短视频平台网络安全事件应急预案

第一章 网络安全事件应急预案概述

1.1 预案目的与适用范围

1.1.1 预案目的

网络安全事件应急预案的制定，旨在建立健全网络安全应急体系，提高我国网络安全事件的应对能力，保证在网络安全事件发生时，能够迅速、高效、有序地开展应急响应工作，最大限度地减轻网络安全事件对国家安全、公共利益和人民群众生活的影响。

1.1.2 适用范围

本预案适用于我国行政区划内的网络安全事件应急响应工作，包括但不限于以下情况：

（1） 网络攻击事件：针对我国关键信息基础设施的网络攻击、入侵、破坏等行为。

（2） 网络安全漏洞事件：关键信息基础设施发觉的安全漏洞，可能引发的安全风险。

（3） 网络安全数据泄露事件：关键信息基础设施数据泄露，可能导致个人信息泄露、经济损失等。

（4） 网络安全事件应急处置：对已发生的网络安全事件进行应急处置，防止事态扩大。

（5） 网络安全事件调查与评估：对网络安全事件进行调查、原因分析，总结经验教训，提高网络安全防护水平。

第二节 预案编制依据

1.1.3 法律法规

（1） 《中华人民共和国网络安全法》

（2） 《中华人民共和国突发事件应对法》

（3） 《信息安全技术 网络安全应急响应要求》

（4） 《信息安全技术 网络安全事件应急响应指南》

1.1.4 政策文件

（1） 《国家网络安全战略》

（2） 《国家网络安全事件应急预案》

（3） 《国家关键信息基础设施安全保护条例》

（4） 《网络安全应急响应行动计划》

1.1.5 行业标准与规范

（1） 信息安全行业标准

（2） 网络安全行业标准

（3） 信息安全风险评估规范

（4） 网络安全监测与预警规范

第三节 预案组织结构

1.1.6 领导机构

网络安全事件应急预案领导机构负责组织、协调、指挥网络安全事件应急响应工作，主要包括：

（1） 国家网络安全应急指挥部

（2） 省级网络安全应急指挥部

（3） 市级网络安全应急指挥部

1.1.7 工作机构

网络安全事件应急预案工作机构负责具体实施网络安全事件应急响应工作，主要包括：

（1） 国家网络安全应急办公室

（2） 省级网络安全应急办公室

（3） 市级网络安全应急办公室

1.1.8 技术支撑机构

网络安全事件应急预案技术支撑机构负责提供技术支持，主要包括：

（1） 国家网络安全应急技术中心

（2） 省级网络安全应急技术中心

（3） 市级网络安全应急技术中心

1.1.9 协作机构

网络安全事件应急预案协作机构负责协助开展网络安全事件应急响应工作，主要包括：

（1） 各级公安机关

（2） 各级通信管理部门

（3） 各级网信部门

（4） 各级国家安全部门

（5） 各级保密部门

（6） 各级财政部门

（7） 各级审计部门

（8） 各级司法部门

（9） 各级教育部门

（10） 各级卫生部门

第二章 网络安全事件分类与分级

第一节 网络安全事件分类

1.1.10 概述

网络安全事件是指在信息网络中，由于人为或自然因素导致的信息泄露、系统破坏、网络瘫痪等安全威胁和损害事件。网络安全事件的分类是为了更好地识别、防范和应对各类安全威胁，保证信息网络的正常运行。以下将从不同角度对网络安全事件进行分类。

1.1.11 分类方法

（1） 按攻击手段分类

（1）恶意代码攻击：包括病毒、木马、蠕虫等。

（2）网络扫描与入侵：包括端口扫描、漏洞扫描、非法访问等。

（3）拒绝服务攻击：包括分布式拒绝服务攻击（DDoS）、网络拥堵等。

（4）网络钓鱼：通过伪装成合法网站或邮件，诱骗用户泄露个人信息。

（5）社会工程学攻击：利用人类信任、好奇等心理特点，实施欺诈行为。

（2） 按攻击对象分类

（1）操作系统攻击：针对 Windows、Linux 等操作系统的攻击。

（2）应用程序攻击：针对 Web 应用、数据库应用等软件的攻击。

（3）网络设备攻击：针对路由器、交换机等网络设备的攻击。

（4）数据攻击：针对数据传输、存储、处理等环节的攻击。

（3） 按攻击目的分类

（1）窃取信息：获取敏感信息，如用户名、密码、信用卡信息等。

（2）破坏系统：使系统瘫痪，导致业务中断。

（3）篡改数据：修改、删除或添加数据，影响数据真实性。

（4）传播恶意代码：感染其他计算机，扩大攻击范围。

第二节 网络安全事件分级

1.1.12 概述

网络安全事件分级是为了对网络安全事件的严重程度进行量化评估，便于实施有针对性的应对措施。以下将从不同角度对网络安全事件进行分级。

1.1.13 分级方法

（1） 按影响范围分级

（1）局部事件：仅影响单个系统或局部网络。

（2）区域事件：影响一个区域内的多个系统或网络。

（3）全局事件：影响整个网络或多个区域。

（2） 按危害程度分级

（1）轻微事件：对系统或网络运行造成轻微影响。

（2）一般事件：对系统或网络运行造成一定影响。

（3）严重事件：对系统或网络运行造成严重影响。

（4）特别严重事件：导致系统瘫痪，业务中断。

（3） 按紧急程度分级

（1）一般紧急：需在短时间内处理的事件。

（2）紧急：需立即处理的事件。

（3）特别紧急：需立即启动应急响应机制的事件。

第三节 事件响应级别划分

1.1.14 概述

事件响应级别划分是为了明确网络安全事件的应对策略和资源分配，保证网络安全事件得到及时、有效的处理。以下将从不同角度对事件响应级别进行划分。

1.1.15 响应级别划分

（1） 局部事件响应级别

（1）一级响应：针对轻微局部事件，由现场运维人员处理。

（2）二级响应：针对一般局部事件，由现场运维人员及安全团队共同处理。

（2） 区域事件响应级别

（1）一级响应：针对轻微区域事件，由区域运维人员处理。

（2）二级响应：针对一般区域事件，由区域运维人员及安全团队共同处理。

（3）三级响应：针对严重区域事件，由区域负责人协调相关资源进行应对。

（3） 全局事件响应级别

（1）一级响应：针对轻微全局事件，由全局运维人员处理。

（2）二级响应：针对一般全局事件，由全局运维人员及安全团队共同处理。

（3）三级响应：针对严重全局事件，由全局负责人协调相关资源进行应对。

（4）四级响应：针对特别严重全局事件，启动应急响应机制，全面应对。

第三章 应急组织架构与职责

第一节 应急组织架构

1.1.16 概述

应急组织架构是应对突发事件的重要保障，明确了应急工作中的指挥调度、资源整合、协调配合等关键环节。应急组织架构应遵循简洁、高效、协同的原则，保证在突发事件发生时，能够迅速、有序地开展应急工作。

1.1.17 应急组织架构的组成

（1） 领导小组：负责应急工作的总体协调、决策和指挥。领导小组由主要领导担任组长，相关分管领导、部门负责人为成员。

（2） 指挥部：根据应急工作需要，设立指挥部，负责现场应急工作的指挥、协调和调度。指挥部设总指挥、副总指挥，下设若干个工作组。

（3）

工作组：根据应急工作内容，设立相应的工作组，如救援组、物资保障组、信息与宣传组、医疗救护组等。各工作组在指挥部的领导下，负责具体应急任务的实施。

（4） 专家组：负责为应急工作提供技术支持和决策建议。专家组由相关领域的专业人士组成。

1.1.18 应急组织架构的运行机制

（1） 领导小组负责应急工作的总体决策和指挥,对应急工作进行统一领导。

（2） 指挥部负责现场应急工作的具体指挥，协调各工作组、专家组开展工作。

（3） 工作组根据应急任务，制定具体的工作方案，落实应急措施。

（4） 专家组为应急工作提供技术支持和决策建议，保证应急工作的科学、有序进行。

第二节 职责分配

1.1.19 领导小组职责

（1） 制定应急工作总体方案，明确应急工作的目标和任务。

（2） 统一领导应急工作，协调各方力量，保证应急工作的顺利开展。

（3） 审议应急资金、物资等保障措施，保证应急资源充足。

（4） 及时向上级报告应急工作情况，协调外部支援。

1.1.20 指挥部职责

（1） 负责现场应急工作的指挥、协调和调度。

（2） 制定现场应急工作方案，明确各工作组任务。

（3） 审核各工作组工作计划，保证应急工作的有序进行。

（4） 及时掌握应急工作动态，调整应急措施。

1.1.21 工作组职责

（1） 救援组：负责现场救援工作，包括人员搜救、物资调配等。

（2） 物资保障组：负责应急物资的筹集、调配和供应。

（3） 信息与宣传组：负责应急信息的收集、整理、发布和宣传。

（4） 医疗救护组：负责现场医疗救护工作，保证伤员得到及时救治。

1.1.22 专家组职责

（1） 为应急工作提供技术支持和决策建议。

（2） 对应急工作进行评估，提出改进措施。

（3） 参与应急演练，提高应急能力。

第三节 应急队伍组成

1.1.23 概述

应急队伍是应急工作的重要力量，主要由以下几部分组成：

（1） 应急管理队伍：负责应急工作的组织、协调和指挥。

（2） 救援队伍：负责现场救援工作。

（3） 专业技术队伍：负责为应急工作提供技术支持。

（4） 志愿者队伍：参与应急工作，提供人力支持。

1.1.24 应急队伍的组成

（1） 应急管理队伍：主要由部门、企事业单位相关人员组成。

（2） 救援队伍：包括消防、公安、卫生、交通等专业救援队伍。

（3） 专业技术队伍：包括地质、气象、环保、通信等领域的专业技术人员。

（4） 志愿者队伍：由热心公益事业的志愿者组成。

1.1.25 应急队伍的培训与演练

（1） 对应急队伍进行定期培训，提高应急能力。

（2） 组织应急演练，检验应急队伍的协同作战能力。

（3） 加强应急队伍的素质建设，保证在突发事件发生时，能够迅速、高效地投入应急工作。

第四章 预警与监测

第一节 预警机制

预警机制是预防自然灾害和公共安全事件的重要环节。我国高度重视预警机制的建设，不断完善相关制度和技术手段，以提高预警的准确性、及时性和有效性。

1.1.26 预警机制的定义

预警机制是指通过监测、分析、评估和预报各类自然灾害和公共安全事件的可能性，提前发出警报，指导相关部门和公众采取防范措施的系统性工作。

1.1.27 预警机制的分类

根据预警对象的不同，预警机制可分为自然灾害预警、灾难预警、公共卫生事件预警和社会安全事件预警等。

1.1.28 预警机制的工作流程

预警机制的工作流程包括监测、分析、评估、预报、发布和响应等环节。

（1） 监测：对各类自然灾害和公共安全事件进行实时监测，收集相关数据。

（2） 分析：对监测数据进行分析，识别潜在风险。

（3） 评估：对风险进行评估，确定预警级别。

（4） 预报：根据预警级别，发布预警信息。

（5） 发布：通过多种渠道向公众发布预警信息。

（6） 响应：各级和相关部门根据预警信息采取应对措施。

第二节 监测系统

监测系统是预警机制的重要组成部分，主要负责收集、处理和传递各类监测数据，为预警分析提供科学依据。

1.1.29 监测系统的构成

监测系统由监测点、监测设备和数据处理中心三部分组成。

（1） 监测点：布置在灾害易发区域，用于收集各类监测数据。

（2） 监测设备：包括气象、地质、水文等监测设备，用于实时采集数据。

（3） 数据处理中心：对监测数据进行处理、分析和存储。

1.1.30 监测系统的主要功能

（1） 实时监测：对各类自然灾害和公共安全事件进行实时监测，保证数据的准确性。

（2） 数据传输：将监测数据及时传输至数据处理中心。

（3） 数据处理：对监测数据进行处理和分析，为预警分析提供支持。

（4） 数据存储：对监测数据进行存储，便于查询和回顾。

第三节 预警信息发布

预警信息发布是预警机制的关键环节，关系到预警信息的传播和公众的防范措施。

1.1.31 预警信息发布的原则

（1） 及时性：保证预警信息在第一时间发布。

（2） 准确性：保证预警信息的准确性，避免误导公众。

（3） 可靠性：保证预警信息来源可靠，避免传播虚假信息。

（4） 简洁性：预警信息应简洁明了，便于公众理解和接受。

1.1.32 预警信息发布的渠道

（1） 传统媒体：电视、广播、报纸等。

（2） 新媒体：微博、客户端等。

（3） 专业预警系统：气象、地质、水文等部门的预警系统。

（4） 社区通知：通过社区、村庄等基层组织进行通知。

1.1.33 预警信息发布的内容

（1） 预警级别：根据风险程度，分为一级、二级、三级和四级。

（2） 预警对象：明确预警针对的自然灾害或公共安全事件。

（3） 预警时间：发布预警信息的时间。

（4） 预警地点：预警涉及的地区。

（5） 预警措施：建议公众采取的防范措施。

（6） 预警解除：预警结束后，发布预警解除信息。

通过以上预警与监测的介绍，我们可以看到预警和监测在自然灾害和公共安全事件防范中的重要作用。在实际工作中，各级和相关部门应加强预警与监测体系建设，提高预警与监测能力，为我国自然灾害和公共安全事件的防范提供有力保障。

第五章 网络安全事件响应流程

网络技术的飞速发展，网络安全问题日益突出。网络安全事件响应流程是保障网络安全的重要环节，主要包括事件报告、事件评估、事件响应和事件恢复四个阶段。以下是网络安全事件响应流程的具体内容。

第一节 事件报告

事件报告是网络安全事件响应的第一步，其主要任务是发觉、记录和报告网络安全事件。以下是事件报告的具体步骤：

（1） 发觉事件：通过网络安全监测系统、日志分析等手段，发觉网络中的异常行为和安全漏洞。

（2） 记录事件：对发觉的事件进行详细记录，包括事件时间、事件类型、涉及系统、影响范围等信息。