潍坊学院文件

潍院政字〔2021〕70 号

潍坊学院关于印发
网络与信息安全事件应急预案的通知

各单位、各部门：

《潍坊学院网络与信息安全事件应急预案》已经校长办公会议研究通过，现印发给你们，请认真贯彻执行。

潍坊学院

2021 年 10 月 20 日

潍坊学院
网络与信息安全事件应急预案

1.总则

为提高学校应对网络与信息安全事件的处置能力，做到预防有效，反应及时，处置得当，维护学校安全稳定和师生的合法权益，依据《中华人民共和国网络安全法》、教育部《教育系统网络与信息安全类突发公共事件应急预案》等法律法规，结合学校实际，制定本预案。

1.1 编制依据

《中华人民共和国网络安全法》《中华人民共和国突发事件应对法》和《刑法》修正案第九条、教育部《教育系统网络与信息安全类突发公共事件应急预案》、《教育部办公厅关于进一步加强高等学校校园网络信息安全工作的意见》等法律法规及文件精神。

1.2 事件分类

本预案所指网络与信息安全事件分为以下三大类：软件系统类事件、信息安全类事件和设施设备故障类事件。

软件系统类事件包括两种：(1)有害程序。分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。(2)网络攻击。

分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

信息安全类事件包括两种:(1)信息破坏。分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。(2)信息内容安全。是指通过网络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校园安全、学校稳定和师生权益的事件。

设施设备故障类事件包括：软硬件自身故障、外围保障设施故障、人为破坏事故和自然灾害等引发的其他设备设施故障。

1.3 组织机构与职责

1.3.1 成立校园网络与信息安全事件应急处置工作领导小组（以下简称领导小组），人员组成如下：

组　长：李　东

副组长：冯滨鲁　丁子信

成　员：办公室、宣传部、学生工作处（武装部）、人事处（教师工作部、人才工作办公室）、教务处（教学质量评建办公室）、科研处（学报编辑部）、招生就业处（校友工作办公室）、实验室与设备管理处（网络信息中心与其合署）、发展规划处（高教研究所）、财务处、国有资产管理处、总务处、保卫处、继续教育学院（潍坊广播电视大学）、安顺校区管理办公室、团委、计算机工程学院、弘德书院、图书馆、档案馆等部门主要负责人。

职责：统一领导和协调学校网络与信息安全事件的预防和处置，协调和督查有关部门、单位对网络与信息安全事件的预防和处置工作。研究确定事件的性质、类型和级别，下达应急处置任务。向上级部门报送有关事件的处置信息。

1.3.2 校园网络与信息安全事件应急处置工作领导小组办公室（以下简称领导小组办公室）设在网络信息中心,网络信息中心主要负责人兼任办公室主任。

职责：负责全校网络与信息安全事件应急预案的制定，提出关于事件性质、类型和级别的意见建议，组织领导小组下达的任务实施。负责对全校网络与信息安全事件的日常管理工作。

1.4 工作原则

1.4.1 统一领导，快速反应。

领导小组统一领导、协调全校网络与信息安全事件应急处置工作，领导小组办公室负责应急工作的日常管理，建立健全应急反应机制，提前预防，及时报告，紧密衔接，迅速处理，将事态影响减至最小。

1.4.2 自建自管，各负其责。

学校各单位、各部门要按照“谁主管、谁主办、谁负责”的原则，加强对本单位所属的网络与信息的安全管理。强化单位、部门主要领导对网络与信息安全事件的处置职责。

1.4.3 依法处置，预防为先。

在处置网络与信息安全突发事件中，要根据实际，合情合理，

依法办事，维护师生合法权益，防止事态扩大激化。要坚持提前防范，及时排查，争取早发现早报告早解决，化解风险，减少不良影响。

2.事件分级

学校网络与信息安全事件根据其危害程度分为四级：特别重大(Ⅰ级)、重大(Ⅱ级)、较大(Ⅲ级)、一般(Ⅳ级)。

2.1 符合下列情形之一的，为特别重大网络与信息安全事件(Ⅰ级)：

(1)用于社会服务的重要信息系统中断运行2小时以上、影响人数1万人以上，并造成了重大社会影响。

(2)校内信息系统中的数据丢失或被窃取、篡改、假冒，对国家安全、社会稳定构成严重威胁。

(3)利用校园网传播重要涉密信息、反动信息、煽动性信息、谣言等情况，可能泄露国家机密，对国家安全、社会稳定构成严重危害，或引发学校大规模突发群体事件，对学校的安全稳定和正常秩序构成特别严重影响、教育教学活动无法正常进行，师生反映强烈并有过激行为的事件。

2.2 符合下列情形之一且未达到特别重大网络与信息安全事件(Ⅰ级)的，为重大网络与信息安全事件(Ⅱ级)：

(1)校内信息系统中断运行2小时以上、影响人数1万人以上。

(2)校内信息系统中的数据丢失或被窃取、篡改、假冒，对

国家安全和社会稳定构成一定威胁，对学校稳定和社会形象构成重大影响。

（3）利用校园网传播重要涉密信息、反动信息、煽动性信息、谣言等情况，对国家安全、社会稳定构成较大危害，可能泄露学校机密，或引发学校突发性群体事件，对学校安全稳定和正常秩序构成严重影响，师生反映强烈的事件。

2.3 符合下列情形之一且未达到重大网络与信息安全事件(Ⅱ级)的，为较大网络与信息安全事件(Ⅲ级)：

（1）校内信息系统中断运行 30 分钟以上，影响人数 5000 人以上。

（2）校内信息系统中的数据丢失或被窃取、篡改、假冒，对国家安全、社会稳定构成一定危害，或对学校安全稳定构成较大威胁，对学校的社会形象形成较大影响。

（3）利用校园网传播涉密信息、反动信息、煽动性信息、谣言等情况，对国家安全、社会稳定构成一定危害，或对学校安全稳定构成较大危害，对学校正常秩序产生较大影响，引起师生员工广泛关注的事件。

2.4 除上述情形外，对学校安全稳定、正常秩序构成一定威胁、对师生权益造成危害和影响的事件，为一般网络与信息安全事件(Ⅳ级)。

3.监测预警

3.1 预防措施

全校各单位、各部门要做好网络与信息安全事件的隐患排查工作，制定和完善管理制度，做好日常管理，避免和减少网络与信息安全事件的发生和危害。具体预防措施包括：

（1）加强教育引导。加强对师生的思想教育工作，掌握舆情动态。按照早发现、早报告、早控制、早解决的要求，把问题解决在萌芽状态，化解和控制风险。

（2）完善应急管理制度。制定和落实本单位、本部门所属的网络管理、机房和配线间管理、信息安全和保密相关制度，指定专门的网络与信息管理员，提高有关人员的责任意识、安全意识和技术水平。

（3）加强技术防范措施。网络信息中心定期对校园网各关键设备和配线间进行巡查，建立校园网基础设施的安全保护制度。工程施工须按校园管网线路图纸操作，或经学校网络管理部门许可。未经许可不得直接切割或改动网络线路和设备。对破坏网络线路、设备和机房、配线间的行为，要建立责任追究制度。

校园网出入口安装必要的监测系统,对校园网进行安全扫描。对全校公共服务器，要根据系统的重要性和影响面，制定分级管理规范。加强对全校各信息系统的实时监测。

重要信息采用安全可靠的运行设备，使用成熟稳定的系统与应用软件，进行必要的数据备份，控制管理访问权限，遵守各项安全管理操作规范。各单位、各部门要有专人负责本单位网站、网页的域名管理、IP 地址管理。

建立严格的信息发布审查和检查制度，有效阻止网络不良信息的传播。落实校级新闻的归口发布规定，各单位、各部门网站（页）的新闻与信息类栏目要有专人管理，先审后发。

3.2 信息报送

最先发现或接到发生网络与信息安全事件的单位或个人，要第一时间向领导小组办公室报告。领导小组办公室视情向领导小组报告，报告内容包括事件的时间、地点、规模、涉及人员和损失情况，事件的危害影响程度和发展趋势等基本情况。

4．应急响应措施

4.1 基本措施

网络与信息安全事件发生后，要及时启动应急预案，实施处置并报送信息。

（1）对于软件系统类事件，及时通知领导小组办公室，领导小组办公室组织技术人员采取措施及时处理，并记录处理步骤和结果，保留相关证据材料，并将处理情况上报领导小组。必要时要追究相关当事人责任。

（2）对于信息安全类事件，首先及时联系信息主管单位负责人，同时通知领导小组办公室，尽快消除不良信息。无法迅速消除或恢复系统、影响较大时要实施紧急关闭，并紧急上报领导小组。属于管理不当或未遵守相关规定而导致的事件，要按规定追究相关责任。

（3）对于设施设备故障类事件，及时通知网络信息中心或设

施设备所属有关单位、部门，同时通知领导小组办公室。设施设备所属单位根据故障原因和性质，组织抢修，并上报领导小组。对于人为破坏导致的设施设备故障，要按规定追究相关责任。

4.2 分级措施

4.2.1 Ⅰ级响应措施

经领导小组确认属于特别重大网络与信息安全事件的，启动Ⅰ级响应措施。

（1）领导小组办公室成员立即到位，向领导小组汇报，研究对策，协调部署应对工作，同时向上级部门报送信息。

（2）领导小组各成员单位进入紧急状态，按领导小组要求开展工作，采用各种手段迅速处置，控制事态防止扩大。各单位、各部门主要负责人保持通讯24小时畅通,学校办公室安排人员值班。领导小组办公室及时监控事态进展，从技术手段保证尽快消除影响，系统恢复正常。

（3）必要时，领导小组第一时间向校内外公开通报处理过程及结果，引导正确舆论，平息师生情绪。

（4）各有关单位、各部门在应急处置过程中，要做好工作记录，尽可能保留相关证据。对于人为破坏的违法行为，将配合公安司法机关依法处理。

4.2.2 Ⅱ级响应措施

（1）领导小组办公室负责人立即到位,向领导小组汇报情况。领导小组迅速研究制定对策，指导各单位、各部门开展应急处置

工作，必要时向上级部门报送信息。

（2）各单位、各部门按领导小组要求开展工作，采用各种手段进行处置，防止事态扩大。各单位、各部门主要负责人保持通讯畅通。领导小组办公室及时监控事态进展，从技术手段保证尽快消除影响，系统恢复正常。

（3）必要时，领导小组及时通过学校新闻中心，公开通报处理过程及结果，引导正确舆论。

（4）各有关单位、各部门在应急处置过程中，要做好工作记录，尽可能保留相关证据。对于人为破坏的违法行为，将配合公安司法机关依法处理。

4.2.3 III级响应措施

（1）领导小组办公室负责人立即到位，迅速研究制定对策，通报和协调相关各部门开展应急处置工作，及时监控事态进展，并向领导小组汇报处置情况。

（2）相关单位、部门及时进行处置，防止事态扩大。网络信息中心从技术上进行指导、支持，保证尽快消除影响、系统恢复正常。

（3）必要时，领导小组及时通过学校新闻中心，公开通报处理过程及结果，引导正确舆论。

（4）各有关单位、部门在应急处置过程中，要做好工作记录，尽可能保留相关证据，并按规定追究相应责任。

4.2.4 Ⅳ级响应措施

（1）领导小组办公室及时通报和协调相关单位、部门开展应急处置工作，及时监控事态进展，必要时向领导小组汇报事件基本情况。

（2）相关单位、部门及时进行处置，防止事态扩大。网络信息中心从技术上进行指导，保证尽快消除影响、系统恢复正常。

（3）各有关单位、部门在应急处置过程中，要做好工作记录，尽可能保留相关证据，并按规定追究相应责任。

5.后期处置

Ⅰ级网络与信息安全事件由学校在上级部门的指导下，组织事件的调查处理和总结评估，部署学校各相关单位、部门负责系统的恢复重建。Ⅱ级及以下网络与信息安全事件由领导小组指导相关部门进行事件调查总结和系统重建。

6.保障措施

6.1 技术支持队伍

加强网络信息中心技术队伍建设，确保校园网公共服务符合技术标准和管理规范。通过技术培训、研讨、承担科研任务等方式不断提高技术人员的业务水平，为校园网络和信息的安全保障提供强大技术支撑。

各单位、各部门要确定至少一名责任心强、有一定网络信息技术应用能力的人员负责网络和信息安全管理，加强与网络信息

中心的业务联系和交流。网络信息中心通过培训、讲座、报告等方式加强对中层单位技术人员的业务指导。

6.2 信息报送机制

以单位、部门信息员报送为主，同时拓宽信息收集渠道，倡导师生参与网络与信息安全事件的信息报告和监督，保证事件的早报告早处理。各单位、各部门要及时收集、分析和评估所属网络和信息方面的信息情报，努力将隐患减至最小。

各单位、各部门要及时与网络信息中心沟通，将重要信息汇总至领导小组办公室。领导小组办公室将信息及时汇总到领导小组，供领导参考。

6.3 经费保障

学校和各单位、各部门对于网络和信息安全方面要有必要的投入,从技术和管理上为日常管理和事件应急工作提供经费支持，并在年度预算中列出。

7.宣传、培训与演练

在领导小组领导下，学校新闻中心、网络信息中心要加强网络与信息安全的法律法规、新闻动态和知识技能的宣传、教育和培训，提高师生的网络与信息安全意识和应对能力。

学校各单位、各部门要将网络与信息安全事件的应急知识列为管理干部和有关人员的培训内容，加强网络与信息安全特别是网络与信息安全应急预案的培训，提高防范意识和技能。领导小

组办公室每年组织至少一次安全培训，不定期针对不同级别安全事件组织 1-2 次演练。

8.附则

8.1 本预案由校园网络与信息安全事件应急处置工作领导小组办公室负责解释。

8.2 本预案自印发之日起施行。

潍坊学院办公室　　2021年10月20日印发