# 网络安全工作情况汇报(六篇)

来源：网络 作者：莲雾凝露 更新时间：2022-08-28

*范文为教学中作为模范的文章，也常常用来指写作的模板。常常用于文秘写作的参考，也可以作为演讲材料编写前的参考。范文怎么写才能发挥它最大的作用呢？下面是小编帮大家整理的优质范文，仅供参考，大家一起来看看吧。网络安全工作情况汇报篇一（一）成立政府...*

范文为教学中作为模范的文章，也常常用来指写作的模板。常常用于文秘写作的参考，也可以作为演讲材料编写前的参考。范文怎么写才能发挥它最大的作用呢？下面是小编帮大家整理的优质范文，仅供参考，大家一起来看看吧。

**网络安全工作情况汇报篇一**

（一）成立政府信息系统安全工作领导小组

我局成立了政府信息系统安全工作领导小组，以班子成员局长陈竑同志为组长，副局长韦典宣同志为副组长，网络管理人员以及信息系统使用的相关人员为成员，负责我局政府信息系统安全工作的统一指挥和组织领导，办公室设在局信息化管理部门。安全小组的成立，明确了政府信息系统安全的主管领导、具体负责管护人员和管理机构。

（二）制定检查方案，确立检查范围

信息部门制定了详细的检查方案，对所要检查的部门、范围、具体要求作了部署，具体内容包括：

1、政府信息系统：检查南宁市电子政务内网统一工作平台、南宁市政务信息报送系统、政民互动综合服务平台、网上信访、南宁市城市管理局政务信息网站、市委机要网、档案管理系统。

2、安全规章制度和安全设备：检查管理制度是否健全；信息系统安全防护设施的状况、防入侵和防病毒情况、人员出入情况；是否与互联网物理隔离；计算机密码、口令的保密状况；计算机软件、程序等电子文件和加密狗的保管、使用情况等。

（三）开展安全检查，及时整改隐患

信息系统安全检查具体措施，一是对本单位政务信息系统的帐户、口令等进行了一次专门的清理检查，并及时将软件更新和升级，消除安全隐患。二是强化网络安全管理工作，对所有接入政府内部网络的计算机设备进行了全面安全检查，对发现有操作系统存在漏洞、防毒软件配置不到位的计算机进行全面升级，确保网络安全。三是规范信息的采集、审核和发布流程，严格信息发布审核，确保所发布信息内容的准确性和真实性。四是严格禁止涉密计算机与互联网相连。

（四）应急响应机制建设情况

1、制定了网络与信息系统安全应急预案，有效处置我局网络与信息的安全性与可靠性；

2、对信息系统数据进行定期备份，不断地健全的灾难备份系统、完善的灾难备份恢复计划，以降低或消除各种灾难对正常工作的影响。

（五）信息技术产品和服务国产化情况

1、终端计算机的保密系统和防火墙、杀毒软件等，皆为国产产品；

2、档案管理系统、人事管理系统等皆为市政府、市委统一指定产品系统。

（六）完善计算机安全管理制度和系统安全保护策略

完善、整理了各个部门、岗位的计算机安全管理制度、操作规程、岗位要求，如重要岗位不准窜岗、混岗；人走机关等。对每一台涉密计算机的安全保护策略进行了检查、发现不规范不安全的地方及时处理解决。

（七）强化操作人员信息安全管理

我局不断加强对计算机使用者的安全培训工作，强化每一个使用者安全使用网络的能力，提高安全防范意识，对每台入网计算机的使用者、ip地址进行登记造册。加强了网络机房安全管理工作。

（八）严格落实责任追究制度。严厉查处违反信息安全规定的行为和泄密事故、信息安全事故，严肃追究惩处责任人和有关负责人的责任。

总之，我局对涉及信息系统方面的规章制度、安全组织及职责、人员管理、体系结构、网络安全、设备和操作系统安全、应用系统安全、数据安全、物理环境安全、应急响应和灾难恢复等环节进行查找、分析和归纳，对已有的安全管理体系和安全措施进行核实和评价。从自查情况看，我局信息系统安全状况总体情况良好，不同类型的网路应用全部实现了物理隔离，多年来未发生过重大信息系统安全事件。

（一）目前存在的问题

1、不少信息系统使用人员安全意识淡薄，在管理上缺乏主动性和自觉性；

2、网络安全技术管理人员配备较少，信息系统安全方面可投入的力量有限；

3、规章制度体系初步建立，但还不够完善，未能覆盖信息系统安全的所有方面，制度的完善已列入今后的重点工作；

4、部分信息系统的数据无可靠备份，出现故障后，会导致系统使用中断；

5、在设备和操作系统安全环节，缺乏有效审计手段，无法建立可行的审计策略；

6、防病毒系统更新、升级滞后，整体运行不稳定，信息系统存在感染计算机病毒的风险隐患。

（二）下一步整改措施

针对以上自查中发现的隐患与不足，为进一步加强信息系统安全，我局应围绕信息系统安全综合治理的工作目标，重点在完善规章制度、丰富技术手段上下功夫，认真开展整改工作。

1、依据《国家信息安全技术标准规范》，结合我市信息系统安全检查工作目录，再次检查规章制度各个环节的安全策略与安全制度，并对其中不完善部分进行了重新修订与修改；

2、组织系统管理员、网络管理员、信息系统使用人员等核心技术人员开展多种形式的信息系统安全知识学习、培训，进一步强化相关工作人员安全意识的教育工作，加强设备安全巡检，防患于未然；

3、修订《市城管局网络与信息安全应急预案》，使之适应信息技术发展的新要求；

4、强化技术a、b角配置，并要求a、b角同时参与技术设备的检修与维护；

5、确保客户端防病毒系统的正确有效，确保安全补丁的及时分发；

6、进一步强化信息系统客户端安全监控及授权管理，确保系统安全。

（一）加强信息网络安全技术人员培训，使安全技术人员及时更新信息网络安全管理知识，提高相关管理及法律法规等的认识，不断地加强信息网络安全管理和技术防范水平。

（二）加大网络安全设备的.投入。

一是要继续加强对乡干部的安全意识教育，提高做好安全工作的主动性和自觉性。

二是要切实增强信息安全制度的落实工作，不定期的对安全制度执行情况进行检查，对于导致不良后果的责任人，要严肃追究责任，从而提高人员安全防护意识。

三是要以制度为根本，在进一步完善信息安全制度的同时，安排专人，完善设施，密切监测，随时随地解决可能发生的信息系统安全事故。

四是要加大对线路、系统等的及时维护和保养，加大更新力度。

五是要提高安全工作的现代化水平，便于我们进一步加强对计算机信息系统安全的防范和信息系统安全工作。

**网络安全工作情况汇报篇二**

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、不宜中学生观看的黄色网页。

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、邪恶侵蚀的“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。

**网络安全工作情况汇报篇三**

根据县委办关于开展网络信息安全考核的通知精神，我镇积极组织落实，对网络安全基础设施建设情况、网络安全防范技术情况及网络信息安全保密管理情况进行了自查，对我镇的网络信息安全建设进行了深刻的剖析，现将自查情况报告如下：

为进一步加强网络信息系统安全管理工作，我镇成立了网络信息工作领导小组，由镇长任组长，下设办公室，做到分工明确，责任具体到人，确保网络信息安全工作顺利实施。

二

我镇的政府信息化建设从xxx年开始，经过不断发展，逐渐由原来的小型局域网发展成为目前的互联互通网络。目前我镇共有电脑29台，采用防火墙对网络进行保护，均安装了杀毒软件对全镇计算机进行病毒防治。

为了做好信息化建设，规范政府信息化管理，我镇专门制订了《xx镇网络安全管理制度》、《xx镇网络信息安全保障工作方案》、《xx镇病毒检测和网络安全漏洞检测制度》等多项制度，对信息化工作管理、内部电脑安全管理、计算机及网络设备管理、数据、资料和信息的安全管理、网络安全管理、计算机操作人员管理、网站内容管理、网站维护责任等各方面都作了详细规定，进一步规范了我镇信息安全管理工作。

针对计算机保密工作，我镇制定了《xx镇信息发布审核、登记制度》、《xx镇突发信息网络事件应急预案》等相关制度，通过定期对网站上的所有信息进行整理，未发现涉及到安全保密内容的信息；与网络安全小组成员签订了《xx镇20xx年网络信息安全管理责任书》，确保计算机使用做到“谁使用、谁负责”；对我镇内网产生的数据信息进行严格、规范管理，并及时存档备份；此外，我镇在全镇范围内组织相关计算机安全技术培训，并开展有针对性的“网络信息安全”教育及演练，积极参加其他计算机安全技术培训，提高了网络维护以及安全防护技能和意识，有力地保障我镇政府信息网络正常运行。

目前，我镇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；

三是对移动存储介质的使用管理还不够规范；

四是遇到恶意攻击、计算机病毒侵袭等突发事件处理能力不够。

针对目前我镇网络安全方面存在的不足，提出以下几点整改意见：

1、进一步加强我镇网络安全小组成员计算机操作技术、网络安全技术方面的培训，强化我镇计算机操作人员对网络病毒、信息安全威胁的防范意识，做到早发现，早报告、早处理。

2、加强我镇干部职工在计算机技术、网络技术方面的学习，不断提高干部计算机技术水平。

3、进一步加强对各部门移动存储介质的管理，要求个人移动存储介质与部门移动存储介质分开，部门移动存储介质作为保存部门重要工作材料和内部办公使用，不得将个人移动存储介质与部门移动存储介质混用。

4、加强设备维护，及时更换和维护好故障设备，以免出现重大安全隐患，为我镇网络的稳定运行提供硬件保障。

随着信息化水平不断提高，人们对网络信息依赖也越来越大，保障网络与信息安全，维护国家安全和社会稳定，已经成为信息化发展中迫切需要解决的问题，由于我镇网络信息方面专业人才不足，对信息安全技术了解还不够，在其他兄弟乡镇或多或少存在类似情况，希望县委办及有关方面加强相关知识的培训与演练，以提高我们的防范能力。

**网络安全工作情况汇报篇四**

为进一步加强我院信息系统的安全管理，强化信息安全和保密意识，提高信息安全保障水平，按照省卫计委《关于xx省卫生系统网络与信息安全督导检查工作的通知》文件要求，我院领导高度重视，成立专项管理组织机构，召开相关科室负责人会议，深入学习和认真贯彻落实文件精神，充分认识到开展网络与信息安全自查工作的重要性和必要性，对自查工作做了详细部署，由主管院长负责安排、协调相关检查部门、监督检查项目，建立健全医院网络安全保密责任制和有关规章制度，严格落实有关网络信息安全保密方面的各项规定，并针对全院各科室的网络信息安全情况进行了专项检查，现将自查情况汇报如下：

我院信息管理系统于xx年xx月由xxxx科技有限公司对医院信息管理系统(his系统)进行升级。升级后的前台维护由本院技术人员负责，后台维护及以外事故处理由xxxx科技有限责任公司技术人员负责。

1、机房安全检查。机房安全主要包括：消防安全、用电安全、硬件安全、软件维护安全、门窗安全和防雷安全等方面安全。医院信息系统服务器机房严格按照机房标准建设，工作人员坚持每天定点巡查。系统服务器、多口交换机、路由器都有ups电源保护，可以保证在断电3个小时情况下，设备可以运行正常，不至于因突然断电致设备损坏。

2、局域网络安全检查。主要包括网络结构、密码管理、ip管理、存储介质管理等;his系统的操作员，每人有自己的登录名和密码，并分配相应的操作员权限，不得使用其他人的操作账户，账户施行“谁使用、谁管理、谁负责”的管理制度。院内局域网均施行固定ip地址，由医院统一分配、管理，无法私自添加新ip，未经分配的ip无法连接到院内局域网。我院局域网内所有计算机usb接口施行完全封闭，有效地避免了因外接介质(如u盘、移动硬盘)而引起中毒或泄密的发生。

3、数据库安全管理。我院对数据安全性采取以下措施：

(1)将数据库中需要保护的部分与其他部分相隔。

(2)采用授权规则，如账户、口令和权限控制等访问控制方法。

(3)数据库账户密码专人管理、专人维护。

(4)数据库用户每6个月必须修改一次密码。

(5)服务器采取虚拟化进行安全管理，当当前服务器出现问题时，及时切换到另一台服务器，确保客户端业务正常运行。

我院his系统服务器运行安全、稳定，并配备了大型ups电源，可以保证在大面积断电情况下，服务器可运行六小时左右。我院的his系统刚刚升级上线不久，服务器未发生过长宕机时间，但医院仍然制定了应急处臵预案，并对收费操作员和护士进行了培训，如果医院出现大面积、长时间停电情况，his系统无法正常运行，将临时开始手工收费、记账、发药，以确保诊疗活动能够正常、有序地进行，待到his系统恢复正常工作时，再补打发票、补记收费项目。

我院的网络与信息安全工作做的比较认真、仔细，从未发生过重大的安全事故，各系统运转稳定，各项业务能够正常运行。但自查中也发现了不足之处，如目前医院信息技术人员少，信息安全力量有限，信息安全培训不全面，信息安全意识还够，个别科室缺乏维护信息安全的主动性和自觉性;应急演练开展不足;机房条件差;个别科室的计算机设备配臵偏低，服务期限偏长。

今后要加强信息技术人员的培养，提升信息安全技术水平，加强全院职工的信息安全教育，提高维护信息安全的主动性和自觉性，加大对医院信息化建设投入，提升计算机设备配臵，进一步提高工作效率和系统运行的安全性。

**网络安全工作情况汇报篇五**

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/-axis206w\"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20xx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干扰器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)最好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。

**网络安全工作情况汇报篇六**

为了认真贯彻落实公安部《关于开展重要信息系统和重点网站网络安全保护状况自检自查工作的通知》文件精神，为进一步做好我院网络与信息系统安全自查工作，提高安全防护能力和水平，预防和减少重大信息安全事件的发生，切实加强网络与信息系统安全防范工作，创造良好的网络信息环境。近期，我院进行了信息系统和网站网络安全自查，现就我院网络与信息系统安全自查工作情况汇报如下：

（一）自查的总体评价

我院严格按照公安部对网络与信息系统安全检查工作的要求，积极加强组织领导，落实工作责任，完善各项信息系统安全制度，强化日常监督检查，全面落实信息系统安全防范工作。今年着重抓了以下排查工作：一是硬件安全，包括防雷、防火和电源连接等；二是网络安全，包括网络结构、互联网行为管理等；三是应用安全，公文传输系统、软件管理等，形成了良好稳定的安全保密网络环境。

（二）积极组织部署网络与信息安全自查工作

1、专门成立网络与信息安全自查协调领导机构

成立了由分管领导、分管部门、网络管理组成的信息安全协调领导小组，确保信息系统高效运行、理顺信息安全管理、规范信息化安全等级建设。

2、明确网络与信息安全自查责任部门和工作岗位

我院领导非常注重信息系统建设，多次开会明确信息化建设责任部门，做到分工明确，责任具体到人。

3、贯彻落实网络与信息安全自查各项工作文件或方案

信息系统责任部门和工作人员认真贯彻落实市工业和信息化委员会各项工作文件或方案，根据网络与信息安全检查工作的特点，制定出一系列规章制度，落实网络与信息安全工作。

4、召开工作动员会议，组织人员培训，专门部署网络与信息安全自查工作

我院每季度召开一次工作动员会议，定期、不定期对技术人员进行培训，并开展考核。技术人员认真学习贯彻有关文件精神，把信息安全工作提升到重要位置，常抓不懈。

（一）网络安全管理情况

1、认真落实信息安全责任制

我院制定出相应信息安全责任追究制度，定岗到人，明确责任分工，把信息安全责任事故降低到最低。

2、积极推进信息安全制度建设

（1）加强人员安全管理制度建设

我院建立了人员录用、离岗、考核、安全保密、教育培训、外来人员管理等安全管理制度，对新进人员进行培训，加强人员安全管理，不定期开展考核。

（2）严格执行机房安全管理制度

我院制定出《机房管理制度》，加强机房进出人员管理和日常监控制度，严格实施机房安全管理条例，做好防火防盗，保证机房安全。

（二）技术安全防范和措施落实情况

1、网络安全方面

我院配备了防病毒软件、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。计算机及网络配置安装了专业杀毒软件，加强了在防病毒、防攻击、防泄密等方面的有效性。并按照保密规定，在重要的涉密计算机上实行了开机密码管理，专人专用，杜绝涉密和非涉密计算机之间的混用。

2、信息系统安全方面

涉密计算机没有违规上国际互联网及其他的信息网的情况，未发生过失密、泄密现象。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）应急工作情况

1、开展日常信息安全监测和预警

我院建立日常信息安全监测和预警机制，提高处置网络与信息安全突发公共能力事件，加强网络信息安全保障工作，形成科学、有效、反应迅速的应急工作机制，确保重要计算机信息系统的实体安全、运行安全和数据安全，最大限度地减轻网站网络与信息安全突发公共事件的危害。

2、建立安全事件报告和响应处理程序

我院建立健全分级负责的应急管理体制，完善日常安全管理责任制。相关部门各司其职，做好日常管理和应急处置工作。设立安全事件报告和相应处理程序，根据安全事件分类和分级，进行不同的上报程序，开展不同的响应处理。

3、制定应急处置预案，定期演练并不断完善

我院制定了安全应急预案，根据预警信息，启动相应应急程序，加强值班值守工作，做好应急处理各项准备工作。定期演练预警方案，不断完善预警方案可行性、可操作性。

（四）安全教育培训情况

为保证我院网络安全有效地运行，减少病毒侵入，我院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。

经过安全检查，我单位信息系统安全总体情况良好，但也存在了一些不足：

1、信息安全意识不够。员工的信息安全教育还不够，缺乏维护信息安全主动性和自觉性。

2、设备维护、更新还不够及时。

3、专业技术人员少，信息系统安全力量有限，信息系统安全技术水平还有待提高。

4、信息系统安全工作机制有待进一步完善。

根据自查过程中发现的不足，同时结合我院实际，将着重以下几个方面进行整改：

一是要继续加强对全员的信息安全教育，提高做好安全工作的主动性和自觉性。

二是要切实增强信息安全制度的落实工作，不定期的对安全制度执行情况进行检查，对于导致不良后果的责任人，要严肃追进责任，从而提高人员安全防范意识。

三是要加强专业信息技术人员的培养，进一步提高信息安全工作技术水平，便于我们进一步加强计算机信息系统安全防范和保密工作。

四是要加大对线路、系统、网络设备的维护和保养，同时，针对信息技术发展迅速的特点，要加大系统设备更新力度。

五是要创新完善信息安全工作机制，进一步规范办公秩序，提高信息工作安全性。

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：

一是对于线路不整齐、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。

二是加强设备维护，及时更换和维护好故障设备。

三是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。

本文档由范文网【dddot.com】收集整理，更多优质范文文档请移步dddot.com站内查找