福建广播电视大学文件

闽电大信息化〔2018〕4号

关于印发《福建广播电视大学网络安全事件处理预案》的通知

各部门、学院：

现将《福建广播电视大学网络安全事件处理预案》印发给你们，请认真遵照执行。

福建广播电视大学信息化中心

2018年9月24日

福建广播电视大学网络安全事件处理预案

一、总则

（一）指导思想

网络与信息安全事关国家的政治稳定、社会安定和经济运行安全。为确保网络正常使用，充分发挥网络在学校办学实践中的作用，促进我校远程教育信息化健康发展，遵照国务院《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网站国际联网管理暂行规定》、《计算机信息网站国际联网安全保护管理办法》和《互联网安全保护技术措施规定》以及省教育厅和我校的有关网络安全管理规定，本着“以防为主”的原则，特制订本预案，以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。

（二）处置原则

按照预防为主、防治结合、快速反应、减少损失的处置原则，做好网络安全事件的处置。

二、处置措施和处置程序

（一）处置措施

1.学校各部门网络安全管理员以及相关工作人员一旦发现安全事件，应根据实际情况第一时间采取断网等有效措施进行处置，将损害和影响降低到最小范围，保留现场，并报告本部门负责人。

2. 部门负责人接到报告后应将相关情况通知福建广播电视大学信息化中心。

3. 信息化中心接到通知后，根据安全事件的实际情况（影响范围、严重程度）决定向宣传部、校领导报告并组织力量开展应急处置。视情况决定是否需要进一步报告省教育厅、省委网信办和省公安厅等。

4. 事发部门应及时跟进事件进展情况。

（二）处置程序

1. 发现情况

（1）网络管理科发现安全事件时及时报告信息化中心领导。

（2）各部门、个人发现网络或机器运行不正常，及时报告网络管理科，由网络管理科采用相应技术手段对出现的状况进行故障诊断，如属于病毒感染、黑客入侵等安全事件及时上报信息化中心领导。

2. 预案启动

一旦发现网络安全事件，应立即将情况向信息化中心汇报，并及时启动预案。

3. 应急处置

根据情况的严重性，及时判断，分析问题，排除问题。

按照网络安全事件发生的性质分别采用以下方案：

（1）病毒传播

当发现有计算机被感染上病毒后，应立即将该机从网络上隔

离开来，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，判断病毒的性质、采用的端口，然后关闭相应的端口，同时在网上公布病毒攻击信息以及防御方法。

如果感染病毒的设备是主服务器，应立即告知有关部门做好相应的清查和数据保护工作。

（2）黑客攻击

当发现网页内容被篡改，应马上断开相应的信息上网链接，并尽快恢复。

当通过入侵检测系统发现有黑客正在进行攻击时，应首先将被攻击的服务器等设备从网络中隔离出来，保护现场。然后分析入侵的来源，区分外网与内网。入侵来自外网的，定位入侵的IP地址，及时关闭入侵的端口，限制入侵的IP地址的访问，在无法制止的情况下可以采用断开网络连接的方法。入侵来自内网的，查清入侵来源，如IP地址、上网帐号等信息，同时断开对应的交换机端口，然后针对入侵方法建设或更新入侵检测设备，最后恢复与重建被攻击或破坏系统。

（3）发现非法信息

如果发现非法信息，应及时通报相关情况，情况紧急的，应先及时采取删除等处理措施，再按程序报告。具体负责的技术人员应做好必要记录，清理非法信息，妥善保存有关记录及日志或审计记录，强化安全防范措施，并将网站重新投入使用。最后需组织力量追查非法信息来源，采取相关措施。

（4）网络故障

当发现外网线路中断，则立即与电信维护部门联系，请求配合测试，要求尽快修复，并跟踪恢复情况及时通知学校各部门。

当发现局域网中断后，应立即判断事故节点，查明故障原因。如属线路故障，应重新安装线路。如属路由器、交换机等网络设备故障，应立即联系相关维修公司查出故障原因，如能维修的要尽早维修好，不能维修的，要及时重新购置，以确保尽早恢复网络通畅。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，并调测通畅。

（5）设备安全

服务器等关键设备损坏后，应立即查明原因，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。

（6）非常时期网上信息监控处理程序

上级或学校领导通知的非常时期，对于监控中发现或者公安部门网上巡检发现我校校园网上出现有害信息的，一方面做好这些信息的备份和记录工作，查清来源地址和发布人；另一方面及时删除，并根据我校管理制度对相关责任人进行处理。

（7）其它

其它不确定因素造成的灾害，结合具体的情况，做出相应的处理。不能处理的可以请求相关专业人员。

4. 情况报告

（1）各部门一旦发现安全事件，应及时将网络安全事件（包括事件名称、事发单位和目标机器 IP 地址，以及危害程度）报告福建广播电视大学信息化中心。

（2）信息化中心根据安全事件的实际情况（影响范围、严重程度）决定上报宣传部、校领导，视情况决定是否需要进一步报告省教育厅、省委网信办和省公安厅等。

5. 发布预警

网络安全事件经相关部门领导审批同意后，将在福建广播电视大学网站和学校公告版发布，对全校人员起警示作用。

6. 预案终止

信息化中心针对所发生的安全事件，判断是属于主动行为还是被动、无意的行为及造成的危害程度，并对相关人员做出相应的处罚和教育，同时终止预案。

三、保障措施

（一）人员保障

福建广播电视大学信息化中心人员和各部处网络安全管理员要明确责任，各司其职，各负其责。

（二）技术保障

制定网络安全策略，购置相应的安全防范专用设备，包括网络防病毒系统、防火墙系统、入侵检测系统、有害信息过滤等安全防护产品，为福建广播电视大学的整体网络安全提供技术保障。

（三）物资保障

每年列出专项经费，用于网站安全技术防范设备的添置、升级、更新，以及外聘专业网络安全服务商、内部工作人员培训的费用。避免应急拖延造成不必要的损失，保证应急响应队伍技术装备的及时更新，以确保应急响应工作的顺利进行。

（四）训练

配合学校职能部门，开展网络安全管理员等相关培训，增强实战经验和应急处理能力，提高技术水平。

四、工作要求

1. 按照信息化中心岗位职责的要求，信息化中心人员各司其责切实加强日常信息网络安全工作的检查、维护，每周或每月升级系统补丁和杀毒软件，检查防火墙的运行情况，及时消除隐患。

2. 发生安全事件时，应急处置工作人员 1 小时内到达现场，一般情况下 1 小时内解决故障，恢复运行；对于有些特别重大而涉及面广的安全事件，也要在 4 小时内解决，不能解决的要及时上报，并说明原因和处理办法，及时请求支援的。

福建广播电视大学党政办公室　　2018 年 9 月 24 日印发