市级融媒体中心网络安全防护基本要求

中共中央宣传部新闻局

发布

国家广播电视总局科技司

2023 年 2 月

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件起草单位：国家广播电视总局广播电视规划院、国家广播电视总局广播电视科学研究院、国家广播电视总局监管中心、中广电广播电影电视设计研究院有限公司、成都东方盛行电子有限责任公司、苏州市广播电视总台、太极计算机股份有限公司、新华三技术有限公司、奇安信科技集团股份有限公司、宁波广播电视集团、北京中科大洋信息技术有限公司、成都索贝数码科技股份有限公司、深信服科技股份有限公司、广信智安（青岛）科技有限公司、华为技术有限公司、北京北大方正电子有限公司、杭州安恒信息技术股份有限公司、深圳市中科网威科技有限公司、武汉广播电视台、贵阳广播电视台、东软集团股份有限公司、三六零数字安全科技集团有限公司。

本文件主要起草人：肖辉、杨木伟、宫铭豪、李炎、董升来、瞿向雷、于成龙、王艳鹏、李望、陈起来、何晶、王磊、张娜、陈奇、唐明、刘科材、杜宏、赵伟、考海鹏、孙黎丽、王琪江、孙岛、党超辉、吴坤生、张永站、卢永波、叶希达、陈光辉、孙国辉、许燕平、张海亮、谢山、侯玉娟、赵占永、甘丽萍、邹力、董伶、王曦光、万晓兰、马凯、姚琼、刘铁柱、皇甫少明、贾晓璐、黄振川。

市级融媒体中心网络安全防护基本要求

1 范围

本文件规定了市级融媒体中心网络安全防护体系构建的基本要求。

本文件适用于市级融媒体中心网络安全防护系统的设计、建设、测试、运维和管理。

注：市级融媒体中心是由地级市、地区、自治州、盟所建设的融媒体中心。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南

GB/T 25069—2022 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 37729—2019 信息技术 智能移动终端应用软件（APP）技术要求

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

GY/T 277—2019 视音频内容分发数字版权管理技术规范

GY/T 321—2019 县级融媒体中心省级技术平台规范要求

GY/T 337—2020 广播电视网络安全等级保护定级指南

GY/T 352—2021 广播电视网络安全等级保护基本要求

市级融媒体中心总体技术规范

市级融媒体中心接口规范

3 术语和定义

GB/T 25069—2022、GB/T 22239—2019、GB/T 22240—2020、GY/T 337—2020、GY/T 352—2021、GY/T 321—2019界定的以及下列术语和定义适用于本文件。

3.1

市级融媒体中心 prefecture-level converged media center

整合地级市、地区、自治州、盟的媒体资源，实现一体化发展的新型媒体机构。

3.2

市级融媒体中心技术系统 prefecture-level converged media center technical system

为市级融媒体中心开展媒体业务及相关服务提供技术支撑、运营维护的技术平台。

3.3

敏感数据 sensitive data

包括但不限于未经行政主管部门批准发布的行业统计数据、行业企事业经营数据、用户数据。

[来源：GY/T 352—2021，3.16，有修改]

3.4

文稿内容 manuscript content

文字类、图片类、图文类、H5链接类新闻内容。

3.5

文稿内容上版 manuscript content select to layout

将文稿内容在网站、客户端和互联网平台等融合发布渠道发布展示，或者将文稿内容选用至报纸版面。

3.6

文稿内容排版 manuscript content typesetting

通过富文本编辑器或可视化方式对文稿内容进行编辑。

4 缩略语

下列缩略语适用于本文件。

APP 应用程序（Application）

HMAC 基于杂凑的消息鉴别码（Hash-based Message Authentication Code）

HTTP 超文本传输协议（HyperText Transfer Protocol）

HTTPS 安全套接层超文本传输协议（HyperText Transfer Protocol over Secure Socket Layer）

H5 超文本标记语言第五版（HTML v5）

IP 互联网协议（Internet Protocol）

SDK 软件开发工具包（Software Development Kit）

SSH 安全外壳协议（Secure Shell）

VPN 虚拟专用网络（Virtual Private Network）

5 市级融媒体中心网络安全基本要求

5.1 概述

市级融媒体中心网络安全防护要求由互联互通接口安全要求、安全技术要求、安全管理要求三部分组成，县级融媒体中心技术系统、省级技术平台、外部平台通过互联互通接口与市级融媒体中心技术平台对接，网络安全框架见图1。

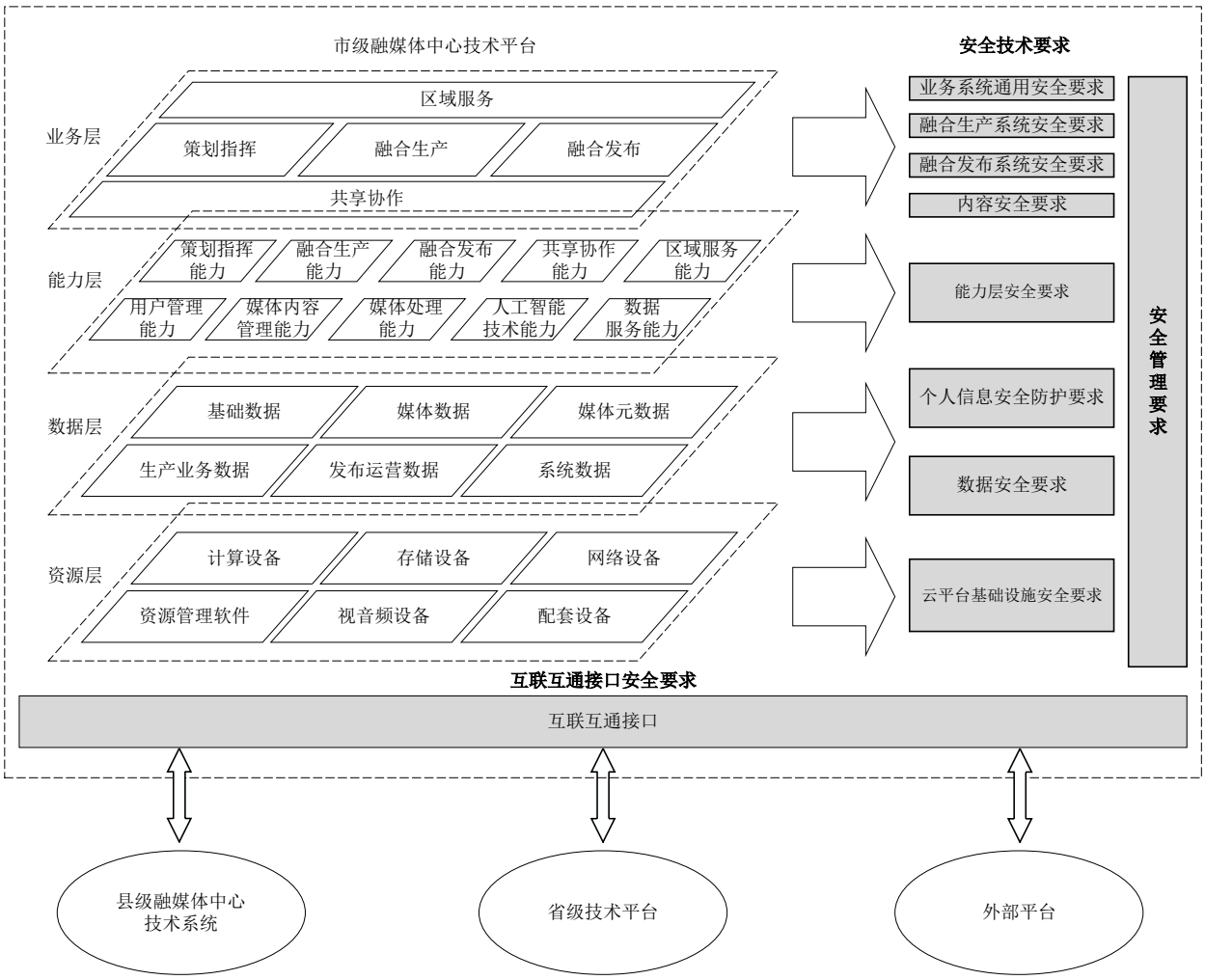

图1　网络安全框架

5.2　总体要求

市级融媒体中心网络安全应满足以下要求。

a) 市级融媒体中心技术平台组成应符合《市级融媒体中心总体技术规范》中的规定，市级融媒体中心接口应符合《市级融媒体中心接口规范》中的规定。

b) 市级融媒体中心信息系统在建设时应同步规划和设计安全方案，建立网络安全保障体系，保障网络安全。

c) 市级融媒体中心应理清网络安全保护边界，明确安全保护工作责任。在系统运行过程中应定期组织开展安全自查、风险评估、等级保护测评和密码应用安全评估，及时发现安全隐患和薄弱环节并予以整改，不断提高网络安全保护能力和水平。市级融媒体中心网络安全防护手段宜通过部署在本地的安全防护系统、设备等实现，根据各地实际情况，也可部分依托相关安全服务平台等外部安全服务能力实现。

d) 市级融媒体中心应采购、使用符合 GB/T 22239—2019、GB/T 39786—2021 规定的网络产品、密码产品及服务。

e) 市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、基础设施要求见《广播电视安全播出管理规定》及其实施细则的相关规定。

5.3　定级要求

网络安全定级要求如下：

a) 按照 GB/T 22240—2020、GY/T 337—2020 的规定，市级融媒体中心的播出系统、融合发布系统安全保护等级为第三级，其他系统安全保护等级为第二级；
b) 当网络功能、服务范围、服务对象和处理的数据等发生重大变化时，市级融媒体中心建设单位或运营单位应变更系统安全保护等级；
c) 市级融媒体中心的信息系统安全保护能力除满足本文件要求外，还应符合 GB/T 22239—2019 和 GY/T 352—2021 的规定。

6 业务层安全要求

6.1 业务系统通用安全要求

6.1.1 安全域划分

安全域划分要求如下。

a) 应按照不同的功能划分不同的安全域，安全域间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；安全域内按业务类型、业务重要性等因素划分不同的子网或网段；应按纵深防御原则将不同系统按重要性或功能性区别部署在层次化网络的核心区域、边界。
b) 三级及以上系统应禁止通过无线方式进行组网，其他系统应限制无线网络的使用，应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。

6.1.2 边界访问控制

边界访问控制要求如下：

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、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。

6.1.3 身份鉴别

身份鉴别要求如下：

a) 业务系统和相关设备应对登录的管理用户进行身份标识和鉴别，身份标识应具有唯一性，身份鉴别口令应满足 8 位以上，由大小写字母、特殊字符、数字四种字符类型的三种及以上组成，口令更换周期应不超过 6 个月；
b) 服务端应启用强制密码复杂度审核功能，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) 三级及以上系统应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对管理用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

6.1.4 业务系统访问控制

业务系统访问控制要求如下。

a) 应对登录的管理用户分配账户和权限，关键业务系统访问控制宜设置单点登录策略。

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，并严格限制默认账号的访问权限。
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) 应限制未登录用户的使用权限，对匿名用户使用记录进行追溯。

6.1.5 入侵防范

入侵防范要求如下：
a) 系统、设备应遵循最小安装的原则，仅安装需要的组件和应用程序；
b) 应关闭不需要的服务、默认共享和高危端口；
c) 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；
d) 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；
e) 三级及以上系统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；
f) 三级及以上系统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；
g) 三级及以上系统当检测到攻击行为时，应记录攻击源 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。

6.1.6 安全审计

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，应保证安全审计措施的有效性和时效性。
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；审计记录保存时长应不少于 6 个月。
d) 三级及以上系统应对审计进程进行保护，防止未经授权的中断。

6.1.7 远程维护

远程维护要求如下：
a) 应能对远程访问市级融媒体中心技术系统的行为进行单独审计，可进行数据分析；
b) 宜对远程访问市级融媒体中心技术系统的用户进行双向身份鉴别。

6.1.8 业务连续性保障

业务连续性保障要求如下：
a) 市级融媒体中心重要业务系统应为网络设备、密码设备等关键设备配置冗余，避免单点故障；
b) 市级融媒体中心应提供重要数据处理系统的热冗余（可配置最小应急系统或镜像软件系统或备份系统等），保证系统的高可用性。

6.1.9 运行监控

运行监控要求如下：
a) 应具备计算资源、网络资源、存储资源监控能力，且具有告警提醒功能；
b) 应具备应用程序、数据库等监测能力，且具有告警提醒功能；
c) 应具备接收和上报安全预警信息的能力；

d) 宜具备网络流量的捕获与还原能力，实现对网络通信原始流量的留存取证；
e) 应支持业务流程和流程执行状态的监控，且具有告警提醒功能；
f) 宜支持关键设备日志及核心服务日志的检测能力，且具有告警提醒功能；
g) 宜支持安全告警信息的保存、展示、统计和分析处理能力。

6.2 融合生产系统安全要求

6.2.1 内容制作

内容制作要求如下：
a) 应物理或逻辑分开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；
b) 应加强对技术系统的病毒防御，对于移动存储介质文件、链接文件等进行病毒、木马的查杀处理后方可导入技术系统中；
c) 应加强用户终端接入控制，对终端接入应实现差异化的安全控制策略，所有接入终端应安装防病毒软件并定期做安全检查，操作系统应及时补丁升级；
d) 应对内容制作系统使用部门和人员按需划分角色、设置权限和分配账号，应按角色权限限定内容文件访问范围。

6.2.2 内容传输

内容传输要求如下：
a) 文件传输完成时应对文件进行完整性校验，确保文件传输一致性；
b) 技术系统之间进行文件传输时，应对文件类型及格式进行限定；
c) 应对节目传输过程中携带的可执行脚本或可执行的二进制文件进行恶意代码检测，避免恶意程序的传播；
d) 应支持对文件传输的渠道、时间、格式类型、操作人员等信息进行记录和留存；
e) 宜支持内容传输身份鉴别信息具有复杂度要求并定期更换。

6.2.3 内容共享

内容共享要求如下。
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) 应对内容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；内容共享应只将账号提供给必须访问内容的人，避免不必要的共享；共享内容应设置有效期，过期后自动失效。
c) 内容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) 应配置相关措施，取消共享目录内所有文件的执行权限。

6.2.4 内容管理

内容管理要求如下。
a) 应对融合生产系统使用部门和人员按需划分角色，设置权限和分配账号；不同人员可按角色权限限定内容文件访问范围。
b) 应保证内容文件生产全流程操作可追溯、状态可留存，实现对内容文件操作日志审计、内容文件多版本比较和管理，审计日志应保留不少于 6 个月。

6.3 融合发布系统安全要求

6.3.1 内容安全传播要求

6.3.1.1 行为安全

对于非法广播电视频道、未取得信息网络传播视听节目许可证的视听节目网站以及未经备案的新闻信息网站，不应进行转播、链接、聚合与集成。

应不存在转载、链接未经授权的新闻文稿、视听节目以及其他未经授权的内容。

6.3.1.2 应用安全

应安装防病毒软件和页面防篡改系统，并定期进行木马病毒查杀和安全漏洞扫描。不存在已公布的中危及以上风险漏洞。

6.3.1.3 传输安全

应根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。传输重要数据（包括但不限于“敏感个人信息”）和核心数据的，应采取校验技术、密码技术、安全传输通道或者安全传输协议等措施。

6.3.2 SDK 集成要求

在集成第三方SDK时（如埋点统计SDK），应向用户明确标识第三方SDK的身份或类型，SDK是否会收集用户敏感信息等。如有收集用户敏感信息行为，应给予明确提示，用户可选择不允许。

6.3.3 融媒体客户端安全要求

6.3.3.1 服务安全性要求

6.3.3.1.1 客户端安全管理要求

应具备节目和信息安全传播管理制度，应具备安全保护技术措施。

6.3.3.1.2 节目安全传播要求

融媒体客户端应满足GB/T 37729—2019中4.7的安全性要求，不应存在已公布的中危及以上风险漏洞。

融媒体客户端宜使用HTTPS协议对传输数据进行加密。

6.3.3.2 客户端用户权限控制要求

融媒体客户端在申请用户权限时，不应“不给权限不让用”，即融媒体客户端安装和运行时，向用户索取与融媒体服务功能无关的权限时，用户拒绝授权后，应用不应退出或关闭。

在不影响融媒体服务功能的前提下，融媒体客户端不应强制捆绑权限。

6.3.3.3 客户端用户行为安全要求

融媒体客户端应具备对评论、弹幕、留言等内容的审核功能，支持过滤、屏蔽违规言论，并支持可溯源，应支持关键词自动识别和过滤，宜支持文字语义识别技术。

融媒体客户端应提供用户举报功能，明确标识举报入口，管理和处置举报信息并建立相应技术手段。

融媒体客户端应支持头像、昵称等用户内容的审核功能。

6.3.3.4 数字版权管理能力要求

宜集成GY/T 277—2019中第10章规定的DRM客户端功能，支持对已获广播电视主管部门批准的信息网络传播视听节目许可证或者备案编号的视听内容的保护。

6.4 内容安全要求

6.4.1 视听内容安全要求

6.4.1.1 内容汇聚

内容汇聚要求如下：

a) 不得汇聚境内外非法广播电视频道、未取得信息网络传播视听节目许可证的视听节目网站内容；
b) 对于通过开放接口获取内容的情况，应明确与内容服务提供者的合作方式和权责划分；
c) 宜具备汇聚内容伪造防范能力，包括但不限于视听内容伪造鉴别能力；
d) 应具备汇聚内容版权信息管理能力，避免因版权授权不清晰引发的纠纷。

6.4.1.2 内容上传与入库

内容上传与入库要求如下。

a) 应设置内容上传目录为不可执行权限；应将上传的文件进行随机重新命名。
b) 节目素材应通过信息标识、检索、筛选等措施，保障节目源可追溯可管理；应记录并留存节目入库相关信息，如时间、渠道、编辑历史等。
c) 应具备黑白名单机制，只允许可确保安全的内容类型进入到内容库。

6.4.1.3 内容管理

内容管理要求如下。

a) 应从业务特征、重要程度等方面对节目内容实行分类分级，以实现不同的管理控制策略，具备特殊价值的节目应有近线备份或异地备份。
b) 应支持对文本、图片、音视频等形式的违法违规不良信息的识别和过滤。
c) 应制定节目内容检测规则，具备实施和更新检测规则的技术措施；宜具有与业务规模相适应的人物、敏感词、敏感标志等敏感信息样本库，可根据变化自行修改更新样本内容；宜支持对节目内容中的敏感信息准确识别和提示，并采用相应的禁用密级处理，保障成品节目内容纯净。
d) 宜在内容发布前采用数字水印技术对原创内容进行版权声明。
e) 宜具备原创内容版权信息管理能力，重要原创内容宜进行第三方版权注册，保护版权。

6.4.1.4 内容发布

内容发布要求如下：

a) 应具备内容发布前的审核能力，确保内容先审后发；
b) 宜针对不同发布渠道嵌入水印信息，支撑重要原创内容版权内容盗版溯源和维权；
c) 相关系统宜具备符合 GY/T 277—2019 的分发版权保护能力，支持对已获广播电视主管部门批准的信息网络传播视听节目许可证或者备案编号的视听内容的保护；
d) 内容向用户展现过程中不应转播、链接、聚合、集成境内外非法广播电视频道、未取得信息网络传播视听节目许可证的视听节目网站和其他非法网站；
e) 宜采用相关技术措施防止内容在传播过程中被非法篡改；
f) 宜采用防盗链技术防止视听节目内容被非法盗链。

6.4.2 文稿内容安全要求

6.4.2.1 文稿内容汇聚

文稿内容汇聚要求如下：

a) 不应汇聚境内外未经备案的互联网网站文稿内容；
b) 不应汇聚境内外未经官方应用市场上架的非法客户端文稿内容；
c) 宜具备对来源于各种渠道的文稿内容语义级、多维度鉴别能力，包括但不限于违禁文字鉴别、低俗污秽文字鉴别、色情敏感违禁图片鉴别、木马色情链接鉴别等；
d) 应具备对汇聚的文稿内容进行版权信息管理能力，如版权所有人、授权范围、授权期限等。在使用版权文稿内容时，应显示标注内容来源，避免因版权授权不清引起的纠纷。

6.4.2.2 文稿内容管理

文稿内容管理要求如下：

a) 文稿内容在分发前应设置多轮审核和校对流程，审核人员和校对人员应由具备相应从业资质和职称的专职人员负责；
b) 文稿内容在分发前应经过多轮审核才可进入待分发库，应支持按不同类型文稿内容设定不同审核流程，审核流程全程应支持留痕，审核流程中任何两个审核环节不能同时由同一人担任；
c) 文稿内容在分发前应设定多次校对环节，专职校对人员应通读文稿，对文字排版、文字质量、报纸小样等进行校对；
d) 宜具备文稿内容语义级、多维度自动鉴别与智能审校能力，包括但不限于违禁文字鉴别、低俗污秽文字鉴别、色情敏感违禁图片鉴别、木马色情链接鉴别等；
e) 应具备原创内容版权信息管理能力，宜借助区块链技术实现对重要原创文稿内容的版权保护；
f) 针对图片类内容在分发前宜采用数字水印技术，对原创内容进行版权保护；
g) 对于面向个人提供互联网投稿、新闻线索提交、新闻报料等服务时，应建立独立于融媒体生产平台的互联网文稿内容库和存储，在提交文稿内容时应提示用户不得提交国家相关法律法规禁止传播的文稿内容。

6.4.2.3 文稿内容上版

文稿内容上版要求如下。

a) 宜采用区块链技术对重要原创文稿内容分发至不同渠道，并记录不同的分发信息，确保重要原创文稿版权内容盗版溯源和维权。
b) 对于用于报纸出版的文稿内容应建立完备的使用状态标准，包括上栏态、签发态、上版态、见报态和转改态等状态。文稿内容处在不同状态时应有对应的使用权限，通过状态流转确保文稿上版安全。
c) 对于用于报纸出版的图片类内容宜使用融媒体平台配套的图片制作软件进行制作，生成报纸出版兼容的图片格式，不宜脱离融媒体平台使用第三方图片制作软件进行制作。

6.4.2.4 文稿内容排版

文稿内容排版要求如下：

a) 发布到融媒体客户端、网站、互联网平台的文稿内容在展现过程中不得转载、链接、聚合境内外未经备案的互联网网站文稿内容和境内外未经官方应用市场上架的客户端文稿内容；
b) 在展示有版权文稿内容时，应按照主管部门相关要求，在展示界面显著位置展示已获主管部门批准的服务类别、服务形式、服务名称、服务地址等互联网新闻信息服务许可证及编号；
c) 针对有版权的图片内容应采用防下载技术防止内容被非法下载；
d) 针对有版权的图片内容应采用防盗链技术防止内容被非法引用；
e) 报纸版面排版流程中应设置专职的版面排版人员和版面审核人员，建立完善的版面审核机制，不同人员应严格控制权限范围，排版全流程操作可追溯，状态可留存；

f） 报纸版面排版流程应具备完善的版面状态，包括开放态、排版态、排版完成态、大样签发态、废弃态等。版面处在不同状态时应有对应的操作权限，通过状态流转确保版面排版安全可控。大样文件进行完整性校验，避免在传版过程中被篡改；排版过程保留文稿内容的全流程修改痕迹。

7 能力层安全要求

能力层安全要求如下：

a） 应为能力模块划分独立的安全域，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，安全域内应按业务类型、业务重要性等因素划分不同的子网或网段；
b） 应支持关键设备冗余机制、负载均衡机制，确保能力调用的连续性；
c） 应为调用实体分配唯一标识和密钥，密钥信息应满足复杂度要求；
d） 应支持限制不同调用实体的资源访问权限。

8 数据层安全要求

8.1 数据安全基本要求

8.1.1 数据安全管理制度

数据安全管理制度要求如下：

a） 应在符合国家法律规范和相关部门的管理制度前提下，合理开展数据要素治理和数据价值挖掘，促进行业数据资源共享和合规流通；
b） 应制定完善的数据安全管理制度，对数据安全防护和数据合规流通提供全面指导，管理制度需包含安全框架设计、组织建设、运维规范、审查机制等方面内容；
c） 应委派专人和组织整体负责数据安全管理，并明确划分责权；
d） 宜建立数据安全运营相关的组织、流程和作业规范，围绕数据全生命周期开展安全巡检、安全处置、安全策略、安全分析、安全应急等安全运营工作，建立数据安全常态化运营机制；
e） 宜建立数据安全监管相关的组织，围绕数据全生命周期开展数据安全合规审计、数据安全业务审计等安全监审工作，建立数据安全常态化监管机制；
f） 应对数据进行分类分级管理，并定期进行风险评估和安全自查。

8.1.2 数据采集安全

数据采集安全要求如下：

a） 应在采集过程中遵循最小原则，对于非必要信息不进行采集；
b） 采集中涉及个人敏感信息，应给予充分的说明，应包含采集的用途、存储和使用方式、加密措施、采集的必要性等，并获得被采集信息者的授权；
c） 从公开数据集、数据提供方、数据合作方等数据源采集到的信息，要进行数据确权，并明确使用范围、使用权限等，应确保采集的数据真实有效。

8.1.3 数据传输和存储安全

数据传输和存储安全要求如下：

a） 应采用密码技术保证数据传输过程中的机密性（媒体文件类数据除外）和完整性；
b） 应使用密码技术对通信双方实体进行身份鉴别，保证实体身份的真实性；
c） 应对数据传输过程进行完整记录，并提供不少6个月的日志存储，为数据传输提供日志审计；
d） 应根据数据重要性、量级、使用频率等因素将数据分类分级存储；

e） 应使用密码技术保证包含敏感数据内容存储的机密性，如个人敏感数据、国家机密数据等数据；
f） 数据存储应建立数据冗余和数据一致性校验策略。

8.1.4 数据使用和共享安全

数据使用和共享安全要求如下：
a） 数据使用和数据共享应提供必要性和使用方式说明，确保数据使用和共享符合监管机制，确保数据的合法合规使用；
b） 数据在使用和共享时，对于敏感数据应采用加密技术保证机密性和完整性，可根据业务需要采用整库加密、表加密、字段加密、数据脱敏等技术方式；
c） 数据在使用和共享时，应对操作过程进行身份鉴别和过程审计，日志记录和审计报告应至少保存 6 个月，审计日志应至少包括时间、事件类型、操作主体、事件内容、操作结果（成功或失败）等内容；
d） 共享数据使用方应对共享数据的操作和使用进行记录，并按照约定的数据使用规则进行检查，对常见的密码破解、拒绝服务、数据爬虫等攻击和异常操作进行检测，并及时阻断、告警和记录；
e） 宜能识别数据访问过程异常，动态调整访问权限，防止越权访问，数据泄露；
f） 宜采用水印等技术保证数据共享过程中数据可追溯；
g） 宜根据数据共享的操作（只读、读写、只写）不同，分配不同的用户账号，使用不同的账号访问对应的文件、目录、数据库等数据源；
h） 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。

8.1.5 数据备份安全

数据备份安全要求如下：
a） 应提供本地或异地数据备份，宜每天进行数据备份，备份介质场外存放；
b） 在环境发生变更时，应保证所备份数据的可恢复；
c） 备份介质应严格管理，防止未经授权访问备份数据；
d） 应采用冗余技术保证关键应用的高可用性。

8.1.6 数据销毁

数据销毁要求如下：
a） 存储数据的存储期限应不超过实现数据处理目的所必要的期限；
b） 应采用消磁、损坏等技术保证敏感数据被彻底销毁。

8.2 个人信息安全保护要求

个人信息安全保护要求应符合 GB/T 35273—2020 的规定。

9 资源层安全要求

9.1 通则

市级融媒体中心资源层包括计算设备、存储设备、网络设备、资源管理软件、视音频设备、配套设备等内容，可直接部署，也可采用云计算技术部署。

云平台基础设施安全要求是针对采用云计算技术部署市级融媒体中心技术系统的情况，在满足其他安全要求的基础上的扩展要求。

9.2 云平台基础设施安全要求

9.2.1 等级保护能力要求

应保证云计算平台安全保护等级不低于其承载的市级融媒体中心技术系统的安全保护等级。
云计算平台应符合GB/T 39786—2021相应等级的密码应用基本要求。

9.2.2 安全防护

安全防护要求如下：

a) 应具有根据市级融媒体中心技术系统需求提供通信传输、边界防护、入侵防范等安全机制的能力；
b) 应具有根据市级融媒体中心技术系统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；
c) 应能检测到市级融媒体中心技术系统虚拟机与宿主机、虚拟机与虚拟机之间的异常流量；
d) 应能在检测到网络攻击行为、异常流量情况下进行告警。

9.2.3 资源隔离

应实现承载的市级融媒体中心技术系统与其他系统资源（计算、存储、网络等）隔离。

9.2.4 镜像和快照保护

镜像和快照保护要求如下：

a) 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；
b) 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。

9.2.5 安全管理

安全管理要求如下：

a) 应保证云服务商对市级融媒体中心技术系统的操作可被市级融媒体中心技术系统责任方审计；
b) 应确保只有在市级融媒体中心授权下，云服务商或第三方才具有市级融媒体中心技术系统的访问与管理权限。

10 互联互通接口安全要求

10.1 总体要求

互联互通接口应符合《市级融媒体中心接口规范》中的规定，包括：市级融媒体中心与省级技术平台、县级融媒体中心之间的接口，市级融媒体中心与外部平台之间的接口，市级融媒体中心对外提供的支撑技术能力开放接口；本章从接口访问控制、接口安全审计、接口认证 3 个方面提出互联互通接口安全的技术要求，互联互通接口其他部分应符合《市级融媒体中心接口规范》中的规定。

10.2 接口访问控制要求

接口访问控制要求如下：

a) 应支持基于协议端口的访问控制功能；
b) 应支持基于 IP 的黑白名单访问控制功能；
c) 应支持交互失败时的交互恢复功能；
d) 宜支持接口调用限流功能，宜具备接口调用限流的手动或自动触发机制。

10.3 接口安全审计要求

接口安全审计要求如下：

a) 应支持对互联互通接口交互的过程和状态进行记录和监控；
b) 应支持接口调用的日志记录，包括但不限于接入验证、修改、控制、传输等日志类型；
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，审计记录应至少保存 6 个月。

10.4 接口认证要求

接口认证安全类功能要求如下：

a) 应支持每次接口调用的身份合法性校验；
b) 接口宜采用杂凑算法对每次请求进行签名验证，防范请求被篡改；
c) 接口宜支持对每次请求进行时间戳超时验证，防范接口重放攻击；
d) 宜采用加密通信协议，防止数据明文传输，如：HTTPS 传输协议。

接口认证安全类实例见附录A。

11 安全管理要求

11.1 安全管理制度

安全管理制度要求如下：

a) 应制定市级融媒体中心网络安全防护工作的总体方针和安全策略，阐明安全工作的总体目标、范围、原则和安全框架等；
a) 应对市级融媒体中心各类管理内容建立安全管理制度，并明确各角色职责、流程描述等内容；
b) 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。

11.2 安全管理人员

安全管理人员要求如下：

a) 市级融媒体中心应设立专职的网络安全管理岗位，负责网络安全管理和密码管理；
b) 应具备岗位设置方案、岗位职责说明书、人才储备计划等文件；
c) 应制定培训、考核计划，对网络安全基础知识、密码基础知识和设备操作知识、岗位操作规程等进行培训和考核。

11.3 安全建设

安全建设要求如下：

a) 应在系统建设前制定安全整体规划和安全方案，并在评审后按照规划和方案建设实施；
b) 应在系统建设前制定工程实施方案。

11.4 安全测评

安全测评要求如下：

a) 应进行上线前的等级保护测评，并出具测评报告，等级保护测评通过后方可上线运行；
b) 应进行上线前的密码应用安全性评估，并出具商用密码应用安全性评估报告；
c) 上线后，应定期进行等级保护测评、风险评估，形成安全测评报告，并及时整改；
d) 上线后，宜定期对重点业务功能和接口进行压力测试，找出性能瓶颈，及时优化迭代；
e) 宜委托行业内测评机构进行安全测评、业务性能测评。

11.5 密码管理

密码管理要求如下：

a) 应使用国家密码管理部门认证核准的密码技术、产品和服务；
b) 应制定密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；
c) 市级融媒体中心技术系统应符合 GB/T 39786—2021 相应等级的密码应用基本要求。

11.6 漏洞和风险管理

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) 市级融媒体中心重要业务系统的安全漏洞修复工作应先在测试环境中测试通过，在生产环境实施时，应对重要文件备份，同时应做好应急预案，发现问题后及时回退。

11.7 网络和系统安全管理

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) 应针对市级融媒体中心重要业务系统建立7×24h网络安全监测制度，及时对网络安全事件进行监测和处理。

11.8 恶意代码防范管理

恶意代码防范管理要求如下：

a) 应提高防病毒意识，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。

11.9 安全事件处置

安全事件处置要求如下：

a) 市级融媒体中心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；
b) 应及时向安全管理部门报告出现的安全事件。

11.10 集中管控

集中管控要求如下：

a) 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不少于 6 个月；
b) 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；
c) 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；
d) 应保证市级融媒体中心重要业务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。

11.11 应急预案管理

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。

附 录 A
（资料性）
接口认证安全类实例

A.1 基于签名验证的接口认证安全类实例

A.1.1 接口描述

基于签名验证的接口认证，在 HTTP 协议的请求头中包含身份 ID、请求时间戳以及 HMAC 数据，由响应方进行信息验证，从而实现接口认证的过程。

请求方法：GET/POST。

请求 URL：见《市级融媒体中心接口规范》中的附录 A。

A.1.2 请求参数

请求头：

Content-Type: application/json

X-Extend-ID: 7aa640627a5fb2650e2718df7113863a（示例值）

X-Extend-Timestamp: 1654516621644（示例值）

X-Extend-Signature: 04b29480233f4def5c875875b6bdc3b1（示例值）

请求体：

{

……

}

请求头参数说明：

——X-Extend-ID 为市级融媒体中心与通信方商议的 ID；

——X-Extend-Timstamp 为本次请求的时间戳；

——X-Extend-Signature 为本次请求的 HMAC 数据。

签名生成方法如下：

X-Extend-Signature = HMAC-X(Key, ID + ″:″ + RequestMethod + ″:″ + RequestPath + ″:″ + Timestamp + ″:″+HASH(RequestBody))

其中：

——Key 为市级融媒体中心与通信方商议的密钥；

——RequestMethod 为本次请求采用的方法，GET 或 POST；

——RequestPath 为本次请求资源路径 URL；

——HASH(RequestBody)为请求体的杂凑值，如果为 GET 请求，此值为空；

——HMAC-X 为基于 HMAC 的密钥摘要生成算法，如 HMAC-SM3 等。

A.1.3 响应参数

响应头：Content-Type: application/json

消息体包含：结果状态、结果描述、data、支撑技术能力开放接口的任务状态值（在支撑技术能力开放接口中才包含，其他接口不包含该值）；data 值、支撑技术能力开放接口的任务状态值见《市级融媒体中心接口规范》中的附录 A。

支撑技术能力开放接口“成功”返回消息体样例如下：

```
{
 "code": 0,
 "message": "成功",
 "task_status":0,
 "data": {
  ……
  }
}
```

其他接口“成功”返回消息体样例如下：

```
{
 "code": 0,
 "message": "成功",
 "data": {
  ……
  }
}
```

或：

```
{
 "code": 0,
 "message": "成功",
 "data": [
   {
      ……
   }
 ]
}
```

“失败”返回消息体样例如下：

```
{
 "code": -1,
 "message": "安全认证失败：签名无效"或"安全认证失败：ID无效"或"安全认证失败：时间戳超时"或"安全认证失败：其他原因"
}
```

注："code"：0表示成功，非0表示失败。

A.2 基于访问令牌的接口认证安全类实例

A.2.1 概述

基于访问令牌的接口认证，由请求方先从响应方处获取访问令牌；在调用实际接口的过程中，请求方将访问令牌放在HTTP协议的请求头中，响应方进行访问令牌验证，从而实现接口认证的过程。在访问令牌有效期内，可进行访问令牌更新、注销操作。

A.2.2 获取访问令牌

A.2.2.1 接口描述

请求方从响应方处获取访问令牌。

请求方法：POST。

请求URL：http(s)://{域名}/{服务名}/{版本}/[{可选值}]/oauth/token?grant_type=password&appid=<APPID>&secret=<SECRET>

URL 参数说明：

——grant_type 值固定为 password；

——appid 值为市级融媒体中心与通信方商议的 ID；

——secret 值为市级融媒体中心与通信方商议的密钥。

A.2.2.2 请求参数

请求头：

Content-Type: application/x-www-form-urlencoded

请求消息体为空。

A.2.2.3 响应参数

响应头：Content-Type: application/x-www-form-urlencoded

消息体包含：结果状态、结果描述。

“成功”返回消息体样例如下：

```
{
 "code": 0,
 "message": "成功",
 "data": {
    "access_token":"7e186b71b666aadcd3c344bc2b7e7007", (示例值)
    "refresh_token":"d5b8db762504c5ba2a4ea410aa6a2edd", (示例值)
    "expires_in":"7200"(示例值)
  }
}
```

消息体参数说明：

——access_token 为获取到的调用实际接口的访问令牌；

——refresh_token 为更新访问令牌的令牌；

——expires_in 为访问令牌的有效时长，单位为秒。

“失败”返回消息体样例如下：

```
{
 "code": -1,
 "message":"获取访问令牌失败：ID无效"或"获取访问令牌失败：密码无效"或"获取访问令牌失败：其他原因"
}
```

注："code"：0表示成功，非0表示失败。

A.2.3 调用实际接口

A.2.3.1 接口描述

调用实际接口。

请求方法：POST。

请求 URL：见《市级融媒体中心接口规范》中的附录 A。

A.2.3.2 请求参数

请求头：

Content-Type：application/json

Authorization：7e186b71b666aadcd3c344bc2b7e7007（示例值）

请求头参数说明：

Authorization 值为 A.2.2.3 获取到的访问令牌：access_token 值。

请求体：

```
{
  ……
}
```

其中，请求具体参数见《市级融媒体中心接口规范》中的附录A。

A.2.3.3 响应参数

响应头：Content-Type: application/json

消息体包含：结果状态、结果描述、data、支撑技术能力开放接口的任务状态值（在支撑技术能力开放接口中才包含，其他接口不包含该值）；data 值、支撑技术能力开放接口的任务状态值见《市级融媒体中心接口规范》中的附录 A。

支撑技术能力开放接口“成功”返回消息体样例如下：

```
{
 "code": 0,
 "message": "成功",
 "task_status":0,
 "data": {
  ……
  }
}
```

其他接口“成功”返回消息体样例如下：

```
{
 "code": 0,
 "message": "成功",
 "data": {
  ……
  }
}
```

或：

```
{
 "code": 0,
```

```
  "message": "成功",
  "data": [
    {
      ……
    }
  ]
}
```

“失败”返回消息体样例如下：

```
{
  "code": -1,
  "message": "令牌认证失败：令牌无效"或"令牌认证失败：其他原因"
}
```

注："code"：0表示成功，非0表示失败。

A.2.4 更新访问令牌

A.2.4.1 接口描述

在有效期内，请求方从响应方处更新访问令牌。

请求方法：POST。

请求URL：http(s)://{域名}/{服务名}/{版本}/[{可选值}]/oauth/refreshToken?grant_type=refresh_token&refresh_token=<refreshToken>

URL 参数说明：

——grant_type 固定为 refresh_token；

——refresh_token 值为 A.2.2.3 获取到的更新访问令牌的令牌：refresh_token 值。

A.2.4.2 请求参数

请求头：

Content-Type: application/x-www-form-urlencoded

请求消息体为空。

A.2.4.3 响应参数

响应头：Content-Type: application/x-www-form-urlencoded

消息体包含：结果状态、结果描述。

“成功”返回消息体样例如下：

```
{
  "code": 0,
  "message": "成功",
  "data": {
    "access_token":"7e186b71b666aadcd3c344bc2b7e7007",（示例值）
    "refresh_token":"d5b8db762504c5ba2a4ea410aa6a2edd",（示例值）
    "expires_in":"7200"（示例值）
  }
}
```

消息体参数说明：

——access_token 为获取到的调用实际接口的新的访问令牌；

——refresh_token 为新的更新访问令牌的令牌；

——expires_in 为新的访问令牌的有效时长，单位为秒。

“失败”返回消息体样例如下：

```
{
 "code": -1,
 "message": "更新访问令牌失败：令牌无效"或"更新访问令牌失败：其他原因"
}
```

注："code"：0表示成功，非0表示失败。

A.2.5 注销访问令牌

A.2.5.1 接口描述

在有效期内，请求方注销访问令牌。

请求方法：DELETE。

请求URL：http(s)://{域名}/{服务名}/{版本}/[{可选值}]/oauth/revokeToken

A.2.5.2 请求参数

请求头：

Content-Type：application/json

Authorization：7e186b71b666aadcd3c344bc2b7e7007（示例值）

请求头参数说明：

Authorization 值为 A.2.2.3 获取到的访问令牌：access_token 值。

请求消息体为空。

A.2.5.3 响应参数

响应头：Content-Type: application/json

消息体包含：结果状态、结果描述。

“成功”返回消息体样例如下：

```
{
 "code": 0,
 "message": "成功"
}
```

“失败”返回消息体样例如下：

```
{
 "code": -1,
 "message": "令牌注销失败：令牌无效"或"令牌注销失败：其他原因"
}
```

注："code"：0表示成功，非0表示失败。

参 考 文 献

[1] 中华人民共和国网络安全法

[2] 中华人民共和国密码法

[3] GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

[4] GB/T 28448—2019 信息安全技术 网络安全等级保护测评要求

[5] GB/T 32920—2016 信息技术 安全技术 行业间和组织间通信的信息安全管理

[6] GB/T 41391—2022 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求

[7] GB/T 41479—2022 信息安全技术 网络数据处理安全要求

[8] GD/J 126—2021 媒体素材安全上载设备技术要求和测量方法

[9] 国家广播电视总局.广播电视网络安全管理办法：广电办发〔2020〕322号.

[10] 国家广播电视总局.广播电视网络安全事件应急预案：广电办发〔2020〕321号.

[11] 国家广播电视总局.广播电视安全播出管理规定（2021年第二次修订）：国家广播电视总局令第8号，国家广播电影电视总局令第62号.

[12] 国家新闻出版广电总局.国家新闻出版广电总局关于印发《广播电视安全播出管理规定》实施细则的通知：新广电发〔2014〕235号.

[13] 中国新闻技术工作者联合会.报业网络安全等级保护定级参考指南V2.0.（2020-11-20）.

[14] 国家广播电视总局.县级融媒体中心建设规范：广电发〔2019〕5号.

[15] 中共中央宣传部、国家广播电视总局.县级融媒体中心网络安全规范.（2019-04-09）.

[16] 国家互联网信息办公室、文化和旅游部、国家广播电视总局关于印发《网络音视频信息服务管理规定》的通知：国信办通字〔2019〕3号.

[17] 国家广播电视总局.国家广播电视总局办公厅关于印发《广播电视基础设施自然灾害灾后恢复重建指导意见》的通知：广电办发[2021]128号.

[18] 国家广播电影电视总局.中华人民共和国信息产业部. 互联网视听节目服务管理规定：国家广播电影电视总局、中华人民共和国信息产业部令第56号.