文档密级：C

系统安全管理规范

一、 总则

1. 目的

为进一步强化公司信息系统运行维护管理工作，建立业务、技术支持相结合，规范、高效运转的综合运行维护管理体制，确保各类系统稳定、安全、高效运行，特制订本制度。

2. 范围

本制度适用于公司所有信息系统的安全管理。主要包括访问控制策略、漏洞扫描、漏洞修补、系统安全策略、安全配置、日志管理和日常操作流程等方面的内容。

3. 职责

信息技术部承担各类系统的技术运维工作，具体系统运维工作由各系统管理员负责。

二、 管理细则

1. 系统安全建设

（1） 应用系统安全方面应符合国家和行业监管要求，并进行安全评估和测试，才允许上线。

（2） 服务器操作系统应选用正版软件并且遵守软件规定的最终用户使用协议。

（3） 系统安装完成，测试通过投入使用前，应删除测试用户和口令，最小化授权用户的权限，最优化安全配置。

2. 系统安全维护

（1） 所有信息系统应由专职的系统管理员负责管理和维护，系统管理员应对上述信息系统进行必要的安全配置，参照《信息系统安全配置标准》。

（2） 管理员应对信息系统进行登记记录，并且按照《信息资产分类分级指南》填写《受控信息资产登记表》。

（3） 信息系统必须实现帐号口令的认证管理方式，对于重要系统使用双因素认证方式。禁止为所有系统无关的人员提供系统用户账号，用户权限的设

置应遵循最小授权和权限分割的原则。口令管理应符合《账号口令管理制度》。

（4） 严格禁止非本系统管理人员直接进入系统进行操作，若在特殊情况下需要外部人员进入服务器进行操作时，必须由本系统管理员登录，并对操作全过程进行记录备案。禁止将系统用户账号及口令直接交给外部人员，在紧急情况下需要为外部人员开放临时账号时，必须获取相关领导批准。

（5） 尽可能减少服务器设备的远程管理方式，如果的确需要进行远程管理，应使用通信加密协议，并且限定远程登录的会话超时时间、远程管理的用户数量、远程管理的终端 IP 地址、登录尝试次数等。

（6） 严禁在服务器上随意安装、卸载系统组件和驱动程序，如确实需要，应及时评测可能由此带来的影响，在获得信息安全工作组的批准下，对生产环境实施评测过的对策，并将整个过程记录备案；

（7） 禁止在服务器上随意下载、安装和使用来历不明、没有版权的软件，严禁安装本地或网络游戏以及即时通讯程序，禁止安装与该服务器所提供服务和应用无关的其它软件；

（8） 禁止在重要的服务器上浏览外部网站网页、接收电子邮件、编辑外来文档以及进行与服务器系统维护无关的其它操作。

（9） 禁止在重要服务器系统上开放具有“写”权限的共享目录，如果确实必要，可临时开放，但要设置强共享口令，并在使用完之后立刻取消共享；

（10） 禁止系统明确不使用的服务、协议和设备的特性，避免使用不安全的服务。

（11） 保证信息系统日志处于正常状态，每月对日志做一次全面的分析，对登录的用户、登录时间、所做的操作做检查，在发现有异常的现象时应及时向负责人报告。

（12） 及时监视、收集服务器操作系统厂商公布的补丁信息，对于非常重要的补丁程序在经过测试无影响的情况下尽快对生产环境设备实施补丁安装；补丁安装应尽量安排在非业务繁忙时段进行，在升级（或修补）前后做好数据的备份工作，同时将整个过程记录备案。

（13） 对于核心业务系统，其操作系统和应用系统补丁必须经过严格的测试和评估，并咨询操作系统厂商后，才可以实施补丁安装。

（14） 定期对服务器操作系统和应用系统进行安全漏洞扫描，漏洞扫描平均频率应不低于三个月一次，重大安全漏洞或蠕虫发布后，应在 1 个工作日内进行；

（15） 当发现服务器设备上存在病毒、异常开放的服务或者开放的服务存在安全漏洞时应及时报告信息安全应急工作组，并采取相应措施。

（16） 应定期对系统进行检查，确保各设备都能正常工作；重要服务器和应用系统检查频率至少每天一次。通过各种手段监控服务器系统的 CPU 利用率、进程、内存和启动脚本等的使用状况。当服务器系统出现以下现象之一时，必须进行安全问题的报告和诊断：

a） 系统中出现异常系统进程或者系统进程数量有异常变化。

b） 系统突然不明原因的性能下降。

c） 系统不明原因的重新启动。

d） 系统崩溃，不能正常启动。

e） 系统中出现异常的系统账号

f） 系统账号口令突然失控。

g） 系统账号权限发生不明变化。

h） 系统出现来源不明的文件。

i） 系统中文件出现不明原因的改动。

j） 系统时钟出现不明原因的改变。

k） 系统日志中出现非正常时间系统登录，或有不明 IP 地址的系统登录。

l） 发现系统不明原因的在扫描网络上其它服务器。

（17） 至少每年一次对所有信息系统进行全面安全评估，评估后应尽快完成对系统的修补和加固，并进行二次评估。

3. 系统安全变更

（1） 在服务器出现变更情况时，系统管理员应及时对配置记录进行更新。

（2） 系统管理员应在系统接入、配置变更、废弃等系统变更操作前进行数据备份，以便在不成功的情况下及时进行恢复。

（3） 新的系统的接入应首先由相关人员提出申请，信息技术部根据实际

业务需要进行审核，确定最佳接入方案，才可以进行实施，禁止私自安装或移动服务器。

（4） 根据业务系统应用的需要，要求服务器配置变更时，应参照《信息系统变更管理制度》相关规定执行。

（5） 任何新的服务器或信息系统接入、配置变更前，都应做好详细的应急预案或应急处理方案。

（6） 服务器废弃前应将服务器上存储的所有敏感数据进行脱敏处理。

（7） 新的服务器在正式上线运行前应进行安全检查并确认后方能正式运行使用。严禁在不测试 或测试不成功的情况下接入网络。检查的内容如下：

a) 查看硬件和软件系统的运行情况是否正常、稳定；

b) 查看 OS 版本和补丁安装情况；

c) OS 是否存在已知的系统漏洞或者病毒、木马等其他安全缺陷；

d) 是否安装了公司统一要求的防病毒软件，病毒库是否升级至最新。

（8） 新的信息在正式上线运行或服务器出现重大配置变更后，应在一段时间内严密监控其运行情况，以及对网络是否带来影响；当发现网络运行不稳定或者出现明显可疑情况时，应及时报告必要时启动应急预案。

三、 附则

1. 对违反上述安全管理条例的员工，依据《信息安全惩戒规范》进行处理。
2. 本制度由公司信息安全局负责解释和修订。
3. 本制度自发布之日起开始执行。

附 1：系统特权用户的授权记录

系统特权用户授权记录

服务器类：

服务器 IP	运行业务系统	账号名	权限角色	用户姓名	登记时间	备注

应用系统类：

应用系统名称	账号名	权限角色	用户姓名	登记时间	所属部门	备注

*此表主要登记业务系统用户权限，记录其姓名、及部门

附 2：补丁测试记录

序号	补丁编号	补丁测试时间	测试系统	测试人员	补丁安装时间	安装系统	安装人员	验证结果
1								
2								

3								
4								
5								
6								
7								
8								
9								

附 3：系统异常行为分析记录单

系统异常行为分析记录

违规行为详细记录（含违规	处理措施	记录	记录