通文旅发〔2022〕21号

网络安全事件应急预案

1 总则

1.1 编制目的

立足城市副中心高质量发展，建立健全通州区文旅系统网络安全事件应急工作机制和应急预案体系，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保障全区文旅系统网络安全运行和公众利益，维护国家安全、公共安全和社会秩序。

1.2 编制依据

依据《中华人民共和国突发事件应对法》《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》《北京市实施<中华人民共和国突发事件应对法>办法》，以及《信息安全技术信息安全事件分类分级指南》《国家网络安全事件应急预案》《北京市突发事件总体应急预案》《北京市网络安全事件应急预案》《通州区突发事件总体应急预案》《北京市通州区网络安全事件应急预案》等相关规定和文件，制订本预案。

1.3 适用范围

本预案主要指导预防和处置发生在通州区文化和旅游局系统范围内。本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者网络数据造成危害，对社会造成负面影响的事件。发生由网络安全事件引发的其他突发事件时，同步依据相关领域应急预案开展应对。

1.4 工作原则

坚持总体国家安全观，牢固树立副中心意识；坚持党组领导、分级负责；坚持统一指挥、科学处置；坚持预防为主，预防与应急相结合；坚持谁主管谁负责、谁运行谁负责；坚持平战结合、网上网下结合，充分发挥各方面力量，密切衔接配合，共同做好全区文旅系统网络安全事件的预防与处置工作。

1.5 事件分级

根据网络和信息系统重要程度、系统损失和社会影响等因素将网络安全事件由高到低分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

1.5.1 特别重大网络安全事件

特别重大网络安全事件是指能够导致特别严重破坏或影响的网络安全事件，包括以下情况：

（1）关键信息基础设施或其他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）国家秘密信息、重要敏感信息和关键数据泄露、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。

1.5.2 重大网络安全事件

重大网络安全事件是指能够导致严重破坏或影响的网络安全事件，包括以下情况：

（1）关键信息基础设施遭受严重或较大级别的系统损失；或其他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）国家秘密信息、重要敏感信息和关键数据泄露、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。

1.5.3 较大网络安全事件

较大网络安全事件是指能够导致较严重影响或破坏的网络安全事件，包括以下情况：

（1）关键信息基础设施遭受较小的系统损失；或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；或一般网络和信息系统遭受较大及以上级别的系统损失；

（2）国家秘密信息、重要敏感信息和关键数据泄露、丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成一定或较严重的威胁；

（3）其他对国家安全、社会秩序、经济建设和公众利益构成一定或较严重的威胁、造成一定或较严重影响的网络安全事件。

1.5.4 一般网络安全事件

一般网络安全事件是指不满足以上条件的网络安全事件，包括以下情况：

（1）重要网络和信息系统或一般网络和信息系统遭受较小的系统损失；

（2）其他对国家安全、社会秩序、经济建设和公众利益基本没有影响，但对个别公民、法人或其他组织的利益造成一定损害的网络安全事件。

2 组织机构与职责

2.1 领导机构与职责

区文旅局党组统一领导全区文旅系统网络安全保障和突发事件预防应对工作。在区文旅局党组的领导下，设立区文旅系统网络安全事件应急指挥部（以下简称“指挥部”），指挥部办公室设置在区文旅局办公室，统筹协调组织全区文旅系统网络安全事件的处置应对工作。

2.1.1 组成人员

区文旅系统网安应急指挥部由总指挥、副总指挥和成员单位有关负责同志组成。总指挥由区文旅局党组书记、局长张华同志担任，负责全区文旅系统网安应急指挥部的领导工作，对全区文旅系统网络安全应急工作实施统一指挥。

副总指挥：

党组成员、副局长 杨根萌

党组成员、副局长 马俊艳

党组成员、副局长 王冬生

党组成员、副局长 盖 畅

党组成员、区文化市场综合执法大队大队长 彭绍常

负责协助总指挥做好区文旅系统网安应急指挥部的领导工作，协调各部门、各基层单位、各文旅行业单位实施应急处置工作。

成员由局机关各科室、各基层单位、各部门、各行业单位负责人等担任。

2.1.2 相关工作职责

（1）研究制定全区文旅系统应对网络安全事件的政策措施和指导意见；

（2）配合市、区两级重大网络与信息安全事件应急指挥部，按照区委网信委部署要求，开展全区文旅系统较大及以上网络安全事件应急处置工作；依法指挥协调或指导协助各科室、各基层单位、各部门做好一般网络安全事件应急处置工作；

（3）总结提升全区文旅系统网络安全事件应对处置工作，制定、修订工作规划；

（4）负责本指挥部所属应急处置队伍、应急物资保障的建设和管理等工作；

（5）承担区委区政府、区委网信委、区应急委交办的其他事项。

2.2 日常工作机构与职责

局机关办公室作为区文旅系统网安应急指挥部日常工作机构。办公室主任由局机关办公室主任担任。 办公室具体承担区文旅系统网络安全事件应急工作的规划、组织、协调、指导和检查工作，其主要职责是：

（1）按照指挥部的要求和指令，组织协调各科室、各基层单位、各部门开展网络安全事件的预防和应对工作；

（2）组织拟订、修订与区文旅系统网络应急指挥部职能相关的应急预案，指导各科室、各基层单位、各部门制定、修订网络安全事件应急预案；

（3）组织协调开展网络安全风险评估、隐患排查、监测预警工作；

（4）组织指导区文旅系统网络安全应急队伍做好应急处置的技术支撑工作；

（5）承担区文旅系统网安应急指挥部的日常工作。

2.4 各相关部门职责

区文旅系统各相关部门按照职责权限，负责本部门、本行业网络安全事件的预防、监测、报告和应急处置工作。

2.5 应急队伍与职责

区文旅系统由建设相关网络系统的部门，结合职责和工作需要，统筹建设本部门网络系统的网络安全应急队伍。各应急队伍由其所在部门负责日常管理。在网络安全事件预警和应急响应过程中，做好 24 小时应急备勤，并按照区文旅系统网安应急指挥部的指挥调度，开展应急处置工作。

3 监测与预警

3.1 监测和报告

3.1.1 安全监测

按照 “谁主管谁负责、谁运行谁负责”的原则，各部门组织对本部门建设运行的网络和信息系统开展网络安全监测工作。各行业主管部门组织指导做好本行业网络安全监测工作，及时掌握本行业网络和信息系统的风险状况。各单位将重要监测信息及时报送至指挥部，由指挥部统一上报至区网络安全指挥部进行处理。

3.1.2 态势会商和信息通报

指挥部各副指挥分别负责分管领域内网络安全态势的分析、评估和信息报送、通报工作。指挥部根据需要定期或不定期组织相关单位开展区文旅系统网络安全态势分析、风险评估、威胁研判、信息通报等。

3.1.3 重要活动和敏感时期的监测报告

北京市和本区承办重要活动、会议期间，相关部门要加强网络安全事件监测和分析研判，及时发现、预警和处置可能造成重大影响的风险隐患和安全事件。重点部门、重点岗位要保持 24小时值班，重要情况及时报送至指挥部。

3.2 预警分级

预警等级分为四级，由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或者可能发生特别重大、重大、较大和一般网络安全事件。

3.3 预警研判和发布

3.3.1 预警发布

文旅系统、各单位组织对监测信息进行研判，认为需要立即采取防范措施的，应及时通知有关部门和单位；认为可能发生网络安全事件的，应及时向指挥部报告，由指挥部统一向区级网络安全负责部门报告。

指挥部接到各单位报告后，应及时组织有关部门分析研判，认为可能发生较大及以上网络安全事件的，应及时报区网安应急指挥部和区委网信委。

蓝色预警由区网安应急指挥部根据监测研判情况在本区发布。涉及全市范围内的预警，由市网信安全应急办公室研判后发布。

黄色预警由市网信安全应急办公室组织研判，报请市网信安全应急指挥部批准后发布。

橙色预警由市网信安全应急指挥部组织研判，报请市委网信委批准后发布。

红色预警由市网信安全应急指挥部组织研判，经市委网信委批准后报请国家网络安全应急办公室发布。

3.3.2 预警信息

预警信息包括网络安全事件的类别、预警级别、起始时间、可能影响范围、警示事项、预防措施和时限要求、发布范围、发布机关等。

3.3.3 发布范围

网络安全事件预警信息发布范围分为面向网络和信息系统运营使用管理单位和面向社会公众两类，由区网安应急办会同事发单位或主管部门研究确定或提出建议。

3.3.4 预警级别的变更

区网安应急办密切关注事态发展，根据实际情况和专家意见，适时向区网安应急指挥部及市网信安全应急办公室报告调整预警级别建议，并将调整结果及时通报至区文旅局。

3.4 预警响应

预警信息发布后，文旅系统各单位应依据发布的预警级别，启动相应的应急预案，组织部署所属人员力量立即响应，进入应急状态，履行承担的职责。

3.4.1 红色、橙色、黄色预警响应

按照国家网络安全应急办公室、市网信安全应急办公室的统一部署和指令，区网安应急指挥部实行 24 小时值班，区文旅系统内有自行建设网络信息系统的相关人员保持通信联络畅通。（区网安应急指挥部加强网络安全事件监测和事态发展信息搜集工作，组织指导应急支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作，重要情况应及时由指挥部报区委网信委及市网信安全应急办公室。）

3.4.2 蓝色预警响应

（1）指挥部组织预警响应，启动应急预案，在区网安应急办的指导下对事态发展情况进行跟踪研判，开展风险评估、风险控制和应急处置准备工作，细化完善防范措施和应急工作方案，协调组织资源调度和部门联动的各项准备工作。

（2）文旅系统网络安全应急指挥部实行 24 小时值班，相关人员保持通信联络畅通。加强网络安全监测和事态发展信息收集工作，重要情况及时报指挥部，由指挥统一报送至区网安应急指挥部、区委网信委和市网信安全应急办公室。指挥部根据事态发展，及时将重要事项通报有关单位。

（3）有自建网络信息系统的相关单位安全应急队伍进入待命状态，针对预警信息研究制定应对方案，检查设备、软件工具等，确保处于良好状态。

3.5 预警解除

蓝色预警由区网安应急指挥部根据实际情况报批后解除，并及时发布预警解除信息。

3.6 预警备案

预警的发布、变更、解除按有关规定向区应急办备案。

4 应急处置

4.1 事件报告和先期处置

4.1.1 事件报告

网络安全事件发生后，事发单位应立即启动本单位网络安全事件应急预案，实施处置，控制事态，消除隐患，同时组织研判，保存电子证物，并做好信息报送工作。文旅系统管理对象要建立健全网络安全事件信息报告机制。网络安全事件发生后，涉事单位应立即将简要情况及联系人通过电话、传真等方式上报指挥部，由指挥部统一报送至区网安应急办。对于初判为较大网络安全事件的，指挥部要在事件确认后 2 小时内，向区网安应急指挥部、区委网信委报告有关情况。对于初判为重大及以上网络安全事件的，应立即报告区网安应急指挥部、区委网信委。上述信息按有关要求同步报区委办值班室、区应急办。报告内容主要包括：网络安全事件发生的时间、涉及的网络和信息系统名称及使用管理单位、地点、原因、信息来源、类型及性质、危害和损失程度、影响单位及业务、发展趋势、应采取的处置措施等。

4.1.2 先期处置

事件发生后，涉事相关单位和部门应立即采取各种技术措施进行先期处置，最大限度控制事态、消除隐患。超出应对能力范围的，提出应对措施建议。在先期处置过程中，应采取手工记录、截屏、文件备份和影像设备记录等多种手段，对网络安全事件发生、发展、处置的过程、步骤、结果进行详细记录，尽可能保存原始证据，为事件处置、调查、处理提供客观证据。对于涉密重要信息，收集数据时应遵守相关管理规定，做好信息保密工作。

4.2 应急响应等级和原则

4.2.1 应急响应等级

应急响应等级网络安全事件应急响应分为Ⅰ、Ⅱ、Ⅲ、Ⅳ四级，分别对应特别重大、重大、较大和一般网络安全事件。Ⅰ级为最高响应级别。

4.2.2 应急响应原则

网络安全事件应急响应遵循“行业管理、分级负责”原则。

（1）发生一般网络安全事件，由区网安应急指挥部及办公室组织有关单位应对。超出本单位应对能力的，由指挥部报请区网信安全应急指挥部提供支援或者组织应对。

（2）发生涉及跨行业的网络安全事件，由指挥部报请区网安应急办负责应对。

（3）可能或已经发生由网络安全事件引发的其他突发事件时，由指挥部及时按规定上报区网安应急办，启动相关领域应急指挥机构协同应对，指挥部与区网安应急指挥部邓指挥机构做好信息共享、工作配合。

（4）当上级成立现场指挥机构统一指挥、协调处置网络安全事件时，下级现场指挥机构应纳入上级现场指挥机构，在上级统一领导下组织开展网络安全事件应对工作。前往网络安全事件现场参加应急处置的各方应急力量要及时向现场指挥机构报到、受领任务，接受现场指挥机构的统一指挥调度，并及时报告现场情况和处置工作进展情况。

4.3 应急响应

4.3.1 Ⅰ级、Ⅱ级、Ⅲ级响应

I 级响应在国家网络安全应急办公室、市网信安全应急指挥部的统一领导和指挥下启动，Ⅱ级响应在市网信安全应急指挥部的统一领导和指挥下启动，Ⅲ级响应在市网信安全应急办公室的统一领导和指挥下启动。

（1）指挥部在区网安应急指挥部指导下进入应急状态，在上级指挥部统一领导、指挥、协调下，负责统筹指挥全区文旅系统应急处置工作及支援保障工作。指挥部实施 24 小时值班，各建设网络信息系统成员单位保持 24 小时联络畅通。

（2）由指挥部安排专人与区网安应急指挥部总指挥指派联络员对接，完成上级指挥部安排的应急处置工作。

（3）指挥部要及时向区网安应急办报送事态发展变化情况和处置进展，指挥部要全面掌握区文旅系统网络和信息系统受影响范围，有关情况及时上报。

（4）有网络信息系统建设的单位，要组织网络安全应急支撑队伍，提出处置方案建议，为指挥部决策提供支撑。

（5）指挥部根据事态发展，及时向区网安应急办求助相关单位和技术力量，根据事件发生原因，采取针对性措施，恢复受破坏的网络和信息系统正常运行，对业务连续性要求高的系统，采用启动备机等方式进行紧急修复，并督促、指导网络和信息系统运营使用管理单位针对性加强防范。

4.3.2 Ⅳ级响应

有网络信息系统建设的单位，要及时组织相关人员对事件信息进行研判，认为属于一般网络安全事件的，及时向指挥部汇报，由指挥部统一向区委网信委提出启动Ⅳ级响应建议。经批准后，由区网安应急指挥部启动Ⅳ级响应，统一指挥、协调、组织应急处置工作。

（1）启动指挥体系。指挥部进入应急状态，指挥部办公室实施 24 小时值班，有网络信息系统建设的单位保持 24 小时联络畅通。成立现场指挥部，根据应急处置工作需要，指挥部总指挥赴现场指挥协调处置。网络安全应急机构进入应急状态，在指挥部统一领导、指挥、协调下，负责本行业、本部门网络信息系统应急处置工作或支援保障工作。

（2）掌握事件动态。指挥部组织各有关单位及时跟踪事态发展变化，全面了解网络和信息系统运行情况，重要信息及时报区网安应急指挥部。

（3）实施应急处置。有网络信息系统建设的单位要及时组织专家队伍、技术力量等方面分析事件发生原因、特点、发展趋势，制定解决方案，实施应急处置。指挥部及时督促、指导有关单位加强防范，防止事态扩散和蔓延。各有关单位根据事件发生原因，采取针对性措施，恢复受破坏的网络和信息系统正常运行，对业务连续性要求高的系统，采用启动备机等方式进行紧急修复。处置情况及时报指挥部，由指挥部向区级指挥部统一报送。

4.3.3 响应级别变更

（1）在应急响应过程中，区指挥部要密切关注事态发展和响应工作进展情况，根据事态变化和应对处置效果及专家建议，适时报请区级指挥部调整响应级别，开展相应处置工作。超出本级应急处置能力的，要及时报告，并作出提高响应级别建议。

（2）网络安全事件本身比较敏感，发生在重点地区或重要活动举办、重要会议召开等特殊时期的，可报请适当提高响应级别。

4.4 重大活动期间的专项应急响应

北京市和本区重大活动、会议期间，在按照突发事件分级响应的基础上，指挥部统筹加强文旅系统网络安全事件的监测预警、通报报告、应急处置工作。结合重大活动地点、规模、特点等，指挥部组织有网络信息系统建设制定网络安全事件专项应急预案。各行业主管科室、基层单位、部门加强网络安全监测预警和分析研判，重点部门、重点岗位保持 24 小时值班，及时发现和处置网络安全隐患。

4.5 信息发布和新闻报道

（1）网络安全事件发生后，需要开展信息发布和新闻报道时，由指挥部安排专人与区网安应急指挥部成立新闻信息组，负责新闻发布工作，起草新闻稿和情况通告，及时、准确、客观报道事件信息，正确引导舆论导向。

（2）对于可能产生较大影响的网络安全事件，对外新闻发布工作应在市网信安全应急办公室的指导下，安排专人与区委宣传部、区委网信办等部门对接，由区级指挥部组织实施。

（3）网络安全事件信息发布和新闻报道工作，须遵守相关法律法规以及相关预案的规定。

4.6 应急结束

在网络安全事件处置已基本完成，次生、衍生灾害和事件危害基本消除，风险得到控制时，启动应急响应的指挥机构可宣布应急结束。

Ⅰ级、Ⅱ级和Ⅲ级响应分别由国家网络安全应急办公室、市网信安全应急指挥部、市网信安全应急办公室宣布结束，指挥部在接收到区网安应急办结束指令，及时通报有关单位。

Ⅳ级响应由指挥部报送至区网安应急指挥部，同意后结束。

5 恢复与总结

5.1 恢复重建

恢复重建工作按照“谁主管谁负责，谁运行谁负责”的原则，由事发单位负责组织制定恢复、整改或重建方案，报相关副总指挥审核后，由总指挥审定后实施。

5.2 调查与总结

特别重大、重大网络安全事件分别由国家网络安全应急办公室、市网信安全应急指挥部组织调查处理和总结评估；较大网络安全事件由市网信安全应急办公室组织事件发生区或部门调查处理和总结评估，总结调查报告报市网安应急指挥部；一般网络安全事件由区网安应急办组织涉事街道乡镇、行业主管部门调查处理和总结评估。

总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。发生网络安全事件的单位及参与应急处置的相关单位，应针对应急响应工作过程中遇到的问题，分析应急预案的科学性和合理性并进行修改完善。事件的调查处理和总结评估工作原则上在应急响应结束后30 天内完成。指挥部办公室建立事件案例库。

5.3 责任与奖惩

网络安全事件应急处置工作实行责任追究制。指挥部对网络安全事件应急管理工作中做出突出贡献的先进集体和个人给予表彰和奖励；对不按照规定制定应急预案、组织开展响应处置工作，迟报、谎报、瞒报和漏报网络安全事件有关情况或者应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处分，构成犯罪的，依法追究刑事责任。

6 预防工作

6.1 日常管理

各单位按职责做好网络安全事件日常预防工作，制定完善相关应急预案，做好网络安全检查、隐患排查、风险评估和容灾备份，健全网络安全信息通报机制，及时采取有效措施，减少和避免网络安全事件的发生及危害，提高应对网络安全事件的能力。

6.2 宣传

各单位应充分利用互联网、电子屏等各种传播媒介及其他有效宣传形式，加强网络安全事件预防处置有关法律、法规和政策的宣传，深入开展应急教育，普及网络安全知识，增强防范意识，提升应急处置技能水平。

6.3 培训

指挥部办公室统筹协调组织各有关单位开展网络安全法律、法规、标准及网络安全预案编制、风险评估、事件分析处置、容灾备份等方面的专业技术培训。各单位要将网络安全事件的应急知识列为行政管理干部和有关人员的培训内容，加强网络安全特别是网络安全应急预案的培训，提高防范意识及技能。

6.4 演练

指挥部办公室按照有关工作要求，协调有关部门，定期组织开展应急演练，模拟处置一般网络安全事件，检验和完善应急预案和应急工作机制，提高网络空间实战能力。各文旅系统企（事）业单位每年至少组织一次网络安全事件应急演练，并将演练情况报指挥部办公室。应急演练应以应急预案为基础，在每次演练前首先确定演练的目标和范围，制定详细严谨的应急演练方案，避免对正常业务造成不必要影响。应急演练的范围可视具体情况而定。

7 保障措施

7.1 建立健全技术支撑体系

7.1.1 健全完善应急指挥平台

加强网络安全应急相关系统平台建设运营。配合推动国家、市、区（行业）三级平台互联互通、信息共享，实现对网络安全事件早发现、早预警、早响应，提高应急处置能力。

7.1.2 完善容灾备份

各行业主管科室要做好对本领域网络和信息系统容灾备份和灾难恢复的指导工作， 确保本行业领域内重要信息系统数据安全和系统灾难恢复，提倡和鼓励采用社会化服务方式实施容灾备份。

7.2 合作机制建设

指挥部办公室统筹加强本系统网络安全应急合作机制建设，建立与区应急相关单位以及专业机构的合作渠道，实现信息共享和应急联动。各行业主管科室及基层单位加强本领域网络安全应急合作机制建设。

7.3 相关保障

指挥部办公室要指导各相关单位加强对网络安全应急装备、工具的储备，及时组织调整、升级软件硬件工具，不断增强应急技术支撑能力。

8 附则

8.1 预案体系

通州区文旅系统网络安全事件应急预案体系由专项预案和单位预案等构成。

本预案为通州区文化和旅游局局机关组织网络安全事件应急处置的区级专项预案，各基层单位、各行业单位预案由各相关单位负责制定。

8.2 预案管理

本预案由通州区文化和旅游局负责制定和解释。

本预案原则上每两年评估一次，并根据实际情况适时修订。

各单位及行业管理单位要根据本预案制定或修订本单位网络安全事件应急预案。各单位应急预案报指挥部办公室备案。

8.3 预案实施

本预案自发布之日起正式实施。

附件：1.网络安全事件分类

2.名词术语

3.网络和信息系统损失程度划分说明

4.网络安全隐患威胁/事件报告表

 北京市通州区文化和旅游局

 2022年7月29日

（联系人：李振；联系电话：17611598721）

（此文主动公开）

北京市通州区文化和旅游局办公室 2022年7月29日印发

附件1

网络安全事件分类

网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、设施设备故障、灾害性事件和其他网络安全事件等。

（1）有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

（2）网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

（3）信息破坏事件分为信息篡改事件、信息假冒事件、信

息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

（4）设施设备故障分为软硬件自身故障、外围保障设施故

障、人为破坏事故和其他设备设施故障。

（5）灾害性事件是指由自然灾害等突发事件导致的网络安

全事件。

（6）其他事件是指不能归为以上分类的网络安全事件。

附件 2

名词术语

一、关键信息基础设施

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，以及其他一旦遭

到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计

民生、公共利益的重要网络设施、信息系统等。

（参考依据：《关键信息基础设施安全保护条例》）

二、重要网络与信息系统

所承载的业务与国家安全、社会秩序、经济建设、公众利益

密切相关的网络和信息系统。

（参考依据：《信息安全技术信息安全事件分类分级指南》

（GB/Z 20986-2007））

三、一般网络与信息系统

受到破坏后，不危害国家安全、社会秩序、经济建设、公众

利益，但会对相关公民、法人和其他组织的合法权益造成一定损

害的信息系统。

四、重要敏感信息

不涉及国家秘密，但与国家安全、经济发展、社会稳定以及

企业和公众利益密切相关的信息，这些信息一旦未经授权披露、

丢失、滥用、篡改或销毁，可能造成以下后果：

1.损害国防、国际关系；

2.损害国家财产、公共利益以及个人财产或人身安全；

3.影响国家预防和打击经济与军事间谍、政治渗透、有组织

犯罪等；

4.影响行政机关依法调查处理违法、渎职行为，或涉嫌违法、

渎职行为；

5.干扰政府部门依法公正地开展监督、管理、检查、审计等

行政活动，妨碍政府部门履行职责；

6.危害国家关键基础设施、政府信息系统安全；

7.影响市场秩序，造成不公平竞争，破坏市场规律；

8.可推论出国家秘密事项；

9.侵犯个人隐私、企业商业秘密和知识产权；

10.损害国家、企业、个人的其他利益和声誉。

（ 参 考 依 据 ：《 信 息 安 全 技 术 云 计 算 服 务 安 全 指 南 》

（GB/T31167-2014））

附件3

网络和信息系统损失程度划分说明

网络和信息系统损失是指由于网络安全事件对系统的软硬件、功能及数据的破坏，导致系统业务中断，从而给事发组织所造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失，说明如下：

1.特别严重的系统损失：造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的；

2.严重的系统损失：造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的；

3.较大的系统损失：造成系统中断，明显影响系统使用效率，使其业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是可承受的；

4.较小的系统损失：造成系统短暂中断，影响系统使用效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。

附件 4

网络安全隐患威胁/事件报告表

报告时间： 年 月 日 时 分 （ 注： 单位名称处需加盖公章）

|  |  |  |
| --- | --- | --- |
| 单位名称  | 报告人 |  |
| 联系电话  | 通讯地址 |  |
| 传真  | 电子邮件 |  |
| 突发网络安全隐患威胁/事件的客体 | 名称： |
| 用途描述： |
| 突发网络安全隐患威胁/事件的简要描述（ 如以前出现过类似情况也应加以说明） | （ 应包括隐患威胁/事件发生时间、 发生隐患威胁/事件的网络和信息系统名称及运营使用管理单位、 地点、 原因、 隐患威胁/事件类型及性质、 危害和损失程度、 影响单位及业务等） |
| 初步判定的事件类别 | □ 有害程序隐患威胁/事件 □ 网络攻击隐患威胁/事件□ 信息破坏隐患威胁/事件 □ 设备设施故障/违规操作□ 灾害性隐患威胁/事件 □ 隐患威胁/事件原因不明 |
| 本次突发网络安全隐患威胁/事件的初步影响状况 | 造成后果  | □ 业务中断 □ 系统破坏□ 数据丢失 □ 其他 |
| 影响范围 | □ 单台主机 □ 多台主机□ 整个信息系统□ 整个局域网□ 其他 |
| 突发网络安全隐患威胁/事件的发展趋势 |  |  |
| 当前采取的应对措施 |  |  |

注： 按照监测实际， 上报网络安全隐患威胁或网络安全事件， 据实填写此表。