华 北 电 力 大 学 文 件

华电校信〔2017〕4 号

关于印发《华北电力大学网络与信息技术安全事件报告、处置流程和应急预案》的通知

校直各单位:

为进一步规范和加强我校网络与信息技术安全工作，构建和谐健康的网络空间环境，根据《中华人民共和国网络安全法》等最新文件精神，结合学校实际，制定了《华北电力大学网络与信息技术安全事件报告、处置流程和应急预案》，经 2017 年第 6 次校长办公会审议通过，现予以印发，请遵照执行。

2017年11月21日

华北电力大学网络与信息技术安全事件报告、处置流程和应急预案

为加强我校网络与信息技术安全工作，建立健全应急响应工作机制，协调相关力量做好应急响应处理，降低安全事件带来的损失与影响，维护正常工作秩序和营造健康的网络环境，保障校园网络与信息系统正常运行，根据《中华人民共和国网络安全法》、《教育部关于加强教育行业网络与信息安全的指导意见》（教技〔2014〕4号）以及教育部《信息技术安全事件报告与处置流程》（教技厅函〔2014〕75号），结合学校实际，制定本流程和预案。

第一章　总则

第一条　网络与信息技术安全事件的定义。根据《信息安全事件分类分级指南》（GB/T 20986-2007，以下简称《指南》，本流程和预案中所称的网络与信息技术安全事件(以下简称安全事件）是指有害程序事件、网络攻击事件、设备设施故障、灾害事件和其他信息技术安全事件。

第二条　适用范围。本流程和预案适用于我校各单位发生的网络与信息技术安全事件的报告、处置和应急响应工作，涉及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。涉及信息内容安全事件的报告、处置流程和应急预案待学校另行发文规定。

第三条　工作原则。统一领导，快速反应，密切配合，科学处置。坚持“谁主管谁负责、谁运行谁负责、谁使用谁负责”的原则，充分发挥各方面力量，共同做好网络与信息技术安全事件的应急处置工作。

第二章　安全事件分类分级与判定

第四条　安全事件分类。网络与信息技术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.有害程序事件: 蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的安全事件。

2.网络攻击事件:校园网络与信息系统因被非法入侵等造成学校门户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。

3.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。

4.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。

第五条　安全事件分级。网络与信息技术安全事件依据可控性、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，事态发展超出网络与信息化办公室（以下简称网信办）的控制能力，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，网信办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。

第六条　安全事件判定。我校各单位一旦发生安全事件，应根据本流程和预案，视信息系统重要程度、损失情况以及对工作和社会造成的影响迅速自主判定安全事件等级。网信办接到报告后，根据事件情况，进一步做出判定。必要时，网信办组织专家组进行判定或报告学校网络安全和信息化领导小组判定。

第三章　组织体系和职责任务

第七条　全校网络与信息技术安全防范及应急处置工作由网络安全和信息化领导小组统一领导、指挥、协调。

第八条　网络安全和信息化领导小组负责决定 I 级和 II 级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；负责对全校各单位贯彻执行安全事件报告、应急处置预案的情况进行督促检查。

第九条　校长办公室负责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。

第十条　网信办负责学校信息技术安全应急工作的统筹管理，并提供技术支撑和保障。根据校内发生的安全事件程度，提出相应级别预案的启动，并及时收集、通报和上报安全事件处置的有关情况。定期组织信息技术安全应急演练，评估并适时组织安全事件应急预案修订。负责组建学校信息技术安全应急技术队伍，完善 24 小时应急值守制度。

第十一条　保卫处、保卫处（保定）负责公安、安全等校外单位或组织介入的重大网络安全事（案）件的应急指挥、协调、调度与处置；负责与公安部门联系，配合做好网络与信息安全事件的应急处置工作。

第十二条　学校各单位应按照安全事件报告与处置流程，做好事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置工作。做到安全事件早发现、早报告、早控制、早解决。

第十三条　学校各单位应组织开展信息技术安全应急预案的宣传、教育和培训，确保相关人员熟悉应急预案。

第十四条　若本安全事件应急预案不能满足需求，相关单位可制订本单位安全应急预案，制订后应及时报网信办备案。

第四章　安全事件的报告与处置

第十五条　I 至 II 级安全事件的报告与处置。报告与处置分为三个步骤：事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置。

（一）事发紧急报告与处置

1. 网络与信息系统运维操作人员一旦发现上述安全事件，

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和主要负责人。

2. 本单位安全责任人接到报告后，应立即组织相关人员赶赴现场进行紧急处置，同时以最快的通讯方式将相关情况通报至网信办，并书面记录安全事件发现过程及汇报过程。涉及人为主观破坏事件应同时报告学校保卫部门。

3. 网信办接到报告后，应做好书面记录，并进一步判定安全事件等级，对确认属 I 至 II 级安全事件的，应迅速报告网络安全和信息化领导小组。

4. 紧急报告内容包括：（1）时间地点；（2）简要经过；（3）事件类型与分级；（4）影响范围；（5）危害程度；（6）初步原因分析；（7）已采取的应急措施。

5. 对确认属 I 至 II 级安全事件的，网信办应立即组织相关技术力量赶赴现场进行协助处置工作。涉及人为主观破坏事件的，学校保卫部门应组织人员赴现场协助处置，并协助公安机关做好相关取证和处置工作。

6. 各单位应及时跟进事件发展情况，出现新的重大情况应及时补报。

（二）事中情况报告与处置

1. 事中情况报告应在安全事件发现后 6 小时内以书面报告的形式进行报送。

2. 事中情况报告由单位安全负责人组织编写，由本单位主

要负责人审核后，签字并加盖公章报送网信办。涉及人为主观破坏事件的，事中情况报告应抄送给保卫处。

3. 安全事件的事中处置包括：及时掌握损失情况、查找和分析事件原因，修复系统漏洞，恢复系统服务，尽可能减少安全事件对正常工作带来的影响。如果涉及人为主观破坏的安全事件应由保卫处联系、配合公安部门和学校保卫部门开展调查。

（三）事后整改报告与处置

1. 事后整改报告应在安全事件处置完毕后 4 个工作日内以书面报告的形式进行报送。

2. 事后情况报告由单位安全负责人组织编写，由本单位主要负责人审核后，签字并加盖公章报送网信办。

3. 安全事件事后处置包括：进一步总结事件教训，研判安全现状、排查安全隐患，进一步加强制度建设，提升安全防护能力。如涉及人为主观破坏的安全事件应继续配合公安部门和学校保卫部门开展调查。

第十六条　III 至 IV 级安全事件的报告与处置。各单位发生 III 至 IV 级安全事件，应及时、自主组织应急处置工作；在事件处置完毕后 6 天内向网信办报送整改报告。

第十七条　预警类信息的报告与处置。各单位要按时、按要求完成上级有关安全部门以及学校网信办等部门通报的预警类信息的处置工作，并按要求形成书面报告并报送网信办。

第五章　安全事件的应急预案

第十八条　预案启动。发生校园网络与信息技术安全事件

后，网信办和突发安全事件的相关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，并按照响应机制对突发事件进行处置。

第十九条　应急响应

I 级至 II 级突发事件响应：网信办立即上报网络安全和信息化领导小组，领导小组再上报至教育部、北京市教委、河北教育厅和市公安局等相关部门，由省、市相关部门会同网络安全和信息化领导小组统一组织、协调指挥应急处置。

II 级突发事件响应：网信办立即上报网络安全和信息化领导小组，由领导小组统一组织、协调指挥进行应急处置。

III 级或 IV 级突发事件响应：网信办和突发安全事件的相关部门共同负责应急处置工作，有关情况报分管校领导。

第二十条　应急处理方式。根据安全事件分类采取不同应急处置方式。

（一）有害程序事件

一般指病毒程序的传播，应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。

（二）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：

1.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。

2.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。

（三）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。

（四）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。

（五）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。

第二十一条　后续处理。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。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。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。

第二十二条　记录上报。安全事件发生时，应按照不同的安全事件等级进行上报，并在事件处置工作中作好完整的过程记录，保存各相关系统日志，直至处置工作结束。

第二十三条　结束响应。系统恢复运行后，网信办对事件造成的损失、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。

第六章　配套制度与问责

第二十四条　人事变更报告。为保障联络通畅，各单位的信息安全工作主管领导、联络员、联络方式发生变更的，应及时向网信办报备。

第二十五条　相关配套机制。各单位应根据实际建立本单位的值守制度，做到安全事件早预警、早发现、早报告、早控制、早解决。各单位应建立健全本单位安全事件应急处置机制，制定安全事件应急预案，定期组织应急演练。

第二十六条　问责制度。各单位应按照流程及时、如实地报告和妥善处置安全事件。如有瞒报、缓报、处置和整改不力等情况，网信办将对相关单位进行约谈或通报；情况严重的，根据《中华人民共和国网络安全法》及学校相关制度文件的责任追究条款

问责处理。

第二十七条　整改落实机制。发生安全事件后，要认真做好整改落实工作，坚持做到事故原因不查清不放过、整改措施未落实不放过、责任人员未受到教育或处理不放过，尽力杜绝类似事件再次发生。

第七章　附则

第二十八条　本流程和预案授权网络与信息化办公室负责解释。

第二十九条　本流程和预案自公布之日起施行，原文件《华北电力大学网络与信息安全事件应急预案》（华电校信〔2013〕4号）同时废止。

华北电力大学校长办公室　　2017年11月21日印发