合肥职业技术学院办公室

校办发〔2022〕4号

关于印发《合肥职业技术学院网络与信息安全事件应急预案（修订）》的通知

各部门、各二级学院：

现将《合肥职业技术学院网络与信息安全事件应急预案（修订）》印发给你们，请遵照执行。

合肥职业技术学院办公室

2022年1月15日

合肥职业技术学院网络与
信息安全事件应急预案（修订）

总则

第一条 为提高学校应对网络与信息安全突发事件的能力，建立健全科学、有效、反应迅速的网络信息安全监测和应急工作机制，预防和减少网络与信息安全突发事件的危害，维护学校安全稳定和教学工作秩序，特制定本预案。

第二条 依据《中华人民共和国网络安全法》、《中华人民共和国突发事件应对法》、《国家网络安全事件应急预案》、《国家信息化领导小组关于加强信息安全保障工作的意见》、《关于信息安全等级保护工作的实施意见》、《关于开展信息安全风险评估工作的意见》、《国家突发事件总体应急预案》、《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际互联网管理暂行规定》、《信息安全事件分类分级指南》（GB/Z 20986-2007）等相关规定。

第三条 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。

第一章 工作原则

第四条 网络与信息安全突发事件的应对需坚持以下原则：

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”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。

第二章　事件分类分级

第六条 事件分类。网络与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、设备设施故障和灾害性事件等。

1.有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

2.网络攻击事件分为拒绝服务攻击事件、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.信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

4.信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会

稳定和公众利益的事件。

5.设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

6.灾害性事件是指由自然灾害等其他突发事件导致的网络与信息安全事件。

第七条 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。

第三章　应急处置工作领导小组及主要职责

第八条　应急处置工作领导小组组成

组　长：校党委书记、校长

副组长：分管宣传部、保卫处、现代教育技术中心工作的校领导，发生网络与信息安全事件的二级学院（部门）分管校领导

成　员：各学院党政主要负责人、各部门主要负责人

第九条　应急处置工作领导小组职责。

1.贯彻落实国家、省及上级单位有关网络与信息安全的方针政策和法律法规，组织制定学校《网络与信息安全事件应急预案》。

2.领导统筹网络与信息安全事件应对工作，建立健全联动处置机制，启动应急预案，负责网络与信息安全事件处置的组织指挥。

3.审定、部署、检查网络与信息安全事件的预防预警、应急处置、调查评估、信息发布、应急保障等工作，研究解决处置工作中的问题。

第十条　应急处置工作领导小组下设办公室，办公室设在现代教育技术中心。

主　任：现代教育技术中心主任

副主任：现代教育技术中心副主任，宣传部分管信息化工作的科长

成　员：宣传部、现代教育技术中心相关工作人员，各部门信息化联系人。

第十一条　应急处置工作领导小组办公室职责。

1.组织起草学校《网络与信息安全事件应急预案》等相关规定。

2.承担值守应急工作，指导各二级学院（部门）建立网络与信息安全突发事件的预警和防控工作；接收并处理网络与信息安全应急信息报告，配合相关部门积极开展应对处置工作。

3.负责网络与信息安全事件的预防预警、应急处置、调查评估、信息发布、应急保障、隐患排查整改等工作；组织开展网络与信息安全培训，定期组织演练；收集信息安全事件报告统计数据、编制统计报告、汇总工作情况、撰写工作总结；负责与上级网络与信息安全应急协调机构的沟通联络工作。

4.负责完成应急处置工作领导小组交办的其它工作。

第四章　信息监测与报告

第十二条 明确网络与信息安全监测责任。

1.宣传部负责互联网舆情监测，以及学校官网、官方新媒体平台的信息监控。

2.现代教育技术中心负责监测网络和信息系统的通信和资源使用异常，网络和信息系统瘫痪，应用服务中断或数据篡改、丢失等情况。

3.保卫处负责外围设施的安保、网络从业人员审查工作，以及

事件发生后与公安机关相关部门的联系协调工作。

4.各二级学院、各部门负责本二级学院、本部门管理的二级网站、应用信息系统、动态性专题网站和新媒体平台的信息审核与监测。

第十三条 落实监测报告责任制。各二级学院、各部门要指定专人负责信息监测工作，要落实责任制，按照“早发现、早报告、早处置”的原则，加强对各类网络与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。

第十四条 当发生网络与信息安全突发事件时，按规定及时向应急处置工作领导小组办公室报告，重大的网络与信息安全突发事件要有日报告和态势进程报告。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。重要敏感时期要实行日报告制度，各二级学院、各部门按照应急处置工作领导小组办公室要求的报告频度及时上报监测情况。

第十五条 各二级学院（部门）负责信息监测的人员一旦发现网络与信息安全事件，应立即采取措施控制事态，及时进行风险评估，并向应急处置工作领导小组办公室报告。

1.对于发生一般(Ⅳ级)级别的网络与信息安全事件，由应急处置工作领导小组办公室处理，并将处理情况向应急处置工作领导小组报告。

2.对于发生较大(Ⅲ级)、重大(Ⅱ级)、特大(Ⅰ级)的网络与信

息安全事件，由应急处置工作领导小组办公室第一时间向应急处置工作领导小组报告，按照本预案处置。应急处置工作领导小组接到报告后，应迅速召开会议，研究确定网络与信息安全突发事件的态势及研究应急处置方案。

第五章　网络与信息安全事件应急处置

第十六条　相关二级学院（部门）对有权限直接处理的校园内发生的网络与信息安全事件，要按以下流程应急处置。

1.校园网络不良信息处置

发生网络与信息安全事件二级学院（部门）的信息员要及时删除不良信息，并清查整个网站所有内容，确保没有任何其它不良信息。

信息员应将事件具体情况以书面形式上报至宣传部及现代教育技术中心。

现代教育技术中心组织相关工作人员立即通过内网防火墙切断网站服务器外网连接。备份不良信息的相关目录、日志。隔离出现不良信息的目录，进行安全性检测，去除不安全隐患，关闭不安全栏目。如果服务器遭到破坏则恢复备份数据。恢复正常后重新连接网站服务器及防火墙外网网络连接，并测试网站运行。

2.校园网络异常和网络恶意攻击事故处置

现代教育技术中心组织相关人员研判确定该攻击来源和影响范围。根据需要可以紧急切断中心网络的服务器及公网的网络连接，

以保护重要数据及信息。如果攻击来自学校外，通过网络安全防护设备对此类攻击进行阻拦和过滤，组织 技术人员并联系专家进行分析研究应对措施，并视情况严重程度决定是否关闭外 网访问；如果攻击来自学校内，查找确定攻击源，切断攻击源相关设备网络连接。查到攻击源计算机 IP 地址后，关闭该计算机校园网络连接，通知使用者及所属部门进行处理。

如果攻击源来自学校内办公电脑，电脑使用者需清除病毒、恶意程序、木马程序或重装操作系统，运行 5 小时以上没有问题后提出联网申请，现代教育技术中心测试无问题后再接入校园网。

如果查明是学校内人员主观恶意网络攻击，应急处置工作领导小组视情节轻重，提交学校相关部门按学校规定进行处理，涉嫌触犯法律的移送公安机关依法处理。

3.网络系统漏洞应急处置

现代教育技术中心接到系统漏洞通报或定期扫描检查发现高危系统漏洞后，组织相关技术人员进行研究分析，制定解决方案。

需要在核心网络设备和服务器进行封闭协议及端口、停止服务的操作由现代教育技术中心在 24 小时内完成处理。

需要通过更新操作系统补丁的操作由现代教育技术中心协助使用部门尽快完成。

需要应用软件进行升级更新处理的，现代教育技术中心通知使用部门联系软件厂商及时完成处理，在没有处理完成前关闭服务器

外网访问。

需要在办公电脑进行升级补丁的，由现代教育技术中心在校园网及时发布漏洞情况和处理步骤的通知，各二级学院（部门）组织进行升级维护工作。

4.计算机病毒应急处置

各二级学院（部门）信息员发现计算机感染病毒后，应立即将感染病毒的办公电脑断网，在病毒彻底清除干净前禁止连接到网络，并对该设备的硬盘进行数据备份。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。

如果感染病毒的设备是服务器，并且反病毒软件无法清除该病毒，信息员应立即联系有关产品厂商研究解决并上报本部门负责人和现代教育技术中心具体负责人。现代教育技术中心负责人组织相关技术人员研究采取恢复备份等措施，并立即告知各相关二级学院（部门）做好相应的清查工作。

5.互联网舆情负面信息

由于学校对校园网以外的互联网舆情负面信息没有直接处理权限，要按以下流程应急响应。

宣传部负责指定专人进行互联网舆情监测，每日定时搜索、收集负面舆情信息，重要敏感时期提高每日搜索次数。突发事件发生后，立刻向应急处置工作领导小组报告，并组织人员 24 小时收集信息，做到第一时间监测、收集、研判舆情发展走向，及时上报舆

情动态。舆情监测及信息收集人员要及时监看网络、广播、电视、报刊等媒体，实时收集核查信息来源、扩散情况（转载转播频率、点击率、收视率）等相关指标，跟踪掌握舆情发展、衍变、处置成效等情况，为应急处置工作领导小组提供参考意见。

在处置负面舆情信息时，坚决维护党和国家权威，维护社会稳定，维护学校形象。应急处置工作领导小组办公室负责及时展开事件调查，快速形成报告， 为澄清事实、消除影响提供有力证据。针对调查情况，及时研究并向应急处置工作领导小组提出事件应急处置的对策和建议。由应急处置工作领导小组根据事件性质及严重程度决定是否向上级主管部门报告、请求支援、删除网上负面信息。

充分发挥团结协作精神，上下沟通、左右协调，步调统一、各司其职，形成强大的工作合力。实事求是、循序渐进地发布信息，统一发布口径，报请应急处置工作领导小组审定，根据事件性质和演变情况决定是否组织新闻发布会。宣传部负责组织做好相关网络、报刊、广播、电视等媒体的联络沟通及接待工作。如校园内发生网络与信息安全事件，需进行信息发布与新闻报道的，参考上述办法。

第六章　后期处置及保障

第十七条　重大处置工作结束后，应急处置工作领导小组办公室对事件处置工作进行总结报告。报告要素：事件发生时间、地点、原因、信息来源，事件类型、性质、危害及损失程度，事件发展趋势、采取处置措施等。

第十八条 校党委表彰奖励在舆情处置工作中做出突出贡献的二级学院和个人，追究引起重大舆情和造成重大负面影响、严重后果的相关责任人的责任。

第十九条 应急保障。

1.信息保障。建立健全并落实网络与信息安全突发事件信息收集、传递、报送、处理等各环节运行机制，完善信息传输渠道，确保信息报送渠道的安全畅通。

2.物资保障。应储备充足物资和备用设备，保障应对网络与信息安全突发事件的需求。

3.资金保障。将应急资金纳入财务预算，为突发事件舆情处置工作提供必要的财力支持。

4.人员保障。其他二级学院（部门）相关人员作为网络与信息安全突发事件应急预备队，可根据工作需要，安排应急工作。

第七章 附则

第二十条 本预案由网络与信息安全事件应急处置工作领导小组办公室负责解释。

第二十一条 本预案自2022年1月15日起实施。

附件

合肥职业技术学院网络与信息安全突发事件应急处置流程图