附件 4:

金华职业技术学院网络和信息安全类突发事件应急处置预案

一、组织机构

学校成立网络与信息安全类突发事件应急处置工作组。

组　长：分管宣传党委副书记

副组长：校办、宣传部负责人

成　员：学生处、团委、保卫处、信息化办公室负责人。工作组办公室设在宣传部。

工作组（应急现场指挥部）主要职责：负责学校网络与信息安全类突发事件的应急处置；通过技术手段对校园网有害信息实施 24 小时监控；及时处置重大有害信息在校园网上大面积传播，或校园网系统遭受大范围黑客攻击和计算机病毒扩散事件；在校园网遭受严重攻击，遇有极其严重、不可控制的大型安全事件时，及时报告、处置和制止，保证校园网正常稳定运行；协调有关部门开展事件应急处置工作；研究对外公布、公开与事件有关信息的口径及发布时间、方式等；会同校应急处置领导小组办公室总结评估应急处置工作。

二、网络运行风险分类与等级划分

（一）网络（含计算机应用系统）运行风险分类

1.自然灾害（如地震、雷电、火灾、洪水等）、事故和人为

破坏（如设备盗抢、设备损毁等）导致的物理类故障;

2.网络通信设备、通信线路、电源电路及机房等基础设施故障导致的基础类故障;

3.计算机应用系统硬件设施或软件系统故障（如软件自身缺陷、系统崩溃、超负荷运行、数据容灾备份等）导致的系统类故障;

4.网络或计算机应用系统遭恶意攻击（包括非法入侵、拒绝服务、篡改数据、漏洞病毒、恶意代码、信息窃取等）导致的安全类故障。

（二）等级确认与划分

1.I 级事件

长时间（时间长度不少于 8 小时）的全网性重大事件。造成校园网主干中断、校园“一卡通”业务整体瘫痪，或者造成大量用户数据信息（金融数据）丢失。

2.Ⅱ级事件

较长时间（时间长度超过 2 小时，低于 8 小时）的全网性事件。造成校园网主干中断、重要校级信息系统业务中断、校内部分区域网络服务中断等。

3.III 级事件

短时(时间长度超过 30 分钟，低于 2 小时)的全网性事件。即校园网主干中断、重要校级信息系统业务中断、校内部分区域网络服务中断。

三、应急响应

（一）网络环境安全事件应急处置

网络环境安全事件由发生事件的单位自行处置，涉及全校性事件由信息化办公室负责处置。对火灾、盗窃、破坏等紧急事件按照国家有关法律法规及学校有关规定处理，影响网络运行和信息安全的重大事件由应急处置工作组统一指挥，协调处置。

遇与供电相关的紧急事件，由学校后勤部门作现场紧急处置，根据停电时间、用电功耗、电池电能储备、网络和信息运行情况等条件作调度，采取包括次要系统停电、减轻负载等措施，密切跟踪参数变化并反馈调整控制，联系相关单位和人员作现场维护。

（二）网络运行事件应急处置

网络运行相关事件包括：线路中断、路由故障、流量异常、域名系统故障等。各单位的网络运行事件由单位主管网络领导负责组织处置；重大事件立即向应急处置工作组报告，工作组统一指挥，组织协调处置。

（三）网络攻击事件应急处置

由各单位按分工和应急流程处置。对于大规模、影响较大的恶意代码、拒绝服务攻击、系统入侵和端口扫描，处置如下：

1.报本单位网络管理负责人和应急处置工作组；

2.按预案通知相关管理人员采取措施，或直接实施控制；

3.处置人员记录事件处理步骤和结果，总结报告。

（四）信息安全事件应急处置

发生信息安全事件应紧急通知本单位信息主管负责人，及时消除非法信息，恢复系统。无法迅速消除或恢复系统，影响较大时实施紧急关闭，并实时上报校应急领导小组。

四、善后和恢复

（一）应急处置后，应及时对II级和II级以上事件进行总结，查明事故原因，全面检查设备、系统和线路。对人为失误而导致网络或计算机应用系统运行故障，要追究有关责任人的责任。对人为攻击，要配合有关部门尽快破案。

（二）信息化办公室根据应急处置中暴露的管理、协调和技术等问题，改进和完善预案，并实施针对性演练；从实际应急处置中提炼有关科技攻关需求,上报有关部门申请立项研究。

五、应急保障

（一）组织保障：成立网络与信息安全类突发事件应急处置工作组，统一协调处理校园网网络、计算机应用系统与信息安全突发事件。

（二）通信保障：应急处置工作组应建立应急通讯录。组内工作人员联络信息如有变更需及时更新，确保应急联络渠道畅通。

（三）环境保障：信息化办公室负责联系后勤中心等部门建立并保持中心机房的电力、空调等网络安全运行基本环境。

（四）技术保障：信息化办公室建立起符合要求的网络安全稳定运行的技术支持力量，并对全校提供力所能及的技术支持和培训服务。

（五）流程保障：信息化办公室建立网络、计算机应用系统应急处置处理流程，负责应急处置各类网络和计算机应用系统运行中发生的突发性安全事件。当出现应急处理流程中断、应急处置无法进行，或者事态范围扩大时，按照事件升级的原则向更高层次紧急通报处理，避免延误。