北方工业大学文件

校发〔2019〕42号

北方工业大学
网络与信息安全应急处置预案

第一章　总　则

第一条　编制目的

为科学应对网络与信息安全突发事件，提高我校应对突发应急事件的处理能力，有效预防、及时控制和妥善处理利用校园网传播有害信息等突发事件，提高安全事件分级响应和跨部门协同处置能力，减轻或消除突发事件的危害和影响，确保学校网络与信息安全，特制定本预案。

第二条　编制依据

根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》、《教育系统网络与信息安全类突发公共事件应急预案》、《信息安全事件分类分级指南》（GB/T20986-2007）、《中国教育和科研计算机网管理办法》、《北京市网络与信息安全事件应急预案》、《北方工业大学校园网管理规定》、《北方工业大学校园网信息安全管理规定》

第三条　适用范围

本预案所称突发性事件，是指自然因素或者人为活动引发的危害学校信息系统安全等有关的事件。

本预案适用于主体为北方工业大学的网络与信息系统，尤其是校园网主干设施和重要信息系统安全突发事件的应急处置。

第四条　工作原则

（1）积极防御，综合防范

立足安全防护，加强预警，重点保护学校基础信息网络和数字校园信息平台等全校性的重要信息系统，从预防、监控、应急处理和应急保障等环节，在法律、管理、技术等方面，采取多种措施，充分发挥各方面的作用。坚持提前防范，及时排查，争取早发现早报告早解决，化解风险，减少不良影响，共同构筑网络与信息安全保障体系。

（2）统一领导，快速反应

网络安全与信息化工作领导小组统一领导、协调全校网络与信息安全事件应急处置工作，领导小组下设办公室负责应急工作

的日常管理，建立健全应急反应机制，充分发挥专家队伍和专业人员的作用。在网络与信息安全突发事件发生时，按照快速反应机制，及时获取充分而准确的信息，跟踪研判，果断决策，迅速处置，最大程度地减少危害和影响。

（3）明确责任，分级负责

学校各单位要按照“谁主管、谁主办、谁负责”的原则，加强对本单位建立和负责的网络与信息系统的安全管理，强化单位主要领导对网络与信息安全事件的处置职责，分级分类建立和完善安全责任制度、协调管理机制和联动工作机制。

（4）科学决策，快速反应

加强在处置网络与信息安全突发事件中，要根据实际，依法办事，合情合理，把保障学校的安全稳定及维护全校师生的合法权益作为首要任务，防止事态扩大激化。以人为本，提前预防，及时报告，紧密衔接，及时采取措施，迅速处理，最大限度地避免信息资产遭受损失，将事态影响减至最小。

第二章　组织机构和职责

第五条　组织机构

学校成立网络安全与信息化工作领导小组，领导小组的主要职责与任务是统一领导全校信息安全应急工作，在校领导组织指挥下，全面负责学校信息系统可能出现的各种突发事件处置工作，负责组织应急技术支撑队伍做好应急处置的技术支撑工作，协调组织各单位网络与信息安全事件的预防、监测、报告和应急

处置工作。各相关单位在学校网络安全工作委员会统一领导下，建立联动工作机制，密切配合，履行职责。

第六条　工作职责

各相关单位的职责如下:

组织机构	职责
网络安全与信息化领导小组	决定 I 级和 II 级网络与信息安全事件应急预案的启动。 督促检查安全事件处置情况及各有关单位在安全事件处置工作中履行职责情况。 对全校各单位贯彻执行应急处置预案、应急处置准备情况进行督促检查。
党委办公室 校长办公室	组织协调有关部门查处利用计算机网络泄密的违法行为。 牵头组织重大敏感时期、重要活动、重要会议期间发生的信息安全事件的协调处置。
网络安全与信息化中心	负责校园基础网络系统安全。 负责计算机病毒疫情和大规模网络攻击事件的处置。 负责校级网络与信息系统安全事件处置的技术支持。
党委宣传部 团委、 学生工作部（研究生工作部）	负责学校舆情监测，对于涉及师生政治思想方面的倾向性、苗头性问题加强分析研判。 负责学生舆情突发事件的处置、 负责应急处置过程中的舆论处置。
安全稳定工作部	密切配合公安部门，做好网络与信息安全事件的处置工作。 负责及时收集、通报和上报网络与信息安全事件应急处置情况。
其他单位	负责本单位内部的网络与信息安全管理和突发事件应急处置，对照本预案建立单位内部应急处置机制。 配合各单位落实相关应急处置措施。

第三章网络与信息安全事件分类与分级

第七条　网络与信息安全事件分类

根据《信息安全事件分类分级指南》（GB/T20986-2007）规定，网络安全事件分为以下 7 类事件。

（1）有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

（2）网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

（3）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

（4）信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

（5）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6）灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。

（7）其他事件是指不能归为以上分类的网络安全事件。国家有关法律法规有明确规定的，按国家有关规定执行。

第八条　网络与信息安全事件分级

网络安全事件依据影响范围、严重程度和可控性，可分为以下四级。

I 级（特别重大）：网络与信息系统发生全校性大规模瘫痪或发生特别严重信息内容安全事件和信息破坏事件；对学校正常工作造成特别严重损害，且事态发展超出学校控制能力的安全事件。

II 级（重大）：学校网络与信息系统造成大面积瘫痪或发生严重信息内容安全事件和信息破坏事件，对学校正常工作造成严重损害，事态发展超出网络安全与信息化中心控制能力，需学校各部门协同处置的安全事件；

III 级（较大）：学校某一区域的网络与信息系统瘫痪或发生较严重信息内容安全事件和信息破坏事件，对学校正常工作造成较严重损害，网络中心可自行处理的安全事件；

IV 级（一般）：学校某一局部网络与信息系统受到一定程度损坏，或发生一定程度信息内容安全事件和信息破坏事件，对学校某些工作有一定影响，但不危及学校整体工作的安全事件，网络安全与信息化中心可自行处理的安全事件。

第四章　预防措施

第九条　管理措施

（1）学校建立健全安全事件监测预警体系。网络安全与信息化中心通过国内主流安全网站、相关安全部门通报等渠道收集计算机操作系统漏洞、网络设备漏洞、木马病毒等预警信息，并及时向学校相关师生用户发布预警信息。同时，网络安全与信息化中心对校学校重要网络设施、信息系统进行监测，出现异常情况及时告警并处理。

（2）各单位严格执行学校网络与信息安全各项管理制度，对本单位所负责管理的信息系统采取相应安全保障措施，重点做好数据备份恢复工作。

（3）特殊时期、重要会议期间，各单位安排本单位工作人员值班，对本单位所辖范围的信息系统、网站进行巡查，重点巡查单位门户、新闻网、论坛等信息流量大、影响面大的网站，做到安全事件早发现、早报告、早控制、早解决。

第十条　技术措施

（1）物理环境：①建设安全、可靠、稳定运行的机房环境，做好防火、防盗、防雷电、防水、防静电、防尘；②对机房实施每天巡检，禁止任何非授权人员进入；③建立备份电源系统，定时检查系统能否正常工作；④　对所有人员进行防火、防盗等基本技能进行培训。

（2）网络设备：①核心设备有冗余，避免单点故障；②采用实名制认证方式入网；③实时监测关键网络设备的端口状态和流量，出现异常及时告警；④预留一定的应急网络设备，发生故障时，可以及时替换使用。

（3）计算机系统：①采用可靠稳定的操作系统，及时安装最新补丁；②关闭所有不必要的服务和端口；③安装有效的防病毒软件，及时更新病毒特征库；④严格限制内部用户的访问权限；⑤对用户和管理员进行安全技术培训；

（4）重要的信息系统（网站）：①网站纳入学校站点群平台集中管理，信息系统采用网络与网络安全与信息化中心分配的虚拟机集中部署；②实时或定期备份信息系统相关数据，采取有效措施防范数据损坏、泄漏和篡改；③向网络安全与信息化中心进行登记备案；④建立严格的信息发布审核制度，尤其关注论坛、

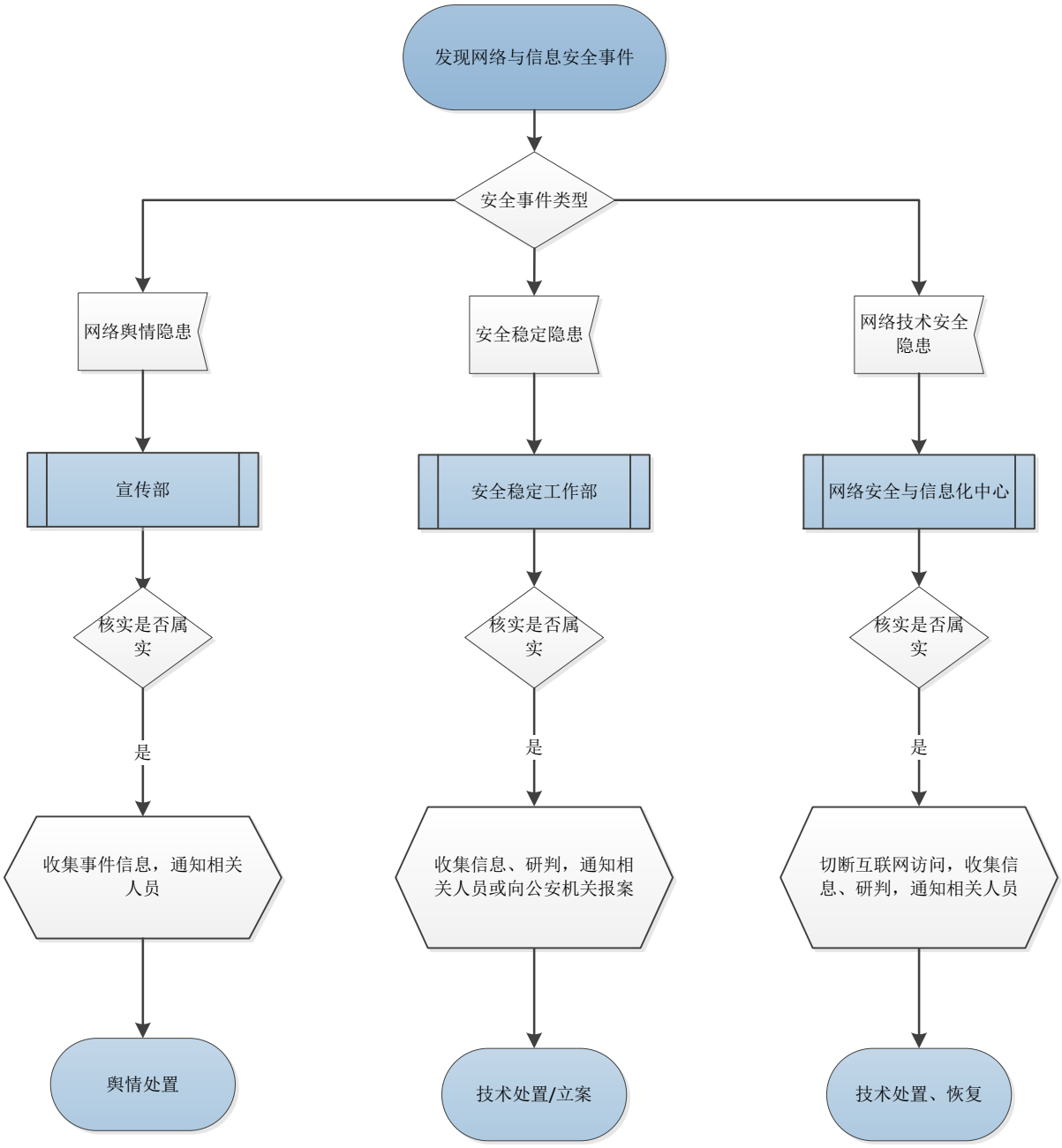
留言板等交互式栏目；⑤监测信息系统（网站）的可用性、安全性，出现异常及时告警;

（5）各级网络边界控制：①在校园网出口边界建立防火墙，在重大安全事件爆发时可以实施访问控制;②在数据中心边界安装入侵监测/防御系统，监测/防御恶意攻击、病毒等非法入侵。

第五章　应急处置措施

第十一条　信息预警研判处置流程

普通用户发现网络安全事件后应进行初步研判，根据相应事件类型向安全稳定工作部、宣传部、网络安全与信息化中心报告。安全稳定工作部、宣传部、网络安全与信息化中心获得用户报告或网安部门、教育部、北京市等有关信息安全部门通报的安全预警信息后，应进行核实，采取有效措施并向相应单位的网络安全负责人进行通报。



第十二条　事件报告与处置流程

（1）发生校园网络安全事件时，应根据实际情况第一时间采取断网等有效措施进行处置，将损害和影响降到最小范围，保留现场，并报告本单位安全责任人。

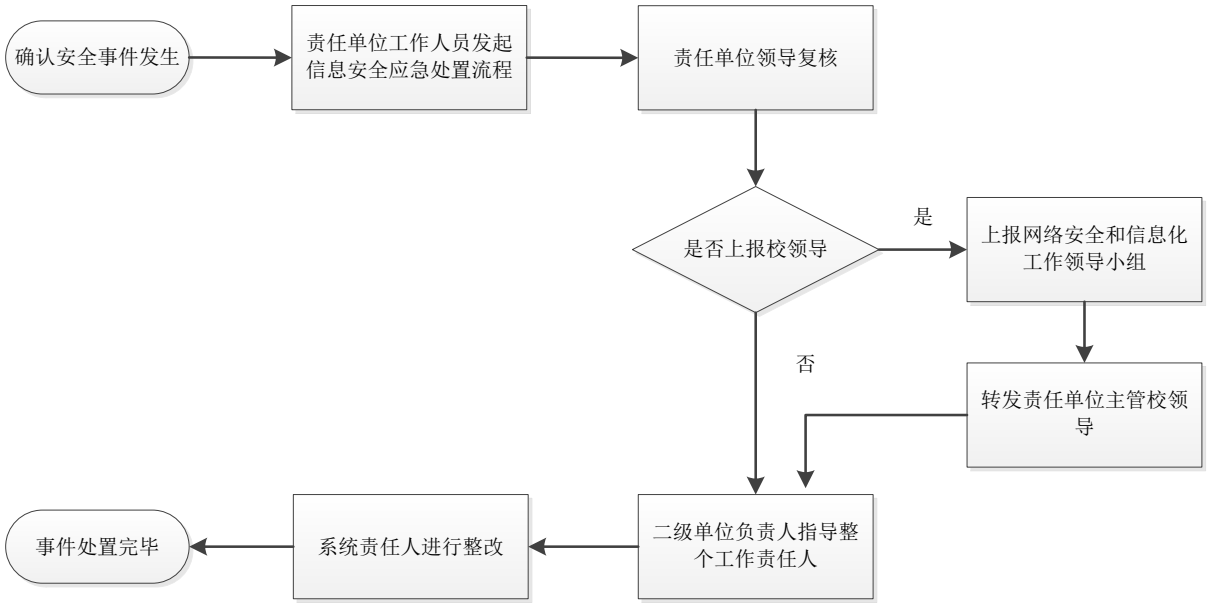
（2）安全负责人评估事件带来的影响和损害，确认突发事件的类别和等级，组织相关人员赶赴现场进行紧急处置，同时以口头通讯的方式将相关情况通报至网络安全与信息化中心。涉及人为主观破坏事件应同时报告学校安全稳定工作部。

（3）网络安全与信息化中心接到报告后，应进一步判定安全事件等级，对确认属Ⅰ至Ⅲ级安全事件的，应报告学校网络安全工作委员会，由学校网络安全工作委员会统一组织、协调指挥进行应急处置。

（4）单位安全负责人提交事中情况报告（事件发现后1小时内，格式见附件1）和事后整改报告（事件处置完毕后1个工作日，格式见附件2），由本单位主要负责人审核后，签字并加盖公章报送网络安全与信息化中心。网络安全与信息化中心酌情决定是否向上级单位汇报。Ⅳ级安全事件由信息系统主管单位自行负责应急处置工作，并向网络安全与信息化中心报送整改报告（事件处置完毕后1天内，格式见附件2）。

第十三条　整改流程

确认网络安全事件发生后，按如下应急处置流程进行整改，各单位必须积极、按时进行安全整改处置，按要求形成书面报告（接到通报后1天内，格式见附件2），报送责任单位。



第十四条　应急处理措施

（1）有害程序事件：及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围；为避免产生更大的损失，保护健康的计算机，必要时可关闭相应的传播端口，甚至相应网络设备的连接端口，及时进行杀毒处理。

（2）网络攻击事件：判断入侵来源的 IP 地址，区分外网与内网，对于外网入侵，限制对方 IP 地址的访问，对于已经造成危害的，应立即采用断开网络连接的方法，避免造成更大损失和影响。对于内网入侵，查清入侵来源，查找相应的计算机和上网用户，同时断开对应的交换机端口。对于无法制止的入侵，应及时关闭被入侵的服务器或相应设备，同时针对入侵方法调整或更新入侵检测/防御设备。

（3）信息破坏事件：重要的信息系统的数据应提前做好异地备份，一旦数据遭到破坏性攻击，应立即断开网络连接，进行

数据恢复。

（4）信息安全事件：校内网站出现不良信息的报案后，应当保留证据，迅速屏蔽该网站的网络端口或拔掉网络连接线，阻止有害信息的传播，根据网站相关日志记录查找信息发布人并做好善后处理；对公安机关要求我校协查的外网不良信息事件，根据校园网上网相关记录查找信息发布人。

（5）设备故障事件：判断故障发生点和故障原因，如遇设备故障问题，网络与网络安全与信息化中心组织相关技术人员尽快抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。如遇停电紧急事件，根据停电时间、UPS 电池的供电能力保障最重要的设备和信息系统继续运行，关闭次要的设备和信息系统，供电恢复后，及时恢复关闭的网络设备。

（6）灾害性事件：根据实际情况，在保障人身安全的前提下，保障数据安全和设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

（7）其它不确定安全事件：可根据总的安全原则，结合具体情况，做出相应处理。

第十五条　事后处理措施

安全事件被抑制后，掌握损失情况、查找和分析事件原因，找出问题根源，明确相应补救措施并彻底清除安全隐患。在确保安全事件解决后，恢复数据、系统服务。

应急处置工作结束后，组织有关人员对事件发生原因、影响、责任及应急处置能力、恢复重建等问题进行全面调查评估，并出

具总结报告。根据应急处置过程中暴露出的管理、协调和技术问题，改进和完善应急预案，定期实施演练，总结经验教训，整改存在隐患，进一步提升安全防护能力。

第六章　保障措施

第十六条　队伍保障

加强网络安全与信息化中心的技术队伍建设，进一步完善学校各部门信息员制度，确保校园网公共服务符合技术标准和管理规范。通过技术培训、研讨、对外交流、参与会议等方式不断提高技术人员的信息安全防范意识和技术水平，为校园网络和信息的安全保障提供强大技术支撑。

加强与学校网络安全专业师生优秀团队、国内主要安全厂商等的合作，确保安全事件处置得当。

收集、建立应急处置工作组和各单位的网络安全负责人、安全管理员联络通讯录，确保在发生突发事件时通信联络畅通。

第十七条　技术保障

重视信息系统的建设和升级换代，重视网络安全整体方案的不断完善，加强技术管理，确保信息系统的稳定与安全，聘请信息安全顾问为应急处置过程和重建工作提供咨询和技术支持。

第十八条　经费保障

网络安全与信息化中心应根据校园网络与信息安全防护和应急处置工作的实际需要，申报网络安全设备及软件的运维专项资金，纳入年度预算，由学校给予资金保障。

第十九条　宣传、培训与演练

学校宣传部、安全稳定工作部、网络安全与信息化中心要利用适当时机，加强网络与信息安全的法律法规、新闻动态和知识技能的宣传教育，提高师生的网络与信息安全意识和应对水平。

网络安全与信息化中心定期对相关工作人员进行网络与信息系统安全知识培训，增强预防意识和应急处置能力，有针对性地开展应急演练，确保相关措施有效落实。

学校各部门要加强网络与信息安全特别是网络与信息安全应急预案的培训，将网络与信息安全事件的应急知识列为管理干部和有关人员的考核内容，提高防范意识和技能。校园网络与信息安全事件应急处置工作领导小组加强与学校各部门的联动，组织协调学校网络与信息安全应急预案演练工作。校园网络与信息安全事件应急处置工作领导小组每年联合学校办公室、宣传部、安全稳定工作部等部门组织至少一次的安全培训和针对不同级别安全事件的预案演练，同时加强人事联动、部门联动等的联合演练，有效提高学校网络与信息安全应急处置能力和水平。校园网络与信息安全事件应急处置工作领导小组将演练情况报告学校网络与信息安全工作领导小组。

本预案是《北方工业大学突发事件应急预案》的重要组成部分，解释权归网络安全与信息化工作领导小组，本预案自下发之日起施行。

附件：1.网络信息安全事件情况报告

2.信息技术安全事件整改报告

北方工业大学

2019 年 5 月 27 日

附件 1

网络信息安全事件情况报告

单位名称：（需加盖公章）　　事发时间：　　年　　月　　日　　时　　分

<table>
<tr><td rowspan="2">联系人姓名</td><td rowspan="2"></td><td>手机</td><td></td></tr>
<tr><td>电子邮箱</td><td></td></tr>
<tr><td>事件分类</td><td colspan="3">□网络舆情事件□安全稳定事件□网络信息安全事件
□其他----------</td></tr>
<tr><td>事件分级</td><td colspan="3">□ I 级□ II 级□ III 级□ IV 级</td></tr>
<tr><td>事件概况</td><td colspan="3"></td></tr>
<tr><td>相关系统基本情况
（如涉及请填写）</td><td colspan="3">1. 系统名称：----------
2. 系统网址和 IP 地址：----------
3. 系统主管单位/部门：----------
4. 系统运维单位/部门：----------
5. 系统使用单位/部门：----------
6. 系统主要用途：----------
----
7. 是否定级□是□否，所定级别：-----
8. 是否备案□是□否，备案号：----------
9. 是否测评□是□否
10. 是否整改□是□否</td></tr>
<tr><td>事件发现与处置的简要经过</td><td colspan="3"></td></tr>
</table>

事件初步估计的危害和影响	
事件原因的初步分析	
已采取的应急措施	
是否需要应急支援及需支援事项	
安全负责人意见（签字）	
主要负责人意见（签字）	

附件 2

信息技术安全事件整改报告

单位名称：（需加盖公章） **报告时间：　　年　　月　　日**

联系人姓名		手机	
		电子邮件	
事件分类	□网络舆情事件□安全稳定事件□网络信息安全事件 □其他----------		
事件分级	□ Ⅰ 级□ Ⅱ 级□ Ⅲ 级□ Ⅳ 级		
事件概况			
相关系统基本情况（如涉及请填写）	1.系统名称：---------- 2.系统网址和 IP 地址：---------- 3.系统主管单位/部门：---------- 4.系统运维单位/部门：---------- 5.系统使用单位/部门：---------- 6.系统主要用途：---------- ---------- 7.是否定级□是□否，所定级别：----- 8.是否备案□是□否，备案号：---------- 9.是否测评□是□否 10.是否整改□是□否		

事件发生的最终判定原因（可加页附文字、图片以及其他文件）	
事件的影响与恢复情况	
事件的安全整改措施	
存在问题及建议	
安全负责人意见（签字）	
主要负责人意见（签字）	

北方工业大学校长办公室　　2019年5月27日印发