首都师范大学文件

首都师大校发〔2020〕2 号

首都师范大学关于印发《首都师范大学网络与信息安全事件应急预案（2019 年修订)》的通知

各院（系）、单位：

《首都师范大学网络与信息安全事件应急预案（2019 年修订)》经 2019 年第 32 次校长办公会研究通过，现予以印发，请遵照执行。

首都师范大学

2020 年 1 月 7 日

首都师范大学
网络与信息安全事件应急预案（2019 年修订）

为加强我校网络与信息安全应急响应工作机制，科学应对网络与信息安全突发事件，有效预防和及时处理网络与信息安全突发事件，确保校园网络与信息系统正常运行，结合我校实际，特制定本预案。

一、适用范围

本预案适用于全校范围内自建自管的网络与信息系统，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。

二、工作原则

坚持统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置；坚持预防为主，预防与应急相结合；坚持谁主管谁负责、谁运行谁负责，充分发挥各方面力量共同做好网络安全事件的预防和处置工作。

三、网络与信息安全事件分类分级

（一）网络与信息安全事件分类

网络与信息安全突发事件依据发生过程、性质和特征的不同，可分为以下四类：

1. 网络攻击事件：校园网络与信息系统因病毒感染、非法入侵等造成学校网站或部门二级网站主页被恶意篡改，应用系统数据被拷贝、篡改、删除等。

2.设备故障事件：校园网络与信息系统因网络设备和计算机软硬件故障、人为误操作等导致业务中断、系统宕机、网络瘫痪。

3.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导致网络与信息系统损毁，造成业务中断、系统宕机、网络瘫痪。

4.信息内容安全事件：利用校园网络在校内外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等。

（二）网络与信息安全分级

网络与信息安全突发事件依据可控性、严重程度和影响范围的不同，可分为以下四级：

I级（特别重大）：学校网络与信息系统发生全校性大规模瘫痪，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全校性瘫痪，对学校正常工作造成严重损害，事态发展超出数字校园建设中心控制能力，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，对学校正常工作造成一定损害，数字校园建设中心可自行处理的安全事件；

IV级（一般）：某一局部网络或信息系统受到一定程度损坏，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。

四、组织机构

（一）学校成立校园网络与信息安全事件应急处置领导小组，全面负责和统一指挥校园网络与信息安全重大突发事件的应急处置工作。领导小组组长由主管网络安全工作的校领导担任，小组成员由学校办公室、宣传部、保卫处、数字校园建设中心等部门主要负责人组成。

（二）学校办公室负责校园网络与信息安全事件应急处置的协调和事件处置情况上报，宣传部负责应急处置过程中相关舆情的处理，保卫处负责应急处置过程中对接上级公安保卫部门，数字校园建设中心负责应急处置过程中相关信息收集和技术处理。

（三）数字校园建设中心作为学校信息化建设的主管部门，负责校园主干网络与主要信息系统安全事件的预防、监测、报告和应急处置，负责对学校其他部门主管的网络信息系统的安全防护情况进行日常检查、指导和督促。

五、预防措施

（一）按照《信息安全事件分类分级指南》，对校园网络通信平台、应用平台和信息系统采取相应安全保障措施。

（二）建立健全安全事件预警预报体系，严格执行校园网络与信息系统安全管理制度，常年坚持校园网络安全工作值班制度。加强对校园网络与学校网站等重点信息系统的监控和安全管理，做好相关数据日志记录，确定合理规则，对校园网络进出信息实行过滤及预警。实行信息网上发布审批制度，对可能引发校园网络与信息安全事件的信息，要认真收集、分析、判断，发现有异常情况时，及时防范处理并逐级报告。

（三）做好服务器及数据中心的数据备份及登记工作，建立灾难性数据恢复机制。

（四）特殊时期，根据学校要求和部署，由数字校园建设中心进行统一安排，组织专业技术人员对校园网络和信息系统采取加强性保护措施，对校园网络通信及信息系统进行不间断监控。

六、处置流程

（一）预案启动

发生校园网络与信息安全事件后，数字校园建设中心和突发安全事件的信息系统建管部门应尽最大可能收集事件相关信息，鉴别事件性质，确定事件来源，弄清事件范围，评估事件带来的影响和损害，确认突发事件的类别和等级，并参照下述响应机制对突发事件进行处置。

（二）应急响应

1.应急响应机制

III 级或 IV 级突发事件响应：数字校园建设中心和突发安全事件的信息系统建管部门自行负责应急处置工作，有关情况报分管校领导。

II 级突发事件响应：数字校园建设中心立即上报分管校领导和校园网络与信息安全事件应急处置领导小组，由领导小组统一组织、协调指挥进行应急处置。

I 级突发事件响应：数字校园建设中心立即上报分管校领导和校园网络与信息安全事件应急处置领导小组，领导小组再上报至市公安局等相关部门，由北京市相关部门会同我校校园网络与信息安全事件应急处置领导小组统一组织、协调指挥应急处置。

2.应急处理方式

根据网络与信息安全事件分类采取不同应急处置方式。

（1）网络攻击事件：判断攻击的来源与性质，关闭影响安全与稳定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，及时请有关技术人员协助，寻找并公布病毒攻击信息，以及杀毒、防御方法。

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。

（2）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。

（3）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。

（4）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）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。不能处理的及时咨询信息安全公司或顾问。

（三）后续处理

1.安全事件进行最初的应急处置后，应及时采取行动，抑制其影响进一步扩大，限制潜在的损失与破坏，同时要确保应急处置措施对涉及的相关业务影响最小。

2.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。

3.在确保安全事件解决后，要及时清理系统，恢复数据、程序、服务，恢复工作应避免出现误操作导致的数据丢失。

（四）记录上报

网络与信息系统安全事件发生时，应及时向校领导和校园网络与信息安全事件应急处置领导小组汇报，并在事件处置工作中作好完整的过程记录，及时报告处置工作进展情况，保存各相关系统日志，直至处置工作结束。

（五）结束响应

系统恢复运行后，数字校园建设中心对事件造成的损失、事件处理流程和应急预案进行评估，对响应流程、预案提出修改意见，总结事件处理经验和教训，撰写事件处理报告，同时确定是否需要上报该事件及其处理过程，需要上报的应及时准备相关材料；属于

重大事件或存在非法犯罪行为的，第一时间向公安机关网络监察部门报案。

七、保障措施

校园网络与信息安全应急处置是一项长期的、随时可能发生的工作，必须做好各项应急保障工作。

（一）队伍保障

重视信息系统安全队伍建设，不断提高工作人员的信息安全防范意识和技术水平，确保安全事件应急处置过程和重建工作中技术人员的在岗与防护能力。

（二）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。

（三）资金保障

数字校园建设中心应根据校园网络与信息系统安全预防和应急处置工作的实际需要，申报网络与信息系统关键设备及软件的运行维护专项资金，提出本年度应急处置工作相关设备和工具所需经费，报财务处纳入年度财政预算，由学校给予资金保障。

（四）安全培训和演练

举办网络与信息系统安全知识培训，加强对师生的计算机操作、信息技能、网络和信息系统安全等相关知识的宣传普及，增强预防意识和简单应急处置能力。有针对性地开展应急抢险救灾演练，确保发灾后应急救助手段及时到位、有效。

八、本预案自公布之日起施行，由数字校园建设中心负责解释

首都师范大学学校办公室　　2020 年 1 月 7 日印发