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 发布　　2020-11-20 实施

中国新闻技术工作者联合会　发布

前 言

本指南依据《中华人民共和国网络安全法》、国务院 147 号令《中华人民共和国计算机信息系统安全保护条例》、中办发[2003]27 号《国家信息化领导小组关于加强信息安全保障工作的意见》、公通字[2004]66 号《关于信息安全等级保护工作的实施意见》、公通字[2007]43 号《信息安全等级保护管理办法》、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》及相关专业实施细则，对报业网络安全等级保护对象的定级工作提供指导。

本指南代替《报业网络安全等级保护定级参考指南 V1.0》

本指南起草单位：中国新闻技术工作者联合会。

本指南主要起草人：罗毅、杨真、段继亮、宋海涛、高沁、吴方、宋明亮、李彦魁、甘永清、马杰、邵德奇、吴川、魏春光、陆军、金君飞、李涛、张洪福、李伟、刘炫、付锦凤、孙新峰、刘毅、侯东民、陈岩、王磊。

本指南技术支持单位：北京意畅科技股份有限公司。

目 录

1 范围

本指南描述了报业非涉及国家秘密的等级保护对象的安全保护等级定级方法和定级流程。

本指南适用于指导报业融媒体/全媒体系统、新闻采编发系统、云计算平台、大数据平台等非涉及国家秘密的等级保护对象的定级工作。

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 22240—2020 信息安全技术 网络安全等级保护定级指南

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2010 信息安全技术 术语

GB/T 29246—2017 信息技术 安全技术 信息安全管理体系 概述和词汇

GB/T 31167—2014 信息安全技术 云计算服务安全指南

3 术语和定义

GB 17859—1999、GB/T 22240—2020、GB/T 22239—2019、GB/T 25069—2010、GB/ T 29246—2017 和 GB/T 31167—2014 和界定的以及下列术语和定义适用于本文件。

3.1 网络安全

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[GB/ T 22239—2019，定义 3.1]

3.2 等级保护对象

报业网络安全等级保护工作直接作用的对象。

注：主要包括信息系统、网络设施和数据资源。

3.3 信息系统

应用、服务、信息技术资产或其他信息处理组件。

[GB/ T 29246—2017，定义 2.39]

注 1：信息系统通常由计算机或其他信息终端及相关设备组成，并按照一定的应用目标和规则进行信息处理或过程控制。

注 2：典型的信息系统如报业融媒体/全媒体系统、新闻采编发系统、云计算平台、大数据平台等。

3.4 通信网络设备

为信息流通、网络运行等起基础支撑作用的网络设备设施。

3.5 数据资源

具有或预期具有价值的数据集合。

注：数据资源多以电子形式存在。

[GB/T 22240—2020，定义 3.5]

3.6 受侵害的客体

受法律保护的、等级保护对象受到破坏时所侵害的社会关系。

注：本文件中简称“客体”。

[GB/T 22240—2020，定义 3.6]

3.7 客观方面

对客体造成侵害的客观外在表现，包括侵害方式和侵害结果等。

[GB/T 22240—2020， 定义 3.7]

4 定级原理及流程

4.1 安全保护等级

根据等级保护对象在国家安全、经济建设、社会生活中的重要程度，以及一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的侵害程度等因素，等级保护对象的安全保护等级分为以下五级：

第一级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成一般损害，但不危害国家安全、社会秩序和公共利益；

第二级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成严重损害或特别严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全；

第三级，等级保护对象受到破坏后，会对社会秩序和公共利益造成严重危害，或者对国家安全造成危害；

第四级，等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害；

第五级，等级保护对象受到破坏后，会对国家安全造成特别严重损害。

4.2 定级要素

4.2.1 定级要素概述

等级保护对象的定级要素包括：

a）受侵害的客体；

b）对客体的侵害程度。

4.2.2 受侵害的客体

等级保护对象受到破坏时所侵害的客体包括以下三个方面：

a）公民、法人和其他组织的合法权益；

b）社会秩序、公共利益；

c）国家安全。

4.2.3 对客体的侵害程度

对客体的侵害程度由客观方面的不同外在表现综合决定。由于对客体的侵害是通过对等级保护对象的破坏实现的，因此对客体的侵害外在表现为对等级保护对象的破坏，通过侵害方式、侵害后果和侵害程度加以描述。

等级保护对象受到破坏后对客体造成侵害的程度归结为以下三种：

a）造成一般损害；

b）造成严重损害；

c）造成特别严重损害。

4.3 定级要素与安全保护等级的关系

定级要素与安全保护等级的关系见表 1 所示。

表 1 定级要素与安全保护等级的关系

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

4.4 定级流程

等级保护对象定级工作的一般流程如图 1 所示。

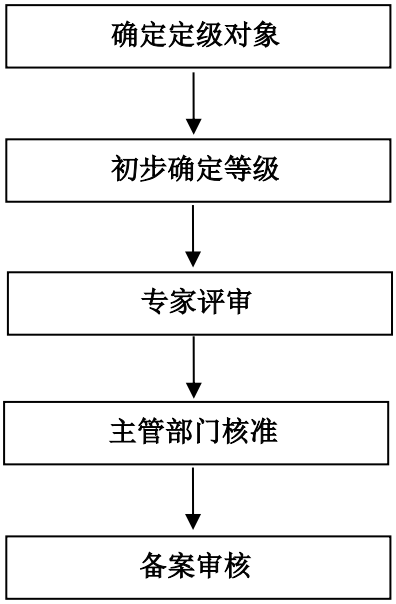

图 1 等级保护对象定级工作一般流程

安全保护等级初步确定为第二级及以上的等级保护对象，其网络运营者依据本文件组织进行专家评审、主管部门核准和备案审核，最终确定其安全保护等级。

安全保护等级初步确定为第一级的等级保护对象，其网络运营者可参照本文件自行确定最终安全保护等级，可不进行专家评审、主管部门核准和备案审核。

5 确定定级对象

5.1 信息系统

5.1.1 定级对象的基本特征

作为定级对象的信息系统应具有如下基本特征：

a）具有确定的主要安全责任主体；

b）承载相对独立的业务应用；

c）包含相互关联的多个资源。

注 1: 主要安全责任主体包括但不限于报业集团及下属单位等法人，以及不具备法人资格的部门等。

注 2: 避免将某个单一的系统组件，如服务器、终端或网络设备作为定级对象。

在确定定级对象时，云计算平台/系统、采用移动互联技术的系统在满足以上基本特征的基础上，还需分别遵循本文件 5.1.2 、5.1.3 的相关要求。

5.1.2 云计算平台/系统

在云计算环境中，云服务客户侧的业务系统和云服务商侧的云计算平台需分别作为单独定级对象，并根据不同服务模式将云计算平台/系统划分为不同的定级对象。

租用公有云服务的单位，对其使用的运行于云计算平台上的业务系统进行定级。同时，所租用的公有云服务平台本身安全等级保护不低于第三级。

使用自建私有云的单位，按所承载业务系统的最高等级对该私有云平台进行定级，运行于该私有云上的业务系统可独立定级。若私有云平台承载单一的业务系统，且该私有云和业务系统由同一安全责任主体负责运维，可合并定级。

5.1.3 采用移动互联技术的系统

采用移动互联技术的系统主要包括移动终端、移动应用和无线网络等特征要素，可作为一个整体独立定级或与相关联业务系统一起定级，各要素不单独定级。

5.2 数据资源

数据资源可单独定级。

当安全责任主体相同时，大数据、大数据平台/系统宜作为一个整体对象定级；当安全责任主体不同时，大数据和大数据平台/系统应独立定级。

5.3 报业网络安全等级保护对象

根据报业实际情况，按照定级对象的基本特征，综合考虑定级对象的业务类型、责任主体和重要性等因素，将报业网络安全等级保护对象进行分类描述，见表 2。

对于信息系统较庞大，尤其是采用云计算平台、融媒体/全媒体等系统的报业单位，如果等级保护对象责任边界一致，责任主体一致，业务关联度较大，也可将表 2 中的多个系统合并为一个等级保护对象进行定级。

表 2 报业网络安全等级保护对象

序号	分类	定级对象	描述
1	新闻生产	融媒体/全媒体系统	传统媒体和新媒体融合工作业务系统。
		新闻采编发系统	报纸采编发信息系统。
		新媒体制作发布系统	网站及移动端等制作与发布系统。
		网站新闻发布系统	独立的互联网网站系统。
		报道指挥系统	实现信息共享、即时沟通、选题策划、指挥协调和传播力分析等功能的业务系统。
		新闻大屏系统	新闻和广告等信息大屏业务系统。
2	业务支撑和服务	云计算平台	基于硬件和软件，提供计算、存储、网络服务和一定安全保障的技术平台系统。
		大数据平台	为融媒体运营和行业公众业务等提供增值服务的系统。
		媒资系统	音视频资料、文本、图片、图表等各类媒体资料数据的存储管理系统。
		舆情系统	为行业和社会提供舆情服务的系统。
		邮件系统	有独立域名的互联网邮件系统。
3	管理	办公经营系统	包括办公、人事、绩效考核、财务、广告、发行、客户关系等系统。
		运维管理系统	实现各业务系统的监测、安全管理、运维管理等功能的信息系统。
4	其他	报业单位认为重要的其他信息系统	

6 确定安全保护等级

6.1 定级方法概述

报业定级对象的定级方法按照以下描述进行。对于通信网络设施、云计算平台/系统等起支撑作用的定级对象和数据资源，参照本指南第 7 节。

定级对象的安全主要包括业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能不同，因此，安全保护等级由业务信息安全和系统服务安全两方面确定。分析定级对象与报社业务的相关性，从业务信息安全角度反映的定级对象安全保护等级称为业务信息安全保护等级；从系统服务安全角度反映的定级对象安全保护等级称为系统服务安全保护等级。

定级方法流程示意图如图 2 所示。

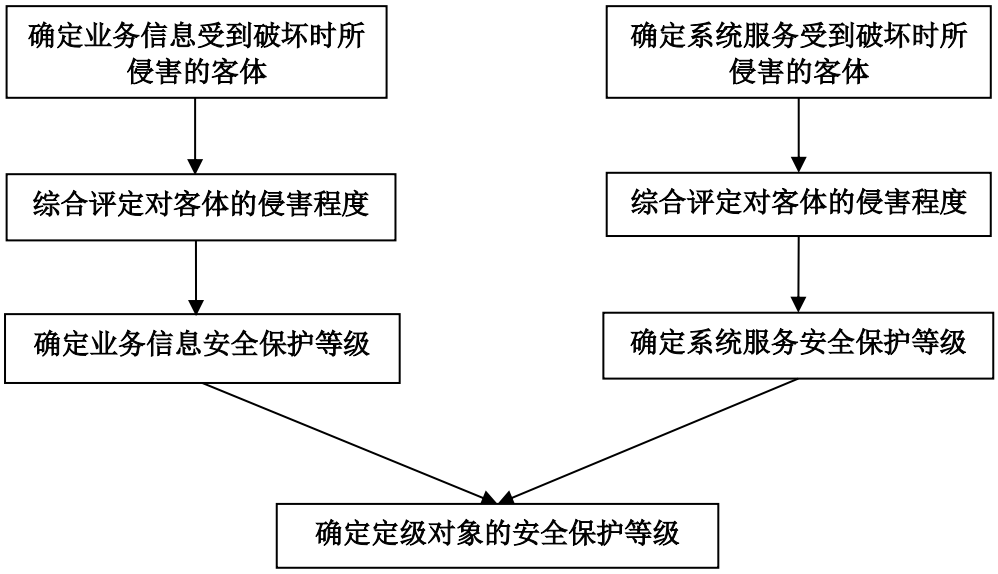

图 2 定级方法流程示意图

具体流程如下：

a）确定受到破坏时所侵害的客体

1）确定业务信息受到破坏时所侵害的客体；

2) 确定系统服务安全受到侵害时所侵害的客体。

b）确定对客体的侵害程度

1）根据不同的受侵害客体，分别评定业务信息安全被破坏对客体的侵害程度；

2）根据不同的受侵害客体，分别评定系统服务安全被破坏对客体的侵害程度。

c）确定安全保护等级

1）确定业务信息安全保护等级；

2）确定系统服务安全保护等级；

3）将业务信息安全保护等级和系统服务安全保护等级的较高者确定为定级对象的安全保护等级。

6.2 确定受侵害的客体

定级对象受到破坏时所侵害的客体包括国家安全、社会秩序、公众利益以及公民、法人和其他组织的合法权益。

侵害国家安全的事项包括以下方面：

——影响国家政权稳固和领土主权、海洋权益完整；

——影响国家统一、民族团结和社会稳定；

——影响国家社会主义市场经济秩序和文化实力；

——其他影响国家安全的事项。

侵害社会秩序的事项包括以下方面：

——影响国家机关、企事业单位、社会团体的生产秩序、经营秩序、教学科研秩序、医疗卫生秩序；

——影响公共场所的活动秩序、公共交通秩序；

——影响人民群众的生活秩序；

——其他影响社会秩序的事项。

侵害公共利益的事项包括以下方面：

——影响社会成员使用公共设施；

——影响社会成员获取公开数据资源；

——影响社会成员接受公共服务等方面；

——其他影响公共利益的事项。

侵害公民、法人和其他组织的合法权益是指受法律保护的公民、法人和其他组织所享有的社会权利和利益等受到损害。

确定受侵害的客体时，首先判断是否侵害国家安全，然后判断是否侵害社会秩序或公众利益，最后判断是否侵害公民、法人和其他组织的合法权益。

6.3 确定对客体的侵害程度

6.3.1 侵害的客观方面

在客观方面，对客体的侵害外在表现为对定级对象的破坏，其侵害方式表现为对业务信息安全的破坏和对系统服务安全的破坏。其中，业务信息安全是指确保定级对象中信息的保密性、完整性和可用性等，系统服务安全是指确保定级对象可以及时、有效地提供服务，以完成预定的业务目标。由于业务信息安全和系统服务安全受到破坏所侵害的客体和对客体的侵害程度可能会有所不同，在定级过程中，需要分别处理这两种侵害方式。

业务信息安全和系统服务安全受到破坏后，可能产生以下侵害后果：

——影响行使工作职能；

——导致业务能力下降；

——引起法律纠纷；

——导致财产损失；

——造成社会不良影响；

——对其他组织和个人造成损失；

——其他影响。

6.3.2 综合判定侵害程度

侵害程度是客观方面的不同外在表现的综合体现。因此，首先根据不同的受侵害客体、不同侵害后果分别确定其侵害程度。对不同侵害后果确定其侵害程度所采取的方法和所考虑的角度可能不同，例如系统服务安全被破坏导致业务能力下降的程度可以从定级对象服务覆盖的区域范围、用户人数或业务量等不同方向而确定，业务信息安全被破坏导致的财物损失可以从直接的资金损失大小 、间接的信息恢复费用等方面进行确定。

在针对不同的受侵害客体进行侵害程度的判断时，参照以下不同的判别基准：

——如果受侵害客体是公民、法人或其他组织的合法权益，则以本人或本单位的总体利益作为判断侵害程度的基准；

——如果受侵害客体是社会秩序、公共利益或国家安全，则以整个行业或国家的总体利益作为判断侵害程度的基准。

不同侵害后果的三种侵害程度描述如下：

——一般损害：工作职能受到局部影响，业务能力有所降低但不影响主要功能的执行，出现较轻的法律问题，较低的财产损失，有限的社会不良影响，对其他组织和个人造成较低损害；

——严重损害：工作职能受到严重影响，业务能力显著下降且严重影响主要功能执行，出现较严重的法律问题，较高的财产损失，较大范围的社会不良影响，对其他组织和个人造成较高损害；

——特别严重损害：工作职能受到特别严重影响或丧失行使能力，业务能力严重下降且或功能无法执行，出现极其严重的法律问题，极高的财产损失，大范围的社会不良影响，对其他组织和个人造成非常高损害；

对客体的侵害程度由对不同侵害结果的侵害程度进行综合评定得出。由于各行业定级对象所处理的信息种类和系统服务特点各不相同，业务信息安全和系统服务安全受到破坏后关注的侵害结果、侵害程度的计算方式均可能不同，报业可根据本行业业务信息和系统服务特点制定侵害程度的综合评定方法，并给出一般损害、严重损害、特别严重损害的具体定义。

6.4 初步确定报业定级对象的安全保护等级

根据报业定级对象的业务信息安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据业务信息安全保护等级矩阵表，见表 3，可得到报业业务信息安全保护等级。

表 3 业务信息安全保护等级矩阵

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

根据报业定级对象的系统服务安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据系统服务安全保护等级矩阵表，见表 4，可得到报业系统服务安全保护等级。

表 4 系统服务安全保护等级矩阵表

系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

作为报业定级对象的初步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的较高者决定。

6.5 报业定级对象受到破坏时侵害的客体

根据报业特点，分析报业定级对象与国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的关系，从而确定定级对象受到破坏时所侵害的客体。

新闻生产类业务信息安全或系统服务安全受到破坏，可能直接造成无法及时正确出报、错误发布权威声音和新闻信息，侵害社会公众知情权等合法权益，甚至可能引起社会秩序混乱乃至社会动荡，可能侵害国家安全。

业务支撑服务和管理类业务信息安全或系统服务安全受到破坏，可能造成新闻采编业务、内部办公流程差错和事故，会给报业单位造成一定的财产损失、经济纠纷和法律纠纷等；可能造成报业单位经营业务差错和事故，侵害社会公众合法权益，引起社会秩序混乱，侵害公共利益。

6.6 报业定级对象受到破坏对客体的侵害程度

报业定级对象的业务信息安全或系统服务安全受到破坏时，对客体的侵害程度与信息系统所属单位的行政级别、类别以及承载业务的重要性、影响程度、用户规模等有关。分别描述如下：

中央级报社的定级对象业务信息覆盖全国，社会影响力大，这些系统的业务信息安全或系统服务安全受到破坏，可能直接造成新闻工作事故，对社会秩序、公共利益造成严重损害，对国家安全造成一般损害；

省级、省会城市报社以及行业报社的定级对象，其业务信息有一定的覆盖面和社会影响力，这些系统的业务信息安全或系统服务安全受到破坏，可能直接造成新闻工作事故，对社会秩序、公共利益造成严重损害；

都市报社的定级对象，其业务在行业内和地区具有一定的覆盖面和社会影响力，这些系统的业务信息安全或系统服务安全受到破坏，可能导致其业务能力下降，破坏严重时可能造成新闻工作事故，对社会秩序、公共利益造成一般损害。

7 报业网络安全等级保护定级参考

综合考虑各级各类报业定级对象的业务信息安全等级和系统服务安全等级，定级对象的安全保护等级定级参考建议，见表 5 所示。

表 5 报业网络安全等级保护定级参考

序号	分类	定级对象	单位类别			
			中央级报社	省级报社	行业报社	都市报社
1	新闻生产	融媒体/全媒体系统	第三级	第三级	第三级	第二级
2		新闻采编发系统	第三级	第三级	第二级	第二级
3		新媒体制作发布系统	第三级	第三级	第二级	第二级
4		网站新闻发布系统	第三级	第二级	第二级	第二级
5		报道指挥系统	第三级	第二级	第二级	第二级
6		新闻大屏系统	第二级	第二级	第二级	第二级
7	业务支撑和服务	云计算平台	第三级	第三级	第三级	第二级
8		大数据平台	第二级	第二级	第二级	第二级
9		媒资系统	第二级	第二级	第二级	第二级
10		舆情系统	第二级	第二级	第二级	第二级
11		邮件系统	第二级	第二级	第二级	第二级
12	管理	办公经营系统	第二级	第二级	第二级	第二级
13		运维管理系统	第二级	第二级	第二级	第二级

各报社根据本单位网络业务功能进行参照定级，安全等级应不低于建议级别。

注：如遇特殊情况，需在定级专家评审会中特别说明。

对于承载多个业务功能的系统，安全等级应高于建议级别。

对于云计算平台，需根据其承载或将要承载的业务系统的重要程度确定其安全保护等级，原则上不低于其承载的业务系统的安全保护等级。

对于涉及大量公民个人信息以及为公民提供公共服务的大数据平台/系统，原则上其安全保护等级不低于第三级。

未在表 5 中列出的报业网络安全等级保护对象，应根据其承载的业务功能，参照 GB/T 22240—2020 或本指南进行定级。

8 专家评审

报业定级对象的安全保护等级初步确定为第二级及以上的，需组织网络安全专家和业务专家对定级结果的合理性进行评审，并出具专家评审意见。

9 等级变更

当等级保护对象所处理的业务信息和系统服务范围发生变化，可能导致业务信息安全或系统服务安全受到破坏后的受侵害客体和对客体的侵害程度发生变化时，需参照 GB/T 22240—2020 或本指南重新确定定级对象和安全保护等级。

参考文献

[1] 《中华人民共和国网络安全法》
[2] GB/T 22240-2020《信息安全技术 网络安全等级保护定级指南》
[3] 国务院 147 号令《中华人民共和国计算机信息系统安全保护条例》
[4] 中办发[2003]27 号《国家信息化领导小组关于加强信息安全保障工作的意见》
[5] 公通字[2004]66 号《关于信息安全等级保护工作的实施意见》
[6] 公通字[2007]43 号《信息安全等级保护管理办法》
[7] GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》

附件目录

附件一：定级报告案例模板

示例 1 融媒体系统：

（定级单位名称）融媒体系统

网络安全等级保护定级报告

一、 （定级单位名称）融媒体系统描述

（一）该系统于 20**年**月完成建设并上线运行，由（开发机构名称）开发建设，（定级单位名称）信息中心和（运维机构名称）负责运维。（定级单位名称）信息中心是该系统的业务主管部门，（定级单位名称）为该信息系统定级的责任单位。

（二）本系统建设**节点（分别在（定级单位名称）核心机房）、（系统托管商名称）云平台。（根据实际节点信息描述）

（定级单位名称）机房网络节点依据分层、分区的设计理念，以模块化的方式进行规划设计，采取核心-汇聚-接入的标准三层网络架构。根据（定级单位名称）网络安全管理要求，划分为 6 个网络区域（外网出口区、外网业务支撑平台区、外网安全管理区、云计算数据中心区、内网业务支撑平台区、内网安全管理区）。

（定级单位名称）网络节点由（外网出口区、外网业务支撑平台区、外网安全管理区、云计算数据中心区、内网业务支撑平台区、内网安全管理区）组成。

（云计算数据中心区由网络交换区、安全管理区、云计算数据中心等）区域组成（根据实际区域信息描述）。

（定级单位名称）支撑平台部署在（系统托管商名称）云平台（根据实际业务情况描述）。

网络总体架构如下图所示：

拓扑图

提供定级系统的网络拓扑图

（三）该系统为（定级单位名称）提供（描述功能和服务）。

该信息系统业务主要包含：（融媒体系统业务的描述，模块组成等）。

二、 （定级单位名称）融媒体系统安全保护等级的确定

(一) 业务信息安全保护等级的确定

1. 业务信息描述

融媒体系统业务信息包括（描述业务信息的分类、内容等）。

目前相关信息存储量为**TB。

2. 业务信息受到破坏时所侵害客体的确定

该业务信息遭到破坏后，所侵害的客体是（定级单位名称融媒体系统）的业务数据（描述业务数据的存放类型、数据内容、重要程度等）。

侵害的客观方面表现为：一旦融媒体系统的业务信息遭到入侵、修改、增加、删除等不明侵害（形式可以包括丢失、破坏、损坏等），会使（定级单位名称）融媒体系统业务数据泄露，严重影响数据和传播的准确性，影响（定级单位名称）正常的业务开展，同时还可能会造成重要数据和信息的泄漏，甚至篡改，造成不良的社会影响等，但不会影响国家安全。

3. 信息受到破坏后对侵害客体的侵害程度

上述结果的侵害程度表现为：对社会秩序和公共利益造成**严重损害**，即会出现**较大范围**的社会不良影响和**较大程度**的公共利益的损害等。

4. 确定业务信息安全等级

根据 GB/T 22240—2020 定级指南，得出业务信息安全保护等级为第三级。

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

（二） 系统服务安全保护等级的确定

1. 系统服务描述

该系统服务主要用来提供（定级单位名称）融媒体系统的业务支撑、生产、办公等服务，其服务范围为（定级单位名称）（根据服务范围的描述）。

2. 系统服务受到破坏时所侵害客体的确定

该系统服务遭到破坏后，所侵害的客体是社会秩序和公共利益。

侵害的客观方面表现为：一旦系统遭到入侵和破坏，会使（定级单位名称）内重要信息泄露，使（定级单位名称）融媒体系统运行受到影响。系统服务被破坏、损坏、被攻击等，系统可用性和连续性被破坏，业务能力下降甚至终止，影响业务正常开展，造成不良影响等。

3. 系统受到破坏后对侵害客体的侵害程度

上述结果的侵害程度表现为：对社会秩序和公共利益造成**严重损害**，即会出现**较大范围**的社会不良影响和**较大程度**的公共利益的损害等。

4. 确定系统服务安全等级

根据 GB/T 22240—2020 定级指南，得出系统服务安全保护等级为第三级。

系统服务被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

三、 安全保护等级的确定

定级对象的安全保护等级由业务信息安全等级和系统服务安全等级的较高者决定。所以，（定级单位名称）融媒体系统的安全保护等级为第三级。

定级对象名称	安全保护等级	业务信息安全等级	系统服务安全等级
（定级单位名称）融媒体系统	第三级	第三级	第三级

示例 2 网站系统：

（定级单位名称）网站系统

网络安全等级保护定级报告

一、 （定级单位名称）网站系统描述

（一）该系统于 20**年**月建设并上线试运行，由（开发公司名称）公司开发建设，（定级单位名称）信息中心和（运维公司名称）负责运维。（定级单位名称）信息中心是该系统的业务主管部门，（定级单位名称）为该信息系统定级的责任单位。

（二）本系统建设部署于（系统托管商名称）云平台。（根据实际节点信息描述）

该系统全部部署于（系统托管商名称）云平台，同时提供虚拟网络、虚拟存储等基础设施。（系统托管商名称）云平台提供了数据库主从备份，异地备份的数据容灾服务，同时也提供了数据独立虚拟网络服务，保证云上面的数据安全。

采用安全组件包括（按等保 2.0 二级系统安全要求建设，网站、数字报、历史资源库等系统共享）防火墙(含 WEB 安全、应用安全、IPSec/SSL VPN、应用交付、堡垒机、数据库审计) 等

网络总体架构如下图所示：

拓扑图

提供定级系统的网络拓扑图

（三）（定级单位名称）网站系统包括统一用户管理、网站内容管理系统、APP 及手机网站内容管理系统、微信微博内容管理系统、数字报内容制作等系统。（按照实际功能描述）

目前页面浏览量（PV）、访问次数、客户端下载量等数据进行描述。

二、 （定级单位名称）网站系统安全保护等级的确定

（一） 业务信息安全保护等级的确定

1. 业务信息描述

网站系统主要包括信息采集、内容加工、内容发布、信息资源管理、数字报等业务，成为报社新媒体业务的基础平台，成为报道宣传、信息发布的重要渠道。

2. 业务信息受到破坏时所侵害客体的确定

该系统业务信息遭到破坏后，所侵害的客体是公民、法人和其他组织的合法权益。

侵害的客观方面表现为：一旦该系统的业务信息安全遭到入侵、修改、增加、删除等不明侵害（形式可以包括丢失、破坏、损坏等），会对公民、法人和其他组织的合法权益造成影响和损害，可以表现为：影响正常工作的开展，导致业务能力下降，引起法律纠纷，造成不良影响等。

3. 信息受到破坏后对侵害客体的侵害程度

上述结果的侵害程度表现为严重损害，即工作职能受到严重影响，业务能力显著下降，出现较严重的法律问题，造成较大范围的不良影响等。

4. 确定业务信息安全等级

根据 GB/T 22240—2020 定级指南，得出业务信息安全保护等级为第二级。

业务信息被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

（二） 系统服务安全保护等级的确定

1. 系统服务描述

该网站系统是报社用于面向社会公众提供发布服务的信息系统，系统服务范围为公民、法人和其他组织。

2. 系统服务受到破坏时所侵害客体的确定

该网站系统遭到破坏后，所侵害的客体是公民、法人和其他组织的合法权益，客观方面表现得侵害结果为，可以对公民、法人和其他组织的合法权益造成侵害，影响正常工作的开展，导致业务能力下降，引起法律纠纷，造成不良影响等。

3. 信息受到破坏后对侵害客体的侵害程度

上述结果的侵害程度表现为严重损害，即工作职能受到严重影响，业务能力显著下降，出现较严重的法律问题，较大范围的不良影响等。

4. 确定系统服务安全等级

根据 GB/T 22240—2020 定级指南标准，得出系统服务安全保护等级为第二级。

系统服务被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

三、 安全保护等级的确定

该系统的安全保护等级由业务信息安全等级和系统服务安全务安等级的较高者决定。所以，（定级单位名称）网站系统安全保护等级为第二级。

信息系统名称	安全保护等级	业务信息安全等级	系统服务安全等级
（定级单位名称） 网站系统	第二级	第二级	第二级

附件二：专家评审意见模板

（定级单位名称）XXX 系统

网络安全等级保护定级专家评审意见

2020 年**月**日，XXX 报社在 XXX（评审地址）组织召开了“XXX 系统”网络安全等级保护定级专家评审会。与会专家（名单附后）听取了 XXX 报社信息中心对系统定级情况的汇报，审阅了定级相关文档，经质询讨论，形成如下意见：

一、XXX 报社依据网络安全等级保护相关法律、法规和技术标准，对“XXX 系统”开展了网络安全等级保护定级工作，定级流程规范、定级材料齐全，符合定级要求。

二、XXX 报社根据系统承载业务的重要程度、系统受到破坏时所侵害的客体、系统受到破坏后对客体的侵害程度，将“XXX 系统”的网络安全保护等级拟定为第*级，其中业务信息安全等级为第*级，系统服务安全等级为第*级。

专家认为定级理由充分，定级结果准确。

专家签字：

专家姓名	单位	职称/职务	联系方式

附件三：专家评审人员说明

网络安全保护等级初步确定为第二级及以上的，需组织网络安全专家和业务专家对定级结果的合理性进行评审，并出具专家评审意见。

专家组人员组成应不少于 3 人，其中包括至少 1 名高级测评师、1 名网络安全专家（需高级职称）、1 名行业内的业务专家（需高级职称）组成。

为能更好的服务会员单位，中国新闻技术工作者联合会可为广大新闻媒体单位推荐相关的专家。

附件四：等级保护合规项参考表

类别	合规项	第二级	第三级
技术合规类	防火墙	非常重要	非常重要
	日志审计与集中管理	非常重要	非常重要
	堡垒机	非常重要	非常重要
	数据备份与恢复	非常重要	非常重要
	网络版杀毒软件	重要	非常重要
	SSL证书	重要	非常重要
	网站防护系统	重要	重要
	终端准入系统	一般重要	重要
	数据库审计	一般重要	重要
	网络运维管理软件	一般重要	重要
	安全态势感知系统	一般重要	重要
管理、服务合规类	成立网络安全领导小组	非常重要	非常重要
	安全制度建设	非常重要	非常重要
	渗透测试服务	非常重要	非常重要
	漏洞管理服务（扫描、加固）	非常重要	非常重要
	安全事件响应服务	重要	非常重要
	安全培训服务	重要	重要
	安全咨询服务	重要	重要
	安全建设方案	重要	重要