# 县局网络安全工作总结(优选47篇)

来源：网络 作者：雾凇晨曦 更新时间：2024-01-21

*县局网络安全工作总结1为了更好的宣传网络安全知识，在全校范围内开展网络安全知识的宣传。我校宣传部、校团委等部门整体规划了设计方案。发挥线上线下多渠道的宣传优势，全方位多角度的对网络安全意识的提升加以宣传。通过校园大屏幕滚动播放相关视频让全校...*

**县局网络安全工作总结1**

为了更好的宣传网络安全知识，在全校范围内开展网络安全知识的宣传。我校宣传部、校团委等部门整体规划了设计方案。发挥线上线下多渠道的宣传优势，全方位多角度的对网络安全意识的提升加以宣传。通过校园大屏幕滚动播放相关视频让全校学生在视觉上得到体验;通过校园广播电台让全校学生在课余时间对相关知识有深入的了解;同时，通过开展班会的方式，使得学生更系统、更全面的了解网络安全方面的知识。

通过以上展开的切实有效的宣传活动，使三初学子从最初对网络安全概念淡漠，逐步上升到树立网络安全自我保护意识。

**县局网络安全工作总结2**

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。

**县局网络安全工作总结3**

为贯彻落实全国网络安全和信息化工作会议的重要讲话精神，根据市委网信办《关于印发网络安全宣传周活动实施方案>的通知》（雅委网信办10号）《石棉县国家网络安全宣传周活实施方案》文件要求，围绕“网络安全为人民，网络安全靠人民”的主题开展宣传活动，现将我乡宣传工作情况报告如下。雅安市国家>

一、网络安全宣传工作开展情况

（一）高度重视，提高认识，确保网络安全宣传活动有序开展。成立由乡党委书记为组长，乡党委副书记、乡长和纪委书记为副组长的回隆彝族乡的国家网络安全宣传活动领导小组，对全乡网络安全宣传活动统一领导。由乡司法所和综治办等站所具体分工，明确职责，确保活动有序推进。

（二）精心组织，稳步推进，确保网络安全宣传活动保质保量。我乡高度重视本次网络安全宣传活动，通过干部职工会议传达全国网络安全会议的重要讲话精神。及时制定网络安全宣传学习活动实施方案，以村为单位有序开展工作。

（三）加强宣传，营造氛围，确保网络安全宣传活动达到目标。充分利用会议、标语横幅、宣传栏、LED显示屏、微信群、到学校宣讲和发放传单等线下线上、室内与室外相结合的宣传方式，营造浓厚氛围，提高群众知晓率。

（四）深入基层，做好思想发动，确保活动取得实实在在的效果。开展志愿服务，组织乡、村青年深入农家、企业和学校开展网络安全宣传活动，在全乡小学通过开展主题班会、发放宣传资料等多种宣传方式，进一步宣传网络安全知识。

二、网络安全宣传活动取得的实效

一是思想认识得到提高。通过网络安全宣传活动的开展，群众、企业、乡干部认识到网络便利生活工作的同时，存在手机中毒和账号密码、个人隐私等重要信息的泄漏等危害，认识到本次国家网络安全宣传活动的重要性。二是加强了青少年教育。通过开展网络安全进校园活动，强化了学生的网络安全意识，提高了防范网上有害信息的能力。

三是营造浓厚氛围。通过线上和线下、室内和室外等宣传方式，在全乡营造网络安全的浓厚氛围，明确网络安全为人民，网络安全靠大家的主题，着力营造人人关注网络安全的良好氛围。四是长效机制得到确定。通过网络安全学习活动，初步建立起回隆乡网络安全工作制度，明确职责、分工，把网络安全宣传工作长期有效的开展，增长群众网络安全知识，提高警惕，预防网络诈骗。

三、下一步工作打算

一是加强学习，进一步提高认识。让群众认识网络安全的重要性，将网络安全落实到生活生产中，网络安全靠人民。二是建章立制，建立网络安全工作的长效机制。三是发现问题及时整治，确保网络安全活动取得实效。四是进一步加强宣传，营造氛围。

**县局网络安全工作总结4**

为认真贯彻落实党的十八大精神，构建和谐、稳定、可持续的良好发展新环境，切实加强我乡应急管理工作建设，不断提高我乡各职能部门、乡辖各单位应对和处置突发公共事件的能力。根据XX县人民政府办公室关于报送20xx年上半年应急管理工作总结的通知要求，结合我乡实际，扎实有效的开展了应急管理各项工作，现将半年来我乡开展应急管理工作总结如下：

1、年初，乡党委、政府立足我乡实际情况，调整充实了应急管理工作领导小组、乡防汛指挥部领导小组，完善了机制、明确了责任，细化了工作，确定了目标，并把应急管理工作纳入各村年终目标考核。

2、建立和完善了《乡防洪预案》、《乡防洪预案》、《乡突发地质灾害应急预案》、《乡地质灾害防治预案》及四个地质灾害点的应急预案，《乡防洪预案》中明确了疏散责任人、撤离路线及老弱病残人员的具体责任人。建立健全了工作机制，切实有效地开展了各项应急工作，达到了有计划、有步骤、有方法、早预防、零伤亡的工作实效。

3、建立健全了应急管理信息台帐，进一步落实了应急机构联系方式，加强了应急管理网络化、信息化、规范化建设。乡政府办公室抓好各项日常报表的按时上报工作，无一件次出现“错、漏、拖、瞒、差”情况发生。

4、及时安排专人参加了由市政府组织的各类安全应急管理培训工作会议和学习，没有一例无故缺席现象，会议及学习过程中参学人员没有迟到、缺席、早退。乡应急办工作人员不定期对我乡的地质灾害点进行排查，发现安全隐患及时整改。

5、乡应急管理工作，按照上级要求和结合我乡实际，乡成立了由20人组成的应急队伍，确保“召之即来、来之能战、战无不胜”的工作实效。各村成立了应急小分队负责处理本辖区的应急突发事件。乡应急办为提高应急突发事件的处置救援工作能力，减少突发事件对社会的危害性，保护人民群众的生命财产安全，维护好社会稳定和谐，做到防灾减灾，把突发灾害损失降低到最低点，切实做好抢险救援工作和对突发事件的应对。乡应急办公室落实专人负责日常各项工作，应急物资储备室落实专人看管，建立好应急物资储备台账和使用台账，不断完善应急物资的储备。

6、为切实保障人民群众的生命、财产安全，科学有效地防治一切突发灾害的发生，我乡积极配合上级部门及时对存在一定安全隐患的地点、地段、行业、部门等进行了科学有效的排查，通过排查，消除了2处安全隐患，同时对存在问题的道路交通、安全生产、药品食品管理、信息通信等领域进行了彻底整治。

7、积极开展了食品药品、、防灾减灾、地震灾害应急、校园及饮用水安全知识等培训工作，认真做到集中学习、广泛宣传，互帮互救，营造了共同参加，群防共治的良好应急防治社会氛围。

8、健全了预警工作机制，完善了预警工作通讯网络建设。抓好汛期防汛值班工作，坚持落实值班有带班领导，值班领导的值班制度，明确了值班人员的职责，保持手机24小时开机，做好值班记录的填写。各村落实值班责任人对本辖区内的重点区域钉死钉牢。乡应急办工作人员时刻关注上级下发的天气预报信息，及时掌握最新天气状况。同时加大对业务知识的学习，应急信息报送员严格按照上级部门要求报送信息。

9、乡政府应急办制定了我乡20xx年防洪应急演练预案，前期各项准备工作正在进行中，计划在6月上旬开展一次防洪演练。

10、督促学校抓好“应急教育示范学校”的创建工作。“应急教育示范学校”创建工作由分管领导亲自抓，学校主要领导具体抓。

11、工作中存在的主要问题

我乡在应急管理工作中还存在一些问题：一是个别党员干部在应急管理工作中认识不足、重视不够。二是应急管理和防灾自救的宣传形式不够多，群众对应急管理的了解不全面、知识掌握不丰富、自救能力不够强。三是应急预案制定不够具体细致，预案质量还有待于提高。四是应急管理工作中资金不足，开展应急演练和应急管理培训资金不足。

总之，我乡应急管理工作，在县委、政府的正确领导下，坚持以十八大精神为指导，认真落实工作职责，完善工作要求，无任何重大危害事件发生，无工作失职情况。我们将在县委、政府的正确领导下，不断查漏补缺，弥补工作中的一些不足，继续开拓创新、锐意进取，为建设幸福而奋斗。

xx局在市局党组的正确领导和大力支持下，高度重视网络与信息安全工作，确立了“网络与信息安全无小事”的思想理念，专门召开会议部署此项工作，全局迅速行动，开展了严格细致的拉网式自查，保障了各项工作的顺利开展。主要做法是：

**县局网络安全工作总结5**

为了更好的宣传网络安全知识，在全校范围内开展网络安全知识的宣传。全方位多角度的对网络安全意识的提升加以宣传。通过校园广播滚动播放让全校学生在听觉上得到体验;通过专栏的介绍相关安全知识;让学生在课余时间对相关知识有深入的了解;同时还通过发动学校的微信公众平台发放网络安全知识。在校少先队部的统一安排下，展出了以“共建网络安全、共享网络文明”为主题的网络安全宣传板报。通过以上展开的切实有效的宣传活动，使学生从最初对网络安全概念淡漠，逐步上升到树立网络安全自我保护意识，并将其运用到生活中，以便更好的创造和谐的网络环境。

**县局网络安全工作总结6**

按照机构改革后的职能划分，县行政审批局是未来政务数据产生量最大的部门，数据安全任务非常艰巨，还存在数据安全设备和技术保障力量不足现象，结合县行政审批局工作现状，现从“源、点、线”三个方面汇报如下：

一是数据源头保安全。县行政审批局是政务数据的主要发生源，工作形式有各单位入驻所用的专网和省市政务外网两种形式。前一种形式，数据的产生在各单位自有或省市垂直系统内，数据输出源在专有工作电脑。要求各单位对各自工作电脑进行监管。县行政审批局采用“一机一线，一系统一防火墙”的模式，确保切断数据泄露的网络接口。后一种形式数据源头在自由开放的网络环境中，且数据提交接口在省市政务系统服务器，无需确保源头数据安全。

二是数据节点保安全。大数据县级数据站是全县大数据产业发展的必要环节，是县域数据汇集的大海，是未来数据安全工作的核心。县行政审批局已对全县现有政务系统和政务数据资源目录进行了梳理，形成了系统和数据资源两张清单，为全县打破数据壁垒、实现数据共享做了软件、硬件两方面安全保障准备工作，确保数据按规范进站，按授权出站。

三是数据线路保安全。数据源到数据站，数据站到上级或友邻数据站的通信需要安全软件来实现。目前现有系统有各自的安全保障措施，待所有审批职能划转后，县行政审批局将统一建设数据安全软件保障体系。

**县局网络安全工作总结7**

1、提高关区骨干网络基础保障能力。

继续进行关区广域骨干网的升级扩容工作，建设关区信息高速公路。

2、继续加强关区机房的建设和安全运行。

根据今年国家公布的《电子信息系统机房设计规范》，提出我关区机房建设要求，加强关区网络和机房安全建设。进行总关机房的扩容工作，增加机房UPS供电能力，优化机房散热效果。更新机房监控系统，对机房进行精细化管理。

3、进行管理网对外接入局域网的建设

根据总署指导方案和我关的实际情况，制定出我关建设方案，清理规范现有系统，满足信息安全要求。

4、进行关区网络维护小组建设

为解决网络维护人力问题，提高网络故障反应速度，以关区网络升级扩容为契机，重点培养几名隶属关网络维护人员，能够对周边隶属关进行网络故障排除。

这一年是紧张有序的过来了，虽然很忙碌，但是公司领导和相关部门各同事都给了我很大帮助，我才能顺利的完成了本年度的任务。为了今后更好的工作，总结经验、完善不足，本人就本年度的工作总结如下：

1、对各部门电脑软件、硬件、邮件打印机、网络的维护工作级时和到位。让设备的的使用故障率降到最低，在故障发生的时候立马当地解决。有不能当地解决的也会在最短的时间内给予解决。

2、及时的对系统补丁进行更新，防止了病毒和黑客通过系统漏洞进行的破坏和攻击。对ie、outlook、office等应用程序也打上最新的补丁，另外还关闭了一些不需要的服务，关闭guset帐号等。3、对中心每台电脑安装防病毒软件，避免了病毒在公司局域网内自我复制相互传播，占用局域网的网络资源，甚至使得系统崩溃，丢失硬盘的重要资料等各种危害，并及时的对软件进行升级，定期的清除隔离病毒的文件夹。

4、项目机房系统更新，系统从原有的更新到xp，重新安装了所有软件，解决了一部分原无法解决的问题，并重新部署杀毒软件解决方案。

5、交换机、路由等网络硬件设备的维护，屏蔽中心不用的端口，安全设置等，保证公司所有电脑的安全正常工作，优化路由运行速度，节约带宽，提高上网的速度化和稳定化，使我们上网的速度大大提高，保证网络顺畅

6、针对服务器，3次被黑客攻击采取相应的解决方案。重新部署服务器。

7、学校服务器，硬件的安装、维修、调试，投影仪设备的定期清理，维护。

8、电话交换机部属置，电话线调整，电话录音设备的安装调试。

9、rtx服务器、邮件服务器、web服务器、搭建、优化、信息整理和测试。用户数据导入和备份。

10、为了最大的节约成本，并针对学校所有计算机设置系统自动休眠，有效地节省了相当一部分资源。

11、加强了对网络设备的维护，对经常出故障的设备采取了相应的解决办法。公司目前一共近80多台电脑，由于机器较多，日常出现故障的情况较为常见，主要的电脑故障有：系统故障，网络故障，软件故障等，很多机器由于长期使用，导致系统中存在大量垃圾文件，系统文件也有部分受到损坏，从而导致系统崩溃，重装系统，另外有一些属网络故障，线路问题等。

近一年来，我始终坚持严格要求自己，勤奋努力，在自己平凡而普通的工作岗位上，努力做好本职工作，从不把情绪带到工作中。在具体工作中，我努力做好服务工作。回顾一年来的工作，我在思想上、学习上、工作上取得了新的进步。但我也认识到自己的不足之处：

1、因为简单的问题重复出现重复解决，可能到位不及时。

2、自己的思路还很窄对现代网络技术的发展认识的不够全面，自己对新技术掌握速度还不够快。

3、有时出现问题我并不知道而领导先知。其实从咱们公司的结构来看这些都是正常的，但我以网管的身份感到惭愧。

20xx年xx月xx日至xx日是首届国家网络信息安全宣传周，为全面加强我校网络安全安全工作，增强师生网络安全意识，依据国家教育局【20xx】xx号文件精神，结合学校实际情况，我校于20xx年xx月xx日——11月30日在全校范围内广泛深入地开展了国家网络信息安全宣传周活动，现将活动总结如下：

**县局网络安全工作总结8**

正文：

首先，服务器上用的是私有的操作系统和数据库，所谓私有，并不是完全自己写，而是说，全部都是进行私有化改造过的，一般使用开源的操作系统和数据库进行改造，比如说操作系统使用free bsd的改，数据库使用mysql的改，网站服务器数量上百时开始实施这个工程的网站比较多，费用是很重要的一方面原因，但更重要的是安全因素。防火墙不仅昂贵，而且会严重降低效率，所以他们一般不会考虑。

改造操作系统的时候，除通信所需的一些命令文件保持原名外，很多命令文件连文件名都换掉(有人认为这是小花样，呵呵)，大量功能被重写， 即使拿到权限坐在服务器面前，也取不到数据。

有网站首席安全官认为放一扇门让别人一个劲砸，不如给人两条路让人选择正确的或者不正确的，所有使用错误帐号和密码去试系统的人，都会被允许以匿名身份登陆到一个shell里，那个shell跟真的系统很象，嗯，只是很象，但其实是个空壳，所有的指令，都会被以最小代价运行，调用假的信息界面出来。有的甚至里面放了陷阱，欺骗性引导 自动送上身份资料或其他一些敏感信息，毕竟 可能通过境外跳板过来，如果不是 主动送上，网站方很难获得 身份资料的。

使用自己的安全策略，对已有的攻击手段都有相应的防护措施，

比如说对syn flood这样的，就是临时降低服务质量，降低半连接等待时间，这样连接的成功率会降低，但是不会造成服务被停。

网络空闲时间经常有欺骗性数据流在办公网络和服务器之间流动，使用强度不高的加密方式加密，让 有事做。

网站内部工作人员使用业务系统登陆网站服务器时，界面上和一般服务器一样，所有的一般命令都可以通过业务系统转换为私有操作系统的专用命令而得到执行，网站内部工作人员也只有很少的知道转换的对照，而且一般都经过分权，做操作系统开发的，不负责服务器的维护，并且不知道安装某个内部版本号操作系统的服务器被部署到什么地方。

帐号及密码按规定必须通过安全的消息平台传递。

有自己部署在不同城市的DNS服务器，所有部署出去的应用都有不在同一机房的备用系统，应急机制设置在自己的DNS服务器这一环节，使用承载其他服务的服务器做交叉的安全状态监测，比如说A1服务器是A服务器的备用系统，使用CDEFGH等服务器来做A服务器安全状态监测，定时通信，并向A1服务器传递通信成功的信号，当失败率超过某个值的时候，A1自动分担A的部分压力，A1服务器上原本承担的非及时服务(不面向客户的，比如说索引服务)被降低优先级。所有服务器之间这么相互监测，通过某个机制保证监测是及时有效的。这样的情况下，即使某家DNS服务商被攻击，自己的网站都还能被大部分用户访问，因为不同地区的DNS还没被刷，用户还是可以使用那些DNS连接到网站的。

一般而言，使用了这些手段，网站的安全性不能说万无一失，也是大大提高的。

**县局网络安全工作总结9**

黑客和计算机病毒都是普遍的威胁，而为大家所熟知的日常网络安全也同样存在各种问题。针对这些问题，主讲人李霭莹老师向学生们介绍了日常生活中，使用网络时存在的安全隐患，并讲解应该从哪些方面来保护自己。为大家提供了很多有价值的宝贵建议，例如：如网络浏览器，是完整安装且更新修正至最新版;安装个人防火墙与更新病毒码至最新的防毒软件等等。同学们在课堂上的认真状态足以见得本次教育活动真正为同学们答疑解惑，达到了预期目的的同时也丰富了同学们的网络知识。通过网络安全宣传周的系列活动，学生对网络安全知识已经有了一个初步的了解，能够自觉遵守《全国青少年网络文明公约》，将良好的网络素养和高尚的网络道德进行到底。同整个社会共同建立一个和谐的网络环境，让更多的人在安全的网络中受益。

网络应用已逐步深入到了同学们的生活中，是学习和生活的必要组成部分，通过此次网络安全活动周的一系列活动，同学们在提高了网络安全防范意识的同时，也希望通过大家共同的努力，可以使互联网可以干净透明，越来越文明，以便于我们更好的在网络世界畅游，更好地学习与生活。

11月21日，国家网络安全宣传周“网络安全知识进万家”活动在市部分高校启动。为贯彻落实中央关于网络安全和信息化的战略部署，响应教育部、省教育厅的号召，同时也是为了加强我校学生树立网络安全的自我保护意识，提高网络安全防范技能，因此于11月24日—30日开展了为期一周的有关网络安全知识宣传系列活动。内容及形式丰富多彩，具体如下：

**县局网络安全工作总结10**

内容丰富

1、针对活动意义和活动目的，确定宣传标语为：共建网络安全，共享网络文明。并张贴在校门口。

2、充分利用板报、班刊广泛宣传网络安全教育相关知识。

3、中心校统一下发光盘，各校组织学生观看影像资料，对学生进行网络安全教育，上好网络安全第一课。

4、全校进行了一次校园网络安全隐患大排查。

5、进行了一次全员参与网络安全演练，各校均于本周举行了网络安全演练。整个撤离过程井然有序，没有意外事故发生。

**县局网络安全工作总结11**

一是思想认识得到提高。通过网络安全宣传活动的开展，群众、企业、乡干部认识到网络便利生活工作的同时，存在手机中毒和账号密码、个人隐私等重要信息的泄漏等危害，认识到本次国家网络安全宣传活动的重要性。二是加强了青少年教育。通过开展网络安全进校园活动，强化了学生的网络安全意识，提高了防范网上有害信息的能力。

三是营造浓厚氛围。通过线上和线下、室内和室外等宣传方式，在全乡营造网络安全的浓厚氛围，明确网络安全为人民，网络安全靠大家的主题，着力营造人人关注网络安全的良好氛围。四是长效机制得到确定。通过网络安全学习活动，初步建立起回隆乡网络安全工作制度，明确职责、分工，把网络安全宣传工作长期有效的开展，增长群众网络安全知识，提高警惕，预防网络诈骗。

**县局网络安全工作总结12**

根据《国家\_关于开展税务信息系统安全检查工作的通知》（国税函[20xx]397号）、《江西省国家税务局关于开展税务信息系统安全减产工作的通知》（赣国税函[]223号）及XX市国税局《关于开展税务信息系统安全检查工作的通知》（信便函[]号），按照相关文件要求和“谁主管谁负责、谁运行谁负责、谁使用谁负责”的原则，我局开展本次信息安全检查专项工作，查找薄弱环节和安全隐患，分析网络与信息系统面临的风险，评估网络与信息系统的安全状况，进一步强化了信息安全意识、规范信息安全管理，切实保障税务网络与信息系统安全运行，现将自查情况报告如下：

一、明确信息安全检查的主管领导和具体负责管理人员，成立信息安全检查工作组，对本单位的信息网络安全进行了全面检查。

组长：XXX副组长：XXX成员：XXXXXX

二、检查重点

（一）信息中心机房及农村分局机房管理情况

经检查，我局信息中心机房及四个农村分局机房都有可靠的防火、防盗设施，安装有空调，能够将温度调节到适宜范围之内，有效保障设备的良好运行，并按照《XX县国家税务局机房管理暂行条例》的规定，建立卫生值日制度，以保持机房机器、设备、器具、地面的整齐、干燥、清洁。

在信息中心主机房配有UPS电源，当外电中断后，立即启动UPS电源，必要时能使用发电机发电，确保网络24小时畅通，保障税收业务的正常开展。

（二）应用系统运行及数据备份情况

我局主要运行的应用系统有FTP和公文处理，应用系统的服务器存放于信息中心主机房，目前运行状况良好，对服务器运行产生的数据做到及时备份、月备份、年备份，并对年备份数据做光盘刻录归档管理。

（三）网络链接及保密安全情况

到市局网络连接的线路目前采用以电信线路为主，移动线路为备用的连接方式，当发生网络故障时，对出现线路级故障时立即启动备用线路，并应迅速判断故障节点，查明故障原因；如属本系统故障，立即组织人员予以恢复，对出现网络设备故障，县局一般都是临时紧急调拨备用周转设备解决，以确保路线的畅通，并要求尽快修复已损坏网络设备；如属电信或移动部门管辖范围，立即与电信或移动维护部门联系，要求线路提供部门对提供给国税系统的光端机、光电转换器等传输设备以及光纤线路进行一次全面的运行故障排查，并制定相应的故障处理预案，对薄弱环节制定相应的保障措施；同时加大日常运行技术服务力度，确保端口级故障10分钟内、设备级故障2小时内、线路级故障3小时内恢复。

按照内外网必须物理分离的原则，内网办公用计算机禁止登录国际互联网（INTERNET），因实际工作需要，确实要上网的，由信息中心统一安排，配备专用的计算机设备使用因特网网络，在上外网时保证互联网与国税内部网络无任何形式的物理链接，以防止网上病毒的感染和黑客的攻击，确保涉密信息的安全。

（四）个人计算机的使用及管理情况

计算机设备的管理和使用落实到个人，遵循谁使用谁负责的原则，全县国税系统计算机设备IP规划由县局信息中心网络管理人员统一设置，在每台计算机设备上贴上“XX县国税局计算机设备身份标识卡”，注明相关信息，并要求其他任何单位及个人不得擅自修改计算机IP地址及名称等信息。

全县国税系统内所有办公用计算机统一安装省局下发的网络版瑞星杀毒软件、北信源桌面安全防护系统、SUS客户端并及时安装最新系统补丁，以防止计算机病毒对计算机及网络设备的破坏；县局机关各部门及各农村分局定期对本部门计算机进行查杀毒工作，并将结果定期向信息中心反馈，发现有计算机被感染上病毒后，立即启用反病毒软件对该机进行杀毒处理，同时通过病毒检测软件进行跟踪、分析，并及时采取阻断、隔离、进入DOS或安全模式进行杀毒、清除。

为保证各应用系统的安全使用，规定各系统用户必须修改用户密码，禁止使用默认密码，确保账号权限不被他人盗用、滥用。

三、信息安全检查发现的主要问题和整改意见

根据上级局相关文件的要求，在自查过程中我们也发现了一些不足之处，主要有以下几个方面需要进行整改。

1、安全意识不够。少数干部安全意识不强，对修改的\'密码等要求不够重视，有些同志仍然存在使用默认密码的情况，要继续加强对机关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。

2、技术水平不够高，由于计算机网络信息安全技术专业性较强，在整体水平上离上级局的要求有一定的差距，以后必须强化培训，提高专业技能，做到人防与技防结合，把计算机安全保护的技术水平看作是保护信息安全的一道看不见的屏障。

3、工作机制有待完善，在信息爆炸的新时代，计算机技术的变化日新月异，创新安全工作机制，适应发展的需要，是信息工作新形势的必然要求，这有利于提高机关网络信息工作的运行效率，有利于办公秩序的进一步规范。

在以后的工作中，我局将加大对信息安全的检查力度，认真落实技术防范措施，由专门人员定期对日常使用情况进行自查，及时发现和消除计算机信息系统安全隐患，不断提高税务信息系统的安全保障能力和信息安全工作水平。

**县局网络安全工作总结13**

针对目前存在的一些网络安全的问题与隐患，我校组织学生11月26日组织三场“网络安全精彩一课”教育巡讲，现代教育技术中心老师为近600名同学们相继带来了精彩的讲说，增长了同学们的网络安全知识，提高了同学们的网络安全防范意识。

开展此次“网络安全精彩一课”教育活动也是积极响应国家的号召。黑客和计算机病毒都是普遍的威胁，而为大家所熟知的日常网络安全也同样存在各种问题。针对这些问题，主讲人老师向学生们介绍了日常生活中，使用网络时存在的安全隐患，并讲解应该从哪些方面来保护自己。为大家提供了很多有价值的宝贵建议，例如确保作业系统与系统软件，如网络浏览器，是完整安装且更新修正至最新版；安装个人防火墙与更新病毒码至最新的防毒软件等等。同学们在课堂上的认真状态足以见得本次教育活动真正为同学们答疑解惑，达到了预期目的的同时也丰富了同学们的网络知识。

根据xx省教育厅下发的《关于开展xx省教育系统第X届国家网络安全宣传周活动的通知》文件精神及相关要求，在校领导的安排部署下，在相关部门同力合作下，我校于XX年XX月XX日至XX日举行全校网络安全知识宣传教育活动，通过网络安全知识的宣传，有效提高了我校师生对网络安全风险和金融网络风险的防御能力。学生通过网络安全教育懂得了如何避免浏览不良网站，学会让网络帮助自己的学习，用网络开拓自己的视野，丰富自己的知识，合理利用网络多方位的提升自己。

我校网络安全宣传周期间，主要通过以下方式大力宣传了网络安全知识：

1、我校在教学楼和大门口等地方悬挂了网络安全宣传标语横幅，有效渲染了网络安全知识学习氛围。

2、通过我校微信公众平台宣传网络安全知识，及网络安全宣传活动情况。

3、通过我校法制教育大会向全体学生讲述了网络安全知识。

4、通过我校XX月XX日举办的《中小学预防儿童意外伤害知识竞赛》，让学校了解更多的网络安全知识。

5、在我校网站信息技术资讯栏目发布了多篇网络安全知识相关，并及时发布有关这次网络安全宣传周的活动记录。

6、各班级组织开展了关于普及网络安全知识主题班会。

在这次网络安全宣传周活动中，我校师生积极配合认真学习网络安全知识，充分认识到了网络给师生工作学习带来的利与弊，增强了防范网络安全风险的意识，懂得了应该文明上网，健康上网。

总之，对中职学生进行网络安全教育是一项系统工程，需要社会、学校、家庭等各个部门通力合作、齐抓共管。以上是我校在网络安全宣传周活动经验总结。

为切实做好20xx年国家网络安全宣传周工作，提高干部群众的国家安全意识，根据相关通知要求，我行高度重视，认真的开展了宣传活动。现将我行开展情况汇报如下：

**县局网络安全工作总结14**

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。

**县局网络安全工作总结15**

上网的人中，很少有谁没被病毒侵害过，但在大多数人将注意力放在对付病毒上时，业内权威人士新近指出，现在要想保证上网安全，必须对以下这三种威胁同时设防。第一是以传统宏病毒、蠕虫等为代表的入侵性病毒；第二是以间谍软件、广告软件、网络钓鱼软件、木马程序为代表的扩展类威胁；第三是以 为首的有目标的专门攻击或无目标的随意攻击为代表的网络侵害。

三大新威胁

Spyware(间谍软件)：主要是用作偷取用户个人资料的恶意程序，如用户使用网上银行、网上购物等电子商务应用时，如果没有相关的防御措施与意识，那么用户的网银账号和密码就很容易被窃取。

Phishing(网络钓鱼软件，又称电子黑饵)：是fishing和phone的缩写。是指盗取他人个人资料、银行及财务账户资料的网络相关诱骗行为，可分为诱骗式及技术式两种。诱骗式是利用特制的电邮，引导收件人连接到特制的网页，这些网页通常会伪装成真正的银行或理财网页，令登录者信以为真，输入信用卡或银行卡号码、账户名称及密码等；技术性的Phishing则是将程序安装到受害者的电脑中，直接盗取个人资料或使用木马程序、按键记录程序等。

只防病毒不安全

目前众多网民已不再是简单地上网浏览网页及收发电邮，随着网上银行、网上购物等电子商务应用的出现，来自网上的威胁不仅仅是传统的病毒了。

有报道称，中国目前已经成 首选的攻击目标，每天有3万台PC机处于随时可能被攻击的失控状态。业内人士指出，未来对电脑及电脑用户造成最大威胁的并不是我们惯常认为的电脑病毒(Virus)，而是一些Spyware(间谍软件)、Adware(广告软件)、Phishing(网络钓鱼软件)、Trojan(木马程序)、Worms(蠕虫)。原因是大部分用户及商业机构对一般的电脑病毒已有一定的防范，譬如安装防毒程序等，再新的病毒也能在短时间内被解决，可是对于Spyware、Trojan及Worms绝大多数网民防范意识较为薄弱。虽然一般的电脑上也安装了防毒程序，但实际上单一的防毒程序并不能阻挡来自网上的侵袭。数码周刊在此向大家介绍如何架构一个缜密的“三防”电脑防御系统，以保证上网安全。

害人四大新趋势

总体来说，以前的 攻击和犯罪的目的性不很明确，他们大多出于好奇、出风头的目的。而现在多是有组织、有目的的经济犯罪。据我们分析， 的攻击大致有如下四大趋势：

1.盗取个人资料

近年来利用Phishing攻击的犯罪增长非常快，主要出现在电子商务应用中。 假借银行之名给银行用户发电子邮件，提示银行系统升级要求用户重新注册，用户一旦轻信进行注册，银行账号即落入 掌中，与此伴随的将是你的银行存款不翼而飞。

2.“僵尸”入侵

从全球来看，僵尸即机器人(BOT)程序在中国的增长最快，而整个亚太区也居于全球前十名。BOT类似于木马程序，它执行的是预先没有设置好的程序，通过所有被程序控制的“僵尸”电脑一同对某一目标发起攻击。这种攻击的危险性最大，因为它不像病毒可以提前监控。

、Spyware偷袭

Symantec的技术中心曾在用户送修的笔记本电脑中发现，其已经被植入了多达近百种的Adware或Spyware软件，

它们一般通过小的用户在下载Flash和小游戏时安装，由于它们不像病毒和蠕虫那么敏感，于是得以在不知不觉中入侵你的电脑。现在一些正规的软件厂商也在应用这些软件来搜集用户的资料。尽管目前这类软件不见得都有害，但它们搜集的毕竟是你的个人隐私信息。这也将成为未来防范的重点。

4.垃圾邮件改头换面

从当前来看，垃圾邮件的总量虽然呈下降态势，但其逃避技术却越来越强。这类邮件中携带着大量的病毒、Phishing、蠕虫、木马及额外的风险。

三防靠六招

人们常常认为，只要安装一些单纯的网络防御产品就等于构建了一个完备的电脑防御系统。殊不知，这些还不足以构建起一个完善的网络整体防御体系，还需要在网络安全管理标准的指导下，通过网络安全管理整体解决方案，结合各种不同的网络防御技术和产品，在整体上维护网络和信息系统的安全。

1.基本防(杀)毒软件不可少

对于一般用户而言，首先要做的就是为电脑安装一套杀毒软件。只要是正规厂商的正版杀毒软件，任选一套即可。安装的步骤很简单，只要将安装盘放入光驱，按照系统的自动安装界面的提示选择安装\*\*杀毒软件→选择安装的语言版本→再一路NEXT即可。

2.个人防火墙设定是关键

在上述防病毒软件中都含有个人防火墙，所以可用同一张光盘运行个人防火墙安装，重点提示防火墙在安装后一定要根据需求进行详细配置。

各种防火墙的设置技巧有一定的共通之处，那就是在选择将目前上网中的“区域连线 ”→“设定值”的“服务”中的大部分连接协议剔除，只保留基本的HTTP、HTTPS、SMTP、POP3项目能够通过防火墙，按下确定后你的电脑就能防范大部分的蠕虫入侵了。

3.斩断Phishing鱼钩

反网络钓鱼组织APWG(Anti-PhishingWorkingGroup)最新统计指出，约有的网络欺诈是针对金融机构而来。从国内前几年的情况看大多Phishing只是被用来骗取QQ密码与游戏点卡与装备，但今年国内的众多银行已经多次被Phishing过了。可以下载一些工具来防范Phishing活动。

4.反间谍、广告软件必杀

要防范Spyware的话，除了需要在电脑上安装有如防毒程序的反间程序，时常监察及清除电脑的Spyware外。还要对将要在计算机上安装的共享软件进行甄别选择，尤其是那些你并不熟悉的，可以登录其 了解详情。此外，在安装共享软件时，不要总是心不在焉地一路单击“OK”按钮，而应仔细阅读各个步骤出现的协议条款，特别留意那些有关Spyware行为的语句。

推荐软件：MircrosoftAntiSpyware是一款专门针对Spyware的程序，支持Windows／XP／。它是用于监测和移除系统中存在的Spyware和其他潜在的不受信任程序的软件。可以减少因为这些软件带来的非法弹出广告窗口、计算机运行速度减慢、对Internet选项设置的随意改动，以及窃取私人信息的情况。但该软件还在测试阶段，所以应谨慎使用。

Adware和其他恶意程序相近，它们中简单的会出现在控制面板的添加或删除程序里，用户可直接把它们移除。不过大部分Adware为了掩人耳目都不会直接显示程序本体，要删除它们就需要利用一些针对性的软件。

5.自建网站黑名单

清除了广告程序后，并不代表已存在浏览器内的问题会自动被还原，还需要用户手动重新更改标题及首页。

6.训练软件认垃圾

相信拥有电子邮箱的用户都受到过不同程度的垃圾邮件(SPAM)骚扰，令人不胜其烦，特别是每每长假过后邮箱被塞爆之虞。为此，用户要做的就是安装一款电邮过滤程序，把SPAM过滤掉。

**县局网络安全工作总结16**

我校在网络安全教育周活动中，对全体师生普及了网络安全知识，使学生了解了更多的网络安全知识，认识到网络安全的重要性，掌握了防范网络安全的一般方法。

为提高全局干部职工的网络安全意识和安全防护技能，9月16日下午，市中区人社局专门组织干部职工集中观看了网络安全系列公益宣传片，宣传片涵盖网络安全法、网络安全金融知识、网络安全意识以及各种网络安全案例等，通过观看宣传片让干部职工切身感受到网络安全就在身边，从而推动大家主动了解和重视网络安全，自觉学习和掌握网络安全知识。

此次举办网络安全公益宣传片集中观看活动，是市中区人社局积极开展20\_年国家网络安全宣传周活动的一项重要举措。连日来，市中区人社局多项举措积极开展以“网络安全为人民，网络安全靠人民”为主题的网络安全宣传周活动。

一是积极安排部署。局领导高度重视，第一时间安排部署，由局办公室制定网络安全宣传周活动实施计划，收集和整理网络安全公益宣传片、宣传海报等资料。

二是广泛宣传发动。结合实际工作，利用微信公众服务号、公示公告栏、集中观看公益宣传片等多种方式积极为网络安全宣传周活动营造氛围，促进网络安全深入干部职工心中，确保网络安全宣传全覆盖。

三是主动自查整改。以这次网络安全宣传周活动为契机，在全局开展网络安全自查行动，动员全局干部职工积极查找在工作中、在生活中可能存在的网络安全隐患，对存在的网络安全隐患及时督促整改。

中央下发关于开展首届国家网络安全宣传周活动的通知后，xx省高度重视，省委迅速制定下发了《关于开展xx省首届“国家网络安全宣传周活动”的通知》，并制定了详细的活动方案。目前，整个活动正在有序推进：

1、xx月xx日上午，xx省委联合教育、工信、公安、通管、人行、新闻出版广电等部门，在x八一广场举行了网络安全宣传周活动启动仪式，省委常委、宣传部长姚亚平，政府副省长、省公安厅厅长郑为文出席活动仪式。同时，在现场举办了网络安全知识图片展、网络安全专家咨询活动，向市民免费发放了《网络安全基础知识手册》、《电信网络安全知识手册》、《金融网络安全知识折页》等资料。

2、xx月xx日至xx日，由xx省委主办，xx网承办，正在开展“网络安全知识”网上竞赛活动，并对成绩优秀者给予一定物质奖励，以调动网民参赛积极性。

3、xx月xx日，由xx省委主办，xx网承办，开展了网络安全专家网上在线访谈活动，通过专家讲解宣传并与网民互动，宣传普及网络安全知识。

4、整个网络安全宣传周期间，由xx省委主办，省移动、电信、联通等公司具体承办，在全省开展了“网络安全知识手机短信”免费推送活动。按照xx省委统一部署，各地各有关部门结合自身实际，也开展了系列丰富多彩的活动。此外，还制定下发了《xx省首届“国家网络安全宣传周活动”宣传报道方案》，对整个活动的宣传报道工作进行了详细部署。

近日，市局以“网络安全为人民、网络安全靠人民”为主题，扎实开展“国家网络安全宣传周”活动，营造起良好的网络安全环境。

**县局网络安全工作总结17**

我校在醒目位置悬挂了宽70厘米、长10米的横幅“共建网络安全，共享网络文明”，并及时召开了全体师生大会，少先队大队部号召全体学生重视网络安全，利用班会、主题队会认真落实网络安全知识活动的各项要求，强化学生网络安全意识的贯彻落实。从抓学生的网络安全意识入手，通过发放100份“致学生的一封信”，使学生和家长认识网络安全的重要性，了解网络安全的相关知识，开展了师生网络安全知识竞赛，激发了全体师生学习网络安全知识的\'积极性，学生的网络安全知识得到了普及。

**县局网络安全工作总结18**

聂利老师的《网络是把双刃剑》、王晓敏老师的《文明上网、守法尊规》等主题课，从不同角度提高了学生的认识，树立了文明上网，网络安全意识！

通过网络安全宣传周的系列活动，广大师生对网络安全知识已经有了更深刻的了解，能够自觉遵守《全国青少年网络文明公约》。我们相信希望通过大家共同的努力，可以使互联网越来越干净，越来越文明。

20xx年，网络管理科以两级关长会议精神为指导，按照“注重基础、加强监控、提高效率、安全稳定”的工作思路，加大科技基础建设，加强各系统运行监控，发挥职能管理，提高运行效率，确保关区网络、机房、视频会议等系统安全稳定运行。全年共加班46人次，共计210个小时，调整防火墙参数近100次，调整网络设备参数100余次，排除网络故障80余次，安装调试网络设备60余台。共维护总署视频会议12次，关区视频会议7次。

**县局网络安全工作总结19**

认真计划并组织华外学生通过线上参与网络安全知识竞赛，深刻了解网络安全教育活动的必要性。我校组织在校同学们进行了多种形式的网络安全知识的学习，并于26日下午参加教育部思政司组织的“全国大学生网络安全知识竞赛”。我校近千名学生参与了此次竞赛。在此活动中，同学们纷纷展现出了较高的积极性，并且取得了优异的成绩，部分同学在竞赛中获得了《全国大学生网络安全知识竞赛参与证书》。据参加竞赛的同学说：“其实竞赛的题目就是我们生活中常见的网络安全问题，通过竞赛这种方式能使我们更加深入的了解网络安全，从而更好的将安全的网络技术运用到学习和生活中。”

**县局网络安全工作总结20**

组织社区网格化管理员召开网络诚信宣传会议，借助网格员日常巡查，将网络诚信宣传带到居民身边，邀请居民共同参与到诚信网络建设中来。

一系列宣传学习举措受到了广大居民的大力支持，通过向社会多方宣传，为全社会营造了良好的绿色网络环境。大家表示，要从自身做起，文明上网、诚信上网，努力为未成年人创造和谐、文明、诚信网络文化，以实际行动努力营造网络文明新风尚。

按照陕西省教育厅办公室《关于开展陕西省教育系统网络安全宣传周活动的通知》要求（陕教保办〔20x〕15号）和《耀州区教育系统网络安全宣传周活动实施方案》，结合我校学生实际，制定了切实可行的网络安全教育周活动方案，在此方案的指导下开展了一系列工作，现将工作开展情况总结如下。

**县局网络安全工作总结21**

经过本次活动，全校师生对网络安全教育有了新的认识。对网络安全教育工作重视程度提高了，参与热情提高了，对网络的安全使用有了更深层次更全面的了解。

全校师生的网络安全意识明显提高。这次宣传活动，让全体师生基本树立了网络安全教育理念，认识到网络安全教育涉及到日常生活中的每一个人，认识到学习掌握应急知识的重要性，构筑出了网络安全的第一道防线，在增强师生们的网络安全防范意识和自我保护技能方面都取得了较好的效果。

我校是全县范围内最大的乡镇中心小学，现有学生1166人，教职工74人。随着计算机及其网络的普及与应用，我校近几年投入了不少经费用于购买了十余台办公电脑，并对学生用机进行了更新换代。学校现已基本实现了办公网络信息化，这无疑极大地提高了我校的工作效率，但也给我校网络信息安全工作带来了严峻考验。

**县局网络安全工作总结22**

根据区、市\_关于统计网络安全的相关要求，我局领导高度重视，及时组织相关人员按要求认真落实，迅速行动，认真组织开展网络系统的安全管理工作，目前各项工作进展有序。现将自查情况总结总结如下：

一、计算机和网络安全情况

（一）网络安全。我局所有计算机均配备了防病毒软件，明确了网络安全责任，强化了网络安全工作。

（二）日常管理。切实抓好内网、外网和应用软件管理，确保“涉密计算机不上网，上网计算机不涉密”，在不涉密电脑上粘贴“禁止处理涉密信息”警示条，严格按照保密要求处理光盘、硬盘、移动硬盘等管理、维修和销毁工作。

二、硬件、软件使用置规范，设备运行状况良好

为进一步加强我局网络安全，我局在机房加装了玻璃隔离门及空调，避免高温、电线短路等造成不必要的损失；为每台终端机都安装了防病毒软件，硬件的运行环境符合要求；目前路由器、防护墙和交换机等网络硬件设备运转正常，各种计算机及辅助设备、软件运转正常。

三、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、提高工作人员计算机技能。在设备维护方面，对出现问题的设备及时进行维护和更换，对外来维护人员，要求有相关人员陪同，并对其身份进行核实，规范设备的维护和管理。

四、网络安全存在的不足及整改措施

目前，我局网络安全仍然存在以下几点不足：一是内网线路不稳定，一时无法解决，网络运营商与设备运营商检查结果相矛盾，影响数据上报进度；二是干部职工安全防范意识较为薄弱。

针对目前我局网络安全方面存在的不足，提出以下几点整改办法：

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

2、加强我局计算机管理同志在计算机技术、网络技术方面的学习，不断提高我局计算机专管人员的技术水平。

**县局网络安全工作总结23**

某某局在市局党组的正确领导和大力支持下，高度重视网络与信息安全工作，确立了“网络与信息安全无小事”的思想理念，专门召开会议部署此项工作，全局迅速行动，开展了严格细致的拉网式自查，保障了各项工作的顺利开展。主要做法是：

一、计算机涉密信息管理情况

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。

二、计算机和网络安全情况

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。

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。

四、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，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。

五、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。

六、自查存在的问题及整改意见

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。

**县局网络安全工作总结24**

(一)部署总署高清视频会议系统

根据总署统一规划，调试开通我关到总署的“高清视频会议系统”。该系统单独使用我关到总署的2M专线，采用硬件系统，比较原软件方式的视频会议系统，画面质量、语音效果都有很大改善。全年共召开12次全国性视频会议。为确保全国海关电视电话会议系统在国庆期间随时可用，根据科技司要求，安排专人于国庆期间(9月21日至10月10日)，对总署视频会议系统开机值班，达到100%出勤率，圆满完成值班任务，受到总署科技司表扬。

同时，做好关区视频会议系统的保障工作。研究新的应用，在监控中心安装实现可视指挥的功能。全年共召开全关区视频会议7次，节省办公经费约112万元(按每次会议16万估算)。

(二)继续进行总关大楼综合布线工作

继续进行去年开始的大楼综合布线系统。一是对弱电井进行了清理改造。清理弱电井内线路，铺设防静电地板，安装接地箱。二是在中心机房迁移网络设备，安装骨干光纤、双绞线配线架。三是完成四层西厅办公区的装修、清理工作。由于大楼已经正常工作，工作时间不能够影响正常办公，而且对卫生、安全有较高的要求，所有工作必须在下班后和节假日进行，加班加点进行施工。截止到11月底，大楼综合布线验收测试工作已经完成。邀请山东省计算机网络质量监督检验站对我关综合布线系统进行抽测，共选取9个楼层的300个信息点和20对光纤。检测合格率达到100%，具备了验收条件。同时，做好大楼礼堂的综合布线和视音频信息点设计工作，确保大楼礼堂满足今后视频会议召开要求。

(三)进行关区网络升级改造

关区骨干网络自20xx年“三网改造”完成后基本没有大的变化。为满足不断增加的网络需求，同时根据关领导的要求，上半年启动了关区广域网网络升级改造工作。经过调研，确定采用MSTP线路和MPLS技术建设关区骨干网络。经过与电信运营商的多次协商，引进多家运营商竞争机制，大幅降低线路租费，为网络升级改造创造了条件。通过引入MPLS技术，能够增强关区网络的安全性，提高网络的可控性，实现业务及管理网传输的负载均衡及互备，实现关区视频监控图像在海关内部网上跨地市传输，提升关区网络平台的综合应用能力，对关区网络建设是一次重大的飞跃。为做好此项工作，我科根据处领导要求积极寻求总署支持，向总署科技司提交了技术方案，并顺利地通过了总署组织的专家组评审论证。

为解决网络改造出现的线路租费缺口，统一规范关区二级现场专线费用，与三家电信运营商签订全省线路资费框架性协议，规范收费标准，清除不合理收费。同时根据海关法和总署监管场所管理办法，将一部分专线费用改为企业支付，节省我关线路经费;经过清理，二级现场线路全年费用由原80多万减少到30多万，弥补了全省网络扩容经费需求。

目前该项目各项准备工作均已完毕，工程已进入实施前的模拟测试阶段。

(四)继续进行关区视频监控系统建设

根据关区视频监控系统建设统一规划，参与并制定大港、邮办、机场、黄岛海关全年的视频监控建设工作方案。配合港务局实现视频监控光纤入户，实现大港港区内的监控。加强对关区视频监控系统的指导和规划，先后到保税物流园区、日照和东营进行实地调研和指导。

针对宽视界传输方式的缺陷，积极探索视频监控网络传输的新模式。以东营海关为试点，采用“分段”的方式实现视频图像的传输，即：由监管场所至海关采用MSTP局域网方式传输，隶属海关再采用2M互联网接入方式，实现总关对其监控图像的实时查看。这种方式投入及运维成本均很低，且图像效果很好，可在关区内推广使用。此外，在该关还进行了视频图像异地存储的测试，确保保税仓库等无海关人员值守场所的监控图像异地保存在隶属海关，满足了监控要求。

(五)加强对外接入局域网联网建设

管理网对外接入局域网是我关对外接入的网络平台。为加强各直属关对外接入局域网的建设，总署下发了“海关管理网对外接入局域网安全建设指导方案”。我科对该方案进行深入研究，组织专题会与安全科、系统科等相关科室共同讨论，调研在我关的可行性，分析我关现状与总署要求的差距，逐步实现外单位与我关的规范接入。此外，今年在对外接入局域网推广了以下工程项目。

1、做好油气液体化工品物流监控系统的推广工作。

为落实总署党组关于加快物流监控系统建设进度的指示精神，进一步提高海关对进出口原油、成品油、液体化工品等商品的物流监控水平，根据总署要求，先后开通了龙口(龙口滨港液体化工码头有限公司)、日照(日照中石油)油汽液体化工品企业等9家企业与我关的线路连接，实现系统的数据传输。

2、实施“关库联网“工程。

为进一步加强税收入库管理，实现入库税收回执自动核销，实施青岛海关与青岛人民银行联网工程。经过积极与青岛人民银行技术部门沟通，制定符合我关实际的联网方案。

3、实施出口加工区联网工程。

按照加工贸易和保税监管改革指导方案的要求，为实现出口加工区信息化管理，实施了出口加工区联网工程。根据我关网络环境，兼顾可行性、安全性、可靠性的要求，我科制定详细联网方案，协调厂商完成了网络设备安装、联跳测试，实施了青岛海关与出口加工区联网工程。实现省内7个出口加工区通过方式接入我关管理网对外接入局域网。

**县局网络安全工作总结25**

一是加强学习，进一步提高认识。让群众认识网络安全的重要性，将网络安全落实到生活生产中，网络安全靠人民。二是建章立制，建立网络安全工作的长效机制。三是发现问题及时整治，确保网络安全活动取得实效。四是进一步加强宣传，营造氛围。

为进一步摸清网络设施底数，增强网络安全意识，落实网络安全主体责任，完善网络安全防护制度，有效防范网络安全事件的发生，按照上级文件要求，园林环卫局积极行动，组织人员开展网络安全自查。

局领导十分重视此次网络安全自查工作，按照“谁主管谁负责、谁使用谁负责”的原则，明确了管理责任。此次自查内容主要包括使用的网络和信息系统基本情况及网络安全管理、防护等情况。局领导按照工作分工对信息系统安全负责，结合自身情况及时制订各项安全管理制度，加强了网络安全技术防范工作的力度，进一步强化了办公设备的使用管理，做到责任明确，具体到人。针对这次自查中发现的问题，我局将组织全局工作人员学习有关网络知识，提高计算机使用水平，确保网络安全。

通过自查，园林环卫局全体干部职工的信息系统安全防范意识和信息资料保密意识得到了进一步增强，园林环卫信息系统安全防范能力得到了进一步提升，自查结束后，我局及时报送了自查报告，为全旗信息系统安全运行管理打下了坚实的基础。

根据凤城市教育局转发的辽宁省委网信办的文件精神，镇小学结合实际，加强领导，落实措施，切实做好了以“网络安全为人民，网络安全靠人民”为主题的宣传周的各项工作，现将活动总结如下：

**县局网络安全工作总结26**

1、建设五层办公区无线视频监控系统

根据处务会决定，进行五楼视频监控系统建设。采用无线技术，联系施工单位到五楼实地查看摄像头、监控主机安装施工位置，确定实施方案。完成四个摄像头更换、调整、测试、验收，目前系统已正式投入运行。

2、完成H986港区联网工程

规划大港港区内的光纤规划。利用港区建设视频监控的时机，完成港务局机房到老海关和H986办公楼的24芯光纤接入。这些光纤除满足港区内视频监控需要外，还能够实现数据传输，解决老海关到H986之间光纤紧张的问题，同时实现了H986的互联网接入。

3、进行机房UPS后备电池的扩容工作

为加强机房运行安全，增加机房电源后备供电时间，进行了UPS后备电池扩容工作。后备时间由45分钟提高到120分钟，大大增加了停电时后备电源的供电时间，使系统管理员有更充裕的时间进行备份和关机，提高了信息系统的安全。

4、完成对我关网关升级。

为解决电信3G无线联网不正常问题，对我关网关进行升级，并更换升级所有用户证书。同时配合系统运行科将武警执勤信息平台从管理网迁移到外联网，实现执勤武警通过互联网访问武警执勤信息平台。

**县局网络安全工作总结27**

县卫生局信息网络安全自查报告

根据县政府办公室《XX县人民政府办公室转发县经信委关于开展信息网络安全专项检查的工作方案和安徽省政府网站安全事件信息报告制度的通知》（X政办[]140号）的文件精神，我局高度重视，认真组织相关人员对我局的办公网络系统进行了全面检查，现将检查的情况报告如下：

一、自查情况

（一）信息网络安全组织落实情况。

成立了县卫生局信息网络安全工作领导小组，局长任组长，分管副局长任副组长，各医疗卫生单位主要负责人为成员，并设臵了专职信息安全员，做到了分工明确、责任到人。

（二）信息网络安全管理规章制度的建立和落实情况。

为确保信息网络安全，我局实行了网络专管员制度、计算机安全保密制度、网络安全管理制度、网络信息安全突发事件应急预案等以有效提高管理人员的工作效率。同时我局结合自身情况制定网络信息安全自查工作制度，做到四个确保：一是信息安全员于每周五定期检查单位计算机系统，确保无隐患问题；二是制定安全检查工作记录，确保工作落实；三是实行领导定期询问制度，由信息安全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网络知识，提高计算机使用水平，加强安全防范。

（三）技术防范措施落实情况。

一是制定了网络信息安全突发事件应急预案，并随着信息化

程度的深入，结合我局实际，不断加以完善；二是严格文件的收发，完善了清点、整理、编号、签收制度，并要求信息管理员严格管理；三是及时对系统和软件进行更新，对重要文件、信息资源做到及时备份，数据恢复；四是计算机由专业公司定点维修，并商定其给予应急技术支持，重要系统皆为政府指定的产品系统；五是涉密计算机经过了保密技术检查，并安装了防火墙。同时配臵安装了专业杀毒软件，加强了在防篡改、防病毒、防攻击、防瘫痪、防泄密等方面的有效性。安装了针对移动存储设备的专业杀毒软件；六是涉密计算机都设有开机密码，由专人保管负责。同时，涉密计算机不和其它计算机之间相互共享。对重要服务器上的应用、服务、端口和链接都进行了安全检查并加固处理。

（四）执行计算机信息系统安全案件、事件报告制度情况。 严格按照《安徽省政府网站安全事件信息报告制度》要求，由专职人员及时向有关部门报告。

（五）有害信息的制止和防范情况。

截至目前，暂未发现我局门户网站及政府信息公开平台存在散播不当政治言论等有害信息的现象，并安排信息安全人员定期浏览排查，及时发现问题。加强对卫生系统工作人员的信息安全宣传教育，提高信息安全防范意识和应急处理能力。

（六）党政机关保密工作。

制定了县卫生局计算机及网络的保密管理制度。办公系统的信息管理人员负责保密管理、密码管理，对计算机享有独立使用权，计算机的用户名和开机密码为其专有，且规定严禁外泄。

（七）重要信息系统等级保护工作开展情况。

按照国家信息安全等级保护有关要求,全面开展卫生系统信息系统的定级、备案和测评工作，对发现的问题及时进行整改。各单位对本单位信息系统进行定级，对二级以上的信息系统办理备案手续，对三级以上信息系统开展信息安全等级测评，根据测评结果，不符合要求的，制定了整改方案进行整改，并加强日常信息系统安全等级保护监督检查工作。

二、存在问题

根据《通知》的具体要求，在自查过程中也发现了一些不足，一是信息管理技术人员较少，信息系统安全方面可投入的力量有限；二是规章制度体系初步建立，但还不完善，未能覆盖信息系统安全的所有方面；三是个别职工保密意识还不够高，要加强防范意识；四是遇到计算机病毒侵袭等突发事件处理不够及时。

三、整改措施

针对以上自查中发现的隐患与不足，为进一步加强信息网络系统安全，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。

（一）强化应急响应机制建设。

制定周密的应急预案，加强应急技术支援队伍建设，认真做好应急演练、重大信息安全事故处臵、重要数据和业务系统备份等各项工作，确保信息系统安全正常运行。

（二）强化制度保障

一是以制度为根本，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；二是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）加强信息安全教育培训

建议举办信息安全技术培训班，对信息安全管理人员进行集中培训，以增强安全防范意识和应对能力，进一步提高政府信息系统安全管理水平。

（四）加强对单位干部的安全意识教育

加强对机关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，增强对计算机信息系统安全的防范和保密意识

**县局网络安全工作总结28**

根据上级网络安全管理文件精神，我站成立了网络信息安全工作领导小组，在组长李旭东站长的领导下，制定计划，明确责任，具体落实，对全站各系统网络与信息安全进行了一次全面的调查。发现问题，分析问题，解决问题，确保了网络能更好地保持良好运行。

一、加强领导，成立了网络与信息安全工作领导小组

为进一步加强网络信息系统安全管理工作，我站成立了网络与信息系统安全工作领导小组，做到分工明确，责任具体到人。安全工作领导小组组长为XXX，副组长XXX，成员有XXX、XXX、XXX。分工与各自的职责如下：站长XXX为计算机网络与信息系统安全保密工作第一责任人，全面负责计算机网络与信息安全管理工作。副站长XXX负责计算机网络与信息安全管理工作的日常事务。XX、XXX负责计算机网络与信息安全管理工作的日常协调、网络维护和日常技术管理工作。

二、我站信息安全工作情况

我站在信息安全管理方面，制定了一系列的管理制度。重要岗位人员全部签订安全保密协议，制定了《人员离职离岗安全规定》、《外部人员访问审批表》。存储介质管理，完善了《存储介质管理制度》。运行维护管理，建立了《信息网络系统日常运行维护制度》。

1、技术防护方面

系统安装正牌的防病毒软件和防火墙，对计算机病毒、有害电子邮件采取有效防范，根据系统服务需求，按需开放端口，遵循最小服务配置原则。一旦发生网络信息安全事故应立即报告相关方面并及时进行协调处理。

2、微软公司将自20xx年4月8日起，停止Windows XP桌面操作系统的用户支持服务，同时也停止系统和安全补丁的推送，由于我站部分计算机仍在使用XP系统，我站网络信息安全小组积极应对这一情况，对部分能够升级的电脑升级到了WIN7系统，对未能升级的内网电脑，我站联系上级信息安全部门对网络安全状况进行了评估，并修改了网络安全策略，保证了系统的安全运行。

3、应急处理方面

拥有专门的网络安全员，对突发网络信息安全事故可快速安全地处理。

4、容灾备份

对数据进行即时备份，当出现设备故障时，保证了数据完整。

三、自查发现的主要问题和面临的威胁分析

1、发现的主要问题和薄弱环节

在本次检查过程中，也暴露出了一些问题，如：由于投入不足，光电系统出现故障，致使系统设备停止运行，虽然不会丢失数据，但是服务会出现中断。

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对计算机安全意识教育和防范技能训练让干部职工充分认识到计算机泄密后的严重性与可怕性。

2、面临的安全威胁与风险

3、整体安全状况的基本判断

我站网络安全总体状况良好，未发生重大信息安全事故。

四、改进措施及整改效果

1、改进措施

为保证网络安全有效地运行，减少病毒和hacker的侵入，我站对相关网络系统操作人员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。

2、整改效果

经过培训教育，全体干部职工对网络信息安全有了更深入的了解，并在工作中时刻注意维护信息安全。

**县局网络安全工作总结29**

要求全体工作人员都应该了解网络安全形势，遵守安全规定，掌握操作技能，努力提高医院网络安全保障能力，提出人人养成良好网络安全习惯的六项规定。

1、禁止用非涉密机处理涉密文件。

2、禁止在外网上处理和存放内部文件资料。

3、所有工作电脑要设置开机口令。

4、禁止在工作网络设置无线路由器等无线设备。

5、严格做到人离开工作电脑即断网断电。

6、禁止在工作网络计算机中安装游戏等非工作类软件。

网络安全关系到民族的兴旺和国家的前途，树立网络安全意识，既是全社会的任务，更是学校教育的一项重要内容。根据《普及工作方案》文件精神，我校积极开展“网络安全”宣传教育活动，通过多种形式广泛宣传网络安全法律法规、政策文件，要求全体教师把学习宣传贯彻《网络安全法》摆在重要位置，充分认识贯彻落实《网络安全法》的重要性和紧迫性，采取多种形式广泛宣传普及《网络安全法》，大力营造良好舆论氛围，进一步推进学校网络安全管理工作，将《网络安全法》宣传教育纳入“七五”普法和法制教育宣传月活动中。现将活动总结如下：

扎实开展\_网络安全法宣传。在师生中普及宣传网络安全法的相关知识，增强网络安全意识。

开展“网络安全法”的主题班会。以“网络安全，人人有责”为主题，教会学生合理安排上网的时间，如何在网上选择性地浏览信息，如何在虚拟网络中自我保护，如何对预防病毒，让同学们清楚地认识到网络安全的重要性，更好的利用网络促进我们学习的进步。通过学习交流，增强同学们对网络安全知识的了解，清楚网络安全的重大意义，更加清晰地意识到维护网络安全人人有责。

此次宣传活动围绕“青少年网络安全”为主题，让学生通过图片、信息以及教师的讲解，体会网络安全的重要性，对学生提出了相关注意事项，通过各项活

为了加强学生树立网络安全的自我保护意识，提高网络安全防范技能，20xx年9月18日-23日，xx中心小学积极开展20xx年国家网络安全宣传周活动。

**县局网络安全工作总结30**

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。

**县局网络安全工作总结31**

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。

为了规范工作人员网络安全相关行为，提高网络安全意识，保护税收信息系统和电子数据的安全，规范计算机网络终端和存储介质的日常使用，为此我局将开展为期一个星期的网络安全检查工作。

**县局网络安全工作总结32**

聂利老师的《网络是把双刃剑》、王晓敏老师的《文明上网、守法尊规》等主题课，从不同角度提高了学生的认识，树立了文明上网，网络安全意识！

通过网络安全宣传周的系列活动，广大师生对网络安全知识已经有了更深刻的了解，能够自觉遵守《全国青少年网络文明公约》。我们相信希望通过大家共同的努力，可以使互联网越来越干净，越来越文明。

这是整理出来的老师课件中的总结，难免有遗漏。20\_/05/28 王志军 第一章

1，paive attack 以及 active attack 的基本含义； 2，Two types of paive attack； 3，Four types of active attack；

4，六种security services 的基本含义； 第二章

 1，对称加密算法的5个步骤及其含义；  2，对称加密算法的2个基本要求；

 3，对称密码体系与非对称密码体系的含义，块密码与流密码的含义；  4，对加密信息的5种密码学分析方法；

 2，AES替代DES和3DES的一些理由（从AES的优点，DES和3DES 的一些缺陷两个方面进行理解）

 3，掌握三种密码分组的操作模式；

 4，理解课堂上所提到的四种密钥分配方式； 

第三章

 1，掌握MAC 的基本含义；

 2，如何使用MAC进行信息验证；

 3，理解one-way hash函数的基本含义；  4，掌握Hash函数的6个基本条件；  5，理解HMAC  1，掌握公钥密码的基本结构；  2，公钥算法的三种典型的应用 ；

 3，掌握RSA公钥算法（一定要会计算）； 第四章

 1，Diffie-Hellman 密钥交换算法 ；  2，什么是数字签名的概念；

 3，什么是public-key certificates（公钥证书）；  1，什么是Kerberos；

 2，Kerberos的4个基本要求是什么；

 3，理解课堂上所讲的“简单授权协议”和“更为安全权的授权协议”；  1，什么是证书链（）；

 2，理解如何去得到一个用户的证书（）,主要是理解书118页图 ；  3， includes three alternative authentication procedures ； 第五章

 1，理解书125页，图中的三种服务类型(PGP)；  2, 理解RFC822电子邮件标准的基本格式；

3,了解 S/MIME协议的一些基本内容；

第六章

 1，理解IPSec的常见应用；  2，IPSec 常见服务有哪些；  3,理解传输模式与隧道模式；

 1，理解Anti-replay service的实现方法；

 2，理解AH协议的Transport 和 tunnel 工作模式；  3,理解ESP协议的Transport 和 tunnel 工作模式；  1，理解Authentication plus confidentiality的三种方式：

ESP with Authentication Option;

Transport Adjacency;

Transport-Tunnel Bundle；

 2，理解Oakley key determination protocol retains the advantages of Diffie-Hellman ； 第七章

 1，理解Web Security Threats的2种分类： in terms of paive and active attacks ； in terms of the location of the threat；

 2，理解SSL connection 以及SSL seion；

 3,理解SSL Record Protocol 所提供的2种服务；

 4,理解Figure (p 228, in book)中提到的 the overall operation steps of the SSL Record Protocol. 1，理解SET 的participants的含义；

 2，理解dual signature(双重签名)的含义和目的； 第八章

 1，理解SNMP 所包括的4个关键元素；  2，理解SNMP代理的功能； 第九章

 1，理解three claes of intruders ；

 2，理解paword file 保护的two ways ；  3，理解入侵检测系统的3个主要优点

本DOCX文档由 www.zciku.com/中词库网 生成，海量范文文档任你选，，为你的工作锦上添花,祝你一臂之力！