# 网络信息安全工作总结2024 网络安全个人工作总结5篇

来源：网络 作者：空谷幽兰 更新时间：2024-06-11

*当工作进行到一段时间后，回顾自己过往的工作，认真反思，并做一个工作总结，积累更多的工作经验，不断改进工作方法，在今后更好地开展工作。下面小编在这里为大家精心整理了几篇，希望对同学们有所帮助，仅供参考。青少年的健康成长，关系到社会的稳定，关系...*

当工作进行到一段时间后，回顾自己过往的工作，认真反思，并做一个工作总结，积累更多的工作经验，不断改进工作方法，在今后更好地开展工作。下面小编在这里为大家精心整理了几篇，希望对同学们有所帮助，仅供参考。

青少年的健康成长，关系到社会的稳定，关系到民族的兴旺和国家的前途。因此，教育和保护好下一代，具有十分重要的意义。中学阶段是一个人成长的重要时期，中学教育尤其是中学生安全教育的成败直接关系到一个人将来是否成为人才。

随着信息时代的到来，形形色色的网吧如雨后春笋般在各个城镇应运而生。它们中有一些是正规挂牌网吧，但多数是一些无牌的地下黑色网吧，这些黑色网吧瞄准的市场就是青少年学生。一些学生迷上网络游戏后，便欺骗家长和老师，设法筹资，利用一切可利用的时间上网。

有许许多多原先是优秀的学生，因误入黑色网吧，整日沉迷于虚幻世界之中，学习之类则抛之脑后，并且身体健康状况日下。黑色网吧不仅有学生几天几夜也打不“出关”的游戏，更有不健康、不宜中学生观看的\_网页。

抓好中学生的网络安全教育与管理，保障中学生的人身财产安全，促进中学生身心健康发展，是摆在我们面前的一个突出课题。

针对这种情况，一是要与学生家长配合管好自己的学生，二是向有关执法部门反映，端掉这些黑色网吧，三是加强网络法律法规宣传教育，提高中学生网络安全意识，在思想上形成一道能抵御外来反动、\_侵蚀的“防火墙”。四是组织学生积极参与学校的安全管理工作，让中学生参与学校的安全管理工作是提高中学生安全防范意识的有效途径。最后，争取相关部门协作，整治校园周边环境，优化育人环境。

学校在加大对校园安全保卫力量的投入、提高保卫人员素质和学校安全教育水平的同时，要积极争取地方政府、公安机关的支持，严厉打击危害学校及中学生安全的不法行为，切实改善校园周边治安状况，优化育人环境。对校门口的一些摊点，校园附近的一些黑色网吧，对中学生存有安全隐患的一切问题，该取缔的取缔，该打击的打击，该解决的尽快解决。

对校内发生的治安事件或安全事故，要依法处理，及时通报。对违反安全规章的学生应予以批评教育，甚至必要的纪律处分，对已发现的安全隐患及时采取有效的防范措施，以此创造一个安全、文明的育人环境，为提高教育教学质量和我国教育事业的发展做出新的贡献。

综上所述，对中学生进行安全教育是一项系统工程，在外部，需要社会、学校、家庭紧密配合;在内部，需要学校的各个部门通力合作、齐抓共管，组织学生积极参与，这样才能达到对中学生进行安全教育的目的。

为进一步加强政府信息\_\_，根据政府办[20\_\_]10号文件精神，我会严格按照文件要求，结合妇联实际，及时查找问题，采取有效措施，政府信息安全\_\_取得实效。

一、 领导重视、责任落实

信息\_\_是维护国家和单位安全和利益的工作，做好信息\_\_是我们的基本职责。我会领导十分重视\_\_，我会成立了信息安全\_\_领导小组，设立办公室，安排专人承办日常工作。领导班子在做好保密带头作用的同时，时时开展保密法规、政策宣传，不定期对单位信息\_\_执行情况进行检查、指导，督促信息\_\_的落实，推进了信息\_\_纵深发展。

二、加强学习、增强认识

今年我会组织各科室学习了《中华人民共和国保守国家秘密法》、《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管理暂行规定》、《中华人民共和国信息公开条例》等保密法律法规，对全体工作人员进行保密教育，提升了职工对\_\_重要性和严肃性的认识，增强了全体干部职工的保密意识。为加强对\_\_的领导，切实落实l\_\_责任制，保守党和国家秘密，我会及时制定了《\_\_制度》、《网站信息报送制度》、《计算机网络管理制度》、《网络管理员工作职责》等制度，对计算机上网安全保密、涉密存储介质保密、计算机维修维护、用户密码安全保密、笔记本电脑安全保密、涉密电子文件保密、涉密计算机系统病毒防治、上网发布信息保密、上网信息涉密审查等各方面都作了详细规定，进一步规范了我会网络与信息安全管理工作。做到涉密信息不上网，上网信息不涉密。

三、严格管理、措施到位

我会涉密工作不多，但领导却很重视\_\_的管理。在各涉密工作中，始终坚持以领导审签制度为原则，采取专人管理和纵向传递，严格做好收文、发文、传阅、销毁等登记管理，专人传递，定人阅办的工作方法，减少了保密信息的流通环节和知晓范围，保证涉密资料在工作中的严肃性和密级性。对于涉密计算机仍然采取专机、专人管理，采用与因特网脱离的裸机工作方式运作，并设置了必要的身份认证，配置了泄密干扰器等措施加强防范。在保密资料制作、存储、传输过程中加载密码设置等措施，有效防范了网络泄密、失密事件。在政府信息公开工作方面，我会成立了信息公开审查领导小组，建立了政府信息公开审查制度，对信息公开进行严格审签，保障了政府信息公开无泄密发生。

四、网络安全存在的不足及整改措施

目前，我会网络安全仍然存在以下几点不足：一是安全防范意识较为薄弱;二是病毒监控能力有待提高;三是如遇到恶意攻击、计算机病毒侵袭等突发事件，可能会导致处理不够及时。

针对目前我会网络安全方面存在的不足，提出以下几点整改办法：

1、加强我会全员计算机操作技术、网络安全技术方面的培训，强化我会计算机操作人员对网络病毒、信息安全的防范意识;

2、加强我会信息及网管人员在计算机技术、网络技术方面的学习，不断提高我会计算机专管人员的技术水平。

3、合理规划及配置相关软硬件系统，保障计算机网络及信息的安全。

网络，在现代社会已经变得十分普遍了，我们随处可以看见使用网络的人，老年人、小孩子、中年人人们使用网络看电影、炒股、浏览新闻、办公等等网络的出现给人们带来了一个崭新的面貌! 有了网络，人们办公更加高效，更加环保，减少了纸张的使用。正好符合了我们当前的环保主题——低碳、节能、减排。并且，现在有很多高校都开设了计算机专业，专门培养这方面的高端人才，但也许，在培养专业的技能之时忽略了对他们的思想政治教育，在他们有能力步入社会的时候，他们利用专业的优势非法攻克了别人的网站成了黑客走上了一条再也回不了头的道路!

确实是，网络不同于我们的现实生活，它虚拟、空泛、看得见却摸不着，而我们的现实生活，给人感觉真实。在我们的现实生活中，我们的活动有着一定的条例、法规规定，在网络世界中，虽然是虚拟的，但是它也有它的制度、法律法规。

在这里，我简单罗列些一些关于网络中的法律法规：早在1991年，国务院就发布了《计算机软件保护条例》，其中第三十条(五)未经软件著作权人或者其合法受让者的同意修改、翻译、注释其软件作品; (六)未经软件著作权人或者其合法受让者的同意复制或者部分复制其软件作品; 在94年又相继出了一系列法律法规条例(一)违反计算机信息系统安全等级保护制度，危害计算机信息系统安全的; (二)违反计算机信息系统国际联网备案制度的; (三)不按照规定时间报告计算机信息系统中发生的案件的; (四)接到公安机关要求改进安全状况的通知后，在限期内拒不改进的; (五)有危害计算机信息系统安全的其他行为的。直到97年，公安部再一次完善了我国关于网络安全的法律法规，明确规定违反法律、行政法规的，公安机关会给予警告，有违法所得的，没收违法所得，对个人可以处罚五千元以下的罚款，对单位处以一万五千元以下的罚款;情节严重的，可以给予六个月以内停止联网、停机整顿的处罚，必要时可以建议原发证、审批机构吊销经营许可证或者取消联网资格;构成违反治安管理行为的，依照治安管理处罚条例的规定处罚;构成犯罪的，依法追究刑事责任。

所以在网络世界中，违法了也一定会追究责任。这和我们的现实生活一样，并不像我们想的，因为网络世界是虚拟的，所以可以乱说，在上面乱整。传播色情、不利于社会安定的话，也一定会受到处罚，对于那些为了利益利用自己高超的技术手段攻破别人的电脑系统，这肯定是违法的，我们在现实生活中也经常看到这样的案例，应该说这些事例给了我们血淋淋的教训，所以，我们在使用网络的时候一定要遵守法律法规，不搞破坏，在网络上进行正常的健康的交流，充分使用网络资源提高我们的学习效率和知识面!

我局对网络信息安全系统工作一直十分重视，成立了专门的领导组，建立健全了网络安全保密责任制和有关规章制度，由局信息中心统一管理，各科室负责各自的网络信息安全工作。严格落实有关网络信息安全保密方面的各项规定，采取了多种措施防范安全保密有关事件的发生，总体上看，我局网络信息安全\_\_做得比较扎实，效果也比较好，近年来未发现失泄密问题。

一、计算机涉密信息管理情况

今年以来，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)实行了与国际互联网及其他公共信息网物理隔离，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。

二、计算机和网络安全情况

一是网络安全方面。我局配备了防病毒软件、网络隔离卡，采用了强口令密码、数据库存储备份、移动存储设备管理、数据加密等安全防护措施，明确了网络安全责任，强化了网络安全工作。

二是信息系统安全方面实行领导审查签字制度。凡上传网站的信息，须经有关领导审查签字后方可上传;二是开展经常性安全检查，主要对SQL注入攻击、跨站脚本攻击、弱口令、操作系统补丁安装、应用程序补丁安装、防病毒软件安装与升级、木马病毒检测、端口开放情况、系统管理权限开放情况、访问权限开放情况、网页篡改情况等进行监管，认真做好系统安全日记。

三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。

三、硬件设备使用合理，软件设置规范，设备运行状况良好。

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，没有出现雷击事故;UPS运转正常。网站系统安全有效，暂未出现任何安全隐患。

四、通讯设备运转正常

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。

五、严格管理、规范设备维护

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、提高员工计算机技能。同时在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。

六、网站安全及

我局对网站安全方面有相关要求，一是使用专属权限密码锁登陆后台;二是上传文件提前进行病素检测;三是网站分模块分权限进行维护，定期进后台清理垃圾文件;四是网站更新专人负责。

七、安全制度制定落实情况

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。

八、安全教育

为保证我局网络安全有效地运行，减少病毒侵入，我局就网络安全及系统安全的有关知识进行了培训。期间，大家对实际工作中遇到的计算机方面的有关问题进行了详细的咨询，并得到了满意的答复。

九、自查存在的问题及整改意见

我们在管理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)加强设备维护，及时更换和维护好故障设备。

(三)自查中发现个别人员计算机安全意识不强。在以后的工作中，我们将继续加强计算机安全意识教育和防范技能训练，让员工充分认识到计算机案件的严重性。人防与技防结合，确实做好单位的网络安全工作。

在21世纪，网络已经成为人们日常生活的一部分，很多人甚至已经离不开网络。有了网络，人们足不出户便可衣食无忧。前些天刚从电视上看到关于年底网购火爆，快递公司也在“春运”的新闻。以前人们找东西得找人帮忙，现在人们找东西找网帮忙。记得有一次钥匙不知道放到了什么地方，就百度了一下“钥匙丢在那里了”，结果按照网友们提示的方案还真给找到了。

网络爆炸性地发展，网络环境也日益复杂和开放，同时各种各样的安全漏洞也暴露出来，恶意威胁和攻击日益增多，安全事件与日俱增，也让接触互联网络的每一个人都不同程度地受到了威胁。在此，我就生活中、工作中碰到看到的各种网络安全问题谈谈自己的体会：

1.有网络安全的意识很重要

谈到网络安全，让我们无奈的是很多人认为这是计算机网络专业人员的事情。其实，每个人都应该有网络安全的意识，这点对于涉密单位人员来说尤其重要。前段时间看了电视剧《密战》，其中揭露的泄密方式多数都是相关人员安全意识薄弱造成：单位要求机密的工作必须在办公室完成，就是有人私自带回家加班造成泄密;重要部门要求外人不得入内，偏有人把闲杂人员带入造成泄密;专网电脑不允许接互联网，有人

接外网打游戏造成泄密;甚至涉密人员交友不慎，与间谍谈恋爱造成泄密。虽然这只是电视剧，但对机密单位也是一种警示。看这部电视剧的时候我就在想，这应该作为安全部门的安全教育片。

不单单是涉密单位，对于个人来说，网络安全意识也特别重要。网上层出不穷的摄像头泄密事件、这“门”那“门”的都是由于个人安全意识淡薄所致。正如老师所说的“看到的不一定是真的!”。

我自己的电脑上有一些自己平时做的软件、系统，虽说没什么重要的，但那也是自己辛苦整出来的呀，所以使用电脑一直很小心，生怕有什么木马、病毒之类的，“360流量监控”的小条一直在我的“桌面”右下角，只要有上传流量肯定得去看看是什么进程在上传。

平时为别人维护系统经常会碰到杀毒软件很久不升级的情况，主人还振振有词的说自己装了杀毒软件的。在他们看来杀毒软件有了就成，剩下的就不用管了，我很多时候这样对他们说：“你养条狗还得天天喂它吃呢!”

2.设备安全—很多技术是我们想不到的

网络设备是网络运行的硬件基础，设备安全是网络完全必不可少的一个环节。

以前听说过电泄密，一直没见过，最近单位有同事拿来了两个“电力猫”(电力线以太网信号传输适配器)，一个接网线插到电源上，另一个在30米内接电源通过接口接网线链接到电脑便可上网。这让我想到，只要有人将涉密的网络线路接到电源线路便可轻易泄密，当然这块国家安全部门肯定有相关的防范措施。

在搜索引擎里搜索诸如：intitle:\"LiveView/-A\_IS206W\"等，可以搜到网络摄像头，在电视剧《密战》中，某涉密部门的监控系统被接入了互联网，间谍就利用监控系统窃取工作人员的屏幕信息和按键信息。在某政府机要室的复印机上安装基于移动网络的发射器，便可再用另外一台接收机上受到所有扫描的机要文件。

1985年，在法国召开的一次国际计算机安全会议上，年轻的荷兰人范〃艾克当着各国代表的面，公开了他窃取微机信息的技术。他用价值仅几百美元的器件对普通电视机进行改造，然后安装在汽车里，这样就从楼下的街道上，接收到了放臵在8层楼上的计算机电磁波的信息，并显示出计算机屏幕上显示的图像。

他的演示给与会的各国代表以巨大的震动。本人最早知道电磁泄密是在20\_\_年为部队某部门开发软件的时候听说的，在部队很多地方时安装了\_的就是为了防止电磁泄密。

硬盘数据不是删掉就不存在了，用诸如EasyRecovery等恢复软件都可以恢复。看来，只有将涉密硬盘用炼钢炉化掉才能保证完全安全。

3.小心木马

最早知道木马，是自己大学期间。当时在网上看到了一款叫“大眼睛”的屏幕发送软件，很好奇就试着用了。大学的机房里的计算机只装常用软件，其他诸如QQ等软件都是在服务器上存放，用的时候自己安装，学生机有保护卡重启就被恢复了，又得装。

于是就将“大眼睛”的客户端放在服务器上取个很吸引人的名字。结果很多同学的屏幕都被我们监控。有同学嘲笑说“不就是个木马嘛!”经过查询才知道有种叫“木马”的程序也是用同样的方法进行隐私窃取。后来自己还做过假的QQ程序盗取别人的QQ，但盗来都给了别人，谁知道现在7、8位QQ号码能这么畅销。

以前电脑都防CIH、蠕虫等病毒，当现在更多的是防木马病毒，主要是由于个人电脑上可以窃取诸如支付宝、QQ账号、网上银行等密码。当你打开不安全的网页、别人发给你的恶意邮件时，当你安装不安全的软件时，当你使用U盘时都可能感染木马病毒。

前一段时间的“360和QQ之争”，在我们的电脑里有很多不安全的的软件，都可能泄露我们的隐私。

4.网页安全

在单位，我负责几个部门的网站维护，主要是网页制作。在一开始编程的时候，根本没想到能被攻击。后来自己做的网站经常被攻击，这才知道诸如SQL注入、Ewebeditor漏洞等攻击手段，所以在编程时会注意到这些方面的安全。比如我的后台数据库一般都是“\_\_\_”。防止数据库被下载。

记得又一次为某部门自己编写了一个留言板程序，结果发布没1天就有3000多条恶意留言，还是英文的，挺让人头疼。最后设臵了验证码、用户验证都不起作用，直到用了检测留言来源网页代码才堵住。原来人家是用工具攻击的。

5.养成良好的上网习惯

网络安全涉及到使用网络的每一个人。对个人来说，要保证自己安全上网，每个人都得养成良好的上网习惯。我想应该包含以下几点：

1)电脑要安装防火墙和杀毒软件，要及时升级，如果电脑上网则设臵为自动升级。并且养成经常性安全扫描电脑;

2)及时更新windows补丁;

3)在确保系统安全的情况下，做好GHOST备份，防止碰到顽固病毒时能及时恢复系统;

4)网友用QQ等发给的网站和程序，不要轻易去点击和执行;

5)不浏览不安全的网页;

6)共享文件要及时关闭共享，在单位经常会在工作组计算机中看到别人共享的东西;

7)不熟悉的邮件不浏览;

8)U盘杀毒后再去打开;

9)不在别人的计算机上登录自己的银行账号、支付宝、QQ等;对于我们每个人来说，提高网络安全意识，学习网络安全知识，是网络时代对我们基本的要求。

【网络信息安全工作总结2024 网络安全个人工作总结5篇】相关推荐文章：

2024教师网络研修心得体会300字5篇

网络舆情处置工作方案范文最新3篇

2024网络信息安全自查报告【精选五篇】

2024广西全区高校资助政策网络知识部分竞赛试题最新

2024最新广西全区高校资助政策网络知识竞赛试题及答案解析

2024广西全区高校资助政策网络知识竞赛试题及答案完整版

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