**XXX单位**

**网络安全管理制度**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479446805)

[2 适用范围 1](#_Toc479446806)

[3 网络安全管理职责 1](#_Toc479446807)

[4 网络运行管理 1](#_Toc479446808)

[4.1 网络运行监测 1](#_Toc479446809)

[4.2 网络值班 2](#_Toc479446810)

[5 网络安全巡检 2](#_Toc479446811)

[6 网络运行报告管理 2](#_Toc479446812)

[7 附则 3](#_Toc479446813)

# 目的

为规范网络的管理和运行维护，提高网络的服务质量，加强数据网络管理，保障信息系统安全、稳定运行，特制定本制度。

# 适用范围

本制度适用于XXX单位网络管理和运行工作。

# 网络安全管理职责

网络管理系统要分别设立网络管理员和网络安全审计员，并分别由不同的人员担任；

网络管理员根据网络访问控制策略要求，进行网络设备参数设置，更新和维护等工作；对网络设备实行分级授权管理，按照不同的管理级别进行权限分配；

网络安全审计员对网络管理员的登录和操作内容进行审计，一月内至少审计一次日志报表；对网络配置与网络访问控制策略进行符合性检查。

# 网络运行管理

## 网络运行监测

网络管理员应定期和不定期地检查网络设备的运行状况，及时查看设备日志，对异常情况的发生，及时上报，并做好记录；对网络设备CPU和内存利用率、数据流量、地址翻译数量、进行均时的监测、跟踪工作，每月形成报表。

网络管理员对网络系统异常和网络系统故障的时间、现象、应急处理方法及结果作详细的记录。

当网络设备发生宕机引起网络拥塞或网络瘫痪等重大安全事件时网络管理员应立即启动紧急响应程序，对网络进行紧急处理，堵塞攻击入口，恢复网络的正常运行，并追查攻击来源，及时上报。

网络审计员应定期网络运维用户访问权限进行复查或评审，以避免可能的用户访问权限过界的现象出现。

网络审计员应定期对网络设备的操作进行审计，同时对审计内容本身进行定期审计，同时审计中要有明确的权限，充分保证审计内容的完全性。

## 网络值班

应指定网络值班人员，并指定网络值班电话，保证工作时间内有人接听。

网络值班人员每日对网络链路进行例行检查，记录网络链路状况。

# 网络安全巡检

巡检（法定工作日）包含但不限于如下内容：

（1）服务器：包括指示灯、系统日志、报警等。

（2）网络设备：包括网络接口状态、网络流量、系统日志、各类报警等。

（3）安全设备：包括网络接口状态、系统日志、各类报警等。

（4）应用系统：包括应用系统运行是否正常，系统服务性能能否满足要求。

（5）备份系统：包括数据备份运行是否正常、是否有可用备份磁带等。

（6）机房环境：包括机房市电输入配电情况、不间断电源系统电压、不间断电源系统电流、不间断电源系统负载率、温度、湿度、卫生、照明、门禁以及其他报警情况。

# 网络运行报告管理

应定期对网络运行情况进行统计分析，管理员每月进行网络运行报告。运行月报应包含设备及应用系统运行情况、存在的主要问题和处理措施、下月主要工作计划等内容。

定期对报告数据应进行认真分析，积极查找问题原因，提出网络合理分析和建议。

# 附则

本文件由XXX单位信息中心负责解释与修订。

本文件自颁布之日起发布执行。