附件 1

县级融媒体中心网络安全规范

中共中央宣传部新闻局

国家广播电视总局科技司

2019 年 4 月 9 日

目　　次

前　　言

本规范按照GB/T 1.1—2009给出的规则起草。

请注意本规范的某些内容可能涉及专利。本规范发布机构不承担识别这些专利的责任。

县级融媒体中心网络安全规范

1 范围

本规范规定了县级融媒体中心的网络安全要求，包括技术要求、管理要求和运维要求。

本规范适用于县级融媒体中心的网络安全建设和监督管理。

2 规范性引用文件

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

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 25069—2010 信息安全技术 术语

GY/T 321—2019 县级融媒体中心省级技术平台规范要求

GD/J 037—2011 广播电视相关信息系统安全等级保护定级指南

GD/J 038—2011 广播电视相关信息系统安全等级保护基本要求

GM/T 0054—2018 信息系统密码应用基本要求

县级融媒体中心建设规范（广电发[2019]5号）

县级融媒体中心运行维护规范

3 术语、定义和缩略语

3.1 术语和定义

GB/T 25069—2010、GB 17859—1999、GB/T 22239—2008、GD/J 038—2011界定的以及下列术语和定义适用于本文件。

3.1.1

县级融媒体中心 county-level converged media center

整合县级广播电视、报刊、新媒体等资源，开展媒体服务、党建服务、政务服务、公共服务、增值服务等业务的融合媒体平台。

3.1.2

省级技术平台 province-level technical platform

为县级融媒体中心媒体服务、党建服务、政务服务、公共服务、增值服务等业务开展提供技术支撑、运营维护的省级云平台。

3.1.3

安全保护能力 security protection ability

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复到先前状态等的程度。

3.2 缩略语

下列缩略语适用于本文件。

API 应用程序编程接口（Application Programming Interface）

HTTPS 安全套接字层超文本传输协议（Hyper Text Transfer Protocol over Secure socket layer）

IP 互联网协议（Internet Protocol）

SSH 安全外壳协议（Secure SHell）

VPN 虚拟专用网络（Virtual Private Network）

PC 个人计算机（Personal Computer）

USB 通用串行总线（Universal Serial Bus）

4 网络安全总体要求

4.1 概述

县级融媒体中心网络安全是县级融媒体中心建设的组成部分，县级融媒体中心网络安全措施包括技术措施、管理措施和运维措施，利用省级技术平台开展的业务系统、第三方业务系统及互联网渠道通过边界防护与县级融媒体中心对接，网络安全体系框架如图1所示。

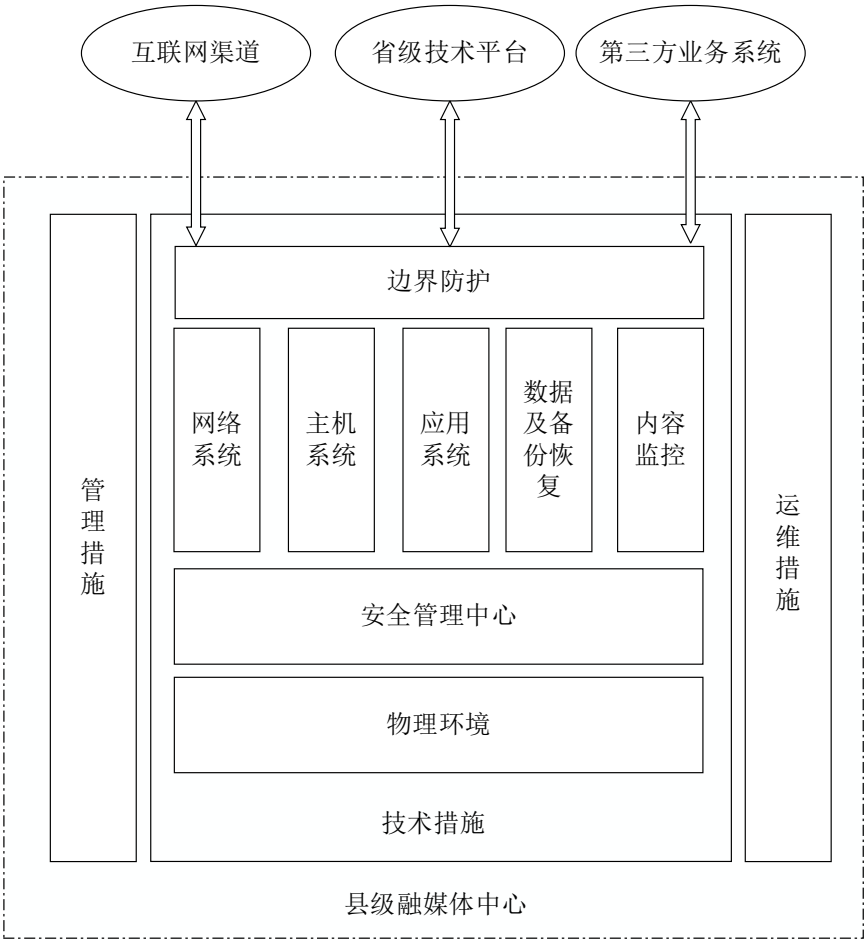

图 1 网络安全体系框架

4.2 基本要求

网络安全应满足以下要求：

a) 县级融媒体中心在建设时应同步规划和设计安全方案，建设网络安全体系，保障网络安全；
b) 县级融媒体中心应按照 GB/T 22240—2008 和 GD/J 037—2011 确定县级融媒体中心网络安全保护等级；
c) 县级融媒体中心部署在省级技术平台的业务系统网络安全应符合 GY/T 321—2019 第 11 章的规定；
d) 县级融媒体中心与省级技术平台的信息互通，采用安全的网络通道或接口进行信息传输，应符合《县级融媒体中心建设规范》5.1 的规定；
e) 县级融媒体中心与第三方的信息互通时，应有身份识别、认证、授权、信息隔离和加密等相关安全手段；
f) 县级融媒体中心的广播电视播出系统安全保护能力应符合 GD/J 038—2011 的规定；
g) 县级融媒体中心的广播电视播出系统的系统配置、技术维护、运行管理、应急处置、基础设施应符合《广播电视安全播出管理规定》的规定；
h) 县级融媒体中心在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；
i) 本规范未提出的其他技术要求，应符合 GB/T 22239—2008 的规定；
j) 县级融媒体中心网络安全管理要求应符合 GB/T 22239—2008 的规定；
k) 县级融媒体中心信息系统中使用的密码技术应符合 GM/T 0054—2018 的规定。

5 网络安全技术要求

5.1 概述

根据《县级融媒体中心建设规范》规定的建设内容，从物理环境、网络系统、主机系统、应用系统、数据及备份恢复、内容监控和安全管理中心7个方面提出网络安全的技术要求。

5.2 物理环境

县级融媒体中心物理环境应符合GB/T 22239—2008的规定。

5.3 网络系统

5.3.1 结构安全

本项要求包括：

a) 应保证信息系统的网络结构稳定，对网络设备进行安全配置和安全加固；应保证融合发布等重要系统的关键网络设备配置冗余、处理能力和网络带宽冗余，满足业务高峰期系统安全、稳定运行的需要；
b) 按照业务的重要性次序定义优先级，保障在网络发生拥堵时优先保证重要业务；
c) 应合理规划路由，确保终端与服务器之间建立安全路径；
d) 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，系统内部应通过有线方式进行组网；
e) 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；
f) 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；
g) 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；

h) 应隔离业务测试区和生产网，所有业务测试、调试和上线前工作均在测试区进行；
i) 应绘制与当前运行情况相符的网络结构拓扑图，并在网络结构变更时及时更新。

5.3.2 安全接入与访问控制

本项要求包括：
a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则；
b) 通过互联网或其他外部公共网络访问县级融媒体中心的信息系统，应使用 VPN 等安全方式接入，通过证书等认证机制，对内部用户权限进行管理，控制粒度为网段、用户/用户组级；
c) 使用 VPN 等安全接入方式访问内部网络时，应对接入的 PC 及移动设备进行安全检查；
d) 应配置备用访问控制策略，在安全风险意外发生时启用该策略；
e) 应定期优化安全访问控制规则，审计、调整冗余策略、冲突策略、无用策略，精简访问控制规则，提高安全运维效率。

5.3.3 安全审计

本项要求包括：
a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个内部用户，对重要的内部用户行为和重要安全事件进行审计；
b) 审计内容包括对关键网络设备的运行状况、内部用户日常行为活动等重要事件；
c) 审计记录应包括但不限于事件的日期、时间、用户名、IP 地址、事件类型、事件是否成功等；
d) 应保护审计记录，定期备份，避免未预期的删除、修改或覆盖等，审计记录至少保存 6 个月；
e) 宜建立集中日志管理中心，对审计日志进行异构集中存储，避免审计日志数据因本地故障不可恢复；
f) 应定期对审计记录进行分析，以便及时发现异常行为。

5.3.4 边界完整性检查

本项要求包括：
a) 应能够对内部用户非授权连到外部网络的行为进行检查或限制；
b) 应能够对非授权设备私自接入内部网络的行为进行检查或限制；
c) 针对内部用户传送重要文件、数据到外网的情况，宜通过内容过滤、防泄漏等手段进行管控。

5.3.5 入侵防范

本项要求包括：
a) 应在与外部网络连接的网络边界处监视端口扫描、木马后门、病毒传播等常见攻击行为，并对攻击行为进行告警、过滤、拦截阻断；
b) 宜具备对新型网络攻击的检测和防御能力；
c) 宜具备对加密流量攻击的检测和防御能力。

5.3.6 恶意代码防范

本项要求包括：
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；
b) 防恶意代码系统应与信息系统内部防恶意代码系统具有不同的恶意代码库。

5.3.7 网络设备防护

本项要求包括：

a) 应对登录网络设备的内部用户进行身份鉴别，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) 应授予对不同角色的内部用户完成各自承担任务所需的最小权限；
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) 应对网络设备进行基本安全配置，明确业务必需的端口，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) 应采用 HTTPS、SSH、VPN 等技术手段，对网络设备进行远程管理，防止鉴别信息在网络传输过程中被窃听；
g) 应定期检查并锁定或撤销网络设备中多余的内部用户账号及调试账号。

5.3.8 安全数据交换

本项要求包括：
a) 融合发布系统与其他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措施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，可通过协议转换的手段，以信息摆渡的方式实现数据交换。

5.4 主机系统

5.4.1 身份鉴别

本项要求包括：
a) 应对业务系统和管理系统的内部用户进行身份标识和鉴别，应为不同内部用户分配不同的用户名，不能多人使用同一用户名；
b) 系统管理内部用户身份鉴别信息应具有不易被冒用的特点，口令长度应符合相关安全等级要求，口令应定期更换，用户名和口令禁止相同，口令满足复杂性要求；
c) 应具备登录失败处理功能，可提供结束会话、限制非法登录次数和自动退出等措施；
d) 宜对登录核心网络设备、主机设备、应用系统的用户进行多重身份验证；
e) 当对服务器进行远程管理时，应采用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。

5.4.2 访问控制

本项要求包括：
a) 应启用访问控制功能，依据安全策略控制内部用户对资源的访问路径与粒度；
b) 应禁止通过 USB、光驱等外设进行数据交换，关闭不必要的服务和端口；
c) 应实现操作系统和数据库系统内部用户的权限分离；
d) 应限制默认账户的访问权限、默认账户的重命名、账户默认口令的修改；
e) 应及时删除多余、过期账户，避免存在共享账户。

5.4.3 安全审计

本项要求包括：

a) 应对系统中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事件；
c) 审计记录应包括但不限于事件的日期、时间、类型、用户、事件是否成功等；
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 6 个月；
e) 宜建立集中日志管理中心，对审计日志进行异构集中存储，避免审计日志数据因本地故障不可恢复；
f) 应定期对审计记录进行分析，以便及时发现异常行为，并进行告警。

5.4.4 入侵防范

本项要求包括：
a) 应遵循最小化安装原则，仅安装业务所需的组件和应用程序，服务器应专机专用，在采集、制播等服务器上关闭不必要的端口；
b) 融合发布系统的终端应根据需要定期更新操作系统安全补丁；
c) 融合发布系统的服务器应根据需要定期更新操作系统安全补丁，更新前应进行测试工作。

5.4.5 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，融合发布系统的服务器可根据需要部署异构的防恶意代码软件，应定期更新防恶意代码软件版本和恶意代码库。

5.4.6 资源控制

本项要求包括：
a) 应配置相关安全策略，限制终端的登录方式、登录范围及登录空闲时长；
b) 应限制单个内部用户对系统资源的最大和最小使用限度。

5.4.7 冗余配置

融合发布系统的核心服务器应具有冗余配置。

5.4.8 完整性配置

与发布直接相关的重要执行文件目录、配置文件目录应设置完整性监控措施，对重要文件的变更进行监控。

5.4.9 数据共享

本项要求包括：
a) 应关闭主机自身的共享服务，所有数据共享通过集中共享服务器进行；
b) 应对数据共享目录进行严格的权限设置，分配访问账号及账号权限，且该账号对其他系统目录无任何访问权限；
c) 共享目录内应单独设置写目录，且为该目录设置独立的账号权限，同时该账号对其他系统目录无任何访问权限；
d) 配置相关措施，取消共享目录内所有文件的执行权限。

5.4.10 移动终端安全

本项要求包括：
a) 移动终端接入网络及访问应用时，应对用户与设备进行认证及授权；
b) 应对进行媒体信息采集的移动终端设备进行安全性检测。

5.5 应用系统

5.5.1 身份鉴别

本项要求包括：

a) 在应用系统正式投入使用之前，应删除临时用户、测试用户、匿名用户、默认用户，修改默认管理员的用户名称和密码；
b) 应对登录业务系统的用户进行身份标识和鉴别；
c) 用户口令应满足密码复杂度要求，至少 6 个月更换一次；
d) 应采用安全连接的方式完成身份鉴别过程。

5.5.2 访问控制

本项要求包括：

a) 应保证所有外部用户不具备登录系统主机的权限，且应用本身不以系统管理员身份运行；
b) 应授予内部用户完成各自执行任务所需的最小权限,且仅能操作特定目录,不能操作系统文件；
c) 应具备会话管理功能，自主设置登录验证次数、最大空闲时间；
d) 应设置相关安全防护措施，保护用户注册信息等个人隐私数据，防止信息泄露；
e) 禁止在互联网暴露管理页面和管理端口，设置 VPN 等安全传输通道，用于日常管理活动，防止管理入口的暴露。

5.5.3 安全审计

本项要求包括：

a) 应具备对各业务系统的安全审计功能；
b) 审计内容应包括操作对象、用户登录、页面访问、数据库连接、配置修改、核心业务的相关操作等；
c) 审计记录应包括但不限于事件的日期、时间、发起者信息、类型、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 6 个月；
e) 宜建立集中日志管理中心，对审计日志进行异构集中存储，避免审计日志数据因本地故障不可恢复。

5.5.4 安全运行

本项要求包括：

a) 可对各业务系统的默认配置参数进行调整，保证应用程序的运行安全；
b) 宜对业务系统收到的请求数据进行安全检测及过滤，避免各类安全攻击。

5.5.5 通信完整性

县级融媒体中心与外部网络进行通信时，应采用校验技术，保证通信过程中的数据完整性。

5.5.6 通信保密性

本项要求包括：

a) 县级融媒体中心与外部网络进行通信时，宜对重要数据的传输建立加密传输通道；
b) 县级融媒体中心与外部网络进行通信时,应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。

5.5.7 软件容错

本项要求包括：

a) 应配置软件镜像或备份，在故障发生时，由镜像或备份继续提供相关功能；
b) 宜配置软件存储策略，使数据存储具备容错性。

5.5.8 资源控制

本项要求包括：

a) 宜限制对自身执行文件和配置文件的修改；
b) 宜对数据库系统进行资源限定，控制粒度为表级，信息系统以不同的连接权限、连接通道访问对应的数据库表；
c) 信息系统宜为不同目的创建对应的内部用户，限制其资源访问。

5.5.9 完整性配置

融合发布等系统各应用模块的执行文件目录和配置文件目录宜设置完整性监控措施，对重要文件的变更进行监控。

5.5.10 数据共享

本项要求包括：

a) 宜为主机分配特定账号和权限访问相关数据；
b) 宜具备统一的 API 接口，供第三方业务系统访问相关数据，且访问过程需经过身份认证；
c) 宜采用密码技术对使用 API 接口传输的数据进行保护，防止共享数据泄露和被破坏；
d) 宜根据数据共享的操作（只读、读写、只写）不同，分配不同的内部用户账号，使用不同的账号访问对应的文件、目录、数据库；
e) 对于通过互联网发布的媒体信息，宜采用防盗链技术防止信息被非法盗取。

5.5.11 移动客户端

本项要求包括：

a) 移动客户端应采用校验技术保证代码的完整性；
b) 移动客户端上线前宜经专业测评机构进行安全检测；
c) 应保证移动终端安装、运行的客户端来自可靠分发渠道或使用可靠证书签名。

5.6 数据及备份恢复

5.6.1 数据完整性

本项要求包括：

a) 应采用密码相关技术，保障重要数据在存储、处理及传输过程中的完整性，支持国密算法；
b) 应监控业务系统重要数据的完整性，对破坏完整性的事件进行告警。

5.6.2 数据保密性

应采用密码相关技术，保障重要数据在存储、处理及传输过程中的保密性，支持国密算法。

5.6.3 备份和恢复

本项要求包括：

a) 重要业务信息应采取冗余备份技术，确保系统能够及时恢复数据；
b) 对于在省级技术平台存储与处理的重要数据，应在本地保留备份。

5.6.4 数据可用性

宜对融合发布系统等发布直接相关内容数据采取多副本、高可用等冗余措施。

5.6.5 个人信息保护

本项要求包括：

a) 应在文件、数据库表级别，对个人公开信息、个人敏感信息进行区别存储；
b) 应采用密码相关技术，对数据库中个人敏感信息进行加密存储，并使用数据脱敏技术，对敏感信息进行模糊化处理，支持国密算法；
c) 应采用密码相关技术，对个人敏感数据文件内容进行加密存储，支持国密算法。

5.7 内容监控

本项要求包括：

a) 应对内容数据进行基于国密算法的数字签名、验签，具备内容防篡改功能；
b) 内容文件全生命周期中的签名变化可追溯；
c) 应对重要内容数据进行基于国密算法加密保护；
d) 应对内容数据存储过程进行访问控制，有效识别和防范已知、未知入侵破坏；
e) 应具备内容数据被非授权访问、操作时的告警通知功能。

5.8 安全管理中心

本项要求包括：

a) 集中部署账号管理、身份认证、运维管理、审计监察等系统，对所有安全措施进行统一管控；
b) 应对人员访问、人员操作、操作工具、命令执行、运维审计和系统运行监控等进行集中管理；
c) 应对设备运行状态进行集中监控，包括漏洞管理、告警与日志管理、事件管理等；
d) 宜对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理。

6 网络安全运维要求

6.1 概述

根据《县级融媒体中心运行维护规范》的运维要求，从介质管理、设备管理、恶意代码防范管理、漏洞防范管理、配置管理、密码管理、备份与恢复管理、终端接入管理和风险评估管理9个方面，提出网络安全的运维要求。

6.2 介质管理

本项要求包括：

a) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并定期盘点；
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，并对介质的归档和查询等进行登记记录；
c) 应根据承载数据和软件的重要程度对介质进行分类和标识管理。

6.3 设备管理

本项要求包括：

a) 应持续跟踪网络设备软件更新情况，在经过测试评估后进行更新，并在更新前对重要文件进行备份；

b) 应确保信息处理设备经过审批才能带离机房或办公地点；
c) 应对机房安全管理做出规定，包括机房物理访问、物品带进带出和机房环境安全等；
d) 应避免在重要区域接待来访人员，包含敏感信息的纸档文件和移动介质等应妥善保管。

6.4 恶意代码防范管理

本项要求包括：
a) 应提高所有用户的防恶意代码意识，外来计算机或存储设备接入系统前应进行恶意代码检查；
b) 应对恶意代码防范要求做出规定，包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等；
c) 应定期检查恶意代码库的升级情况，并形成报告。

6.5 漏洞防范管理

本项要求包括：
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做出评估并及时进行修补；
b) 实施漏洞扫描或漏洞修补前，应对可能的风险进行评估和充分准备，并做好数据备份和回退方案；
c) 漏洞扫描或漏洞修补后应进行验证测试；
d) 宜定期对移动客户端、网站等对互联网开放的系统开展渗透测试工作。

6.6 配置管理

本项要求包括：
a) 应记录和保存信息系统的基本配置信息，包括网络拓扑结构、各设备安装的软件组件及其版本信息、补丁信息和配置参数等。配置信息记录应予以保管，不得扩散；
b) 应定期对信息系统相关的网络设备、操作系统、数据库、中间件等 IT 设备开展安全健康状态巡检和配置核查工作，对发现的问题进行整改。

6.7 密码管理

应符合国家密码管理的规定。

6.8 备份与恢复管理

本项要求包括：
a) 应规定需要定期备份的重要业务信息、系统数据及软件系统等；
b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等；
c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份和恢复策略；
d) 应建立控制数据备份和恢复的程序，对备份和恢复过程进行记录，所有文件和记录应妥善保存。

6.9 安全事件处置

本项要求包括：
a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件；
b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，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等；
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。

6.10 应急预案管理

本项要求包括：

a） 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；

b） 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练。

6.11 终端接入管理

本项要求包括：

a） 应确保移动终端在安全的网络环境下接入，确保移动终端通过授权接入；

b） 应进行账号管理，对申请账号、建立账号、删除账号等进行控制；

c） 内部终端接入相关网络与信息系统时，应经过相关部门审核；

d） 外部终端接入网络访问，应进行访问权限管理；

e） 终端设备应安装防病毒软件，定期升级病毒库；

f） 应定期检查非法接入和非法外联行为，发现异常行为，立即处理并记录。

6.12 风险评估管理

应建立网络安全风险评估机制，定期开展网络安全风险评估，并针对安全风险采取相应安全措施。

参 考 文 献

[1] 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
[2] 中华人民共和国网络安全法
[3] 新闻出版广播影视网络安全管理办法（试行）（新广办发[2017]4号）
[4] 广播电视安全播出管理规定（广电总局第62号令）