鞍山市医疗保障事务服务中心
文 件 处 理 单

<table>
<tr><td>来文机关：中共鞍山市医疗保障局党组文件</td><td rowspan="3">文件标题：
网络与信息安全突发事件应急管理预案</td></tr>
<tr><td>文号：鞍医保党组发[2020]25 号</td></tr>
<tr><td>密级：</td></tr>
<tr><td>来文日期：2020 年 7 月 28 日</td><td>办文时限：</td></tr>
<tr><td>拟办意见：
送请泰芳主任、鸣松主任阅示。</td><td>刘大伟</td></tr>
<tr><td colspan="2">领导批示：
请信息技术部要高度重视网络与信息安全，制定应急预案。请泰芳主任对网络信息工作中涉及安全和突发性的问题及时上报、及时处理。
29/7　28/7</td></tr>
<tr><td colspan="2">处理结果：</td></tr>
</table>

注：请阅处后及时返回办公室。

中共鞍山市医疗保障局党组文件

鞍医保党组发〔2020〕25 号

网络与信息安全突发事件应急管理预案

一、总则

（一）编制目的

为保障网络信息安全，及时有效地应对网络与信息安全事件，建立健全信息安全应急响应机制，确保计算机信息系统的实体安全、运行安全和数据安全，更好地预防控制和最大限度地消除网络与信息安全各类突发事件的危害和影响，提高处置突发事件的能力，制定本预案。

（二）编制依据

《国家网络与信息安全事件应急预案》、《辽宁省网络与信息安全应急预案》、《中华人民共和国计算机信息系统安全保护条例》、《计算机病毒防治管理办法》，《中华人民共和国公务员法》、《鞍山市政府信息系统安全检查实施办法》（鞍政办发〔2010〕21 号）。

（三）适用范围

本预案适用于鞍山市医疗保障局网站、“鞍山医保”APP、“鞍山医保”微信公众号、鞍山市人力资源和社会保险管理信息系统、财务软件系统等信息系统。

（四）工作原则

1、统一领导，分级负责。全局网络与信息安全突发事件应急工作要坚持统一领导，按照“谁应用、谁管理、谁负责”的原则，各部门各司其职，共同履行应急处置工作的管理职责。

2、预防为主，加强监控。坚持预防与应急相结合，立足安全防护，加强预警，建立和完善信息安全监控体系和管理机制，加强对网络与信息安全隐患的日常监测，保证对网络与信息安全事件做到快速觉察、快速反应、及时处理、及时恢复。

二、组织机构

（一）应急管理机构

为了更好地处置网络与信息安全事件，保证网络突发事件应急指挥调度工作迅速、高效、有序地进行，成立鞍山市医疗保障局网络和信息安全事件应急处理领导小组（以下简称应急领导小组），组成人员如下：

组长：程新凯 杜鸣松

副组长：陈国志 徐泰芳

领导小组下设应急处理办公室，办公室设在局综合科。

（二）工作职责

应急领导小组主要负责全局网络与信息安全事件的应急处置工作的统一部署、整体规划、组织协调和决策指挥。

应急办公室主要职责：

（1）负责预警、监测机制正常运行。

（2）负责突发事件的分析定级，并上报应急领导小组。

（3）负责对领导小组决定事项的执行情况进行监督、检查。

（4）负责应急事件的总结工作，消除突发事件造成的不良影响。

（5）负责日常应急演练工作的开展及网络与信息安全知识的培训、指导。

三、预防、监测、预警

（一）预防与监测

完善网络与信息安全事件预防监测制度，按照“早发现、早报告、早处置”的原则，加强对网络与信息安全事件的信息收集、分析判断和持续监测。应做到以下几个方面：

1、定时对网络的连通情况进行检查。

2、定时对网络和应用系统各模块的运行情况进行检查。

3、定期对机房的环境和服务器的运行状态进行检查。

4、定时对各部门信息发布情况进行检查。

5、实时对网络入侵及攻击情况进行监测。

6、全局工作人员应严格遵守我局制定的《存储设备报废销毁管理规定》，规范使用计算机终端和移动存储设备。

（二）预警

1、接收预警

应急处理办公室接收上级部门和其他权威机构发布的预警信息，并将预警信息中的事件类别、波及范围、危害程度、持续时间上报领导小组。

2、预警响应

在领导小组的指挥下，应急处理办公室根据预警情况作出响应：

（1）确定应采取的应急措施。

（2）通过我局协同办公平台发布预警公告，协调相关部门做好应急保障准备工作。

四、分类分级

（一）事件分类

网络与信息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、误操作事件等。

1、有害程序事件分为计算机病毒入侵、木马侵害、网页恶意代码事件、网络钓鱼、干扰等。

2、网络攻击事件分为拒绝服务攻击、后门攻击、漏洞攻击、网络扫描窃听等。

3、信息破坏事件分为信息篡改、信息假冒、信息泄漏、信息窃取、信息丢失等。

4、信息内容安全事件是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、灾害性事件是指自然灾害等其他突发事件导致的网络与信息安全事件。

7、误操作事件指由于人为操作失误引起的对信息系统的破坏，并因此产生恶劣影响的事件。

（二）事件分级

本预案将网络与信息安全事件分为四级：Ⅰ级（特别重大）、Ⅱ级（重大）、Ⅲ级（较大）、Ⅳ级（一般）。

1、符合下列情形之一的，为特别重大网络与信息安全事件（Ⅰ级）：

（1）信息系统或网站中断运行24小时以上、影响人数50万以上。

（2）信息系统或网站中的数据丢失或被窃取、篡改、假冒，对社会秩序和公共利益构成特别严重威胁或导致特别重大经济损失。

（3）通过我局网站或协同办公平台传播反动信息、煽动性信息、涉密信息、谣言等，对国家安全和社会稳定构成特别严重危害的事件。

（4）发生特别重大自然灾害，造成系统无法继续运行。

（5）严重损坏我局形象，影响特别严重的网络与信息安全事件。

（6）其他对社会秩序和公共利益构成特别严重威胁、造成特别严重影响的网络与信息安全事件。

2、符合下列情形之一且未达到特别重大网络与信息安全事件（I级）的，为重大网络与信息安全事件（II级）：

（1）信息系统或网站中断运行8小时以上、影响人数10万以上。

（2）信息系统或网站中的数据丢失或被窃取、篡改、假冒，对社会秩序和公共利益构成严重威胁或导致重大经济损失。

（3）通过我局网站或办公平台传播反动信息、煽动性信息、涉密信息、谣言等，对国家安全和社会稳定构成严重危害的事件。

（4）发生重大自然灾害，对信息系统和数据造成严重破坏。

（5）损坏我局形象，影响严重的网络与信息安全事件。

（6）其他对社会秩序和公共利益构成严重威胁、造成严重影响的网络与信息安全事件。

3、符合下列情形之一且未达到重大网络与信息安全事件(II级)的，为较大网络与信息安全事件(III级)：

（1）信息系统或网站中断运行4小时以上、影响人数1万以上。

（2）信息系统或网站中的数据丢失或被窃取、篡改、假冒，对社会秩序和公共利益构成较大威胁或导致较大经济损失。

（3）通过我局网站或办公平台传播反动信息、煽动性信息、涉密信息、谣言等，对国家安全和社会稳定构成较大

危害的事件。

（4）信息系统或网站由于有害程序的影响造成部分功能不可用。网站由受到网络攻击事件造成部分模块功能不可用。

（5）发生较大规模自然灾害，对信息系统和数据造成较大破坏。

（6）损坏我局形象，影响较大的网络与信息安全事件。

（7）其他对社会秩序和公共利益构成较大威胁、造成较大影响的网络与信息安全事件。

4、除上述情形外，对社会秩序和公共利益构成一定威胁、造成一定影响的网络与信息安全事件，为一般网络与信息安全事件(Ⅳ级)。

为了妥善处置信息安全事件，当事件级别难以判定时，按上限定级。

五、应急处置

（一）信息报告

网络与信息安全事件发生后，应急处理办公室对事件进行动态监测，及时将事件的性质、危害程度和损失情况及处置工作等情况上报领导小组，不得隐瞒、缓报、谎报。

（二）应急响应

对发生网络与信息安全事件，要根据初步研判的事件等级，进入对应的响应状态。

1、启动指挥体系

Ⅰ级、Ⅱ级、Ⅲ级响应：领导小组进入应急状态，履行应急处置工作的统一领导、指挥、协调职责；应急处理办公室进入应急状态，在领导小组统一指挥下，组织协调相关人员负责本部门应急处置工作或支援保障工作，相关部门人员应24小时值班，并派出联络员参加应急处理办公室工作。

Ⅳ级响应：应急小组办公室进入应急状态，组织协调相关人员负责应急处置工作。

2、掌握事件动态

（1）跟踪事态发展。事件发生地部门及时将事态发展变化情况和处置进展情况报应急处理办公室。

（2）检查影响范围。应急处理办公室全面了解事件的波及范围和影响，并将有关情况报领导小组。

（三）应急处置措施

应急处理办公室要组织相关人员及时研究对策意见，必要时候可以聘请专家组和应急技术支撑队伍对工作进行决策部署。要迅速建立与现场指挥的通讯联系，控制事态，防止蔓延，做好处置消除隐患，各类事件应急预案如下。

1、网站、网页出现非法言论

（1）发现非法内容，管理员立即关闭网站，切断非法信息传播源，向应急处理办公室报告，同时做好现场保护。

（2）应急处理办公室将事故情况、发生原因一并上报领导小组。

（3）上报公安机关，做好取证工作，追查非法信息来源。

（4）清除非法信息，检查网站的安全防护设施，确保信息安全后，将网站、网页重新投入使用。

（5）应急管理办公室将处理结果上报领导小组。

2、网络攻击或病毒感染造成网站、信息系统运行异常

（1）发现网络攻击或软件遭到病毒感染后，应及时停止系统运行，并向应急处理办公室汇报，同时做好现场保护。

（2）应急处理办公室接到报告后，制定事件处理方案，组织相关人员对事件进行处理。

（3）管理员首先将被攻击（或病毒感染）的服务器、终端等设备从网络中隔离出来。

（4）追查破坏来源，消除攻击或病毒感染的源头。对于人为故意破坏，情节严重的上报公安机关。

（5）修复被攻击（或病毒感染）的设备，恢复破坏的系统数据，检查并完善安全防范措施。

（6）应急管理办公室将处理结果上报领导小组。

3、数据库发生故障

（1）数据库发生故障时，管理员应及时向应急处理办公室报告。

（2）应急处理办公室对故障产生的影响进行预判，同时向领导小组报告。

（3）局技术人员对数据及系统进行修复，修复有困难的，在征得应急处理办公室的许可下，可向软硬件供应商提请支援。

（4）在数据修复期间，应急处理办公室协调所涉及的

部门延缓业务处理或手工处理。

（5）确实无法修复的，将数据恢复为最近时间的数据备份，各部门补充所丢失的信息。

（6）数据修复完成后，数据库正常投入运行。应急管理办公室将处理结果上报领导小组。

4、设备发生故障

（1）发现设备损坏后，立即向应急处理办公室报告。

（2）应急处理办公室接到报告后，组织相关人员查明损坏原因并安排人员对设备进行恢复。不能恢复的，立即联系设备供应商进行维修。

（3）不能短时间内恢复的情况，应急管理办公室应将预计的恢复时间告知相关部门，以便各部门妥善安排工作。

（4）对于不能修复的设备，一般设备采取备用设备替代的方式维持运行；关键、必要的设备，在征得领导同意的情况下，优先购买，保证重要业务顺利开展。

5、内部中心域网中断

（1）网络中断后，网络管理员应立即判断故障节点，查明故障原因，并向应急管理办公室报告。

（2）线路故障，对线路进行修复；路由器、交换机等网络设备故障，采用备用设备替换。

（3）如故障情况较严重，网络中断时间超过2小时，应向应急领导小组报告，并发出公告，以便各部门安排工作。

6、外部线路中断

（1）网络中断后，网络管理员应立即判断故障节点，

查明故障原因，并向应急管理办公室报告。

（2）可即时恢复范围，立即予以恢复；电信运营商管辖范围，立即与运营商的维护部门联系，要求尽快恢复。

（3）如故障情况较严重，网络中断时间超过2小时，应向应急领导小组报告，并发出公告，以便各部门安排工作。

7、供电中断

发生供电中断时，管理员应立即与相关部门取得联系，掌握供电中断的原因和时间，并根据原因和时间做如下安排：

（1）预计停电在10小时以内，由UPS供电；

（2）预计停电在10-20小时，关掉非关键设备，确保服务器、路由器、交换机等设备供电；

（3）预计停电超过20小时，白天工作时间关键设备运行，晚上所有设备停机。

（四）应急结束

应急处理办公室提出应急结束的建议，应急响应的结束由领导小组决定。

六、后期处置

（一）善后处置

在应急处置工作结束后，应急处理办公室组织相关部门迅速采取措施，尽快恢复正常工作。

应急处理办公室组织有关人员和专家组成事件调查组，查明事件原因，统计网络设备损失情况、系统数据损坏情况、我局形象危害情况，并根据统计结果进行分析，总结经验，弥补不足，形成事件处理档案。

（二）消除不良影响

对于传播非法信息等严重影响社会秩序和公共利益的事件，在应急结束后，应急管理办公室组织相关部门通过电视、报纸、网络等多渠道对事件的原因、处理过程、处理结果等信息进行发布，消除此类事件产生的不良影响。

七、应急保障

（一）应急队伍保障

负责应急工作的成员，由高素质、责任心强、有一定技术水平和业务能力的人员担任，形成一支长期稳定的应急保障队伍。

（二）专家队伍

应急处理办公室是事件处理的主要力量，处理特殊事件时，如果人员不足或需要特殊技能的人才，在安全允许的情况下，可以聘请专业的技术人员共同处理，为网络与信息安全事件的预防和处置提供技术咨询，参与重要信息的研判、网络与信息安全事件的调查和总结评估工作。

（三）应急装备保障

在处理特殊事件时，局内的信息化设备要统一调用，保证系统、资源的快速恢复，如果需要另行购置设备，按局内设备采购规定进行，特殊紧急须立即购买的设备，要及时向领导请示。

八、附则

（一）培训及演练

加强对网络安全和应急预案的宣传教育工作；对应急指

挥管理机构和保障人员进行技术培训，提高他们的理论水平和应急意识；定期或不定期地模拟各类突发事件，进行应急事件处理演练，提高应急响应和处理突发事件的能力，做到警钟长鸣、常备不懈。

（二）责任与奖惩

为了提高应急工作的效率和积极性，对于在事件预警、应急响应和事件处理过程中表现突出的人员，给予表彰；对于玩忽职守、隐报瞒报、响应及处置严重失职的人员按有关规定处理。

（三）其他

1、本预案要做年度评估，随着信息网络的快速发展和我局信息化建设水平的逐步提高，结合相关法律、法规，修订和完善本预案。

2、本预案由应急处理小组办公室负责解释。

3、本预案自发布之日起施行。

中共鞍山市医疗保障局党组

2020年7月22日

中共鞍山市医疗保障局综合科　　2020年7月22日印发