成 都 市 技 师 学 院 文 件

成技院发〔2018〕48 号

成都市技师学院
关于印发《成都市技师学院
校园网络安全应急预案》的通知

各部门:

经学院研究同意，现将《成都市技师学院校园网络安全应急预案》印发给你们，请遵照执行。

成都市技师学院

2018 年 11 月 5 日

成都市技师学院
校园网络安全应急预案

为切实做好学院校园网络突发事件的防范和应急处理工作，进一步提高学院预防和控制网络突发事件的能力和水平，减轻或消除突发事件的危害和影响，确保校园网络与信息安全，结合学院工作实际，制定本预案。

第一章　总　则

第一条　本预案所称突发性事件，是指自然因素或者人为活动引发的危害学院校园网网络设施及信息安全等有关的灾害。

第二条　本预案的指导思想是根据互联网网络安全相关条例和学院有关计算机网络及信息安全基本要求。

第三条　本预案适用于发生在学院校园网络上的突发性事件应急工作。

第四条　应急处置工作原则：统一领导、统一指挥、各司其职、整体作战、发挥优势、保障安全。

第二章　组织机构和职责任务

第五条 学校网络安全与信息化工作领导小组是学校网络安全领导和决策机构，负责网络安全事件的组织指挥协调，组长由院长担任，副组长由分管副院长担任，成员由学院各处室、系部、校区负责人组成。领导小组办公室设在信息中心，负责具体应急处置工作，办公室主任由分管副院长担任，副组长由信息中心主任和新闻宣传中心主任担任，成员由学院信息中心、新闻宣传中心等处室系部相关人员组成。

（一）领导小组主要职责:

1. 加强领导，健全组织，强化工作职责，完善各项应急预案的制定和各项措施的落实。

2. 充分利用各种渠道进行网络安全知识的宣传教育，组织、指导全院网络安全常识的普及教育，广泛开展网络安全和有关技能训练，不断提高广大师生的防范意识和基本技能。

3. 认真搞好各项物资保障，严格按照预案要求积极配备网络安全设施设备，落实网络线路、交换设备、网络安全设备等物资，强化管理，使之保持良好工作状态。

4. 采取一切必要手段，组织各方面力量全面进行网络安全事故处理工作，把不良影响与损失降到最低点。

5. 调动一切积极因素，全面保证和促进学校网络安全稳定地运行。

（二）领导小组办公室主要职责:

1. 信息中心负责网络安全日常事务，对学院网络进行监管，异常时发出预警，组织实施处置突发情况。

2. 新闻宣传中心负责整个学院网站的安全管理、舆情监督和应急处置。

3. 各处室系部应配备网站管理员和信息系统管理员，分别负责本部门网站和信息系统的安全管理。

第三章　网站不良信息事故处理预案

第六条　由学院新闻宣传中心负责整个学院网站的安全管理和应急处置；各处室系部负责部门网站的安全管理和应急处置，特别是要加强论坛贴吧的安全管理。

（一）一旦发现学校网站上出现不良信息（或者被黑客攻击修改了网页），立刻通知新闻宣传中心及时关闭网站。

（二）备份不良信息出现的目录、备份不良信息出现时间前后一个星期内的HTTP连接日志、备份防火墙中不良信息出现时间前后一个星期内的网络连接日志。

（三）打印不良信息页面留存。

（四）完全隔离出现不良信息的目录，使其不能再被访问。

（五）删除不良信息，并清查整个网站所有内容，确保没有任何不良信息，重新开通网站服务。

（六）修改该目录名，对该目录进行安全性检测，升级安全级别，升级程序，去除不安全隐患，关闭不安全栏目，重新开放该目录的网络连接，并进行测试，正常后，重新修改该目录的上级链接。

（七）全面查对HTTP日志，防火墙网络连接日志，确定该不良信息的源IP地址，如果来自校内，则立刻全面升级此次事件为最高紧急事件，立刻向领导小组组长汇报，视情节严重程度领导小组可决定是否向公安机关报案。

（八）从事故一发生到处理事件的整个过程，必须保持向学院院领导汇报此次事故的发生情况、发生原因、处理过程。

第四章　校园网络安全处置预案

第七条　处置措施。处置的基本措施分灾害发生前与灾害发生后两种情况。

（一）灾害发生前，信息中心要预先对灾害预警预报体系进行建设，开展灾害调查，编制灾害防治规划，建设专业监测网络，并规划建设灾害信息管理系统，及时处理灾害讯情信息。

加强灾害险情巡查。信息中心要充分发挥专业监测的作用，进行定期和不定期的检查，加强对灾害重点部位的监测和防范，发现有不良险情时，要及时处理并向学院院领导报告。

建立健全灾情速报制度，保障突发性灾害紧急信息报送渠道畅通。

（二）灾害发生后，立即启动应急预案，采取应急处置程序，判定灾害级别，并立即将灾情向学院分管院领导报告，在处置过程中，应及时报告处置工作进展情况，直至处置工作结束。

第八条 处置程序

（一）发现情况

学院信息中心要严格执行值班制度，做好校园网信息系统安全的日常巡查及其日志保存工作，以保障最先发现灾害并及时处置此突发性事件。

（二）预案启动

一旦灾害发生，立即启动应急预案，进入应急预案的处置程序。

（三）应急处置方法

在灾害发生时，首先应区分灾害发生是否为自然灾害与人为破坏两种情况，根据这两种情况把应急处置方法分为两个流程。

流程一：当发生的灾害为自然灾害时，应根据当时的实际情况，在保障人身安全的前提下，首先保障数据的安全，然后是设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

流程二：当人为或病毒破坏的灾害发生时，具体按以下顺序

进行：判断破坏的来源与性质，断开影响安全与稳定的信息网络设备，断开与破坏来源的网络物理连接，跟踪并锁定破坏来源的IP或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照灾害发生的性质分别采用以下方案：

1. 病毒传播：针对这种现象，要及时断开传播源，判断病毒的性质、采用的端口，然后关闭相应的端口，在网上公布病毒攻击信息以及防御方法。

2. 入侵：对于网络入侵，首先要判断入侵的来源，区分外网与内网。入侵来自外网的，定位入侵的IP地址，及时关闭入侵的端口，限制入侵地IP地址的访问，在无法制止的情况下可以采用断开网络连接的方法。入侵来自内网的，查清入侵来源，如IP地址、上网帐号等信息，同时断开对应的交换机端口。然后针对入侵方法建设或更新入侵检测设备。

3. 信息被篡改：这种情况，要求一经发现马上断开相应的信息上网链接，并尽快恢复。

4. 网络故障：一旦发现，可根据相应工作流程尽快排除。

5. 其它没有列出的不确定因素造成的灾害，可根据总的安全原则，结合具体的情况，做出相应的处理。不能处理的可以请示相关的专业人员。

（四）情况报告。灾害发生时，一方面按照应急处置方法进行处置，同时需要判定灾害的级别，首先向学院网络安全领导小

组汇报，并及时报告处置工作进展情况，直至处置工作结束。

情况报告内容包括：灾害发生的时间、地点，灾害的级别，灾害造成的后果，应急处置的过程、结果，灾害结束的时间，以后如何防范类似灾害发生的建议与方案等。

（五）发布预警。灾害发生时，可根据灾害的危害程度适当地发布预警，特别是一些在其它地方已经出现，或在安全相关网站发布了预警而学院信息网络还没有出现相应的灾害，除了在技术上进行防范以外，还应当向网络信息用户发布预警，直至灾害警报解除。

（六）预案终止。经专家组鉴定，灾害险情或灾情已消除，或者得到有效控制后，由学院的网络安全与信息化工作领导小组宣布险情或灾情应急期结束，并予以公告，同时预案终止。

第五章　保障措施

灾害应急防治是一项长期的、持续的、跟踪式的、深层次的和各阶段相互联系的工作，是有组织的科学与社会行为，而不是随每次灾害的发生而开始和结束的活动。因此，必须做好应急保障工作。

第九条　人员保障。重视人员的建设与保障，确保在灾害发生前的人员值班，灾害处置过程和灾后重建中的人员在岗与战斗

力。

第十条 技术保障。重视网络信息技术的建设和升级换代，在灾害发生前确保网络的强劲与安全，灾害处置过程中和灾后重建中的相关技术支撑。

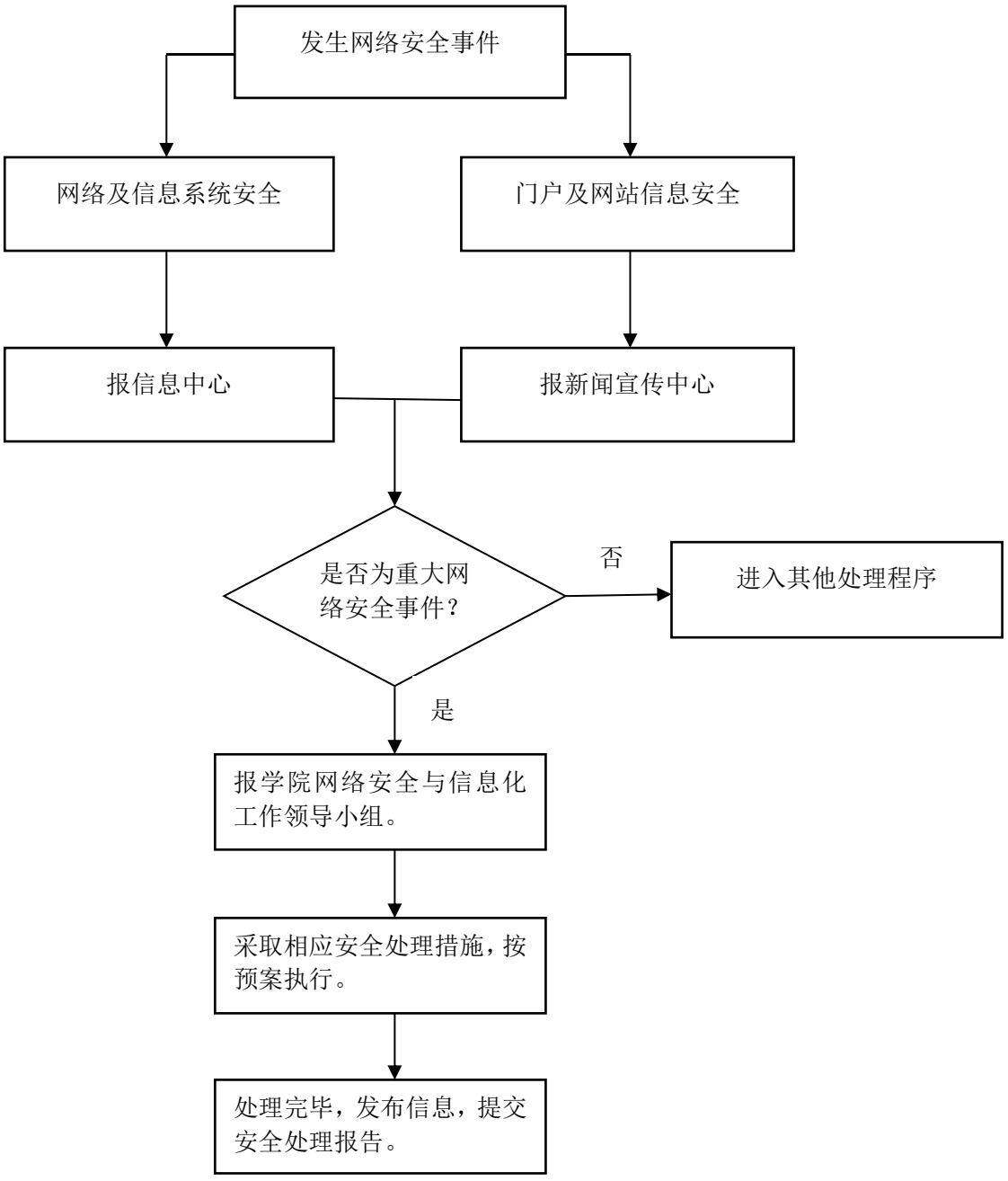
第十一条 物资保障。学院要根据近年来全国甚至全世界网络安全防治工作所需经费情况，购买相应的应急设施。建立应急物资储备制度，保证应急抢险救灾队伍技术装备的及时更新，以确保灾害应急工作的顺利进行。

第十二条 训练和演练。加强学院网络用户的防灾、减灾知识的宣传普及，增强这些用户的防灾意识和自救互救能力。有针对性地开展应急抢险救灾演练，确保发灾后应急救助手段及时到位和有效。

第六章 附 则

第十三条 本预案由信息中心负责解释，自二〇一八年十二月一日起执行，执行之日起原成技院〔2015〕118号文件作废。

网络安全应急处理流程图



成都市技师学院办公室　　2018年11月5日印发