吉林建筑大学文件

校字〔2021〕205号　　签发人：陈　雷

关于印发《吉林建筑大学网络信息中心应急处置预案》的通知

学校各部门、单位：

为切实加强我校网络安全保障，有效防范蓄意攻击破坏信息系统及传播、粘贴非法信息等突发事件的发生，根据我校系统网络和信息系统建设及应用的现状，特制定本预案。请各单位认真执行。

吉林建筑大学

2021年12月9日

吉林建筑大学网络信息中心应急处置预案

一、网站不良信息处置预案

1. 网络信息中心工作人员随时监视网站信息内容，同时接收各方面信息举报和反馈。

2. 发现网上出现非法信息时，工作人员立即禁止该信息内容的访问，并联系相关网站负责人员进行核实，删除或修改非法内容后再开放访问权限。

3. 如发现重大舆情问题，应立即保留证据并上报部门领导和网络安全领导小组。

4. 工作人员应尽量追查非法信息来源，并妥善保存有关记录及日志，以备整理汇报。

二、网络恶意攻击处置预案

1. 当工作人员发现网页内容被篡改，或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从网络中隔离出来，保护现场，同时尽快开展恢复与重建工作。

2. 追查攻击来源或系统漏洞，核实之后尽快修补后门或漏洞，并把攻击来源 IP 加入防护软件黑名单。

3. 如情况较为严重时，应立即向部门领导和吉林建筑大学网络安全与信息化领导小组汇报，并向公安部门报警。

三、感染病毒处置预案

1. 当发现网络信息中心自管数据中心服务器感染病毒后，

应立即将其从网络上隔离出来。

2．尽快对服务器的重要数据进行备份。

3．通知服务器使用部门启用杀毒软件进行全面杀毒处理，同时对其他机器进行病毒扫描和检测。

4．如果无法处理病毒，应作好相关记录，同时立即向部门领导和吉林建筑大学网络安全与信息化领导小组汇报。

5.如果感染病毒的关键服务器设备，应尽快修复处理，无法立即解决时，应更换替代设备，尽力保证网络和服务正常运行。

四、网络中断处置预案

1．第一时间判断是广域网还是局域网故障。

2．若为局域网网络故障，应立即判断故障节点，查明故障原因。如属线路故障，应重新安装或维修线路；如属路由器、交换机、防火墙等设备故障，应立即更换相关设备，并与厂商联系维修或更换问题设备;如属设备配置文件破坏,应迅速重新配置，并调试畅通。如遇无法解决的技术问题，应立即向有关厂商或专业机构请求支援。

3．若为广域网故障，应迅速判断故障节点，查明故障原因，并向适当切换为四家运营商其他线路,以保证全校师生的正常网络访问。如不能马上解决的问题，应及时向部门领导和吉林建筑大学网络安全领导小组汇报，同时立即与供应商技术部门联系，请求修复。

4．故障解决之后，把具体情况整理汇总上报网络安全领导小组。

五、设备安全处置预案

1. 发现关键设备损坏后，工作人员应立即查明原因。

2. 若能够自行恢复，应立即用备件替换受损部件。若不能自行恢复，应立即与设备供应商联系，维修或更换。

3. 若设备不能短时间内修复，应向部门领导和网络安全与信息化领导小组汇报，并告知各相关单位，暂缓使用。

吉林建筑大学党政办公室　　2021 年 12 月 9 日印发