武昌首义学院
信息系统安全应急预案

一、总则

（一）编制目的

为提高我校处理网络与信息安全突发事件的能力，形成科学、有效、反应迅速的应急工作机制，确保我校校园网络重要计算机信息系统的实体安全、运行安全和数据安全，最大限度地减轻网络信息安全突发事件的危害，保护正常教学秩序，促进学校的和谐发展。结合本校工作实际，特制定本应急预案。

（二）编制依据

根据《中华人民共和国计算机信息系统安全保护条例》、《政府信息系统安全检查指南》、GB/T20269-2006《信息安全技术信息系统安全管理要求》、GB/T20270-2006《信息安全技术网络基础安全技术要求》、 GB/T20281-2006《信息安全技术防火墙技术要求和测试评价方法》、GB/T19716-2005《信息技术信息安全管理使用规则》等有关法规、规定，制定本预案。

（三）本预案适用于武昌首义学院网络与信息安全应急处理工作。

二、应急组织机构及职责

成立信息系统应急处理领导小组，负责领导、组织和协调全校信息系统突发事件的应急保障工作。

（一）领导小组成员：

组长：主管校长

副组长：校办主任、信息技术中心主任

成员：校办公室、信息技术中心、保卫处、设备处、宣传部党委组织部学生处教务处等部门相关人员组成。

应急小组日常工作由信息技术中心承担，其他各相关部门积极配合。

（二）领导小组职责：制订专项应急预案，负责定期组织演练，监督检查各部门在本预案中履行职责情况。对发生事件启动应急救援预案进行决策，全面指挥应急救援工作。

三、工作原则

（一）积极防御、综合防范

立足安全防护，加强预警，重点保护重要信息网络和关系教学安全的重要信息系统；从预防、监控、应急处理、应急保障和打击不法行为等环节，在管理、技术、宣传等方面，采取多种措施，充分发挥各方面的作用，构筑网络与信息安全保障体系。

（二）明确责任、分级负责

按照“谁主管谁负责”的原则，分级分类建立和完善安全责任制度、协调管理机制和联动工作机制。加强计算机信息网络安全的宣传和教育，进一步提高工作人员的信息安全意识。

（三）落实措施、确保安全

要对机房、网络设备、服务器等设施定期开展安全检查，对发现安全漏洞和隐患的进行及时整改。

（四）科学决策，快速反应

加强技术储备，规范应急处置措施和操作流程，网络与信息安全突发公共事件发生时，要快速反应，及时获取准确信息，跟踪研判，及时报告，果断决策，迅速处理，最大限度地减少危害和影响。

四、预防预警

（一）完善网络与信息安全突发公共事件监测、预测和预警制度。

加强对各类网络与信息安全突发事件和可能引起突发网络与信息安全突发公共事件的有关信息的收集、分析、判断和持续监测。当检查到有网络与信息安全突发事件发生或可能发生时，应及时对发生事件或可能发生事件进行调查核实、保存相关证据，并立即向应急领导小组报告。报告内容主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施建议等。

若发现下列情况应及时向应急领导小组报告：利用网络从事违法犯罪活动；网络或信息系统通信和资源使用异常；网络或信息系统瘫痪，应用服务中断或数据篡改、丢失；网络恐怖活动的嫌疑和预警信息；其他影响网络与信息安全的信息。

（二）设定信息安全等级保护，实行信息安全风险评估。

通过相关设备实时监控网络工作与信息安全状况。各基础信息网络和重要信息系统建设要充分考虑抗毁性和灾难恢复，制定并不断完善信息安全应急处理预案。针对信息网络的突发性、大规模安全事件，建立制度优化、程序化的处理流程。

（三）做好服务器及数据中心的数据备份及登记工作，建立灾难性数据恢复机制。

一旦发生网络与信息安全事件，立即启动应急预案，采取应急处置措施，判定事件危害程度，并立即将情况向有关领导报告。在处置过程中，应及时报告处置工作进展情况，直至处置工作结束。

五、处置流程

（一）预案启动

在发生网络与信息安全事件后，信息中心应尽最大可能迅速收集事件相关信息，鉴别事件性质，确定事件来源，弄清事件范围和评估事件带来的影响和损害，一旦确认为网络与信息安全事件后，立即将事件上报工作组并着手处置。

（二）应急处理预案

分别按照如下相应的事件处理预案执行:

1、《网络于信息安全处理预案》

2、《信息技术中心机房停电应急处理预案》

3、《机房门卫值班应急处理事项》

4、《信息技术中心突发灾难事件应急处理预案》

5、《信息技术中心突发治安事件应急处理预案》

（三）后续处理

安全事件进行最初的应急处置以后，应及时采取行动，抑制其影响的进一步扩大，限制潜在的损失与破坏，同时要确保应急处置措施对涉及的相关业务影响最小。安全事件被抑制之后，通过对有关事件

或行为的分析结果，找出其根源，明确相应的补救措施并彻底清除。在确保安全事件解决后，要及时清理系统、恢复数据、程序、服务，恢复工作应避免出现误操作导致数据丢失。

（四）记录上报

网络与信息安全事件发生时，应及时向网络与信息安全应急处置工作组汇报，并在事件处置工作中作好完整的过程记录，及时报告处置工作进展情况，保存各相关系统日志，直至处置工作结束。

六、保障措施

（一）应急设备保障

对于重要网络与信息系统，在建设系统时应事先预留一定的应急设备，建立信息网络硬件、软件、应急救援设备等应急物资库。在网络与信息安全突发公共事件发生时，报领导同意后，由应急工作组负责统一调用。

（二）数据保障

重要信息系统均应建立容灾备份系统和相关工作机制，保证重要数据在遭到破坏后，可紧急恢复。各容灾备份系统应具有一定的兼容性，在特殊情况下各系统间可互为备份。