中国地质大学（北京）

信息网络中心文件

信息网络中心　　2015.3.1

中国地质大学（北京）网络突发事件应急预案

一、预案目的

为了保障校园网络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校园网络所带来的损失，维护学校正常的工作和生活，结合校园网实际情况，特制订校园网络突发事件应急预案。

二、适用范围

1.校园网络设备故障导致网络中断，接入商 ISP 光纤线路意外中断。

2.DNS、认证服务器、计费服务器故障导致的网络故障。

3.校园主页篡改及应用程序故障，数据库故障等。

4、其它原因引起的信息网络故障。

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。

序号	角色	姓名	电话	职责

1	组长	黄维平	13911716950	接到紧急报告后，召集小组成员，全面负责应急恢复工作。
2	副组长	于磊	15801381953	负责具体协调、网络核心设备调试、恢复，ISP 故障相关联系等工作。
3	成员	刘全	13693119892	负责线缆及各楼宇机房相关工作
4		程印乾	13466717692	负责网关认证系统恢复工作
5		梁洁胜	13811158520	宿舍区及外围测试
6		吴志远	13439879791	负责校园主页与数据库信息安全
7		郝日青	13717845108	负责一卡通系统运行与维护
8		冯家刚	18608718312	负责数据灾备与恢复，安全处理日志记录分析
9		魏玮	18608718312	CMS 安全管理、日志记录分析
10		苏荣	18608718312	二级单位托管网站安全管理、日志记录分析

四、故障范围定义及故障影响范围

信息网络中心对突然发生的网络故障，按照学校对正常办公、教学、服务影响，划分为：严重（I 级）、重大（II 级）、一般（III 级）

1、I 级网络故障

故障定义：网络核心设备损坏、接入商 ISP 光纤线路意外中断、DNS 或认证服务器故障、校园主页遭篡改。

处理流程：

（1）值班人员根据故障现象通知相关责任人进行处理，

（2）相关责任人记录备案，做出故障信息传递上报故障组长。

（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：

- **网络核心设备损坏**

处理流程：

（1）值班人员发现核心设备报警、损坏后，立即报告网络应急组长和副组长。组长立即召集相关人员到场。

（2）相关人员到场后，根据现场情况，判断设备损坏程度，如果是配置文件等软件故障，立即分析配置，从备份系统中恢复相应配置，恢复服务。

（3）如果发现硬件故障，立即启动备用设备，并且根据现有配置对新设备进行配置导入，根据对应端口将各个楼宇汇聚设备插入到相应端口。同时联系设备供应商，提供技术支持并且启动保修程序，尽快将故障设备送检送修。

- **接入商 ISP 光纤线路意外中断**

处理流程：

（1）值班人员发现出口流量中断后，立即报告网络应急小组组长和副组长。组长立即召集相关人员到场。

（2）查看网络出口流量负载均衡设备，按照既定策略，

将故障 ISP 流量调整到其他备份线路。

（3）立即联系故障 ISP 相关负责人，双方确定事故类型，并按照以下程序处理：

如果是光纤模块故障，立即更换新光纤模块。

如果是光芯故障，和 ISP 双方同时调整到另外一对光芯。

如果是整个光纤完全断开，立即联系熔接光纤。

如果是连接设备故障，立即更换设备。

各个出口 ISP 负责人及光纤熔接联系人方式如下：

ISP 名称	联系人及电话	职务	备注
中国联通	石磊 18610116622 谢奇 13910900174	副总 技术售后	
中国电信	朱红侠 13370166092 保修 010-58504000	客户经理 保修电话	
电信通	支欣 13810778855 罗元茹 18601963633	客户经理 客服经理	
教育网	北京邮电大学网络中心 张晓东 62283042 13520211171	北邮网络中心	
华成时代公司	朱彦龙 13811914608 刘勇 13911559124	客户经理 工程经理	光纤熔接

- **DNS、认证服务器出现故障或受到攻击导致全校无法上网**

处理流程：

（1）值班人员发现 DNS 或者认证服务器出现故障后，立即报告网络应急小组组长和副组长。组长立即召集相关人员

到场。

（2）DNS 故障处理流程：首先重启服务，如果故障依旧，重启服务器，如果故障依旧，立即开启虚拟机备份 DNS 服务器，修改 IP 地址，启动 DNS 服务。用虚拟化 DNS 备用服务器提供服务。

（3）认证服务器故障处理流程：目前认证服务器为一台在线服务器和一台冷备服务器的方式，两台服务器的设置完全一样。如果在线主机出现故障，立即启动备份主机，并将光纤从故障主机上拔插到备份服务器上，保证服务尽快恢复。

- **校园主页遭篡改**

处理流程：

（1）值班人员发现校园主页被篡改，立即报告网络应急小组组长和副组长。组长立即召集相关人员到场。

（2）立即将被攻击的主页服务器等设备从网络中隔离出来，对重要数据进行备份。

（3）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。

（4）向上级主管单位汇报攻击以及处理情况，向公安部门报告整个事件过程，配合公安部门查处。

2、II 级网络故障

故障定义：楼宇网络设备故障、计费系统故障、校园网及应用系统故障

影响范围：故障发生所在楼宇全部网络、某个重要业务功能不能使用

处理流程:

（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，作出故障信息传递，2 小时内解决故障

具体故障排除按照以下流程进行操作：

- **一卡通服务器出现故障导致全校无法正常使用一卡通**

处理流程：

（1）值班人员发现一卡通 Web 查询系统或圈存机各项服务无法正常使用时，立即报告网络应急小组组长和副组长。组长立即召集相关人员到场。

（2）一卡通服务器故障处理流程：如果 Web 查询、银校或圈存某个子系统无法正常使用、而一卡通主系统运行正常，则对应子系统服务器故障，需重启相应子系统服务器和应用程序，若故障依旧，技术人员需立即修复相关服务器；如果一卡通主管理系统和各子系统均无法正常使用，则一卡通中心服务器故障，需首先重启一卡通应用程序，如果故障依旧，应立即切换服务到备用服务器，避免长时间服务中断，同时技术人员应立即修复故障服务器。

- **楼宇网络设备故障**

值班人员从运维系统发现各楼宇交换机出现故障后，立即报告网络应急小组组长和副组长。组长立即召集相关人员到场。

（1）如果设备可以远程登录，立即查询交换机日志，分析故障原因，常见故障原因有：网络攻击，查明攻击源并处理，端口模块或光纤链路故障，需及时更换模块或者链路，无法自行处理的，联系厂商工程师远程或者现场处理。

(2)若无法远程登录，需赶往机房现场分析原因，一般故障解决方案如下：

楼宇机房断电：立即联系后勤电工检查线路。

光纤故障：如果光芯故障，立即换成另外一对光芯。如果整条光缆意外损坏，立即联系熔接公司，进行光缆检测、熔接。

设备故障：如果重启或者修改配置都无法解决问题则可能设备硬件出现故障，立即在学十九楼备件库中查找同型号设备进行更换，同时联系售后公司给予技术支持和维修支持。

设备品牌	相关联系人	职务	备注
Cisco 产品	户兰香 18611373622 肖庄林 18510482890	副总经理 工程师	
H3C 产品	赵炳辉 13366245566 朱彦龙 13811914608	厂家销售 华成售后	
光缆故障	朱彦龙 13811914608 刘勇 13911559124	客户经理 工程经理	
深澜计费	郑晓来 18910180222 邱瑞 13683093263	技术经理 售后技术	

- **计费系统故障**

（1）.判断计费系统是否受到网络攻击，如果受到网络攻击，执行以下步骤：

A) 根据日志查找攻击源。

B) 调整防火墙策略，加强计费系统安全性。

（2）.如计费系统问题源于自硬件损坏，执行以下步骤：

A)启动备用服务器。

B)将计费系统数据库远程备份文件从 202.204.105.228 服务器拷贝至备用服务器。

C)计费系统数据库恢复。

D)计费系统上线。

- **校园网及应用系统故障**

（1）校园网站受攻击时的紧急处置措施

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，首先检查校园网运行状态，排除因网络故障引起的不正常情况，同时立即将被攻击的服务器等设备从网络中隔离出来，并且向领导汇报情况。

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

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。

(2) 软件系统遭受破坏性攻击的紧急处置措施

A)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。

B)立即向技术人员、网络管理员报告,并将系统停止运行。

C)启动备用网站系统，立即进行软件系统和数据的恢复。尽量减小我校软件系统的对外服务宕机时间

D)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。

以下是各软件系统的负责人员名单和联系方式

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	
邮件系统	冯家刚	18515219312	
VPN 系统	冯家刚	18515219312	
数字校园	吴志远	13439879791	
一卡通	郝日青	13717845108	

(3)硬件故障的紧急处置措施

A)一旦硬件故障，应立即向技术人员、网络管理员报告，并将系统停止运行。

B)启动备用服务器，立即进行网站系统的恢复，尽量减小学校网站的对外服务宕机时间

C)联系厂家硬件维修

(4)数据库安全紧急处置措施

A)各数据库系统要至少准备两个以上数据库备份。

B)一旦数据库崩溃，应立即向技术人员报告，同时暂缓上传数据。

C)利用数据库备份，恢复数据库

D)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。

E)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

3、III 级网络故障

（1）故障定义：楼层接入或者汇聚设备出现故障、楼层设备间或机柜电源出现故障、无线接入 AP 发生故障

影响范围：故障发生所在楼层网络、单个无线接入 AP 点所辐射范围

处理流程：

（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，作出故障信息传递，2 小时内保证解决故障

处理流程

- 楼层接入或汇聚设备出现故障

远程登陆处理相应故障

如不能解决，到达现场重启设备

如设备重启不生效，则启用相同型号的备用设备替换

- 单个无线接入 AP 发生故障

通过无线网总控制器配合无线网管理软件对该 AP 进行设置

如不能解决，到达现场重启 AP

如 AP 重启不生效，则启用相同型号的备用 AP 替换

- 电源出现故障

到达现场接通电源如不能处理,则联系学校后勤处节能与动力科。

节能与动力科联系电话：82321499

五、监控与预警

1、加强网络监控制度，做到“早发现、早报告、早处置”的原则。

2、监控网络设备、线路、系统的运行情况，并做好巡视、检查工作记录

3、值班人员岗前培训，建立完善的值班制度。

4、发生故障后的报告制度，逐级上报制度。

六、善后处置

突发事件处理结束后，要及时总结事件发生的原因，并提出相应的整改意见，预防同类事件的再次发生。

本预案发布之日起实施。