附件1

滁州学院网络安全事件应急处置工作流程

为规范网络安全事件的应急处置过程，明确具体处置方法，特制定本流程。

**一、有害程序事件处置流程**

一旦发现有害程序事件，应执行以下应急处置流程：

1.立即切断感染有害程序主机与网络的连接，同时对该计算机的重要数据进行数据备份；

2.对事件进行初步处置，搜集相关信息，对事发情况进行报告；

3.利用防病毒软件对该计算机进行杀毒处理，并对同一局域网内其他计算机进行有害程序扫描和清除工作；

4.如果满足下列情况之一的，事件应升级响应：

⑴ 现行防病毒软件无法清除该有害程序的

⑵ 在1小时内无法处理完毕的

⑶ 有害程序不断通过网络扩散的

5.有害程序清理完毕后，恢复系统和相关数据，检查数据的完整性；

6.有害程序事件处理完毕，将计算机重新接入网络；

7.对事件处置情况进行报告，强化安全防范措施，总结防范经验。

**二、网络攻击事件处置流程**

一旦发生网络攻击（远程控制、后门攻击等）行为，应执行以下应急处置流程：

1.应立即切断主机与网络的连接；

2.对事件进行初步处置，对事发情况进行报告；

3.对入侵行为进行鉴定，做好必要的记录，妥善保存有关日志和审计信息；

4.追查攻击源，修改防火墙等设备的安全配置阻断入侵渠道；分析后台数据操作日志，判断是否发生数据失窃；同时进行事中情况报告；

5.事态无法控制或造成严重后果，事件应升级响应；情节严重的、构成违法犯罪的，需及时上报公安机关立案侦查；

6.修复或重建被攻击或破坏的系统，重新将恢复后的系统接入网络；

7.对事件处置情况进行报告，强化安全防范措施，总结防范经验。

一旦发现遭受拒绝服务攻击而导致系统访问流量异常、系统无法正常访问时，应执行以下应急处置流程：

1.发现可能遭受拒绝服务攻击时，首先对事件进行初步处置，进行事发情况报告；

2.技术人员对受攻击行为进行鉴定，做好必要记录，妥善保存有关日志和审计信息；

3.通过技术手段进行分析，追查攻击源，修改防火墙等设备的安全配置阻断攻击源，缓解、消除事件的影响，同时进行事中情况报告；

4.事态无法控制或持续造成影响，事件应升级响应；

5.消除攻击隐患，提取相关攻击证据后，恢复系统正常运行；

6.对事件处置情况进行报告，强化安全防范措施，总结防范经验。

**三、信息破坏安全事件处置流程**

一旦发现信息破坏事件，应执行以下应急处置流程：

1.对事件进行初步处置，对事发情况进行报告；

2.立即组织对事件进行勘察，做好必要记录，妥善保存有关日志和审计信息；

3.阻断信息破坏的渠道消除安全隐患，实施备份数据恢复工作，有关工作实施同时进行事中情况报告；

4.事态无法控制或造成恶劣影响，事件应升级响应；情节严重的、构成违法犯罪的，需及时上报公安机关立案侦查；

5.对事件处置情况进行报告，强化安全防范措施，总结防范经验。

**四、信息内容安全事件处置流程**

一旦发现信息内容安全事件，立即报告学校宣传部，由宣传部指导相关单位进行应急处置。

**五、设备设施故障事件处置流程**

数据中心机房网络及计算存储设备发生故障时，应执行以下应急处置流程：

1.判断故障发生点和故障原因，对事件进行初步处置，对事发情况进行报告；

2.尽快抢修故障设备，优先保证校园网主干网络和主要应用系统的运转；

3.设施故障排除后，系统恢复正常运行，进行事后总结报告，采取措施防止类似事件发生。

数据中心机房其他外部设备发生故障时，应执行以下应急处置流程：

1.空气调节系统故障：立即联系维保单位进行处理；若室内温度高于室外温度，打开机房门进行通风散热。

2.UPS系统故障。工作人员应立即查看情况，确认发生故障后，应立即联系厂家在线检查；在线检查不能解决故障时，联系厂家进行现场维修。

**六、灾害性事件处置流程**

一旦发生灾害性事件，应执行以下应急处置流程：

1.对事件进行初步处置，对事发情况进行报告；

2.发生的灾害为自然灾害时，根据实际情况，在保障人身安全的前提下，首先保障数据安全，其次是核心设备、普通设备安全；

3.发生灾害性事件后，立即组织对事件进行勘察，做好必要记录，妥善保存有关日志和审计信息，有关工作实施同时进行事中情况报告；

4.情节严重乃至事态无法控制的，事件应升级响应；

5.处理完毕后及时恢复系统或网站运行；

6.对事件处置情况进行报告，强化安全防范措施，总结防范经验。

**七、其他信息安全事件处置流程**

发生其他网络安全事件后，应执行以下应急处置流程：

1.对事件进行初步处置，对事发情况进行报告；

2.根据实际情况，与事发涉及的相关单位协商后妥善处理具体问题，如遇盗窃等事件，参照《安徽省学校安全条例》进行应急处理；

3.情节严重乃至事态无法控制的，事件应升级响应；

4.处理完毕后及时恢复相关服务；

5.对事件处置情况进行报告，强化安全防范措施，总结防范经验。