算机领用人对于计算机的系统登陆必须设置帐号密码，且不得将密码告诉其他人员，严格控制非使用人员使用计算机。

第十三条 计算机领用人对自己的计算机应经常进行病毒检测与杀毒。严禁外单位人员操作信息系统，严禁使用外来盘片，以防泄密和病毒侵入。

第十四条 计算机领用人操作计算机时不得使用一些危险性的命令，严禁擅自使用分区及格式化硬盘等操作。

第十五条 计算机操作人员不得随意在各终端及局域网上安装任何与工作无关的软件程序。各单位所使用的计算机和软件系统，除审批通过的管理软件外。

第三章 网络系统安全管理

第十六条 网络系统安全的内涵包括五个方面：

机密性：确保信息不暴露给未授权的实体或进程。

完整性：未经授权的人不能修改数据，只有得到允许的人才能修改数据，并且能够分辨出被篡改的数据。

可用性：得到授权的实体在合法的范围内可以随时随地访问数据，网络的攻击者不能阻碍网络资源的合法使用。

可控性：可以控制授权范围内的信息流向和行为方式。

可审查性：一旦出现安全问题，网络系统可以提供调查的依据和手段。

第十七条 网络管理员应尽可能地改善网络系统的安全策略设置，尽量减少安全漏洞。关闭不使用的服务，对不同级别的网络用户设置相应的资源访问权限。

第十八条 网络管理员应当做好系统记录，定期检查，发现问题，及时解决。

第十九条 重要的信息网络系统自运行开始必须作好备份与恢复等应急措施，一旦系统出现问题能够及时恢复正常。网络管理员负责网络系统的备份与恢复的技术规划、实施和操作，并作好详细的记录。

第二十条 管理员应对操作系统和数据库管理系统中进行系统运行记录和数据库运行记录的转储保存以备查。

第二十一条 重要大型数据库必须运行于专门的服务器或工作站上，并异地备份。

第二十二条 网络安全检测。为使网络长期保持较高的安全水平，网络管理员应当用网络安全检测工具对网络系统进行安全性分析，及时发现并修正存在的安全漏洞。网络管理员在系统检测完成后，应编写检测报告，需详细记叙检测的对象、手段、结果、建议和实施的补救措施与安全策略。检测报告存入系统档案。

第二十三条 网络反病毒。病毒的危害性巨大，对系统和信息的破坏程度具有不可测性，计算机用户和系统管理员应针对具体情况采取预防病毒技术、检测病毒技术和杀毒技术。

第四章 信息安全管理

第二十四条 信息安全是指通过各种计算机、网络和密码技术，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：

（一）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，避免因为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。

（二）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。

（三）信息传播安全

要加强对信息的审查，防止和控制非法、有害的信息通过我部的信息网络系统传播，避免对国家利益、公共利益以及个人利益造成损害。

第二十五条 信息的内部管理

（一）各部门在向网络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；

（二）根据情况，采取网络病毒监测、查毒、杀毒等技术措施，提高网络的整体抗病毒能力；

（三）各部门应对本单位的信息进行审查，各网站和栏目信息的负责单位必须对所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，应及时报告公司相关部门；

（四）涉及公司机密的信息的存储、传输等应指定专人负责，并严格按照国家有关保密的法律、法规执行；

（五）个人计算机中的涉密文件不可设置为共享，个人电子邮件的收发要实行病毒查杀。

第二十六条 涉及公司机密的信息，其电子文档资料须加密存储；在传输过程中视情况及公司的有关规定采用文件加密传输或链路传输加密。

第二十七条 任何单位和个人不得从事以下活动：

（一）利用信息网络系统制作、传播、复制有害信息；

（二）入侵他人计算机；

（三）未经允许使用他人在信息网络系统中未公开的信息；

（四）未经授权对信息网络系统中存储、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；

（五）未经授权查阅他人邮件；

（六）盗用他人名义发送电子邮件；

（七）故意干扰网络的畅通运行；

（八）从事其他危害信息网络系统安全的活动。

第五章 人员管理

第二十八条 安全的人员管理原则网络信息系统的安全管理的最根本核心是人员管理，提高安全意识，行于具体的安全技术工作中。为此，安全的人事组织管理主要基于以下三个原则：

（一）每一项与安全有关的活动，都必须有两人或多人在场；

（二）参与安全管理活动的人员由系统主管领导指派，要求工作认真可靠，能胜任此项工作；

（三）相关人员应签署工作情况记录以证明安全工作已得到保障。负责的安全活动范围包括：

（一）访问控制使用证件的发放与回收；

（二）信息处理系统使用的媒介发放与回收；

（三）处理保密信息；

（四）硬件和软件的维护；

（五）系统软件的设计、实现和修改；

（六）重要程序和数据的删除和销毁等。

第二十九条 在信息处理系统工作的人员不得打听、了解或参与职责以外的任何与安全有关的事情，除非系统主管领导批准。

第三十条 安全的人事管理的实现

信息系统的安全管理应根据管理原则和该系统处理数据的保密性，制订相应的管理制度或采用相应的规范。包括：

（一）根据工作的重要程度，确定该系统的安全等级 ；

（二）根据确定的安全等级，确定安全管理的范围；

（三）制订严格的操作规程；

操作规程根据职责明确和多人负责的原则，各负其责，不超越自己的管辖范围；对工作调动和离职人员要及时调整相应的授权。

（四）制订完备的系统维护制度；

对系统进行维护时，采取数据保护措施，如数据备份等。维护时要首先经主管部门批准，并有安全管理人员在场，故障的原因、维护内容和维护前后的情况要详细记录。

第三十条 系统管理员有权对局域网络以及各单位计算机进行定期检查或不定期抽查，凡有违反本制度的单位、部门或个人，应及时报告公司领导，视情节对部门或个人给予适当的经济处罚和行政处分。