国家网络安全事件报告管理办法

（2025 年 9 月 11 日　国家互联网信息办公室）

第一条 为规范网络安全事件报告管理，及时控制网络安全事件造成的损失和危害，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《关键信息基础设施安全保护条例》等法律法规，制定本办法。

第二条 在中华人民共和国境内建设、运营网络或者通过网络提供服务的网络运营者，在发生网络安全事件时，应当按照本办法的规定进行报告。

第三条 国家网信部门负责统筹协调全国网络安全事件报告管理工作。省级网信部门负责统筹协调本行政区域内网络安全事件报告管理工作。

第四条 网络运营者在发现或获知涉及本单位的网络安全事件时，应当按照《网络安全事件分级指南》（见附件）进行研判，属于较大以上网络安全事件的，按以下程序报告：

涉及关键信息基础设施的，网络运营者应当第一时间向保护工作部门、公安机关报告，最迟不得超过 1 小时。属于重大、特别重大网络安全事件的，保护工作部门在收到报告后，应当第一时间向国家网信部门、国务院公安部门报告，最迟不得超过半小时。

网络运营者属于中央和国家机关各部门及其直属单位的，应当及时向本部门网信工作机构报告，最迟不得超过 2 小时。属于重大、特别重大网络安全事件的，各部门网信工作机构在收到报告后，应当第一时间向国家网信部

门报告，最迟不得超过 1 小时。国家网信部门收到报告后及时向有关部门通报。

其他网络运营者应当及时向属地省级网信部门报告，最迟不得超过 4 小时。属于重大、特别重大网络安全事件的，省级网信部门在收到报告后，应当第一时间向国家网信部门报告，最迟不得超过 1 小时，并同时向同级有关部门通报。

本行业领域有专门规定的，网络运营者还应当按照行业主管监管部门要求报告。

涉嫌违法犯罪的，网络运营者应当及时向公安机关报案。

第五条 网络运营者应当以合同等形式要求为其提供网络安全、系统运维等服务的组织或个人，及时向其报告监测发现的网络安全事件，并协助其按照本办法规定报告网络安全事件。

第六条 鼓励社会组织和个人报告所获悉的较大以上网络安全事件。

第七条 报告网络安全事件时，应当包括下列内容：

（一）涉事单位名称及涉事系统或设施基本情况；

（二）网络安全事件发现或发生的时间、地点、类型、级别，以及已造成的影响和危害，已采取的措施及效果；对勒索软件攻击事件，还应当包括要求支付赎金的金额、方式、日期等；

（三）事态发展趋势及可能造成的进一步影响和危害；

（四）网络安全事件原因初步分析意见；

（五）溯源调查工作线索，包括但不限于可能的攻击者信息、攻击路径、存在的漏洞等；

（六）拟进一步采取的应对措施以及请求支援事项；

（七）网络安全事件现场保护情况；

（八）其他应当报告的情况。

对于规定时间内不能判定事发原因、影响或发展趋势等网络安全事件情况的，可先报告第一项、第二项内容，其他情况及时补报。

网络安全事件报告后出现新的重要情况或调查工作取得阶段性进展的，涉事单位应当及时报告。

第八条 网络安全事件处置工作结束后，网络运营者应当于 30 日内对相关事件发生原因、应急处置措施、造成的危害、责任追究、完善整改情况、教训等进行全面分析总结，形成事件处置总结报告按照原渠道上报。

第九条 网信部门建设 12387 网络安全事件报告热线电话和网站、邮箱、传真等方式，统一接收网络安全事件报告。

第十条 网络运营者未按照本办法规定报告网络安全事件的，有关主管部门按照有关法律、行政法规的规定进行处罚。

因网络运营者迟报、漏报、谎报或者瞒报网络安全事件，造成重大危害后果的，对网络运营者及有关责任人依法从重处罚。

承担网络安全事件报告的部门未按照本办法规定报告网络安全事件的，依据有关法律、行政法规和网络安全工作责任制追究相关单位和人员责任。

第十一条 发生网络安全事件时，网络运营者已采取合理必要的防护措施，按照应急预案进行处置、有效降低网络安全事件影响和危害，并按照本办法规定及时报告的，可视情从轻或不予追究相关单位和人员责任。

第十二条 本办法所指网络安全事件是指由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷或故障、不可抗力等因素，对网络和信息系统或其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。

本办法所指网络运营者是指网络的所有者、管理者和网络服务提供者。

本办法所指《网络安全事件分级指南》参照《信息安全技术 网络安全事件分类分级指南》国家标准（GB/T 20986-2023）制定，以有限枚举的方式给出相关事件的分级定量指标。

第十三条 涉及国家秘密的网络安全事件报告，按照有关部门规定执行。

第十四条 本办法自 2025 年 11 月 1 日起施行。

附件

网络安全事件分级指南

一、特别重大网络安全事件

符合下列情形之一的，为特别重大网络安全事件：

1.重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

2.核心数据、重要数据、海量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

3.其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

通常情况下，满足下列条件之一的，可判别为特别重大网络安全事件：

1.省级以上党政机关门户网站、中央重点新闻网站因攻击、故障，导致24 小时以上不能访问。

2.关键信息基础设施整体中断运行 6 小时以上或主要功能中断运行 24 小时以上。

3.影响一个或多个省级行政区 50%以上人口，或者 1000 万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等工作、生活。

4.核心数据、重要数据泄露或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

5.泄露 1 亿人以上公民个人信息。

6.省级以上党政机关门户网站、中央重点新闻网站、超大型网络平台等被攻击篡改，导致违法有害信息特大范围传播。以下情况之一，可认定为“特大范围”：

（1）在主页上出现并持续 6 小时以上，或在其他页面出现并持续 24 小时以上；

（2）通过社交平台转发 10 万次以上；

（3）浏览或点击次数 100 万以上；

（4）省级以上网信部门、公安机关认定为是“特大范围传播”的。

7.造成 1 亿元以上的直接经济损失。

8.其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

二、重大网络安全事件

符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：

1.重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

2.核心数据、重要数据、大量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。

3.其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

通常情况下，满足下列条件之一的，可判别为重大网络安全事件：

1.地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站因攻击、故障，导致 6 小时以上不能访问。

2.关键信息基础设施整体中断运行 1 小时以上或主要功能中断运行 3 小时以上。

3.影响一个或多个地市级行政区 50%以上人口，或者 100 万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等的工作、生活。

4.核心数据、重要数据泄露或被窃取、篡改、仿冒，对国家安全和社会稳定构成严重威胁。

5.泄露 1000 万人以上公民个人信息。

6.地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站，大型以上网络平台等被攻击篡改，导致违法有害信息大范围传播。以下情况之一，可认定为“大范围”：

（1）在主页上出现并持续 2 小时以上，或在其他页面出现并持续 12 小时以上；

（2）通过社交平台转发 1 万次以上；

（3）浏览或点击次数 10 万以上；

（4）省级以上网信部门、公安机关认定为是“大范围传播”的。

7.造成 2000 万元以上的直接经济损失。

8.其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

三、较大网络安全事件

符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：

1.重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。

2.重要数据、较大量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。

3.其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

通常情况下，满足下列条件之一的，可判别为较大网络安全事件：

1.地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站因攻击、故障，导致 2 小时以上不能访问。

2.关键信息基础设施整体中断运行 10 分钟以上或主要功能中断运行 30 分钟以上。

3.影响一个或多个地市级行政区 30%以上人口，或者 10 万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等工作、生活。

4.重要数据泄露或被窃取，对国家安全和社会稳定构成较严重威胁。

5.泄露 100 万人以上公民个人信息。

6.党政机关、企事业单位门户网站，重点新闻网站，网络平台等被攻击篡改，导致违法有害信息较大范围传播。以下情况之一，可认定为“较大范围”：

（1）在主页上出现并持续 30 分钟以上，或在其他页面出现并持续 2 小时以上；

（2）通过社交平台转发 1000 次以上；

（3）浏览或点击次数 1 万以上；

（4）省级以上网信部门、公安机关认定为是“较大范围传播”的。

7.造成 500 万元以上的直接经济损失。

8.其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

四、一般网络安全事件

除上述网络安全事件外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件。

注：本指南中的“以上”均包括本数。