遵义医药高等专科学校网络安全突发事件应急机制

为提高我校处理网络与信息安全突发事件的能力，形成科学、有效、反应迅速的应急工作机制，确保我校校园网络重要计算机信息系统的实体安全、运行安全和数据安全，最大限度地减轻网络信息安全突发事件的危害，保护师生权益，维护正常社会秩序、教学秩序，促进学校的和谐发展，特制定本预案。

一、适用范围

本预案适用于我校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Ⅰ—Ⅳ级网络与信息安全突发事件和可能导致Ⅰ—Ⅳ级的网络与信息安全突发事件的应对处置工作。

二、 指导思想

以维护学校正常的教学秩序和营造绿色健康的网络环境为中心，按照“预防为主，积极处置”的原则，进一步完善学校校园网络管理机制，提高突发事件的应急处置能力。

三、处置原则

网络与信息安全事件应急处置，依照“统一领导，快速反应，密切配合，科学处置”的组织原则和“谁主管谁负责、谁运行谁负责、谁使用谁负责”的协调原则，充分发挥各方面力量，共同做好网络与信息安全事件的应急处置工作。

四、组织机构及职责

（一）全校网络与信息安全事件应急处置工作由学校校园网络安全管理领导小组统一指导、指挥、协调。各相关单位须坚决执行领导小组的决定，密切配合，履行职责。

（二）相关职责

组织机构	职责
校园网络安全管理领导小组	1. 决定 I 级和 II 级网络与信息安全事件应急预案的启动。 2. 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。 3. 对全校各部门贯彻执行应急处置预案、应急处置准备情况进行督促检查。
党政办公室	1. 组织协调有关部门查处利用计算机网络泄密的违法行为。 2. 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。
校园网络安全管理领导小组办公室 网络信息中心	1. 定期组织检查计算机信息网络系统安全运行情况，及时排除各种安全隐患。 2. 负责计算机病毒疫情和大规模网络攻击事件的处置。 3. 负责校级网络与信息系统安全事件处置的技术支持。 4. 发生安全事故或计算机违法犯罪案件时，立即向公安机关网监部门报告并采取妥善措施，保护现场，避免危害的扩散，畅通与公安机关网监部门联系渠道
宣传部 团委 学生处	1. 负责学校舆情监测，对于涉及师生政治思想方面的倾向性、苗头性问题加强分析研判。 2. 负责舆情突发事件的处置。 3. 负责应急处置过程中的舆论处置。
保卫处	1. 密切配合公安部门，做好网络与信息安全事件的处置工作。 2. 负责及时收集、通报和上报网络与信息安全事件应急处置情况。
宣传部	负责校园网站新闻、图片、资源的上传及审核工作
其他系（部）、处（室）	1. 负责本部门内部的网络与信息安全管理和突发事件应急处置。 2. 配合校园网络安全管理领导小组落实相关应急处置措施。

五、应急处置

（一）响应分级

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，分为以下四级。

应急响应级别	响应条件	影响范围	控制事态的能力
Ⅰ级（特别重大）	发生严重有害程序事件、网络攻击事件、设备设施故障、灾害性事件造成全校大面积网络与信息系统瘫痪； 发生严重信息内容安全事件和信息破坏事件；	对学校正常工作造成特别严重损害	事态发展超出学校控制能力的安全事件
II级（重大）	发生有害程序事件、网络攻击事件、设备设施故障、灾害性事件造成全校性网络与信息系统瘫痪； 发生信息内容安全事件和信息破坏事件；	对学校正常工作造成严重损害	事态发展超出技术部门控制能力，需要学校各部门协同处置的安全事件
III级（较大）	发生有害程序事件、网络攻击事件、设备设施故障、灾害性事件造成学校某一区域网络与信息系统瘫痪；	对学校正常工作造成一定损害	网络信息中心可处理的安全事件
Ⅳ级（一般）	发生有害程序事件、网络攻击事件、设备设施故障、灾害性事件造成学校某一局部网络与信息系统故障	对学校某些工作造成影响，但不危及学校整体工作	网络信息中心可处理的安全事件

（二）校园网应急处理程序

1．接受事件报告：要留下报告人的联系电话和部门；

2．报告内容：事件报告接受人员在接受报告后的第一时间通知校园网络安全管理领导小组办公室；事故发生的时间、地点、机器号，事故的简要情况、故障现象、发生时正在操作情况等。

3．识别事件（由校园网络安全管理领导小组识别案事件的性质和严重性：病毒感染、系统入侵、恶意用户、不良信息等。），并决定是否启动事件处理程序。

4. 处置工作流程：

发现事故→报告事故→分析事故→技术处理→结果留存

（三）监测与预警

1.学校的网络与信息系统要进一步完善网络与信息安全突发事件监测、预测、预警制度。要落实责任制按照“早发现、早报告、早处置”的原则，加强对各类网络信息安全突发事件和可能引发突发事件的有关信息的收集、分析判断和持续监测。当发生网络信息安全突发事件时，应及时按规定向有关部门报告。初次报告最迟不得超过2小时，重大和特别重大的网络信息安全突发事件必须实行态势进程报告和日报告制度。报告内容主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施等。

2.学校校园网络安全管理领导小组应确立两个及以上的联系方式（电话：28776262，邮箱：xxzx@zunyiyizhuan.cn），师生可通过电话互联网等多种联系方式进行报警，避免因信息网络突发事件发生后，必要的信息通报与指挥协调通信渠道中断。

3.网络管理人员应定期对校园网的硬件设备进行一次状态检查。对用户上网实行监控，若发现有异常行为应立即关闭该用户的网络连接，及时记录在案，并对其警告和批评教育，严重违法行为立即上报有关部门。所有服务器的相关责任人认真做好检查记录，了解服务器的服务水平，对异常现象和事故及时处理并做好记录。

（四）校园网应急处理措施

网络信息安全预警处理与发布：对于可能发生或已经发生的网络信息安全突发事件，应立即采取措施控制事态，并在 2 小时内进行相应的风险评估，并及时按规定向校园网络安全管理领导小组报告；发现网络信息安全突发事件或事故时，信息中心配合对突发事件或事故进行风险评估，并把评估信息及时反馈给校园网络安全管理领导小组。

1．网站、网页出现非法言论事件紧急处置措施：

(1)网站、网页由信息中心人员负责监视信息内容。

(2)发现在网上出现非法信息时，信息中心应立即向校园网络安全管理领导小组负责人通报情况；情况紧急的，应先及时采取删除等处理措施，再按程序报告。

(3)信息安全相关负责人应在接到通知后赶到现场，作好必要记录，清理非法信息，妥善保存有关记录及日志或审计记录，强化安全防范措施，并将网站网页重新投入使用。

(4)追查非法信息来源，并将有关情况向校园网络安全管理领导小组汇报。

(5) 校园网络安全管理领导小组召开小组会议，如认为事态严重，则立即公安部门报警。

2．黑客攻击事件紧急处置措施

(1)当发现网页内容被篡改，或通过入侵检测系统发现有黑客正在进行攻击时，应立即向信息安全负责人通报情况。

(2)信息安全相关负责人应在接到通知后立即赶到现场，并首先将被攻击的服务器等设备从网络中隔离出来，保护现场，并将有关情况向校园网络安全管理领导小组汇报。

(3)对现场进行分析，并写出分析报告存档，必要时上报主管部门。

(4)恢复与重建被攻击或破坏系统。

(5) 校园网络安全管理领导小组召开小组会议，如认为事态严重，则立即向公安部门报警。

3．病毒事件紧急处置措施

(1)当发现有计算机被感染上病毒后，应立即向信息中心报告，将该机从网络上隔离开来。

(2)信息中心在接到通报后立即赶到现场。

(3)对该设备的硬盘进行数据备份。

(4)启用反病毒软件对该机进行杀毒处理，同时通过病毒检测软件对其他机器进行病毒扫描和清除工作。

(5)如果现行反病毒软件无法清除该病毒，应立即向校园网络安全管理领导小组报告，并迅速联系有关产品商研究解决。

(6) 校园网络安全管理领导小组召开会议，认为情况严重的，应立即向公安部报警。

(7)如果感染病毒的设备是主服务器，信息中心应立即告知职能部门做好相应的清查工作。

4．软件系统遭破坏性攻击的紧急处置措施

(1)各职能部门负责人应做好对重要的软件系统的备份，与软件系统相对应的数据必须每周按时进行备份，并将它们保存于安全处。

(2)一旦软件遭到破坏性攻击，应立即向信息中心报告，并将该系统停止运行。 .

(3) 检查信息系统的日志等资料，确定攻击来源，并将有关情况向汇报，再恢复软件系统和数据。

(4) 校园网络安全管理领导小组召开会议，如认为事态严重，则立即向公安部门报警。

5．数据库安全紧急处置措施

(1)信息中心做好主要数据库系统的双盘备份设置，并至少要准备两个以上数据库备份。

(2)一旦数据库崩溃，信息中心应立即启动备用系统，对事件经评估后，决定是否向校园网络安全管理领导小组负责人报告。

(3)在备用系统运行期间；信息安全工作人员应对系统进行维修并作数据恢复。

(4)如果两套系统均崩溃而无法恢复，应立即向有关厂商请求紧急支援。

6．广域网外部线路中断紧急处置措施

(1)广域网线路中断后，各处室、办公室信息负责人员并立即向信息中心汇报。

(2)、信息中心负责人员接到报告后，应迅速组织信息中心人员判断故障节点，查明故障原因。

(3)如属我校管辖范围，由信息中心工作人员立即予以恢复。

(4)如属电信部门管辖范围，立即与电信维护部门联系，要求修复。

7．局域网中断紧急处置措施

(1)各部门平时应准备好网络设备管理，存放在指定的位置。

(2)局域网中断后，信息中心人员应立即判断故节点，查明故障原因，并向网络中心负责人汇报。

(3)如属线路故障，应重新安装线路。

(4)如属路由器、交换机等网络设备故障，应立即从指定位置将备用设备取出接上，并调试通畅。

(5)如属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调测通畅。

8．设备安全紧急处置措施

(1)服务器关键设备损坏后，值班人员应立即向信息中心报告。

(2)信息中心人员立即查明原因。

(3)如果能够自行恢复，信息中心人员应立即用备件替换受损部件。

(4)如属不能自行恢复的，立即与设备提供商联系，请求派维护人员前来维修。

(5)如果设备一时不能修复，应向校园网络安全管理领导小组汇报。

六、保障措施

（一）队伍保障

加强队伍建设，不断提高安全岗位工作人员的信息安全防范意识和技术水平，确保安全事件处置得当。

（二）技术保障

不断完善网络安全整体方案，加强技术管理，确保信息系统的稳定与安全。

（三）资金保障

信息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维专项资金，提出本年度应急处置工作相关设备和工具所需经费，上报至财务处纳入年度预算，由学校给予资金保障。

（四）安全培训和演练

信息中心定期对相关工作人员进行网络与信息系统安全知识培训，增强预防意识和应急处置能力，有针对性地开展应急演练，确保相关措施有效落实。

信息技术网络管理中心

2018年10月1日