ICS 35.020
CCS L 70
备案号：126546-2025

DB11

北 京 市 地 方 标 准

DB11/T 1599—2025
代替 DB11/T 1599—2018

政务部门信息安全应急预案编制指南

Preparation guidelines for government departments' information security emergency plans

2025 - 09 - 23 发布　　2026 - 01 - 01 实施

北京市市场监督管理局　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替DB 11/T 1599—2018《政务部门信息安全应急预案编制指南》，与DB 11/T 1599—2018相比，除编辑性改动外，主要技术变化如下：

a) 增加了引言，说明了政务部门信息安全范围。
b) 更改了“信息系统”“信息安全事件”“应急预案”“关键信息基础设施”的术语和定义（见3.1、3.2、3.3、3.4,2018年版的3.1、3.2、3.3、3.4）；
c) 更改了应急预案体系架构内容（见4.1，2018年版的4.1）；
d) 更改了事件分类分级（见A.1.4,2018年版的A.1.4）；
e) 增加了事件处置实操（见C.2.2）。

本文件由北京市政务服务和数据管理局提出。

本文件由北京市政务服务和数据管理局归口并组织实施。

本文件起草单位：北京市政务服务和数据管理局、北京市大数据中心、中国科学院信息工程研究所、北京启明星辰信息安全技术有限公司、北京金睛云华科技有限公司。

本文件主要起草人：桑磊、荣晓燕、康振、肖静、周琼、王竹欣、陆畅、刘宝旭、邢文茹、于天杰、于铮、高磊、赵云、王晨阳、商益祥、朱向明、张萌、高子为、于梓丰、张奇、张雯婷、王汉臣、刘仁、王俊锋、温国念。

本文件及其所代替文件的历次版本发布情况为：

——2018年首次发布为DB 11/T 1599—2018；

——本次为第一次修订。

引　言

DB11/T 1599—2018《政务部门信息安全应急预案编制指南》自实施以来，在规范政务部门信息安全应急管理工作中发挥了重要作用。为贯彻落实国家网络安全和数据安全相关法律法规最新要求，需对该标准进行修订完善，以适应网络安全形势变化和技术发展趋势，进一步提升政务部门信息安全应急能力。

本文件所称政务部门信息安全，特指各级行政机关、事业单位等政务部门所建设和运营的全部信息系统（包括政务网站、业务系统、数据库、网络基础设施及相关软硬件设施等）的安全。

政务部门信息安全应急预案编制指南

1 范围

本文件确立了政务部门信息安全应急预案的预案体系、编制流程、综合预案、分项预案和现场处置方案的基本内容。

本文件适用于政务部门信息安全应急预案的编制与修订工作，其他社会组织和单位信息安全应急预案的编制可参照本标准执行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20984—2022 信息安全技术 信息安全风险评估方法

GB/T 20985.1—2017 信息技术 安全技术 信息安全事件管理 第1部分：事件管理原理

GB/T 20986—2023 信息安全技术 网络安全事件分类分级指南

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南

GB/T 24363—2009 信息安全技术 信息安全应急响应计划规范

GB/T 31509 信息安全技术 信息安全风险评估实施指南

GB/T 32926 信息安全技术 政府部门信息技术服务外包信息安全管理规范

GB/T 43697—2024 数据安全技术 数据分类分级规则

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息系统 information system

应用、服务、信息技术资产或其他信息处理组件的组合。

[来源：GB/T 25069—2022,3.696]

3.2

信息安全事件 information security incident

与可能危害组织资产或损害其运行相关的、单个或多个被识别的信息安全事态。

[来源：GB/T 25069—2022,3.684]

3.3

网络安全事件 cybersecurity incident

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者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。

[来源：GB/T 20986—2023,3.4]

3.4

应急预案 emergency plan

一种关于备份、应急响应和灾后恢复的计划。

[来源：GB/T 25069—2022,3.767]

3.5

关键信息基础设施 critical information infrastructure

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、国防科技重要行业和领域，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。

[来源：GB/T 39204—2022,3.1]

4 应急预案体系

4.1 应急预案体系架构

政务部门信息安全应急预案体系由信息安全综合应急预案、信息安全分项应急预案和现场处置方案构成，如图1所示。

图1　政务部门信息安全应急预案体系

4.2　政务部门信息安全综合应急预案

政务部门信息安全综合应急预案是按照上级应急预案要求，应对信息安全事件的综合性应急响应程序和要求。是政务部门信息安全应急预案体系的总纲，是管辖范围内所有分项预案、现场处置方案的综合指导性文件。

政务部门信息安全综合应急预案明确本政务部门信息安全应急工作的基本要求。

4.3 政务部门信息安全分项应急预案

政务部门信息安全分项应急预案是在综合应急预案指导下，对某种类型或某几种类型的信息安全事件、信息系统等预先制定的应急响应预案，可分为网络安全事件应急预案、信息系统应急预案和重点时期信息安全保障预案三类。

政务部门信息安全分项应急预案是综合应急预案的细化，对应急人员、应急流程、保障措施等提出具体要求，对技术要求进行针对性设计。

4.4 现场处置方案

现场处置方案是在综合应急预案和分项应急预案的指导下，针对政务部门信息系统制定的适合现场应急处置的技术性方案或操作指南，具体指导现场工作人员开展相关信息系统或各类信息安全事件应急响应工作。

5 应急预案编制流程

5.1 基本流程

应急预案编制的基本流程为启动应急预案编制、应急体系调查、风险评估、业务影响分析、应急资源和能力评估、应急预案编制、应急预案评审、应急预案发布及备案、应急预案管理与维护。应急预案编制流程如图2所示。

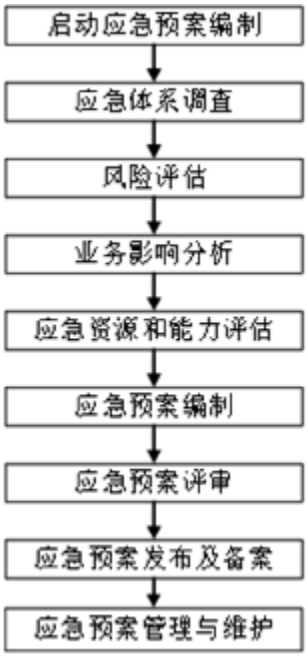


图2 应急预案编制流程

5.2 启动应急预案编制

5.2.1 根据应急保障目标，政务部门成立由应急工作负责人员、相关领域的专家、相关系统使用人员、运维人员、保障人员等专业技术队伍组成的应急预案编制工作组。

5.2.2 制定应急预案编制计划，明确各小组的职责、成员及接口人、预案编制计划时间表及各阶段的具体目标、预案编制工作开展的方式及方法等。

5.2.3 提供开展应急预案编制工作所需的各项资源。

5.3 应急体系调查

5.3.1 收集了解政务部门的组织机制、信息化建设、现有的应急体系等信息；收集已有的应急预案、已发生的应急事件及处置手段和方法等应急相关资料；评估现有应急体系的完备性。

5.3.2 应急体系调查包括但不限于以下方面：

a) 已有的应急预案，包括正在使用及废弃的预案；
b) 应急处置事件总结，包括原因、过程、处置手段及方法；
c) 现有的应急体系情况，包括人力、物力、技术、制度等；
d) 现有应急体系分析、评价。

5.4 风险评估

5.4.1 风险评估是编制应急预案的关键过程，风险评估的结果是确定重点应急对象，划分应急响应优先级的依据，政务部门可结合已有的安全措施和风险评估的结果确定应急响应工作的重点。

5.4.2 风险评估工作主要完成以下工作：

a) 整理信息系统列表；
b) 确定风险评估的目标；
c) 制定风险评估的工作计划，确定工作方式方法；
d) 对资产、威胁和脆弱性进行识别；
e) 甄别现有安全措施；
f) 对残余风险及其可能导致的后果进行评估。

5.5 业务影响分析

业务影响分析围绕信息安全事件展开，分析其发生时的损失及恢复所需的信息系统资源，包括但不限于以下内容：

a) 业务现状分析，明确业务流程、功能、渠道和连续性；
b) 信息系统现状分析，明确功能、拓扑、关联关系、中断影响；
c) 数据现状分析，明确数据资产分布、开展数据分类分级工作；
d) 分析信息安全事件影响；
e) 分析信息系统应急处置优先级及恢复目标的确定。

5.6 应急资源和能力评估

应急资源和能力评估至少包括物质资源、人力资源、技术资源、流程资源、外包服务商评估，具体评估包括但不限于以下内容：

a) 物质资源评估：评估可用于信息安全应急响应工作的各项工具、设备和设施资源，确定在应急响应工作中可投入使用的物质资源，包括资源的类型、功能、作用和投入时间等；
b) 人力资源评估：评估在信息安全应急响应工作中可以投入的人力资源、组织架构、技术支撑等，重点评估各应急岗位投入人员的数量、人员的技术能力和相关经验；
c) 技术资源评估：评估在信息安全应急响应工作中的技术资源，包括采用的安全技术和安全产品，以及安全产品之间的互补性及可能存在的缺陷等；
d) 流程资源评估：评估信息安全应急响应工作中现有的流程资源，包括明确资产和安全风险、应急响应工作的职责分配、现有的应急预案和灾难恢复计划、应急资源的分布情况和其他应急机构的应急支援流程、应急资源的统一调配流程、以往信息安全事件及处理经验等；

e) 外包服务商评估：评估外包服务商在实际操作中的能力和应急响应程度，包括服务商资质、应急响应能力、应急响应物资等，并按照 GB/T 32926 对外包服务商进行安全评估。

5.7 应急预案编制

政务部门结合实际工作，完成应急预案的编制，应急预案需符合以下要求：

a) 符合信息安全相关法律法规要求；
b) 符合国家、行业和地方标准的相关要求；
c) 合规、准确、完整；
d) 方便查阅；
e) 在紧急情况启用时便于实施。

5.8 应急预案评审

5.8.1 应急预案编制完成后，政务部门对应急预案的适用性、科学性、合理性、针对性及规范性进行审核。应急预案的审核分为内部审核和专家评审，审核后及时根据评审意见对应急预案进行修订。

5.8.2 组织政务部门内信息安全应急管理相关的人员对应急预案进行内部审查，审查内容包括但不限于以下方面：

a) 应急组织体系；
b) 应急需求；
c) 预案可操作性；
d) 信息一致性；
e) 有效性；
f) 可控性；
g) 文字内容可读性。

5.8.3 组织信息安全、应急保障、应急管理等领域的专业人员成立的预案评审组对应急预案进行专家审查，评审组专家不少于 5 人，审查包括但不限于以下内容：

a) 应急预案规范性；
b) 应急预案体系的合理性；
c) 应急处置过程风险可控性；
d) 应急处置流程的科学性。

5.9 应急预案发布及备案

评审通过后的应急预案按规定审批并正式发布。应急预案发布后，政务部门组织相关人员进行应急预案培训和演练，明确职责、分工、安全事件处置方法和流程等，并根据相关要求向有关主管部门备案。

5.10 应急预案管理和维护

5.10.1 正式发布的应急预案文档的管理，需符合以下要求：

a) 专人负责管理和维护；
b) 应急预案修订后统一更新；
c) 最新版本的应急预案及时培训并发放给参与应急响应工作的相关人员。

5.10.2 为确保应急预案的有效性，应急预案的维护包括但不限于以下情况：

a) 业务流程的变化、信息系统的变更、组织机构调整、人员的变更等情况需要及时在应急预案文档中反映；

b) 在测试、演练和实际执行中有详细地记录，对测试、演练和执行的效果进行评估，根据评估对应急预案文档进行修订；
c) 每年组织一次评审或修订。

6 综合应急预案基本内容

6.1 基本内容及编制要求

6.1.1 政务部门信息安全综合应急预案包括总则、事件分类分级、组织机构及职责、预警及信息报告、应急响应、恢复重建、保障措施及监督管理等内容，对应急处置的基本原则、应急组织结构、组织职责、应急响应的总体思路及应急救援活动的组织协调等提出具体要求。

6.1.2 综合应急预案根据有关应急预案体系的要求，全面考虑，科学划分事件等级，覆盖应急工作全过程。政务部门信息安全综合应急预案编制示例见附录A。

6.2 总则

总则包括应急预案的编制目的、编制依据、工作原则、适用范围、应急预案体系及其他内容，具体要求如下：

a) 编制目的：介绍制定信息安全应急预案的原因和制定应急预案的目标；
b) 编制依据：相关的法律法规、规章、标准和规范性文件以及应急预案等；
c) 工作原则：应急工作的原则宜简明扼要，明确具体；
d) 适用范围：应急预案的作用范围；
e) 应急预案体系：应急预案体系文件的构成情况，可用框图、组织结构图等形式表达；
f) 其他：其他需要说明事项。

6.3 信息安全事件分类分级

6.3.1 政务部门可结合工作实际，根据信息安全事件的起因、表现和结果等情况，对应急预案中的信息安全事件分类进行适当合并或细化。

6.3.2 政务部门可结合工作实际，根据信息系统的重要程度、系统损失程度和社会影响程度等情况，对应急预案中的信息安全事件分级的等级进行适当调整和细化。

6.4 角色及职责

角色及职责符合GB/T 24363要求。

6.5 预警及信息报送

6.5.1 政务部门加强信息安全监测、预防和预警工作，信息安全事件的监测方式方法、预防和预警工作符合 GB/T 24363 的要求。

6.5.2 政务部门建立完善的信息安全事件报告和通报制度，明确事件报告流程与通报对象，以保障事件能够得到及时、有效地响应。

6.6 应急响应

应急响应包括基本响应、分级响应、响应程序、处置措施、应急结束要求、应急总结等。基本要求如下：

a) 基本响应：规定当发生信息安全事件后需首先开展的工作，包括紧急措施（先期处置）、事件识别、信息上报和情况通报等；
b) 分级响应：规定根据信息安全事件危害程度、影响范围和对事态控制的能力，按照信息安全事件的分级启动应急响应；
c) 响应程序：规定根据信息安全事件级别和发展态势，启动应急指挥机制、调配应急资源、应急救援及扩大应急等响应程序；
d) 处置措施：规定根据信息安全事件风险等级、信息安全事件危害程度和影响范围制定的应急处置措施原则和具体要求；
e) 应急结束：规定现场应急响应结束的基本条件和要求；
f) 应急总结：规定收集、整理和记录信息安全事件过程的各种相关信息。对于需要上报的事件宜规定准备的材料和上报部门。

6.7 恢复重建

6.7.1 应急响应工作结束后，对信息安全事件造成的损失和影响以及恢复重建能力进行分析评估，根据评估结果制定相应的系统加固或重建方案，通过版本升级、漏洞修复、修改安全配置和增加安全机制等方法对系统的安全性进行加强，或对系统进行重建。

6.7.2 总结应急工作，具体工作包括但不限于以下内容：

a) 分析和总结事件发生的原因；
b) 分析和总结事件的现象；
c) 评估系统的损坏程度；
d) 评估数据安全影响程度；
e) 评估事件导致的损失；
f) 分析和总结应急处置记录；
g) 评审应急预案的效果和效率，提出改进建议；
h) 评审应急响应措施的效果和效率，提出改进建议；
i) 对相关单位和人员的表彰和惩罚。

6.8 保障措施

6.8.1 保障措施包括应急队伍保障、应急通信保障、专业应急设备保障及重要数据备份保障等内容，保障措施基本内容如下：

a) 应急队伍保障：应急响应的人力资源，包括应急专家、应急队伍和外部合作队伍等；
b) 应急装备保障：信息网络硬件、软件的清单和管理责任人及其联系方式等内容，明确应急通信保障措施和重要数据备份机制等；
c) 其他保障：根据应急工作需求确定其他相关保障措施，包括但不限于经费保障、交通运输保障、治安保障、技术保障及后勤保障。
d) 监督管理部分基本要求如下：
    1) 应急预案培训：明确对人员开展应急预案培训的计划、方式和要求，相关人员了解应急预案内容，熟悉应急职责、应急程序和处置方案；
    2) 应急预案演练：规定应急预案演练的形式、范围、频次、内容、演练评估和总结等；
    3) 应急预案修订：规定应急预案修订的基本要求和修订周期，并规定应急预案评审周期；
    4) 应急预案备案：规定应急预案的报备部门及备案要求；
    5) 应急预案实施：规定应急预案发布与实施的具体时间以及负责制定与解释的部门；
    6) 附件。

6.8.2 政务部门信息安全综合应急预案的附件包括但不限于以下内容：

a) 应急处置流程图：根据信息安全事件级别与类型，使用图表形式展现各处置阶段的参与部门与处置权限，包括完整的应急响应过程中的各个环节；
b) 有关应急部门、机构或人员的联系方式：编制至少包括小组名称、姓名、职位、工作电话、手机及电子邮箱等内容的联系人表，当发生变化时及时进行更新。信息系统较多时可采用京办建群等方式进行沟通；
c) 应急信息接报、处理、上报等规范化格式文本：信息安全事件报告文本内容包括单位名称、报告人、联系电话、通讯地址、电子邮件、事件报告时间、信息系统名称、主要用途及信息安全事件的简要描述等信息；
d) 有关协议或备忘录：包括与相关应急救援部门签订的应急救援协议或备忘录。

7 分项应急预案基本内容

7.1 基本内容及编制要求

政务部门在制定信息安全分项预案时，针对政务部门的信息系统、网络安全事件的特点，对应急组织、流程和技术保障措施具体设计。政务部门信息安全事件应急预案编制示例参考附录B。

7.2 总则

总则部分基本内容如下：

a) 编制目的：制定分项应急预案的原因和制定预案的目标；
b) 工作原则：分项应急工作的原则宜简明扼要，明确具体；
c) 适用范围：分项预案的作用范围，说明解决哪些问题，适用于哪些系统及对系统进行描述；
d) 其他：根据需求说明其他事项。

7.3 组织机构及职责

应急机构涉及相关的单位和人员包括但不限于：系统责任单位、系统业务人员、基础运维人员、安全运维人员、系统建设单位及各类设备设施的生产商或代理商以及其他必要的供应链厂商等。根据政务部门的信息系统、信息安全事件或者重点时期保障中的安全风险，明确应急组织形式、构成单位或人员；明确各机构的工作任务及主要负责人的职责。

7.4 风险分析与预案启动

对信息系统或重点时期保障期间发生某种具体或特定类型信息安全事件的可能性进行分析，预判信息安全事件发生的风险、严重程度、影响范围等，结合信息系统的重要程度或重点时期保障级别，启动相应等级的应急预案。包括但不限于以下内容：

a) 可能发生的信息安全事件类型；
b) 信息安全事件可能发生的时间；
c) 信息安全事件发生前可能出现的征兆；
d) 信息安全事件可能引发的次生、衍生信息安全事件；
e) 信息安全事件对关键信息基础设施业务运行产生的危害程度及影响范围。

7.5 应急响应流程

根据信息安全事件响应的级别，明确应急响应的报告程序、报告内容、报告方式和责任人等，对信息安全事件接报和记录、应急指挥机构启动、资源调配、应急处置、扩大应急等响应程序提出具体要求。

7.6 应急处置措施

信息安全事件应急处置措施主要分为：应急准备、分析确认、抑制根除、恢复运行。针对信息系统可能发生的信息安全事件的风险、信息安全事件危害程度和影响范围，制定相应的应急处置措施，明确处置原则和具体要求。

7.7 保障措施

明确分项预案各类应急响应的人力资源、技术资源及后勤保障资源等，包括应急队伍、应急设备保障、应急保障经费、跨部门协作保障等。

7.8 宣传、培训和演练

对分项预案的宣传教育和信息安全相关知识培训等工作提出要求，包括对信息安全工作人员定期培训，使其熟悉信息安全相关知识，掌握故障排除步骤及实操技能；落实岗位应急职责，熟悉应急预案体系、应急响应程序和处置方案等内容；定期开展信息安全应急演练，检验信息安全工作人员的业务技能，同时验证预案的有效性。

7.9 附件

附件内容包括但不限于以下方面：

a) 应急物资装备的名录或清单：包括应急预案涉及的主要物资和装备名称、型号、性能、数量、存放地点、运输和使用条件、管理责任人和联系电话等；
b) 关键的路线标识、应急工具清单和图纸：包括详细的网络拓扑图，应急专用工具清单、位置及保管人，应急专用工具操作指导书，机房相关平面布置图纸等。

8 现场处置方案基本内容

8.1 组织各类信息安全的专业组织和技术专家、部门运维、使用人员等共同参与现场处置方案制定，对应急处置中的各个方面提出具体细致的要求，确保其针对性和指导性。现场处置方案可参考附录 C。

8.2 针对发生的信息安全事件，从技术操作的角度加以规范，明确处置原则和具体处置步骤，细化应急处置手册。现场处置方案包括但不限于：

a) 恶意程序事件-计算机病毒事件应急处置手册；
b) 网络攻击事件－网络扫描探测事件应急处置手册；
c) 数据安全事件－数据篡改事件应急处置手册；
d) 信息内容安全事件－反动宣传事件应急处置手册；
e) 设备设施故障事件－技术故障事件应急处置手册；
f) 违规操作事件－权限滥用事件应急处置手册；
g) 安全隐患事件－网络漏洞事件应急处置手册；
h) 异常行为事件－访问异常事件应急处置手册；
i) 不可抗力事件-自然灾害事件应急处置手册；
j) 其他事件应急处置手册。

附 录 A
（资料性）
北京市某局信息安全事件综合应急预案示例

A.1 总则

A.1.1 编制目的

为完善北京市某局应急预案体系，健全信息安全应急工作机制，提高应对信息安全突发事件的能力，预防信息安全事件的发生，降低造成的损失和危害，特编制此预案。

A.1.2 编制依据

《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》《网络数据安全管理条例》《关键信息基础设施安全保护条例》《国家网络安全事件报告管理办法》《国家突发公共事件总体应急预案》《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》等法律、法规、规章等。

A.1.3 工作原则

坚持统一指挥、密切协同、快速反应、科学处置；坚持以预防为主，预防与应急相结合；坚持谁主管谁负责、谁运营谁负责等原则。充分发挥各方面技术力量，共同做好某局信息安全事件的预防与应对工作。

A.1.4 事件分类分级

A.1.4.1 事件分类

综合考虑信息安全事件的起因、威胁、攻击方式、损害后果等因素，对信息安全事件进行分类，分为恶意程序事件、网络攻击事件、数据安全事件、信息内容安全事件、设备设施故障事件、违规操作事件、安全隐患事件、异常行为事件、不可抗力事件和其他事件等10类，每类之下再分若干子类。

（1）恶意程序事件包括计算机病毒事件、网络蠕虫事件、特洛伊木马事件、僵尸网络事件、恶意代码内嵌网页事件、恶意代码宿主站点事件、勒索软件事件、挖矿病毒事件、混合攻击程序事件和其他恶意程序事件等10个子类；

（2）网络攻击事件包括网络扫描探测事件、网络钓鱼事件、漏洞利用事件、后门利用事件、后门植入事件、凭据攻击事件、信号干扰事件、拒绝服务事件、网页篡改事件、暗链植入事件、域名劫持事件、域名转嫁事件、DNS污染事件、WAN劫持事件、流量劫持事件、BGP劫持攻击事件、广播欺诈事件、失陷主机事件、供应链攻击事件、APT事件和其他网络攻击事件等21个子类；

（3）数据安全事件包括数据篡改事件、数据假冒事件、数据泄露事件、社会工程事件、数据窃取事件、数据拦截事件、位置检测事件、数据投毒事件、数据滥用事件、隐私侵犯事件、数据损失事件和其他数据安全事件等12个子类；

（4）信息内容安全事件包括反动宣传事件、暴恐宣扬事件、色情传播事件、虚假信息传播事件、权益侵害事件、信息滥发事件、网络欺诈事件和其他信息内容安全事件等8个子类；

（5）设备设施故障事件包括技术故障事件、配套设施故障事件、物理损害事件、辐射干扰事件和其他设备设施故障事件等5个子类；

（6）违规操作事件包括权限滥用事件、权限伪造事件、行为抵赖事件、故意违规操作事件、误操作事件、人员可用性破坏事件、资源未授权使用事件、版权违反事件和其他违规操作事件等9个子类；

（7）安全隐患事件包括网络漏洞事件、网络配置合规缺陷事件、其他安全隐患事件等3个子类；

（8）异常行为事件包括访问异常事件、流量异常事件和其他异常行为事件等3个子类；

（9）不可抗力事件包括自然灾害事件、事故灾难事件、公共卫生事件，社会安全事件和其他不可抗力事件等5个子类；

（10）其他事件指未归为上述分类的信息安全事件。

A.1.4.2 事件分级

按照电子政务实际建设需要，结合信息安全事件影响程度和响应级别，将信息安全事件分为特别重大（一级）、重大（二级）、较大（三级）、一般（四级）、较小（自管级）事件。

涉及特别重大（一级）、重大（二级）的按照《北京市网络安全事件应急预案》要求执行，由市网信部门负责事件的应急处置工作，某局信息安全相关部门配合完成信息安全事件的现场应急处置工作；某局负责较大（三级）、一般（四级）、较小（自管级）信息安全事件的处置工作。必要时，可由市重大网络与信息安全事件应急指挥部指导开展应急处置工作。

特别重大（一级）、重大（二级）信息安全事件的分级标准参照《国家网络安全事件报告管理办法》《北京市网络安全事件应急预案》等文件执行。

（一）较大（三级）信息安全事件

较大（三级）信息安全事件是未达到重大（二级）信息安全事件，但对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的信息安全事件，包括。

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、造成较严重影响的信息安全事件。

通常情况下，满足下列条件之一的，可判别为较大信息安全事件：

1.党政机关、事业单位门户网站，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（含）以上或主要功能中断运行30分钟以上。

3.影响一个或多个区30%（含）以上人口，或者10万人（含）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（含）以上公民个人信息或10万人（含）以上公民敏感个人信息，对国家安全和社会稳定构成较严重威胁的事件。

6.党政机关、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（含）以上，或在其他页面出现并持续2小时（含）以上。

（2）通过社交平台转发1000次（含）以上。

（3）浏览或点击次数1万（含）以上。

（4）市网信部门、公安机关认定为是“较大范围传播”的。

7.造成500万元（含）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、造成较严重影响的信息安全事件。

（二）一般（四级）信息安全事件

一般（四级）信息安全事件是未达到较大（三级）信息安全事件，但对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的事件。

通常情况下，满足下列条件之一的，可判别为一般信息安全事件：

1.党政机关、事业单位门户网站，重点新闻网站因攻击、故障，导致不能访问。

2.关键信息基础设施主要功能中断运行或整体中断运行。

3.重要信息系统因攻击、故障中断，业务受到影响，影响居民用水、用电、用气、用油、取暖、交通出行、就医、购物等工作、生活。

4.泄露公民个人信息，造成一般社会危害。

5.党政机关、事业单位门户网站，重点新闻网站，网络平台等被恶意攻击篡改，导致违法有害信息传播。

6.党政机关、事业单位门户网站，重点新闻网站，网络平台等被恶意入侵，被攻击者植入木马、暗链、后门等，存在严重的安全隐患。

7.其他导致较小的业务损失，造成一般社会危害的信息安全事件。

（三）较小（自管级）信息安全事件是指未达到一般信息安全（四级）事件，未造成社会危害的信息安全事件，包括：

1.等保一级、二级信息系统因攻击、故障中断，未造成社会危害。

2.数据遭到篡改、破坏、泄露或者非法获取、非法利用，但未达到一般信息安全事件（四级）条件。

3.其他由于各种原因导致的未达到一般信息安全事件（四级）条件的系统中断、服务中断、设备故障等信息安全事件。

A.1.5 适用范围

本预案适用于北京市某局信息安全事件的预防和处置工作。

某局信息系统相关信息详见附件。

A.2 组织机构与职责

北京市某局信息安全事件应急组织机构，由信息安全领导小组、信息安全工作小组和信息安全实施小组、信息安全运行小组、信息安全专家组组成，负责信息安全事件的预防和应对工作。相关角色分配如下：

A.2.1 信息安全领导小组

组　长：局长

组　员：XXX

负责协调并推动政务信息安全保障体系的建立与完善；指导和监督各部门重要信息系统与基础设施的安全保障工作；组织信息安全培训；根据法律法规和最新趋势推动信息安全政策的更新；协调处理政务领域的重大信息安全事件，确保政务工作的连续性和信息安全管理体系的有效性。

A.2.2 信息安全工作小组

组　长：信息安全主管部门主要领导

组　员：XXX

负责信息安全基础设施的规划和管理工作；负责组织开展事件监测和应急处置工作；负责组织信息安全应急预案的制定工作，负责指导开展应急演练；负责政务信息系统的风险评估与测试的监督、检查、指导工作；负责安全管理人员的培训；提供安全管理和安全技术方案的咨询。

A.2.3 信息安全实施小组

组　长：相关部门主要领导

组　员：XXX

负责实施具体的应急处置工作，包括信息安全事件的应急响应，制定具体处置方案，调查事件原因，分析事件影响范围等。

A.2.4 信息安全运行小组

组　长：相关部门主要领导

组　员：XXX

负责信息系统的日常运维，包括备份中心的日常管理、安全监测系统的运行和维护，开展应急预案的编制、测试、培训和演练等。

A.2.5 信息安全专家组

负责提供紧急情况下的应急技术方案和技术支援，对重大信息安全事件进行评估，提出启动应急响应程序的建议，分析信息安全事件的原因及造成的危害，并为整个应急响应过程提供必要的技术支持。

A.3 监测预警

A.3.1 监测

北京市某局在落实国家网络安全等级保护工作制度基础上，重点做好信息安全事件的风险评估和监测预警工作。

A.3.1.1 风险评估

北京市某局信息安全工作小组负责本局政务信息系统的风险评估与控制工作的监督、检查和指导。定期组织开展局内信息安全技术检查与自查，了解和掌握分管领域内信息系统的风险状况。根据需要，建立并维护风险源管理系统，以强化风险管理措施，进而提升信息系统安全防护能力。

A.3.1.2 安全监测

北京市某局信息安全运行小组负责信息安全监测系统运营、维护和管理工作，根据需要对局内信息系统、网站域名及流量数据进行持续性安全监测，定期对设备告警信息及日志进行分析，及时发现并准确识别网站及信息系统中的潜在安全隐患。

北京市某局信息安全运行小组负责对监测信息进行研判，认为需要立即采取预防措施的，应及时通知有关部门或单位立即采取针对性的措施，迅速修复安全漏洞，有效遏制并预防信息安全事件的发生；对可能发生较大及以上信息安全事件的信息，应及时上报信息安全领导小组，并向市网信安全应急办公室报告，涉及政务信息系统的，同时向市政务服务和数据管理局报告。

A.3.2 预警响应

预警级别分为一级、二级、三级、四级，分别用红色、橙色、黄色、蓝色表示，分别对应可能发生特别重大、重大、较大、一般信息安全事件。

北京市某局可以根据监测研判情况在本部门发布黄色以下预警。

当收到本部门或市网信等部门发布的信息安全预警信息，或本部门因某项重大活动而需要进行信息安全保障时，信息安全工作小组应按照发布的预警和保障级别，启动并执行相应的应急预案。组织与部署所属技术力量和应急队伍进行响应并进入应急状态，以有效应对潜在的信息安全威胁，确保信息安全得到充分保障。

A.4 应急响应

A.4.1 事件发现和汇报

信息安全运行小组根据各自职责分工，及时收集、分析、汇总信息系统安全运行情况，一旦发生安全事件及时通知信息安全工作小组。

对于暂时无法判明等级的信息安全事件，立即将事件简要情况及联系人通过电话、京办等途径上报信息安全领导小组。

A.4.2 先期处置

信息安全事件发生后应做好如下先期处置工作：

（1）控制事态发展，防控蔓延。相关人员根据需要及时采取断网（拔网线）等技术措施及时控制事态发展，最大限度地降低事件危害；

（2）信息及时上报。在先期处置的同时要按照预案要求，及时上报；

（3）原因分析与影响评估。尽快分析事件发生原因，并结合信息系统运行和承载业务的特点，初步评估事件的影响范围、危害程度和可能波及的领域，据此提出针对性的应对措施和建议；

（4）详细记录与证据保存。在先期处置过程中，应保留安全日志信息、设备告警信息、路由配置信息、数据包信息等相关证据。通过采取手工记录、屏幕截图、文件备份和影像设备记录等技术手段，对事件发生、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，为后续事件溯源、调查和处置提供客观证据；

（5）技术支持与态势研判。信息安全工作小组在接报事件信息后，要及时介入并动态掌握事件的发展情况，评估事件的影响和可能波及的范围，研判事件的发展态势，根据需要提供相应的技术支持。

A.4.3 基本响应

信息安全事件发生后，在先期处置基础上，根据事件级别启动信息安全事件应急预案，及时掌握事件的发展动态，统筹并调配应急资源。必要时配合市网信部门组建现场指挥部，以高效、有序地应对信息安全突发事件的应急处置工作。

A.4.4 分级响应

信息安全事件应急响应由高到低分为一级、二级、三级、四级、自管级，分别对应特别重大、重大、较大、一般和自管级信息安全事件。

A.4.4.1 一级、二级响应

对于特别重大、重大信息安全事件的应急响应按照《北京市网络安全事件应急预案》要求执行一级、二级响应，并配合市网信部门完成信息安全突发事件的现场应急处置工作。

A.4.4.2 三级、四级响应

对于一般和较大信息安全事件，由信息安全领导小组启动三级、四级响应，统一指挥、协调并组织应急处置工作。部门内各成员单位做好事件处置过程中的配合和协助工作。若涉及跨区、跨部门的信息安全事件，按照《北京市网络安全事件应急预案》要求执行，配合市网信部门完成信息安全突发事件的现场应急处置工作。

（1）启动指挥体系

信息安全组织机构进入应急状态，各成员保持24小时联络畅通，信息安全领导小组统筹协调事件应急处置工作，确保各项措施得到有效地执行。

（2）掌握事件动态

①跟踪事态发展。信息安全工作小组需密切关注事态的发展变化，及时将事态发展变化情况和处置进展情况报信息安全领导小组；

②检查影响范围。信息安全工作小组及时了解主管范围内的其他信息系统是否受到事件的波及或影响，组织相关人员对事态进行研究，并根据需要对受到影响的系统进行核查；

③及时通报情况。信息安全工作小组负责汇总上述有关情况，报信息安全领导小组及市网信部门，涉及政务信息系统的，同时报市政务服务和数据管理局。

（3）处置实施

①控制事态防止蔓延。在信息安全领导小组的指挥下，信息安全实施小组应及时采取技术措施，阻止事件蔓延，同时督促、指导相关运行单位有针对性地加强防范，确保事态得到有效控制。信息安全运行小组加强对局内信息系统、网站域名及流量数据安全监测；

②消除安全隐患。信息安全实施小组尽快分析事件发生原因，并根据原因有针对性地采取恢复措施，消除安全隐患，恢复受破坏系统正常运行。必要时，可请求市级信息安全技术支撑机构派遣应急队伍支援；

③及时开展调查取证。信息安全工作小组组织开展事件调查和责任评估工作，并将调查评估结果报信息安全领导小组；

④信息发布。信息安全领导小组根据事件应急的实际情况，组织形成各阶段工作简报，根据需要报告有关部门。

A.4.4.3 自管级响应

信息安全实施小组启动自管级响应，按照相关预案有序进行应急处置，指挥并协调所属技术力量开展事件处置工作；信息安全实施小组负责将事件信息、处置进展情况及时向信息安全工作小组报告。

A.4.4.4 响应升级

在事件处置过程中，若事态发展表明事件影响未得到有效控制，或当前的人力物力资源不能够满足应急处置的需要且超出本单位应急处置能力时，应及时提升响应等级。

A.4.5 应急结束

根据应急处置进展情况，信息安全工作小组会同信息安全专家组进行综合评估，在确认信息安全事件得到抑制、信息系统业务恢复正常，其衍生危害已经根除，安全隐患已在可控范围内的前提下，提出应急结束建议，并报相关部门批准。

三级、四级响应结束：由信息安全工作小组报信息安全领导小组审核后，由信息安全领导小组决定。

自管级响应结束：由信息安全工作小组自行决定。

A.5 恢复重建

A.5.1 系统重建

恢复重建工作遵循“谁主管谁负责，谁运行谁负责”的原则。如有需要，可以由信息安全工作小组负责组织制定恢复、整改或重建方案，报信息安全领导小组审核批准实施。

A.5.2 事件总结

信息安全事件应急处置工作结束后，信息安全工作小组适时组织信息安全实施小组和信息安全运行小组等相关部门针对信息安全事件进行复盘和责任调查。对突发事件应急处置过程的处置效率和应急响应流程进行全面评估，并在20天内将评估报告报送信息安全领导小组。

信息安全工作小组组织编写处置报告，总结经验教训，建立事件案例库，并据此提出改进工作的要求和意见。

A.6 保障措施

A.6.1 技术支撑队伍

由信息安全工作小组负责遴选一批经由国家有关部门资质认可的，管理规范且服务能力较强的企事业单位将其纳入信息安全应急支援队伍体系。通过财政经费采购信息安全技术支持与应急服务，加强与市级信息安全保障机构的联系，确保必要时能够有效调动机关团体、企事业单位等保障力量，进行技术支援。

A.6.2 经费保障

信息安全相关部门将信息安全事件预防和应急工作列入年度经费预算。

A.7 宣传、培训和演练

A.7.1 宣传教育

信息安全工作小组每年组织有关部门，通过信息安全通知公告、宣传展板制作、法律法规教育等形式开展宣传教育工作，普及局内人员的信息安全知识，提升安全意识。

A.7.2 培训

信息安全工作小组负责统筹协调各有关单位，定期开展涵盖信息安全法规标准解读、风险评估方法、事件分析处置技巧以及容灾备份策略在内的专业技术培训活动。通过这些培训，旨在确保信息安全工作人员能够全面、深入地掌握并熟练运用相关技能，以有效提升信息安全防护与应急响应能力。

A.7.3 演练

信息安全工作小组负责指导每年不定期策划并执行信息安全应急演练，通过模拟真实事件场景，强化实战处置技能，同时全面检验并优化现有应急预案，确保预案的有效性与可操作性。

A.8 预案管理

A.8.1 预案制定与解释

本预案由北京市某局信息安全工作小组制定并负责解释。

A.8.2 预案审核

本预案由北京市某局信息安全领导小组组织审核。

A.8.3 预案修订

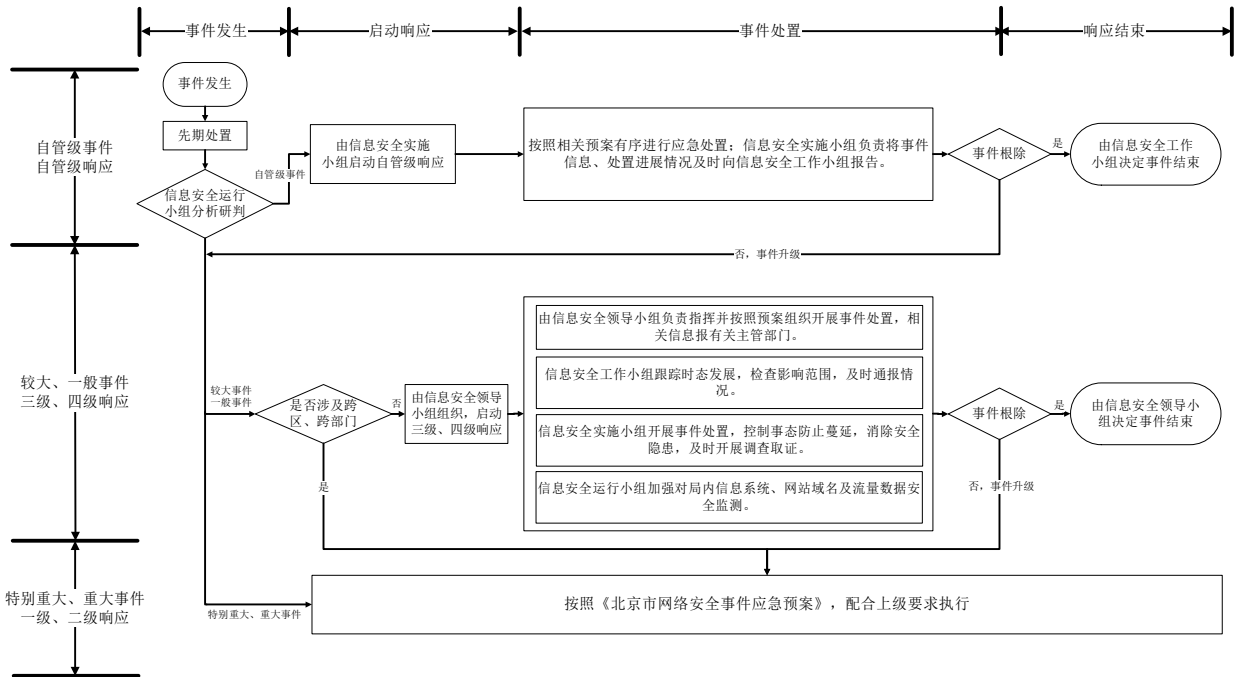
本预案原则上每年评估一次，根据实际情况适时修订。

A.8.4 预案实施

本预案自发布之日起正式实施。

A.9 附件

A.9.1 信息安全领导小组名单
A.9.2 信息安全工作小组名单
A.9.3 信息安全实施小组名单
A.9.4 信息安全运行小组名单
A.9.5 信息系统及责任人列表
A.9.6 信息安全应急事件通报表
A.9.7 信息系统及IP列表、资产列表
A.9.8 信息安全事件应急处置流程图



图A.1 信息安全事件应急处置流程图

附 录 B
（资料性）
北京市某局网络攻击事件－网页篡改事件应急预案示例

B.1 总则

B.1.1 编制目的

为建立健全北京市某局信息安全应急机制，规范网页篡改事件中各单位工作责任，提高应对网页篡改事件的应急处理能力，最大程度地降低网页篡改事件造成的损害，保障某局各项业务的正常运行，特制定本预案。

B.1.2 编制依据

《北京市网络安全事件应急预案》
《北京市某局信息安全事件综合应急预案》

B.1.3 适用范围

本预案针对北京市某局发生的网页篡改事件。

B.2 应急组织机构及职责

B.2.1 安全运行维护单位

在信息安全工作小组（该小组见综合预案）指导下，负责监测信息安全事件，实施网络攻击信息系统应急处理方案，并在安全服务厂商、信息系统网络维护单位和各部门单位的协助下，实施应急处理工作，尽快恢复信息系统的正常运转。

B.2.2 安全服务机构

在信息安全工作小组的指导下，对网络攻击事件造成的影响进行分析，给出处置解决方案，并负责网页篡改事件应急响应处理，协助安全运行维护单位解决安全维护工作。

B.2.3 信息系统运行维护单位

在信息安全工作小组协调下，协助安全运行维护单位进行网页篡改事件的应急处置工作，提供必要的详细网络配置文档、服务器配置文档、业务数据配置清单。对被篡改的服务器数据进行数据备份，处置完成后对系统业务进行恢复。

B.2.4 其他部门单位

其他部门单位负责配合安全运行维护单位和信息系统运行维护单位进行网页篡改事件的应急处理工作，提供网络、系统配置文档和重要数据清单。

B.3 事件分类分级

B.3.1 事件分类

按照网络攻击事件的表现形式，本处置预案将网页篡改事件大致分为如下三类：

域名劫持事件：网站内容并非真正遭到篡改，而是域名指向被修改，会遭遇内容异常、页面跳转或访问受限等问题，进而可能遭受钓鱼攻击、信息泄露等安全风险；

图片/文字被篡改事件：网站页面的图片或者文字被篡改，用户通过浏览器可以看到被篡改的内容，进而可能受到误导、欺诈或传播虚假信息等安全风险；

挂马/暗链事件：网站被篡改的内容用户通过浏览器访问时不可见，但植入的恶意代码会在用户不知情的情况下被执行，可能导致用户设备感染病毒或遭受其他形式的攻击。

B.3.2 事件分级

引用《北京市某局信息安全事件综合应急预案》分级标准。

B.3.3 应急启动

发生突发事件后，第一时间向信息安全工作小组报告。安全运行维护单位根据突发事件的分类分级标准，分析事件的影响程度并预判事件级别，进行先期处置。

如确定为四级及以上事件，报信息安全领导小组，并按照综合预案处置。

如为自管级事件，启用本预案响应流程。

B.4 应急响应

网页篡改是针对网站的较常见攻击方法，一旦确认发生，应立即通知信息安全工作小组，针对网页篡改事件展开应急处置工作，对于超出应急响应处理能力的工作，可以请求市信息安全应急队伍提供相应的技术支持。

网页篡改事件应急响应流程主要分为：事件通报、应急准备、分析确认、抑制根除、恢复运行和分析总结六个阶段。

B.4.1 事件通报

当值班人员发现并确认网页篡改事件后，应立即采取紧急措施，对涉事服务器进行物理隔离（断网）（对于接入云服务的系统，应迅速与云服务商建立联动机制，执行相应的隔离措施），并将事件的基本情况及时上报至信息安全工作小组。为减轻可能产生的社会影响，物理隔离（断网）操作完成后，应立即在网站上发布系统维护公告页面，告知用户当前系统状态及预计恢复时间。

信息安全工作小组接到报告后，立即组织开展应急响应，判断事件影响范围，并视情况通报市网信部门，涉及政务信息系统的，同时报市政务服务和数据管理局。

B.4.2 应急准备

通知安全运行维护单位迅速赶赴现场开展事件处置，如发现不能处置此次事件，应及时请求市信息安全应急队伍协助进行处置。

准备事件分析所需软件和硬件，软件主要有日志分析工具，木马扫描工具，账号、进程、端口查看工具，挂马、暗链检查工具；硬件主要有应急笔记本和移动硬盘，笔记本要安装好上述软件。

B.4.3 分析确认

事发后应尽最大可能收集事件相关信息，鉴别事件性质，追溯事件来源，并综合评估事件的影响范围与潜在损害。事件分析过程包括但不限于以下几个方面：

（1）分析网站访问日志，追踪攻击者的完整攻击链，包括其进行的扫描活动、所利用的漏洞类型，以及实施篡改的具体时间点；

（2）利用专业安全工具，对网站程序代码进行深度扫描，定位并识别出攻击者可能植入的木马、后门或其他恶意代码；

（3）利用工具查看服务器账户、进程、服务及启动项等信息，看攻击者是否留有其他后门；

（4）利用检测工具对网站进行全方位扫描，及时发现并清除可能存在的挂马链接或暗藏的攻击代码。

B.4.4 抑制根除

（1）清除页面中的挂马、暗链并修复相关漏洞；

（2）更新WEB服务器操作系统用户账号密码和WEB服务应用程序用户账号密码；

（3）部署防篡改软件或防篡改设备，以达到防篡改目的；

（4）妥善保存日志信息（单独服务器存储或者定期转储），强化安全防范措施。

B.4.5 恢复运行

抑制根除完成后，恢复被篡改的网页，对网站服务器进行安全加固，并进行全面的安全检测。消除隐患后将网站重新投入使用，在上线后一定时期内严密监控信息系统，一旦发现异常及时处置。

B.4.6 分析总结

在完成对整个信息安全事件的抑制、根除、恢复与加固处理后，汇总事件概述、处理流程、结果分析、经验教训及建议措施，形成详细报告上报给信息安全领导小组。若事件涉及应急支援的，则还需将相关情况上报至市网信部门，涉及政务信息系统的，同时向市政务服务和数据管理局报告，以确保信息的全面透明及跨部门协作的有效性。

B.5 恢复重建

B.5.1 跟踪后续处理

应急响应结束后，制定相应的系统加固方案，尽快恢复系统正常工作，安全运行维护单位加强安全监测，跟踪后续处理情况。

B.5.2 情况汇报和经验总结

应急处理结束后，信息安全工作小组组织对事件处理情况、经验教训进行总结，对达到四级及以上事件级别的，需向信息安全领导小组汇报。

B.6 宣传、培训和演练

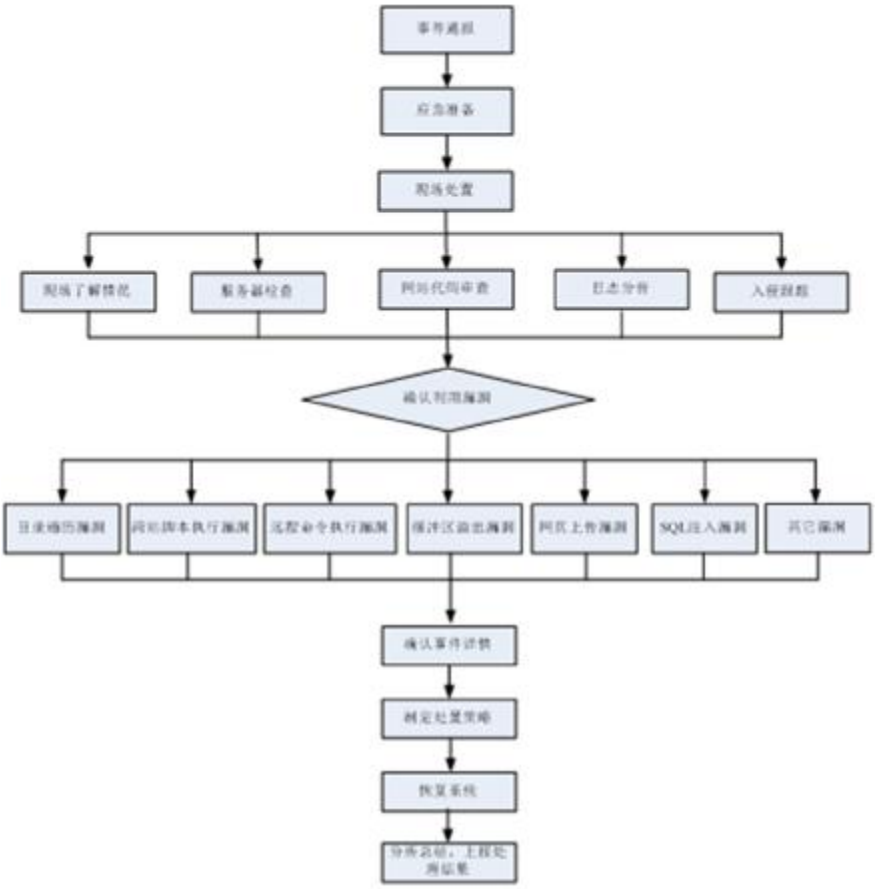
应加强对系统运维人员及其他相关人员的宣传教育工作，定期对有关人员进行技术培训，组织针对网页篡改事件的应急演练，确保各应急预案的有效实施，不断提高应急处理的能力。

B.7 预案的管理与更新

本预案的管理与更新职责由信息安全工作小组承担，并坚持实施周期性的评审机制。随着技术的不断进步、系统结构的变更以及安全策略的更新，预案应及时进行相应的修订，修订后的预案经评审通过后发布生效。

B.8 附件

B.8.1 应急响应流程图



图B.1 应急响应流程图

B.8.2 应急组织机构成员名单

B.8.3 信息系统及运维机构人员和联系方式

B.8.4 网络拓扑图、设备、IP地址、物理位置等信息系统相关信息

B.8.5 网页篡改事件应急处置手册

附 录 C
（资料性）
北京市某局网络攻击事件－网页篡改事件应急处置手册

C.1 应急准备阶段

C.1.1 保障对象识别

（1）网站基本情况：网站域名、IP地址、责任单位、软件开发单位、硬件厂商、日常运维和安全运维单位等；

（2）网站开发运行环境：网站使用的开发平台和编程语言、网站服务器操作系统类型及版本、WEB服务器软件类型及版本、后台数据库软件类型及版本、内容管理系统（CMS）相关情况等；

（3）网站外围支撑情况：信息安全域划分情况、防火墙访问控制策略设置、域名解析系统的部署和配置情况、安全监测和审计措施部署情况等；

（4）网站保障目标：若保障网站存在多个信息系统，应划分优先级，以确保重要系统能够优先获得足够的人力物力资源。

C.1.2 风险识别评估

根据网页篡改事件可能的路径，对安全风险进行识别与评估，了解已采取的安全措施及仍存在的安全风险。

表C.1 可能攻击路径风险识别评估

可能攻击路径	要素	漏洞描述
网络层	域名系统	所有提供域名访问的网站
	互联网路由	所有需要经过互联网的网站
	ARP 劫持	使用不具有 ARP 防护功能交换机接入的网站
主机层	操作系统账号弱口令	所有网站
	操作系统的系统软件存在安全漏洞	所有网站
	操作系统上安装的应用软件存在安全漏洞	所有网站
应用层	应用代码安全漏洞	所有内容动态显示的网站
内容管理系统	内容管理系统账号弱口令	使用内容管理系统的网站
	内容管理系统所在主机操作系统存在安全问题	使用内容管理系统的网站
	内容管理系统的应用程序存在安全漏洞	使用内容管理系统的网站

C.1.3 应急资源准备

（1）网站服务器备份：对网站服务器硬件、网站源代码、数据库等进行备份。

（2）应急处置工作：日志分析工具、网站代码对比工具、漏洞扫描工具、恶意进程检查工具、数据包分析工具等。

C.2 事件确认与应急处置阶段

C.2.1 事件处置步骤

步骤一：判断是否由于遭受域名劫持造成的“伪”篡改。用ping命令实现，若ping命令返回的IP地址信息与实际不一致，则通过正确的IP地址访问受害网站，检查网站内容是否正常。当确定是由于域名系统遭受攻击而造成域名解析被错误定向，则应及时修改域名服务器的相关解析数据，并检查域名服务器是否遭受攻击。对于大型门户网站，应尽快协调运营商清除公共域名解析服务器中的错误缓存，以降低事件造成的影响；

步骤二：判断是否由于遭受局域网ARP攻击（地址解析协议攻击）造成网页被“伪”篡改。从两个方面进行检查，一是直接本地登录网站所在服务器，从本地访问网站，检查网页内容是否被篡改；二是使用网络协议分析工具，检查局域网是否存在异常的ARP数据报文。一旦确认ARP攻击是导致网页篡改的原因，立即利用监控工具或ARP攻击检测软件定位实施攻击的主机，为后续的安全处置提供依据；

步骤三：分析日志以确认攻击方式。通过分析WEB访问日志、网络审计日志以及设备记录日志等，可以对通过WEB应用系统实施攻击进行准确判断，确定网页篡改的方式，有针对性地采取管理和技术措施，避免事件再次发生；

步骤四：检查漏洞。当因日志信息保存不完整或无法从日志中获知网页篡改的途径时，则只能通过检查漏洞来尝试处置。漏洞检查的范围应包括主机系统安全漏洞、网站应用代码安全漏洞、数据库软件安全漏洞等。对发现的各类安全漏洞进行必要的修复并更换后台登录密码，重新恢复网站系统运行，加强监测，以防止事件再度发生；

步骤五：总结分析。结合处置过程和结果对本次事件进行回顾，内容应涵盖攻击源与动机分析、安全事件影响评估、安全策略有效性评估、风险管理与预防策略的制定，以及建立持续监测与改进机制，确保网站系统的长期安全稳定运行。

C.2.2 事件处置实操

当通过网页篡改事件发生的表现以及判断方法怀疑或者确认事件发生时，应当立即启动应急预案，开展应急处置，同时向相关部门或团队报告，确保信息传递的及时性和准确性，尽快了解问题的性质、影响范围和严重程度，为后续处理提供决策依据。主要处置手段和方法包括：

C.2.2.1 隔离受影响区域

（1）服务器层面

使用云服务器的：登录云服务提供商的管理控制台。例如，在云控制台中找到对应的服务器实例，点击“停止”按钮，将服务器停止运行，使其从网络中隔离，防止外部继续访问被篡改的内容。

（2）使用本地服务器

1）对于Windows服务器：直接拔掉服务器的网线。若服务器有多张网卡，确保拔掉所有连接外网的网线。然后，通过“Ctrl + Shift + Esc”组合键打开任务管理器，在“服务”选项卡中找到Apache、Nginx等WEB服务相关进程（如“Apache2.4”“Nginx”），右键点击选择“结束任务”。

2）对于Linux服务器：使用命令行工具，输入“sudo ifconfig eth0 down”（假设服务器的网络接口为eth0），禁用服务器的网络连接；使用命令“sudo systemctl stop apache2”（若使用Apache服务器）或“sudo systemctl stop nginx”（若使用Nginx服务器），关闭WEB服务相关进程。

（3）网页层面（仅针对具体页面篡改）：

1）Apache服务器

打开服务器上的文本编辑器，如在Linux系统下使用vim编辑器，输入命令“sudo vim /etc/apache2/sites - available/000 - default.conf”（假设使用默认的虚拟主机配置文件）打开配置文件。在该配置文件中找到被篡改页面的URL路径相关配置，例如，若被篡改页面为“/news.html”，找到包含该路径的配置代码段，更改配置为页面不可见。

2）Nginx服务器

同样使用文本编辑器打开Nginx的虚拟主机配置文件，如“sudo vim /etc/nginx/sites - available/default”。找到被篡改页面的URL路径相关配置，更改配置为页面不可见。

C.2.2.2 关闭相关功能

（1）确定受影响功能

根据之前的评估和用户反馈，明确哪些功能与被篡改的内容相关联。例如，如果发现用户登录后出现的个人信息页面被篡改，那么与用户登录、个人信息展示相关的功能都可能存在风险。

（2）功能关闭操作

1）WEB 应用程序功能模块

对于基于PHP的WEB应用，以WordPress为例，若评论功能被恶意篡改，找到评论功能对应的PHP文件，通常在“wp - includes”目录下的“comment - functions.php”文件，文尾添加“add_filter ('comments_open', '__return_false'); add_filter('pings_open', '__return_false')”关闭评论。

对于基于 Python Django 框架的 WEB 应用，若用户注册功能出现问题，找到注册视图函数所在的文件，一般在“views.py”文件中。在注册视图函数开头，添加代码“return HttpResponse ('注册功能暂时关闭维护')”，这样当用户访问注册页面时，将看到提示信息，注册功能关闭。

2）数据库操作相关功能

若使用 MySQL 数据库，使用数据库管理工具 MySQL Workbench，选择“新建连接” → 输入 IP、端口、用户名 → 启用 SSH 隧道 → 连接。假设某个查询功能被恶意篡改用来获取敏感数据，该查询功能对应的存储过程名为“sensitive_query”，使用命令“ALTER PROCEDURE sensitive_query DISABLE;”禁用该存储过程。

若使用 SQL Server 数据库，使用数据库管理工具 SQL Server Management Studio，连接到对应的数据库实例。在对象资源管理器中，展开“可编程性” - “存储过程”节点，找到被篡改的存储过程，右键点击选择“修改”，在存储过程代码中添加“RETURN;”语句，使其无法执行。

C.2.3 恢复原始内容

（1）选择备份文件恢复

1）本地磁盘备份：若备份存储在本地磁盘，打开文件资源管理器（在 Windows 系统下）或使用命令行工具（在 Linux 系统下，如“cd /backup/website”），进入备份存储目录。查看备份文件的生成时间，优先选择距离篡改事件发生时间最近的备份文件，进行完整性校验。实施数据恢复，并对恢复结果进行确认。

2）网络存储设备备份：若使用网络存储设备，如 NAS（网络附加存储），在电脑上打开网络邻居（Windows 系统）或使用“smbclient”命令（Linux 系统）连接到 NAS 设备。找到网站备份文件夹，查看备份文件的详细信息，包括文件大小、修改时间等，确保备份文件完整且未被篡改。实施数据恢复，并对恢复结果进行确认。

3）云备份服务：以 XX 云盘备份为例，打开浏览器，登录 XX 云官网。在云盘文件列表中找到网站备份文件，点击文件右侧的“详情”按钮，查看文件的上传时间、文件大小等信息。同时，可尝试在云盘内对备份文件进行简单预览（若支持），确认文件内容正常。实施数据恢复，并对恢复结果进行确认。

（2）手动恢复

对于被篡改的网页文件，使用文本编辑器打开文件。

1）在 Windows 系统下使用 Notepad++；在 Linux 系统下，使用 vim 编辑器，输入“vim /var/www/html/index.html”，进入文件编辑模式，逐行检查文件内容，删除被恶意添加的代码或内

容。例如，如果发现网页文件中插入了恶意的 JavaScript 代码，将其删除，并确保文件的原有代码结构正确。

2）对于丢失或损坏的文件，如果本地存有原始文件副本，将其重新上传到服务对应目录。例如，使用 FTP 工具（如 FileZilla），将本地文件上传到服务器的/var/www/html/images/目录下，实施数据恢复，并对恢复结果进行确认。

（3）数据库恢复

1）数据库管理工具登录

MySQL 数据库：打开数据库管理工具 MySQL Workbench ，选择“新建连接” → 输入 IP、端口、用户名 → 启用 SSH 隧道 → 连接。

SQL Server 数据库：打开数据库管理工具 SQL Server Management Studio，在“连接到服务器”对话框中，输入服务器名称、身份验证方式（如 Windows 身份验证或 SQL Server 身份验证），点击“连接”。

2）数据恢复操作

针对被篡改的数据表，若有部分数据备份，根据数据的逻辑关系进行手动修复。例如，在 MySQL 数据库中，假设用户表“users”中的部分用户密码被篡改，且有之前的用户密码哈希值备份。已知用户 ID 为 1 的用户密码被篡改，备份的正确密码哈希值为“correct_hash_value”，使用 SQL 语句“UPDATE users SET password_hash = 'correct_hash_value' WHERE user_id = 1;”进行修复。

C.3 后攻击处置与系统加固策略

由于客观复杂性，即使处置人员保证准确定位了事件发生的技术原因与实施路径，也可能存在攻击者蓄意隐藏的后门程序，不能确保在原有系统上完全根除。因此还需进行一系列的事后处置工作，具体包括：

（1）根据入侵者可能使用的技术手段制订相应的安全加固方案，完善现有的安全机制等；

（2）对应用防火墙和安全防护系统做相应的配置策略进行优化，以提升其自动检测和阻止类似攻击的能力；

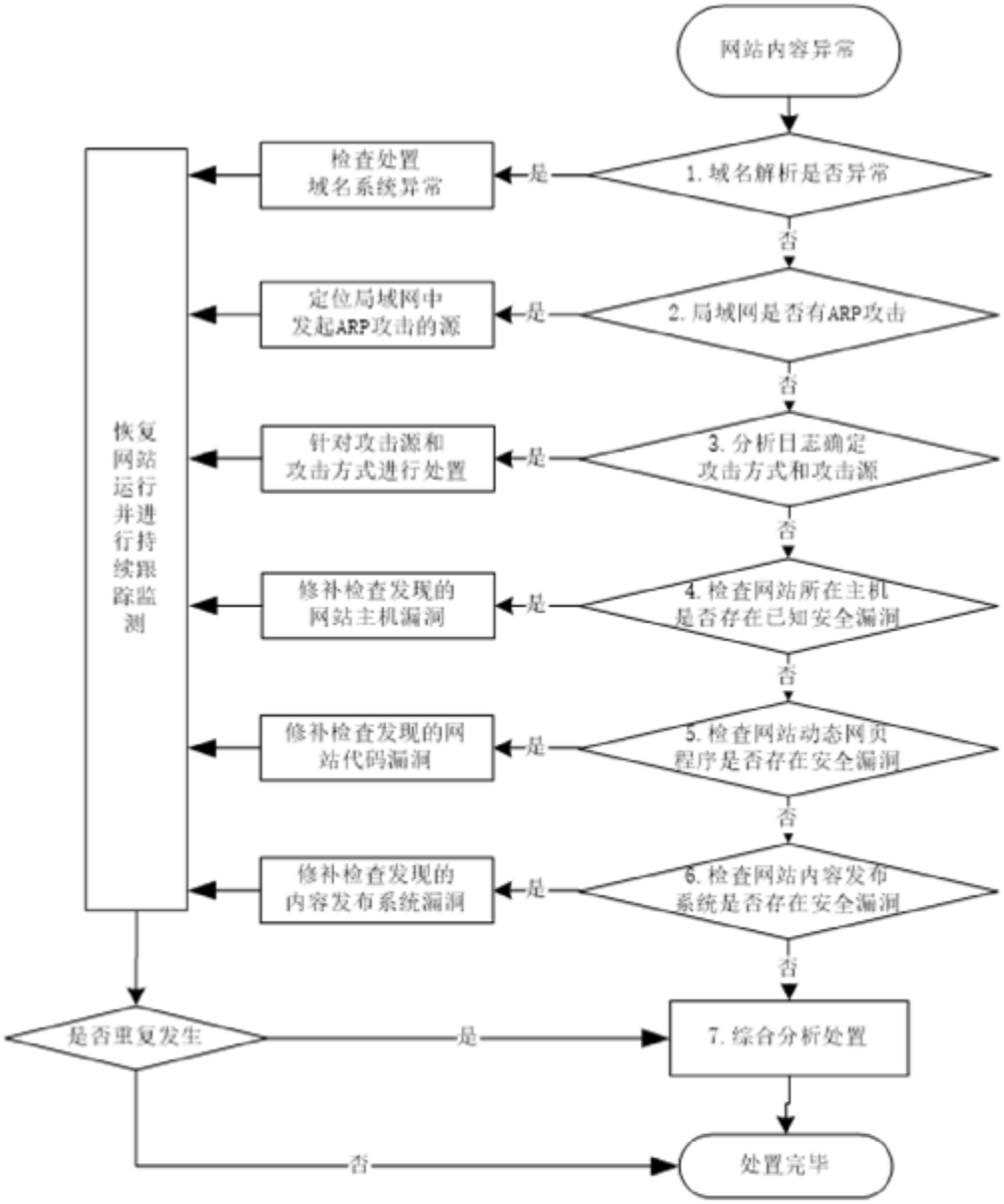
（3）对整个网站系统进行重新部署，包括重新安装操作系统、优化软件架构、重新部署应用系统等；

（4）进行全面的安全检测，包括源代码安全审查、安全漏洞的修复以及禁用不必要的服务和端口等；

（5）更换所有相关口令，包括操作系统、数据库、中间件、应用系统（管理）等，加强口令管理，确保口令的复杂性和安全性。

C.4 附件

C.4.1 网页篡改事件应急处置流程图



图C.1 网页篡改事件应急处置流程图