信息系统安全管理办法

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配套设备、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，保障网络系统的硬件、软件及其系统中的数据，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

第五条 本制度适用于公司全体员工及实习生及其使用的信息系统。

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，U 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经授权的实体或进程。

完整性：数据修改需要经过相关授权，只有特定员工根据授权进行数据修改。

可用性：得到授权的实体在合法合理的范围内可以随时随地通过网络使用信息系统。。

可控性：可以根据授权管理网络系统使用的权限范围。

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 信息技术部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 信息技术部应当做好系统记录，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。信息技术部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 信息技术部应对操作系统和数据库管理系统中进行系统运行记录（System Log）和数据库运行记录（Database Log）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，信息技术部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。信息技术部在系统检测完成后，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，计算机用户和信息技术部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

信息技术部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。信息技术部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、有害的信息通过公司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）各部门在向信息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）各部门应对本部门的信息进行审查，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，应及时报告信息技术部及风险和内控委员会；

（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 口令管理

第二十八条 具有口令功能的计算机、网络设备等，必须使用口令对用户的身份进行验证和确认。对于网络系统，公司设专职或兼职信息技术部，负责日常的口令管理工作。

第二十九条信息技术部负责给新增加的用户分配初始口令；帮助用户开启被锁定的口令，对非法操作及时查明原因；解决口令使用过程中出现的问题；协助用户保护公司机密不受侵害；定期向主管领导汇报口令使用情况和需要解决的问题。

第三十条 定期更换口令。口令的最长使用时间不能超过 90 天，长度不小于八位。当口令使用期满时，应更换新的口令。

第三十一条 系统保密员必须有能力更改口令。当口令使用期满、被其他人知悉或认为口令不保密时，系统保密员可按照口令更改程序变换口令。口令更换操作应在保密条件下进行。

第三十二条 对口令数据库的访问和存取必须加以控制，以防止口令被非法修改或泄露。

第三十三条 当系统提供的访问和存取控制机制不够完善时或机制虽然完善，但可能出现系统转储等情况时，应对存储的口令加密。

第三十四条 公司提供员工使用的系统，如有保密要求，将系统定义为涉密系统。根据涉密程度分为秘密级，机密级，绝密级系统。涉密系统的身份认证应当符合以下要求：

（一）口令应当由信息技术部集中产生供用户选用；

（二）信息系统的口令长度不得少于八个字符，口令更换周期不得长于 90 天；

（三）口令在网络中必须加密传输。

第三十五条 用户应记住自己的口令，不应把它记载在不保密的媒介物上，严禁将口令贴在终端上。输入的口令不应显示在显示终端上。

第六章 人员管理

第三十六条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，都必须有两人或以上人员在场；

（二）参与安全管理活动的人员由信息技术部负责人指派，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。

第三十七条 参与安全管理活动的人员不得打听、了解或参与职责以外的任何与安全有关的事情。

第三十八条 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）制订相应的机房出入管理制度；

对于安全等级要求较高的系统，要实行分区控制，限制工作人员出入与己无关的区域。出入管理采用证件识别或安装自动识别登记系统，采用磁卡、身份卡等手段，对人员进行识别、登记和管理。

（四）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。

（五）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。

（六）制订应急措施。

制订系统在紧急情况下，如何尽快恢复的应急措施，使损失减至最小。

第三十九条 信息技术部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。公司有权视情节对部门或个人给予经济处罚或行政处分。

第七章 附则

第四十条 本制度由信息技术部负责修订及解释,并由公司风险和内控委员会审订通过后生效。