河南开封科技传媒学院重要敏感期网络维稳工作方案

为了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，确保我校校园网信息安全，结合学校工作实际，按照 “谁主管、谁主办、谁负责”的原则，根据《国家网络安全法》、《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中国教育和科研计算机网管理办法》、《河南开封科技传媒学院校园网信息网络安全管理制度》制定本预案。

一、重要敏感期维稳工作领导小组

组长：郑逢斌

副组长：王艳

成员：王宝祥 方云录

职责：负责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，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

目前已部署的网络安全设备及软件有：防火墙、WEB防火墙、防病毒模块、入侵检测系统、僵木蠕检测系统、日志服务器、上网行为管理，数据备份等。 具体预防措施包括：

**1.完善应急管理制度。**落实《校园信息网络安全管理制度》、《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。重点监控校内对外服务器、河南开封科技传媒学院贴吧、微博、抖音、快手等自媒体平台及各微信群及时掌握校内网络舆情动态。

**2.加强信息监控。**通过清博大数据系统，做好相应的配置、管理和日志保存工作，发现问题及时上报。同时，建立完备的网络评论员制度，通过人工方式手动监控校园网主页及二级网站的信息；特殊时期，24小时轮流值班，专业监控访问地址，有不清楚、不常用的外来访问的地址重点监控。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，尤其是信息网络中心。

**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，督促各部门及二级学院做好各自网络维护及检查工作。实验室逐一检查，备案整改到位。

（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，要第一时间向向校园网信息安全事件应急处置工作领导小组报告。报告内容包括事件的时间、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、 应急基本措施

校园网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。

（一）对于病毒传播类事件，要及时断开传播源，判断病毒的性质、传播端口，然后关闭相应的端口，在网上公布病毒攻击信息以及防御方法，并将处理情况上报校园网信息安全应急处置工作领导小组。

（二）对于黑客攻击与入侵类事件，保留相应的证据，判断入侵的来源，区分外网与内网。入侵来自外网的，定位入侵的IP地址，及时关闭入侵的端口，限制入侵地IP地址的访问，在无法制止的情况下可以采用断开网络连接的方法。入侵来自内网的，查清入侵来源，如IP地址、上网帐号等信息，同时断开对应的交换机端口。如有信息被篡改，一经发现马上断开相应的信息上网链接，并尽快恢复。

（三）对于有害信息类事件，及时报告校园网信息安全事件应急处置工作小组，通知该系统的负责人，对有害信息进行截屏记录，保留日志等证据后进行清除，尽量查清信息来源与责任人。对于来自外网的IP地址，保留相应的访问记录；对于来自我校的IP地址，立即进行定位查证工作，查证结果及时向校园网信息安全事件应急处置工作领导小组报告。

1. 对其它可能出现的问题，请根据安全事件报告和处置管理制度执行。

河南开封科技传媒学院

 2023年2月22日