

福建中医药大学办公室文件

闽中医办〔2022〕4号

福建中医药大学办公室关于印发《福建中医药大学网络安全事件应急预案》的通知

各学院（部），各处、室，各直属机构，各附属单位：

《福建中医药大学网络安全事件应急预案》已经校长办公会 2022 年第 1 次会议审议通过，现印发给你们，请遵照执行。
特此通知。

福建中医药大学办公室
2022 年 1 月 19 日



福建中医药大学网络安全事件应急预案

一、总则

(一) 编制目的

根据《国家网络安全事件应急预案》《福建省网络安全事件应急预案》和《福建省教育系统网络安全事件应急预案》要求，健全完善学校网络安全事件应急工作机制，规范网络安全事件工作流程，提高学校网络安全应急处置能力，预防和减少网络安全事件造成的损失和危害，维护学校安全稳定。

(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》《关于加强教育行业网络与信息安全工作的指导意见》《教育系统网络安全事件应急预案》《福建省网络安全事件应急预案》《福建省教育系统网络安全事件应急预案》《信息安全技术信息安全事件分类分级指南》（GB/Z20986-2007）等文件。

(三) 适用范围

本预案适用于福建中医药大学各学院（部），各处、室，各直属机构网络与信息系统的突发安全事件应急处置。

(四) 事件分类

按照《教育系统网络安全事件应急预案》《福建省网络安全事件应急预案》《福建省教育系统网络安全事件应急预案》等规定，本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对学校 and 各单位网络和信息系统或者其中的数据造成危害，对学校师生造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、设备设施故障、灾害性事件和其他事件。

网络安全事件分类以及信息内容安全事件应对，参照有关规定和办法。

(五) 事件分级

参照《教育系统网络安全事件应急预案》《福建省网络安全事件应急预案》《福建省教育系统网络安全事件应急预案》等事件分级规定，结合学校实际，可能造成的危害，可能发展蔓延的趋势等，学校网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

1. 符合下列情形之一的，为特别重大网络安全事件（Ⅰ级）：

（1）网站、信息系统被攻击篡改或破坏性病毒、文件传播，导致反动言论或者谣言等违法信息大面积扩散，给国家、社会、学校带来严重损害；

（2）国家机密、大面积个人信息或关键数据丢失或被窃取、

篡改；

(3) 其他对学校安全稳定和正常秩序构成特别严重威胁，造成特别严重影响的网络安全事件。

2. 符合下列情形之一且未达到特别重大网络安全事件等级的，为重大网络安全事件（Ⅱ级）：

(1) 网站、信息系统被攻击篡改或破坏性病毒、文件传播，导致反动言论或者谣言等违法信息在一定范围内扩散，给国家、社会、学校带来严重损害的；

(2) 较大数量的个人信息或关键数据丢失或被窃取、篡改；

(3) 其他对学校安全稳定和正常秩序构成较为严重威胁，造成较为严重影响的网络安全事件。

3. 符合下列情形之一且未达到重大网络安全事件等级的，为较大网络安全事件（Ⅲ级）：

(1) 网站、信息系统被攻击篡改或破坏性病毒、文件传播，导致反动言论或者谣言等违法信息小范围扩散，给国家、社会、学校带来轻微损害的；

(2) 学校关键信息基础设施遭受网络攻击，学校门户网站、关键业务或校级核心业务信息系统（网站）遭受较小损失，导致一定程度影响师生工作、生活，或者造成较小经济损失，或者造成轻微不良社会影响的；

(3) 其他对学校安全稳定和正常秩序构成较小威胁，造成较

小影响的网络安全事件。

4. 一般网络安全事件（IV级）：

除上述情形外，对学校安全稳定和正常秩序构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

（六）工作原则

1. 统一指挥、密切协同。学校网络安全和信息化领导小组（以下简称“网信领导小组”）统筹协调全校网络安全应急指挥工作，建立与上级主管部门和网络安全职能部门、专业机构等多方参与的协调联动机制，加强预防、监测、报告和应急处置等环节的紧密衔接，做到快速响应、正确应对、果断处置。

2. 分级管理、强化责任。按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，学校各职能部门、各学院、直属单位党组织对本部门、本单位网络安全工作负主体责任。领导班子主要负责人是网络安全工作第一责任人，主管网络安全的领导班子成员是直接负责人。

3. 预防为主、平战结合。坚持事件处置和预防工作相结合，做好事件预防、预判、预警工作，加强应急支撑保障能力和安全态势感知能力建设。提高网络安全事件快速响应和科学处置能力，抓早抓小，争取早发现、早报告、早控制、早解决，严控网络安全事件风险和影响范围。

二、组织机构与职责

（一）领导机构与职责

网信领导小组统筹协调学校网络安全事件应急工作，指导学校各部门、各单位网络安全事件应急处置；发生特别重大网络安全事件和重大网络安全事件时，负责组织指挥和协调事件处置。

（二）办事机构与职责

在网信领导小组的领导下，网信领导小组办公室负责网络安全应急管理事务性工作，对接上级主管部门并负责向上级主管部门报告网络安全事件情况，提出特别重大网络安全事件应对措施建议，统筹组织网络安全事件的预防、监测、报告和应急工作，指导网络安全支撑单位做好应急处置的技术支撑工作。

1. 网信领导小组职责

（1）根据网络安全事件事态发展，向上级主管部门汇报有可能演变成I级和II级的网络安全事件，并做好相关准备工作；

（2）责成网信领导小组办公室组织技术力量响应和处置涉及学校的I级和II级网络安全事件；

（3）督促检查网络安全事件处置情况及各有关单位在网络安全事件处置工作中履行职责情况。

2. 网信领导小组办公室职责

(1) 负责网络安全工作的组织、协调和监督，制定相关制度和应急预案；

(2) 根据校内发生的网络安全事件程度提出III 级及以下级别预案的启动，组织协调各单位落实应急预案，共同做好处置工作；

(3) 负责及时收集、通报和上报网络安全事件处置的有关情况。

(4) 对全校各二级单位、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。

3. 校内二级单位、部门

(1) 校内各单位、各部门在网信领导小组办公室指导下负责本单位内部发生的网络信息安全管理 and 突发事件的应急处置工作，应对照依据本预案，建立本部门网站及信息系统相应的应急预案，报网信领导小组办公室备案；

(2) 当发生网络安全事件时，应先通过电话紧急通知网络安全与信息化办公室，随后按要求在OA系统上填写《网络安全事件报告单》（见附件1）；

(3) 积极支持配合网信领导小组办公室及网络安全与信息化办公室进行应急响应处置工作。

4. 网络安全与信息化办公室职责

(1) 负责校园基础网络、核心网络系统安全，保证校园

网络提供不间断服务；

（2）负责全校性信息系统的安全事件处置工作；

（3）负责计算机病毒疫情和大规模网络攻击事件的处置；

（4）负责全校网络安全事件处置的技术支持工作。

5. 校内各单位、各部门的官方微博、微信、移动APP客户端（以下简称“两微一端”）等新媒体平台按照《福建中医药大学微信、微博等新媒体平台管理办法》及《福建中医药大学管理服务类教育移动互联网应用管理办法》进行登记、备案和管理，按照“谁主管谁负责、谁运维谁负责、谁发布谁负责”的原则，落实保障措施。

三、监测与预警

（一）预警分级

建立健全校内网络与信息系统（网站）监测预警机制，按照紧急程度、发展态势和可能造成的危害程度，学校网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生特别重大、重大、较大和一般网络安全事件。

（二）安全监测

网信领导小组办公室通过多种渠道监测、发现已经发生的网络安全事件，将掌握的情况立即通知学校相关单位。

网络安全与信息化办公室负责进行全校范围内网络与信

息系统（网站）实施安全监测；通过多种途径监测、汇总漏洞、病毒、网络攻击等网络安全威胁信息，依托协同办公、邮件等平台实现安全威胁信息的发布。

各单位按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的要求，负责实施本单位网络与信息系统（网站）的安全监测，一旦发现网络安全威胁应立即报送预警信息至网络安全与信息化办公室，不得迟报、谎报、瞒报、漏报。

（三）预警研判和发布

网信领导小组办公室对监测信息进行研判，对发生网络安全事件的可能性及其可能造成的影响进行分析评估，认为需要立即采取防范措施的及时通知校内有关单位；认为可能发生重大以上（含重大）网络安全事件的信息，应立即向网信领导小组报告，网信领导小组向上级主管部门报告。

网信领导小组可根据网信领导小组办公室的监测研判情况，发布学校黄色及以下预警，网信领导小组办公室可根据监测研判情况发布蓝色预警。对达不到预警级别但又要发布警示信息的，可发布风险提示信息。

预警信息包括预警级别、起始时间、可能影响范围、警示事项、应采取的措施、时限要求等。

（四）预警响应

1. 红色和橙色预警响应

(1) 网信领导小组办公室组织预警响应工作，接受上级部门对预警响应的指导，联系有关部门、专业机构和专家，组织对事态发展情况进行跟踪研判，研究制定防范措施和应急工作方案，协调调度资源，做好各项准备，重要情况报学网信领导小组。

(2) 组织跟踪和分析研判，密切关注事态发展，做好监测分析和信息搜集工作；开展应急处置或准备、风险评估；密切关注舆情动态，加强教育引导，采取有效措施管控风险。

(3) 有关单位应按照网信领导小组办公室要求，实行 24 小时值守，相关人员保持通信畅通。

(4) 网信领导小组办公室做好与专业机构沟通协调的准备工作；信息中心进入待命状态，研究制定应对方案，检查应急设备、软件工具等，确保处于良好状态。

2. 黄色预警响应

(1) 网信领导小组办公室按网信领导小组要求，会同网络安全与信息化办公室和事发单位做好预警响应工作。

(2) 网信领导小组办公室及时将事态发展情况上报网信领导小组。

3. 蓝色预警响应

网信领导小组办公室根据预案，组织做好预警响应工作。

(五) 预警解除

网信领导小组根据实际情况，确定是否解除黄色预警；网信

领导小组办公室确定是否解除蓝色预警；及时发布预警解除信息。

四、应急处置

（一）初步处置

网络安全事件发生后，网络安全与信息化办公室采取相关技术措施将影响降到最低，并提取网络攻击、网络入侵或网络病毒等证据。网络安全与信息化办公室应组织应急队伍和工作人员根据不同的事件类型和事件原因，采取科学有效的应急处置措施。

经分析研判初判为特别重大、重大网络安全事件的，网信领导小组办公室应立即报告网信领导小组，由学校上报省教育网安应急办；对人为破坏活动，应同时报当地网信部门和公安机关。

（二）应急响应

网络安全事件应急响应分为Ⅰ级、Ⅱ级、Ⅲ级、Ⅳ级等四级，分别对应学校特别重大、重大、较大和一般网络安全事件。

1. Ⅰ级响应

发生特别重大网络安全事件，由网信领导小组报省教育网安应急办，提出Ⅰ级响应的建议，经批准后，成立应急响应工作组。

（1）启动指挥体系

①工作组进入应急状态，履行应急处置工作统一领导、指挥、协调的职责。工作组成员保持24小时联络畅通，网信领导小组办公室和网络安全与信息化办公室24小时值守。

②校内有关单位、网信领导小组办公室、网络安全与信息化

办公室和人员进入应急状态，在工作组的统一领导、指挥及协调下组织人员开展应急处置或支援保障工作，启动 24 小时值守，并派员参加应急响应工作组的工作。

(2) 掌握事件动态

①跟踪事态发展。学校工作组与与教育厅网信领导小组办公室保持联系，及时填写《教育系统网络安全事件情况报告》，将事态发展变化情况和处置进展情况上报教育厅网信领导小组办公室。

②检查影响范围。校内有关单位立即了解本单位主管的网络和信息系统是否受到事件的波及或影响，并将有关情况及时报网信领导小组办公室。

③及时通报情况。网信领导小组办公室负责整理上述情况，重大事项及时报学校应急响应工作组和省教育网安应急办，并通报校内有关单位。

(3) 决策部署

工作组组织校内有关单位、专家组、应急技术支撑队伍等方面及时研究对策意见，对处置工作进行决策部署。

(4) 处置实施

①控制事态防止蔓延。采取各种技术措施、管控手段，最大限度阻止和控制事态蔓延。

②消除隐患恢复系统。根据事件发生原因，针对性制定解决

方案，备份数据，保护设备、排查隐患。对业务连续性要求高的受破坏网络与信息系统要及时组织恢复。

③调查取证。事发单位应在保留相关证据的基础上，开展问题定位和溯源追踪工作。积极配合当地网信部门和公安机关开展调查取证工作。

④信息发布。宣传部根据实际，组织网络安全突发事件的应急新闻工作，未经批准，校内其他单位一律不得擅自发布相关信息。

⑤协调上级主管部门支持。处置中需要技术及工作支持的，由网信领导小组办公室根据实际，报请工作组批准后，商省教育网安应急办予以支持。

⑥次生事件处置。对于引发或可能引发其他安全事件的，网信领导小组办公室应及时按程序上报。在相关部门应急处置中，网信领导小组办公室应做好协调配合工作。

2. II级响应

网络安全事件的II级响应，由省教育网安应急办确定并发布。

(1) 事发后网信领导小组办公室及校内有关单位进入应急状态，按照相关应急预案做好应急处置工作。

(2) 网信领导小组办公室及时填写《教育系统网络安全事件情况报告》，报省教育网安应急办，同时并将有关重大事项及时通

报网信领导小组和校内有关单位。

(3) 网信领导小组办公室协调其他单位和网络安全应急技术支撑队伍配合和支持处置工作。

(4) 校内有关单位根据通报，结合各自实际有针对性的加强防范，防止造成更大范围影响和损失。

3. III级响应

III级响应由网信领导小组确定，网信领导小组办公室会同网络安全与信息化办公室和事件发生单位按相关预案进行应急响应。

4. IV级响应

事件发生单位和网络安全与信息化办公室按相关预案进行应急响应。

(三) 应急结束

1. I级和II级响应结束

由网信领导小组办公室提出建议，经学校应急响应工作组上报省教育网安应急办批准后结束，并及时通报校内有关单位。

2. III级响应结束

由网信领导小组办公室、网络安全与信息化办公室和事件发生单位会商，根据实际情况结束III级响应状态。

3. IV级响应结束

校内事件发生单位完成应急处置并经信息中心确认后，报网

信领导小组办公室批准解除IV 级响应状态。

五、调查与评估

特别重大网络安全事件和重大网络安全事件由网信领导小组组织有关单位，配合上级主管部门开展调查处理和总结评估工作，并将调查评估结果汇总上报省教育网安应急办。

较大网络安全事件由网信领导小组办公室组织有关单位开展调查处理和总结评估工作，并将调查评估结果汇总上报网信领导小组。

一般网络安全事件由校内事发单位自行组织开展调查处理和总结评估工作，并将结果报网信领导小组办公室备案。

网络安全事件总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。网络安全事件的调查处理和总结评估工作应在应急响应结束后 5 天内完成。

六、预防工作

（一）日常管理

学校各单位、各部门应配合网信领导小组办公室，按照网络安全等级保护、关键信息基础设施防护等相关要求落实各项防护措施，做好网络安全检查、风险评估和容灾备份，加强信息系统（网站）的安全保障能力。

（二）监测预警和通报

学校各单位、各部门应加强网络安全监测预警和通报，及时

发现并处置安全威胁。网信领导小组办公室应全面掌握校内信息系统（网站）情况，指导、监督各单位、各部门及时修复安全漏洞，全面排查安全隐患，提高发现和应对网络安全事件的能力。

（三）应急演练

网信领导小组办公室每年至少组织一次应急演练，每年年底前将演练情况报省教育网安应急办。

（四）宣传教育

学校各单位、各部门应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 and 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。

（五）工作培训

学校各单位应定期组织网络安全培训，将网络安全事件的应急知识列为培训内容，加强网络安全特别是网络安全事件应急预案的学习，提高网络安全管理和技术人员的防范意识及安全技能。

七、责任与奖惩

对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者在应急管理工作中有其他失职、渎职行为的，依照《福建中医药大学网络安全责任制落实考核评价办法（试行）》相关规定进行考核评价；构成犯罪的，依法

追究刑事责任。

八、附则

（一）预案管理

本预案原则上每年评估一次，根据实际情况适时修订。修订工作由网信领导小组办公室组织。

学校各单位、各部门要根据本单位管理的业务信息系统、网站等网络信息资产的具体情况和本预案制定或修订本单位的网络安全事件应急预案。各预案要做好与本预案的衔接，并报网信领导小组办公室备案。

（二）预案解释

本预案由网信领导小组办公室负责解释。

（三）预案实施时间

本预案自印发之日起实施。

附件：福建中医药大学网络安全事件报告处置单

附件

福建中医药大学网络安全事件报告处置单

单位名称：（公章） 事发时间：

联系人姓名		手机	
事件分类	☐ 有害程序事件 ☐ 信息破坏事件 ☒ 灾害事件 ☐ 网络攻击事件 ☒ 设备设施故障 ☐ 其他		
事件分级	☐ I 级 ☐ II 级 ☐ III 级 ☐ IV 级		
事件概况			
信息系统的基本情况（如涉及请填写）	1. 系统名称： 2. 系统网址和 IP 地址：		
事发网络和信息 系统功能描述			
事件发生时间、 事态发展与处置 的简要经过			
事件初步估计的 危害和影响（影			

响程度、影响人数、紧急损失等情况)	
事件原因的初步分析	
已采取的应急措施和效果	
是否需要应急支援及需支援事项和工作建议	
信息管理员意见 (签字)	
主要负责人意见 (签字)	

