文档密级：C

网络安全管理规范

一、 总则

1. 目的

为了确保公司网络系统安全，对公司网络安全活动实施控制，特制定本规范。

2. 适用范围

适用于对公司信息系统网络安全的管理。

3. 职责

信息技术部-基础架构局负责公司整个网络系统的日常管理、实施、维护等工作。

二、 管理细则

1. 维护管理

（1） 任何个人不得擅自修改网络资源配置、网络权限和网络安全等级。

（2） 网络管理员应根据需要增加、修改或删除网络过滤规则，符合数据传送的保密性、可用性，使用最小化规则。

（3） 网络管理员定期对监测节点设备上的声光告警信号和维护控制台的告警显示信息，发现问题并及时处理，为网络稳定运行提供基本保障。

（4） 定期对网络设备、线路、各楼层汇聚机房及配套设施进行巡视巡检、清洁、数据备份等操作。

（5） 发生突发性网络安全事件，由信息安全委员会负责协调处理，信息安全应急工作小组协助配合，并对故障现象和处理过程作详细记录。

（6） 对基础数据网设备进行操作时须严格按照操作手册执行。

（7） 应定期进行安全检查，检查当前运行的网络配置数据与网络现状是否一致，如不一致应及时更新。

（8） 检查缺省启动的网络配置文件是否为最新版本，如不是应及时更新。

（9） 网络发生变化时，及时更新网络配置数据，并做相应记录。

（10） 网络配置数据应及时备份，备份结果至少要保留到下一次修改前。

（11） 对重要网络数据备份应实现异质备份、异址存放。

（12） 重要的网络设备策略调整，如安全策略调整、服务开启、服务关闭、网络系统外联、连接外部系统等变更操作必须填写申请表，经主管同意后方可调整。

（13） 网络资源命名按信息中心规范进行，建立完善的网络技术资料档案（包括：网络结构，设备型号，性能指标等）。

（14） 重要网络设备的口令要定期更改，一般要设置八个字符以上，口令设置应无任何意义，最好能包含非数字和字母在内的字符，同时采用大小写混用的方式；口令要存档保存。

（15） 需建立并维护整个系统的拓扑结构图，拓扑图体现网络设备的型号、名称以及与线路的链接情况等。

（16） 涉及与外单位联网，应制定详细的资料说明备案；需要接入内部网络时，必须通过相关的安全管理措施，报主管领导审批后，方可接入和接出。

（17） 内部网络不得与互联网进行物理连接，如需要，应设置严格的访问控制策略；不得将有关涉密信息在互联网上发布，不得在互联网上发布非法信息；在互联网上下载的文件需经过检测后方可使用，不得下载带有非法内容的文件、图片等。

（18） 尽量减少使用网络传送非业务需要的有关内容，尽量降低网络流量；禁止涉密文件在网上共享。

（19） 所有网络设备都必须根据采购要求购置，并根据安全防护等级要求放置在相应的安全区域内或区域边界处，合理设置访问规则，控制通过的应用及用户数据。

2. 变更管理

（1） 网络变更是指公司调整网络结构和网络设备配置、网络扩容、新设备并网运行、设备搬迁、网络设备漏洞修补等工作。

（2） 网络变更由基础架构局负责，并和各部门及设备厂商一起制定技术方案和实施细则，报信息安全领导委员会批准。

（3） 所有重大网络变更必须提前五个工作日以书面形式报信息安全领导委员会，经审核批准后方可执行。

（4） 重大的网络变更必须事先进行严格的测试验证，确保网络安全，同时制定明确的技术方案，在技术方案中须含有回退预案。

（5） 申请批复后，信息技术部应及时负责召开工作会议，落实工作步骤和具体细节。

（6） 工作执行前，必须对系统准备情况进行一次现场检查，确保准备工作充分。

（7） 变更工作应安排在业务运行低谷时段，如夜晚、周末。

（8） 变更工作完成后，安排维护人员加强值班监控，密切注意系统运行情况，及时分析话务统计数据，前后比较，变更后必须加强值班监视，并按相关规定上报结果。

（9） 应保持与国家相关部门和设备厂商的沟通，对他们发布的危险漏洞进行关注，并根据实际情况对漏洞进行评估和修补。

（10） 至少一季度一次对网络设备进行漏洞扫描，根据漏洞扫描的结果对各种漏洞进行加固和升级规避处理。

（11） 由设备厂商提供的新软件版本和补丁，必须经主管批准后，测试合格并提交由基础架构局和设备厂商双方共同确认的测试报告，确认安装计划后才能在全网安装实施。未经批准不得擅自执行升级。

3. 备份管理

➢ 备份周期：网络管理员对维护的网络设备配置每半年备份一次；日常性维护，网络设备配置文件发生变更前也需要保留备份文件；突发性维护尽可能在可备份情况下进行备份。

➢ 备份位置：至少需要放在文件服务器，冷备、重要及核心设备须有异地备份。

➢ 备份文件命名规则：设备名称+IP 地址(取最后字节)+备份日期

➢ 备份方式：可采用手工或自动备份方式。

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。