江苏开放大学
江苏城市职业学院 文件

苏开大（苏城院）信息〔2020〕2 号

网络监测与事件汇报制度

一、 网络监测

第一条 建立健全网络与信息安全组织机构，成立本单位网络与信息安全小组各小组将工作责任落实到个人。

第二条 建立健全网络与信息安全岗责体系和规章制度。

第三条 明确自身信息系统的信息安全等级、信息安全保护等级。

第四条 网络管理员、安全员必需随时监控网络设备、安全设备的运行状况，通过网管工具及时发现问题，解决问题，自己不能解决的问题及时上报。

第五条 安全员要监控防病毒网关等设备的运行情况，及时查看设备防病毒库是否最新；系统管理员要监测计算机的病毒情况，检查计算机是否都安全了防病毒软件，病毒库是否更新为最新。

二、 事件汇报

第六条 安全管理员接收从机房值班转来的事件或安全监控系统产生的需要跟进的事件，根据事件的范围、影响和紧急程度对安全事件进行分类。

1.紧急/严重安全事件：关键业务系统由于安全原因崩溃、系统性能严重下降，已无法提供正常服务；网络出口由于网络安全原因非正常中断、堵塞，严重影响用户使用；系统由于安全原因停止服务或者信息被篡改造成恶劣影响。

2.普通安全事件：影响部分/个别用户和非关键的业务系统，系统或网络性能轻微下降（<20%），仍可以提供正常服务。

第七条 遇有紧急/严重安全事件，安全管理员须立刻将事件通报给信息安全主管领导。

第八条 信息安全主管领导协调、组织相关资源，处理安全事件，并通告相关部门。

1.安全管理员联合联系安全服务商，系统管理员负责相应的系统，对事件进行诊断、定位，查找问题根源。

2.找到原因后需要确定受影响的系统范围，进行紧急修复，如系统隔离、设置防火墙、路由器规则，更新系统补丁等。在进行修复时应注意采取措施进行证据的收集和保全，记录或复制入侵证据、破坏和损失，归档备查。

3.恢复系统服务和数据，解决安全事件后，安全管理员联合安全服务商和系统管理员对受到影响的系统进行全面评估，并对存在类似隐患的所有系统进行分析统计，制定相应的安全加固，安全防护等解决方案，并由安全管理员负责跟进落实。

第九条 对于普通安全事件，由安全管理员进行调查处理，必要时联合安全服务商和系统管理员。

第十条 进行安全修复、加固防护所进行的配置和更改工作，都需要进行相关测试，并严格按照《信息系统资源调整管理办法》办理。

第十一条 安全管理员负责填写并维护《系统及网络安全监控记录》，负责安全事件的跟踪管理。

江苏开放大学信息化建设处

2020 年 7 月 18 日