中国地质大学（北京）

信息网络中心文件

信息网络中心　　2013.10.15

违法有害信息处理应急预案

一、预案目的

为了保障我校网站及各类信息系统遇到突发性事件时能够尽快恢复受影响的服务，最大化的减少突发事件给我校信息安全所带来的损失，维护学校正常的工作和生活，结合校园信息安全实际情况，特制订我校信息安全突发事件应急预案。

二、适用范围

1、校园网主页受攻击被篡改，出现非法政治标语、出现黄赌毒等违法信息等。

2、二级部门主页受攻击，出现非法政治标语、出现黄赌毒等违法信息等。

3、各类应用系统被攻击，出现不能服务或者服务出错情况。

4、出现师生身份相关信息泄露，师生密码等关键信息被

盗等。

三、组织机构

信息网络中心是本预案的工作执行机构，为具体执行部门，网络故障应急小组包括网络、线缆、主要服务器等相关人员。

组长：黄维平　电话：13911716950 职责：接到紧急报告后，召集小组成员，全面负责应急恢复工作。

副组长：于磊电话：15801381953 职责：负责具体协调、组织小组成员参与应急工作。

成员：吴志远电话：13439879791 职责：负责校园主页与数据库信息安全。

成员：苏荣　电话：13683360640 职责：负责托管信息网络中心二级部门主页与学工系统安全。

成员：魏纬　电话：13520925683 职责：负责 CMS 系统及信息网络中心管理的二级部门主页。

成员：刘嫚　电话：13683360640 职责：负责人事系统安全。

四、应急流程

目前我校各网站、应用系统的管理均设有严格授权，管理员定期会修改管理密码，即对于管理员上传的文件信息具有可追可查。同时管理员的选择也是挑选政治合格、技术过

硬的人员，应该说从管理上基本杜绝了管理员恶意上传违法有害信息的情况。

根据违法有害信息危害特点，本着违法有害信息处理无小事，只要网站和信息系统出现违法有害信息时，处理流程如下：

（1）根据故障现象通知相关负责老师进行处理，

（2）相关负责老师记录备案，做出故障信息传递上报故障小组组长。

（3）根据故障原因进行判断故障点，会同相关单位提出解决方案。

（4）提交故障说明，突发事件处理结束后，组织相关技术人员总结事件发生的故障原因，成技术文档，最后以文字形式提交单位。

具体故障排除按照以下流程进行操作：

1、校园网主页应急流程

校园网主页包含主页网站、单点登录、LDAP等组成，按照构成分为网站和相应的软件系统，具体处置措施如下：

网站受攻击时应急流程

当发现网站被攻击时，如访问速度慢、网页内容被篡改、系统不稳定等情况

（1）检查校园网运行状态，排除因网络故障引起的不正常情况

（2）立即将被攻击的服务器等设备从网络中隔离出来，同时向领导汇报情况。

（3）将重要数据从被攻击服务器中备份到其他介质上，启用反病毒软件对这些数据进行杀毒处理，如发现反病毒软件无法清除病毒，应立即向领导报告

（4）分析日志文件，查找网站被攻击的原因；如果是操作系统漏洞，对操作系统进行补丁升级，修复系统漏洞；如果是软件系统漏洞，查询相似的被攻击情况和解决方案，进行修补工作

软件系统遭受破坏性攻击应急流程

（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，并将它们保存于安全处。

（2）立即向技术人员、网络管理员报告，并将系统停止运行。

（3）启动备用网站系统，立即进行软件系统和数据的恢复，尽量减小学校网站的对外服务宕机时间。

（4）查找软件遭受破坏性攻击原因，一旦查明，找出解决方案，并记录在案。

2、二级部门主页应急流程

二级部门主页根据管理方式不同，分为信息网络中心管理、委托信息网络中心管理和自建自管三种，根据管理模式不同，分为如下应急流程：

信息网络中心管理二级网站应急流程

（1）值班人员发现二级部门主页遭到攻击后立刻通知相关负责老师进行处理。负责人：魏玮，电话：13520925683。

（2）负责老师到场后，首先检查被攻击对象，根据具体情况进行处理：

1） 网站网页被篡改

a）立刻在 cms 中停止被篡改站点，重新发布该网站，并尽快将网站重新投入使用；

b）妥善保存有关记录及系统日志等信息；

c）如需追查非法信息，立刻联系相关负责老师追查信息来源；

d）及时将有关情况向网络应急小组组长和副组长汇报，认为情况比较严重的，由领导小组会商后，上报公安部门。

2） 服务器被攻击或感染病毒

a）先将被攻击的服务器从网络中隔离出来；

b）启用反病毒软件进行杀毒处理；

c）通过日志等记录，分析攻击原因，查找安全漏洞，

尽快解决，必要时修改服务器密码，尽快恢复服务器正常运行；

d) 如果情况严重至服务器瘫痪，可重建虚拟机，联系康邦公司，重新部署应用系统；导入备份数据，恢复二级部门网站。

康邦公司联系人：申慧颖，电话：15810623872。

e) 及时将有关情况向网络应急小组组长和副组长汇报，认为情况比较严重的，由领导小组会商后，上报公安部门。

3) 数据库被攻击

a) 立刻联系数据库负责人和 cms 负责人；

数据库负责人：吴志远，电话：13439879791。

cms 负责人：魏玮，电话：13520925683。

b) 如果数据库崩溃，通知二级单位暂缓上传数据；

c) 查找异常数据，使用备份数据进行数据恢复；

d) 分析有关记录及系统日志，查找和解决漏洞；

e) 及时将有关情况向网络应急小组组长和副组长汇报，认为情况比较严重的，由领导小组会商后，上报公安部门。

3、应用系统应急流程

(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，并将它们保存于安全处。

(2)立即向应用系统管理员报告，并将系统停止运行，

应用系统管理员联系方式见表3。

(3)启动备用应用系统，立即进行软件系统和数据的恢复，尽量减小我校软件系统的对外服务宕机时间。

(4)查找软件遭受破坏性攻击原因，一旦查明，找出解决方案，并记录在案。

(5)及时向上级主管部门报告，对造成用户信息泄露的，及时向公安部门报案。

表3 软件系统管理员联系方式

软件名称	相关联系人	联系方式	备注
人事系统	刘嫚	13683543105	
学工系统	苏荣	13683360640	
科研系统	刘嫚	13683543105	
教务系统	刘嫚	13683543105	
数字校园	吴志远	13439879791	
一卡通	郝日青	13717845108	