为妥善应对和处置档案馆计算机档案信息网络突发事件，营造健康向上的网络环境，根据《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络国际联网安全保护管理办法》等有关法规文件精神，结合档案馆实际情况，特制定本应急方案。

一、指导思想

以维护正常的档案工作和营造绿色健康的网络环境为中心，按照“预防为主，积极处置”的原则，进一步完善档案馆计算机档案信息网络管理机制，提高突发事件的应急处置能力。

二、组织领导

成立计算机档案信息网络系统安全保护工作领导小组

三、日常工作中注意防范的事项：

1、主要检查项目：

（1）内网计算机与外网物理隔离，杜绝非法外联；

（2）涉密计算机与外网隔离；

（3）严禁将非涉秘的计算机用于涉密业务工作。

2、安装正版防病毒软件，启动实时监控；定期升级病毒库并查杀病毒。

3、定期升级操作系统，安装系统补丁。

4、定期备份重要文档。

5、设置 8 位以上用户密码，定期更换密码。

6、建立健全重要数据及时备份和突发情况下数据恢复机制。

7、访问：国家计算机网络应急技术处理协调中心 http://www.cert.org.cn/index.shtml，及时了解计算机网络安全动态。

8、注意事项：

（1）不要随意登陆不明网站；

（2）下载软件程序要在正规网站；

（3）对 MSN 、QQ 发来的链接谨慎点击；

（4）不要打开不明邮件；

（5）重要信息要进行物理隔离；

（7）取消 LAN 不必要的链接；

（8）关闭不必要端口；禁用邮件匿名转发、信使服务等功能。

四、发现异常情况，遵循以下步骤：

第 1 步：立刻断开网络（内、外网）。切断计算机与网络的物理连接，拔掉计算机网线；

第 2 步：查杀病毒。对系统进行一次全面的病毒查杀，消除系统和网络中存在的木马程序和病毒；

第 3 步：升级系统。在其它能正常使用的计算机上，下载操作系统的补丁及升级包，用 U 盘复制到出现故障的计算机上，升级操作系统，安装系统补丁；

第 4 步：升级病毒库，在其它能正常使用的计算机上，下载最新病毒库，用 U 盘复制到出现故障的计算机上，更新病毒库后，再次查杀病毒；

第 5 步：更换用户、系统口令和密码；

第 6 步：联系现代教育中心人员检查、排除其它故障；

第 7 步：做好有关现场处置工作；

第 8 步：如发生重大计算机网络受破坏和攻击事件，及时断网并报告现代教育中心。