阿城区教育系统网络与信息安全应急预案

为确保全区教育系统网络正常安全使用，妥善处理危害网络与信息安全的突发事件，最大限度地遏制突发事件的影响和有害信息的扩散，按照国务院《互联网信息服务管理办法》和省、市相关部门的规定，特制订本预案。

一、工作原则

遵循“谁主办、谁负责”的原则，统一管理，分级负责，快速反应，高效处置。

二、组织机构

建立阿城区教育系统网络与信息安全管理工作领导小组，负责对全系统网络与信息安全管理工作的全面领导，贯彻执行各级关于加强网络与信息安全管理的文件，督促指导学校采取有力措施加强管理，监督检查各学校、单位网络信息安全措施的落实情况。在教育系统网络与信息安全管理工作领导小组的直接领导下，由局办公室、信息科和教育信息中心组织相关人员负责网络重大突发事件应急处置的指挥和协调。阿城区教育系统网络与信息安全管理领导小组，由主管信息工作的副局长任组长，信息科科长、各学校校长任副组长，信息科和信息中心人员、各学校主管校长为成员。各学校和局属事业单位均应建立相应的安全管理工作小组，重点加强网上信息监控巡查，重点监控可能出现有害信息的站点;及时组织有关部门和专业技术人员对网络上出现的突发事件进行处理，并根据情况的严重程度上报有关部门;切实担负起本单位网络与信息安全管理工作职责，与区公安局网络监察大队保持紧密联系，确保反应迅速，及时做好有关案件的调查、取证等工作。

 三、应急处置措施

（一）平台出现非法言论时的紧急处置措施

1、平台由本周值周长负责密切监视信息内容。每一小时检查一次。

2、发现网上出现非法信息时，负责人员应立即向信息安全组组长通报情况；情况紧急的应先及时采取隔离、删除等处理措施，再按程序报告。

3、信息安全组具体负责的技术人员应在接到通知后十分钟内赶到现场，作好必要的记录，清理非法信息，强化安全防范措施，并将平台、网页重新投入使用。

4、平台维护员应妥善保存有关记录及日志或审计记录。

5、平台维护工作人员应立即追查非法信息来源。

6、工作人员会商后，将有关情况向安全领导小组汇报有关情况。

7、安全领导小组召开安全领导小组会议，如认为情况严重，应及时向有关上级机关和公安部门报警。

（二）黑客攻击时的紧急处置措施

1、当有关负责人员平台内容被篡改，或通过入侵检测系统发现有黑客正在进行攻击时,应立即向网络安全员通报情况。

2、网络安全员应在十分钟内赶到现场，并首先应将被攻击的服务器等设备从网络中隔离出来，保护现场，同时向信息安全领导小组副组长汇报情况。

3、网络安全员和网络管理员负责被破坏系统的恢复与重建工作。

4、网络安全员协同有关部门共同追查非法信息来源。

5、安全领导小组会商后，如认为情况严重，则立即向公安部门或上级机关报警。

（三）病毒安全紧急处置措施

1、当发现计算机感染病毒后，应立即将该机从网络上隔离出来。

2、对该设备的硬盘进行数据备份。

3、启用反病毒软件对该机进行杀毒处理，同时进行病毒检测软件对其他机器进行病毒扫描和清除工作。

4、如发现反病毒软件无法清除该病毒，应立即向安全小组负责人报告。

5、信息安全小组相关负责人员在接到通报后，应在十分钟内赶到现场。

6、经技术人员确认确实无法查杀该病毒后，应作好相关记录，同时立即向信息安全领导小组副组长报告，并迅速联系有关产品商研究解决。

7、安全领导小组经会商后，认为情况极为严重，应立即向公安部门或上级机关报告。

8、如果感染病毒的设备是服务器或者主机系统，经领导小组组长同意，应立即告知各下属单位做好相应的清查工作。

（四）软件系统遭受破坏性攻击的紧急处置措施

1、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有多日备份，并将它们保存于安全处。

2、一旦软件遭到破坏性攻击，应立即向网络安全员、网络管理员报告，并将系统停止运行。

3、网络安全员和网站维护员负责软件系统和数据的恢复。

4、网络安全员和网络管理员检查日志等资料，确认攻击来源。

5、安全领导小组认为情况极为严重的，应立即向公安部门或上级机关报告。

（五）数据库安全紧急处置措施

1、各数据库系统要至少准备两个以上数据库备份，平时一份放在机房，另一份放在另一安全的建筑物中。

2、一旦数据库崩溃，应立即向网络安全员报告，同时通知各下属单位暂缓上传上报数据。

3、信息安全员应对主机系统进行维修，如遇无法解决的问题，立即向上级单位或软硬件提供商请求支援。

4、系统修复启动后，将第一个数据库备份取出，按照要求将其恢复到主机系统中。

5、如因第一个备份损坏，导致数据库无法恢复，则应取出第二套数据库备份加以恢复。

6、如果两个备份均无法恢复，应立即向有关厂商请求紧急支援。

（六）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，有关人员应立即启动备用线路接续工作，同时向网络安全员报告。

2、网络安全员接到报告后，应迅速判断故障节点，查明故障原因。

3、如属我方管辖范围，由网络管理员协同网络安全员立即予以恢复。如遇无法恢复情况，立即向网络运营商请求支援。

4、如属网络运营商管辖范围，立即与网络运营商联系，请求修复。

5、如果主、备用线路同时中断，网络安全员应在判断故障节点，查明故障原因后，尽快与其他相关领导和工作人员研究恢复措施，并立即向安全领导小组汇报。

6、经安全领导小组同意后，应通告各下属单位相关原因，并暂缓上传上报数据。

（七）局域网中断紧急处置措施

1、局域网中断后，网络管理员和网络安全员应立即判断故障节点，查明故障原因，并向网络安全领导小组副组长汇报。

2、如属线路故障，应重新安装线路。

3、如属路由器、交换机等网络设备故障，应立即与设备提供商联系更换设备，并调试畅通。

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，并调试畅通。如遇无法解决的技术问题，立即向上级单位或有关厂商请求支援。

5、如有必要，应向安全领导小组组长汇报。

（八）设备安全紧急处置措施

1、服务器等关键设备损坏后，有关人员应立即向网络管理员和网络安全员汇报。

2、网络管理员和网络安全员应立即查明原因。

3、如果能够自行恢复，应立即用备件替换受损部件。

4、如果不能自行恢复的，立即与设备提供商联系，请求派维修人员前来维修。

5、如果设备一时不能修复，应向安全领导小组领导汇报，并告知各下属单位，暂缓上传上报数据。

（九）人员疏散与机房灭火预案

1、一旦机房发生火灾，应遵照下列原则：首先确保人员安全；其次确保关键设备、数据安全；三是确保一般设备安全。

2、人员疏散的程序是：机房值班人员立即火警警报，并通过119电话向公安消防请求支援，所有不参与灭火的人员按照预先确定的线路，迅速从机房中撤出。

3、人员灭火的程序是：首先切断所有电源，取出灭火器进行灭火。

（十）外电中断后的设备

1、外电中断后，机房值班人员应立即切换到备用电源。

2、机房值班人员应立即查明原因，并向值班领导汇报。

3、如因机关内部线路故障，请机关服务部门迅速恢复。

4、如果是供电局的原因，应立即与供电局联系，请供电局迅速恢复供电。

5、如果供电局告知需长时间停电，应做如下安排：

（1）预计停电2小时以内，由UPS供电。

（2）预计停电24小时，关掉所有设备。

（十一）发生自然灾害后的紧急处置措施

1、上级单位平时储备一套下级单位的关键设备。

2、一旦发生自然灾害，导致设备损坏，由灾害发生单位向上级计算机网络与信息安全领导小组请求支援。

3、上级计算机网络与信息安全领导小组接到下级单位的支援请求后，应在24小时内派遣人员携带有关设备赶到现场。

4、到达现场后，寻找安全可靠的地点，重新构建新的系统和网络，并将相关数据予以恢复。

5、经测试符合要求后，支援小组才能撤离。

（十二）关键人员不在岗的紧急处置措施

1、对于关键岗位平时应做好人员储备，确保一项工作有两人能操作。

2、一旦发生关键人员不在岗的情况，先向值班领导汇报情况。

3、经值班领导批准后，由备用人员上岗操作。

4、如果备用人员无法上岗，请求上级单位支援。

5、上级单位在接到请求后，应立即派遣人员进行支援

四、保障措施

1、强化日常管理，确保涉密信息不上网。按照“上网信息不涉密，涉密信息不上网”的要求，严格信息发布审核，加大监管力度。各校要对本单位信息网络进行全面筛查，严禁在联接校园网的终端上存储、处理和传输涉密信息，严禁在校园内网上刊登传播涉密信息和不良信息，对所有联网终端和网络进行检查，不符合联网规定的予以清除。

2、强化安全防护措施，杜绝安全隐患。各校要组织对本校的信息安全风险评估，查找可能存在的安全隐患、安全漏洞、薄弱环节，进一步提升信息安全防范水平。对教育局及各学校的帐户、口令等进行一次清理检查，及时更新和升级，消除安全隐患。

3、完善网络与信息安全应急预案，并组织演练。要建立相应的应急预案，明确应急处理流程临时处置权限。落实应急技术支撑队伍，组织开展好应急演练，做到应急预案任务明确、组织实施科学、可操作性强，确保相关人员熟知熟用。

4、严格执行信息安全规定。禁止将涉密信息系统接入国际互联网等公共信息网络; 禁止在涉密计算机与非涉密计算机之间交叉使用U盘等移动存储设备; 禁止在没有防护措施的情况下将公共信息网络上的数据复制到涉密信息系统; 禁止涉密计算机、涉密移动存储设备与非涉密计算机、非涉密存储设备混用; 禁止使用具有无线互联功能的设备处理涉密信息。

5、严格落实责任制，完善保密规章制度。按照“谁主管谁负责、谁使用谁负责”的原则，认真履行网络信息安全职责。对网络信息安全各项制度进行一次全面梳理，重点抓好信息安全管理制度、应急预案、制度、信息发布审核制度的完善与落实。

本预案自印发之日起实施。