**网络安全威胁信息发布管理办法**

(征求意见稿)

**第一条** 为规范网络安全威胁信息发布行为，有效应对网络安全威胁和风险，保障网络运行安全，依据《中华人民共和国网络安全法》等相关法律法规，制定本办法。

**第二条** 发布网络安全威胁信息，应以维护网络安全、促进网络安全意识提升、交流网络安全防护技术知识为目的，不得危害国家安全和社会公共利益，不得侵犯公民、法人和其他组织的合法权益。

**第三条**发布网络安全威胁信息，应坚持客观、真实、审慎、负责的原则，不利用网络安全威胁信息进行炒作、牟取不正当利益或从事不正当商业竞争。

**第四条**发布的网络安全威胁信息不得包含下列内容：

　　(一)计算机病毒、木马、勒索软件等恶意程序的源代码和制作方法；

　　(二)专门用于从事侵入网络、干扰网络正常功能、破坏网络防护措施或窃取网络数据等危害网络活动的程序、工具；

　　(三)能够完整复现网络攻击、网络侵入过程的细节信息；

　　(四)数据泄露事件中泄露的数据内容本身；

　　(五)具体网络的规划设计、拓扑结构、资产信息、软件源代码，单元或设备选型、配置、软件等的属性信息；

　　(六)具体网络和信息系统的网络安全风险评估、检测认证报告，安全防护计划和策略方案；

　　(七)其他可能被直接用于危害网络正常运行的内容。

**第五条**发布网络和信息系统被攻击破坏、非法侵入等网络安全事件信息前，应向该事件发生所在地地市级以上公安机关报告。各级公安机关应及时将相关情况报同级网信部门和上级公安机关。

**第六条**任何企业、社会组织和个人发布地区性的网络安全攻击、事件、风险、脆弱性综合分析报告时，应事先向所涉及地区地市级以上网信部门和公安机关报告；

　　发布涉及公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的网络安全攻击、事件、风险、脆弱性综合分析报告时，应事先向行业主管部门报告；

　　发布全国性或跨地区、跨行业领域的综合分析报告时，应事先向国家网信部门和国务院公安部门报告。

**第七条**未经政府部门批准和授权，任何企业、社会组织和个人发布网络安全威胁信息时，标题中不得含有“预警”字样。

**第八条**发布具体网络和信息系统存在风险、脆弱性情况，应事先征求网络和信息系统运营者书面意见，以下情况除外：

　　(一)相关风险、脆弱性已被消除或修复；

　　(二)已提前30日向网信、电信、公安或相关行业主管部门举报。

**第九条**通过下列平台发布信息的，平台运营者、主办单位接到有关部门通报、用户举报，或自行发现平台上存在违反本办法的发布行为和发布内容的，应当立即停止发布、采取消除等处置措施，防止违规内容扩散，保存有关记录，并向地市级以上网信部门、公安机关报告。

　　1.报刊、广播电视、出版物；

　　2.互联网站、论坛、博客、微博、公众账号、即时通信工具、互联网直播、互联网视听节目、应用程序、网络硬盘等；

　　3.公开举行的会议、论坛、讲座；

　　4.公开举办的网络安全竞赛；

　　5.其他公共平台。

**第十条**违反本办法规定发布网络安全威胁信息的，由网信部门、公安机关根据《中华人民共和国网络安全法》的规定予以处理。

**第十一条**涉及国家秘密、涉密网络的网络安全威胁信息发布活动，按照国家有关规定执行。

**第十二条**本办法所称网络安全威胁信息，包括：

　　(一)对可能威胁网络正常运行的行为，用于描述其意图、方法、工具、过程、结果等的信息。如：计算机病毒、网络攻击、网络侵入、网络安全事件等。

　　(二)可能暴露网络脆弱性的信息。如：系统漏洞，网络和信息系统存在风险、脆弱性的情况，网络的规划设计、拓扑结构、资产信息、软件源代码，单元或设备选型、配置、软件等的属性信息，网络安全风险评估、检测认证报告，安全防护计划和策略方案等。

**第十三条** 本办法自发布之日起实施。