**三明学院校园网络与信息安全应急处置预案**

**一、 总则**

（一）指导思想：减轻和消除网络安全突发事件造成的危害和影响，维护学校的安全和稳定，“统一领导、统一指挥、各司其职、整体作战、发挥优势、保障安全”。

 （二）适用范围：三明学院校园网。

 （三）处置原则：快速、有效。

**二、组织指挥和职责任务**

 （一）组织指挥

 由三明学院网络信息安全工作领导小组授权的领导组织指挥。

 （二）职责任务

 及时向上级汇报。

 各学院、部门的网络安全员应配合网络中心技术人员进行技术处理，无法处理的应尽可能完整地保护现场并及时通知公安部门。

**三、处置措施和处置程序**

 （一）处置措施

 1．在严重情况下，网络中心技术人员通过技术手段切断校园网络与外界的连接；

 2．通知当班领导及校领导；

 3．物理隔离出现安全事故的设备，复制相关日志，并进行适当的技术处理以保持现状。

 （二）处置程序

 1．发现情况：校内各处值班人员发现网页的互动栏目、网页异动、网络病毒、入侵、反动邮件等网络安全事故；

 2．预案启动：一旦发现以上任何一种或其他重大网络安全事故，本预案即时启动，并通知上级领导；

 3．应急处置：尽可能保持现场，在安全事故发现后10分钟响应，在30分钟内必须按规定的处置措施进行处理；

 4．情况报告：在技术人员采取相应的应急措施后，各值班人员要负责及时将备案汇总向校党政办报告。校办根据实际情况，向当日值班校领导、主管校领导汇报或向省教育厅主管部门及省公安厅主管部门汇报；

 5．发布预警：在三明学院网络信息安全工作领导的部署下，向相关职能部门发布预警；

 6．预案终止：技术人员根据事件处理的结果或领导指示，恢复网络连接及其相应措施以终止预案恢复正常使用。

**四、保障措施**

 （一）人员保障

 敏感期间，安排24小时专人值班。各学院、部门、所安排网络安全员24小时监控网页的互动栏目等。

 （二）技术保障

 防火墙系统、WAF、IPS、漏洞扫描、数据库安全审计、抗拒绝服务产品系统、运维安全管理产品系统（堡垒机）、入侵防护产品系统。网络中心人员可通过远程环境或现场操作及时反应，并由网络安全产品厂家的技术支持。网页的互动栏目采用先审后发机制。

 （三）物质保障

 关键岗位配备有移动电话，保证24小时开机。

 （四）训练和演练

 通过校内各种宣传形式对师生员工进行正面引导、宣传并落实我校园关于网络安全的各项规章制度。各学院、处、所安排人员参加公安部门的网络安全培训。敏感时期之前，在校园网络安全领导小组统一部署下，安排全校范围演练。

**五、工作要求**

 所有值班人员必须坚持在岗、保证通讯畅通、工作认真负责。如在网络安全突发事件出现擅自离岗、脱岗的行为，造成学校不可挽回的损失，学校将按相关规定对其进行处理。

**三明学院网络信息安全工作领导小组**

**2017年7月**