网站故障恢复与应急预案

为妥善应对网站处置信息安全突发事件，确保网站和重要信息系统的安全可靠运行，特制定本应急预案。

一、网络与信息安全组织机构

网络与信息安全领导小组

主要领导：

分管领导：

网络技术维护人员：

网络安全员：

二、应急处置措施

（一）网站、网页出现非法言论时的紧急处置措施

1、网站、网页由网络技术维护人员随时密切监视信息内容。每天上、下午不少于二次。

2、发现网上出现非法信息时，网络技术维护人员应立即登录后台，上传更新原始页面。

3、网络安全员应妥善保存有关记录及日志或审计记录。

4、网络技术维护人员和网络安全员会商后，将有关情况向安全领导小组领导汇报。

5、安全领导小组召开安全领导小组会议，如认为情况严重，应及时向有关上级机关和公安部门报警。

（二）黑客攻击时的紧急处置措施

1、当网络技术维护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,应立即向网络安全员通报情况。

2、网络安全员应在十分钟内与省信息中心取得联系，首先应将被攻击的服务器等设备从网络中隔离出来，保护现场，同时向安全领导小组副组长汇报情况。

3、网络技术维护人员和网络安全员负责被破坏系统的恢复与重建工作。

4、网络安全员协同有关部门共同追查非法信息来源。

5、安全领导小组会商后，如认为情况严重，则立即向公安部门或上级机关报警。

（三）病毒安全紧急处置措施

1、当发现计算机感染有病毒后，应立即将该机从网络上隔离出来。

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，同时进行病毒检测软件对其他机器进行病毒扫描和清除工作。

4、如发现反病毒软件无法清楚该病毒，应立即向安全小组负责人报告。

5、安全小组相关负责人员在接到通报后，应在十分钟内赶到现场。

6、经技术人员确认确实无法查杀该病毒后，应作好相关记

录，同时立即向安全领导小组副组长报告，并迅速联系有关产品商研究解决。

7、安全领导小组经会商后，认为情况极为严重，应立即向公安部门或上级机关报告。

8、如果感染病毒的设备是服务器或者主机系统，经领导小组组长同意，应立即告知各下属单位做好相应的清查工作。

（四）软件系统遭受破坏性攻击的紧急处置措施

1、重要的软件系统平时必须存有备份，与软件系统相对应的数据必须有多日备份，并将其保存于安全处。

2、一旦软件遭到破坏性攻击，网络技术维护人员和网络安全员应将系统停止运行。

3、网络安全员和网络技术维护人员负责软件系统和数据的恢复。

4、网络安全员和网络技术维护人员检查日志等资料，确认攻击来源。

5、安全领导小组认为情况极为严重的，应立即向公安部门或上级机关报告。

（五）数据库安全紧急处置措施

1、各数据库系统要至少准备两个以上数据库备份，平时一份放在机房，另一份放在另一安全的建筑物中。

2、一旦数据库崩溃，应立即向网络安全员报告，同时通知各下属单位暂缓上传上报数据。

3、网络安全员和网络技术维护人员应对主机系统进行维修，如遇无法解决的问题，立即向上级单位或软硬件提供商请求支援。

4、系统修复启动后，将第一个数据库备份取出，按照要求将其恢复到主机系统中。

5、如因第一个备份损坏，导致数据库无法恢复，则应取出第二套数据库备份加以恢复。

6、如果两个备份均无法恢复，应立即向有关厂商请求紧急支援。

（六）广域网外部线路中断紧急处置措施

1、广域网主线路中断后，网络安全员应立判断故障节点，查明故障原因后，尽快与其他相关领导和工作人员研究恢复措施，并立即向安全领导小组汇报。

2、如属我方管辖范围，由网络技术维护人员协同网络安全员立即予以恢复。如遇无法恢复情况，立即向有关厂商或者省信息中心请求修复。

3、经安全领导小组同意后，应通告各下属单位相关原因，并暂缓上传上报数据。

（七）局域网中断紧急处置措施

1、局域网中断后，网络技术维护人员和网络安全员应立即判断故障节点，查明故障原因，并向安全领导小组副组长汇报。

2、如属线路故障，应重新安装线路。

3、如属路由器、交换机等网络设备故障，应立即更换备用设备并设备提供商联系，并调试畅通。

4、如属路由器、交换机配置文件破坏，应迅速按照要求恢复或重新配置，并调试畅通。如遇无法解决的技术问题，立即向上级单位或有关厂商请求支援。

5、如有必要，应向安全领导小组组长汇报。

（八）设备安全紧急处置措施

1、小型机、服务器等关键设备损坏后，网络技术维护人员和网络安全员应立即查明原因。

2、如果能够自行恢复，应立即用备件替换受损部件。

3、如果不能自行恢复的，立即与设备提供商联系，请求派维修人员前来维修。

4、如果设备一时不能修复，应向安全领导小组领导汇报，并告知各下属单位，暂缓上传上报数据。

（九）人员疏散与机房灭火预案

1、一旦机房发生火灾，应遵照下列原则：首先保人员安全；其次保关键设备、数据安全；三是保一般设备安全。

2、人员疏散的程序是：机房值班人员立即按响火警警报，并通过 119 电话向公安消防请求支援，所有人员戴上防毒面具，所有不参与灭火的人员按照预先确定的线路，迅速从机房中撤出。

3、人员灭火的程序是：首先切断所有电源，灭火值班人员戴好防毒面具，从指定位置取出泡沫灭火器进行灭火。

（十）外电中断后的设备

1、机房将所有服务设备接入 UPS。当电源系统发生故障时，系统将由 UPS 供电。

2、机房值班人员应立即查明原因，并向值班领导汇报。

3、如因单位内部线路故障，请单位服务部门迅速恢复。

4、如果是供电局的原因，应立即与供电局联系，请供电局迅速恢复供电。

5、如果供电局告知需长时间停电，应做如下安排：

（1）预计停电 4 小时以内，由 UPS 供电。

（2）预计停电时间超过 4 小时，由网络技术维护人员等手工关掉所有设备，确保机器正常关机。

（十一）关键人员不在岗的紧急处置措施

1、对于关键岗位平时应做好人员储备，确保一项工作有两人能操作。

2、一旦发生关键人员不在岗的情况，首先应向值班领导汇报情况。

3、经值班领导批准后，由备用人员上岗操作。

4、如果备用人员无法上岗，请求上级单位支援。