附件 1

铁岭市市场监督管理局网络信息安全应急预案

为保证全局网络信息安全，加强和完善网络与信息安全管理，层层落实责任，有效预防、及时控制网络信息突发事件的发生，最大限度地消除突发事件造成的危害和影响，确保信息系统和网络运行通畅，结合实际，特制定本办法。

一、总则

（一）工作目标

保障铁岭市市场监督管理局网络信息系统的安全性、完整性、准确性，保障网络、计算机、服务器等相关配套设备设施及系统运行环境的安全。

（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》、《互联网信息服务管理办法》、《计算机网络信息安全保密制度》、《涉密存储介质保密管理规定》等相关法律、法规的规定，制定本预案。

（三）基本原则

1. 预防为主。根据《中华人民共和国网络安全法》的要求，建立、健全计算机信息安全管理制度，有效预防网络与信息安全事故的发生。

2. 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。各科室和直属单位应积极支持和协助应急处置工作。

3. 果断处置。一旦发生网络与信息安全事故，应迅速反应，及时启动应急处置预案，尽最大力量减少损失，尽快恢复网络与系统运行。

（四）适用范围

本预案适用于市局机关及各直属单位。

二、组织体系

铁岭市市场监督管理局网络信息安全工作领导小组为市局网络信息安全应急处置的组织协调机构，负责网络与信息安全应急响应工作的整体规划、组织协调和决策指挥。

三、预防预警

按照“早发现、早报告、早处置”的原则，加强对各科室和直属单位有关信息的收集、分析判断和持续监测。当发生网络信息安全突发事件时，按规定及时向网络安全领导小组报告，初次报告最迟不得超过1小时，重大和特别重大的网络信息安全突发公共事件实行态势进程报告和日报告制度。报告内容主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施等。网络信息安全领导小组接到报告后，应迅速召开网络安全领导小组会议，研究确定网络与信息安全突发公共事件的等级，根据具体情况启动相应的应急预案，并向相关主管部门进行汇报。

四、网络信息安全应急预案处置措施和处置程序

（一）网站、网页出现非法言论时的应急预案

1.负责网站维护的市局办公室技术人员随时监控网站、网页信息内容。

2. 发现在网上出现非法信息时，办公室技术人员立即向网络信息安全工作领导小组汇报情况,并作好记录。清理非法信息，采取必要的安全防范措施，将网站、网页重新投入使用；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.办公室技术人员应妥善保存有关记录、日志或审计记录，将有关情况向网络信息安全工作领导小组汇报,并及时追查非法信息来源。

（二）黑客攻击或软件系统遭破坏性攻击时的应急预案

1. 当办公室技术人员通过入侵监测系统发现有黑客正在进行攻击时，应立即向网络信息安全工作领导小组报告，并同时断开网络，保留系统日志。

2. 软件如遭到破坏性攻击(包括严重病毒入侵等)时，办公室技术人员要将被攻击(或病毒感染)的服务器等设备从网络中隔离出来,保护现场,并同时向网络信息安全领导小组报告情况。初步查清原因及破坏程度,如情况复杂,应及时向公安机关报案。

3.办公室技术人员负责恢复与重建被攻击或被破坏的系统，恢复系统数据，并及时追查非法信息来源。

（三）数据库发生故障时的应急预案

1. 一旦数据库崩溃，铁岭市局办公室技术人员应立即进行数据及系统修复。

2. 无法修复的，在征得网络信息安全工作领导小组许可的情况下，可立即向软硬件提供商请求支援。

3. 在取得相应技术支援也无法修复的，应向网络信息安全工作领导小组报告，在征得许可、并可在业务操作弥补的情况下，由铁岭市局办公室技术人员利用最近备份的数据进行恢复。

（四）设备安全发生故障时的应急预案

1. 服务器、路由器等关键设备损坏后，铁岭市局办公室技术人员立即查明原因，并向网络信息安全工作领导小组汇报。

2. 如果能够自行恢复，应立即用相应的备件替换受损部件。

3. 如属不能自行恢复的，立即与设备提供商联系，请求维护人员前来维修。

4. 如果设备一时不能修复，应向网络安全领导小组汇报，并告知各部门，暂缓上传上报数据，直到故障排除设备恢复正常使用。

（五）内部局域网发生故障中断时的应急预案

1. 办公室技术人员应申领必要的网络备用设备，存放在指定的位置。

2. 局域网中断后，负责网络安全的技术人员应立即判断故障节点，查明故障原因，并向网络信息安全工作领导小组汇报。

3. 如属线路故障，应及时通知网络维护商重新恢复线路。

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，替换故障设备，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。

（六）政务网外部线路中断时的应急预案

1. 政务网线路中断后，办公室技术人员应向网络信息安全工作领导小组报告。

2. 办公室技术人员应迅速判断故障节点，查明故障原因。

3. 属可即时恢复范围，由办公室技术人员立即予以恢复。

4. 属运营商管辖范围，办公室技术人员应立即与电信运营商的维护部门联系，要求尽快修复。

5. 如果恢复时间预计超过两小时，应立即向网络信息安全工作领导小组汇报。经网络安全领导小组同意后，应通知各单位暂缓上传上报数据。

（七）外部电路中断后的应急预案

1. 外部电路中断后，办公室负责人员应立即向网络信息安全工作领导小组汇报情况。

2. 如因局内电路故障，由办公室负责人员通知维修人员迅速恢复。

3. 如果是局外部的原因，由办公室立即与供电局联系，请供电局或机关事务服务中心迅速恢复供电；如果供电局告知需长时间停电，提前做好存档工作。

（八）机房发生火灾时的应急预案

1. 一旦机房发生火灾，应遵循下列原则：首先保证人员安全；其次保证关键设备、数据安全；三是保证一般设备安全。

2. 人员灭火和疏散的程序是：应首先切断机房内电源，同时通过 119 电话报警。并从最近的位置取出灭火器进行灭火，其他人员按照预先确定的路线，迅速从机房中有序撤出。

五、预案终止

灾害险情已消除，或者得到有效控制后，由网络信息安全领导小组宣布险情或灾情应急期结束，并予以公告，同时预案终止。