

北京语言大学文件

校信息〔2019〕4号

北京语言大学网络信息安全事件应急预案

第一章 总则

第一条 编制目的。建立学校网络信息安全事件应急响应工作机制，有效预防并科学应对网络信息安全突发事件，保障校园网络与信息系统正常运行。

第二条 编制依据。根据《中华人民共和国计算机信息系统安全保护条例》、教育部《教育系统网络安全事件应急预案》、教育部《信息技术安全事件报告与处理流程》等有关法律法规，结合学校工作实际，制定本预案。

第三条 适用范围。本预案适用于对北京语言大学计算机网络及信息安全突发事件（以下简称安全事件）的组织指挥、应急行动、后期处置。

第四条 工作原则。应急处置遵循“统一领导、预防为主、快速反应、科学处置”的原则和“谁主管、谁负责，谁使用、谁负责，谁运维、谁负责”的分级负责原则，实行预防与处置相结合。

第二章 安全事件的分类分级

第五条 安全事件依据发生过程、性质和特征不同，可分为以下五类：

- （一）网络攻击事件：由于遭受有害程序感染、非法入侵或其他技术手段的网络攻击，造成校园网络和信息系统运行异常，或造成信息被篡改、假冒、泄漏、窃取等而导致的安全事件。
- （二）设备故障事件：由于信息系统或硬件设施和基础设施故障、人为误操作等，造成信息系统破坏、业务中断、系统宕机、网络瘫痪等导致的安全事件。
- （三）灾害性事件：因洪水、火灾、雷击、地震、台风、非正常停电等外力因素造成网络与信息系统损毁，导致业务中断、系统宕机、网络瘫痪等安全事件。
- （四）信息内容安全事件：利用校园网、校外论坛及自媒体等传播法律法规禁止的信息，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安全事件。
- （五）其他安全事件：不能归为以上四个基本分类的安全事件。

第六条 安全事件按照可控性、严重程度和影响范围不同，可划分为四级：

- （一）I级（特别重大）：安全事件导致校园网全局性瘫痪；统一运行的核心业务系统（网站）遭受特别

严重损失，造成系统大面积瘫痪，丧失业务处理能力；统一运行的核心业务系统（网站）重要敏感信息或关键数据丢失或被窃取、篡改；其他对学校安全稳定和正常秩序构成特别严重威胁，造成特别严重影响的网络安全事件。

（二）II级（重大）：安全事件导致校园网发生大规模瘫痪；核心业务信息系统（网站）遭受严重系统损失，造成系统瘫痪，业务处理能力受到重大影响；网络病毒在全校大面积爆发；核心业务信息系统（网站）的重要敏感信息或关键数据发生丢失或被窃取、篡改；其他对学校安全稳定和正常秩序构成严重威胁，造成严重影响的网络安全事件。

（三）III级（较大）：事件导致校园网某一区域网络瘫痪；重要业务信息系统（网站）遭受较大系统损失，明显影响系统效率，业务处理能力受到影响；网络病毒在全校多个区域范围内广泛传播；重要业务信息系统（网站）的信息或数据发生丢失或被窃取、篡改、假冒；其他对学校安全稳定和正常秩序构成较大威胁，造成较大影响的网络安全事件。

（四）IV级（一般）：除上述情形外，对学校安全稳定和正常秩序构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

第三章 组织机构及职责

第七条 北京语言大学网络安全和信息化领导小组是安全事件应急处理的指挥机构，其主要职责：

- （一）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监督与检查；
- （二）根据安全事件程度决定相应级别应急预案的启动，组织协调相关单位落实应急预案，共同做好处置工作；
- （三）负责及时通报和上报安全事件应急处置的有关情况；
- （四）负责审定应急预案的更新及修订。

第八条 其它单位职责包括：

- （一）信息化办公室：负责制定、完善应急预案以及其他相关制度；根据安全事件的程度向网络安全和信息化领导小组建议相应级别预案的启动；组织协调相关单位落实应急预案，共同做好处置工作；负责及时收集、通报和上报安全事件处置的有关情况和整改方案；定期对应急处置工作进行有针对性的培训和应急演练；负责校园基础网络系统安全，保障校园网络服务不中断；负责针对校园网的网络攻击、设备故障类事件的处置，第一时间断开被攻击主机、关闭不需要的服务，查找病毒源，修补系统漏洞，查看日志并寻找入侵源头，

完善防火墙、路由器等网络安全设备的过滤规则；负责全校安全事件处置的技术支持工作。

(二) 党委宣传部：负责学校舆情监测和信息内容安全类事件的处置，对于涉及师生政治思想方面的预警性、倾向性、苗头性的问题，要加强分析研判，妥善有效应对。

(三) 保卫处：负责涉及人为破坏类安全事件的处置，配合重大安全事件的处置，联系公安部门。

(四) 学校办公室：负责网络信息安全事件的总体协调工作。

(五) 其他各单位：负责本单位网站和信息系统安全事件的处置工作。

第四章 处置程序

第九条 事件报告：发生安全事件后，信息化办公室和涉事单位应第一时间采取断网等有效措施，将损害和影响降低到最小范围，保留现场，并报告本单位分管领导和信息化办公室负责人。

第十条 事件定级：信息化办公室组织有关单位，尽最大可能收集安全事件相关信息，鉴别性质，确定来源，弄清范围，评估安全事件带来的影响和损害，确认安全事件的类别和等级。

第十一条 应急响应：根据安全事件等级采取相应的响应方式。

- (一) I级：信息化办公室立即上报网络安全和信息化领导小组，并由学校报告上级主管部门和公安部门，公安部门指挥协调校外有关单位和我校协同进行应急处置。
- (二) II至III级：信息化办公室应立即上报网络安全和信息化领导小组，由领导小组指挥、协调成员单位进行应急处置。涉及人为主观破坏事件时视情节严重程度由学校保卫处报告当地公安部门。
- (三) IV级：信息化办公室组织相关单位及时、自主进行应急处置，做好处置记录。

第十二条 应急处置方式：根据安全事件分类采取不同应急处置方式。

- (一) 网络攻击事件：判断攻击的来源与性质，关闭影响安全的网络设备和服务器设备，断开信息系统与攻击来源的网络物理连接，跟踪并锁定攻击来源的IP地址或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照事件发生的性质采取以下方案：

病毒传播：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端口，甚至相应楼层的网络，及时进行杀毒处理。

外部入侵：判断入侵的来源，区分外网与内网，评价入侵可能或已经造成的危害。对入侵未遂、未造成损害的，且评价威胁很小的外网入侵，定位入侵的 IP 地址，及时关闭入侵的端口，限制入侵的 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。

内部入侵：查清入侵来源，如 IP 地址、所在办公室等信息，同时断开对应的交换机端口，针对入侵方法调整或更新入侵检测设备。对于无法制止的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

- (二) 设备故障事件：判断故障发生点和故障原因，迅速联系 IT 运维公司尽快抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。
- (三) 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。
- (四) 信息内容安全事件：接到校内网站出现不良信息的报案后，应迅速屏蔽该网站的网络端口或拔掉网络连接线，阻止有害信息传播，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

校外论坛或自媒体的不良信息事件，根据校园网上网相关记录查找信息发布人。

- (五) 其它不确定安全事件：可根据总的的原则，结合具体情况，做出相应处理，不能处理的及时咨询上级信息安全机构。

第十三条 后续处理：

- (一) 安全事件经初步应急处置后，应及时采取措施，抑制其影响进一步扩大，限制潜在的损失与破坏。
- (二) 安全事件被抑制后，通过对有关事件或行为的分析结果，找出问题根源，明确相应补救措施并彻底清除。
- (三) 安全事件处置后，及时清理系统，恢复数据、程序和服务。

第五章 总结报告

第十四条 系统恢复运行后，信息化办公室对事件造成的损失、事件处理流程等进行分析评估，总结经验教训，撰写事件处理报告。

发生 I 至 III 级事件，在报告学校的同时，应按照教育部办公厅《信息技术安全事件报告与处置流程（试行）》报告上级主管部门。属于重大事件或存在非法犯罪行为的，还须第一时间向公安机关报案。应按照以下流程报告：

- (一) 事发紧急报告：事件发生后立即以口头通讯方式报上级主管部门，涉及人为主观破坏事件应同时

报当地公安机关。报告内容包括：时间地点，简要经过，事件类型与分级，影响范围，危害程度，初步原因分析，已采取的紧急措施。

(二) 事中处置报告：应在事件发生后 8 小时内以书面报告形式报送，报送内容和形式见附件 3。

(三) 事后整改报告：应在事件处置完毕后 5 个工作日内以书面报告形式报送，报送内容和格式见附件 4。

如上级部门调整事件的报送时间要求，按照调整后的要求报送。

第六章 预防保障措施

第十五条 加强网络与信息系统安全管理，健全工作制度和建立预报预警监测体系，避免和减少网络信息安全事件发生。

第十六条 加强技术储备与保障工作，不断完善网络安全技术防护体系，确保信息系统的稳定与安全。建立通信保障应急管理机构和校外专业安全公司信息沟通机制，适时组织相关专家和机构分析当前网络安全，对网络应急预案及实施情况进行评估，开展现场研究。

第十七条 建立灾害险情巡查制度。宣传部及各单位信息员应随时监控所辖网站内容，信息化办公室做好校园网络与信息安全的日常巡查及日志保存工作，以保证最先发现灾害并及时处置突发性事件。

第十八条 加强安全培训和演练，信息化办公室应定期组织相关单位信息员进行安全知识培训，增强防范意识和应急处置能力。开展应急处置演练，确保相关措施的有效落实。

第十九条 加强资金保障，信息化办公室应根据校园网络和信息安全防护和应急处置工作实际需要，提出用于安全防护的软硬件设备及运行维护经费预算，报财务处纳入年度经费预算，以专项经费列支。

第七章 预案解释与实施

第二十条 本预案由信息化办公室负责解释。

第二十一条 本预案经学校 2019 年 7 月 11 日校长办公会讨论通过，自发布之日起执行。原《北京语言大学网络与信息系统安全应急响应管理规定》（校网技字〔2015〕5 号）同时作废。

- 附件：
1. 应急管理培训登记表
 2. 应急演练记录
 3. 安全事件报告表
 4. 安全事件整改报告

北京语言大学
2019 年 7 月

附件1

应急管理培训登记表

记录顺序号：

No.	姓名	所属单位	培训教师	培训内容	培训地点	培训日期	培训学时	考核时间	是否合格

附件3

安全事件报告表

单位名称：（需加盖公章） 事发时间： 年 月 日 时 分

联系人姓名	手机	
	电子邮箱	
事件分类	<input type="checkbox"/> 有害程序事件 <input type="checkbox"/> 网络攻击事件 <input type="checkbox"/> 信息破坏事件 <input type="checkbox"/> 设备设施故障 <input type="checkbox"/> 灾害事件 <input type="checkbox"/> 其他_____	
事件分级	<input type="checkbox"/> I级 <input type="checkbox"/> II级 <input type="checkbox"/> III级 <input type="checkbox"/> IV级	
事件概况		
信息系统的基本情况（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 <input type="checkbox"/> 是 <input type="checkbox"/> 否，所定级别： _____ 8. 是否备案 <input type="checkbox"/> 是 <input type="checkbox"/> 否，备案号： _____ 9. 是否测评 <input type="checkbox"/> 是 <input type="checkbox"/> 否 10. 是否整改 <input type="checkbox"/> 是 <input type="checkbox"/> 否	
事件发现与处置的简要经过		
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	
单位安全负责人意见 (签字)	
单位主要负责人意见 (签字)	

附件4

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	<input type="checkbox"/> 有害程序事件 <input type="checkbox"/> 网络攻击事件 <input type="checkbox"/> 信息破坏事件 <input type="checkbox"/> 设备设施故障 <input type="checkbox"/> 灾害事件 <input type="checkbox"/> 其他_____	
事件分级	<input type="checkbox"/> I级 <input type="checkbox"/> II级 <input type="checkbox"/> III级 <input type="checkbox"/> IV级	
事件概况		
信息系统的基本情况 (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 <input type="checkbox"/> 是 <input type="checkbox"/> 否, 所定级别: _____ 8. 是否备案 <input type="checkbox"/> 是 <input type="checkbox"/> 否, 备案号: _____ 9. 是否测评 <input type="checkbox"/> 是 <input type="checkbox"/> 否 10. 是否整改 <input type="checkbox"/> 是 <input type="checkbox"/> 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)		