**泰山护理职业学院网络安全应急预案**

为确保发生网络安全问题时各项应急工作高效、有序地进行，最大限度地减少损失，根据互联网网络安全相关条例及上级相关部门文件精神，结合我院校园网工作实际，特制定本预案。

学院成立网络安全应急领导小组负责学院网络安全应急处理，领导小组办公室设在信息中心。

一、网站不良信息事故处理预案

（一）一旦发现学院网站上出现不良信息（或者被黑客攻击修改了网页），立刻关闭网站。

（二）备份不良信息出现的目录。

（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，并测试网站运行。

（六）修改该目录名，对该目录进行安全性检测，升级安全级别和程序，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，如果来自院内，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。领导小组可视情节严重程度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，必须保持向领导小组组长汇报，解释此次事故的发生情况、发生原因、处理过程。

二、网络服务器设备处理预案

（一）广域网外部线路中断紧急处置措施

1. 广域网主、备用线路中断一条后，网络管理员应立即启动备用线路接续工作，同时向应急处理工作小组报告。

2. 网络管理员应尽快判断故障节点，查明故障原因。

3. 如属学院管辖范围，由网络管理员立即予以修复。

4. 如属运营商管辖范围，立即与运营商维护部门联系，要求恢复。

5. 如果主、备用线路同时中断，网络管理员应在判断故障节点，查明故障原因后，尽快研究恢复措施，并立即向应急处理工作小组组长汇报。

6. 经应急处理工作小组同意后，应通知相关部门相关原因，并暂缓使用业务系统和上传数据。

（二）局域网中断紧急处置措施

1. 局域网中断后，网络管理员应立即判断故障节点，查明故障原因，并向应急处理工作小组组长汇报。

2. 如属线路故障，应重新安装线路。

3. 如属路由器、交换机等信息系统设备故障，应立即通知供应商进行保修。

4. 如属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调试通畅。

（三）设备安全紧急处置措施

服务器、存储设备等关键设备损坏后，信息中心服务器、存储硬件管理员应立即向信息系统管理人员及应急处理小组报告。

1. 服务器、存储设备管理员立即查明原因。

2. 如果能够自行恢复，应立即用备件替换受损部件。

3. 如属不能自行恢复，立即与设备提供商联系，请求派维护人员前来维修。

4. 如果设备一时不能修复，应向应急处理工作小组组长汇报，并告之相关部门，暂缓使用受影响的业务系统。

三、学院重大网络事件处理预案

（一）关闭其它与该网络相连，有可能对该网络造成不利影响的一切网络设备及计算机设备，保障该网络的畅通。

（二）对重要网络设备提供备份，出现问题需尽快更换设备。

（三）对外网连接进行监控，清除非法连接，出现重大问题立刻向上级部门求救。

（四）事先应向领导小组汇报本次事件中所需用到的设备、环境，以及可能出现的事故及影响，在事件过程中出现任何问题应立刻向领导小组组长汇报。

四、日常管理

（一）领导小组依法发布有关消息和警报，全面组织各项网络安全防御、处理工作。各有关组员随时准备执行应急任务。

（二）网络管理员对校园内外所属网络硬件软件设备及接入网络的计算机设备定期进行全面检查，封堵、更新有安全隐患的设备及网络环境。

（三）加强对校园网内计算机设备的管理，加强对学院网络的使用者（学生和教师）的网络安全教育。加强对重要网络设备的软件防护以及硬件防护，确保正常的运行软件硬件环境。

（四）加强各类值班值勤，保持通讯畅通，及时掌握学院情况，全力维护正常教学、工作和生活秩序。

（五）按预案准备落实各项物资及相关经费。

五、其他

（一）在应急行动中，学院各部门要密切配合，服从指挥，确保政令畅通和各项工作的落实。

（二）各部门应根据本预案，结合本部门实际情况，认真制定本部门的应急预案，并切实落实各项组织措施。

（三）本预案从发布之日起施行。

（四）本预案由网络安全应急领导小组负责解释。