应在关键网络节点处监视网络攻击行为。

7.1.2.4 恶意代码防范

应在关键网络节点处进行恶意代码检测和清除，并维护恶意代码防护机制有效性，及时升级和更新特征库。

7.1.2.5 安全审计

要求如下：

a） 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b） 审计记录应包括事件的日期、时间、IP 地址、事件类型、事件是否成功及其他与审计相关的信息；
c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

7.1.2.6 可信验证

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

7.1.3 安全计算环境

7.1.3.1 身份鉴别

要求如下：

a） 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
b） 应启用登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
c） 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听，如：HTTPS、SSH、VPN 等。

7.1.3.2 访问控制

要求如下：

a） 应对登录的用户分配账户和权限；
b） 应重命名或删除默认账户，修改默认账户的默认口令；
c） 无法重命名或删除的默认账户，应阻止其直接远程登录；
d） 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
e） 应授予管理用户所需的最小权限，实现管理用户的权限分离；
f） 应限制未登录用户的使用权限，可对匿名用户使用记录进行追溯。

7.1.3.3 安全审计

要求如下：

a） 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b） 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

7.1.3.4 入侵防范

要求如下：

a） 应遵循最小安装的原则，仅安装需要的组件和应用程序；

b） 应关闭不需要的系统服务、默认共享和高危端口；

c） **应能通过漏洞扫描工具、人工漏洞排查等手段，发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；**

d） **应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；**

e） **应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求。**

7.1.3.5 恶意代码防范

应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。

7.1.3.6 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

7.1.3.7 数据完整性

应采用校验技术保证重要数据在传输过程中的完整性，包括但不限于调度信息、鉴别数据、重要业务数据和重要个人信息等。

7.1.3.8 数据备份恢复

要求如下：

a） 应提供重要数据的本地数据备份与恢复功能；

b） **应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备份场地。**

7.1.3.9 剩余信息保护

应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。

7.1.3.10 个人信息保护

要求如下：

a） **应仅采集和保存业务必需的用户个人信息；**

b） **应禁止未授权访问和非法使用用户个人信息。**

7.1.3.11 业务连续性保障

播出直接相关系统关键设备应配置冗余，当某节点设备出现故障时，切换到备份设备继续运行，切换过程不能对正常播出产生影响。

7.1.4 安全管理中心

7.1.4.1 系统管理

要求如下：

a） **应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；**

b） **应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。**

7.1.4.2 审计管理

要求如下：

a） **应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；**

b） **应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。**

7.2 云计算安全扩展要求

7.2.1 安全通信网络

7.2.1.1 网络架构

要求如下：

a） 应保证云计算平台不承载高于其安全保护等级的业务应用系统；

b） 应实现不同云服务客户虚拟网络之间的隔离；

c） **应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力。**

7.2.2 安全区域边界

7.2.2.1 访问控制

要求如下：

a） 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；

b） **应在不同等级的网络区域边界部署访问控制机制，并设置访问控制规则。**

7.2.2.2 入侵防范

要求如下：

a） **应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；**

b） **应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；**

c） **应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量。**

7.2.2.3 安全审计

要求如下：

a） **应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；**

b） **应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。**

7.2.3 安全计算环境

7.2.3.1 访问控制

要求如下：

a） 应保证当虚拟机迁移时，访问控制策略随其迁移；

b） 应允许云服务客户设置不同虚拟机之间的访问控制策略。

7.2.3.2 镜像和快照保护

要求如下：

a） **应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；**

b） **应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改。**

7.2.3.3 数据完整性和保密性

要求如下：

a） 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；

b） **应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；**

c） **应保证虚拟机镜像和快照文件备份在不同物理服务器；**

d） **应确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施。**

7.2.3.4 数据备份恢复

要求如下：

a） **云服务客户应在本地保存其业务数据的备份；**

b） **应提供查询云服务客户数据及备份存储位置的能力。**

7.2.3.5 剩余信息保护

要求如下：

a） **应保证虚拟机所使用的内存和存储空间回收时得到完全清除；**

b） **云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。**

7.3 移动互联安全扩展要求

7.3.1 安全区域边界

7.3.1.1 边界防护

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

7.3.1.2 访问控制

要求如下：

a） 无线接入设备应开启接入认证功能，并且禁止使用 WEP 方式进行认证，如使用口令，长度不小于 8 位字符；

b） **应保证无线网络通过受控的边界设备接入内部网络。**

7.3.1.3 入侵防范

要求如下：

a） **应能够检测到非授权无线接入设备和非授权移动终端的接入行为；**

b） **应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为；**

c） **应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；**

d） **应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等；**

e） **应禁止多个 AP 使用同一个认证密钥。**

7.3.2 安全计算环境

7.3.2.1 移动终端管控

要求如下：

a） **应保证移动终端安装、注册并运行终端管理客户端软件；**

b） **移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程数据擦除等；**

c） 发布直播数据的移动终端宜为专用终端。

7.3.2.2 移动应用管控

要求如下：

a） 应具有选择应用软件安装、运行的功能；

b） **应只允许指定证书签名的应用软件安装和运行；**

c） **专用移动应用软件应具备防二次打包工具篡改程序文件，以防止移动应用程序的代码、图片、配置、布局等被增加、修改或删除。**

8 第三级安全要求

8.1 安全通用要求

8.1.1 安全通信网络

8.1.1.1 网络架构

要求如下：

a） 应保证**网络设备**的业务处理能力满足业务高峰期需要；

b） 应保证网络各个部分的带宽满足业务高峰期需要；

c） 应根据系统功能、业务流程、网络结构层次、业务服务对象等因素划分不同网络区域，并按照方便安全管理和控制的原则为各网络区域分配地址；

d） 应避免将播出直接相关系统等重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；

e） **应具备通信线路、关键网络设备、关键安全设备和关键计算设备的硬件冗余，保证系统的可用性；**

f） **应具备不同路由的双链路接入保障；**

g） 应配备与实际运行情况相符的网络拓扑图。

8.1.1.2 通信传输

要求如下：

a） 应采用**校验技术、密码技术或特定协议转换技术**保证通信过程中数据的完整性；

b） **应采用密码技术或特定协议转换技术保证通信过程中数据的保密性。**

8.1.1.3 可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，**并在应用程序的关键执行环节进行动态可信验证**，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

8.1.2 安全区域边界

8.1.2.1 边界防护

要求如下：

a） 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；
b） **应能够对非授权设备私自联到内部网络的行为进行检查和限制；**
c） **应能够对内部用户非授权联到外部网络的行为进行检查和限制；**
d） **播出直接相关系统应禁止通过无线方式进行组网，非播出直接相关系统应限制无线网络的使用，强化无线网络区域边界防护措施，保证无线网络通过受控边界设备接入内部网络。**

8.1.2.2 访问控制

要求如下：

a） 应在网络边界根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
b） 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
c） 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
d） 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；
e） **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，对用户和权限进行管理，赋予最小访问权限，控制粒度为用户级；**
f） **应对进出网络的数据流实现基于应用协议和应用内容的访问控制；**
g） **宜在会话处于非活跃一定时间或会话结束后终止网络连接。**

8.1.2.3 **入侵防范**

要求如下：

a） **应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；**
b） **应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；**
c） **应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；**
d） **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。**

8.1.2.4 **恶意代码和垃圾邮件防范**

要求如下：

a） 应在关键网络节点处进行恶意代码检测和清除，并维护恶意代码防护机制有效性，及时升级和更新特征库；
b） **应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新；**
c） **部署在关键网络节点的防恶意代码产品宜与系统内部防恶意代码产品具有不同的恶意代码库。**

8.1.2.5 **安全审计**

要求如下：

a） 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b） 审计记录应包括事件的日期、时间、IP 地址、事件类型、事件是否成功及其他与审计相关的信息；
c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

d） **应能对播出控制操作行为、远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析；**

e） **应定期对审计记录进行分析，以便及时发现异常行为。**

8.1.2.6 可信验证

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，**并在应用程序的关键执行环节进行动态可信验证，**在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

8.1.3 安全计算环境

8.1.3.1 身份鉴别

要求如下：

a） 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

b） 应启用登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

c） 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听，如：HTTPS、SSH、VPN 等；

d） **应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。**

8.1.3.2 访问控制

要求如下：

a） 应对登录的用户分配账户和权限；

b） 应重命名或删除默认账户，修改默认账户的默认口令；无法重命名或删除的默认账户，应阻止其直接远程登录；

c） 应及时删除或停用多余的、过期的账户，避免共享账户的存在；

d） 应授予管理用户所需的最小权限，实现管理用户的权限分离；

e） **应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；**

f） **访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；**

g） **应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问；**

h） **应用系统应提示首次登录用户修改预设的默认口令；**

i） 应限制未登录用户的使用权限，可对匿名用户使用记录进行追溯；

j） **播出直接相关系统的特权命令（如播出文件调整，播出节目单调整）应在服务器或专用操作终端执行。**

8.1.3.3 **安全审计**

要求如下：

a） 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

b） 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

d） **应对审计进程进行保护，防止未经授权的中断。**

8.1.3.4 入侵防范

要求如下：

a） 应遵循最小安装的原则，仅安装需要的组件和应用程序；

b） 应关闭不需要的系统服务、默认共享和高危端口；

c） 应能通过漏洞扫描工具、人工漏洞排查等手段，发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

d） 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

e） 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

f） **应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。**

8.1.3.5 恶意代码防范

要求如下：

a） **应采用免受恶意代码攻击的技术措施或采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断；**

b） **通过移动介质进行数据上传时，应在移动介质接入前采用两种或两种以上病毒库对移动介质进行恶意代码查杀。**

8.1.3.6 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，**并在应用程序的关键执行环节进行动态可信验证，**在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

8.1.3.7 数据完整性

要求如下：

a） **采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于调度信息、鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要媒体内容数据和重要个人信息等；**

b） **采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要媒体内容数据和重要个人信息等。**

8.1.3.8 数据保密性

要求如下：

a） **应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；**

b） **应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。**

8.1.3.9 数据备份恢复

要求如下：

a） 应提供重要数据的本地数据备份与恢复功能，**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；**

b） 应提供异地数据**实时**备份功能，利用通信网络将重要数据实时备份至备份场地；

c） **应提供重要数据处理系统的热冗余，保证系统的高可用性；**
d） **建立敏感数据样本库并进行定期维护及时更新，支持其他应用通过多种接口方式使用。**

8.1.3.10 剩余信息保护

要求如下：
a） 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
b） **应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。**

8.1.3.11 个人信息保护

要求如下：
a） 应仅采集和保存业务必需的用户个人信息；
b） 应禁止未授权访问和非法使用用户个人信息；
c） **应具备用户个人信息全生命周期管理功能。**

8.1.3.12 业务连续性保障

要求如下：
a） **播出直接相关系统应保证节目传输链路的冗余，并能够在发生故障时切换；**
b） 播出直接相关系统关键设备应配置冗余，当某节点设备出现故障时，切换到备份设备继续运行，切换过程不能对正常播出产生影响。

8.1.4 安全管理中心

8.1.4.1 系统管理

要求如下：
a） 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；
b） 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

8.1.4.2 审计管理

要求如下：
a） 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
b） 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

8.1.4.3 安全管理

要求如下：
a） **应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；**
b） **应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。**

8.1.4.4 集中管控

要求如下：

a） **应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；**

b） **应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；**

c） **应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；**

d） **应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录留存时间符合国家和行业法律法规要求；**

e） **应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；**

f） **应具备网络安全实时监测、态势感知、风险预警、统一展示和安全事件应急处置的能力；**

g） **应保证系统范围内的时间由唯一确定的时钟产生，以保证各种数据的管理和分析在时间上的一致性。**

8.2 云计算安全扩展要求

8.2.1 安全通信网络

8.2.1.1 网络架构

要求如下：

a） 应保证云计算平台不承载高于其安全保护等级的业务应用系统；

b） 应实现不同云服务客户虚拟网络之间的隔离；

c） 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；

d） **应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；**

e） **应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务。**

8.2.2 安全区域边界

8.2.2.1 访问控制

要求如下：

a） 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；

b） 应在不同等级的网络区域边界部署访问控制机制，并设置访问控制规则。

8.2.2.2 入侵防范

要求如下：

a） 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

b） 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

c） 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；

d） **应在检测到网络攻击行为、异常流量情况时进行告警。**

8.2.2.3 安全审计

要求如下：

a） 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；

b） 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

8.2.3 安全计算环境

8.2.3.1 身份鉴别

要求如下：

a） **当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制；**

b） **应具有云服务客户首次登录强制修改初始密码措施。**

8.2.3.2 访问控制

要求如下：

a） 应保证当虚拟机迁移时，访问控制策略随其迁移；

b） 应允许云服务客户设置不同虚拟机之间的访问控制策略。

8.2.3.3 入侵防范

要求如下：

a） **应能检测虚拟机之间的资源隔离失效，并进行告警；**

b） **应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警；**

c） **应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。**

8.2.3.4 镜像和快照保护

要求如下：

a） 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；

b） 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；

c） **应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；**

d） **应保证虚拟机镜像和快照文件备份在不同物理存储。**

8.2.3.5 数据完整性和保密性

要求如下：

a） 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；

b） 应确保只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；

c） **应使用校验码或密码技术确保虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；**

d） **应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。**

8.2.3.6 数据备份恢复

要求如下：

a） 云服务客户应在本地保存其业务数据的备份；

b） 应提供查询云服务客户数据及备份存储位置的能力；

c） **云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；**

d） **应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。**

8.2.3.7 剩余信息保护

要求如下：

a） 应保证虚拟机所使用的内存和存储空间回收时得到完全清除；

b） 云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。

8.2.4 安全管理中心

8.2.4.1 集中管控

要求如下：

a） **应能对物理资源和虚拟资源按照策略做统一管理调度与分配；**

b） **应保证云计算平台管理流量与云服务客户业务流量分离；**

c） **应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；**

d） **应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。**

8.3 移动互联安全扩展要求

8.3.1 安全区域边界

8.3.1.1 边界防护

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

8.3.1.2 访问控制

无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。

8.3.1.3 入侵防范

要求如下：

a） 应能够检测到非授权无线接入设备和非授权移动终端的接入行为；

b） 应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为；

c） 应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；

d） 应禁用无线接入设备和无线接入网关存在风险的功能，如：SSID 广播、WEP 认证等；

e） 应禁止多个 AP 使用同一个认证密钥；

f） **应能够阻断非授权无线接入设备或非授权移动终端。**

8.3.2 安全计算环境

8.3.2.1 移动终端管控

要求如下：

a） 应保证移动终端安装、注册并运行终端管理客户端软件；

b） 移动终端应接受移动终端管理服务端的设备生命周期管理、设备远程控制，如：远程锁定、远程数据擦除等；

c） 用于发布直播数据的移动终端宜为专用终端。

8.3.2.2 移动应用管控

要求如下：

a） 应具有选择应用软件安装、运行的功能；
b） 应只允许指定证书签名的应用软件安装和运行；
c） **应具有软件白名单功能，应能根据白名单控制应用软件安装、运行；**
d） 专用移动应用软件应具备防二次打包工具篡改程序文件，以防止移动应用程序的代码、图片、配置、布局等被增加、修改或删除；
e） 专用移动应用软件**应根据实际业务对移动应用上传文件的类型、大小进行限制。**

9 第四级安全要求

9.1 安全通用要求

9.1.1 安全通信网络

9.1.1.1 网络架构

要求如下：

a） 应保证网络设备的业务处理能力满足业务高峰期需要；
b） 应保证网络各个部分的带宽满足业务高峰期需要；
c） 应根据系统功能、业务流程、网络结构层次、业务服务对象等因素划分不同网络区域，并按照方便安全管理和控制的原则为各网络区域分配地址；
d） 应避免将播出直接相关系统等重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；
e） 应具备通信线路、关键网络设备、关键安全设备和关键计算设备的硬件冗余，保证系统的可用性；
f） **应按照业务服务的重要程度分配带宽，优先保障重要业务；**
g） 应具备不同路由的双链路接入保障；
h） 应配备与实际运行情况相符的网络拓扑图。

9.1.1.2 通信传输

要求如下：

a） 应采用校验技术、密码技术或特定协议转换技术保证通信过程中数据的完整性；
b） 应采用密码技术或特定协议转换技术保证通信过程中数据的保密性；
c） **应在通信前基于密码技术对通信的双方进行验证或认证；**
d） **应基于硬件密码模块对重要通信过程进行密码运算和密钥管理；**
e） **应使用协议对管理流量与媒体内容数据流等业务流量进行分离传输。**

9.1.1.3 可信验证

可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的**所有执行环节**进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，**并进行动态关联感知。**

9.1.2 安全区域边界

9.1.2.1 边界防护

要求如下：

a） 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信；
b） 应能够对非授权设备私自联到内部网络的行为进行检查和限制；
c） 应能够对内部用户非授权联到外部网络的行为进行检查和限制；
d） 播出直接相关系统应禁止通过无线方式进行组网；非播出直接相关系统，应限制无线网络的使用，强化无线网络区域边界防护措施，保证无线网络通过受控边界设备接入内部网络；
e） **应能够在发现非授权设备私自联到内部网络的行为或内部用户非授权联到外部网络的行为时，对其进行有效阻断；**
f） **应采取可信验证机制对接入到网络中的设备进行可信验证，保证接入网络的设备真实可信；**
g） **应能够对敏感数据泄露行为进行检查，准确定出位置，并对其进行有效阻断。**

9.1.2.2 访问控制

要求如下：
a） 应在网络边界根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；
b） 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；
c） 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出；
d） 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力；
e） **应在网络边界对媒体内容数据和其他数据进行区分，媒体内容数据外的其他数据应通过协议转换等手段实现数据交换；**
f） 应对进出网络的数据流实现基于应用协议和应用内容的访问控制；
g） 宜在会话处于非活跃一定时间或会话结束后终止网络连接。

9.1.2.3 入侵防范

要求如下：
a） 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为；
b） 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为；
c） 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析；
d） 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。

9.1.2.4 恶意代码和垃圾邮件防范

要求如下：
a） 应在关键网络节点处进行恶意代码检测和清除，并维护恶意代码防护机制有效性，及时升级和更新特征库；
b） 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新；
c） 部署在关键网络节点的防恶意代码产品宜与系统内部防恶意代码产品具有不同的恶意代码库。

9.1.2.5 安全审计

要求如下：
a） 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b） 审计记录应包括事件的日期、时间、IP 地址、事件类型、事件是否成功及其他与审计相关的信息；
c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

d） 应能对播出控制操作行为、远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析；
e） 应定期对审计记录进行分析，以便及时发现异常行为。

9.1.2.6 可信验证

可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，**并在应用程序的所有执行环节进行动态可信验证，**在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，**并进行动态关联感知。**

9.1.3 安全计算环境

9.1.3.1 身份鉴别

要求如下：
a） 应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；
b） 应启用登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
c） 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听，如：HTTPS、SSH、VPN 等；
d） 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

9.1.3.2 访问控制

要求如下：
a） 应对登录的用户分配账户和权限；
b） 应重命名或删除默认账户，修改默认账户的默认口令；无法重命名或删除的默认账户，应阻止其直接远程登录；
c） 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
d） 应授予管理用户所需的最小权限，实现管理用户的权限分离；
e） 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
f） 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；
g） 应对重要主体和客体设置安全标记，**并依据强制访问控制规则**控制主体对有安全标记信息资源的访问；
h） 应用系统应**强制**首次登录用户修改预设的默认口令；
i） 应限制未登录用户的使用权限，可对匿名用户使用记录进行追溯；
j） 播出直接相关系统的特权命令（如播出文件调整，播出节目单调整）应在服务器或专用操作终端执行。

9.1.3.3 安全审计

要求如下：
a） 应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b） 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c） 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

d） 应对审计进程进行保护，防止未经授权的中断。

9.1.3.4 入侵防范

要求如下：

a） 应遵循最小安装的原则，仅安装需要的组件和应用程序；
b） 应关闭不需要的系统服务、默认共享和高危端口；
c） 应能通过漏洞扫描工具、人工漏洞排查等手段，发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；
d） 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；
e） 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；
f） 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。

9.1.3.5 恶意代码防范

要求如下：

a） **应采用主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断；**
b） 通过移动介质进行数据上传时，应在移动介质接入前采用两种或两种以上病毒库对移动介质进行恶意代码查杀。

9.1.3.6 可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，**并在应用程序的所有执行环节进行动态可信验证，**在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心，**并进行动态关联感知**。

9.1.3.7 数据完整性

要求如下：

a） 采用密码技术保证重要数据在传输过程中的完整性，包括但不限于调度信息、鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要媒体内容数据和重要个人信息等；
b） 采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要媒体内容数据和重要个人信息等；
c） **在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。**

9.1.3.8 数据保密性

要求如下：

a） 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等；
b） 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

9.1.3.9 数据备份恢复

要求如下：

a） 应提供重要数据的本地数据备份与恢复功能，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；
b） 应提供异地数据实时备份功能，利用通信网络将重要数据实时备份至备份场地；
c） 应提供重要数据处理系统的热冗余，保证系统的高可用性；
d） **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，提供业务应用的实时切换；**
e） 建立敏感数据样本库并进行定期维护及时更新，支持其他应用通过多种接口方式使用。

9.1.3.10 剩余信息保护

要求如下：
a） 应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
b） 应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

9.1.3.11 个人信息保护

要求如下：
a） 应仅采集和保存业务必需的用户个人信息；
b） 应禁止未授权访问和非法使用用户个人信息；
c） 应具备用户个人信息全生命周期管理功能。

9.1.3.12 业务连续性保障

要求如下：
a） 播出直接相关系统应保证节目传输链路的冗余，并能够在发生故障时切换；
b） 播出直接相关系统关键设备应配置冗余，当某节点设备出现故障时，切换到备份设备继续运行，切换过程不能对正常播出产生影响。

9.1.4 安全管理中心

9.1.4.1 系统管理

要求如下：
a） 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计；
b） 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。

9.1.4.2 审计管理

要求如下：
a） 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计；
b） 应通过审计管理员对审计记录进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。

9.1.4.3 安全管理

要求如下：

a） 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；
b） 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。

9.1.4.4 集中管控

要求如下：
a） 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
b） 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
c） 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测；
d） 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录留存时间符合国家和行业法律法规要求；
e） 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理；
f） 应具备网络安全实时监测、态势感知、风险预警、统一展示和安全事件应急处置的能力；
g） 应保证系统范围内的时间由唯一确定的时钟产生，以保证各种数据的管理和分析在时间上的一致性。

9.2 云计算安全扩展要求

9.2.1 安全通信网络

9.2.1.1 网络架构

要求如下：
a） 应保证云计算平台不承载高于其安全保护等级的业务应用系统；
b） 应实现不同云服务客户虚拟网络之间的隔离；
c） 应具有根据云服务客户业务需求提供通信传输、边界防护、入侵防范等安全机制的能力；
d） 应具有根据云服务客户业务需求自主设置安全策略的能力，包括定义访问路径、选择安全组件、配置安全策略；
e） 应提供开放接口或开放性安全服务，允许云服务客户接入第三方安全产品或在云计算平台选择第三方安全服务；
f） **应提供对虚拟资源的主体和客体设置安全标记的能力，保证云服务客户可以依据安全标记和强制访问控制规则确定主体对客体的访问；**
g） **应提供通信协议转换或通信协议隔离等的数据交换方式，保证云服务客户可以根据业务需求自主选择边界数据交换方式；**
h） **应为第四级业务应用系统划分独立的资源池。**

9.2.2 安全区域边界

9.2.2.1 访问控制

要求如下：
a） 应在虚拟化网络边界部署访问控制机制，并设置访问控制规则；
b） 应在不同等级的网络区域边界部署访问控制机制，并设置访问控制规则。

9.2.2.2 入侵防范

要求如下：

a） 应能检测到云服务客户发起的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

b） 应能检测到对虚拟网络节点的网络攻击行为，并能记录攻击类型、攻击时间、攻击流量等；

c） 应能检测到虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；

d） 应在检测到网络攻击行为、异常流量情况时进行告警。

9.2.2.3 安全审计

要求如下：

a） 应对云服务商和云服务客户在远程管理时执行的特权命令进行审计，至少包括虚拟机删除、虚拟机重启；

b） 应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计。

9.2.3 安全计算环境

9.2.3.1 身份鉴别

要求如下：

a） 当远程管理云计算平台中设备时，管理终端和云计算平台之间应建立双向身份验证机制；

b） 应具有云服务客户首次登录强制修改初始密码措施。

9.2.3.2 访问控制

要求如下：

a） 应保证当虚拟机迁移时，访问控制策略随其迁移；

b） 应允许云服务客户设置不同虚拟机之间的访问控制策略。

9.2.3.3 入侵防范

要求如下：

a） 应能检测虚拟机之间的资源隔离失效，并进行告警；

b） 应能检测非授权新建虚拟机或者重新启用虚拟机，并进行告警；

c） 应能够检测恶意代码感染及在虚拟机间蔓延的情况，并进行告警。

9.2.3.4 镜像和快照保护

要求如下：

a） 应针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；

b） 应提供虚拟机镜像、快照完整性校验功能，防止虚拟机镜像被恶意篡改；

c） 应采取密码技术或其他技术手段防止虚拟机镜像、快照中可能存在的敏感资源被非法访问；

d） 应保证虚拟机镜像和快照文件备份在不同物理存储。

9.2.3.5 数据完整性和保密性

要求如下：

a） 应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定；

b） 应保证只有在云服务客户授权下，云服务商或第三方才具有云服务客户数据的管理权限；

c） 应使用校验技术或密码技术保证虚拟机迁移过程中重要数据的完整性，并在检测到完整性受到破坏时采取必要的恢复措施；

d） 应支持云服务客户部署密钥管理解决方案，保证云服务客户自行实现数据的加解密过程。

9.2.3.6 数据备份恢复

要求如下：

a） 云服务客户应在本地保存其业务数据的备份；
b） 应提供查询云服务客户数据及备份存储位置的能力；
c） 云服务商的云存储服务应保证云服务客户数据存在若干个可用的副本，各副本之间的内容应保持一致；
d） 应为云服务客户将业务系统及数据迁移到其他云计算平台和本地系统提供技术手段，并协助完成迁移过程。

9.2.3.7 剩余信息保护

要求如下：

a） 应保证虚拟机所使用的内存和存储空间回收时得到完全清除；
b） 云服务客户删除业务应用数据时，云计算平台应将云存储中所有副本删除。

9.2.4 安全管理中心

9.2.4.1 集中管控

要求如下：

a） 应能对物理资源和虚拟资源按照策略做统一管理调度与分配；
b） 应保证云计算平台管理流量与云服务客户业务流量分离；
c） 应根据云服务商和云服务客户的职责划分，收集各自控制部分的审计数据并实现各自的集中审计；
d） 应根据云服务商和云服务客户的职责划分，实现各自控制部分，包括虚拟化网络、虚拟机、虚拟化安全设备等的运行状况的集中监测。

9.3 移动互联安全扩展要求

9.3.1 安全区域边界

9.3.1.1 边界防护

应保证有线网络与无线网络边界之间的访问和数据流通过无线接入网关设备。

9.3.1.2 访问控制

无线接入设备应开启接入认证功能，并支持采用认证服务器认证或国家密码管理机构批准的密码模块进行认证。

9.3.1.3 入侵防范

要求如下：

a） 应能够检测到非授权无线接入设备和非授权移动终端的接入行为；
b） 应能够检测到针对无线接入设备的网络扫描、DDoS 攻击、密钥破解、中间人攻击和欺骗攻击等行为；
c） 应能够检测到无线接入设备的 SSID 广播、WPS 等高风险功能的开启状态；
d） 应禁用无线接入设备和无线接入网关存在风险的功能，如 SSID 广播、WEP 认证等；

e） 应禁止多个 AP 使用同一个认证密钥；
f） 应能够阻断非授权无线接入设备或非授权移动终端。

9.3.2 安全计算环境

9.3.2.1 移动终端管控

要求如下：
a） 应保证移动终端安装、注册并运行终端管理客户端软件；
b） 移动终端应接受移动终端管理服务端的生命周期管理、设备远程控制，如：远程锁定、远程数据擦除等；
c） **应保证移动终端只用于指定业务；**
d） 用于发布直播数据的移动终端宜为专用终端。

9.3.2.2 移动应用管控

要求如下：
a） 应具有选择应用软件安装、运行的功能；
b） 应只允许指定证书签名的应用软件安装和运行；
c） 应具有软件白名单功能，应能根据白名单控制应用软件安装、运行；
d） **移动终端应能够接受移动终端管理服务端推动的移动应用软件管理策略，并根据策略对软件实施管控；**
e） 专用移动应用软件应具备防二次打包工具篡改程序文件，以防止移动应用程序的代码、图片、配置、布局等被增加、修改或删除；
f） 专用移动应用软件应根据实际业务对移动应用上传文件的类型、大小进行限制。

10 第五级安全要求（略）

11 安全物理环境要求

11.1 安全通用要求

11.1.1 物理位置选择

要求如下：
a） 机房场地应选择在具有防震、防风和防雨等能力的建筑内；
b） 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。

11.1.2 物理访问控制

要求如下：
a） 机房出入口应配置电子门禁系统，控制、鉴别和记录进入的人员；
b） 需进入播出相关机房的来访人员应经过申请和审批流程，并限制其活动范围并监控其活动过程。

11.1.3 防盗窃和防破坏

要求如下：
a） 应将机房设备或主要部件进行固定，并设置明显的不易除去的标识；

b） 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；
c） 应设置机房防盗报警系统或设置有专人值守的视频监控系统。

11.1.4 防雷击

要求如下：
a） 应将各类机柜、设施和设备等通过接地系统安全接地；
b） 应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。

11.1.5 防火

应符合GY 5067的相关要求。

11.1.6 防水和防潮

要求如下：
a） 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
b） 应采取措施防止机房内水蒸气结露、水管泄漏和地下积水的转移与渗透；
c） 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。

11.1.7 防静电

要求如下：
a） 应安装防静电地板或地面并采用必要的接地防静电措施；
b） 应采用措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。

11.1.8 温湿度控制

要求如下：
a） 机房应设置温、湿度自动调节设施；
b） 机房的温度范围应在18℃～26℃之内，第四级网络所在机房的温度范围应在19℃～25℃之内；
c） 机房的湿度范围应在35%～65%之内，第四级网络所在机房的湿度范围应在40%～60%之内。

11.1.9 电力供应

要求如下：
a） 应在机房供电线路上配置稳压器和过电压防护设备；
b） 应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；
c） 应设置冗余或并行的电力电缆线路为系统供电；
d） 三级及以上网络应接入两路外电，其中至少一路宜为专线，当一路外电发生故障时，另一路外电不应同时受到损害。

11.1.10 电磁防护

要求如下：
a） 电源线和通信线缆应隔离铺设，避免互相干扰；
b） 三级及以上网络应对关键设备或关键区域实施电磁屏蔽。

11.2 云计算安全扩展要求

11.2.1 基础设施位置

应保证云计算基础设施位于中国境内。

11.3 移动互联安全扩展要求

11.3.1 无线接入点的物理位置

应为无线接入设备的安装选择合理位置，避免过度覆盖和电磁干扰。

12 安全管理要求

12.1 安全通用要求

12.1.1 安全管理制度

12.1.1.1 安全策略

应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

12.1.1.2 管理制度

要求如下：

a） 应对安全管理活动中的各类管理内容建立安全管理制度，从安全组织、安全责任、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网络安全管理工作；
b） 应对管理人员或操作人员执行的日常管理操作建立操作规程；
c） 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。

12.1.1.3 制定和发布

要求如下：

a） 应指定或授权专门的部门或人员负责安全管理制度的制定；
b） 安全管理制度应通过正式、有效方式发布至所有相关部门和岗位。

12.1.1.4 评审和修订

要求如下：

a） 应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订；
b） 应及时更新安全管理制度和操作规程，并进行版本控制。

12.1.2 安全管理机构

12.1.2.1 岗位设置

要求如下：

a） 应成立指导和管理网络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担任或授权，并通过正式文件发布；
b） 应设立网络安全管理工作的职能部门，负责网络安全各项工作的组织和落实，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责；

c） 应设立系统管理员、审计管理员、安全管理员等岗位，并定义部门及各个工作岗位的职责。

12.1.2.2 人员配备

要求如下：

a） 应配备一定数量的系统管理员、审计管理员和安全管理员等；
b） 第三级及以上网络应配备专职安全管理员，不可兼任。

12.1.2.3 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） 播出直接相关操作系统和应用系统的补丁更新应由部门负责人审批通过后方可实施。

12.1.2.4 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网络安全职能部门内部的合作与沟通，定期召开协调会议，共同协作处理网络安全问题；
b） 应加强与行业内外相关网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通；
c） 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；
d） 应按照《广播电视网络安全事件应急预案》的要求，与本级广播电视行政主管部门建立信息通报和应急处置联动机制，制定信息通报和应急处置流程。

12.1.2.5 审核和检查

要求如下：

a） 应定期进行常规安全检查，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） 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。

12.1.3 安全管理人员

12.1.3.1 人员录用

要求如下：

a） 应指定或授权专门的部门或人员负责人员录用；
b） 应规范人员录用过程，应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核；
c） 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。

12.1.3.2 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） 应取回配发给离岗员工的各种身份证件、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，关键岗位人员并承诺调离后的保密义务后方可离开。

12.1.3.3 安全意识教育和培训

要求如下：
a） 应定期对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施；
b） 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训；
c） 应定期对网络安全各相关岗位的人员进行安全技能、政策及安全意识的考核，通过后方可上岗。

12.1.3.4 外部人员访问管理

要求如下：
a） 应确保在外部人员物理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） 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限，并登记备案；
c） 外部人员离场后应及时清除其所有的访问权限；
d） 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息；
e） 应制定外部人员（如服务组织、合同商、系统开发商、集成商等相关人员）安全管理要求，包括安全角色和责任；
f） 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。

12.1.4 安全建设管理

12.1.4.1 定级和备案

要求如下：
a） 应按照国家和行业标准、规范确定保护对象的边界和安全保护等级，以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由；
b） 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定；
c） 应保证定级结果经过本单位批准；
d） 应将定级和备案材料报本级广播电视行政主管部门审核；
e） 应将定级和备案材料报相应公安机关备案；
f） 应将定级和备案结果报本级广播电视行政主管部门备案；
g） 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。

12.1.4.2 安全方案设计

要求如下：
a） 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施；
b） 应根据国家和行业标准，设计保护对象的网络安全方案和策略，制定详细的安全整体规划和安全建设方案；
c） 应组织相关部门和有关安全专家对安全整体规划、安全建设方案等进行论证和审定，经过批准后才能正式实施。

12.1.4.3 产品采购和使用

要求如下：

a） 应确保网络安全产品采购和使用符合国家的有关规定；

b） 应确保密码产品与服务的采购和使用符合国家密码主管部门的要求；

c） 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

12.1.4.4 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；

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，对文档使用进行控制；

e） 应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测，并审查软件中可能存在的后门漏洞等；

f） 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制；

g） 应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查；

h） 应对个人信息的收集进行明示，并符合国家法律法规要求。

12.1.4.5 外包软件开发

要求如下：

a） 应在软件安装之前检测软件包中可能存在的恶意代码；

b） 应保证开发单位提供软件设计的相关文档和使用指南；

c） 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道；

d） 应对个人信息的收集进行明示，并符合国家法律法规要求。

12.1.4.6 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；

c） 第三级及以上网络应通过第三方工程监理控制项目的实施过程。

12.1.4.7 测试验收

要求如下：

a） 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告；

b） 应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容，播出直接相关系统测评应确保安全播出不受影响，宜委托行业内测评机构进行等级测评；

12.1.4.8 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；

d） 应对安全管理人员进行网络安全方面专业培训。

12.1.4.9 等级测评

要求如下：

a） 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改；
b） 应在发生重大变更或级别发生变化时及时进行等级测评；
c） 应选择国家和行业认可的测评机构进行等级测评；
d） 播出直接相关系统测评宜委托行业内测评机构。

12.1.4.10 服务供应商选择

要求如下：

a） 应确保服务商供应商的选择符合国家和行业的有关规定；
b） 应与选定的服务商供应商签订相关的协议，明确整个服务供应链各方需履行的网络安全相关义务；
c） 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

12.1.5 安全运维管理

12.1.5.1 环境管理

要求如下：

a） 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理；
b） 应建立机房安全管理制度，对机房物理访问、机房环境安全和工作人员行为等进行规定；
c） 应不在重要区域接待来访人员，不随意放置含有敏感数据的纸质文件和移动介质等。

12.1.5.2 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；
c） 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。

12.1.5.3 介质管理

要求如下：

a） 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，并根据存档介质的目录清单定期盘点；
b） 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质归档和查询进行登记记录；
c） 应对存储介质的送出维修以及销毁等进行严格的管理，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。

12.1.5.4 设备维护管理

要求如下：

a） 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；
b） 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、维修和服务的审批、维修过程的监督控制等；

c） 信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密；
d） 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。

12.1.5.5 漏洞和风险管理

要求如下：
a） 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补；
b） 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题；
c） 播出直接相关系统的安全漏洞应先在测试环境中测试通过，并对重要文件备份后进行修补，同时做好应急预案，发现问题后及时回退。

12.1.5.6 网络和系统安全管理

要求如下：
a） 应划分不同的管理员角色进行网络和系统的运维管理，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；
b） 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制；
c） 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定；
d） 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置；
e） 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容；
f） 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为和趋势；应至少每周进行分析、统计工作；
g） 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库；
h） 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据；
i） 应严格控制通过外部网络进行运维，经过审批后方可开通运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道，播出直接相关系统不应通过外部网络进行运维；
j） 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网、信息系统非法接入和非法外联及其他违反网络安全策略的行为；
k） 应针对播出直接相关系统建立 7×24 网络安全监测制度，及时对网络安全事件进行监测和处理。

12.1.5.7 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，对外来计算机或存储设备接入系统前进行恶意代码检查；
b） 应定期验证防范恶意代码攻击的技术措施的有效性。

12.1.5.8 配置管理

要求如下：

a） 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等；
b） 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库；
c） 应制定对恶意代码库、入侵检测规则库、防火墙规则库、漏洞库等网络安全相关重要配置项定期更新的制度。

12.1.5.9 密码管理

要求如下：
a） 应遵循密码相关国家标准和行业标准；
b） 应使用国家密码管理主管部门认证核准的密码技术和产品。

12.1.5.10 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） 应记录变更实施过程，并妥善保存所有文档和记录；
c） 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；
d） 与播出直接相关的信息系统中，重要配置修改、操作系统升级、应用软件升级、恶意代码库更新等重要变更应先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应用。

12.1.5.11 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，备份程序和恢复程序等；
d） 三级及以上网络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。

12.1.5.12 安全事件处置

要求如下：
a） 按照国家和行业相关规定及时上报网络安全事件和可疑事件；
b） 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，规定安全事件的处置和响应流程；
c） 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；
d） 对造成系统中断和造成信息泄露的重大安全事件应采用不同的处理程序和报告程序。

12.1.5.13 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，包括启动应急预案的条件、应急组织构成、应急资源保障、应急处置流程、系统恢复流程、事后教育和培训等内容；
b） 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；

c） 应组织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；
d） 应组织相关的人员进行应急预案演练，应急预案的演练应至少每年举办一次；
e） 应定期对原有的应急预案重新评估和修订完善，根据系统变更、管理要求的变化等及时更新应急预案。

12.1.5.14 外包运维管理

要求如下：
a） 应确保外包运维服务商的选择符合国家的有关规定；
b） 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；
c） 应保证选择的外包运维服务商在技术和管理方面均具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确；
d） 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感数据的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

12.1.5.15 安全播出重要保障期管理

要求如下：
a） 在重要安全播出保障期前，应开展隐患排查，完善各项防范措施，并与相关单位部门建立协调联动机制，发生网络安全事件时，各负其责，快速处置；
b） 在重要安全播出保障期间，重点部门、重要岗位应建立 24 小时值班制度，并加强网络安全状态监测。

12.2 云计算安全扩展要求

12.2.1 安全建设管理

12.2.1.1 云服务商选择

要求如下：
a） 应选择安全合规的云服务商，其所提供的云计算平台应为其所承载的业务应用系统提供相应等级的安全保护能力；
b） 应在服务水平协议中规定云服务的各项服务内容和具体技术指标；
c） 应在服务水平协议中规定云服务商的权限与责任，包括管理范围、职责划分、访问授权、隐私保护、行为准则、违约责任等；
d） 应在服务水平协议中规定服务合约到期时，完整提供云服务客户数据，并承诺相关数据在云计算平台上清除；
e） **应与选定的云服务商签署保密协议，要求其不得泄露云服务客户数据。**

12.2.1.2 供应链管理

要求如下：
a） 应确保选定的云服务平台符合国家和行业的有关规定；
b） 应将供应链安全事件信息或安全威胁信息及时传达到云服务客户；
c） 应将供应商的重要变更及时传达到云服务客户，并评估变更带来的安全风险，采取措施对风险进行控制。

12.2.2 安全运维管理

12.2.2.1 云计算环境管理

云计算平台的运维地点应位于中国境内，境外对境内云计算平台实施运维操作应遵循国家相关规定。

12.3 移动互联安全扩展要求

12.3.1 安全建设管理

12.3.1.1 移动应用软件采购

要求如下：

a） 应保证移动终端安装、运行的应用软件来自可靠分发渠道或使用可靠证书签名；

b） 应保证移动终端安装、运行的应用软件由**指定的**开发者开发。

12.3.1.2 移动应用软件开发

要求如下：

a） 应对移动业务应用软件开发者进行资格审查；

b） 应保证开发移动业务应用软件的签名证书合法性；

c） 移动应用软件应对运行环境进行安全检测，限制其在不安全环境下使用，包括但不限于普通用户获取系统最高权限、模拟器等。

12.3.2 安全运维管理

12.3.2.1 配置管理

要求如下：

a） 应建立合法无线接入设备和合法移动终端配置库，用于对非法无线接入设备和非法移动终端的识别；

b） 应保证用于发布直播数据的移动终端只接入到安全的无线网络中。

附 录 A
（规范性）
安全要求的选择和使用

由于等级保护对象承载的业务不同，对其的安全关注点会有所不同，有的更关注信息的安全性，即更关注对搭线窃听、假冒用户等可能导致信息泄密、非法篡改等；有的更关注业务的连续性，即更关注保证系统连续正常的运行，免受对系统未授权的修改、破坏而导致系统不可用引起业务中断。

不同级别的等级保护对象，其对业务信息的安全性要求和系统服务的连续性要求是有差异的，即使相同级别的等级保护对象，其对业务信息的安全性要求和系统服务的连续性要求也有差异。

等级保护对象定级后，可能形成的定级结果组合应符合表A.1的规定。

表A.1 等级保护对象定级结果组合

安全保护等级	定级结果的组合
第一级	S1A1
第二级	S1A2，S2A2，S2A1
第三级	S1A3，S2A3，S3A3，S3A2，S3A1
第四级	S1A4，S2A4，S3A4，S4A4，S4A3，S4A2，S4A1
第五级	S1A5，S2A5，S3A5，S4A5，S5A5，S5A4，S5A3，S5A2，S5A1

安全保护措施的选择应依据上述定级结果，本文件中的技术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）；其他安全保护类要求（简记为G）。本文件中所有安全管理要求均标注为G,安全要求及属性标识应符合表A.2的规定。

表A.2 安全要求及属性标识

技术 / 管理	分类	安全控制点	属性标识
安全技术要求	安全物理环境	物理位置选择	G
		物理访问控制	G
		防盗窃和防破坏	G
		防雷击	G
		防火	G
		防水和防潮	G
		防静电	G
		温湿度控制	G
		电力供应	A
		电磁防护	S
	安全通信网络	网络架构	G
		通信传输	G
		可信验证	S

表 A.2（续）

技术 / 管理	分类	安全控制点	属性标识
	安全区域边界	边界防护	G
		访问控制	G
		入侵防范	G
		可信验证	S
		恶意代码防范	G
		安全审计	G
	安全计算环境	身份鉴别	S
		访问控制	S
		安全审计	G
		可信验证	S
		入侵防范	G
		恶意代码防范	G
		数据完整性	S
		数据保密性	S
		数据备份恢复	A
		剩余信息保护	S
		个人信息保护	S
		业务连续性保障	A
	安全管理中心	系统管理	G
		审计管理	G
		安全管理	G
		集中管控	G
安全管理要求	安全管理制度	安全策略	G
		管理制度	G
		制定和发布	G
		评审和修订	G
	安全管理机构	岗位设置	G
		人员配备	G
		授权和审批	G
		沟通和合作	G
		审核和检查	G
	安全管理人员	人员录用	G
		人员离岗	G
		安全意识教育和培训	G
		外部人员访问管理	G
	安全建设管理	定级和备案	G
		安全方案设计	G
		产品采购和使用	G
		自行软件开发	G

表 A.2（续）

技术 / 管理	分类	安全控制点	属性标识
		外包软件开发	G
		工程实施	G
		测试验收	G
		系统交付	G
		等级测评	G
		服务供应商选择	G
	安全运维管理	环境管理	G
		资产管理	G
		介质管理	G
		设备维护管理	G
		漏洞和风险管理	G
		网络和系统安全管理	G
		恶意代码防范管理	G
		配置管理	G
		密码管理	G
		变更管理	G
		备份与恢复管理	G
		安全事件处置	G
		应急预案管理	G
		外包运维管理	G
		重要安全播出保障期管理	G

对于确定了级别的等级保护对象，应依据表A.1的定级结果，结合表A.2使用安全要求，应按照以下过程进行安全要求的选择。

a） 根据等级保护对象的级别选择安全要求。方法是根据本文件，第一级选择第一级安全要求，第二级选择第二级安全要求，第三级选择第三级安全要求，第四级选择第四级安全要求，以此作为出发点。

b） 根据定级结果，基于表 A.1 和表 A.2 对安全要求进行调整。根据系统服务保证性等级选择相应级别的系统服务保证类(A 类）安全要求；根据业务信息安全性等级选择相应级别的业务信息安全类(S 类）安全要求；根据系统安全等级选择相应级别的安全通用要求(G 类）。

c） 针对不同单位或不同对象的特点，分析可能在某些方面的特殊安全保护能力要求，选择较高级别的安全要求或其他标准的补充安全要求。对于本文件中提出的安全要求无法实现或有更加有效的安全措施可以替代的，可以对安全要求进行调整，调整的原则是保证不降低整体安全保护能力。

保证不同安全保护等级的对象具有相应级别的安全保护能力是安全等级保护的核心。选用本文件中提供的安全要求是保证等级保护对象具备一定安全保护能力的一种途径和出发点，在此出发点的基础上，可以参考等级保护的其他相关标准和安全方面的其他相关标准，调整和补充安全要求，从而实现等级保护对象在满足等级保护安全要求基础上，又具有自身特点的保护。

附 录 B
（规范性）
等级保护对象整体安全保护能力的要求

网络安全等级保护的核心是保证不同安全保护等级的对象具有相适应的安全保护能力。第5章提出了不同级别的等级保护对象的安全保护能力要求，第6章～第12章分别针对不同安全保护等级的对象应该具有的安全保护能力提出了相应的安全要求。

依据本文件分层面采取各种安全措施时，还应考虑以下总体性要求，保证等级保护对象的整体安全保护能力。

a） 构建纵深的防御体系

本文件从技术和管理两个方面提出安全要求，在采取由点到面的各种安全措施时，在整体上还应保证各种安全措施的组合从外到内构成一个纵深的安全防御体系，保证等级保护对象整体的安全保护能力。应从通信网络、网络边界、局域网络内部、各种业务应用平台等各个层次落实本文件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

本文件以安全控制的形式提出安全要求，在将各种安全控制落实到特定等级保护对象中时，应考虑各个安全控制之间的互补性，关注各个安全控制在层面内、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，保证各个安全控制共同综合作用于等级保护对象上，使得等级保护对象的整体安全保护能力得以保证。

c） 保证一致的安全强度

本文件将安全功能要求，如身份鉴别、访问控制、安全审计、入侵防范等内容，分解到等级保护对象的各个层面，在实现各个层面安全功能时，应保证各个层面安全功能实现强度的一致性。应防止某个层面安全功能的减弱导致整体安全保护能力在这个安全功能上削弱。例如，要实现双因子身份鉴别，则应在各个层面均实现基于标记的访问控制，并保证标记数据在整个等级保护对象内部流动时标记的唯一性等。

d） 建立统一的支撑平台

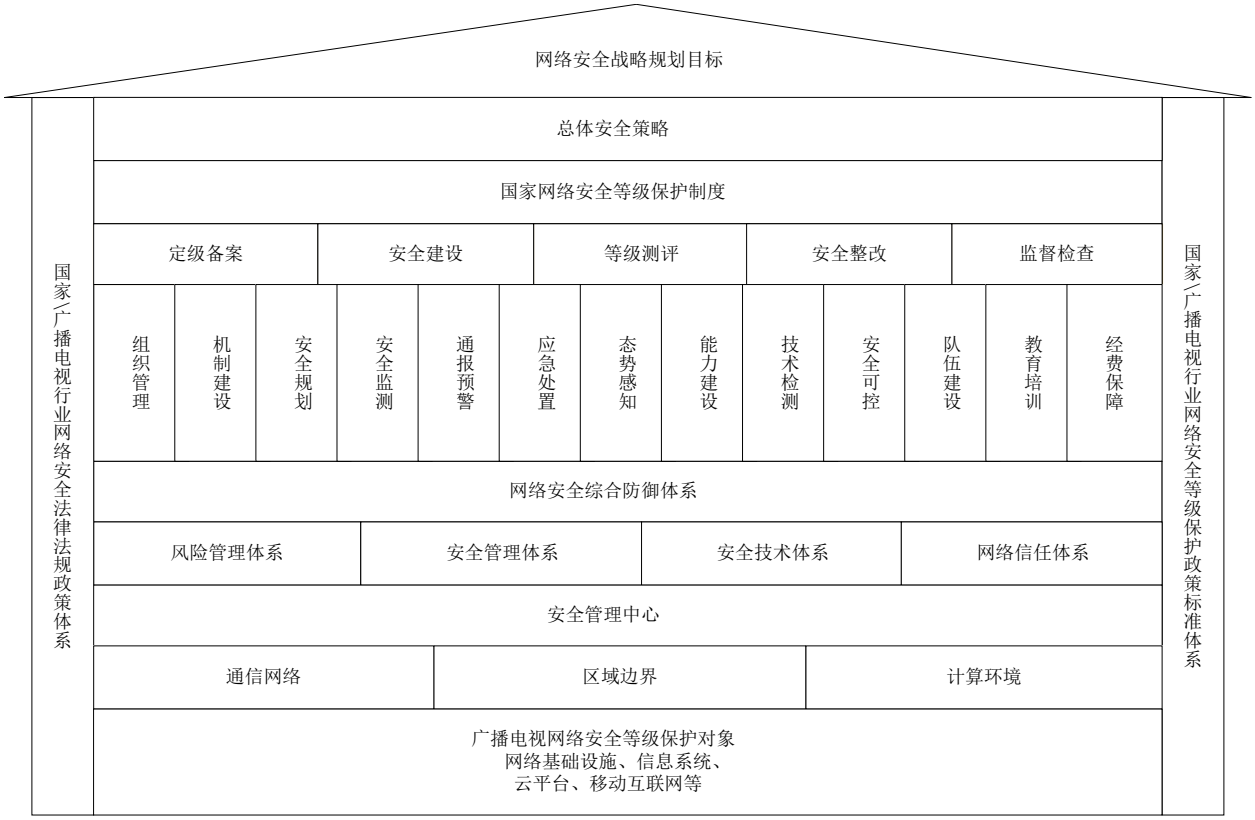
本文件针对较高级别的等级保护对象，提到了使用密码技术、可信技术等，多数安全功能（如身份鉴别、访问控制、数据完整性、数据保密性等）为了获得更高的强度，均要基于密码技术和可信技术，为了保证等级保护对象的整体安全保护能力，应建立基于密码技术的统一支撑平台，支持高强度身份鉴别、访问控制、数据完整性、数据保密性等安全功能的实现。

e） 进行集中的安全管理

本文件针对较高级别的等级保护对象，提到了实现集中的安全管理、安全监控和安全审计等要求，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，各个安全控制在可控情况下发挥各自的作用，应建立集中的管理中心，集中管理等级保护对象中的各个安全控制组件，支持统一安全管理。

附 录 C
（规范性）
等级保护安全框架和关键技术使用要求

在开展网络安全等级保护工作中应首先明确等级保护对象，广播电视网络安全等级保护对象主要包括信息系统、广播电视网络设施和数据资源；确定了等级保护对象的安全保护等级后，应根据不同对象的安全保护等级完成安全建设或安全整改工作；应针对等级保护对象特点建立安全技术体系和安全管理体系，构建具备相应等级安全保护能力的网络安全综合防御体系。应依据国家网络安全等级保护政策和标准，开展组织管理、机制建设、安全规划、安全监测、通报预警、应急处置、态势感知、能力建设、监督检查、技术检测、安全可控、队伍建设、教育培训和经费保障等工作。等级保护安全框架如图C.1所示。



图C.1 等级保护安全框架

应在较高级别等级保护对象的安全建设和安全整改中注重使用一些关键技术。

a） 可信计算技术

应针对计算资源构建保护环境，以可信计算基(TCB)为基础，实现软硬件计算资源可信；针对信息资源构建业务流程控制链，基于可信计算技术实现访问控制和安全认证，密码操作调用和资源的管理等，构建以可信计算技术为基础的等级保护核心技术体系。

b） 强制访问控制

应在高等级保护对象中使用强制访问控制机制，强制访问控制机制需要总体设计、全局考虑，在通信网络、操作系统、应用系统各个方面实现访问控制标记和策略，进行统一的主客体安全标记，安全标记随数据全程流动，并在不同访问控制点之间实现访问控制策略的关联，构建各个层面强度一致的访问控制体系。

c） 审计追查技术

应立足于现有的大量事件采集、数据挖掘、智能事件关联和基于业务的运维监控技术，解决海量数据处理瓶颈，通过对审计数据快速提取，满足信息处理中对于检索速度和准确性的需求；同时，还应建立事件分析模型，发现高级安全威胁，并追查威胁路径和定位威胁源头，实现对攻击行为的有效防范和追查。

d） 结构化保护技术

应通过良好的模块结构与层次设计等方法来保证具有相当的抗渗透能力，为安全功能的正常执行提供保障。高等级保护对象的安全功能可以形式表述、不可被篡改、不可被绕转，隐蔽信道不可被利用，通过保障安全功能的正常执行，使系统具备源于自身结构的、主动性的预防能力，利用可信技术实现结构化保护。

e） 多级互联技术

应在保护各等级保护对象自治和安全的前提下，有效控制异构等级保护对象间的安全互操作，从而实现分布式资源的共享和交互。随着对结构网络化和业务应用分布化动态性要求越来越高，多级互联技术应该在不破坏原有等级保护对象正常运行和安全的前提下，实现不同等级之间的多级安全互联、互通和数据交换。

附 录 D
（资料性）
云计算应用场景说明

本文件中将采用了云计算技术的信息系统，称为云计算平台/系统。云计算平台/系统由设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件等组成。软件即服务(SaaS)、平台即服务(PaaS)、基础设施即服务(IaaS)是三种基本的云计算服务模式。如图D.1所示，在不同的服务模式中，云服务商和云服务客户对计算资源拥有不同的控制范围，控制范围则决定了安全责任的边界。在基础设施即服务模式下，云计算平台/系统由设施、硬件、资源抽象控制层组成；在平台即服务模式下，云计算平台/系统包括设施、硬件、资源抽象控制层、虚拟化计算资源和软件平台；在软件即服务模式下，云计算平台/系统包括设施、硬件、资源抽象控制层、虚拟化计算资源、软件平台和应用软件。不同服务模式下云服务商和云服务客户的安全管理责任有所不同。

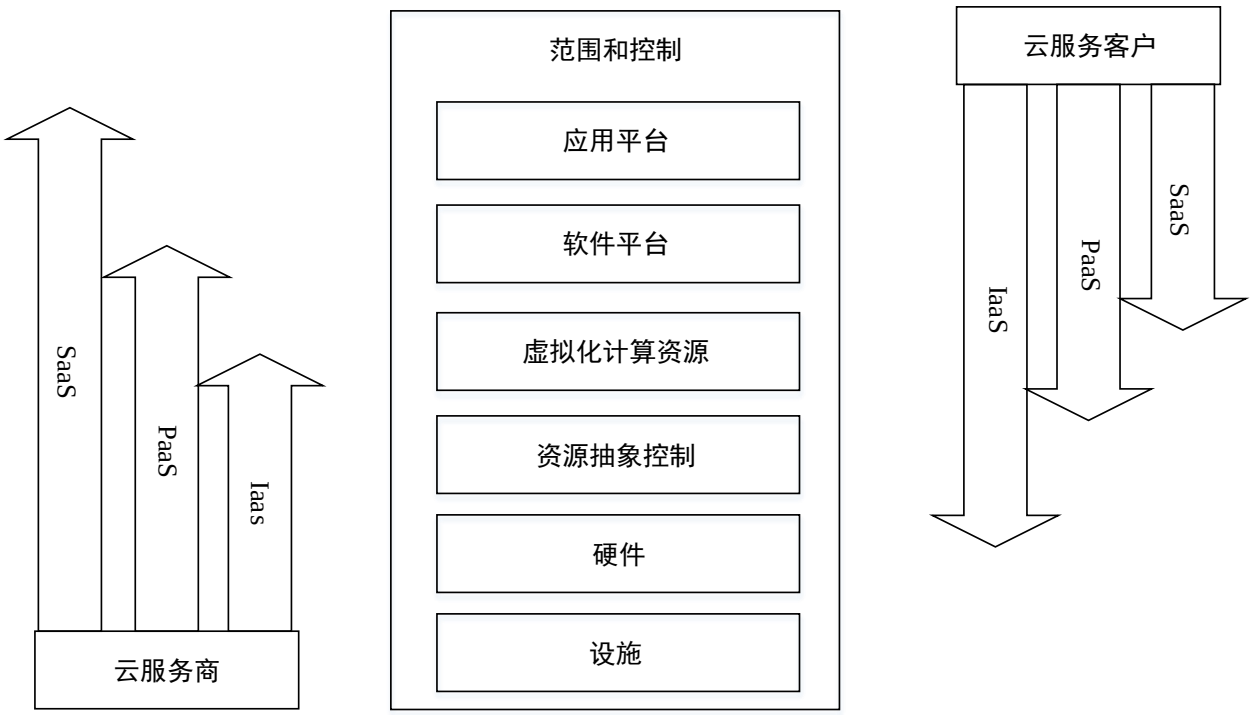


图 D.1 云计算服务模式与控制范围的关系

附 录 E
（资料性）
移动互联应用场景说明

采用移动互联技术的等级保护对象其移动互联部分由移动终端、移动应用和无线网络三部分组成，移动终端通过无线通道连接无线接入设备接入，无线接入网关通过访问控制策略限制移动终端的访问行为，如图E.1所示，后台的移动终端管理系统负责对移动终端的管理，包括向客户端软件发送移动设备管理、移动应用管理和移动内容管理策略等。本文件的移动互联安全扩展要求主要针对移动终端、移动应用和无线网络部分提出特殊安全要求，与安全通用要求一起构成对采用移动互联技术的等级保护对象的完整安全要求。

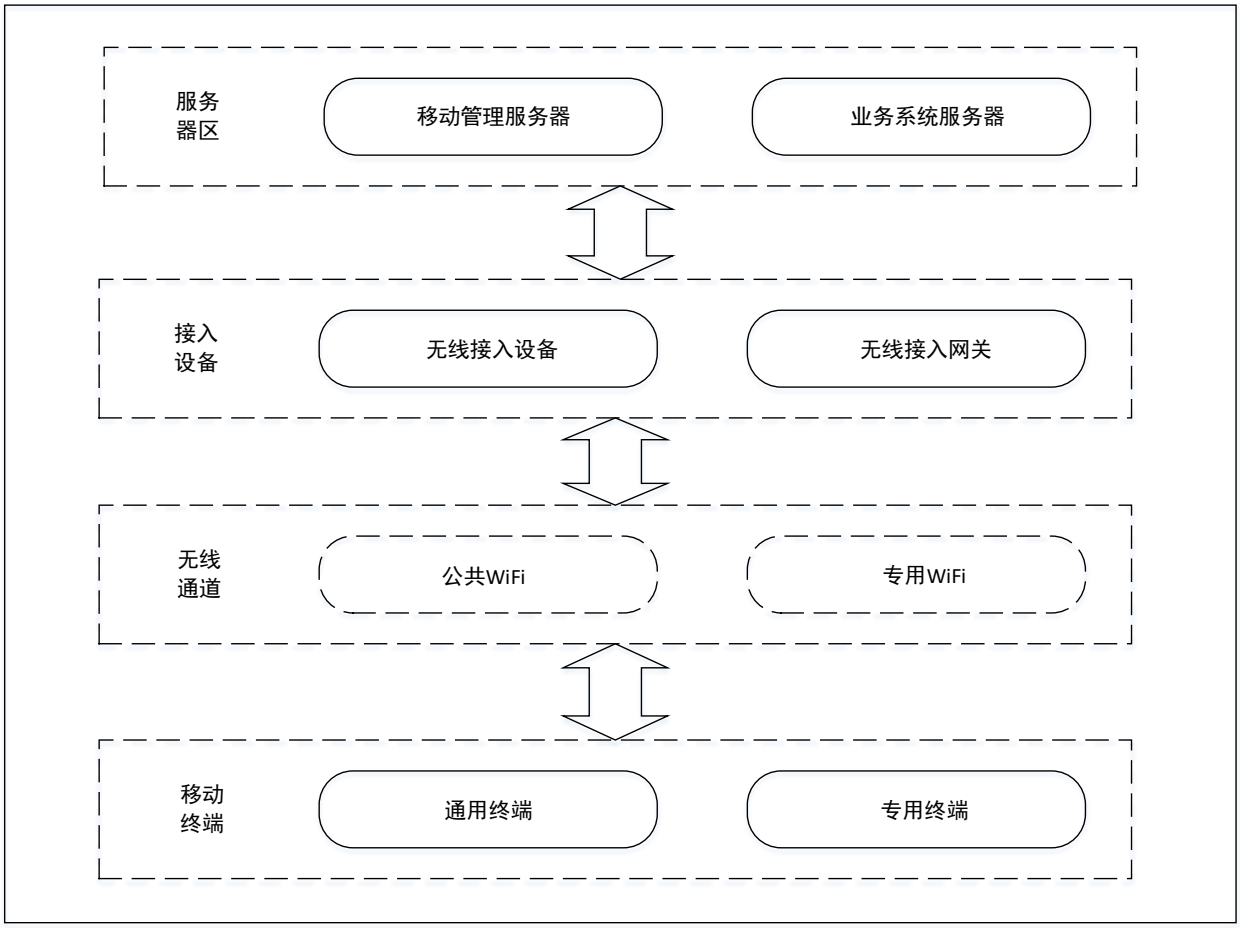


图 E.1 移动互联应用架构

参 考 文 献

[1] GB/T 2887 计算机场地通用规范
[2] GB 50174 数据中心设计规范
[3] GY/T 321—2019 县级融媒体中心省级技术平台规范要求
[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
[5] 县级融媒体中心建设规范（广电发[2019]5号）