河南工业大学网络安全事件
应急预案与处置流程

一、适用范围

本预案根据教育部《教育系统网络安全事件应急预案》编制，适用于河南工业大学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。

二、术语和定义

本预案所称的网络与信息系统，是指由河南工业大学校园网络、计算机及其相关配套设备、设施构成，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理系统。

信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件等七个基本分类。

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”的基本原则，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

1、全校网络与信息安全事件应急处置工作由学校信息化领导小组统一指挥、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。

2、职责分工

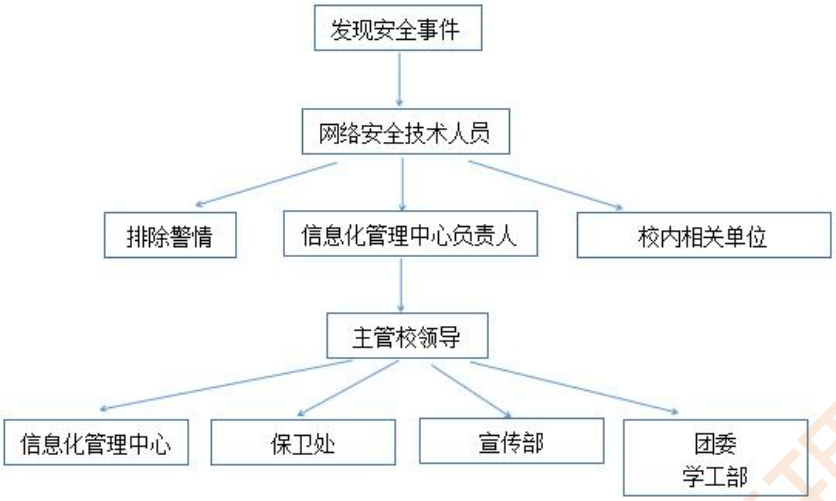
组织机构	职责
网络安全和信息化工作领导小组	决定Ⅰ级和Ⅱ级网络与信息安全事件应急预案的启动。 对全校各单位贯彻执行应急处置预案、应急处置准备情况进行督促检查。 督促检查安全事件处置情况及各有关单位在安全事件处置工作中履行职责情况。
党委办公室 校长办公室	组织协调有关部门查处利用计算机网络泄密的违法行为。 牵头组织重大敏感时期、重要活动、重要会议期间发生的信息安全事件的协调处置。
信息化管理中心	负责校园基础网络系统安全。 负责计算机病毒传播和大规模网络攻击事件的处置。 负责校级网络与信息系统安全事件处置的技术支持。
党委宣传部 校团委 学生工作部 研究生工作部	负责学校舆情监测，对于涉及师生政治思想方面的倾向性、苗头性问题加强分析研判。 负责舆情突发事件的处置。 负责应急处置过程中的舆论处置。
保卫处	密切配合公安部门，做好网络与信息安全事件的处置工作。
其他单位	负责本单位内部的网络与信息安全管理和突发事件应急处置，对照本预案建立单位内部应急处置机制。 配合各单位落实相关应急处置措施。

五、应急处置

1、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，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、核心设备设施故障、灾害性事件所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；	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、灾害性事件造成局部性网络与信息系统瘫痪； 发生信息内容安全事件；	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较小范围的网络与信息系统瘫痪；	对学校正常工作造成一定损害	信息化管理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小范围内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	信息化管理中心可处理的安全事件

2、响应程序



3、常见安全问题紧急处理流程

（一）有害程序事件：首先确认有害程序的源 IP 地址，对有害程序源地址的网络进行限制，再联系相应的网络管理员进行问题排查。有害程序处理完毕，经信息化管理中心核查无误后，恢复源地址的网络访问。

（二）网络攻击事件：首先根据网络攻击源进行追踪，对网络攻击事件的源地址进行封禁处理。若攻击源是公网地址，则在出口防火墙对攻击源进行限制。若攻击源是内网地址，则在网络交换机上对攻击源进行限制，联系相应的网络管理员进行问题排查处理。

（三）信息内容安全事件：对于信息内容安全事件，首先在反代上取消相应服务发布，其次在 DNS 上停止该服务的解析。及时联系相应的系统管理员进行处理，按《河南工业大学信息系统测试通报制度和系统版本管理办法》执行相关操作。处理完成后，经过信息化管理中心审核通过后，再启用 DNS 解析和反代发布。

对于没有及时处理或不予配合的应用系统，信息化管理中心有权终止服务，因此造成的不良影响由对应系统单位负责。

（四）设备设施故障、灾害性事件：网络安全管理员及时处理设备设施故障，并及时上报信息化管理中心主任。对于灾害性事件网络安全管理员应第一事件采取措施并上报相关负责人。

六、保障措施

1、队伍与技术保障

加强网络安全队伍建设，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。

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。

2、设备与资金保障

信息化管理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、软件的部署及安全运维专项资金，上报财务纳入年度预算。

3、安全培训和演练

信息化管理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，落实网络 24 小时安全值班制度，确保相关措施有效落实。

信息化管理中心

2020 年 4 月 21 日