关于印发《阜新市广播电视领域安全管理办法》的通知

阜文旅广电发[2021]18号

各县区广电局、广电台，市广播电视台，北方联合网络公司阜新分公司，市中继站、监测台：

现将《阜新市广播电视领域安全管理办法》印发给你们，请结合实际，认真贯彻实施。请各级广播电视制播传输及监测单位立即制定完善《建党100周年安全播出重要保障期应急预案》，并于6月15日前报市文旅广电局广播电视管理科备案。

阜新市文化旅游和广播电视局

2021年6月1日

（此件公开发布）

阜新市广播电视领域安全管理办法

为了加强我市广播电视和网络视听行业安全保障工作，确保在播出安全、网络安全和设施保护方面万无一失，根据《广播电视安全播出管理规定》（国家广电总局令第62号）及专业实施细则，特制定本办法。

本办法适用于我市各级广播电视行政管理局、广播电视播出机构、广播电视无线转播台站和广播电视有线传输单位。在组织机构、安全播出管理、网络安全管理和广播电视设施保护等方面给予规范。

一、广播电视行政管理局

（一）组织机构

设立并及时调整由局长任组长（总指挥），辖区内广播电视播出单位主要岗位安全责任人为成员的广播电视安全播出领导小组（指挥部）和网络安全和信息化领导小组，承担安全播出管理、网络安全管理、设施保护管理职责。

（二）安全播出管理

1、安全播出管理事件事故管理

负责执行总局重大事件事故报告制度；组织开展辖区广播电视重大事件、事故调查处置及通报整改工作；督促建立按节目传

输环节、分工明确的协调管理机制。

2、重要保障期管理

重要保障期前动员部署，组织制定重保期工作方案；重要节目和重点时段领导带班；建立重保期信息通报机制。

3、应急管理

对辖区内安全播出单位的安全播出应急突发事件预案给予备案。

（三）网络安全管理

1、定期组织召开辖区广播电视播出单位网络安全例会。

2、负责编制本级行业网络安全事件应急预案，并定期组织开展演练。

3、配合公安机关部署网络安全执法检查工作，定期检查辖区内运行单位网络安全责任制落实情况；组织技术力量，对辖区内重要网络和信息系统开展专项检查、抽测抽查，督促相关单位进行整改。

4、建立网络安全信息通报制度，及时将发现的网络安全事件、风险、威胁等，通知辖区内相关单位，根据需要发布预警、组织应急处置。

5、定期组织辖区内相关单位网络安全教育及培训。

（四）设施保护管理

1、定期组织召开设施保护工作领导小组会议。

2、定期开展日常广播电视设施保护工作检查、督导。

3、每年对广播电视设施保护工作开展年度检查、督导、考核。

二、广播电视安全播出责任单位

广播电视安全播出责任单位包括广播电视台、无线转播发射台站和有线电视传输单位。

（一）组织机构

1、设立并及时调整由“一把手”任组长，主要岗位安全责任人为成员的广播电视安全播出领导小组和网络安全和信息化领导小组，承担安全播出管理、网络安全管理、设施保护管理职责。

2、单位内部设立技术维护和运行管理机构。

（二）安全播出管理

1、日常管理

（1）制度管理

制定机房管理制度、值班及交接班制度、安全制度、供配电管理制度、维护检修制度、技术档案管理制度等，并在相应岗位上墙。

（2）技术管理

各中心控制和转播岗位配置预警信息接收终端；新建及改扩建播出系统前必须开展安全播出评估。

（3）信息报送机制

发生特大、重大事件事故后，立即向辖区广播电视安全播出领导小组报告。

（4）运行维护

机房值班记录、检修记录、系统指标测试记录齐全；消防、电力和防雷设施第三方年检材料齐全；播出设施所在地的楼宇、场地的供电设施维护、安全管理边界、责任主体明确。重要部位进出口设立电子门禁，电脑设立密码，防止人员跨部位流动和使用设备。

2、重要播出保障期管理

重要保障期前，制定重要保障期工作方案和应急预案，做好动员部署、安全防范和技术准备；重要节目和重点时段，主管领导应当现场指挥；加强值班和监测，并做好应急准备；严格执行零报告制度。

3、应急管理

（1）应急协调预案

具备与系统外单位的协调预案，并定期组织演练；具备与系统内上下游单位的协调预案，并定期组织演练。

（2）突发事件应急预案

具备非法破坏类事件应急预案，并定期组织演练；具备自然灾害类事件应急预案，并定期组织演练。

（3）故障处置预案

供配电故障应急预案，并定期组织演练；播出重要环节故障应急预案，并定期组织演练。

（4）C 波段干扰协调保护

按照总局关于 C 波段受 5G 基站干扰协调保护（广电发[2019]3 号）的文件要求，采取有效措施防范 5G 基站对 C 波段卫星节目源的干扰。

（三）网络安全管理

1、日常管理

建立包括网络安全人员管理、机房管理、设备管理、系统建设和运维管理、服务外包管理等制度。

2、应急预案

（1）预案制定

制定本单位网络安全事件应急预案，并及时修订。

（2）应急演练

每年至少按照应急预案开展一次网络安全应急演练。

3、安全检测

对网络的安全性和可能存在的风险每年至少进行一次检测评估，发现问题及时整改。

4、经费保障

将网络安全建设、运行维护、教育培训、测试评估、监测预警、应急演练和处置等所需经费纳入年度预算。

5、人员培训

每年组织网络安全教育，每年组织开展网络安全培训。

6、边界防护

（1）网络物理隔离或在网络边界处部署了必要的安全防护设备(如防火墙、网闸、防病毒产品等)，并根据业务实际情况设置安全策略。

（2）应关断所有非必需的访问路径和访问端口(如 445,3389)，制定详细的访问控制策略。

7、网络架构

（1）核心交换机、重要服务器等设备配置在线冗余。

（2）有网络拓扑图且与当前运行情况一致。

8、数据上载

在进行本地文件上载时,应对文件进行两种不同恶意代码库的杀毒软件进行杀毒，或采用 P2 卡、蓝光等专业设备进行上载。

9、审计日志

（1）开启审计功能，对关键网络设备、重要服务器、终端、数据库、主要应用软件的运行状况、用户行为等重要事件进行日志记录。

（2）采用专用集中审计设备对日志进行管理，且日志记录保存时间不少于六个月。

10、身份认证

（1）用户登录网络设备、主机、数据库、应用软件时应进行身份认证，无弱口令、默认口令、通用口令、长期不变口令。

（2）网络设备、主机、数据库、应用软件启用登录失败处理功能。

11、访问控制

（1）禁止通过互联网进行远程维护管理，必须使用时要有技术保护措施。

（2）采用专用受控终端进行系统维护。

12、运行状态监测

对重要服务器的运行状态和关键网络设备状态、关键节点的网络流量进行监测。

（四）设施保护管理

1、综合防控

（1）组织落实

设立设施保护领导小组和专门机构。

（2）防范制度

制订突发事件总体应急预案及消防、治安、反恐等分预案；制订重要保障期突发事件应急预案；制订日常安全巡逻、巡查、门卫、值班制度，重要部位设立电子门禁。

（3）消防安全

逐级签订消防安全责任书，落实消防安全主体责任；消防设

施、灭火器材、消防安全标志配置齐全、完好有效，并具备火灾自动报警功能；重点部位明确消防安全重点部位、设置防火标志。

（4）治安防控

单位周界围墙(栏)应设置防入侵报警系统和视频监控系统；周界围墙(栏)出入口设有门卫、传达室，负责查验、办理出入人员、车辆证件手续；核心要害部位应安装门禁、电视监控等技防设施，实行封闭式控制、安保人员负责出入口控制，查验进入人员证件手续；对进入核心要害部位的临时人员、施工人员进行审核登记。