浙江中医药大学文件

浙中医大发〔2021〕87号

浙江中医药大学关于印发网络与信息安全事件应急预案（试行）的通知

各部门、单位：

《浙江中医药大学网络与信息安全事件应急预案（试行）》已经校长办公会议审议通过，现印发给你们，请遵照执行。

浙江中医药大学

2021年7月19日

浙江中医药大学网络与信息安全事件应急预案
（试行）

第一章 总则

第一条 为完善网络与信息安全事件应急工作机制，规范网络安全事件处置工作流程，提高网络与信息安全事件应急处置能力，预防和减少网络安全事件造成的损失和危害，维护学校安全稳定和正常教学秩序，根据《教育系统网络安全事件应急预案》《浙江省网络安全事件应急预案》要求，结合我校实际，特制定本预案。

第二条 坚持统一领导、密切协同、快速反应、科学处置；坚持预防为主，平战结合；坚持“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，充分发挥各方面力量共同做好网络与信息安全事件的预防和处置工作。

第三条 本预案适用于全校范围内自建自管的网络与信息系统（网站），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。

第二章 职责与要求

第四条 网络与信息安全工作领导小组审定网络与信息安全应急预案；决定 I 级和 II 级网络与信息安全事件应急预案的启动，组织、协调和监督预案执行情况。

第五条 网络与信息安全工作领导小组统筹协调、指挥全校网络与信息安全事件应急工作。发生重大（I 级）和较重大（II 级）网络与信息安全事件时，成立应急处置工作组，负责组织指挥和协调事件处置。发生重大（I 级）网络安全事件时，在浙江省教育网络与信息安全工作领导小组统一指挥下开展应急处置工作。

第六条 信息技术中心负责制定网络与信息安全相关制度和应急预案；负责组织开展网络与信息安全事件应急预案的宣传、教育和培训，确保相关人员熟悉应急预案；及时收集网络与信息安全突发事件相关信息，处置III级安全事件，对可能演变为 I 级、II 级的网络与信息安全事件，及时向网络与信息安全工作领导小组提出启动相应应急预案的建议；负责安全事件被抑制后，找出问题根源，彻底清除危害，恢复数据与服务。

第七条 各单位各部门负责网络与安全事件的初步判断、报告,协助信息技术中心完成安全事件处置和整改报告。

第八条 学校师生员工有义务及时向信息技术中心及时报告信息安全事件，不得在未授权情况下对外公布、尝试或利用所发现的安全漏洞或安全问题。

第三章 安全事件分类分级

第九条 依据发生过程、性质和特征的不同，学校网络与信息安全突发事件可分为以下几类。

（一）网络攻击事件：因病毒感染、非法入侵等造成学校各

类网站特别是主页被恶意篡改，应用系统数据被拷贝、篡改、删除等。

（二）设备故障事件：因网络设备和计算机软硬件故障、人为误操作等导致业务中断、系统宕机、网络瘫痪。

（三）灾害性事件：因洪水、火灾、雷击、地震、台风、非正常停电等外力因素导致网络与信息系统损毁，造成业务中断、系统宕机、网络瘫痪。

（四）信息内容安全事件：利用校园网络在校内外传播法律法规禁止的信息，并危害国家安全、社会稳定和公众利益等。

第十条 依据可控性、严重程度和影响范围的不同，学校网络与信息安全事件等级可分为三级：

（一）I 级（重大）：造成全校性大规模网络瘫痪或者发生严重信息内容安全事情，对学校造成严重损害，且事态发展超出学校控制能力的安全事件；

（二）II 级（较大）：造成全校性大规模网络瘫痪或者发生严重信息内容安全事情，对学校造成较严重的损害，事态发展超出信息技术中心控制能力，需学校各部门协同处置的安全事件；

（三）III 级（一般）：校园某一区域的网络与信息系统瘫痪，影响了学校正常工作，信息技术中心可处理的安全事件。

第四章　处置流程

第十一条　预案启动。发生校园网络与信息安全事件后，信

息技术中心应立即采取措施控制事态，进行风险评估，判定安全事件的类别、等级，上报网络与信息安全领导小组，必要时启动相应的预案，参照下述应急响应机制进行处置。

第十二条 应急响应。根据网络与信息安全事件分类分级采取不同应急响应措施：

III 级安全事件响应：信息技术中心协同涉事单位进行应急处置，并将有关情况报给网络与信息安全工作领导小组。

II 级突发事件响应：信息技术中心立即上报网络与信息安全工作领导小组，由领导小组统一组织、协调指挥进行应急处置。

I 级突发事件响应：信息技术中心立即对事件进行初判后并上报网络与信息安全工作领导小组，领导小组研判后再上报浙江省教育厅网安应急办，在省教育厅网安应急办指挥下开展应急处置。

第十三条 应急处理。根据网络与信息安全事件分类采取不同应急处置措施：

（1）网络攻击事件：判断攻击的来源与性质，关闭影响安全与稳定的网络设备和服务器设备，断开信息系统与攻击来源的网络物理连接，跟踪并锁定攻击来源的 IP 地址或其它网络用户信息，修复被破坏的信息，恢复信息系统。

（2）设备故障事件：判断故障发生点和故障原因，迅速抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。

（3）灾害性事件：根据实际情况，在保障人身安全的前提

下，保障数据安全和设备安全，包括硬盘的拔出与保存、设备的断电与拆卸、搬迁等。

（4）信息内容安全事件：接到校内网站有不良信息的报案后，第一时间屏蔽该网站的网络端口或拔掉网络连接线，阻止有害信息传播，根据网站相关日志记录查找信息发布人并做好处理。

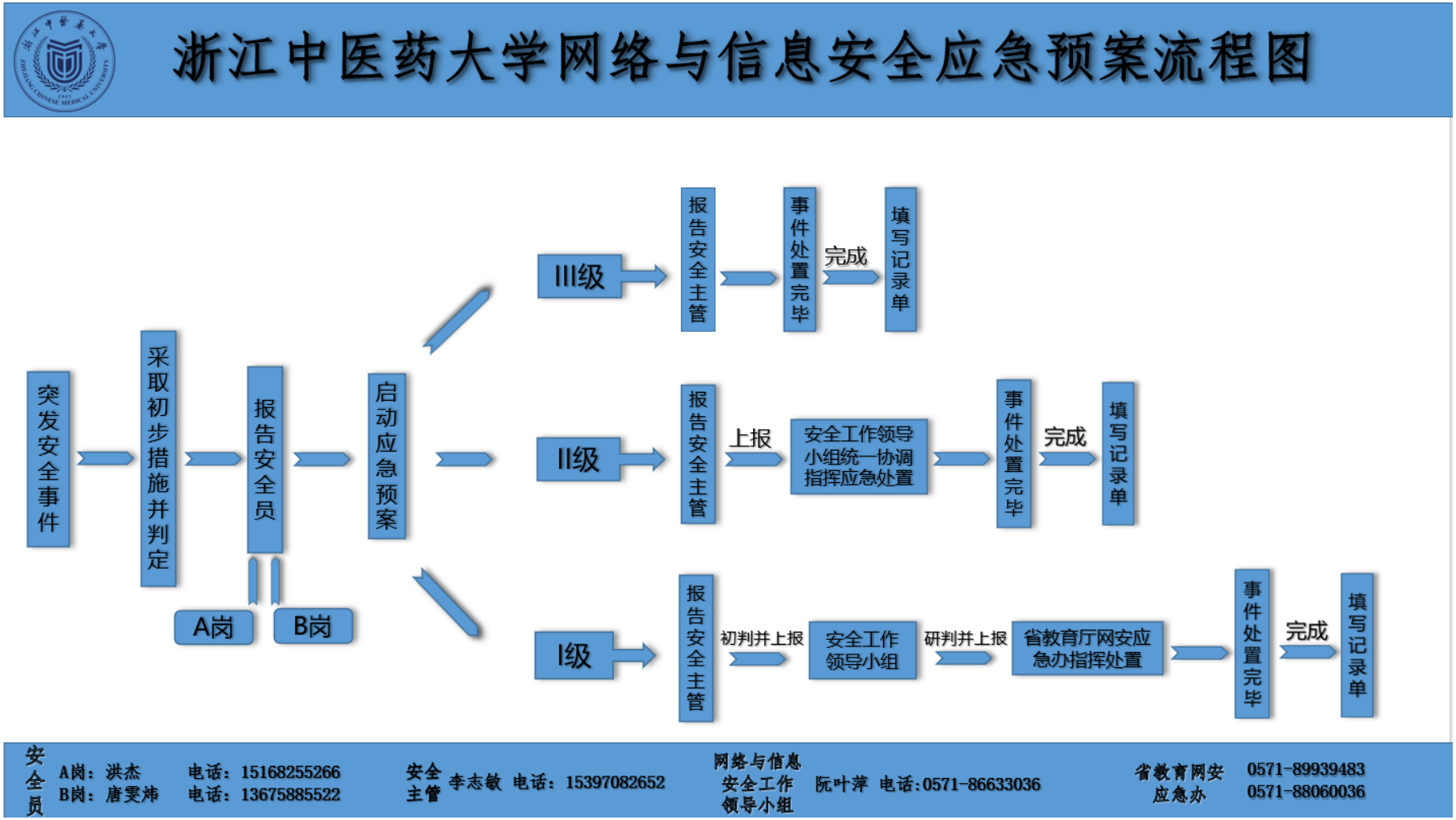
第十四条 应急结束。网络与信息系统安全事件应急处置得到有效控制后，将处置中的工作进展以及监测统计数据上报网络与信息安全领导小组，提出应急结束的建议，经领导批准后实施。

第五章 附则

第十五条 本预案自发布之日起实施，由信息技术中心负责解释。

附件：浙江中医药大学网络与信息安全应急预案流程图

附件


浙江中医药大学网络与信息安全应急预案流程图
突发安全事件
采取初步措施并判定
报告安全员
A岗
B岗
启动应急预案
III级
报告安全主管
事件处置完毕
完成
填写记录单
II级
报告安全主管
上报
安全工作领导小组统一协调指挥应急处置
事件处置完毕
完成
填写记录单
I级
报告安全主管
初判并上报
安全工作领导小组
研判并上报
省教育厅网安应急办指挥处置
事件处置完毕
完成
填写记录单
安全员
A岗：洪杰 电话：15168255266
B岗：唐雯炜 电话：13675885522
安全主管 李志敏 电话：15397082652
网络与信息安全工作领导小组 阮叶萍 电话:0571-86633036
省教育网安应急办 0571-89939483
0571-88060036

抄送：各二级党组织。

浙江中医药大学办公室　　2021年7月20日印发