河南农业大学文件

农大信息〔2021〕1号

关于印发《河南农业大学校园网络突发事件应急预案》的通知

各学院，校直各单位，许昌校区：

现将《河南农业大学校园网络突发事件应急预案》印发给你们，请认真贯彻落实。

河南农业大学

2021年11月23日

河南农业大学
校园网络突发事件应急预案

一、总则

（一）编制目的

根据《教育系统网络安全事件应急预案》要求，健全完善校园网络突发事件应急工作机制，提升校园网络安全应急处置能力，维护正常工作秩序和营造健康的网络环境，结合学校工作实际，特制定本预案。

（二）编制依据

《中华人民共和国突发事件应对法》《中华人民共和国网络安全法》等法律法规，《国家突发公共事件总体应急预案》《突发事件应急预案管理办法》《国家网络安全事件应急预案》《教育系统网络安全事件应急预案》《关于加强教育行业网络与信息安全工作的指导意见》《信息安全技术信息安全事件分类分级指南》(GB/Z 20986-2007)等文件。

（三）适用范围

本预案适用于我校的网络与信息安全突发事件，指导全校网络与信息安全突发事件的应对处置工作。

（四）工作原则

1.积极防御，综合防范。立足安全防护，加强预警，采取多

种措施，共同构筑网络与信息安全保障体系。

2.以人为本，快速反应。按照本预案工作机制，及时获取充分准确的信息，跟踪研判，果断决策，迅速处置，尽快控制局面。

3.明确责任，加强协作。按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，各司其职，各尽其力，共同履行应急处置工作的管理职责。

4.规范流程，加强演练。规范应急处置措施与操作流程，定期进行预案演练，确保应急预案发挥重要作用。

二、事件分类及分级

（一）事件分类

根据《信息安全技术信息安全事件分类分级指南》，将安全事件划分为以下六类：有害程序事件、网络攻击事件、信息破坏事件、设备故障事件、灾害性事件和其他事件。

1.有害程序事件。

有害程序事件是指蓄意制造、传播有害程序，或是因受到有害程序的影响而导致的网络安全事件。有害程序事件包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合攻击程序事件、网页内嵌恶意代码事件和其它有害程序事件。

2.网络攻击事件。

网络攻击事件是指通过网络或其他技术手段，利用信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力攻击对信息系统实

施攻击，并造成信息系统异常或对信息系统当前运行造成潜在危害的网络安全事件。网络攻击事件包括拒绝服务攻击事件、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。

信息破坏事件是指通过网络或其他技术手段，造成信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的网络安全事件。信息破坏事件包括信息篡改事件、信息假冒事件、信息泄漏事件、信息窃取事件、信息丢失事件和其它网络破坏事件。

4.设备设施故障。

设备设施故障是指由于信息系统自身故障或外围保障设施故障而导致的网络安全事件，以及人为的使用非技术手段有意或无意的造成信息系统破坏而导致的网络安全事件。设备设施故障包括软硬件自身故障、外围保障设施故障、人为破坏事故和其它设备设施故障。

5.灾害性事件。

灾害性事件是指由于不可抗力对信息系统造成物理破坏而导致的网络安全事件。灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的网络安全事件。

6.其他事件。

其他事件是指不能归为以上基本分类的网络安全事件。

（二）事件分级

网络与信息安全事件分为四级：特别重大(Ⅰ级)、重大(Ⅱ级)、较大(Ⅲ级)、一般Ⅳ级)。

1.特别重大(Ⅰ级)

网络与信息系统发生全局性大规模瘫痪，事态发展超出自己的控制能力，对国家安全、社会秩序、学校利益造成特别严重损害的突发事件。

2.重大(Ⅱ级)

网络与信息系统造成全局性瘫痪，对国家安全、社会秩序、学校利益造成严重损害，需要上级相关部门协同处置的突发事件。

3.较大(Ⅲ级)

某一部分的网络与信息系统瘫痪，对学校的网络安全、教育教学秩序、教师和学生的权益造成一定损害，但可以在一定时间内通过相应技术手段进行重建和恢复，不需要跨部门协同处置的突发事件。

4.一般(Ⅳ级)

单一网络与信息系统受到一定程度的损坏，对教师和学生的教育教学、办公及宣传工作有一定影响，但不危害学校的网络整体安全和秩序的突发事件。

三、组织机构和职责任务

（一）领导机构与职责

学校网络与信息安全事件防范及应急处置工作由网络安全与信息化工作领导小组统一领导、指挥和协调。负责组织Ⅰ级和Ⅱ级校园网络突发事件应急预案的启动，督促检查网络突发事件处置情况及校内各单位（部门）在网络突发事件处置工作中履行职责情况；负责对全校各单位（部门）贯彻执行网络安全事件报告、应急处置预案的情况进行督促检查。

（二）办事机构与职责

党委宣传部负责全校网站的信息安全及其突发事件的应急处置工作，并指导、督促校内二级网站管理单位做好网站信息安全及突发事件的处置工作。

学校信息化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网络突发事件的协调处置；学校网络安全应急工作的技术支撑和保障。根据校内发生的网络突发事件程度，提出相应级别预案的启动，并及时收集、通报和上报网络突发事件处置的有关情况。

（三）校内相关单位与职责

学校各单位（部门）负责按照网络突发事件的处置预案，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；定期组织开展网络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。做到网络突发事件早发现、早报告、

早控制、早解决。

四、网络突发事件的处置预案

（一）等级判定

一旦发生网络突发事件，各相关单位应根据《信息安全技术信息安全事件分类分级指南》，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自主判定安全事件等级。

（二）处置流程

校园网络突发事件的事发、事中、事后各环节的报告与处置按照《河南农业大学关于印发〈信息技术安全事件报告与处置流程（试行）》的通知〉（校政信息〔2017〕3号）执行。Ⅰ级（特别重大）事件须向校长报告，Ⅱ级(重大)事件须向主管信息化工作的副校长报告，Ⅲ级(较大)事件须向校长办公室主任报告，Ⅳ级(一般)事件须向信息化办公室主任报告。

（三）应急处置措施

根据网络安全事件分类采取不同应急处置措施。

1.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。

2.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措施。

（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。

（3）信息破坏事件。判断信息破坏的原因，尽快恢复原始信息，查找信息窃取渠道，阻断信息窃取或信息泄露的途径，避免造成进一步损失。

（4）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。

（5）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。

（6）其它安全事件。可根据总的安全原则，结合具体情况，做出相应处理。

（四）后续处理

网络突发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。网络突发事件被抑制后，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。

五、预防措施

（一）加强网络与信息安全日常管理与防控

定期对网管人员进行安全责任意识教育和技术培训，健全有关网络与信息安全工作制度，建立预报预警监测体系，做好网络安全检查、风险评估和容灾备份，避免和减少网络与信息安全事故的发生。

（二）采取必要的技术防范措施，建立安全、稳定的网络运行环境

在校园网出入口安装监测系统，定期扫描网络漏洞，实时监测校园网和关键信息。重要信息系统要使用高可靠性设备和成熟

稳定的软件系统，并及时升级操作系统，做好系统与数据备份。遵守安全操作规范，内部用户适当限制访问权限，关闭不必要的网上服务等。

（三）加强网络安全宣传教育

将网络安全教育作为国家安全教育的重要内容，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传教育。同时，充分利用网络安全周等各种活动形式和传播媒介，开展网络安全基本知识和技能的宣传活动，提高在校师生的网络安全意识。

六、配套制度与问责

（一）人事变更报告

各单位的信息技术安全工作主管领导、主管部门负责人、联络员的联络方式发生变更，应及时将变更情况报信息化办公室。

（二）相关配套机制

各单位应根据实际建立值守制度，做到安全事件早发现、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。

（三）责任追究

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的，将对相关单位予以通报并追究相关人员的责任。

七、附则

本预案由信息化办公室负责解释，自印发之日起施行。

河南农业大学校长办公室　　2021年11月23日印