汕尾市工业和信息化局

汕工信函〔2023〕102号

关于印发《汕尾市工业和信息化局网络安全事件应急预案》的通知

局各科室、直属单位：

因人员调整，现对《汕尾市工业和信息化局网络安全事件应急预案》进行调整，请遵照执行。

汕尾市工业和信息化局

2023年3月20日

汕尾市工业和信息化局网络安全事件应急预案

为切实做好汕尾市工业和信息化局网络安全突发事件的防范和应急处理工作，进一步提高我局预防和控制网络安全突发事件的能力和水平，减轻或消除突发事件的危害和影响，确保网络的正常运行和信息安全，根据互联网网络安全相关条例及省、市政府有关文件精神，结合工作实际，制定本预案。

第一章　总则

第一条　本预案所称网络安全事件，是指自然因素或者人为活动以及软硬件本身缺陷或故障引发的危害网络设施及信息安全等有关事件。

第二条　本预案的指导思想是以习近平新时代中国特色社会主义思想为指导，确保汕尾市工业和信息化局网络安全。

第三条　应急处置工作原则：统一领导、统一指挥、各司其职、整体作战、发挥优势、保障安全。

第二章　领导机构

建立统一领导、职责明确、协调配合的网络安全事件应急组织体系。成立安全事件应急响应领导小组，以局党组书记为组长，局党组成员为副局长，各科室主要负责人为成员。

负责领导和协调本单位网络安全事件处置工作。领导小组见附件。

第三章　预防措施

第四条　局各科室负责人签定网络安全责任书。

第五条　为确市工信局网络安全，应采用以下防范措施：

1、技术方面。安装防火墙、计算机杀毒软件，对电脑主机、网络设备、安全设备进行必要的配置，定时进行漏洞扫描，及时安装、升级应用软件和操作系统补丁，对重要数据定时进行备份。

2、管理方面。建立健全网络与信息安全各项管理制度，落实网络安全责任制，加强检查，做好系统日常维护，开展网络安全培训等。

第四章　处置措施

第六条　处置程序。

（一）发现情况。

局各科室是做好网络信息系统和电脑设备的日常巡查，办公室做好局网站的日常巡查，以保证最先发现信息系统和网站网络安全事件并及时处置。

（二）预案启动。

一旦发生网络与信息安全事件，立即启动应急预案，进入应急预案的处置程序。

（三）应急处置方法。

在网络安全事件发生时，首先应区分是否为自然灾害与人为破坏两种情况，根据这两种情况把应急处置方法分为两个流程。

流程一：当发生的网络与信息安全事件为自然灾害时，应根据当时的实际情况，在保障人身安全的前提下，首先保障数据的安全，然后是设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

流程二：当人为或病毒破坏的网络安全事件发生时，具体按以下顺序进行：判断破坏的来源与性质，断开影响安全与稳定的网络设备，断开与破坏来源的网络物理连接，跟踪并锁定破坏来源的IP或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照网络与信息安全事件发生的性质分别采用以下方案：

一、网站、网页出现非法言论事件紧急处置措施

1.网站、网页由办公室负责随时密切监视信息内容。

2.发现在网上出现非法信息时，办公室应立即向所属信息安全负责人通报情况；情况紧急的，应先及时采取删除等处理措施，再按程序报告。

3. 局网络安全事件应急响应领导小组办公室应在接到通知后立即赶到现场，作好必要记录，清理非法信息，妥善保存有关记录及日志或审计记录，强化安全防范措施，并将网站网页重新投入使用。

二、黑客攻击事件紧急处置措施

1.当办公室发现网页内容被篡改，或通过入侵检测系统发现有黑客正在进行攻击时，应立即向局网络安全事件应急响应领导小组通报情况。

2.局网络安全事件应急响应领导小组负责人通知网站运维公司将被攻击的服务器等设备从网络中隔离出来，保护现场，并将有关情况向本单位网络与信息安全事件应急响应领导小组汇报。

3.对现场进行分析，并写出分析报告存档，必要时上报所属主管部门。

4.恢复与重建被攻击或被破坏的系统。

三、病毒事件紧急处置措施

1.各科室人员当发现有计算机被病毒感染后，应立即向办公室报告，办公室迅速联系有关第三方机构，将该机从网络上隔离开来。

2.对该设备的硬盘进行数据备份。

3.启用反病毒软件对该机进行杀毒处理，同时通过病毒检测软件对其他机器进行病毒扫描和清除工作。

4.如果现行反病毒软件无法清除该病毒，应立即向本部门网络与信息安全事件应急响应领导小组报告，并研究解决。

四、局域网中断紧急处置措施

1.应准备好网络备用设备，存放在指定的位置。

2.局域网中断后，信息安全负责人员应立即判断故障节点，查明故障原因，并向本部门网络安全事件应急响应领导小组汇报。

3.如属线路故障，应重新安装线路。

4.如属路由器、交换机等网络设备故障，应立即从指定位置将备用设备取出接上，并调试通畅。

5.如属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调测通畅。

（四）网络安全事件报告制度。

建立网络安全事件报告制度，发生网络安全事件时，一方面按照应急处置方法进行处置，同时需要判定网络与信息安全事件的级别，首先向网络安全事件应急响应领导小组汇报，如有必要同时向网信部门、公安机关汇报，并及时报告处置工作进展情况，直至处置工作结束。

情况报告内容包括：网络与信息安全事件发生的时间、地点，网络与信息安全事件的级别，造成的后果，应急处置的过程、结果，网络与信息安全事件结束的时间，以后如何防范类似网络与信息安全事件发生的建议与方案等。

（五）发布预警。

网络与信息安全事件发生时，可根据灾害的危害程度适当地发布预警，特别是一些在其它地方已经出现，或在相关网站发布的安全预警而本部门网络还没有出现的相应信息

安全事件，除了在技术上进行防范以外，还应当向网络用户发布预警，直至网络与信息安全事件警报解除。

（六）预案终止。

当网络与信息安全事件影响已消除，或者得到有效控制后，局网络安全事件应急响应领导小组宣布网络安全事件应急期结束，同时预案终止。

第五章　保障措施

网络安全事件应急防治是一项长期的、持续的、跟踪式的、深层次的和各阶段相互联系的工作，是有组织的科学与社会行为，而不是随每次网络与信息安全事件的发生而开始和结束的活动。因此，必须做好应急保障工作。

第七条　人员保障。

重视人员的建设与保障，确保在网络安全事件发生前的人员值班、网络与信息安全事件处置过程中和事后重建中的人员在岗与战斗力。

第八条　技术保障。

重视网络的建设和升级换代，确保在网络与信息安全事件发生前网络信息系统的强劲与安全、网络与信息安全事件处置过程中和事后重建中的相关技术支撑。

第九条　训练和演练。

开展本部门网络信息安全应急管理、应急处置培训，对应急处置人员进行技能培训，提高防范意识及技能。有针对

性地开展应急演练，确保事发后应急救助手段及时到位和有效。

第六章　附则

第十条　本预案内各条款与相关法规冲突时，以相关法规为准。

第十一条　在处置网络安全事件的过程中，必须遵循国家有关安全和保密法规。

第十二条　根据实际需要和有关规定，本预案将不断进行修改和完善。

第十三条　本预案自印发之日起实施。

汕尾市工业和信息化局网络安全

应急工作领导小组

组　长：詹文杰

副组长：卢承恒、郑新钦（网络安全直接责任人）、
吴光群、张杭彬、陈景冰

成　员：徐渭滨、庄志远、罗佳华、李杰伟、郑校君
黄群义、廖小岸、钟东旭、马　斌、吴　扬
陈启福、黄晋沿、叶思臻、张善青、陈岳立

领导小组办公室设在市工业和信息化局办公室，郑新钦兼任领导小组办公室主任，陈景冰任办公室副主任。办公室成员：徐渭滨、庄志远、吴 扬、马 斌、钟润楷。

领导小组办公室职责：按照省市有关规定，出现网络安全问题，第一时间关停网站或电脑设备，及时取证，分析查找原因，进行查处、整改，尽最快时间、最大程度消除社会负面影响；遇到重大网络安全事件第一时间向市委网信办和公安部门汇报；清查原因，追究相关责任。