湖北大学文件

校信建管字〔2018〕1号

关于印发《湖北大学网络与信息系统（网站）安全突发事件应急预案》的通知

学校各单位：

经校党委常委会研究审定，现将《湖北大学网络与信息系统（网站）安全突发事件应急预案》予以印发，请认真组织学习并遵照执行。

湖北大学

2018年1月8日

湖北大学网络与信息系统（网站）安全突发事件应急预案

第一章 总则

第一条 为有效预防、及时控制和妥善处理我校网络与信息系统（网站）安全类突发事件，提高快速反应和应急处理能力，建立健全应急工作机制，确保校园网和重要计算机信息系统（网站）的实体安全、运行安全和数据安全，最大限度地减少网络与信息系统（网站）安全突发公共事件的危害，保护师生公共利益，制定本预案。

第二条 本预案编制依据《中华人民共和国网络安全法》、《计算机信息系统安全保护条例》、《湖北大学突发公共事件应急预案》等法律法规和规范性文件。

第三条 本预案适用于湖北大学各类网络与信息系统（网站）安全类突发事件的应急处置工作。本预案所指的网络与信息系统（网站）安全类突发事件是指：自然灾害（如地震、台风、雷电、洪水等）、事故灾害（如电力中断、网络损坏或火灾等）、人为破坏（如人为破坏网络线路、通信设施，黑客攻击、病毒攻击等）、设备软硬件故障等原因严重影响到校内各单位网络与信息系统（网站）的正常运行，出现业务中断、系统破坏、数据破坏或信息失泄密等，可能造成不良影响以及造成一定程度直接和间接经济损失的事件。

第四条 对网络与信息系统（网站）安全突发事件要分级处置。

第五条 网络与信息系统（网站）安全应急工作遵循“统一领导、分级负责、预防为本、及时控制、快速反应、以人为本”的原则。发生网络与信息系统（网站）安全突发事件时，相关单位第一责任人要立即深入第一线，掌握情况，开展工作，控制局

面。坚持预防与应急处置相结合，立足于安全防范，加强预警。在网络与信息系统（网站）安全突发公共事件发生时，按照快速反应机制，迅速处置，处置时注意区分突发事件性质，在依法处置的基础上，最大程度地减少危害和影响。

第二章　组织体系及职责

第六条 坚持学校党委、行政的统一领导，湖北大学网络与信息系统（网站）安全突发事件应急处置工作由湖北大学网络安全与信息化领导小组负责，下设应急处置办公室，与学校网络安全与信息化领导小组办公室合署办公。其主要职责是：组织协调学校网络与信息系统（网站）安全工作中可能出现的各种突发事件的处置工作，研究解决突发事件处置工作中的重大问题；组织制定学校网络与信息系统（网站）安全应急预案及其修订、完善工作，对突发事件相关信息进行及时收集、分析和研判，有效指导网络与信息系统（网站）安全工作。

第七条 在网络与信息系统（网站）安全事件发生时：

1. 学校办公室负责与主管部门和上级单位（如湖北省网信办、湖北省教育厅、武汉市网信办等）的沟通与协调。

2. 信息化建设与管理处负责校园网硬件设施、公共信息平台的安全及突发事件的应急处置工作，并为学校网络与信息系统（网站）安全工作及突发事件处置提供技术支撑。

3. 党委宣传部负责规范校内网站管理，并负责网络舆情管理及网络突发事件的预防和处理，同时指导、督促校内二级网站管理单位加强网站内容审核管理，做好网站信息安全及突发事件舆情监控的处置工作。

4. 保卫部（处）负责与公安机关、国家安全机关等部门的联络沟通，并协助相关单位进行网络与信息系统（网站）安全事件的查处。

第八条 各院系、职能部门、直属单位负责本单位网站和业务系统的信息安全和突发事件的处置工作。各院系、职能部门、直属单位也应制定相应的应急预案，包括应急预案的启动条件、应急处理流程、系统恢复流程，应急事件结束后要进行事后教育和培训。

第三章 突发事件分级

第九条 网络与信息系统（网站）安全突发事件按照可控性、严重程度和影响范围划分为四级：

特别重大网络与信息系统（网站）安全事件（Ⅰ级） 网络或信息系统（网站）发生全校性大规模瘫痪或出现长时间（时间长度不少于 12 小时）的全网性重大事件，或由于遭遇黑客攻击及其他原因造成信息恶意篡改、重要信息泄露产生非常严重影响的事件，或由于网站非法信息、谣言等引发学校大规模群体性事件，对学校教学、科研、办公秩序造成特别严重的影响，事态发展超出学校控制能力的突发事件。

严重网络与信息系统（网站）安全事件（Ⅱ级） 较大范围网络或信息系统（网站）发生严重故障，或较长时间（时间长度超过 4 小时，低于 12 小时）的全网性事件，或由于遭遇黑客攻击及其他原因造成一般（部分）信息篡改、泄露产生严重影响的事件，或由于网站非法信息、谣言等引发师生强烈反应，对学校教学、科研、办公秩序造成严重影响，需要跨部门协同处置的突发事件。

较大网络与信息系统（网站）安全事件（Ⅲ级） 局部区域网络或信息系统（网站）发生故障，或由于网站不良信息、谣言等，对学校教学、科研、办公秩序造成一定危害或影响，但不需要跨部门协同处置的突发事件。

一般网络与信息系统（网站）安全事件（Ⅳ级） 个别区域

网络或个别信息系统（网站）受到一定程度损坏，学校工作受到一般影响，但不危害正常工作秩序的突发事件。

第四章 安全措施与预防

第十条 加强网络与信息系统（网站）安全日常管理与防控。学校定期对网络与信息系统（网站）安全人员进行安全责任意识教育和技术培训，建立预报预警监测体系，避免和减少网络与信息系统（网站）安全事故的发生。

第十一条 加强技术防范措施，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，定期进行安全隐患排查和网络漏洞扫描，实时监测校园网和关键信息，每月通报存在安全隐患的信息系统和单位。

第十二条 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，口令账号规范管理，内部用户适当限制访问权限，关闭不必要的网络服务及端口等。

第五章 突发事件处置

第十三条 突发事件处置程序：

1. 各单位发现信息系统（网站）Ⅰ级、Ⅱ级安全事件，应在第一时间关闭服务或断开网络，进行分析确认、判定级别，并立即报应急处置办公室。

2. 应急处置办公室接到报告后及时做出决断，指挥有关部门启动应急预案并及时予以处置。

3. 事发单位与相关单位密切协作，进行紧急处置。并及时向应急处置办公室报告处置工作进展情况。

4. 事发单位配合应急处置办公室做好详细备案、查处及报告等工作。

5. 经专家组鉴定，突发事件险情或灾情已消除，或者得到有

效控制后，由应急处置办公室办公室宣布应急期结束，并予以公告，同时预案终止。

事发单位在第一时间需向应急处置办公室报送突发事件书面报告。报告内容应包括：事件发生时间、地点、内容，事件发生原因、处理情况及采取的措施，事故报告部门、报告时间等。

第十四条 突发事件情况报告：

突发事件发生时，一方面按照应急处置方法进行处置，同时按照网络与信息系统（网站）安全事件报告制度逐级上报。Ⅰ级（特别重大）事件须向党委书记和校长报告，Ⅱ级(重要)事件和Ⅲ级(较大)事件须向主管网络安全与信息化工作的副校长报告，Ⅳ级(一般)事件须向应急处置办公室主任报告。

第十五条 突发事件具体处置：

在灾害发生时，首先判断突发事件是否为自然灾害还是人为破坏两种情况，根据这两种情况把应急处置方法分为两个流程。

流程一：当突发事件为自然灾害时，应根据当时的实际情况，在保障人身安全的前提下，首先保障数据安全，然后是设备安全。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。

流程二：当人为或病毒破坏的事件发生时，具体按以下顺序进行：判断破坏的来源与性质，断开影响安全与稳定的设备，断开与破坏来源的网络物理连接，跟踪并锁定破坏来源的 IP 或其它信息，先备份然后修复被破坏的信息，恢复信息系统。

按照灾害发生的性质分别采用以下方案：

（一）网站出现不良信息、遭遇攻击处置措施：

1. 网站管理员应随时密切监视网站信息内容，发现网页内容被篡改、出现不良信息或遭遇攻击，应及时予以处置，并向应急

处置办公室报告情况。

2. 应急处置办公室接到报告后应作好必要的记录，同时指导校内有关部门，协助网站管理员，立即“先备份后删除”不良信息、修复破坏信息，查找、断开攻击来源，尽快恢复网站运行。

3. 对独立运行的网站管理员应妥善保存有关记录及日志，配合应急处置办公室追查非法信息来源，查找遭受攻击原因，完善防范措施。

4. 情况严重的，根据突发事件级别应及时向有关领导汇报，启动Ⅰ级或Ⅱ级预案。

5. 一旦发现不良信息传播速度超过处理速度，对独立运行的网站管理员可采取紧急措施关闭网站或所在网络。当网站管理员处置不够及时，应急处置办公室有权采取措施直接关闭部分或全部校园网。

（二）信息系统遭受破坏性攻击处置措施：

1. 所有应用系统日常应定期备份存储，其对应数据应有多日备份，并保存于安全处。

2. 应用系统遭到破坏性攻击，应立即停止应用系统运行，同时报告应急处置办公室。

3. 系统管理员应迅速配合应急处置办公室，检查系统日志，查找攻击来源和原因，采取相应处理措施，尽快恢复应用系统运行。

4. 情况严重的，根据突发事件级别应及时向有关领导汇报，启动相应的应急预案。

5. 一旦发现信息系统有不良信息传播速度超过处理速度或产生数据泄露，系统管理员可采取紧急措施关闭系统或所在网络。当系统管理员处置不及时或无法处置时，应急处置办公室有权采取措施直接关闭部分或全部校园网。

（三）校园网中断紧急处置措施：

1. 校园网中断后，信息化建设与管理处应立即判断故障节点，查明故障原因。

属学校管辖范围的，网络管理员立即赶赴现场予以恢复。属线路故障，应抢修维护线路；属路由器、交换机等网络设备故障，应立即与设备提供商联系更换设备，并调试畅通；属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调试畅通。如遇无法恢复情况，立即向有关厂商请求支援。

在学校管辖范围外的，立即与网络运营商（如电信、移动、联通、教育网等）联系，要求修复。

2. 预计网络中断 2 个小时以上的，应及时向应急处置办公室汇报，并由信息化建设与管理处发布停网原因通告。

3. 情况严重的，根据突发事件级别应及时向有关领导汇报。

（四）设备损坏紧急处置措施：

1. 核心网络设备、小型机、服务器、存储等关键设备损坏后，有关管理人员应立即向部门分管领导汇报，同时迅速查明原因。

2. 能够自行恢复并有备件设备的，应立即用备件替换受损部件。不能自行恢复且没有备件设备的，立即与设备提供商联系，请求派维修人员前来维修。

3. 如果设备 2 个小时内不能修复，应向应急处置办公室汇报，并根据实际情况采取相应处置措施。

4. 情况严重的，根据突发事件级别应及时向有关领导汇报。

（五）机房火灾应急处置措施：

1. 一旦机房发生火灾，要在第一时间内向武汉市公安消防 119 指挥中心报警，同时通知校保卫部（处）。分管领导和相关负责人要在第一时间赶到现场，组织抢救和灭火工作。

2. 机房火灾应急处置应遵照下列原则：一保人员安全；二保

关键设备、关键数据安全；三保一般设备安全。

3. 火灾发生要立即启动消防预案，迅速疏散人员，并根据现场实际情况联系校后勤保障部门，采取断电等安全措施，避免继发性危害。在消防队伍赶到现场后，提供施救信息，配合消防队伍组织救人和灭火抢险工作。

4. 情况严重的，根据突发事件级别应及时向有关领导汇报。

（六）其他情况的处置：

1. 如果设备或信息系统（网站）修复所需时间较长，应通过网站、官方微信、微门户等媒体做好宣传解释工作。

2. 其它未列出的不确定因素造成的灾害，可根据总安全原则，结合具体的情况，做出相应处理。

第六章 突发事件报告制度

第十六条 发生网络与信息系统（网站）安全事件的单位应当在发生事件后，首先以口头方式立即向应急处置办公室报告，并在第一时间将有关材料报送至应急处置办公室备案。报告内容包括：突发事件发生的时间、地点，突发事件级别，造成的后果，应急处置的过程、结果，突发事件结束的时间，以后如何防范类似灾害发生的建议与方案等。

重大网络涉政、涉稳事件、舆情信息须在发现的第一时间紧急向分管校领导、应急处置办公室报告。

第十七条 发生网络与信息系统（网站）安全事件的单位应当首先保护现场，立即与网络隔离，对发生的事件进行调查核实、保存相关证据。在处置过程中，任何单位和个人不得保留、存储、散布、传播所发现的有害信息。

第十八条 发生重大网络与信息系统（网站）安全事件的单位应当按照规定及时如实地报告事件的有关信息，不得瞒报、缓报或者授意他人瞒报、缓报。任何单位或个人如发现有瞒报、缓

报、谎报重大信息安全事件的情况时，有权直接向学校有关部门举报。

第十九条 发生重大网络与信息系统（网站）安全事件，有关责任单位、责任人有瞒报、缓报和漏报等失职情况，学校将予以通报批评；对造成严重不良后果的，将视情节轻重追究责任领导和责任人的责任；构成犯罪的，依法追究其法律责任。

第七章 附则

第二十条 重大活动期间，各级单位、部门应遵照国家和湖北省有关部门的相关规定，在以上规定的基础上，采取其他必要的应急处置措施。

第二十一条 本预案由湖北大学网络安全与信息化领导小组办公室负责解释。

第二十二条 本预案自发布之日起施行。

湖北大学学校办公室 2018 年 1 月 8 日印发

校对:孙 倩