附件1：

一、网络与信息安全应急（响应）协调领导小组

组　　长：局主要领导

副 组 长：局分管领导

成　　员：局机关各科室、下属单位负责人

二、网络与信息安全应急（响应）协调领导小组办公室

主　任：局办公室主任（兼）

成　员：局机关各科室、下属单位的网络与信息安全联络员

附件2：

重大信息安全事件报告表

报告时间：　年　月　日　时　分

单位名称：　　报告人：

联系电话：　　通讯地址：

传真：　　电子邮件：

发生重大信息安全事件的网络与信息系统名称及用途：

负责部门：　　负责人：

重大信息安全事件的简要描述(如以前出现过类似情况也应加以说明)：

初步判定的事故原因：

当前采取的应对措施：

本次重大信息安全事件的初步影响状况：

事件后果：

影响范围：　　严重程度：

值班电话：

传真：

附件 3：

重大信息安全事件处理结果报告表

原事件报告时间:　　年　　月　　日　　时　　分

备案编号:　　年　　月　　日　第　　号　总第　　号

单位名称:

联系人:　　联系电话:

通讯地址:

网络或信息系统名称及用途:

已采用的安全措施:

重大信息安全事件的补充描述及最后判定的事故原因:

对本次重大信息安全事件的事后影响状况:

事件后果:

影响范围:

严重程度:

本次重大信息安全事件的主要处理过程及结果:

针对此类事件应采取的保障网络与信息系统安全的措施和建议:

报告人签名:

附件 4：

网络与信息安全应急处理指南

1、网站、网页出现非法言论事件紧急处置措施

(1)网站、网页由主办部门的值班人员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,值班人员应立即向本单位信息安全负责人通报情况;

(3)信息安全相关负责人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。

(4)追查非法信息来源,并将有关情况向本单位网络领导小组办公室汇报。

(5)信息化领导小组办公室召开小组成员会议,如认为事态严重,则立即报局网络与信息安全应急协调领导小组或向公安部门报警。

2、黑客攻击事件紧急处置措施

(1)当有关值班人员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，应立即向信息安全负责人通报情况。

(2)信息安全相关负责人应在接到通知后立即赶到现场，并首先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信息化领导小组办公室汇报。

(3)对现场进行分析，并写出分析报告存档。

(4)恢复与重建被攻击或破坏系统。

(5)信息化领导小组办公室召开小组成员会议,如认为事态严重,则立即报局网络与信息安全应急协调领导小组或向公安部门报警。

3、病毒事件紧急处置措施

(1) 当发现有计算机被感染上病毒后,应立即向信息安全负责人报告，将该机从网络上隔离开来。

(2) 信息安全相关负责人员在接到通报后立即赶到现场。

(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,应立即向本单位信息化领导小组办公室报告，并迅速联系有关产品商研究解决。

(5) 信息化领导小组成员经会商，认为情况严重的，应立即报局网络与信息安全应急协调领导小组或向公安部门报警。

(6) 如果感染病毒的设备是主服务器,经本单位信息化领导小组办公室同意，应立即告知各下属单位做好相应的清查工作。

4、软件系统遭破坏性攻击的紧急处置措施

重要的软件系统平时必须做好备份工作，并将它们保存到安全的地方；一旦软件遭到破坏性攻击，应立即向信息安全负责人报告，并将该系统暂停运行；信息安全负责人要认真检查信息系统的目志等资料，确定攻击来源，并将有关情况向本单位信息化领导小组办公室汇报，再恢复软件系统和数据；信息化领导小组办公室召开小组成员会议，如认为事态严重，则立即报局网络与信息安全应急协调领导小组或向公安部门报警。

5、数据库安全紧急处置措施

主要数据库系统应做多个数据库备份；一旦数据库崩溃，值班人员应立即启动备用系统，并向信息安全负责人报告；在备用系统运行期间，信息安全工作人员应对主机系统进行维修并作数据恢复。

6、广域网外部线路中断紧急处置措施

(1) 广域网线路中断后，值班人员应立即向信息安全负责人报

告。

(2)信息安全相关负责人员接到报告后，应迅速判断故障节点，查明故障原因。

(3)如属我方管辖范围，由信息安全工作人员立即予以恢复。

(4)如属电信、网通、联通部门管辖范围，立即与其维护部门联系，要求修复。

7、局域网中断紧急处置措施

设备管理部门平时应准备好网络备用设备，存放在指定的位置。局域网中断后，信息安全相关负责人员应立即判断故障节点，查明故障原因，有必要时并向网络安全组组长汇报。

如属线路故障，应市政府信息中心或相关通讯部门重新安装线路。

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。

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。

8、设备安全紧急处置措施

如果服务器等关键设备损坏后，值班人员应立即向信息安全负责人报告。信息安全相关负责人员要立即查明原因。如果能够自行恢复，应立即用备件替换受损部件。如属不能自行恢复的，
立即与设备提供商联系，请求派维护人员前来维修。如果设备一时不能修复，应向本单位信息化领导小组办公室汇报。