湛江市麻章区人民政府办公室

湛江市麻章区人民政府办公室关于印发麻章区政府网站突发事件应急预案的通知

各镇人民政府、区直及驻区有关单位:

《麻章区政府网站突发事件应急预案》业经区人民政府同意，现印发给你们，请认真贯彻执行。执行过程中如遇到问题，请径向区人民政府办公室政务公开组反映。

附件：麻章区政府网站突发事件应急预

湛江市麻章区人民政府办公室

2018年3月2日

麻章区政府网站突发事件应急预案

一、总则

（一）编制目的

为维护区政府网络安全，预防和遏制网站突发事件的发生，提高预防和控制政府网站突发事件的能力和水平，减轻和消除突发事件造成的危害和影响，确保政府网站安全可靠运行。

（二）编制依据

根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》等有关法律、法规，制定本预案。

（三）编制原则

1、积极防御、综合防范。采取多种措施，充分发挥各方面的作用，共同构筑网络与信息安全保障体系。

2、明确责任、分级负责。按照“谁主管谁负责、谁运营谁负责”的原则，建立和完善安全责任制、协调管理机制和联动工作机制。

3、以人为本、快速反应。按照快速反应机制，及时获取充分而准确的信息，迅速处置，最大程度地减少危害和影响。

4、依靠科学、平战结合。树立常备不懈的观念，定期进

行预案演练，确保应急预案切实可行。

（四）适用范围

本预案适用于区政府网站发生网络突发事件的应对处置工作。

（五）突发事件分类分级

1、突发事件分类：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、灾害性事件及其他事件等。

（1）有害程序事件是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的信息安全事件，包括计算机病毒事件、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）网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的信息安全事件，包括拒绝服务攻击事件、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）信息破坏事件是指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件，包括信息篡改事件、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）信息内容安全事件是指利用信息网络发布、传播危害国家安全、社会稳定和公众利益的内容的安全事件，包括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国家安全、社会稳定和公众利益的事件。

（5）设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的信息安全事件，以及人为的使用非技术手段有意或无意的造成信息系统破坏而导致的信息安全事件，包括软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6）灾害性事件是指由于不可抗力对信息系统造成物理破坏而导致的信息安全事件，包括由自然灾害等其他突发事件导致的网络与信息安全事件。

（7）其他事件，包括不能归为以上6个基本分类的信息安全事件。

2、突发事件分级：分为特别重大(I级)、重大(II级)、较大(III级)、一般(IV级)。

（1）特别重大安全事件（I级）。能够导致特别严重影响或破坏的信息安全事件，包括以下情况：使特别重要的信息系统遭受特别严重的系统损失（比如全国联网的业务应用系统中断服务2小时以上等），产生特别重大的社会影响。

（2）重大安全事件（II 级）。能够导致严重影响或破坏的信息安全事件，包括以下情况：使特别重要的信息系统遭受严重的系统损失，或使重要的信息系统遭受特别严重的系统损失，产生重大的社会影响。

（3）较大安全事件（III 级）。能够导致较严重影响或破坏的信息安全事件，包括以下情况：使特别重要的信息系统遭受较大的系统损失，或使重要的信息系统遭受严重的系统损失，一般信息系统遭受特别严重系统损失，产生较大的社会影响。

（4）一般安全事件（（IV 级）。不满足以上条件的信息安全事件，包括以下情况：使特别重要的信息系统遭受较小的系统损失，或使重要的信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失，产生一般的社会影响。

二、组织机构

（一）区政府网络与信息安全应急领导小组

组　长：罗红霞　　区委常委、常务副区长

副组长：李康养　　区政府办公室主任

成　员：颜荣生　　区委改革办公室副主任、区新闻中心主任

戴红娣　　区政府办公室副主任

宋晓燕　　区委宣传部副部长

孙康荣　区文广新局副局长

叶　就　区公安分局副局长

郭　瑜　区政府应急办公室主任

陈　钊　区信息管理中心主任

朱阅峰　区信息管理中心副主任

张雅娟　区府办政务公开组负责人

（二）安全应急的值班机构、机制

区政府网站与信息安全应急领导小组办公室设在区信息管理中心，由陈钊担任办公室主任，成员由朱阅峰、张雅娟组成。值班电话：0759-2733796、2733063。实行值班制度，由领导小组办公室统一安排人员值班。

三、应急处理

（一）信息监测与报告

按照“早发现、早报告、早处置”的原则，加强对政府网站与信息安全突发公共事件和可能引发突发公共事件的有关信息的收集、分析判断和持续监测。当发生网络与信息安全突发公共事件时，值班工作人员及时向网络与信息应急安全领导小组报告，同时向区公安分局报告，初次报告最迟不得超过1小时。

（二）预警处理与信息发布

对于可能发生或已经发生的网络与信息安全突发公共事件，值班工作人员及网络技术人员应立即采取措施控制事态，

并在 2 小时内进行风险评估，判定事件等级并发布预警，必要时应启动相应的预案，同时向区公安分局通报情况。在突发事件应急处置过程中，看突发事件发展的态势，必要时向区委区政府主要领导及上级有关部门汇报，以网络与信息安全应急领导小组名义召开新闻发报会，向公众公布事态发展的最新动态。

（三）奖惩

网络与信息系统重大信息安全事件的报告和处置管理工作坚持“统一领导、归口负责”的原则。网络与信息安全应急领导小组成员单位应当按照规定及时地如实报告事件的有关信息，不得迟报、漏报或瞒报。对迟报、漏报或瞒报等失职情况，网络与信息安全应急领导小组将予以通报批评；对造成严重不良后果的，追究责任领导和责任人的行政责任；构成犯罪的，依法追究其法律责任。

四、应急响应

（一）系统故障应急处置

1、当发生系统故障事件时，网络技术人员应及时通知网络与信息安全应急领导小组办公室，必要时向网络与信息安全应急领导小组汇报。

2、分析事件发生源头，切断事件源头，控制事件范围，必要时停止系统运行。

3、网络技术人员应及时查看安全日志对异常事件发生

源头、发生原因、影响范围做出判断，并提出补救措施。

4、针对事件原因查找系统漏洞，提出系统安全策略调整方案，并报网络与信息安全应急领导小组办公室审批。审批通过后根据系统安全策略调整方案，对安全设备、应用系统等的安全控制策略做出相应调整，确认无误后恢复系统运行。

5、网络技术人员将系统异常事件处理报告提交应急领导小组办公室归档。

（二）网络攻击应急处置

1、网络技术人员根据安全设备的报警和日志，确定攻击目标和攻击来源。

2、网络技术人员对攻击目标采取关闭或隔离措施，详细检查被攻击系统是否留有恶意代码，更改密码增强安全防范策略，必要时对系统和数据进行紧急备份。

3、网络技术人员对攻击来源进行隔离，分析原因，调整安全防范策略，阻断攻击行为。

4、网络技术人员在对系统进行安全评估后，恢复系统上线运行。

5、网络技术人员完成系统异常事件处理报告，对于恶意攻击上报主管部门，并提交网络与信息安全应急领导小组办公室归档。

（三）病毒爆发应急处置

1、网络技术人员根据安全设备和网络杀毒软件的报警和日志，分析攻击来源，并对攻击来源和攻击区域及时采取隔离措施。

2、对重要的网络服务器和业务应用系统紧急备份，防止因病毒造成数据丢失，必要时可暂停系统运行。

3、及时通知防病毒厂商，通报病毒爆发情况并寻求技术支持。

4、获得处理建议后及时通过网站、电话等渠道公布，并通知各部门管理员处理措施，控制病毒进一步传播、升级病毒库、清除病毒。

5、分析病毒产生原因，传播途径，采取补救措施，纠正违规行为。

6、网络技术人员在对系统进行安全评估，确认病毒已得到控制或清除后，恢复系统上线运行。

7、网络技术人员完成系统异常事件处理报告，将恶意制造或传播病毒的情况根据情况上报有关部门。

（四）机房突发事件应急处置

1、火警。值班工作人员要随时提高警惕，如发现机房内有异常气味，应仔细、认真地巡视机房各处，直到查清原因，确实无危险情况为止。如发现机房内有烟雾，甚至火焰，对烟雾产生处，应检查原因，尤其应注意活动地板下的情况，尽力扑灭，必要时启用灭火系统。对重大火情，一方面要尽快报警，同时要采取一切措施控制并扑灭火焰。

2、水警。机房内如有水管破裂等严重水情时，要切断电源，然后设法排水，保护机房内各种设备的安全。对无法控制的严重水情，要立即报警。机房顶部漏水时，应设法用容器及塑料布保护机房各种设备不被淋湿。情况严重时应切断电源，并通知维修部门。

（五）网络设备及应用服务器异常事件的应急处置

1、网络技术人员对网络设备及服务器异常事件进行原因分析。

2、及时发布信息，对事件原因、处理措施及恢复时间进行通知、公告。

3、如属于硬件故障，及时启用备用设备，并将故障设备报修。

4、如属于软件故障，根据故障程度进行紧急调试或启用最近一次备份进行数据恢复。

5、网络技术人员完成系统异常事件处理报告。

五、附 则

（一）预案的制定

本预案由区政府办公室负责制订、修订，报区政府批准后实施。

（二）解释部门

本预案由麻章区人民政府办公室负责解释。

（三）实施时间

本预案自印发之日起实施。