东北大学秦皇岛分校文件

东秦校〔2018〕55 号

关于印发《东北大学秦皇岛分校网络与信息安全突发事件应急处置预案》的通知

各部门:

为进一步加强我校网络与信息安全管理，确保基础网络与其他重要业务信息系统的安全、高效运行，确保在发生突发性网络与信息安全事件时，能够迅速、高效、有序的进行应急处理，避免或最大限度的减轻事故的损失，根据有关规定，结合我校实际，学校研究制定了《东北大学秦皇岛分校网络与信息安全突发事件应急处置预案》。现印发给你们，请遵照执行。

东北大学秦皇岛分校

2018 年 11 月 16 日

东北大学秦皇岛分校网络与信息安全突发事件应急处置预案

第一章 总则

第一条 为了切实做好学校网络与信息安全突发事件的防范和应急处理工作，进一步提高我校预防和控制网络与信息安全突发事件的能力和水平，减轻或消除突发事件的危害和影响，确保我校校园网络与信息安全，结合学校实际情况，制定本预案。

第二条 本预案所称突发性事件，是指因自然因素或人为活动引发的危害学校校园网络及信息安全的有关事件。

第三条 本预案适用于东北大学秦皇岛分校范围内自建自管的网络和信息系统，尤其是校园网主干设施和重要信息系统的突发信息安全事件的应急处置。

第二章 职责任务

第四条 按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，防范为主，加强监控，统一指挥、高效协调、各司其职、保障安全。采取全校统一管理和各部门分级负责的管理体制，学校主要负责人是信息技术安全工作的第一责任人，主管信息化工作的校领导为信息技术安全工作的分管责任人，各部门负责人为其部门信息安全工作的第一责任人。

第五条 遇突发的网络与信息安全事件，应及时控制事态，限制在最短时间、最小范围内，使影响和损失减少到最低程度，并尽快

恢复学校正常的教学、科研和生活秩序。落实工作责任和责任追究制。凡在执行本预案过程中，因工作延误、渎职或不服从指挥、不及时处理，产生严重后果的，要追究相关人员责任。

第三章 组织机构

第六条 学校网络安全管理与信息化建设工作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。

第七条 信息化建设与管理办公室作为学校信息化建设运行的主管部门，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，必要时信息化建设与管理办公室协助相关主管部门完成突发事件的技术处理。

第八条 学校各部门负责对其主管的网络信息系统安全事件的预防、监测和应急处置，并及时向学校网络安全管理与信息化建设工作领导小组报告。

第四章 分类分级

第九条 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:

（一）网络攻击事件: 学校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。

（二）设备故障事件: 学校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。

（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。

（四）信息内容安全事件：利用学校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。

第十条 网络与信息安全事件分级

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，事态发展超出信息化主管部门控制能力，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，信息化主管部门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。

第五章 事件预防

第十一条 按照信息系统等级保护与信息安全分类分级指南要求，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。

第十二条 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。

第十三条 做好关键设备的冗余备份工作，做好信息数据的备份及登记工作，建立灾难性数据恢复机制。

第十四条 特殊时期，根据学校要求和部署，由信息化建设与管理办公室进行统一安排，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。

第六章 事件处置

第十五条 预案启动

发生校园网络与信息安全事件后，信息化建设与管理办公室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。

第十六条 应急响应

（一）应急响应机制

III 级或 IV 级突发事件响应：信息化建设与管理办公室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：信息化建设与管理办公室立即上报分管校领导和校网络安全管理与信息化建设工作领导小组，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：信息化建设与管理办公室立即上报分管校领导和校网络安全管理与信息化建设工作领导小组，领导小组再上报至市公安局等相关部门，由相关部门会同我校网络安全管理与信息化建设工作领导小组统一组织、协调指挥、应急处置。

（二）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网络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，定位入侵的网络地址，及时关闭入侵端口，限制入侵的网络地址访问。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，如网络地址、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。

第十七条 后续处理

（一）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。

（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）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。

第十八条 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网络安全管理与信息化建设工作领导小组汇报，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。

第十九条 结束响应

系统恢复运行后，信息化建设与管理办公室对事件造成的损失、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。

第七章 支持保障

第二十条 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）人员保障

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

信息化建设与管理办公室与信息系统主管部门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，并上报至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

举办师生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和有效。

第八章 附则

第二十一条 本预案由信息化建设与管理办公室负责解释。

第二十二条 本预案自发布之日起执行，配套办法另行制定。

东北大学秦皇岛分校学校办公室　　2018 年 11 月 19 日印发