北京市公共互联网网络安全
突发事件应急预案

1. 总则

1.1 编制目的

建立健全北京市公共互联网网络安全突发事件应急组织体系和工作机制，提高北京市公共互联网网络安全突发事件综合应对能力，确保及时有效地控制、减轻和消除北京市公共互联网网络安全突发事件造成的社会危害和损失，保证北京市公共互联网持续稳定运行和数据安全。

1.2 编制依据

1.2.1 法律法规

（1）《中华人民共和国突发事件应对法》（中华人民共和国主席令第 69 号发布）

（2）《中华人民共和国网络安全法》（全国人民代表大会常务委员会于 2016 年 11 月 7 日发布）

（3）《中华人民共和国电信条例》（2000 年 09 月 25 日国务院令第 291 号发布）

1.2.2 政策文件

（1）《国家突发公共事件总体应急预案》（国务院于 2006 年 1 月发布）

（2）《国家网络安全事件应急预案》（中网办发文〔2017〕4 号）

（3）《通信网络安全防护管理办法》（中华人民共和国工业和信息化部令第 11 号）

（4）《公共互联网网络安全突发事件应急预案》（工信

部网安〔2017〕281号）

（5）《北京市突发事件预警信息发布管理暂行办法》（京政办发〔2013〕4号）

1.3 适用范围

本预案适用于北京市行政区域内面向社会提供服务的基础电信企业、域名注册管理和服务机构（以下简称域名机构）、互联网企业（含工业互联网平台企业）发生网络安全突发事件的应对工作。

本预案所称网络安全突发事件，是指突然发生的，由网络攻击、网络入侵、恶意程序等导致的，造成或可能造成严重社会危害或影响，需要电信主管部门组织采取应急处置措施予以应对的网络中断（拥塞）、系统瘫痪（异常）、数据泄露（丢失）、病毒传播等事件。

工业和信息化部和北京市通信管理局对国家和本市重大活动期间网络安全突发事件应对工作另有规定的，从其规定。

1.4 工作原则

北京市公共互联网网络安全突发事件应急工作坚持统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置；坚持预防为主，预防与应急相结合；落实北京市基础电信企业、域名机构、互联网企业的主体责任；充分发挥网络安全专业机构、网络安全企业和专家学者等各方面力量的作用。

2. 组织体系

2.1 组织机构与职责

在北京市网络安全和信息化领导小组（以下简称市网信领导小组）统筹协调下，在工业和信息化部网络安全应急办公室（以下简称部应急办）统一指挥下，北京市通信管理局负责组织、指挥、协调北京市基础电信企业、域名机构、互联网企业开展公共互联网网络安全突发事件的预防、监测、报告和应急处置工作，负责较大和一般等级的北京市公共互联网网络安全突发事件的指挥和协调。办事机构设在北京市通信管理局网络安全管理处。

2.2 其他相关单位职责

北京市基础电信企业、域名机构、互联网企业负责本单位网络安全突发事件预防、监测、报告和应急处置工作，为其他单位的网络安全突发事件应对提供技术支持。

中国信息通信研究院等网络安全专业机构受北京市通信管理局委托，协助监测、报告北京市公共互联网网络安全突发事件和预警信息，为北京市公共互联网网络安全应急工作提供决策支持和技术支撑。

鼓励网络安全企业支撑参与北京市公共互联网网络安全突发事件应对工作。

3. 事件分级

根据社会影响范围和危害程度，公共互联网网络安全突

发事件分为四级：特别重大事件、重大事件、较大事件、一般事件。具体参照《公共互联网网络安全突发事件应急预案》（工信部网安〔2017〕281号）有关规定（附件一）。

4. 监测预警

4.1 事件监测

北京市基础电信企业、域名机构、互联网企业应当对本单位网络和系统的运行状况进行密切监测，一旦发生本预案规定的北京市公共互联网网络安全突发事件，初步判定是特别重大或重大事件，应当立即向部应急办报告，同时报北京市通信管理局；初步判定是较大或一般事件,应当立即通过电话等方式向北京市通信管理局报告，不得迟报、谎报、瞒报、漏报。

4.2 预警监测

北京市基础电信企业、域名机构、互联网企业、网络安全专业机构、网络安全企业应当通过多种途径监测、收集漏洞、病毒、网络攻击最新动向等网络安全隐患和预警信息，对发生北京市公共互联网网络安全突发事件的可能性及其可能造成的影响进行分析评估，认为可能发生特别重大或重大事件，应当立即向部应急办报告，同时报北京市通信管理局；认为可能发生较大或一般事件，应当立即向北京市通信管理局报告。

4.3 预警分级

按照紧急程度、发展态势和可能造成的危害程度，北京市公共互联网网络安全突发事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色标示，分别对应可能发生特别重大、重大、较大和一般网络安全突发事件。

4.4 预警发布

北京市通信管理局及时汇总分析北京市公共互联网网络安全突发事件隐患和预警信息，必要时组织相关单位、专业技术人员、专家学者进行会商研判。

红色、橙色预警由部应急办统一发布。

黄色、蓝色预警由北京市通信管理局按照《北京市突发事件预警信息发布管理暂行办法》在北京市行政区域内进行预警发布，并报相关上级单位。

对达不到预警级别但又需要发布警示信息的，北京市通信管理局可以发布风险提示信息。

4.5 预警响应

部应急办发布红色、橙色预警后，北京市通信管理局立即全面了解北京市受影响情况，在部应急办指挥、协调下组织各相关基础电信企业、域名机构、互联网企业开展相关工作，加强对重要网络、系统的网络安全防护；组织研究制定防范措施和应急工作方案，协调调度各方资源，做好各项准备工作，重要情况报相关上级单位。

北京市通信管理局发布黄色、蓝色预警后，各相关基础

电信企业、域名机构、互联网企业应当针对即将发生的网络安全突发事件的特点和可能造成的危害，加强网络安全风险监测，加强事态跟踪分析评估，密切关注事态发展，重要情况报北京市通信管理局。

4.6 预警解除

红色、橙色预警由部应急办统一解除。

黄色、蓝色预警发布后，经北京市通信管理局组织研判确定不可能发生突发事件或风险已经解除的，按照《北京市突发事件预警信息发布管理暂行办法》解除预警，解除已经采取的有关措施，并报相关上级单位。

5. 应急处置

5.1 响应分级

公共互联网网络安全突发事件应急响应分为四级：I 级、II 级、III 级、IV 级，分别对应已经发生的特别重大、重大、较大、一般事件的应急响应。

5.2 报告制度

北京市公共互联网网络安全突发事件发生后，事发单位初步判定是特别重大或重大事件，应当立即向部应急办报告，同时报北京市通信管理局；初步判定是较大或一般事件，应当立即向北京市通信管理局报告。信息报送内容应包括事件发生单位概况、事件发生时间、事件简要经过、初步估计的危害和影响、已采取的措施，以及其他应当报告的情况。报

送信息模板参考《北京市网络安全突发事件信息报送表》(附件二)。

来不及形成文字的，可先用电话口头报告，再呈送书面文字报告；来不及呈送详细报告的，可先做简要报告，再根据事态发展和处理情况，随时续报。

北京市通信管理局及时向相关上级单位报告突发事件处置进展情况；及时向社会公众通告突发事件情况，宣传避免或减轻危害的措施，公布咨询电话，引导社会舆论。未经北京市通信管理局同意，各相关单位不得擅自向社会发布突发事件相关信息。

5.3 先行处置

北京市公共互联网网络安全突发事件发生后，事发单位在按照本预案规定立即报告的同时，应当立即启动本单位应急预案，组织本单位应急队伍和工作人员采取应急处置措施，尽最大努力恢复网络和系统运行，尽可能减少对用户和社会的影响，同时注意保存网络攻击、网络入侵或网络病毒的证据。

5.4 启动响应

I 级响应根据国家有关决定或经部领导小组批准后启动，II 级响应由部应急办决定启动。

启动 I 级、II 级响应后，北京市通信管理局立即全面了解北京市受影响情况，在部应急办指挥、协调下开展相关工作。

III 级、IV 级响应由北京市通信管理局启动。

启动 III 级、IV 级响应后，北京市通信管理局立即将突发事件情况向相关上级单位报告；北京市通信管理局和相关单位进入应急状态，实行 24 小时值班，相关人员保持联络畅通；北京市通信管理局视情况组织相关单位集中办公，设立应急恢复、攻击溯源、影响评估、信息发布等工作机构。

5.5 事态跟踪

启动 I 级、II 级响应后，事发单位和网络安全专业机构、网络安全企业应当持续加强监测，跟踪事态发展，检查影响范围，密切关注舆情，及时将事态发展变化、处置进展情况、相关舆情报部应急办，同时报北京市通信管理局。

启动 III 级、IV 级响应后，北京市通信管理局组织相关单位加强事态跟踪研判。事发单位和网络安全专业机构、网络安全企业应当持续加强监测，及时将事态发展情况、处置进展情况等报北京市通信管理局。

5.6 决策部署

启动 III 级、IV 级响应后，北京市通信管理局紧急召开会议，听取各相关方面情况汇报，研究紧急应对措施，对应急处置工作进行决策部署。北京市通信管理局组织相关力量加强研判，形成《北京市网络安全突发事件研判结果表》（附件三），向事发单位下发《北京市网络安全突发事件处置任务单》（附件四）。

针对突发事件的类型、特点和原因，要求相关单位采取

但不限于以下措施：带宽紧急扩容、控制攻击源、过滤攻击流量、修补漏洞、查杀病毒、关闭端口、启用备份数据、暂时关闭相关系统等；对大规模用户信息泄露事件，要求事发单位及时告知受影响的用户，并告知用户减轻危害的措施；防止发生次生、衍生事件的必要措施；其他可以控制和减轻危害的措施。

5.7 结束响应

突发事件的影响和危害得到控制或消除后，I 级响应根据国家有关决定或经部领导小组批准后结束；II 级响应由部应急办决定结束；III 级、IV 级响应由北京市通信管理局决定结束，并报相关上级单位。

6. 事后总结

6.1 调查评估

北京市公共互联网网络安全突发事件应急响应结束后，事发单位要及时调查突发事件的起因（包括直接原因和间接原因）、经过、责任，评估突发事件造成的影响和损失，总结突发事件防范和应急处置工作的经验教训，提出处理意见和改进措施，在应急响应结束后 10 个工作日内形成总结报告，具体参照《北京市网络安全突发事件处置总结报告》（附件五），报北京市通信管理局。北京市通信管理局汇总并研究后，在应急响应结束后 20 个工作日内形成报告，按程序上报。

6.2 奖惩问责

对在应急事件响应过程中做出突出贡献的单位和个人，北京市通信管理局给予表彰和奖励。

对不按照规定制定应急预案和组织开展演练，迟报、谎报、瞒报和漏报突发事件重要情况，或在预防、预警和应急工作中有其他失职、渎职行为的单位或个人，由北京市通信管理局给予约谈、通报或依法、依规给予问责或处分。基础电信企业有关情况纳入企业年度网络与信息安全责任考核。

7. 预防与应急准备

7.1 预防保护

北京市基础电信企业、域名机构、互联网企业应当根据有关法律法规和国家、行业标准的规定，建立健全网络安全管理制度，采取网络安全防护技术措施，建设网络安全技术手段，定期进行网络安全检查和风险评估，及时消除隐患和风险。北京市通信管理局在相关上级单位统筹协调下，依法开展网络安全监督检查，指导督促相关单位消除安全隐患。

7.2 应急演练

北京市通信管理局组织开展北京市公共互联网网络安全突发事件应急演练，提高相关单位网络安全突发事件应对能力。北京市基础电信企业、大型互联网企业、域名机构要积极参与北京市通信管理局组织的应急演练，并应每年组织开展一次本单位网络安全应急演练，应急演练情况要向北京

市通信管理局报告。

7.3 宣传培训

北京市通信管理局组织开展网络安全应急相关法律法规、应急预案和基本知识的宣传教育和培训，提高北京市相关企业和社会公众的网络安全意识和防护、应急能力。北京市基础电信企业、域名机构、互联网企业要面向本单位员工加强网络安全应急宣传教育和培训。鼓励开展各种形式的网络安全竞赛。

7.4 手段建设

北京市通信管理局规划建设网络安全应急指挥系统，汇集、存储、分析有关突发事件的信息，开展应急指挥调度，并与工业和信息化部网络安全应急指挥平台实现互联互通；指导北京市基础电信企业、大型互联网企业、域名机构等单位规划建设本单位突发事件信息系统，并与北京市通信管理局应急指挥系统实现对接。

7.5 工具配备

北京市基础电信企业、域名机构、互联网企业和网络安全专业机构应加强对木马查杀、漏洞检测、网络扫描、渗透测试等网络安全应急装备、工具的配备，及时调整、升级软件硬件工具。鼓励研制开发相关技术装备和工具。

8. 保障措施

8.1 落实责任

北京市基础电信企业、域名机构、互联网企业要落实网络安全应急工作责任制，把责任落实到单位领导、具体部门、具体岗位和个人，建立健全本单位网络安全应急工作体制机制。

8.2 经费保障

北京市基础电信企业、域名机构、大型互联网企业应当安排专项资金，支持本单位网络安全应急队伍建设、手段建设、应急演练、应急培训等工作开展。

8.3 队伍建设

北京市基础电信企业、域名机构、大型互联网企业要建立专门的网络安全应急队伍，加强网络安全人才储备，提升本单位网络安全应急能力。支持北京市网络安全企业提升应急支撑能力，促进北京市网络安全应急产业发展。

8.4 社会力量

建立北京市网络安全应急专家组，充分发挥专家在应急处置工作中的作用。从网络安全专业机构、相关企业、科研院所、高等学校中选拔网络安全技术人才，形成北京市网络安全技术人才库。

9. 附则

9.1 预案管理

本预案原则上每年评估一次，根据实际情况适时进行修订，并报工业和信息化部备案。

北京市基础电信企业、域名机构、互联网企业要制定本单位公共互联网网络安全突发事件应急预案。北京市基础电信企业、域名机构、大型互联网企业的应急预案要向北京市通信管理局备案。

9.2 预案解释

本预案由北京市通信管理局负责解释。

9.3 预案实施时间

本预案自印发之日起实施。

附件一：公共互联网网络安全突发事件分级

根据社会影响范围和危害程度，公共互联网网络安全突发事件分为四级：特别重大事件、重大事件、较大事件、一般事件。

1.特别重大事件

符合下列情形之一的，为特别重大网络安全事件：

（1）全国范围大量互联网用户无法正常上网；

（2）.CN 国家顶级域名系统解析效率大幅下降；

（3）1 亿以上互联网用户信息泄露；

（4）网络病毒在全国范围大面积爆发；

（5）其他造成或可能造成特别重大危害或影响的网络安全事件。

2.重大事件

符合下列情形之一的，为重大网络安全事件：

（1）多个省大量互联网用户无法正常上网；

（2）在全国范围有影响力的网站或平台访问出现严重异常；

（3）大型域名解析系统访问出现严重异常；

（4）1 千万以上互联网用户信息泄露；

（5）网络病毒在多个省范围内大面积爆发；

（6）其他造成或可能造成重大危害或影响的网络安全事件。

3.较大事件

符合下列情形之一的，为较大网络安全事件:

（1）1 个省内大量互联网用户无法正常上网;

（2）在省内有影响力的网站或平台访问出现严重异常;

（3）1 百万以上互联网用户信息泄露;

（4）网络病毒在 1 个省范围内大面积爆发;

（5）其他造成或可能造成较大危害或影响的网络安全事件。

4.一般事件

符合下列情形之一的，为一般网络安全事件:

（1）1 个地市大量互联网用户无法正常上网;

（2）10 万以上互联网用户信息泄露;

（3）其他造成或可能造成一般危害或影响的网络安全事件。

附件二：北京市网络安全突发事件信息报送表

事发单位	
事发时间	
事件描述	
初步评估的危害和影响	
已采取的措施	

附件三：北京市网络安全突发事件研判结果表

事件名称	
事发时间	
事件情况概述	
研判单位	
事件等级	□Ⅰ级　□Ⅱ级　□Ⅲ级　□Ⅳ级
事件具体描述	
处置方案及建议	

附件四：北京市网络安全突发事件处置任务单

执行单位	
事件名称	
事件等级	□Ⅰ级　□Ⅱ级　□Ⅲ级　□Ⅳ级
事发时间	
事件描述	
处置措施	

附件五：北京市网络安全突发事件处置总结报告

执行单位	
事件名称	
事发时间	
事件起因	
事件简要经过	
事件造成的 影响和损失	
处理意见和改进措施	