上海市长宁区建设和管理委员会

长建委发〔2023〕55号

区建管委

为进一步加强区建管委网络安全工作，建立健全网络安全事件应急工作机制，提高应对突发网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护公众利益，维护国家安全、公共安全和社会秩序，保障城区运行安全。特制定区建管委网络安全事件应急预案。

一、

本预案根据中央、本市网络安全相关应急预案及《上海市长宁区网络安全事件应急预案》编制，适用于区建管委及下属事业单位管辖范围内发生的网络安全事件的预防和处置工作。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，施行预防与应急相结合；坚持“谁主管谁负责，谁运行谁负责”原则，充分发挥各方力量共同做好网络安全事件的预防和处置工作。

、

区建管委网络安全和信息化领导小组负责统筹协调组织区建管委网络安全保障工作，对处置网络安全事件实施统一指挥。各科室、事业单位负责职责范围内突发事件应急处置工作。

、

各科室、事业单位做好管辖范围内网络安全事件的风险评估和隐患排查工作，及时采取有效措施，避免和减少网络安全事件的发生及危害。

（一）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、信息内容安全事件、设备设施故障、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、信息安全内容事件：指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害本区国家安全、社会稳定和公众利益的事件。

5、设备设施故障：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。

6、灾害性事件：是指有自然灾害等其他突发事件导致的网络安全事件。

7、其他事件：不能归为以上分类的网络安全事件。

（二）预警等级：网络安全事件预警等级分为四级，由高到低依次用红色、橙色、黄色、蓝色表示。

1、红色预警：特别重大网络安全事件，包括：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，丧失业务处置能力；国家重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对本区国家安全和社会稳定构成特别严重威胁；其他对本区国家安全、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。

2、橙色预警：重大网络安全事件，包括：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者局部瘫痪，业务处理能力受到极大影响；国家重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对本区国家安全和社会稳定构成严重威胁；其他对本区国家安全、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。

3、黄色预警：较大网络安全事件，包括：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；国家重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对本区国家安全和社会稳定构成较严重威胁；其他对本区国家安全、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。

4、蓝色预警：一般网络安全事件，包括：除上述情形外，对本区国家安全、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。

（三）预警监测：各科室、各事业单位按照“谁主管谁负责、谁运营谁负责”的要求，负责管辖范围内网络和信息系统的网络安全维护，督促相关运维公司开展网络安全监测、管理和应急处置工作。

区委网络安全和信息化委员会办公室（以下简称区委网信办）根据危害性和紧急程度，在一定范围内发布网络安全事件预警信息。区建管委网络安全和信息化领导小组办公室收到相关信息后，第一时间报区建管委党政主要领导、网络安全分管领导，并牵头相关科室、事业单位进入预警期。

（四）预警响应：进入预警期后，相关科室、事业单位立即采取预防措施，会同运维公司检查可能受到影响的网络和信息系统，做好相关安全风险的排查和修复工作，并将最新情况及时报区建管委网络安全和信息化领导小组办公室。

根据事件性质，区建管委网络安全和信息化领导小组办公室、相关科室负责人、相关事业单位网络安全分管领导、联络

员以及运维公司技术支撑人员处于应急待命状态，并保障所需应急设备和网络资源处于随时可调用状态。此外，加强监测，定期向区委网信办报告最新监测情况。

（三）预警解除：区委网信办将根据实际情况，发布预警解除信息。区建管委网络安全和信息化领导小组办公室接收到相关信息后，第一时间报区建管委党政主要领导、网络安全分管领导、相关科室、事业单位负责人。

、

（一）应急响应：发生网络安全事件的科室或事业单位必须半小时内口头、1小时内书面报告区建管委网络安全和信息化领导小组办公室。由领导小组办公室报党政主要领导和网络安全分管领导后，上报区委网信办、区委区府总值班室，由区委网信办提出处置建议并批准后组织实施。

处置网络安全事件应急响应等级分为四级：Ⅰ级、Ⅱ级、Ⅲ级和Ⅳ级，分别对应特别重大、重大、较大、一般网络安全事件。事件的响应等级根据区委网信办的判定等级。

各科室、事业单位应及时主动上报重要网络安全监测信息和处置情况，避免未报、迟报、漏报和瞒报等情况。

（二）应急处置：对于一般、较大网络安全事件，在接到区委网信办提出的应急响应等级和应急处置要求后，区建管委网络安全和信息化领导小组办公室第一时间牵头相关科室、事业单位开展应急处置，启动应急措施。

对于特别重大、重大网络安全事件，必须由区委网信办统一指挥网络安全事件的处置工作。

（三）信息发布：网络安全事件的信息发布和舆论引导工作，由区委网信办、区新闻办统一组织发布。各科室、事业单位不得自行任意发布相关信息和舆论答复。

（四）后期处置：网络安全事件处置后，区建管委网络安全和信息化领导小组办公室协助区委网信办对网络安全事件的起因、性质、影响、损失、责任和经验教训等进行调查和评估。

、

区建管委网络安全和信息化领导小组、各科室、各事业单位要落实网络安全工作责任制，把责任落实到具体岗位和个人，并建立健全应急工作机制。

区建管委网络安全和信息化领导小组办公室要加强网络安全特别是网络安全应急预案的培训，提高防范意识和技能。

各科室、事业单位要根据实际需要，做好网络与信息系统设备储备工作。

如有网络安全技术支撑需求，由区建管委网络安全和信息化领导小组办公室统一向区委网信办争取相关技术人员支持。

本预案自印发之日起实施，由区建管委网络安全和信息化领导小组办公室负责解释，根据实际情况变化，适时评估修订。

长宁区建设和管理委员会

2023年8月1日

长宁区建设和管理委员会　　2023年8月2日印发