# 如何写网络安全心得体会学习网络安全心得(精)

来源：网络 作者：紫云轻舞 更新时间：2024-06-25

*如何写网络安全心得体会学习网络安全心得(精)一我局加强组织领导，强化宣传教育，落实工作责任，加强日常监督检查，将涉密计算机管理抓在手上。对于计算机磁介质（软盘、u盘、移动硬盘等）的管理，采取专人保管、涉密文件单独存放，严禁携带存在涉密内容的...*

**如何写网络安全心得体会学习网络安全心得(精)一**

我局加强组织领导，强化宣传教育，落实工作责任，加强日常监督检查，将涉密计算机管理抓在手上。对于计算机磁介质（软盘、u盘、移动硬盘等）的管理，采取专人保管、涉密文件单独存放，严禁携带存在涉密内容的磁介质到上网的计算机上加工、贮存、传递处理文件，形成了良好的安全保密环境。对涉密计算机（含笔记本电脑）实行了内、外网物理隔离，并按照有关规定落实了保密措施，到目前为止，未发生一起计算机失密、泄密事故；其他非涉密计算机（含笔记本电脑）及网络使用，也严格按照局计算机保密信息系统管理办法落实了有关措施，确保了机关信息安全。

一是网络安全方面。我局严格计算机内、外网分离制度，全局仅有几个科室因工作需要保留外网，其余计算机职能上内网，对于能够上外网的计算机实行专人专管和上网登记制度，并且坚决杜绝计算机磁介质内网外混用的做法，明确了网络安全责任，强化了网络安全工作。

二是日常管理方面切实抓好外网、网站和应用软件“五层管理”，确保“涉密计算机不上网，上网计算机不涉密”，严格按照保密要求处理光盘、硬盘、u盘、移动硬盘等管理、维修和销毁工作。重点抓好“三大安全”排查：一是硬件安全，包括防雷、防火、防盗和电源连接等；二是网络安全，包括网络结构、安全日志管理、密码管理、ip管理、互联网行为管理等；

三是应用安全，包括网站、邮件系统、资源库管理、软件管理等。

我局每台终端机都安装了防病毒软件，系统相关设备的应用一直采取规范化管理，硬件设备的使用符合国家相关产品质量安全规定，单位硬件的运行环境符合要求，打印机配件、色带架等基本使用设备原装产品；防雷地线正常，对于有问题的防雷插座已进行更换，防雷设备运行基本稳定，没有出现过雷击事故。网站系统安全有效，暂未出现任何安全隐患。我局网络系统的组成结构及其配置合理，并符合有关的安全规定；网络使用的各种硬件设备、软件和网络接口也是通过安全检验、鉴定合格后才投入使用的，自安装以来运转基本正常。

我局对电脑及其设备实行“谁使用、谁管理、谁负责”的管理制度。在管理方面我们一是坚持“制度管人”。二是强化信息安全教育，就网络安全及系统安全的有关知识进行了培训，提高员工计算机技能。同时在全局开展网络安全知识宣传，使全体人员意识到了，计算机安全保护是“三防一保”工作的有机组成部分。而且在新形势下，计算机犯罪还将成为安全保卫工作的重要内容。在设备维护方面，专门设置了网络设备故障登记簿、计算机维护及维修表对于设备故障和维护情况属实登记，并及时处理。对外来维护人员，要求有相关人员陪同，并对其身份和处理情况进行登记，规范设备的维护和管理。

为确保计算机网络安全、实行了网络专管员制度、计算机安全保密制度、网站安全管理制度、网络信息安全突发事件应急预案等以有效提高管理员的工作效率。同时我局结合自身情况制定计算机系统安全自查工作制度，做到四个确保：一是系统管理员于每周五定期检查中心计算机系统，确保无隐患问题；二是制作安全检查工作记录，确保工作落实；三是实行领导定期询问制度，由系统管理员汇报计算机使用情况，确保情况随时掌握；四是定期组织全局人员学习有关网络知识，提高计算机使用水平，确保预防。

我们在自查过程中发现了一些管理方面存在的薄弱环节，今后我们还要在以下几个方面进行改进。

（一）对于线路不整齐、暴露的，立即对线路进行限期整改，并做好防鼠、防火安全工作。

（二）自查中发现个别人员网络和信息安全意识不强。在以后的工作中，我们将继续加强网络和信息安全教育和防范技能训练，让干部职工充分认识到网络和信息安全的重要性。人防与技防结合，确实做好单位的网络安全工作。

**如何写网络安全心得体会学习网络安全心得(精)二**

为了加强我校教育信息网络安全管理，保护信息系统的安全，促进我校信息技术的应用和发展，保障教育教学和管理工作的顺利进行，并配合省公安厅、省教育厅(豫公通[20xx]220号文件精神，对我校计算机信息系统开展以“反黑客、反破坏、扫黄打非、清理垃圾邮件”为主要内容的安全大检查，净化校园网络环境，不断提高学校计算机信息系统安全防范能力，从而为学生提供健康，安全的上网环境。

一、领导重视，责任分明，加强领导

为了认真做好迎检准备工作，进一步提高教育网络信息安全工作水平，促进教育信息化健康发展，我校建立了专门的网络信息安全管理组织，成立了由分管领导、网络管理员组成的计算机网络信息安全管理领导小组。负责制定学校计算机信息系统安全管理的办法和规定，协调处理全校有关计算机信息系统安全的重大问题;负责学校计算机信息系统的建设、管理、应用等工作;负责信息系统安全的监督、事故的调查和处罚。学校网络管理人员要在学校计算机安全管理领导小组的领导下，负责校园网的安全保护工作和设备的维护工作，必须模范遵守安全管理制度，积极采取必要的防范技术措施，预防网络安全事故的发生。

二、完善制度，加强管理

为了更好的安全管理网络，我校建立了健全的安全管理制度：

(一)计算机机房安全管理制度

1、重视安全工作的思想教育，防患于未然。

2、遵守“教学仪器设备和实验室管理办法”，做好安全保卫工作。

3、凡进入机房的人员除须遵守校规校纪外，还必须遵守机房的各项管理规定，爱护机房内的所有财产，爱护仪器设备，未经管理人员许可不得随意使用，更不得损坏，如发现人为损坏将视情节按有关规定严肃处理。

4、机房内禁止吸烟，严禁明火。

5、工作人员必须熟悉实验室用电线路、仪器设备性能及安全工作的有关规定。

6、实验室使用的用电线路必须符合安全要求，定期检查、检修。

7、杜绝黄色、迷信、反动软件，严禁登录黄色、迷信、反动网站，做好计算机病毒的防范工作。

8、工作人员须随时监测机器和网络状况，确保计算机和网络安全运转。

9、机房开放结束时，工作人员必须要关妥门窗，认真检查并切断每一台微机的电源和所有电器的电源，然后切断电源总开关。

(二)操作人员权限等级分配制度

1、校领导统一确定操作人员职能权限。

2、电教组成员负责管理、维修学校所有计算机，出现重大事故应及时报上级领导。

3、教师用户帐号、密码由网络管理员发放，并统一管理。

4、学校计算机管理人员需定期维护计算机软件和数据，重要信息定期进行检查和备份。

5、网络管理员负责校园用户计算机系统能够正常上网，为用户提供日常网络维护服务和日常数据备份。

(三)账号安全保密制度

1、网络用户的账号、密码不得外传、外借。

2、非法用户使用合法用户的账号进入校园网的，追究该帐号拥有者的安全责任。

(四)计算机病毒防治制度

1、学校购买使用公安部颁布批准的电脑杀毒产品。

2、未经许可证，任何人不得携入软件使用，防止病毒传染。

3、凡需引入使用的软件，均须首先防止病毒传染。

4、电脑出现病毒，操作人员不能杀除的，须及时报电脑主管处理。

5、在各种杀毒办法无效后，须重新对电脑格式化，装入正规渠道获得的无毒系统软件。

6、建立双备份制度，对重要资料除在电脑贮存外，还应拷贝到软盘上，以防遭病毒破坏而遗失。

7、及时关注电脑界病毒防治情况和提示，根据要求调节电脑参数，避免电脑病毒侵袭。

(五)安全教育培训制度

1、学校组织教师认真学习《计算机信息网络国际互联网安全保护管理办法》,提高教师的维护网络安全的警惕性和自觉性。

2、学校负责对本校教师进行安全教育和培训，使教师自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，使他们具备基本的网络安全知识。

3、校管理中心对信息源接入的骨干人员进行安全教育和培训，使之自觉遵守和维护《计算机信息网络国际互联安全保护管理办法》，杜绝发布违犯《计算机信息网络国际互联网安全保护管理办法》的信息内容。

(六)、事故和案件及时报告制度

1、任何单位和个人不得利用互联网制作、复制、查阅和传播下列信息：

煽动抗拒、破坏宪法和法律、行政法规实施。

煽动颠覆国家政权，推翻社会主义制度。

煽动分裂国家、破坏国家统一。

煽动民族仇恨、民族歧视、破坏民族团结。

捏造或者歪曲事实、散布谣言，扰乱社会秩序。

宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪。

公然侮辱他人或者捏造事实诽谤他人。

损害国家机关信誉。

其他违反宪法和法律、行政法规。

如发现有上述行为，保留有关原始记录，并填写好《安全日志》，在12小时内向上级报告。

2、接受并配合区电教中心和公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

3、发现有关计算机病毒、危害国家安全、违反国家有关法律、法规等计算机安全案情的，应在12小时以内向上级报告。

4、计算机机房设管理员一名，其职责是每天不定期浏览主页或自己页面，负责领导还应经常巡视操作者，如发现有违反上述规定者应立即制止并报告校园网安全领导小组。

(七)、面对大面积病毒应急处理方案

1、制定计算机病毒防治管理制度和技术规程，并检查执行情况;

2、培训计算机病毒防治管理人员;

3、采取计算机病毒安全技术防治措施;

4、对网站计算机信息系统应用和使用人员进行计算机病毒防治教育和培训;

5、及时检测、清除计算机系统中的计算机病毒，并做好检测、清除的记录;

6、购置和使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品;

7、向公安机关报告发现的计算机病毒，并协助公安机关追查计算机病毒的来源;

8、对因计算机病毒引起的计算机信息系统瘫痪、程序和数据严重破坏等重大事故及时向公安机关报告，并保护现场。

除以上健全的安全管理制度外，我校也认真落实相关安全技术措施，安全基础措施良好拥有完善的安全保护措施，设有学校重要部位值班制度，做到昼夜值班，任何人不得擅自进入微机房。

本文档由站牛网zhann.net收集整理，更多优质范文文档请移步zhann.net站内查找