中国地质大学（北京）

信息网络中心文件

信息网络中心　　2020.9.21

中国地质大学（北京）网络安全事件管理规范

第一章　总　则

第一条　为规范和加强中国地质大学（北京）网络安全事件的管理工作，保障基础信息网络和重点信息系统安全，遵循“以安全保发展，在发展中求安全”和“积极防御，综合防范”的指导方针，特制定本规范。

第二条　本规范所称网络安全事件，是指由于自然或者人为的原因，在我中心所维护、管辖内发生的造成信息泄露人或经济损失以及严重、产生影响的事件。

第三条　为提高中国地质大学（北京）网络安全事件通报和应急处理的效率和效果，利于安全事件的统计分析和严重程度的确定，根据国家网络安全事件等级处理方法，对安全事件进行等级划分。

第四条　为提高中国地质大学（北京）应对突发网络安全事件的组织指挥能力和应急处置能力，结合实际情况，制定网络安全事件处理流程。

第五条　本规范适用中国地质大学（北京）信息系统的网络安全应急处理工作。

第二章　管理机制

第六条　设立网络安全保障组，为中国地质大学（北京）信息网络中心处理网络安全突发事件应急工作的综合性议事、协调机构；主要职责是：

1. 按照国家网络安全等级保护的要求开展处置工作；

2. 研究决定中国地质大学（北京）的网络安全等级保护和应急工作的有关重大问题；

3. 决定网络安全突发事件应急预案的启动，组织力量对突发事件进行处置。

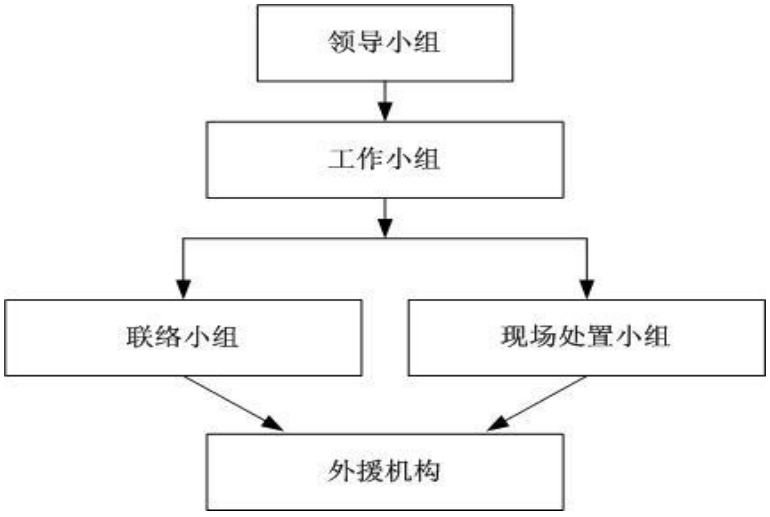

图 1 网络安全保障组人员构成

第七条　中国地质大学（北京）网络安全保障组各小组的职责：

1. 领导小组职责：协调推进中国地质大学（北京）网络与网络安全应急机制和工作体系建设，对有关事项做出重大决策，组织和调度必要的人、财、物等资源。

2. 工作小组职责：研究拟定网络与网络安全应急处置工作的规划、计划和政策，督促检查相关部门和网络安全专项应急预案的执行情况，确保安全策略的制定与执行；组织培训和演练；紧急情况启动应急预案。

3. 联络小组职责：负责及时通报重大紧急事件、定期了解外援机构的变动情况，及时更新其技术人员及联系方式等信息；向各工作组传达领导小组的工作指令；收集各工作组工作进展情况，并及时向领导小组报告和向相关部门通报。

4. 现场处置小组职责：识别网络与信息系统正常运行的主要威胁，进行现场处理；检查威胁造成的结果，评估事件带来的影响和损害；快速响应发现的网络故障事件；执行网络故障的诊断、排查和恢复操作；定期通过网管软件、网络运行报告等工具对网络的使用情况进行分析，尽早发现网络的异常状况，排除网络隐患。

5. 外援机构职责：负责提供紧急情况下的应急技术方案和应急技术支援体系；积极配合现场实施人员进行故障处理。

第八条 负责网络安全事件的报告，安全事件分类定级，应急响应等具体工作，主持应急预案与各项安全管理制度的制定、修改和维护工作。

第九条 建立外部专家、第三方服务单位、领导机关的联系名单，通过定期召开会议和各种联系方式，保证信息及相关工作人员的沟通畅通。

第三章 安全事件分类分级

第十条 网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等 7 个基本分类。

第十一条 针对中国地质大学（北京）信息系统中可能存在的对网络和信息系统有重大影响的事件，根据故障发生后的影响规模和范围、影响程度、影响持续时间、是否需要调用备用资源等要素，进行事件风险分析，确定事件故障等级，进而采取相应的故障控制措施。中国地质大学（北

京）网络和信息系统的故障可划分为四级，针对不同等级的故障启动不同级别的应急方案。

1. 一级事件：规模大、范围广、影响持续时间长（比如发生不可预见的灾难性事故，如：火灾、水灾和地震等）；网络发生大规模瘫痪，事态发展超出中国地质大学（北京）的控制能力。

a）造成全网 5 分钟以上网络中断等事件；

b）造成中国地质大学（北京）网络核心和汇聚节点网络设备整机、机房服务器和基础设施（如 UPS、空调等）停止运行的事件；

2. 二级事件：规模较大、范围较广；影响持续时间较长；本地无备用资源，需从设备供应商或设备维护商紧急调用备件；造成严重损害，需要跨部门、跨地区，在中国地质大学（北京）领导协调下，协同处置的突发公共事件。

a）核心节点网络设备部件失效；

b）核心层网络光缆链路中断；

c）重要信息系统（网络安全等级三级及以上）故障或遭受攻击；

3. 三级事件：范围较小、突然发生、影响持续时间较短；造成中国地质大学（北京）校内（多个部门）无法正常使用网络和信息系统；但可以采取临时措施恢复网络畅通。

a）汇聚层节点网络设备部件失效；

b）汇聚层网络链路中断；

c）网络安全等级三级以下，非面向公众服务的系统出现故障或遭受攻击；

d）跨部门区域范围内群体终端计算机中毒，或无法正常使用。

4. 四级事件：范围小；影响信息系统或较少的网络用户；影响持续

时间短；本地有备用资源，或虽无备用资源，但可以采取临时措施恢复网络畅通；不需要跨部门、跨地区协同处置的突发事件。

第四章　应急启动流程

第十二条　根据以上定义的事件分级，当安全事件的要素满足启动应急预案要求时，进入相应的应急启动流程，实行分级响应：

1.　现场处置小组从用户的故障申告、检测得知网络安全事件后，应在第一时间赶赴网络故障现场。

2. 现场处置小组针对故障事件做出初步的分析判断。若是电源接触不好、物理连线松动、操作系统故障或者能在最短时间内自行解决的软件问题，及时按照有关操作规程进行故障处理；否则，现场处置小组将故障大致定性为设备故障、线路故障、信息系统故障等三种故障之一，及时告之联络小组，并采取措施避免事件影响范围的扩大。

3. 联络小组向工作小组报告，在工作小组的授权后启动相应的应急预案；针对灾难性、网站域名被劫持的一级事件和影响重要业务运行的二级事件，还要及时向上级机关进行报告。

4. 现场处置小组根据故障类型及时与外援机构取得联系：其中，设备故障的，可与网络设备维护商和主机设备维护商联系或查看设备的备份情况，要求设备维护商在尽可能短的时间内将备件送达故障现场；信息系统故障的，应与系统维护商联系，由系统维护商进行现场或远程技术支持；线路故障的，可与网络运营商联系，密切协作力求通信线路在短时间内恢复正常。

5. 现场处置小组在上级机构或外援机构的配合下，充分利用应急预案的资源准备，采取有力措施进行故障处理，及时恢复网络的正常通信状

态和信息系统的正常运行。

6. 联络小组通知业务部门网络或系统恢复正常，并向工作小组报告故障处理的基本情况；重大事件形成文字资料，以书面形式报告给上级机构。

7. 现场处置小组总结整个处理过程中出现的问题，认真填写网络安全事件处理结果备案表进行备案，并及时改进应急预案。

第五章　安全预防制度

第十三条　实行安全责任制；中国地质大学（北京）网络安全和信息化工作领导小组对中国地质大学（北京）网络安全工作负总责，安全管理员对运行系统安全工作负责，其他工作人员也均有维护信息系统安全的责任和义务。

第十四条　实行安全管理员制度。配备安全管理员，安全管理员要保持相对稳定，确需变动的要及时补报；安全管理员要及时了解安全工作情况，迅速传达上级有关安全工作的指示精神和要求，定期向主管领导汇报安全工作情况。

第十五条　实行安全教育制度，定期或不定期举办“安全教育活动”，采取多种形式和手段开展安全教育；充分利用各种活动课程，有计划地对工作人员进行安全预防教育，使他们接受比较系统的网络安全知识教育，切实增强中国地质大学（北京）全员的安全意识和安全防护能力。

第十六条　实行安全工作巡查制度，领导每月组织进行一次安全检查，同时还要根据特定情况不定期组织检查；检查内容包括；对安全工作是否重视，各种规章制度是否健全，措施是否得力有效并得到落实，各种设施设备是否有安全隐患等；检查应认真仔细，发现问题，及时处理，消

除隐患。

第十七条 实行应急演练制度；中国地质大学（北京）应定期组织演练，模拟处置影响较大的网络安全事件，检验预案的可执行性，提高全员素质和抗事故的能力。

第六章 保障措施

第十八条 技术支撑保障：

信息网络中心筹建预警与应急处理的技术平台，进一步提高安全事件的发现和分析能力：从技术上逐步实现发现、预警、处置、通报等多个环节和不同的网络、系统、部门之间应急处理的联动机制。

第十九条 应急队伍保障：

1、 信息网络中心不断加强应急管理队伍建设，加强网络安全人才培养，强化网络安全宣传教育，建设一支高素质、高技术的网络安全核心人才和管理队伍，提高中心网络安全防御意识。

2、 专业安全外包运维人员为我委的应急保障提供专业的技术支撑，保障信息系统安全，加强网络安全应急处置能力。

第二十条 物资条件保障：

1、 信息网络中心安排专项资金用于预防或应对网络安全突发事件，提供必要的经费保障，强化网络安全应急处理工作的物资保障条件。

2、 网络和信息系统故障的恢复需依靠一定的资源，主要包括人力资源、物力资源和文档资料等。应立足现有条件，以尽可能少的投资和现有的设备达到应急恢复网络通信的要求：

a) 人力资源：平时至少两名网络管理员保障信息系统网络安全，在可能的情况下使更多的技术人员掌握通信网络的基本知识；保障每个信

息系统有一名负责人。

b）物力资源：现在库存的设备、部门中其他机构使用的设备，确保相似或兼容的设备可以由现场处置小组在应急情况下调配使用。

c）外援力量：网络设备维护商可以在发生设备故障时保证网络通信的及时恢复；设定供应商应该在得到通知后多长时间必须进行响应。

d）文档资料：包括网络系统工程文档、网络系统维护手册、网络系统操作手册、网络设备配置参数、网络系统拓扑图以及 IP 地址规范及分布情况等；另外，网络管理员的账号和口令定期更新后，也应整理成文档。

e）实物标示：路由器、交换机、防火墙、配线架、机架和服务器等应事先作好相关标记，注明槽位、端口的物理布线情况，并在进行线路调整后及时更新记录；对网络通信设备和服务器应事先制作好服务卡片，记录：设备名称、设备型号、设备 IP 地址、设备供应商、系统集成商、网络运营商、使用人员、维护人员及其联系方式等信息。

第二十一条 技术储备保障：

信息网络中心筹建并组织有关专家和科研力量，开展应急运作机制、应急处理技术、预警和控制等研究，组织参加相关培训，推广和普及新的应急技术。

第七章　应急演练

第二十二条 应急演练目标：

1、 根据制定的应急演练工作计划，完成应急演练的准备、计划、实施以及分析工作，保证演练工作的技术性，体现演练工作的价值。

2、 通过应急演练，考察网络和业务系统抵抗外部攻击的能力，反映在发生突发的安全事件时，安全应急体系是否有效运转并发挥积极作用，能否在最短的时间内有效地解决安全事件。

第二十三条 应急演练的策略：

1、安全事件应急演练应该按照如下策略进行：

a）分重点、分层次、分系统、分阶段进行应急演练。

b）实施演练要先易后难，逐步积累经验。

c）重视作为应急基础的资源条件的就绪状态。

d）尽量做到实施演练的突然性。

2、应急演练的要求：

在开展信息系统应急演练的实际工作中，除了要遵循上述演练的策略和原则外，还要遵循应急演练工作的一般性要求，综合考虑各种可能因素，与业务部门进行认真的沟通，制定详细的演练方案，保证演练的顺利进行。

a）演练不能影响正常生产，这是对演练工作的基本要求。

b）演练必须是可控的。

c）演练应当尽量接近真实。

第二十四条 实施步骤：

根据制定的安全应急演练工作计划：

1、 申请准备阶段：

选定预案演练的范围。提交应急演练申请，预测演练风险威胁，提交应急演练的范围、时间及执行者信息，做好应急演练目标系统的备份工作，并制定回复方案，要求整个过程真实但是可控。

2、 第一阶段：事件模拟

根据既定的应急演练方案，在与应急预案中涉及到的所有相关人员，背对背的情况下，制造安全事件。

3、 第二阶段：应急组织评估

在紧急事件发生的同时，考察安全事件应急的组织结构的健全行、协调性、沟通的畅通性和组织成员职责是否明确。

4、 第三阶段：预警机制评估

考察在应急预案的流程中，事件发现的时限是否符合规定，事件预警和监控的渠道是否畅通。

5、 第四阶段：应急事件响应评估

考察相关人员的响应速度，和处理效率。

6、 第五阶段：应急事件处理评价

根据应急事件处理的结果和过程，客观的对预先制定的各个考察点进行评价。

第八章　附则

第二十五条 本规范由中国地质大学（北京）信息网络中心负责解释。

第二十六条 本规范自发布之日起施行。

附件：

1、网络安全事故报告表

2、网络安全事件处理结果备案表

3、网络安全保障组各小组成员及联系方式

网络与网络安全突发事件报送表

编号：

报告时间：_____年___月___日___时___分

<table>
<tr><td>单位名称</td><td></td><td>报告人</td><td></td></tr>
<tr><td>联系电话</td><td></td><td>通讯地址</td><td></td></tr>
<tr><td>传真</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td rowspan="2">突发网络与网络安全事件的客体</td><td colspan="3">名称：</td></tr>
<tr><td colspan="3">用途描述：</td></tr>
<tr><td>突发网络与网络安全事件的简要描述</td><td colspan="3">（1.应包括事件发生时间、发生事故网络信息系统名称及运营使用单位、地点、原因、事件类型及性质、危害和损失程度、影响单位及业务等；2.如以前出现过类似情况也应加）</td></tr>
<tr><td>初步判定的事件类别</td><td colspan="3">☐有害程序事件 ☐网络攻击事件 ☐信息破坏事件 ☐信息内容安全事件 ☐设备设施故障 ☐灾害性事件 ☐事件原因不明 _____</td></tr>
<tr><td rowspan="2">本次突发网络与信息事件的初步影响状况</td><td>事件后果</td><td colspan="2">☐业务中断 ☐系统破坏 ☐数据丢失 ☐其他_</td></tr>
<tr><td>影响范围</td><td colspan="2">☐单台主机 ☐多台主机 ☐整个信息系统 ☐整个局域网 ☐其他_____</td></tr>
<tr><td rowspan="4">事发单位目前掌握的材料</td><td colspan="2">系统结构拓扑图</td><td>☐有 ☐没有</td></tr>
<tr><td colspan="2">系统硬件设备及其配置参数清单</td><td>☐有 ☐没有</td></tr>
<tr><td colspan="2">系统软件设备及其配置参数清单</td><td>☐有 ☐没有</td></tr>
<tr><td colspan="2">应用软件源代码及其配置参数清单</td><td>☐有 ☐没有</td></tr>
</table>

	系统运维记录	□有 □没有
	系统审计日志	□有 □没有
	系统操作权限分配列表	□有 □没有
	单位应急处置人员联系表	□有 □没有
突发网络与网络安全事件的发展趋势		
当前采取的应对措施		

网络安全事件处理结果备案表

编号：

<table>
<tr><td colspan="4">原事件报告报告时间：　　年　　月　　日　　时　　分　　秒</td></tr>
<tr><td colspan="4">备案编号：　　年　　月　　日　　第　　号</td></tr>
<tr><td>报告单位</td><td></td><td>报告人</td><td></td></tr>
<tr><td>联系电话</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td colspan="4">发生网络安全事件的网络与信息系统名称和用途</td></tr>
<tr><td colspan="4">系统是否经过安全评测：　☐ 是　　☐ 否</td></tr>
<tr><td colspan="4">网络安全事件的补充描述及最后评定事故原因：</td></tr>
<tr><td colspan="4">本次安全事件的事后影响状况、事件后果</td></tr>
<tr><td colspan="4">本次安全事件的主要处理过程与结果</td></tr>
<tr><td colspan="4">针对此类事件应采取的保障网络与信息系统安全的措施与建议</td></tr>
<tr><td>备案人（签名）</td><td></td><td>所属部门</td><td></td></tr>
</table>

网络安全保障组各小组成员及联系方式

编号：

1、领导小组

组长：_____

联系电话：_____ 电子邮件：_____

2、工作小组

组长：_____ 部门：_____

联系电话：_____ 电子邮件：_____

部门	成员	联系电话	电子邮件

3、联络小组

组长：_____ 部门：_____

联系电话：_____ 电子邮件：_____

部门	成员	联系电话	电子邮件

4、现场处置小组

组长：_____ 部门：_____

联系电话：_____ 电子邮件：_____

部门	负责人	所负责网络或信息系统	联系电话	电子邮件

5、外援机构

a. 上级单位

上级单位	联系人	单位/职务	移动电话	固定电话

b. 签约合作单位

维护商	所负责网络或信息系统	紧急情况联系人	联系电话	现场处置小组对应人
