

上海电力学院网络与信息安全应急处置预案

为了切实做好网络与信息安全突发事件的防范和应急处理工作，进一步提高我校预防和控制网络与信息安全突发事件的能力和水平，减轻或消除突发事件的危害和影响，保证校园网络的正常运行，结合本校实际，制定本预案。

一、应急处置工作的目标

在最短时限内，及时、果断处理在本校范围内发生的危害网络与信息安全的突发性事件，维护校园网络信息安全与稳定。

二、应急预案启动

有下列情况应启动应急预案：

1. 网站、网页出现非法言论。
2. 网络遭受黑客攻击。
3. 计算机网络出现病毒。
4. 软件系统遭受破坏性攻击。
5. 数据库系统出现故障。
6. 广域网外部线路中断。
7. 局域网大范围中断。
8. 服务器等关键网络设备故障。
9. 网络中心机房外电中断。

三、组织领导

成立网络与信息安全领导小组，领导小组的主要职责与任务是统一领导全校网络与信息安全的应急工作，全面负责学校网络与信息安全可能出现的各种突发事件处置工作，协调解决灾害处置工作中的重大问题等。下设网络与信息安全应急处置工作组，由现代教育技术中心、宣传部、保卫处、学生处、教务处、综合管理处等部门成员组成，具体负责学校网络与信息安全应急处置工作。

四、应急预案启动时的应急处理措施

1. 网站、网页出现非法言论时的紧急处置措施

- (1) 网站、网页由各相关使用部门的具体负责人员随时密切监视信息内容。每天不少于5次；非常时期，每半小时监控一次，必要时，24小时监控。
- (2) 发现网上出现非法信息时，负责人员应立即向应急处置工作组通报情况；情况紧急的应先及时采取删除等处理措施，再按程序报告。
- (3) 应急处置工作组人员应在接到通知后十分钟内进行处理，作好必要的记录，清理网站上的非法信息，强化安全防范措施后方可将网站网页重新投入使

用。

- (4) 应急处置人员应妥善保存有关记录及日志或审计记录。
- (5) 应急处置人员应立即追查非法信息来源，若非法信息来源于校内，则由本院保卫处和网络技术人员进行处理，同时报告校网络与信息安全领导小组负责人，根据管理制度对非法传播者及时处置，并报知上级公安部门备案；若非法信息来自于校外，则立即报知上报公安部门，并由技术人员将这些信息保存、记录 IP 地址，以备上级公安部门互联网突发事件处置行动组调用。

2. 黑客攻击时的紧急处置措施

- (1) 当有关负责人员发现网页内容被篡改，或通过防火墙、入侵检测系统发现有黑客正在进行攻击时，应立即向应急处置工作组通报情况。
- (2) 应急处置人员应在十分钟内进行处理，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，同时向网络与信息安全领导小组汇报情况。
- (3) 应急处置人员负责被破坏系统的恢复与重建工作，修补漏洞、强化安全措施后方可将被攻击的服务器设备接入网络。
- (4) 应急处置人员追查非法信息来源。
- (5) 网络与信息安全领导小组会商后，如认为情况严重，则立即向上海市教委和公安部门汇报。

3. 计算机网络病毒安全紧急处置措施

- (1) 当发现网络上出现病毒，并影响网络的正常运行后，应立即找出感染病毒机器。
- (2) 将感染病毒机器和网络隔离，待病毒彻底清除后方允许再次接入网络。
- (3) 网络中心技术人员要针对该款病毒进行研究，做好相应的病毒发作特征及解决方案。

4. 软件系统遭受破坏性攻击的紧急处置措施

- (1) 重要的软件系统平时必须存有备份，与软件系统相对应的数据必须有多日备份，并将它们保存于安全处。
- (2) 一旦软件遭到破坏性攻击，应立即停止软件系统。
- (3) 网络管理人员负责软件系统和数据的恢复。
- (4) 网络管理人员检查日志等资料，确认攻击来源。
- (5) 安全领导小组认为情况极为严重的，应立即向上海市教委和公安部门报告。

5. 数据库安全紧急处置措施

- (1) 各数据库系统要至少准备两个以上数据库备份，平时一份放在机房，另一份放在另一安全的建筑物中。
- (2) 一旦数据库崩溃，应急处置组人员应对主机系统进行维修，如遇无法解决的问

题，立即向上级单位或软硬件提供商请求支援。

- (3) 系统修复启动后，将第一个数据库备份取出，按照要求将其恢复到主机系统中。
- (4) 如因第一个备份损坏，导致数据库无法恢复，则应取出第二套数据库备份加以恢复。
- (5) 如果两个备份均无法恢复，应立即向有关厂商请求紧急支援，并向网络与信息安全领导小组汇报。

6. 广域网外部线路中断紧急处置措施

- (1) 广域网线路中断后，网络管理员接到报告后，应迅速判断故障节点，查明故障原因。
- (2) 如属我校管辖范围，由网络管理员予以恢复。如遇无法恢复情况，立即向有关厂商请求支援。
- (3) 如属电信部门管辖范围，立即与电信维护部门联系，请求修复。

7. 局域网大范围中断紧急处置措施

- (1) 局域网出现大范围中断现象后，网络管理员应立即判断故障节点，查明故障原因。
- (2) 如属线路故障，应重新安装线路。
- (3) 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。
- (4) 如属路由器、交换机等网络设备故障，应立即调换备机，如无备机，立即向设备提供商联系更换设备，并调试畅通；并向网络与信息安全领导小组领导汇报。

8. 服务器等关键网络设备故障安全紧急处置措施

- (1) 服务器等关键设备损坏后，网络管理人员应立即查明原因。
- (2) 如果能够自行恢复，应立即用备件替换受损部件。
- (3) 如果不能自行恢复的，立即与设备提供商联系，请求派维修人员前来维修。
- (4) 如果设备一时不能修复，应向网络与信息安全领导小组汇报。

9. 网络中心机房外电中断后的处置措施

- (1) 外电中断后，机房会自动切换到备用电源。
- (2) 检查断电原因，如因内部线路故障，请综合管理处协助迅速恢复。
- (3) 如果是供电局的原因，应立即与供电局联系，请供电局迅速恢复供电。
- (4) 如果供电局告知需长时间停电，应做如下安排：
 - a) 预计停电 1 小时以内，由 UPS 供电。
 - b) 预计停电 1-3 小时，关掉非关键设备，确保各主机、路由器、交换机供电。
 - c) 预计停电超过 3 小时，关掉非关键设备，确保各主机、路由器、交换机

供电。UPS 使用 4 小时后，关闭所有的设备。

五、保障措施

网络与信息安全的防治工作是一项长期的、持续的、跟踪式的、深层次的和各阶段相互联系的工作，是有组织的科学与社会行为，而不是随着每次灾害的发生而开始和结束的活动。因此，必须做好应急保障工作。

1. 人员保障

重视网络管理人员队伍的建设与保障，确保在灾害发生前的人员值班，灾害处置过程和灾后重建中的人员在岗与战斗力。

2. 技术保障

重视网络信息技术的建设和升级换代，在灾害发生前确保网络信息系统的安全与稳定，灾害处置过程中和灾后重建中的相关技术支撑。

3. 物资保障

网络与信息安全应急处置工作组，报请学校领导小组批准后，根据学院财力情况及网络管理的实际需要，适当购入一些网络与信息安全保障设备。

4. 训练和演练

加强全校网络信息用户的防灾、减灾知识的宣传普及，增强这些用户的防灾意识和自救互救能力。有针对性地开展应急抢险救灾演练，确保发生灾害时的应急救助手段及时到位和有效。

上海电力学院现代教育技术中心

2012 年 10 月

附件一：网络与信息安全领导小组成员

组 长：周光耀、李和兴

副组长：石奇光、李国荣、张浩

组 员：王飞、毛静涛、魏国强、施启胜、李家珉、石笑寒、龙根勇、魏建华
王耀廷、王秋侠、陆玮、陈发堂、赵玲、涂和平、韦钢、唐忠、李永光、
解群、王国华、江晓花、周洁明、苏少华、欧阳元煌、徐广新、王轩、
江广华、马进明、张仙智、潘耀芳、周慧杰、何西培、谈蓓月、于善安、
刘莉

附件二：网络与信息安全应急处置工作组成员

组 长：魏国强

副组长：何光营

组 员：程娟、王菲、王旭、秦劲松、杨辉、赵建明、何鹏飞、程斌
杨锦程、刘裕、羌亮