**中国轻工业信息中心**

**网络和信息安全突发事件应急处置规程**

一、网站出现非法信息的应急处置规程

（一）发现网站出现非法信息时，网站内容管理部门应及时向信息中心相关领导报备，并立即采取必要技术手段,对相关信息做屏蔽、删除等处理措施，防止非法信息扩散。

（二）网络服务处和出现问题的网站管理部门应协同追查非法信息来源，并确定相关责任人。

（三）网络服务处在查清事件发生原因的基础上，及时总结经验教训，提出强化安全防范的措施，以书面形式报告中心信息安全领导小组。

（四）领导小组根据书面报告，决定是否追究相关责任人责任等事宜。

二、黑客攻击的紧急处置规程

（一）发现网页内容被篡改，或通过入侵检测手段等发现有黑客正在进行攻击时,应立即向网络服务处报告。

（二）网络服务处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，同时向中心信息安全领导小组报备。

（三）恢复或重建被破坏的系统。

（四）追查黑客攻击来源。

（五）情况严重时，召开信息安全领导小组会议；经会议批准，可向公安部门报警。

（六）总结经验教训，对事故点进行相应的安全加固,并采取有效的防范措施。

三、病毒防治应急处置规程

（一）当计算机使用人员发现其计算机被感染上病毒后，若无法清除该病毒，应第一时间将计算机从网络上物理断开。

（二）向网络服务处报告，确定病毒的性质和危害，对病毒进行进一步查杀。

（三）若该病毒已经在局域网内扩散，并严重影响日常办公及网络安全，应立即向信息安全领导小组报告。

（四）信息安全领导小组根据报告，确定具体的处置方式，保证网络畅通和计算机安全。

（五）总结经验教训，采取有效的防范措施。

四、软件系统异常应急处置规程

（一）发现系统软件和应用软件响应异常时，软件应用部门应立即向网络服务处报告。

（二）网络服务处对系统软件和应用软件进行检查，根据具体情况决定最终将采取停用、修复等何种应对手段,并向中心信息安全领导小组报备。

（三）网络服务处配合软件应用部门,通过检查访问各类日志记录等资料，确认分析异常原因。

（四）情况严重的，召开信息安全领导小组会议。

（五）总结经验教训，采取有效的防范措施。

五、广域网外部线路中断应急处置规程

（一）广域网线路若中断后，应立即向中心信息安全领导小组报备。

（二）网络服务处应迅速判断故障节点，查明故障原因。

（三）如属信息中心内部管辖范围，由系统管理员立即予以恢复；如遇无法恢复情况，立即向有关厂商请求支援；如属通信部门管辖范围，立即与通信维护部门联系，请求及时修复。

（四）总结经验教训，采取有效的防范措施。

六、局域网中断应急处置规程

（一）局域网中断后，网络服务处应判断故障节点，查明故障原因，并向中心信息安全领导小组报备。

（二）如属线路故障，应立即抢修线路；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；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，向相关厂方技术专家请求支援。

（五）总结经验教训，采取有效的防范措施。

七、设备故障应急处置规程

（一）发现服务器等关键设备损坏后，应立即开展设备故障排查原因，并向网络服务处负责人报告。

（二）网络服务处指定系统管理员并向中心信息安全领导小组汇报情况。

（三）如果能够自行恢复，应立即用备件替换受损部件；如果不能自行恢复的，立即与设备提供商联系，请求相关技术人员现场解决。

（四）如果设备一时不能修复，应向领导小组再汇报，视具体情况决定是否启动应急预案。

（五）总结经验教训，采取有效的防范措施。

八、机房着火应急处置规程

（一）一旦机房发生火灾，应遵照下列原则：首先保证人员安全；其次保证关键设备和数据安全；三是保证一般设备安全。

（二）人员疏散程序：机房值班人员立即按响火警警报，并通过119电话向消防部门请求支援，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。

（三）灭火程序：规范化的机房启动气体灭火系统进行灭火。

（四）灭火后，迅速组织抢修受损的基础设施，减少损失，尽快恢复正常工作并向中心信息安全领导小组汇报。

（五）总结经验教训，采取有效的防范措施。

九、电力中断应急处置规程

（一）发生电力中断，应立即向中心信息安全领导小组报备。

（二）属内部电力线路故障的，网络服务处应迅速组织力量恢复电力；属供电局供电故障的，应立即与供电局联系，请供电局迅速恢复供电。

（四）如供电局告知需长时间停电，预计停电三小时以上，应由UPS供电，视情况关闭一些服务器等设备，涉及业务中断的，通知相关业务部门；如区域内全部停电，则关掉所有关键设备，暂停一切业务。

（五）电力恢复后，网络服务处应重新启动设备，恢复业务运行。