网络和信息安全类突发事件应急处置预案

1 预警和预防机制

1.1 预警与预防信息

网络信息中心应通过监测及时发现异常状态和潜在的问题，对异常状态给出预警信息并及时处理。

1.2 预防行动

校园网的信息安全日常工作由网络信息中心牵头，各成员单位分工负责。网络信息中心要按要求安排值班，并将值班安排上报，确保做到人人到岗到位、联络畅通，处理及时准确。

1.3 预防措施

1.3.1 网站、网页出现非法言论事件紧急处置措施

网站、网页由主办部门的值班人员负责随时密切监视信息内容，发现在网上出现非法信息时，值班人员应立即向主管信息安全负责人通报情况，情况紧急的，应先及时采取处理措施，防止有害信息的扩散，再按程序报告。

信息安全相关负责人应在接到通知后立即赶到现场，做好必要纪录，清理非法信息，妥善保存有关记录及日志，在确保安全问题解决后将网站网页重新投入使用。

事后追查非法信息来源，并将有关情况向主管部门汇报。

1.3.2 黑客攻击事件紧急处置措施

当有关值班人员发现网页内容被篡改，或通过入侵检测系统发现有黑客正在进行攻击时，应立即向信息安全负责人通报情况。信息安全相关负责人应在接到通知后立即赶到现场，并首先将被攻击的服务器等设备从网络中隔离出来，并清除木马、系统漏洞、后门，检查系统所有密码，关闭不必要的端口。对现场进行分析，并写出分析报告进行存档，及时恢复和重建被攻击或受破坏的系统，并向主管部门汇报。

1.3.3 病毒事件紧急处置措施

用户发现重要计算机被感染上病毒后，应立即向信息安全负责人报告，将该机从网络中隔离开来。信息安全相关负责人应在接到通知后立即赶到现场，对该设备的硬盘进行数据备份，启用反病毒软件对该机进行杀毒处理，同时通过病毒检测软件对其他机器进行病毒扫描和清除工作。如果现行反病毒软件无法清除该病毒，应立即联系有关产品商研究解决，并向公安部门汇报。

1.3.4 软件系统遭破坏性攻击的紧急处置措施

重要的软件系统平时必须存有备份，与软件系统相对应的数据必须按本单位备份规定的间隔时间按时进行备份，妥善保管。一旦遭到破坏性攻击，应立即向信息安全相关负责人报告，并将该系统停止运行。检查信息系统的日志等资料，确定供给来源，再恢复软件系统和数据。如认为事态严重，则立即向公安部门报警。

1.4.5 网络中断紧急处置措施

设备管理部门平时应准备好网络备用设备，存放在指定的位置。网络中断后，信息安全相关负责人应立即判断故障节点，查明故障原因。如属线路故障，应及时检查线路，调整或重新安装线路。如属网络设备故障，应及时恢复或更换设备，并调试通畅。

1.4.6 设备安全紧急处置措施

小型机、服务器等关键设备损坏后，值班人员应立即向信息安全负责人报告。信息安全相关负责人立即查明原因，如果能够自行恢复，应立即用备件替换受损部件，如属不能自行恢复的，立即与设备提供商联系，请求派维护人员前来维修，如果设备一时不能修复，应向应急工作组。

2 应急响应

2.1 网络运行事件处置

网络运行相关事件由网络信息中心负责，重大事件立即向应急工作组报告。事件包括线路中断、路由故障、流量异常、域名系统故障等。遇大规模的恶意移动代码、拒绝服务攻击、系统入侵和端口扫描等事件，管理员应及时记录现场，通知单位应急负责人和中心主管，决定上报或通报，同时采取措施加以控制，处置人员记录事件处理步骤和结果，总结报告。

2.2 信息安全事件处置

发生信息安全事件应紧急通知信息主管负责人，及时消除非法信息，恢复系统。无法迅速消除和恢复的系统，影响较大时实施紧急关闭、并紧急上报应急工作组。

2.3 网络环境安全事件处置

网络环境安全相关事件由网络信息中心负责处置。对火灾、盗窃、破坏等紧急事件按照国家消防有关法律法规、学校有关规定处理。影响网络运行和信息安全的重大事件由网络与信息安全类突发事件应急处理工作组统一指挥处置。

遇供电相关紧急事件，根据停电事件、用电功耗、电池电能储备、供电管理部门信息、网络和信息运行情况等条件作调度，包括次要系统停电减轻负载等措施，密切跟踪参数变化并反馈、调整、控制，联系相关公司和人员作现场维护。