**温州职业技术学院网络与信息安全事件应急预案**

**（征求稿）**

为建立学院网络与信息安全应急响应工作机制，有效预防并科学应对网络与信息安全突发事件，确保校园网络与信息系统正常运行，结合我院实际，特制定本预案。

**一、适用范围**

本预案适用于温州职业技术学院全院范围内的网络与信息系统，尤其是校园网主干设施和重要信息系统（网站）安全突发事件的应急处置工作。

**二、编制依据**

根据《中华人民共和国计算机信息系统安全保护条例》、《计算机病毒防治管理办法》、《信息安全事件分类分级指南》（GB/T20986-2007）、《浙江省突发公共事件总体应急预案》、《浙江省网络与信息安全应急预案》、《温州市电信网络与信息系统安全应急预案》，制定本预案。

三、工作原则

统一领导，快速反应，密切配合，科学处置。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应急处置工作。

四、网络与信息安全事件分类分级
（一）网络与信息安全事件分类

根据网络与信息安全突发事件的性质、特征和发生过程，主要分为以下四类：

1、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。

2、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。

3、网络攻击事件：校园网络与信息系统因病毒感染、非法入侵等造成学院网站、微信、微博被恶意篡改，应用系统数据被拷贝、篡改、删除等。

4、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，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等。

（二）网络与信息安全分级

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的不同，可分为以下四级：

Ⅰ级（特别重大）：信息系统（网站）非法信息引发大规模群体性事件，对国家安全、社会秩序、经济建设和公共利益造成特别严重损害，需要报告上级应急部门和公安部门，并由上级应急部门和公安部门统一应急响应和处置的突发公共事件。

Ⅱ级（重大）：造成全院性网络与信息系统瘫痪，或由于信息系统（网站）非法信息引发师生反应强烈并有过激行为，对社会秩序、公共利益等造成一定损害，对学院正常工作造成严重损害，需要报告学院网络安全工作领导小组组长，并需跨部门协同处置的安全事件。

Ⅲ级（较大）：学院某一区域的网络与信息系统瘫痪，或由于信息系统（网站）敏感信息、谣言等，对学院正常工作造成一定损害，学院网络安全工作领导小组办公室可自行处理的安全事件。

Ⅳ级（一般）：某一局部网络或信息系统受到一定程度损坏，对学院某些工作有一定影响，但不危及学院整体工作的安全事件，现代教育技术中心可自行处理的安全事件。

五、应急组织领导体系及职责任务

（一）组织机构

学院网络安全工作领导小组统一领导、指挥、协调全院网络与信息安全防范及应急处置工作，领导小组下设办公室，负责处理领导小组日常事务工作，办公室工作由现代教育技术中心（部门）承担。（温职院〔2016〕38号）

（二）职责及任务

1、学院网络安全工作领导小组：①负责网络信息安全工作的组织、协调和监督，制定相关制度和应急预案；②决定I 级和II 级网络与信息安全事件应急预案的处置，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。

2、学院网络安全工作领导小组办公室: ①根据网络信息安全事件程度提出相应级别预案的启动，上报领导小组，决定Ⅲ级和Ⅳ级网络与信息安全事件应急预案的处置，组织协调成员单位落实应急预案，共同做好处置工作；②负责及时收集、通报和上报网络信息安全事件处置的有关情况； ③对全院各单位贯彻执行预案以及在事件处置工作中履行职责情况进行检查督办；④网络与信息安全防护体系建设，信息安全等级保护建设实施；⑤开展网络与信息安全知识的宣传教育和培训。

（三）其它单位职责

1、党委院长办公室：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；负责涉密级信息网络泄密类事件的处理。

2、党委宣传部：负责学院舆情监测和信息内容安全类事件的处置，对于涉及师生政治思想方面的预警性、倾向性、苗头性的问题加强分析研判，有效应对。

3、现代教育技术中心：负责校园基础网络系统安全，保证校园网络服务不中断；负责网络攻击、设备故障类事件的处置；负责全院网络信息安全事件处置的技术支持工作。

4、保卫处：负责有关学院网络的安全保卫，协助做好网络安全事故处置工作，同时密切联系公安部门，负责涉及人为破坏类事件的处置，配合重大安全事件的处置。

 5、各学院、职能部门负责本单位网站和业务信息系统的安全管理和突发事件的应急处置工作，应对照本预案，建立本部门应急处置机制。

六、预防措施

1. 加强网络与信息系安全管理，健全工作制度和建立预报预警监测体系，避免和减少网络信息安全事件发生。

2. 健全技术防护体系，在校园网出入口、数据中心、重要信息系统等重要部位，安装必要的安全防御检测工具，进行实时监测和定期扫描，发现异常情况及时防范处理并逐级报告。同时做好操作系统升级杀毒，数据备份、安全审计等日常管理工作。

3.建立灾害险情巡查制度。宣传部及各网站管理员应随时监控网站、微信、微博内容，现代教育技术中心严格执行值班制度，做好校园网络与信息安全的日常巡查及日志保存工作，早期发现灾害并及时处置突发性事件。

4.特殊时期，根据工作需要，由学院网络安全工作领导小组办公室进行统一部署和安排，组织专业技术人员对校园网络和信息系统采取加强性保护措施，对校园网络通信及信息系统进行不间断监控。

七、应急处置

（一）先期处置

发生校园网络信息安全事件后，各学院、各职能部门12小时内上报学院网络安全工作领导小组办公室，由办公室收集安全事件相关信息，采取先期处置，同时研判事件性质，确定事件来源，弄清事件范围，评估事件带来的影响和损害，确认突发事件的类别和等级，并参照下图响应机制对突发事件进行处置。

**学院发生网络安全事件**

**学院网络安全工作领导小组办公室先期处置，启动网络信息安全应急处置工作程序。**

**Ⅰ级：上报学院网络安全工作领导小组、上级应急部门和公安部门，配合统一组织、协调进行应急处置。**

**Ⅲ、Ⅳ级：学院网络安全工作领导小组办公室协调相关责任单位，开展应急处置工作。**

**确认研判**

**安全事件等级**

**Ⅱ级：上报学院网络安全工作领导小组，统一组织、协调进行应急处置。**

**事故处理**

**事件调研**

**追究责任**

图：安全事件报告与处置流程

**（二）应急响应**

1.应急响应机制

I级突发事件响应：上报学院网络安全工作领导小组、上级应急部门和公安部门，由上级应急部门和公安部门组织协调有关单位和我院协同进行应急处置。

II级突发事件响应：学院网络安全工作领导小组办公室应立即上报学院网络安全工作领导小组，由领导小组统一组织、协调指挥进行应急处置。

III或IV级突发事件响应：学院网络安全工作领导小组办公室协调相关责任单位（现代教育技术中心、党委宣传部、保卫处等），自行负责应急处置工作，做好处置记录。

2、应急处理方式

根据网络与信息安全事件分类采取不同应急处置方式。

（1）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。

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

（3）网络攻击事件：判断攻击的来源与性质，关闭影响安全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。

（4） 信息内容安全事件：接到校内网站出现不良信息的报案后，应迅速屏蔽该网站的网络端口或断开网络连接，阻止有害信息传播，查找信息发布人并做好善后处理。对公安机关要求我院协查的外网不良信息事件，根据校园网上网相关记录查找信息发布人。

（5）其它不确定安全事件：可根据总的安全原则，结合具体情况，做出相应处理，不能处理的及时咨询国家信息安全机构。

**（三）后续处理**

1.安全事件进行最初的应急处置后，应及时采取行动，并在事件处置工作中作好完整的过程记录，及时向学院网络安全工作领导小组办公室报告处置工作进展情况，保存各相关系统日志，直至处置工作结束。

2.安全事件被抑制后，通过对有关事件或行为的分析结果，找出问题根源，明确相应补救措施并彻底清除。

3.在确保安全事件解决后，要及时清理系统，恢复数据、程序、服务，恢复工作应避免出现误操作导致的数据丢失。

4.系统恢复运行后，学院网络安全工作领导小组办公室对事件造成的损失、事件处理流程等进行分析评估，总结经验教训，撰写事件处理报告。

**（四）记录上报**

网络与信息系统安全事件发生时，应及时向学院网络安全工作领导小组汇报，并在事件处置工作中作好完整的过程记录，及时报告处置工作进展情况，保存各相关系统日志，直至处置工作结束。

**（五）结束响应**

系统恢复运行后，学院网络安全工作领导小组办公室对事件造成的损失、事件处理流程和应急预案进行评估，对响应流程、预案提出修改意见，总结事件处理经验和教训，撰写事件处理报告，同时确定是否需要上报该事件及其处理过程，需要上报的应及时准备相关材料；属于重大事件或存在非法犯罪行为的，及时向公安部门报案。

**八、保障措施**

校园网络与信息安全应急处置是一项长期的、随时可能发生的工作，必须做好各项应急保障工作。

（一）队伍保障

加强队伍建设，不断提高工作人员的信息安全防范意识和技术水平，确保安全事件应急处置科学得当。

（二）技术保障

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。根据工作需要聘请信息安全顾问为应急处置过程和重建工作提供咨询和技术支持。

（三）经费保障

学院网络安全工作领导小组办公室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及软件的运行维护专项资金，提出本年度应急处置工作相关设备和工具所需经费，并纳入年度财政预算，由学院给予资金保障。

（四）安全培训和演练

学院网络安全工作领导小组办公室负责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抢险救灾演练，确保相关措施的有效落实。

九、本预案自公布之日起施行，由学院网络安全工作领导小组办公室负责解释。

各学院、部门信息安全应急响应联系人

|  |  |  |  |
| --- | --- | --- | --- |
| **学院/部门** | **安全责任领导** | **安全管理员** | **安全管理员****手机及座机电话** |
| 党院办、外事办 |  |  |  |
| 组织部、统战部、离退休管理处 |  |  |  |
| 宣传部 |  |  |  |
| 纪检监察审计室 |  |  |  |
| 工会 |  |  |  |
| 学工部（学生处）、团委 |  |  |  |
| 教务处（产学合作处） |  |  |  |
| 资产管理处 |  |  |  |
| 科技开发处 |  |  |  |
| 教学质量监控处 |  |  |  |
| 人事处 |  |  |  |
| 招生就业处 |  |  |  |
| 保卫处 |  |  |  |
| 计财处 |  |  |  |
| 图书馆 |  |  |  |
| 现代教育技术中心 |  |  |  |
| 学报编辑部 |  |  |  |
| 高等职业教育研究所 |  |  |  |
| 后勤基建处（四方公司） |  |  |  |
| 瑞安学院 |  |  |  |
| 党院办、外事办 |  |  |  |
| 组织部、统战部、离退休管理处 |  |  |  |
| 宣传部 |  |  |  |
| 纪检监察审计室 |  |  |  |
| 成教学院 |  |  |  |

 温州职业技术学院网络与信息安全工作领导小组办公室，

**24小时值班电话 ：86680039**