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

广播电视相关信息系统
安全等级保护基本要求

Baseline for classified protection

of broadcasting related information system

2011-05-31 发布　　2011-05-31 实施

国家广播电影电视总局科技司　发布

目　　次

前　言

本技术文件依据《中华人民共和国计算机信息系统安全保护条例》（国务院147号令）、《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）、《关于信息安全等级保护工作的实施意见》（公通字[2004]66号）、《信息安全等级保护管理办法》（公通字[2007]43号）和GB/T 22240-2009 《信息安全技术 信息系统安全等级保护定级指南》、GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》、《广播电视安全播出管理规定》（总局62号令），对广播电视相关信息系统安全等级保护基本要求进行规范。

在本技术文件条款中，加粗字表示较低等级中没有出现或增强的要求。

本技术文件按照GB/T 1.1-2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则编制。

本技术文件由国家广播电影电视总局科技司归口。

本技术文件起草单位：国家广播电视安全播出调度中心、北京捷成世纪科技股份有限公司。

本技术文件主要起草人：张瑞芝、关丽霞、沈传宝、王鸣皓。

广播电视相关信息系统安全等级保护基本要求

1 范围

本技术文件规定了不同安全等级的广播电视相关信息系统的基本保护要求，包括技术要求、物理要求和管理要求三部分。

本技术文件适用于指导广电行业开展广播电视相关信息系统的信息安全等级保护安全规划、建设和自查，也可作为信息安全职能部门对广播电视相关信息系统信息安全进行监督、检查和指导的依据。办公系统、网站发布系统以及其他与广播电视生产业务无关的信息系统参照国家相关标准执行。本文中的信息系统是指由计算机及其相关的和配套的设备、网络构成的对广播电视业务信息进行采集、加工、存储、传输、检索等处理的系统。

对于涉及国家秘密的信息系统，应按照国家保密工作部门的相关规定和标准进行保护。对于涉及密码的使用和管理，应按照国家密码管理的相关规定和标准实施。

2 规范性引用文件

下列文件对于本技术文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本技术文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本技术文件。

GB 50174-93 电子信息系统机房设计规范

GY 5067-2003 广播电视建筑设计防火规范

3 术语和定义

GB/T 22239-2008、GB/T 22240-2008和GB/T 25070-2010确立的以及下列术语和定义适用于本文件。

3.1

广播电视相关信息系统

承载广播电视制作、播出、传输、覆盖等生产业务相关的信息系统。

3.2

外部网络

本单位广播电视生产业务相关信息系统之外的网络，如办公网络、外单位网络、国际互联网或其它公共网络等。

3.3

网络安全域

同一系统内有相同或相似的安全保护需求，相互信任，并具有相同或相似的安全访问控制和边界控制策略的网络或子网，相同或相似的网络安全域共享一样的安全策略。安全域内还可以进一步划分安全子域、子网或网段。

4 广播电视相关信息系统安全防护基本要求概述

4.1 信息系统安全保护等级

根据广播电视相关信息系统所提供的系统服务和承载的业务信息受到破坏时对国家安全、社会秩序和公共利益或对公民、法人和其他组织的合法权益的侵害程度等，由低到高划分为第一级至第五级，定义见《广播电视相关信息系统安全等级保护定级指南》。

4.2 不同等级的安全保护能力

不同等级的信息系统应具备的基本安全保护能力如下：

a) 第一级安全保护能力：应能够防护系统免受来自拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后，能够恢复部分功能。

b) 第二级安全保护能力：应能够防护系统免受来自拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难、以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。

c) 第三级安全保护能力：应能够在统一安全策略下防护系统免受来自拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难、以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。

d) 第四级安全保护能力：应能够在统一安全策略下防护系统免受来自拥有丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难、以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。

e) 第五级安全保护能力：（略）。

4.3 整体安全保护能力要求

广播电视相关信息系统安全防护的核心是保证与播出相关的信息系统具备与其安全保护等级相适应的安全保护能力。参照GB/T 22039信息安全技术信息系统安全等级保护基本要求，基本防护要求包含技术要求、物理要求和管理要求。其中第5章到第9章分别针对不同安全保护等级信息系统应该具有的安全保护能力，从网络安全（基础网络安全和边界安全）、主机安全（终端系统安全、服务端系统安全）、应用安全、数据安全几个层面提出了相应的安全防护要求。根据广播电视安全播出管理规定，全国各级播出单位在机房环境和播出管理方面统一要求，因此本文第10章和第11章对广播电视相关信息系统的物理安全以及管理安全方面提出的安全防护要求是通用性要求，除特殊说明外，其它条款适用于各安全等级的广播电视相关信息系统。基本技术要求、物理要求和管理要求是确保信息系统安全不可分割的组成部分。

需要特殊说明的是，满足基本安全防护要求是保证信息系统具有相应等级安全保护能力的前提。但针对于不同的播出单位来说，广播电视相关信息系统是一个整体，除了依据本文提出的分层面采取各种安全措施，还应从播出单位信息系统的业务特殊性等方面考虑总体性要求，保证信息系统的整体安全保护能力。

作为安全播出单位信息系统的整体信息安全要求，应当在信息系统安全建设时，充分考虑以下安全要求：

a）构建纵深的防御体系

本文从技术、物理和管理三个方面提出基本安全要求，在采取由点到面的各种安全措施时，系统整体上还应保证各种安全措施的组合，从以下两个方面构建安全纵深防御体系，保证信息系统整体的安全保护能力：根据各信息系统与播出业务的相关程度，从生产综合系统、制作系统、播出系统等信息系统安全层面，构建从外到内的业务安全纵深；同时还应从基础网络安全、边界安全、计算环境（主机、应用）安全等多个层次落实本文中提到的各种安全措施，形成纵深防御体系。

b）采取互补的安全措施

本文以安全控制组件的形式提出基本安全防护要求，在将各种安全控制组件集成到特定信息系统中时，应考虑各个安全控制组件功能的整体性和互补性，关注各个安全控制组件在层面内、层面间和功能间产生的连接、交互、依赖、协调、协同等相互关联关系，保证各个安全控制组件共同综合作用于信息系统的安全功能上，使得信息系统的整体安全保护能力得以保证。

c）进行集中的安全管理

本文在第三级及以上级别信息系统的安全功能管理要求上，提到了统一安全策略、统一安全管理等要求，为了保证分散于各个层面的安全功能在统一策略的指导下实现，各个安全控制组件在可控情况下发挥各自的作用，应建立安全管理中心，集中管理信息系统中的各个安全控制组件，支持统一安全管理。

建立有安全管理中心的播出单位可根据广播电视相关信息系统的特点，将各个等级信息系统的安全管理统一纳入到安全管理中心中，实现跨系统的安全管理中心。

4.4 基本技术要求的三种类型

GB/T 22239-2008 信息安全技术信息系统安全等级保护基本要求中，根据保护侧重点的不同，技术类安全要求进一步细分为：保护数据在存储、传输、处理过程中不被泄漏、破坏和免受未授权的修改的信息安全类要求（简记为S）；保护系统连续正常的运行，免受对系统的未授权修改、破坏而导致系统不可用的服务保证类要求（简记为A）和通用安全保护类要求（简记为G）。

根据《广播电视相关信息系统安全等级保护定级指南》，作为定级对象的信息系统的安全保护等级由业务信息安全保护等级和系统服务安全保护等级较高者决定。本文在进行安全防护基本要求设计时，根据广播电视相关信息系统的特点，分别针对不同安全保护等级的信息系统设计了相应的信息安全类要求、服务保证类要求和通用安全保护类要求，因此本文中不再对各安全等级的信息安全类要求、服务保证类要求和通用安全保护类要求进行区分，各定级对象根据确定的安全保护等级进行安全防护。

5 第一级防护要求

5.1 基础网络安全

5.1.1 结构安全

要求如下：

a) 应保证关键网络设备的业务处理能力和网络带宽满足业务需要；

b) 应绘制与当前运行情况相符的网络拓扑结构图。

5.1.2 网络设备防护

要求如下：

a) 应对登录网络设备的用户进行身份鉴别；

b) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

c) 应该对网络设备进行基本安全配置，关闭不必要的服务和端口；

d) 当对网络设备进行远程管理时，应采用HTTPS、SSH等安全的远程管理手段，防止用户身份鉴别信息在网络传输过程中被窃听。

5.2 边界安全

5.2.1 访问控制

要求如下：

a) 应在网络边界部署访问控制设备，根据安全策略提供明确的允许/拒绝访问，控制粒度为网段级；

b) 通过外部网络对提供非公众服务的信息系统进行访问时应使用安全方式接入，并对用户权限进行管理，控制粒度为用户组级。

5.2.2 安全数据交换

要求如下：

a) 播出系统与其它信息系统之间进行数据交换时，应对文件类型及格式进行限定；

b) 应限定可以通过移动介质交换数据的主机，所有通过移动介质上载的内容应经过两种以上的防恶意代码产品进行恶意代码检查后，方可正式上载到内部网络；对蓝光、P2等专业移动介质可通过特定的防护机制进行上载。

5.3 终端系统安全

5.3.1 身份鉴别

应对登录终端操作系统的用户进行身份标识和鉴别。

5.3.2 访问控制

应依据安全策略控制用户对资源的访问，禁止通过USB等外设进行数据交换，关闭不必要的服务和端口等。

5.3.3 恶意代码防范

应当部署防恶意代码软件，并定期更新防恶意代码软件版本和恶意代码库。

5.4 服务端系统安全

5.4.1 身份鉴别

要求如下：

a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

b) 系统管理用户身份鉴别信息应具有不易被冒用的特点，口令应定期更换，用户名和口令禁止相同；

c) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

5.4.2 访问控制

要求如下：

a) 应启用访问控制功能，依据安全策略控制用户对资源的访问，根据需要禁止通过USB、光驱等外设进行数据交换，关闭不必要的服务和端口等；

b) 应限制默认帐户的访问权限，重命名Windows系统默认帐户，修改帐户的默认口令；

c) 应及时删除多余的、过期的帐户，避免存在共享帐户。

5.4.3 恶意代码防范

应部署防恶意代码软件，并定期更新防恶意代码软件版本和恶意代码库。

5.4.4 入侵防范

要求如下：

a) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序；

b) 应定期更新操作系统补丁。

5.5 应用安全

5.5.1 身份鉴别

要求如下：

a) 应对登录应用系统的用户进行身份标识和鉴别，应为不同用户分配不同的用户名，不能多人使用同一用户名；

b) 系统管理用户身份鉴别信息应具有不易被冒用的特点，口令应定期更换，用户名和口令禁止相同；

c) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

5.5.2 访问控制

要求如下：

a) 应启用访问控制功能，依据安全策略控制用户对资源的访问，控制粒度为用户级；

b) 删除临时帐户和测试帐户，重命名默认帐户，修改其默认口令，限制其访问权限，不允许匿名用户登录。

5.5.3 软件容错

应提供数据有效性检验功能，保证通过人机接口输入或通信接口输入的数据长度、格式、范围、数据类型等符合设定要求，防止诸如SQL注入、跨站攻击、溢出攻击等恶意行为。

5.6 数据安全与备份恢复

5.6.1 数据完整性

应能够检测到用户身份鉴别信息、调度信息、播出节目等重要业务数据在传输过程中完整性受到破坏。

5.6.2 数据保密性

应采用加密或其他有效措施实现用户身份鉴别信息的存储保密性。

5.6.3 备份和恢复

应能够对重要业务信息进行备份和恢复。

6 第二级防护要求

6.1 基础网络安全

6.1.1 结构安全

要求如下：

a) 应保证关键网络设备的业务处理能力和网络带宽**具备冗余空间，满足业务高峰期需要；**

b) 应为新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心交换机、汇聚交换机等关键网络设备配置冗余；

c) 应根据各信息系统与播出的相关程度进行层次化网络结构设计，形成网络纵深防护体系，新闻制播系统中的直播演播室系统、播出整备系统、播出系统等播出直接相关系统应位于纵深结构内部，系统内部不应通过无线方式进行组网；

d) 应根据信息系统功能、业务流程、网络结构层次、业务服务对象等合理划分网络安全域；

e) 安全域内应根据业务类型、业务重要性、物理位置等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；

f) 同一安全域内重要网段与其他网段之间应采取可靠的技术隔离手段；

g) 应绘制与当前运行情况相符的网络拓扑结构图。

6.1.2 安全审计

要求如下：

a) 应对关键网络设备的运行状况、用户行为等重要事件进行日志记录；

b) 审计记录应包括事件的日期、时间、用户名、IP 地址、事件类型、事件是否成功等；

c) 应保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录至少保存 90 天；

d) 应定期对审计记录进行分析，以便及时发现异常行为。

6.1.3 网络设备防护

要求如下：

a) 应对登录网络设备的用户进行身份鉴别，**身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换，用户名和口令禁止相同；**

b) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和连接超时自动退出等措施；

c) 应该对网络设备进行基本安全配置，关闭不必要的服务和端口；

d) 应对网络设备的管理员登录地址进行限制，仅允许指定 IP 地址或 IP 段访问；

e) 当对网络设备进行远程管理时，应采用HTTPS、SSH等安全的远程管理手段，防止用户身份鉴别信息在网络传输过程中被窃听。

6.2 边界安全

6.2.1 访问控制

要求如下：

a) 应在网络边界部署访问控制设备，根据安全策略提供明确的允许/拒绝访问，控制粒度为网段级；

b) 通过外部网络对信息系统进行访问时应使用安全方式接入，**根据需要采用数字证书等强制认证方式**，并对用户权限进行管理，控制粒度为**用户级**。

6.2.2 安全数据交换

要求如下：

a) 播出系统与其它信息系统之间进行数据交换时，应对文件类型及格式进行限定；

b) 应限定可以通过移动介质交换数据的主机，所有通过移动介质上载的内容应经过两种以上的防恶意代码产品进行恶意代码检查后，方可正式上载到内部网络；对蓝光、P2等专业移动介质可通过特定的防护机制进行上载；

c）信息系统与外部网络进行数据交换时，应通过数据交换区或专用数据交换设备等完成内外网数据的安全交换；

d) 数据交换区对外应通过访问控制设备与外部网络进行安全隔离，对内应采用安全的方式进行数据交换，必要时可通过协议转换的手段，以信息摆渡的方式实现数据交换；

6.2.3 入侵防范

应在与外部网络连接的网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等。

6.2.4 恶意代码防范

要求如下：

a) 应在与外部网络连接的网络边界处进行恶意代码检测和清除，并维护恶意代码库的升级和检测系统的更新；

b) 防恶意代码产品应与信息系统内部防恶意代码产品具有不同的恶意代码库。

6.2.5 安全审计

要求如下：

a) 应在与外部网络连接的网络边界处进行数据通信行为审计；

b) 审计记录应包括事件的日期、时间、用户名、IP 地址、事件类型、事件是否成功等；

c) 应保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录至少保存 90 天；

d) 应定期对审计记录进行分析，以便及时发现异常行为。

6.2.6 边界完整性

应能够对内部网络用户私自联到外部网络的行为进行检查。

6.3 终端系统安全

6.3.1 身份鉴别

应对登录终端操作系统的用户进行身份标识和鉴别，**口令应有复杂度要求并定期更换，用户名和口令禁止相同。**

6.3.2 访问控制

应依据安全策略控制用户对资源的访问，禁止通过 USB 等外设进行数据交换，关闭不必要的

服务和端口等。

6.3.3 入侵防范

操作系统应遵循最小安装的原则，仅安装业务需要的组件和应用程序，并保持操作系统补丁及时得到更新。新闻制播系统、播出整备系统、播出系统等播出直接相关系统的终端可根据需要进行更新。

6.3.4 恶意代码防范

应部署**具有统一集中管理功能的**防恶意代码软件，并定期更新防恶意代码软件版本和恶意代码库；**新闻制播系统、播出整备系统、播出系统等播出直接相关系统的终端可根据需要进行部署。**

6.4 服务端系统安全

6.4.1 身份鉴别

要求如下：

a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别，**应为不同用户分配不同的用户名，不能多人使用同一用户名；**

b) 系统管理用户身份鉴别信息应具有不易被冒用的特点，口令应定期更换，用户名和口令禁止相同；

c) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

d) 当对服务器进行远程管理时，应采用HTTPS、SSH等安全的远程管理手段，防止用户身份鉴别信息在网络传输过程中被窃听。

6.4.2 访问控制

要求如下：

a) 应启用访问控制功能，依据安全策略控制用户对资源的访问，根据需要禁止通过 USB、光驱等外设进行数据交换，关闭不必要的服务和端口等；

b) 应实现操作系统和数据库系统特权用户的权限分离；

c) 应限制默认帐户的访问权限，重命名 Windows 系统默认帐户，修改帐户的默认口令；

d) 应及时删除多余的、过期的帐户，避免存在共享帐户。

6.4.3 安全审计

要求如下：

a) 应对系统中的接口服务器、Web服务器、应用服务器、数据库服务器等重要服务器的操作系统和数据库进行审计，审计粒度为用户级；

b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

c) 审计记录至少应包括事件的日期、时间、类型、用户名、客户端IP地址、访问对象、结果等；

d) 应保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录至少保存 90 天；

e) 应定期对审计记录进行分析，以便及时发现异常行为。

6.4.4 入侵防范

要求如下：

a) 操作系统应遵循最小安装的原则，仅安装业务需要的组件和应用程序，**关闭不必要的服务和端口；**

b) 应定期更新操作系统补丁，**新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器可根据需要进行更新**。

6.4.5 恶意代码防范

应部署**具有统一管理功能**的防恶意代码软件，并定期更新防恶意代码软件版本和恶意代码库；**新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器可根据需要进行部署和更新**。

6.4.6 资源控制

要求如下：

a) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；

b) 应根据安全策略设置登录终端的操作超时锁定；

c) 应限制单个用户对系统资源的最大或最小使用限度。

6.4.7 冗余配置

新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器应具有冗余配置。

6.5 应用安全

6.5.1 身份鉴别

要求如下：

a) **应提供独立的登录控制模块，或者将登录控制模块集成到统一的门户认证系统中，**应对登录应用系统的用户进行身份标识和鉴别，应为不同用户分配不同的用户名，不能多人使用同一用户名；

b) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识；

c) 系统管理用户身份鉴别信息应具有不易被冒用的特点，口令应定期更换，用户名和口令禁止相同；

d) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

6.5.2 访问控制

要求如下：

a) 应启用访问控制功能，依据安全策略控制用户对资源的访问，**控制粒度为文件和数据库表级；**

b) 删除临时帐户和测试帐户，重命名默认帐户，修改其默认口令，限制其访问权限，不允许匿名用户登录；

c) 访问控制的覆盖范围应包括与资源访问相关的主体（信息系统用户）、客体（用户所访问的数据）及它们之间的操作（读、写、修改、删除等）；

d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。如系统管理员不建议拥有系统审计员权限、一般系统用户不建议拥有系统管理员权限等。

6.5.3 安全审计

要求如下：

a）应提供新闻制播系统、播出整备系统、播出系统等播出直接相关系统安全审计功能；

b）审计内容应包括用户登录、修改配置、核心业务操作等重要行为，以及系统资源的异常使用等；

c）审计记录至少应包括事件的日期和时间、事件类型、客户端 IP 地址、描述和结果等；

d）应保证无法删除、修改或覆盖审计记录，审计记录至少保存 90 天。

6.5.4 通信完整性

信息系统与外部网络进行通信时，应采用校验码技术、特定的音视频文件格式、特定协议或等同强度的技术手段等进行传输，保证通信过程中的数据完整性。

6.5.5 通信保密性

信息系统与外部网络进行通信时，在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证，并对通信过程中的用户身份鉴别信息等敏感信息字段进行加密。

6.5.6 软件容错

要求如下：

a）应提供数据有效性检验功能，保证通过人机接口输入或通信接口输入的数据长度、格式、范围、数据类型等符合设定要求，防止诸如SQL注入、跨站攻击、溢出攻击等恶意行为，对非法输入进行明确的错误提示并报警；

b）当软件发生故障时，信息系统应能够继续提供部分功能，确保能够实施使系统恢复正常或保护数据安全的必要措施。

6.5.7 资源控制

要求如下：

a）当信息系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b）应能够对应用系统的最大并发会话连接及单个帐户的多重并发会话进行限制。

6.6 数据安全与备份恢复

6.6.1 数据完整性

应能够检测到用户身份鉴别信息、调度信息、播出节目等重要业务数据在传输过程中完整性受到破坏。

6.6.2 数据保密性

应采用加密或其他有效措施实现用户身份鉴别信息的存储保密性。

6.6.3 备份与恢复

应能够对重要业务信息进行备份和恢复。

7 第三级防护要求

7.1 基础网络安全

7.1.1 结构安全

要求如下：

a）应保证主要网络设备的业务处理能力和网络带宽具备冗余空间，满足业务高峰期需要；

b）应为信息系统的核心交换机、汇聚交换机等关键网络设备配置冗余，避免关键节点存在单点故障；

c）应根据各信息系统的播出相关度进行层次化网络结构设计，形成网络纵深防护体系，新闻制播系统中的直播演播室系统、播出整备系统、播出系统等播出直接相关系统应位于纵深结构内部，系统内部不应通过无线方式进行组网；

d）应根据信息系统功能、业务流程、网络结构层次、业务服务对象等合理划分网络安全域；

e）安全域内应根据业务类型、业务重要性、物理位置等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；

f）同一安全域内重要网段与其它网段之间应采取可靠的技术隔离手段；

g）应绘制与当前运行情况相符的网络拓扑结构图。

7.1.2 安全审计

要求如下：

a）应对关键网络设备的运行状况、用户行为等重要事件进行日志记录；

b）审计记录应包括事件的日期、时间、用户名、IP 地址、事件类型、事件是否成功等；

c）应保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录至少保存 90 天；

d）应定期对审计记录进行分析，以便及时发现异常行为；

e）应为安全管理中心提供集中管理的接口。

7.1.3 网络设备防护

要求如下：

a）应对登录网络设备的用户进行身份鉴别，身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换，用户名和口令禁止相同；

b）主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；

c）应具有登录失败处理功能，可采取结束会话、限制非法登录次数和连接超时自动退出等措施；

d）应该对网络设备进行基本安全配置，关闭不必要的服务和端口；

e）应对网络设备的管理员登录地址进行限制，仅允许指定 IP 地址或 IP 段访问；

f）当对网络设备进行远程管理时，应采用HTTPS、SSH等安全的远程管理手段，防止用户身份鉴别信息在网络传输过程中被窃听；

g）应实现网络设备特权用户的权限分离；

h）能够通过SNMP V3及以上版本或其它安全的网络管理协议提供网络设备的监控与管理接口。

7.2 边界安全

7.2.1 访问控制

要求如下：

a）应在网络边界部署访问控制设备，根据安全策略提供明确的允许/拒绝访问，控制粒度为**IP地址段及端口级**；

b）应对进出网络的信息进行过滤，实现对应用层协议命令级的控制，仅允许HTTP、FTP、TELNET、SSH等信息系统使用的协议，禁止一切未使用的通信协议和端口；

c）重要网段应采用IP与MAC地址绑定或其它网络准入控制措施等技术手段防止地址欺骗；

d）通过外部网络对信息系统进行访问时应使用安全方式接入，根据需要采用数字证书等强制认证方式，并对用户权限进行管理，控制粒度为用户级。

e）应限制与外部网络连接的最大流量数及网络连接数，按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要业务；

7.2.2 安全数据交换

要求如下：

a）播出系统与其它信息系统之间进行数据交换时，应对文件类型及格式进行限定；

b）应限定可以通过移动介质交换数据的主机，所有通过移动介质上载的内容应经过两种以上的防恶意代码产品进行恶意代码检查后，方可正式上载到内部网络；对蓝光、P2等专业移动介质可通过特定的防护机制进行上载；

c）信息系统与外部网络进行数据交换时，应通过数据交换区或专用数据交换设备完成内外网数据的安全交换；

d）数据交换区对外应通过访问控制设备与外部网络进行安全隔离，对内应采用安全的方式进行数据交换，必要时可通过协议转换的手段，以信息摆渡的方式实现数据交换；

7.2.3 入侵防范

要求如下：

a）应在**信息系统的网络边界**处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫攻击等，**播出整备系统、播出系统等信息系统的边界可根据需要进行部署；**

b）当检测到攻击行为时，记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

7.2.4 恶意代码防范

要求如下：

a）应在**信息系统的网络边界**处进行恶意代码检测和清除，并维护恶意代码库的升级和检测系统的更新，**播出整备系统、播出系统等播出直接相关系统的边界可根据需要进行部署**；

b）防恶意代码产品应与信息系统内部防恶意代码产品具有不同的恶意代码库。

7.2.5 安全审计

要求如下：

a）应在与外部网络连接的网络边界处进行数据通信行为审计；

b）审计记录应包括事件的日期、时间、用户名、IP 地址、事件类型、事件是否成功等；

c）应保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录至少保存 90 天；

d）应定期对审计记录进行分析，以便及时发现异常行为；

e）应为安全管理中心提供集中管理的接口。

7.2.6 边界完整性

要求如下：

a）应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；

b）应能够对内部网络用户私自联到外部网络的行为进行检查，**准确定出位置，并对其进行有效阻断。**

7.3 终端系统安全

7.3.1 身份鉴别

应对登录终端操作系统的用户进行身份标识和鉴别，口令应有复杂度要求并定期更换，用户名和口令禁止相同。

7.3.2 访问控制

应依据安全策略控制用户对资源的访问，禁止通过 USB、**光驱**等外设进行数据交换，关闭不必要的服务和端口等。

7.3.3 安全审计

要求如下：

a）应对系统中的重要终端进行审计，审计粒度为用户级；

b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用及其它与审计相关的信息；

c）审计记录至少应包括事件的日期、时间、类型、用户名、访问对象、结果等；

d）应保护审计进程，避免受到未预期的中断；

e）应保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录至少保存 90 天；

f）应定期对审计记录进行分析，以便及时发现异常行为；

g）应为安全管理中心提供集中管理的接口。

7.3.4 入侵防范

要求如下：

a）操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并保持系统补丁及时得到更新；

b）通过设置升级服务器等方式定期更新操作系统补丁；新闻制播系统、播出整备系统、播出系统等播出直接相关系统的终端可根据需要进行更新。

7.3.5 恶意代码防范

应部署具有统一集中管理功能的防恶意代码软件，并定期更新防恶意代码软件版本和恶意代码库；新闻制播系统、播出整备系统、播出系统等播出直接相关系统的终端可根据需要进行部署。

7.4 服务端系统安全

7.4.1 身份鉴别

要求如下：

a）应对登录操作系统和数据库系统的用户进行身份标识和鉴别，应为不同用户分配不同的用户名，不能多人使用同一用户名；

b）系统管理用户身份鉴别信息应具有不易被冒用的特点，口令应定期更换，用户名和口令禁止相同；

c）应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

d）当对服务器进行远程管理时，应采用HTTPS、SSH等安全的远程管理手段，防止用户身份鉴别信息在网络传输过程中被窃听；

e) 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

7.4.2 访问控制

要求如下：

a）应启用访问控制功能，依据安全策略控制用户对资源的访问，根据需要禁止通过USB、光驱等外设进行数据交换，关闭不必要的服务和端口等；

b）应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；

c）应实现操作系统和数据库系统特权用户的权限分离；

d）应限制默认帐户的访问权限，重命名 Windows 系统默认帐户，修改帐户的默认口令；

e）应及时删除多余的、过期的帐户，避免共享帐户的存在；

f）应对高风险服务器的重要信息资源设置敏感标记，并应依据安全策略严格控制用户对有敏感标记的重要信息资源的操作。

7.4.3 安全审计

要求如下：

a）应对系统中的接口服务器、Web服务器、应用服务器、数据库服务器等重要服务器的操作系统和数据库进行审计，审计粒度为用户级；

b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用及**其它与审计相关的信息**；

c）审计记录至少应包括事件的日期、时间、类型、用户名、客户端IP地址、访问对象、结果等；

d）应保护审计进程，避免受到未预期的中断；

e）应保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录至少保存 90 天；

f）应定期对审计记录进行分析，以便及时发现异常行为；

g）应为安全管理中心提供集中管理的接口。

7.4.4 入侵防范

要求如下：

a）操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，关闭不必要的端口和服务；

b）**通过设置升级服务器等方式**定期更新操作系统补丁，新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器可根据需要进行更新；

c）应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

d）应能够对操作系统重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。

7.4.5 恶意代码防范

应部署具有统一管理功能的防恶意代码软件，并定期更新防恶意代码软件版本和恶意代码库；新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器可根据需要进行部署和更新。

7.4.6 资源控制

要求如下：

a）应通过设定终端接入方式、网络地址范围等条件限制终端登录；

b）应根据安全策略设置登录终端的操作超时锁定；

c）应限制单个用户对系统资源的最大或最小使用限度；

d）应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

7.4.7 冗余配置

新闻制播系统、播出整备系统、播出系统等播出直接相关系统的核心服务器应具有冗余配置，**并能够在发生故障时进行及时切换。**

7.5 应用安全

7.5.1 身份鉴别

要求如下：

a) 应提供独立的登录控制模块，或者将登录控制模块集成到统一的门户认证系统中，应对登录应用系统的用户进行身份标识和鉴别，应为不同用户分配不同的用户名，不能多人使用同一用户名；

b) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识；

c) 系统管理用户身份鉴别信息应具有不易被冒用的特点，口令应定期更换，用户名和口令禁止相同；

d) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

e) 应对管理用户和重要业务操作用户采用两种或两种以上组合的鉴别技术对其身份进行鉴别。

7.5.2 访问控制

要求如下：

a) 应启用访问控制功能，依据安全策略控制用户对资源的访问，控制粒度为文件、数据库表级；

b) 删除临时帐户和测试帐户，重命名默认帐户，修改其默认口令，限制其访问权限，不允许匿名用户登录；

c) 访问控制的覆盖范围应包括与资源访问相关的主体（信息系统用户）、客体（用户所访问的数据）及它们之间的操作（读、写、修改、删除等）；

d) 应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。如系统管理员不建议拥有系统审计员权限、一般系统用户不建议拥有系统管理员权限等；

e) 应对高风险服务器的重要信息资源设置敏感标记，并应依据安全策略严格控制用户对有敏感标记的重要信息资源的操作。

7.5.3 安全审计

要求如下：

a) 应能提供覆盖到每个用户的审计功能；

b) 审计内容应包括用户登录、修改配置、核心业务操作等重要行为，以及系统资源的异常使用等；

c) 审计记录至少应包括事件的日期和时间、事件类型、客户端 IP 地址、描述和结果等；

d) 应保证无法单独中断审计进程；

e) 应保证无法删除、修改或覆盖审计记录，审计记录至少保存 90 天；

f) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能；

g) 应为安全管理中心提供集中管理的接口。

7.5.4 通信完整性

应采用校验码技术、特定的音视频文件格式、特定协议或等同强度的技术手段等进行传输，保证通信过程中的数据完整性。

7.5.5 通信保密性

信息系统与外部网络进行通信时，在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证，并对通信过程中的用户身份鉴别信息等敏感信息字段进行加密。

7.5.6 软件容错

要求如下：

a) 应提供数据有效性检验功能，保证通过人机接口输入或通信接口输入的数据长度格式、范围、数据类型等符合设定要求，防止诸如 SQL 注入、跨站攻击、溢出攻击等恶意行为，对非法输入进行明确的错误提示并报警；

b) 应提供自动保护功能，当故障发生时自动保护当前状态，保证系统能够进行恢复。

7.5.7 资源控制

要求如下：

a) 当信息系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b) 应能够对应用系统的最大并发会话连接及单个帐户的多重并发会话进行限制；

c) 应能够对一个时间段内可能的并发会话连接数进行限制；

d) 应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；

e) 应能够对系统服务水平降低到预先规定的最小值进行检测和报警。

7.6 数据安全与备份恢复

7.6.1 数据完整性

应能够检测到**系统管理数据**、用户身份鉴别信息、调度信息、播出节目等重要业务数据在传输**和存储**过程中完整性受到破坏，**并在检测到其完整性遭到破坏时采取必要的恢复措施。**

7.6.2 数据保密性

应采用加密或其他有效措施实现用户身份鉴别信息的存储保密性。

7.6.3 备份与恢复

要求如下：

a) 应能够对重要信息进行本地备份和恢复，完全数据备份至少每周一次，增量备份或差分备份至少每天一次，备份介质应在数据执行所在场地外存放；

b) 应能够对重要信息进行异地备份，利用通信网络将关键数据定时批量传送至备用场地。

7.7 安全管理中心

7.7.1 运行监测

要求如下：

a) 应对网络链路状态、信息系统的核心交换机、汇聚交换机等关键网络设备状态、设备端口状态、端口 IP 地址、关键节点的网络流量等进行监控；

b) 应对信息系统重要服务器的运行状态、CPU 使用率、内存的使用率、网络联网情况等进行监控；

c) 应对信息系统数据库的运行状态、进程占用 CPU 时间及内存大小、配置和告警数据等进行

监控；

d）应对信息系统重要应用软件的运行状态、响应时间等进行监控；

e）应对终端的非法接入及非法外联情况进行监控；

f）应对监控的异常情况进行报警，并对报警记录进行分析，采取必要的应对措施。

7.7.2 安全管理

要求如下：

a）应对信息系统的恶意代码、补丁升级等进行集中统一管理；

b）应对网络设备、服务器、应用系统、安全设备等的安全事件信息进行关联分析及风险预警；

c）信息系统网络设备、终端、服务器以及应用等保持时钟同步。

7.7.3 审计管理

要求如下：

a）应对基础网络、边界安全、服务器及应用系统的安全审计进行集中管理；

b）应对审计记录进行统计、查询、分析及生成审计报表；

c）应对 90 天以上的审计日志进行归档，归档日志至少保存一年以上。

8 第四级防护要求

8.1 基础网络安全

8.1.1 结构安全

要求如下：

a）应保证**网络设备**的业务处理能力和网络带宽具备冗余空间，满足业务高峰期需要；

b）应为信息系统的**网络设备和通信线路**配置冗余，避免关键节点存在单点故障；

c）应根据各信息系统的播出相关度进行层次化网络结构设计，形成网络纵深防护体系，四级信息系统应位于纵深结构内部，系统内部不应通过无线方式进行组网；

d）应根据信息系统功能、业务流程、网络结构层次、业务服务对象等合理划分网络安全域；

e）安全域内应根据业务类型、业务重要性、物理位置等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；

f）同一安全域内重要网段与其他网段之间应采取可靠的技术隔离手段；

g）应绘制与当前运行情况相符的网络拓扑结构图。

8.1.2 安全审计

要求如下：

a）应对**网络设备**的运行状况、用户行为等重要事件进行日志记录；

b）审计记录应包括事件的日期、时间、用户名、IP 地址、事件类型、事件是否成功等；

c）应定期对审计记录进行分析，**及时发现异常行为，并生成审计报表；**

d）应提供安全审计记录存储与保护等功能，审计记录应无法被删除、修改或覆盖等，审计记录至少保存 90 天；

e）应为安全管理中心提供集中管理的接口。

8.1.3 网络设备防护

要求如下：

a）应对登录网络设备的用户进行身份鉴别，身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换，用户名和口令禁止相同；

b) 主要**网络设备**应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别，**身份鉴别信息至少有一种是不可伪造的**；

c) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

d) 应该对网络设备进行基本安全配置，关闭不必要的服务和端口；

e) 应对网络设备的管理员登录地址进行限制，**至少控制到 IP 地址**；

f) 当对网络设备进行远程管理时，应采用 HTTPS、SSH 等安全的远程管理手段，防止用户身份鉴别信息在网络传输过程中被窃听；

g) 应实现网络设备特权用户的权限分离；

h) 能够通过 SNMP V3 及以上版本或其它安全的网络管理协议提供网络设备的监控与管理接口。

8.2 边界安全

8.2.1 访问控制

要求如下：

a) 应在网络边界部署访问控制设备，启用访问控制功能；

b) 应对进出网络的信息进行过滤，实现对应用层协议命令级的控制，仅允许 HTTP、FTP、TELNET、SSH 等信息系统使用的协议，禁止一切未使用的通信协议和端口；

c) 重要网段应采用 IP 与 MAC 地址绑定或其它网络准入控制措施等技术手段防止地址欺骗。

8.2.2 安全数据交换

要求如下：

a) 播出系统与其它信息系统之间进行数据交换时，应对文件类型及格式进行限定；

b) 应限定可以通过移动介质交换数据的主机，所有通过移动介质上载的内容应经过两种以上的防恶意代码产品进行恶意代码检查后，方可正式上载到内部网络；对蓝光、P2等专业移动介质可通过特定的防护机制进行上载；

c) 应在网络边界处对媒体数据和其它数据进行区分，视频媒体数据外的其它数据应通过协议转换的手段，以信息摆渡的方式实现数据交换。

8.2.3 入侵防范

要求如下：

a) **可根据需要**在信息系统的网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；

b) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警**并自动采取相应动作。**

8.2.4 恶意代码防范

要求如下：

a) 应在信息系统的网络边界处对媒体数据和信息数据进行区分，根据需要对信息数据进行恶意代码检测和清除，并利用离线更新、手工更新的方式进行恶意代码库更新；

b) 防恶意代码产品应与信息系统内部防恶意代码产品具有不同的恶意代码库。

8.2.5 边界完整性

要求如下：

a) 应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；

b) 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

8.3 终端系统安全

8.3.1 身份鉴别

应对登录终端操作系统的用户进行身份标识和鉴别，口令应有复杂度要求并定期更换，用户名和口令禁止相同；

8.3.2 访问控制

应依据安全策略控制用户对资源的访问，禁止通过 USB、光驱等外设进行数据交换，关闭不必要的服务和端口等。

8.3.3 安全审计

要求如下：

a) 应对系统中的重要终端进行审计，审计粒度为用户级；

b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用及其它与审计相关的信息；

c) 审计记录至少应包括事件的日期、时间、类型、用户名、访问对象、结果等；

d) 应保护审计进程，避免受到未预期的中断；

e) 应保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录至少保存 90 天；

f) 应定期对审计记录进行分析，以便及时发现异常行为；

g) 应为安全管理中心提供集中管理的接口。

8.3.4 入侵防范

要求如下：

a) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序；

b) **可根据需要利用离线更新、手工更新的方式进行操作系统补丁的更新。**

8.3.5 恶意代码防范

可根据需要部署具有统一集中管理功能的防恶意代码软件，**并利用离线更新、手工更新的方式根据需要进行恶意代码库更新。**

8.4 服务端系统安全

8.4.1 身份鉴别

要求如下：

a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别，应为不同用户分配不同的用户名，不能多人使用同一用户名；

b) 系统管理用户身份鉴别信息应具有不易被冒用的特点，口令应定期更换，用户名和口令禁止相同；

c) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

d) 当对服务器进行远程管理时，应采用 HTTPS、SSH 等安全的远程管理手段，防止用户身份鉴别信息在网络传输过程中被窃听；

e) 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，**身份鉴别信息至少有一**

种是不可伪造的。

8.4.2 安全标记

应对接口服务器等系统边界的高风险服务器的主体和客体设置敏感标记。

8.4.3 访问控制

要求如下：

a) 应启用访问控制功能，依据安全策略控制用户对资源的访问，根据需要禁止通过 USB、光驱等外设进行数据交换，关闭不必要的服务和端口等;;

b) 应启用强制访问控制功能，依据安全策略和敏感标记控制主体对客体的访问，控制粒度应达到主体为用户级或进程级，客体为文件、数据库表、记录和字段级；

c) 应根据管理用户的角色分配权限，实现管理用户的权限分离，**仅授予管理用户所需的最小权限；**

d) 应实现操作系统和数据库系统特权用户的权限分离；

e) 应限制默认帐户的访问权限，重命名 Windows 系统默认帐户，修改帐户的默认口令；

f) 应及时删除多余的、过期的帐户，避免共享帐户的存在。

8.4.4 安全审计

要求如下：

a) 应对系统中的接口服务器、Web 服务器、应用服务器、数据库服务器等重要服务器的操作系统和数据库进行审计，审计粒度为用户级；

b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用及其它与审计相关的信息；

c) 审计记录至少应包括事件的日期、时间、类型、用户名、客户端 IP 地址、访问对象、结果等；

d) 应保护审计进程，避免受到未预期的中断；

e) 应保护审计记录，避免受到未预期的删除、修改或覆盖等，审计记录至少保存 90 天；

f) 应定期对审计记录进行分析，以便及时发现异常行为。

g) 应为安全管理中心提供集中管理的接口。

8.4.5 入侵防范

要求如下：

a) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，关闭不必要的端口和服务；

b) **可根据需要利用离线更新、手工更新的方式进行操作系统补丁的更新；**

c) 应能够检测到对服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

d) 应能够对操作系统重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。

8.4.6 恶意代码防范

可根据需要部署具有统一集中管理功能的防恶意代码软件，**并利用离线更新、手工更新的方式根据需要进行恶意代码库更新。**

8.4.7 资源控制

要求如下：

a）应通过设定终端接入方式、网络地址范围等条件限制终端登录；

b）应根据安全策略设置登录终端的操作超时锁定；

c）应限制单个用户对系统资源的最大或最小使用限度；

d）应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

8.4.8 冗余配置

业务服务器应具有冗余配置，并能够在发生故障时进行及时切换。

8.5 应用安全

8.5.1 身份鉴别

要求如下：

a）应提供独立的登录控制模块，或者将登录控制模块集成到统一的门户认证系统中，应对登录应用系统的用户进行身份标识和鉴别，应为不同用户分配不同的用户名，不能多人使用同一用户名；

b）应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识；

c）系统管理用户身份鉴别信息应具有不易被冒用的特点，口令应定期更换，用户名和口令禁止相同；

d）应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

e）应对管理用户和重要业务操作用户采用两种或两种以上组合的鉴别技术对其身份进行鉴别，**其中一种是不可伪造的。**

8.5.2 安全标记

应对接口服务器等系统边界的高风险服务器承载的业务应用的主体和客体设置安全标记。

8.5.3 访问控制

要求如下：

a）应启用**自主**访问控制功能，依据安全策略控制用户对资源的访问，控制粒度为文件和数据库表级；

b）删除临时帐户和测试帐户，重命名默认帐户，修改其默认口令，限制其访问权限，不允许匿名用户登录；

c）自主访问控制的覆盖范围应包括与资源访问相关的主体（信息系统用户）、客体（用户所访问的数据）及它们之间的操作（读、写、修改、删除等）；

d）应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。如系统管理员不建议拥有系统审计员权限、一般系统用户不建议拥有系统管理员权限等；

e）应通过比较安全标记来确定授予还是拒绝主体对客体的访问。

8.5.4 安全审计

要求如下：

a）应能提供覆盖到每个用户的审计功能；

b）审计内容应包括用户登录、修改配置、核心业务操作等重要行为，以及系统资源的异常使用等；

c）审计记录至少应包括事件的日期和时间、事件类型、客户端 IP 地址、描述和结果等；

d）应保证无法单独中断审计进程；

e）**提供安全审计记录存储与保护等功能，**审计记录应无法被删除、修改或覆盖等，审计记录至少保存 90 天；

f）应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能；

g）应为安全管理中心提供集中管理的接口。

8.5.5 通信完整性

应采用校验码技术、特定的音视频文件格式、特定协议或等同强度的技术手段等进行传输，保证通信过程中的数据完整性。

8.5.6 软件容错

要求如下：

a）应提供数据有效性检验功能，保证通过人机接口输入或通信接口输入的数据长度格式、范围、数据类型等符合设定要求，防止诸如 SQL 注入、跨站攻击、溢出攻击等恶意行为，对非法输入进行明确的错误提示并报警；

b）应提供自动保护功能，当故障发生时自动保护当前状态，保证系统能够进行恢复。

8.5.7 资源控制

要求如下：

a）当信息系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b）应能够对应用系统的最大并发会话连接及单个帐户的多重并发会话进行限制；

c）应能够对一个时间段内可能的并发会话连接数进行限制；

d）应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；

e）应能够对系统服务水平降低到预先规定的最小值进行检测和报警。

8.6 数据安全与备份恢复

8.6.1 数据完整性

要求如下：

a）应能够检测到系统管理数据、用户身份鉴别信息、调度信息、播出节目等重要业务数据在传输和存储过程中完整性受到破坏，并在检测到其完整性遭到破坏时采取必要的恢复措施；

b）应避免来自基于通用通信协议的攻击破坏数据完整性，可采用对信息系统的网络边界处的重要通信提供专用通信协议或安全通信协议服务等方式。

8.6.2 数据保密性

应采用加密或其他有效措施实现用户身份鉴别信息的存储保密性。

8.6.3 备份与恢复

要求如下：

a）应能够对重要信息进行本地备份和恢复，完全数据备份至少每周一次，增量备份或差分备份至少每天一次，备份介质应在数据执行所在场地外存放；

b）应建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备，提供业务应用的及时切换；

c）应能够对重要信息进行异地备份，利用通信网络将关键数据定时批量传送至备用场地；

d）应提供数据存储系统的硬件冗余，保证系统的高可用性。

8.7 安全管理中心

8.7.1 运行监测

要求如下：

a）应对网络链路状态、信息系统的核心交换机、汇聚交换机等关键网络设备状态、设备端口状态、端口 IP 地址、关键节点的网络流量等进行监控；

b）应对信息系统重要服务器的运行状态、CPU 使用率、内存的使用率、网络联网情况等进行监控；

c）应对信息系统数据库的运行状态、进程占用 CPU 时间及内存大小、配置和告警数据等进行监控；

d）应对信息系统重要应用软件的运行状态、响应时间等进行监控；

e）应对终端的非法接入及非法外联情况进行监控；

f）应对监控的异常情况进行报警，并对报警记录进行分析，采取必要的应对措施。

8.7.2 安全管理

要求如下：

a）应对信息系统的恶意代码、补丁升级等进行集中统一管理；

b）应对网络设备、服务器、应用系统、安全设备等的安全事件信息进行关联分析及风险预警；

c）信息系统网络设备、终端、服务器以及应用系统等保持时钟同步。

8.7.3 审计管理

要求如下：

a）应对基础网络、边界安全、服务器及应用系统的安全审计进行集中管理；

b）应对审计记录进行统计、查询、分析及生成审计报表；

c）应对 90 天以上的审计日志进行归档，归档日志至少保存三年以上。

9 第五级防护要求（略）

10 通用物理安全要求

10.1 物理位置的选择

要求如下：

a）机房的位置选择应符合《电子信息系统机房设计规范》（GB50174）的相关规定；

b）机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；

c）机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁，远离产生粉尘、油烟、有害气体以及生产或贮存具有腐蚀性、易燃、易爆物品的工厂、仓库、堆场等。

10.2 物理访问控制

要求如下：

a）信息系统机房出入口应设置电子门禁系统，控制、鉴别和记录进入的人员；第四级信息系统机房出入口还应安排专人值守；

b）需进入播出机房的来访人员应经过申请和审批流程，并限制和监控其活动范围。

10.3 防盗窃和防破坏

要求如下：

a）应将设备或主要部件进行固定，并设置明显的不易除去的标记；

b）应将公共区域信号线缆铺设隐蔽处，可铺设在地下或管道；

c）应利用光、电等技术设置机房防盗报警系统；

d）应在与播出相关的机房设置安防监控报警系统。

10.4 机房环境

要求如下：

a）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；

b）机房应有防水防潮措施，应充分考虑水管泄漏和凝露的可能性，并做好相应的预防措施；

c）第四级信息系统机房应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警；

d）机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内；

e）应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

f）电源线和通信线缆应隔离铺设，避免互相干扰。

10.5 机房消防设施

要求如下：

a）机房消防设施的配置应符合GY 5067的有关规定；

b）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；

c）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；

d）机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

10.6 电力供应

机房的配电应符合“广播电视安全播出管理规定实施细则”的相关要求。

11 通用管理安全要求

11.1 总要求

要求如下：

a）应制定信息安全工作的总体方针和安全策略，说明安全工作的总体目标、范围、原则和安全框

架等；

b）应成立指导和管理信息安全工作的领导小组，设立信息安全管理工作的职能部门；

c）应制定各项信息安全制度和操作规程，明确信息安全管理各项要求，形成由安全方针、管理制度、细化流程等构成的全面的信息安全管理制度体系，使等级保护工作常态化、制度化。

11.2 安全管理机构

11.2.1 岗位设置

要求如下：

a）应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；

b）应设立信息安全管理工作的职能部门，负责信息安全各项工作的组织和落实，配备专职安全管理员；

c）具有第三级及以上信息系统的单位应设立系统管理员、网络管理员、安全管理员等岗位，并明确各个工作岗位的职责、分工和技能要求；

d）应制定文件明确安全管理机构各个部门和岗位的职责。

11.2.2 授权和审批

要求如下：

a）应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；

b）应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；

c）应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；

d）应记录审批过程并保存审批文档。

11.2.3 沟通和合作

要求如下：

a）应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题；

b）应加强与系统内外相关工作单位的合作与沟通，确保信息安全各项工作的顺利开展；

c）具有三级及以上信息系统的单位应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。

11.2.4 审核和检查

要求如下：

a）安全管理员应负责定期进行信息安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；

b）应定期进行全面信息安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

c）信息安全主管部门应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。

11.2.5 制度管理

要求如下：

a）应建立信息安全管理制度、操作规程等从访问控制、系统设计、系统建设、系统验收、系统运维、应急处置、人员管理、文件档案管理、审核检查等方面规范各项信息安全管理工作；

b）信息安全管理部门负责制定信息安全管理制度和操作规程，并进行版本控制；

c）应组织专家和相关部门人员对安全管理制度和操作规程进行论证和审定，并定期对其合理性和适用性进行审定，根据需要进行修订；

d）信息安全管理制度应通过有效方式发布至所有相关部门和岗位。

11.3 人员安全管理

11.3.1 人员上岗

要求如下：

a）应规范人员上岗过程，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；

b）应签署保密协议和岗位安全协议。

11.3.2 人员离岗

要求如下：

a）应规范人员离岗过程，及时终止离岗员工的所有访问权限；

b）应取回各种身份证件、钥匙、徽章等以及单位提供的软硬件设备；

c）应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。

11.3.3 培训与考核

要求如下：

a）应定期对各类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；

b）应对信息安全各相关岗位的人员定期进行安全技能、政策及安全认知的考核；

c）应对信息安全培训和考核情况进行记录并保存。

11.3.4 外部人员访问管理

要求如下：

a）应确保在外部人员访问受控区域前先提出申请，批准后由专人全程陪同或监督，并登记备案；

b）应对外部人员允许访问的区域、系统、设备、信息等内容进行书面的规定，并按照规定执行。

11.4 系统建设管理

11.4.1 系统定级

按照国家和行业标准、规范合理确定信息系统的边界和安全保护等级，并根据要求进行信息系统定级评审、审批、报备工作。

11.4.2 安全方案设计

要求如下：

a）根据信息系统的等级划分情况，应由专门的部门对信息系统的安全建设进行总体规划，统一考虑信息安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划、远期和近期建设计划等；

b）应根据国家和行业标准、规范合理设计信息系统的信息安全方案和策略，制定详细的建设方案；

c）应组织相关部门和有关安全技术专家对信息安全的规划、建设方案等进行论证和审定，并且经过批准后，才能正式实施；

d）应根据等级测评、安全评估的结果调整和修订信息安全的规划、建设方案等。

11.4.3 产品采购和使用

要求如下：

a）应确保安全产品采购和使用符合国家的有关规定；

b）应确保密码产品采购和使用符合国家密码主管部门的要求；

c）采购前应对产品进行选型测试，确定其适用性后方可采购。

11.4.4 自行软件开发

要求如下：

a）应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制；

b）应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

c）应制定代码编写安全规范，要求开发人员参照规范编写代码，并审查软件中可能存在的后门漏洞等；

d）应确保提供软件设计的相关文档和使用指南，并由专人负责保管；

e）应确保对程序资源库的修改、更新、发布进行授权和批准。

11.4.5 外包软件开发

要求如下：

a）应根据国家、行业相关标准和开发需求检测软件质量；

b）应在软件安装之前检测软件包中可能存在的恶意代码；

c）应要求开发单位提供软件设计的相关文档和使用指南；

d）应要求开发单位提供软件源代码，并审查软件中可能存在的后门漏洞等。

11.4.6 工程实施

要求如下：

a）应指定或授权专门的部门或人员负责工程实施过程的管理；

b）应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程；

c）应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。

11.4.7 测试验收

要求如下：

a）应委托具有资质的第三方对系统进行安全性测试，并出具安全性测试报告；

b）在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；

c）应对系统测试验收的控制方法和人员行为准则进行书面规定；

d）应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；

e）应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

11.4.8 系统交付

要求如下：

a）应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

b）应对负责系统运行维护的技术人员进行相应的技能培训；

c）应提供系统建设过程中的文档和指导用户进行系统运行维护的文档。

11.4.9 系统备案

要求如下：

a）应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用；

b）应将系统等级及相关材料报系统主管部门备案；

c）应将系统等级及其他要求的备案材料报相应公安机关备案。

11.4.10 等级测评

要求如下：

a）在系统运行过程中，应按照国家和行业标准、规范要求对系统进行等级测评，发现不符合相应等级保护标准要求的及时整改；

b）应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；

c）应选择国家和行业认可的信息安全资质单位进行等级测评。

11.4.11 安全服务商选择

要求如下：

a）应确保安全服务商的选择符合国家和行业的有关规定；

b）应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；

c）应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。

11.5 系统运维管理

11.5.1 环境管理

要求如下：

a）应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；

b）应指定部门负责机房安全，对机房的出入、服务器的开机或关机等工作进行管理；

c）应建立机房安全管理制度，规范机房物理访问、机房环境安全、工作人员行为等。

11.5.2 资产管理

要求如下：

a）应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

b）应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；

c）应根据资产的重要程度对资产进行标识管理，并选择相应的管理措施；

d）应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

11.5.3 介质管理

要求如下：

a）应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；

b）应确保介质存放在安全的环境中，并根据所承载数据和软件的重要程度对介质进行分类和标识管理，进行相应的控制和保护；

c）应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对经批准带出工作环境的存储介质进行登记和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不应自行销毁；

d）应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同。

11.5.4 设备管理

要求如下：

a）应定期对信息系统相关的各种设备、线路等进行维护；

b）应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；

c）应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；

d）应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备的启动/停止、加电/断电等操作；

e）应确保信息处理设备必须经过审批才能带离机房或办公地点。

11.5.5 网络安全管理

要求如下：

a）应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；

b）应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；

c）应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；

d）应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补，播出直接相关的信息网络根据需要进行；

e）应保证所有与外部系统的连接均得到授权和批准；

f）应定期检查信息系统非法接入和非法外联的行为。

11.5.6 系统安全管理

要求如下：

a）应根据业务需求和系统安全分析确定系统的访问控制策略；

b）应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装，播出直接相关的信息系统根据需要进行；

c）应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定；

d）应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；

e）应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；

f）应定期对运行日志和审计数据进行分析，以便及时发现异常行为。

11.5.7 恶意代码防范管理

要求如下：

a）应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；

b）应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定；

c）应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对防恶意代码产品上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

11.5.8 密码管理

应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。

11.5.9 变更管理

要求如下：

a）应确认系统中要发生的变更，并制定变更方案；

b）应建立变更管理制度，系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施后将变更情况向相关人员通告；

c）应建立变更控制的申报和审批文件化程序，对变更影响进行分析，记录变更实施过程，并妥善保存所有文档和记录；

d）应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练；

e）与播出直接相关的信息系统中，操作系统升级、应用软件升级、恶意代码库更新等应在测试环境中测试通过，确认所升级内容对安全播出没有影响，方可在信息系统中应用。

11.5.10 备份与恢复管理

要求如下：

a）应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b）应建立备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范；

c）应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

d）应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存；

e）三级及以上信息系统应定期测试恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

11.5.11 安全事件处置

要求如下：

a）应制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

b）按照国家和行业相关规定及时上报信息安全事件和可疑事件；

c）应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；

d）应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，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应妥善保存。

11.5.12 应急预案管理

要求如下：

a）应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、后处理等内容；

b）应根据系统变更、管理要求的变化等及时更新应急预案；

c）应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；

d）应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次；

e）应定期对应急预案进行演练。

参考文献

[1] GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
[2] GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南
[3] GB/T 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求
[4] 总局62号令《广播电视安全播出管理规定》及各专业实施细则