**周口文理职业学院**

**重要敏感期网络维稳工作方案**

为在重要敏感时期有效预防、及时控制和妥善处理利用校园网传播有害信息等突发事件，提高快速反应和应急处置能力，减轻或消除突发事件的危害和影响，确保校园网信息安全，按照“谁主管、谁主办、谁负责”的原则，根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》、《周口文理职业学院网络信息安全管理办法》、《周口文理职业学院网络与信息安全事件应急预案》等相关法律法规及规章制度，并结合学校工作实际，特制定本方案。

一、重要敏感期维稳工作领导小组

组长：韩广飞

副组长：周天义

成员：赵可可 候振 王振明 李洋 韩鹏

职责：负责预防校园不良信息的传播、校园病毒的危害、校园非法访问、校园恶意破坏、校园对外服务器等事务，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。

二、预防措施和信息报送

（一） 预防措施

学校目前已部署的网络安全设备及软件有：防火墙、WEB防火墙、下一代防火墙、入侵检测系统、运维审计、上网行为管理等。具体预防措施包括：

**1.完善应急管理制度。**落实《周口文理职业学院网络信息安全管理办法》、《校园网值班人员工作条例》，提高有关人员的责任意识、安全意识和技术水平。值班人员加强网络安全意识，注意掌握舆情动态，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。工作人员重点监控校内对外服务器及各个信息系统，及时掌握校内网络安全动态。

**2.加强信息监控。**学校通过舆情监控系统，做好相应的配置、管理和日志保存工作，发现问题及时上报。重点监控校内对外服务器，周口文理职业学院网站、微信公众号、抖音等自媒体平台及各微信群，及时掌握校内网络舆情动态。特殊时期，24小时轮流值班，专人监控访问地址，严控网络舆情事件，提高政治站位，值班人员手机24小时不关机。

**3.加强全校应急组织管理工作。**在敏感时期针对可能出现的问题，召开各学院及各职能部门的网络管理员培训会议，督促各部门做好各自网络维护及检查工作。

（二）信息报送

最先发现或接到发生校园网信息安全事件的人，要第一时间向学校网络安全和信息化领导小组报告。报告内容包括事件发生的时间、地点、涉及人员和软硬件情况，事件的危害影响程度和发展趋势等基本情况。

三、 应急处理方式

校园网信息安全事件发生后，根据网络与信息安全事件分类采取不同应急处置方式。

（一）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。按照事件发生的性质采取以下方案：

病毒传播：及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围；为避免产生更大的损失，保护健康的计算机，必要时可关闭相应的端口，甚至相应楼层的网络，及时进行杀毒处理。

外部入侵：判断入侵来源，区分外网与内网，评价入侵可能或已经造成的危害。对入侵未遂、未造成损害的，且评价威胁较小的外网入侵，定位入侵的IP地址，及时关闭入侵的端口，限制入侵IP地址的访问。对于已经造成危害的，应立即断开网络连接，避免造成更大损失和影响。

内部入侵：查清入侵来源，如IP地址、所在位置等信息，同时断开对应的交换机端口，针对入侵行为调整入侵检测和防御策略。对于无法制止的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

（二）设备故障事件：判断故障发生点和原因，迅速联系设备厂商抢修故障设备，优先保证校园网主干网络和主要信息系统的运转。

（三）灾害性事件：根据实际情况，在保障人身安全的前提下，保障数据和设备安全。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。

（四）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拔掉网络连接线，阻止有害信息传播，查找信息发布人并做好善后处理。对公安机关要求我校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。

（五）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上级信息安全机构。

周口文理职业学院 2024年2月28日