江苏卫星地球站
信息系统安全保护实施细则
2017 年试行版本

摘要

本细则包括技术要求、物理要求和管理要求三个部分

奚晓轶

xxy@jsbc.com

目录

江苏卫星地球站信息系统安全保护实施细则（2017 年试行版本）

1 适用范围

1.1 本细则包括技术要求、物理要求和管理要求三个部分

1.2 本细则适用与标清抗干扰系统、标清网管系统和标清博汇信号监测系统；高清抗干扰系统、高清网管系统和高清风格信号监测系统。

2 规范性引用文件

- 《中华人民共和国网络安全法》
- 《中华人民共和国广播电影电视行业暂行技术文件》GD/J 038—2011
- 《新闻出版广播影视网络安全管理办法(试行)》
- 《新闻出版广播影视网络安全事件应急预案(试行)》苏新广技[2017]9

3 技术要求

3.1 总要求

- 本细则中适用的技术系统按第二级安全保护能力进行防护。
- 本细则中适用的技术系统采用物理隔离进行防护，即不允许以任何形式（无线方式、有线方式、VPN 远程等方式）接入互联网、办公网和台内网。

3.2 基础网络安全

3.2.1结构安全

a) 标清网管系统和高清网管系统分为两层结构网络，即设备网络和监控服务器、客户机组网网络。两个网络

采用不同的物理交换机和不同的网段设置，由设备采集服务器(双网卡)应用程序使用专用协议互转互通。

b) 标清抗干扰系统和高清抗干扰系统采用物理隔离方式。

c) 标清博汇信号监测系统和高清风格信号监测系统采用物理隔离方式。

3.2.2安全审计

a) 审计记录应包括事件的时间、事件级别、用户、事件分类和事件内容；

b) 定期对审计记录进行分析，以便及时发现异常行为；

c) 服务器审计包括：应用程序、安全、系统；

d) 客户机审计包括：应用程序、安全、系统。

3.2.3网络设备防护

a) 设备登录用户名和口令由专用登录终端统一管理；

b) 应对网络设备进行基本安全配置，关闭不用的服务和端口；

c) 本细则适用的系统属于物理隔离，不允许对网络设备进行远程管理。

3.3 边界安全

3.3.1访问控制

本细则适用的系统属于物理隔离，不允许任何方式接入。

3.3.2安全数据交换

a) 本细则适用的系统中涉及的服务器、客户终端本地策略设置不允许安装 USB 大容量驱动器；

b) 下载数据需使用 USB 刻录光驱刻录 DVD 光盘；

c) 上载数据时，使用两种最新病毒扫描软件对数据进行病毒扫描，在系统管理员监督下开启本地策略，允许 USB 大容量驱动器上载数据。

3.3.3入侵防范

本细则适用的系统属于物理隔离，不允许任何方式接入。

3.3.4恶意代码防范

a) 每个月使用离线方式（执行安全数据交换上载数据方式）更新服务器和客户终端上的杀毒软件病毒库；

b) 每个星期二执行全盘扫描。

3.4 数据安全与备份恢复

3.4.1标清网管系统和高清网管系统网络中传输的监控数据使用加密传输方式；

3.4.2标清网管系统和高清网管系统的数据库每个月自动执行数据库备份至 NAS；

3.4.3标清网管系统和高清网管系统的数据库每年进行完整数据库备份并刻录光盘。

4 物理要求

4.1 物理访问控制

4.1.1细则中涉及的系统机房入口设置电子门禁系统，控制、鉴别和使用视频摄像方式记录进入的人员；

4.1.2需进入播出机房的来访人员应经过申请和审批流程，并派专人陪同，限制和监控其活动范围。

4.2 防盗窃和防破坏

4.2.1应将公共区域信号线缆铺设隐蔽处，可铺设在地下或管道；

4.2.2应设置 24 小时保安人员，盘查携带设备出门的人员，不符合出门流程的应扣押设备；

4.2.3应在与播出相关的机房设置安防监控报警系统。

4.3 机房环境

4.3.1机房的温湿度、防尘、防静电、电磁防护、接地、布线等按照 GB 50174-93 的有关规定执行；

4.3.2机房设置温、湿度自动调节设施，机房空调、精密空调和抽湿机，对机房温湿度进行实时监控并进行语音告警；

4.3.3采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

4.3.4电源线和通讯线缆应隔离铺设，避免互相干扰。

4.4 消防设施

4.4.1机房消防设施的配置应符合 GY 5067 的有关规定

4.4.2机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；

4.4.3机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。

4.5 电力供应

a) 采用双路外电的双机并联热备份 UPS 进行供电；
b) 双路供电中断采用油机发电供电。

5 管理要求

5.1 人员安全管理

5.1.1人员上岗：应对上岗人员的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核

5.1.2人员离岗：应及时终止离岗员工的所有访问权限；收回各种身份证件、电子门禁卡和单位提供的软硬件设备

5.1.3考核和培训：定期对卫星站人员进行安全意识教育、岗位技能培训和相关安全政策、技术培训；对安全培训和考核情况进行记录并保存。

5.1.4外部人员访问管理 :需进入播出机房的来访人员应经过申请和审批流程，并派专人陪同，限制和监控其活动范围。

5.2 系统运维管理

5.2.1环境管理

a) 定期对机房空调、供配电、抽湿机等设施进行维护；
b) 定期对安防录像系统设施进行维护；
c) 定期对门禁系统设施进行维护管理，删除没有权限的电子门禁卡。

5.2.2资产管理

a) 指定信息系统资产的责任人；
b) 信息系统资产规范化标识。

5.2.3介质管理

a) 数据库备份光盘交由技术管理部统一封存；
b) 上传、下载数据统一使用 USB 刻录光驱进行数据交换，使用完的光盘进行统一销毁；
c) 外送维修信息系统设备时必须将内部存储硬盘留下并交安全员保管；
d) 信息系统硬盘无法使用时，必须进行物理销毁。

5.2.4设备管理

a) 定期对信息系统相关的各种设备、线路进行维护；
b) 对终端计算机、工作站、服务器和网络设备的操作必须规范化，按操作规程实现主要设备的启动/停止、加电/断电等操作；
c) 细则涉及的信息系统处理设备涉外维修时必须拆除内部存储硬盘并交安全员保管；
d) 细则涉及的信息系统处理设备不允许带离机房。

5.2.5网络安全管理

a) 不允许接入任何其它网络，如办公网、互联网等；
b) 不允许任何方式的远程维护操作；
c) 定期更新病毒库和系统补丁；
d) 定期检查网络安全配置，封堵无用的端口和服务；
e) 定期检查安全策略，更新口令。

5.2.6系统安全管理

a) 不允许接入大容量 USB 存储设备；
b) 每个星期执行全盘病毒扫描；
c) 定期检查系统日志进行分析，以便及时发现异常行为。

5.2.7恶意代码防范

a) 每个星期执行恶意代码扫描；
b) 每个月离线更新病毒库；
c) 发现恶意代码产品应及时分析处理，并形成书面报告和总结汇报。

5.2.8密码管理

应建立密码使用管理制度，定期更新服务器密码。

5.2.9变更管理

a) 应确认系统中要发生的变更，并制定书面变更方案；
b) 变更方案应向主管领导申请，变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向值班人员通告；
c) 操作系统、恶意代码库和应用程序应在变更前做好相关测试，确认所升级内容对安全播出没有影响，方可升级
d) 变更过程失败必须可以撤销，应能恢复到变更前的业务水平；
e) 变更后的信息系统必须满足变更前的安全等级要求。

5.2.10 备份与恢复管理

a) 三个月自动执行完整数据库备份到 NAS；
b) 每年备份信息系统的业务数据库并刻录光盘保存；
c) 不定期对备份的数据进行有效性检查。

5.2.11 安全事件处置

病毒扫描和漏洞扫描发现可疑程序应立即隔离并现场评估其影响范围、程度，收集证据，书面记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均妥善保存。

5.2.12 应急预案管理

a) 应急预案每年审核、修订一次；
b) 应急预案培训、考核每年举办一次；
c) 不定期进行应急预案演练。