

春节后网络保障工作总结精选38篇

作者：小六 来源：网友投稿

本文原地址：<https://xiaorob.com/zongjie/fanwen/208641.html>

ECMS帝国之家，为帝国cms加油！

春节后网络保障工作总结1

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。

春节后网络保障工作总结2

6月1日至6月23日，自治区环保厅组织开展了全区环保系统网络安全自查工作。为做好相关工作，自治区污染物监控与信息中心按厅办要求，制定了《20__年全区环境保护行业网络安全检查工作方案》，并按照方案对我区三级环保机构网络与信息系统进行了全面检查，对环保厅本级在用的网站系统、邮件系统、自行监测系统、自行监测系统等15个信息系统进行了漏洞扫描和安全检测，并委托专业安全公司从外部进行了渗透测试。

通过检查，我区各级环保系统共有网络与信息系统77个，其中部署在互联网上系统有各级环保部门网站系统、自治区环保厅电子邮件系统、自治区环保厅企业自行监测平台等，部署在全区环保专网上的系统有重点污染源自动监控系统、排污费征收全程信息化系统、环境监察移动执法信息管理系统、建设项目管理系统等。

通过自查，各级环保部门在用的网络及信息系统未发现较大安全隐患，总体运行状况较为安全。

春节后网络保障工作总结3

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带来了严峻考验。

>一、切实加强组织领导，建立健全各项网络安全管理规章制度。

- 1、为确保学校网络安全管理工作顺利开展，学校特成立了校长任组长的网络信息安全管理领导小组，全面负责该工作的实施与管理。
- 2、建立健全了一系列的学校网络安全管理规章制度。包括：《校园网用户信息安全管理规定》、《学校网络信息安全保障措施》、《学生上机守则》、《计算机室管理制度》、《计算机室管理员职责》、《办公室电脑使用管理暂行规定》等。通过制定与实施、切实让相关人员担负起对信息内容安全的监督管理工作责任。

>二、认真开展好学校网站的备案工作。

按县局有关文件精神，我校迅速成立了专人负责学校网站备案工作。根据文件要求，在如实了解学校网站虚拟空间提供服务商的安全信息后，及时填写好相关材料报县科教局电教站，并由县电教站送市局进行审批。与此同时，我校自行到_门的网站上进行网上备案和进行重要信息系统安全保护登记备案工作。

>三、建立起了一支相对稳定的网络安全管理队伍。

我校高度重视网络信息安全工作的队伍建设。学校从在职教师中挑选出一批具有一定计算机知识的人员作为网络管理员和网络安全员，并保持队伍的相对稳定。此外，学校还购买了网络管理书籍供网管人员自学，并大力支持网管人员参加各级各类网络技术知识培训，从而大大提高了网管的业务素质和技术水平。

>四、计算机维护及其病毒防范措施。

学校电脑除去电脑室100台，另有24套多媒体电脑，日常维护工作量非常大。由于机器较多，日常出现故障的情况较为常见，为此，我校成立了专人负责学校计算机系统及软件维护，由于平日能及时有效地维护，因此学校内各计算机使用均正常，无出现重大故障。

目_络计算机病毒较多、传播途径也较为广泛，可以通过浏览网页、下载程序、邮件传播等方式传播。为了做好防范措施，学校每台机器都安装了杀毒软件，并定期自动升级，对发现病毒的机器及时的进行处理。多年来，学校机器无出现严重中毒情况，电脑内重要信息未出现泄露而造成重大影响事件。

>五、大力开展文明上网、安全上网等宣传教育。

春节后网络保障工作总结4

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

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：MicrosoftAntiSpyware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。

春节后网络保障工作总结5

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。

春节后网络保障工作总结6

根据县委网络办、县公安局、县工信局关于20xx年安福县网络安全执法检查工作方案的通知精神，我单位积极组织落实，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，对我单位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：

一、成立领导小组

为进一步加强网络信息系统安全管理工作，我单位成立了网络信息工作领导小组，由左小圆主任任组长，王明股长任副组长，下设业务股，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、我单位网络安全现状

我单位的政府信息化建设从20xx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。目前我单位共有电脑两百多台，采用防火墙对网络进行保护，均安装了杀毒软件对全单位计算机进行病毒防治。

三、我单位网络安全管理

为了做好信息化建设，规范政府信息化管理，我单位专门制订了建立了《人员管理制度》、《运维管理制度》、《外包管理制度》、《机房管理制度》等管理制度等多项制度，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，进一步规范了我单位信息安全管理。我单位定期或不定期进行网络安全监测，掌握网络最新安全运行情况，网络安全检查的主要手段有网络设备的报警检查、运维巡检平台的主机监测、服务启日志检查、安全漏洞扫描、物理机房安全检查等，我单位结合多种技术手段进行网络安全监测，对网络安全事件进行及

时的预警，极大的降低了信息系统的网络安全风险。此外，我单位在全单位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，有力地保障我单位政府信息网络正常运行。

四、网络安全存在的不足及整改措施

目前，我单位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。

针对目前我单位网络安全方面存在的不足，提出以下几点整改意见：

- 1、进一步加强我单位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，强化我单位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、加强我单位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，为我单位网络的稳定运行提供硬件保障。

五、对信息安全检查工作的意见和建议

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，由于我单位网络信息方面专业人才不足，对信息安全技术了解还不够，在其他兄弟乡单位或多或少存在类似情况，希望县委网络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。

春节后网络保障工作总结7

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。

>一、对全局的网络环境进行了优化整合。

配合专业公司和运营商做好线路的搭建设备的安装以及网络的测试，重新划分网段，规划内网ip地址，在州局下发部分设备的同时自筹资金XX万元采购了路由器等网络设备。

>二、做好网络节点的优化整改。

根据文件要求，对全局网络节点进行了进一步优化整改，做到设备线路整洁规范，保持环境的整洁干净，明确了一名网络管理及运维人员。

>三、做好系统和网络安全风险分析。

按照要求规范全局人员应用系统的岗位权限，加强机和网络设备管理，实行定期巡检制度，确保各项工作顺利开展。

>四、安排专人负责违规外联日常监控工作。

掌握各类违规外联事件产生的原因与监控机制，主动监控本级违规外联情况，及时核实与处置，以免事态进一步扩大。

>五、开展网络安全培训。

针对当_络安全存在的问题开展了一次全局网络安全知识培训会。

读书破万卷下笔如有神，以上就是虎知道为大家整理的4篇《网络安全保障工作总结》，希望对您的写作有一定的参考作用，更多精彩的范文样本、模板格式尽在虎知道。

春节后网络保障工作总结8

建设一个安全可靠、稳定可管理的网络已成为人们的共识，对校园网而言，这可能需要管理者们付出更大的努力。高校校园网服务于教学科研的宗旨，决定其必然是一个管理相对宽松的开放式系统，无法做到像企业网一样进行严格统一的管理，这使得保障校园网安全成为一个大挑战。

上海交通大学从自身情况出发，应用了以下六项措施保障网络安全。

措施1 网络交换路由设备的安全配置

根据不同控制策略的要求，对校园网边界路由器，各校区核心交换机，汇聚点交换机以及楼内三层交换机分级配置合理的访问控制列表(ACL)，从而保障网络安全。机制如下：

对蠕虫病毒常见传播端口和其他特征的控制，可以有效控制蠕虫病毒大面积扩散；

对常见木马端口和系统漏洞开放端口的控制，可以有效降低网络攻击和扫描的成功率；

对IP源地址的检查将使部分攻击者无法冒用合法用户的IP地址发动攻击；

对部分ICMP报文的控制将有助于降低Smuff攻击的威胁。

在网络安全日常管理维护和出现病毒爆发或其他突发安全威胁时，合理配置ACL将有助于快速定位和清除威胁。

措施2 采取静态IP地址管理模式

上海交通大学长期以来一直采用校园网用户静态IP地址管理模式。所有网络用户入网前需要事先从网络中心申请获取静态IP地址。网络中心收到申请后在用户接入的二层交换机上完成一次用户MAC-接入交换机端口的绑定，并在用户楼内三层交换机上实现用户IP-MAC的一一绑定，使用这种方法来确认最终用户，消除IP地址盗用等情况。虽然看上去比较复杂，但由于网络中心针对校园网中使用的各种不同厂家和类型交换机，都开发了相应的绑定程序，所有的绑定管理工作都由程序自动完成，所以管理人员的工作量并不大。网络中心的网管数据库里存放着全校范围内数千台接入交换机的端口-用户房间端口信息数据，以及所有用户的详细使用信息和相关IP-MAC资料，所有这些都为建立可管理的安全校园网提供了基础。

这种管理模式的好处很多：一旦出现扫描攻击，垃圾邮件等网络安全事件，根据IP/MAC/端口可以在第一时间迅速定位来源，从而为采取下一步处理措施提供准确的依据。这样一个完整准确的用户信息系统的存在，为以后构想中的网络自防御体系创造了条件。

措施3 中央集中控制病毒

在病毒的防控方面，学校采取中央集中控制管理的模式，统一采购网络版杀毒软件，免费提供给校内用户使用，使得病毒库可以及时快速升级。此外，建立一个校内网络安全站点，及时发布安全公告，提供一些安全建议和相关安全工具下载也是十分必要的。

在冲击波病毒爆发以后，网络中心开始思考如何应对由于微软操作系统漏洞引起的大规模蠕虫病毒感染，

当年就建立了微软软件更新(SUS)站点，给校园网用户提供微软操作系统补丁的快速自动更新。今年又建立了微软Windows软件更新(WSUS)站点和Linux系列操作系统的自动更新站点，提供操作系统、微软Office应用程序、SQL数据库的校内快速自动更新服务。因为WSUS的数据库里可以存储所有用户的更新信息，所以网络中心就可以掌握校内计算机的漏洞分布情况，并且谁装了补丁谁没装一目了然。为了普及校内计算机安装自动更新，尽可能的消除操作系统级别的安全隐患，我们计划于近期进行半强制性的安装。

措施4 积极防范网络攻击

我们在校园网边界出口部署了IDS，核心路由器上启用了NetFlow、sFlow等进行监控，对关键的网络节点通过端口镜像、分光等方式进行进一步分析处理网络数据包，通过部署基于Nessus的漏洞扫描服务器对校园网计算机进行定期安全扫描。

及时查看并分析处理这些监控数据和报表有助于在第一时间发现异常网络安全事件并进行处理，防患于未然。

实践证明，选用合适的软件和分析处理方式将会大幅度提高工作效率。商业软件固然不错，但很多开源软件如Etheral、Ntop、Nessus等在这些方面一样做得很优秀，并且易于用户根据自己的需要进行二次开发。

措施5 统一身份认证

对于无线网络的安全而言，用户接入认证是非常关键的。网络中心使用了校内统一身份认证来限制校外用户未经授权的无线访问。由于WEP认证具有天然的弱安全性，网络中心又同时提供了基于的认证平台进行校内统一身份认证并鼓励用户使用。

措施6 鼓励学生当网管

宿舍网的网络安全管理在很多学校往往是比较头疼的，上海交大网络中心在这方面取得了让学校师生满意的成绩，而且，网络中心也没有太多人力深陷其中。根本原因还是在学校有关部门的大力配合下，建立了一支由数百人组成的学生宿舍网管员队伍，每个楼都配有至少一名学生网管员，一般在楼内招聘。日常管理由学生工作部门负责，工资待遇纳入学校勤工助学体系，但网管员具体工作由网络中心加以指导。

通过培训这些学生网管员掌握基本的网络安全意识和基本技能，大量的网络安全问题都消失在萌芽状态。当处于病毒爆发期或有网络安全突发事件时，分布在全校各处的学生网管员也可以第一时间做出响应，协助网络中心的工作。

结束语

很多时候，校园网络安全管理人员都会发出这个感慨：发现病毒和攻击其实并不难，难的是面对层出不穷的大量病毒和攻击时，如何去快速响应处理。要实现网络安全，单单依靠网络中心的力量肯定是不够的，要动员各部门院系的力量，激发学生的兴趣和创造力，建立专门的网络安全队伍，通过培训等各方面途径来提高所有网络用户的网络安全意识。只有网络安全意识深入人心，才有可能创造出一个长期的良好的校园网安全环境。

春节后网络保障工作总结9

一、加强领导，落实人员保障

乡高度重视网络安全工作，年初召开党委会研究确定乡党委副书记、纪委书记曹英负责本乡网络安全工作，并由乡党政办具体承担网络安全管理工作，任勇兼职网络安全员，保障工作顺利开展。

二、健全制度体系，加强技术防护

年初，由具体承担网络安全管理工作的乡党政办起草了涵盖人员管理、资产管理、采购管理、外包管理、教育培训等方面的网络安全管理制度体系，并在分管领导审定并交乡党委会研究通过后以正式文件形式下发；按照国家网络安全政策和标准规范要求，建立健全了术防护体系及安全防护措施。按照分散管理模式对所有终端计算机、移动存储介质进行管理，各具体管理人员负责各自管理计算机防病毒软件安装、漏洞修复、密码设置管理等安全防护措施的实施，并由乡网络安全处进行监督检查，保障网络安全。

三、健全安全应急体系，加强宣传教育培训

按照国家网络与信息安全事故应急预案要求，建立健全了网络安全应急工作体系。按要求与重点岗位人员签订了安全保密协议，制定了人员离岗离职管理措施，今年全乡无重大网络安全事件发生；采用职工会统一组织学习、业余时间自学等方式对全乡干部进行了网络安全知识培训，各干部职工网络安全意识良好。

四、工作中的不足和困难

一是部分干部职工对网络安全工作的重视还不够，工作中仍存在许多网络安全隐患，如互联网上传输涉密信息等情况；二是由于本乡财政紧张，无充足资金购置密码设备、入侵检测设备、安全审计设备等硬件设备，只能在能力范围内进行网络安全防护，无法做到彻底消除网络安全隐患。

五、下一步工作打算及建议

在今后的工作中，乡将进一步加大对干部职工的教育培训力度，力争不出现网络安全事件。希望上级部门加大对乡镇网络安全的支持力度，落实经费保障，以便更好的开展工作。

春节后网络保障工作总结10

20xx年以来全乡严格执行《单位计算机网络安全管理制度》，全年未发生信息泄漏、网络入侵等安全事故，计算机网络运行良好，具体总结如下。

一、强化意识

领导重视为了加强计算机网络安全建设，我乡成立了专门的网络安全领导小组，成员由政法干部和乡纪委成员组成，乡长任组长。小组主要监督乡政府网络安全制度的执行，同时督促网络服务商做好线路检查、维修工作，以“防控结合，预防为先”的工作思路出发，提高政府部门网络信息安全能力，强化政府工作人员在网络化办公过程中的信息安全意识。最大限度地预防和减少了网络安全事故的发生，维护全乡网络信息安全。

二、措施得力

针对乡政府部门干部职工网络信息安全知识匮乏、安全技能低下的问题，乡政府专门组织了网络信息安全培训，参训率达100%，培训后还进行了考核，在操作人员的层面上有效保证了政府网络安全。通过制定和执行《单位计算机网络安全管理制度》，保证了在日常操作过程中的信息安全。通过在政府办公场所网络信息安全制度上墙，提高工作人员网络安全意识，形成网络信息安全常态化。

三、监管到位

乡网络安全领导小组联合乡纪委，利用群众路线教育实践活动作风建设为契机，狠抓网络信息安全，形成对网络安全违规行为形成高压态势。对不符合网络信息安全规定的行为及时制止，对违规操作人员进行及时教育，对造成不良后果的责任单位、责任人给与纪律处分计入个人档案，并与单位和个人的评先，晋级和奖金挂钩。

春节后网络保障工作总结11

20__年以来全乡严格执行《单位计算机网络安全管理制度》，全年未发生信息泄漏、网络入侵等安全事故，计算机网络运行良好，具体总结如下。

一、强化意识

领导重视为了加强计算机网络安全建设，我乡成立了专门的网络安全领导小组，成员由政法干部和乡纪委成员组成，乡长任组长。小组主要监督乡政府网络安全制度的执行，同时督促网络服务商做好线路检查、维修工作，以“防控结合，预防为先”的工作思路出发，提高政府部门网络信息安全能力，强化政府工作人员在网络化办公过程中的信息安全意识。最大限度地预防和减少了网络安全事故的发生，维护全乡网络信息安全。

二、措施得力

针对乡政府部门干部职工网络信息安全知识匮乏、安全技能低下的问题，乡政府专门组织了网络信息安全培训，参训率达100%，培训后还进行了考核，在操作人员的层面上有效保证了政府网络安全。通过制定和执行《单位计算机网络安全管理制度》，保证了在日常操作过程中的信息安全。通过在政府办公场所网络信息安全制度上墙，提高工作人员网络安全意识，形成网络信息安全常态化。

三、监管到位

乡网络安全领导小组联合乡纪委，利用群众路线教育实践活动作风建设为契机，狠抓网络信息安全，形成对网络安全违规行为形成高压态势。对不符合网络信息安全规定的行为及时制止，对违规操作人员进行及时教育，对造成不良后果的责任单位、责任人给与纪律处分计入个人档案，并与单位和个人的评先，晋级和奖金挂钩。

春节后网络保障工作总结12

学校接到重庆市巴南区教育委员会关于转发巴南区信息网络安全大检查专项行动实施方案的通知后，按文件精神立即落实相关部门进行自查，现将自查情况作如下报告：

一、充实领导机构，加强责任落实

接到文件通知后，学校立即召开行政办公会议，进一步落实领导小组及工作组，落实分工与责任人（领导小组见附件一）。鱼洞二小网络安全大检查专项行动由学校统一牵头，统一指挥，学校信息中心具体负责落实实施。信息中心设立工作小组（工作小组见附件一），小组成员及各自分工落实管理、维护、检查信及培训，层层落实，并坚决执行谁主管谁负责、谁运行谁负责、谁使用谁负责的管理原则，保障我校校园网的绝对安全，给全校师生提供一个安全健康的网络使用环境。

二、开展安全检查，及时整改隐患

1、我校网络中心、功能室、微机室、教室、办公室等都建立了使用及安全管理规章制度，且制度都上墙张贴。

2、网络中心的安全防护是重中之重，我们分为：物理安全、网络出入口安全、数据安全等。物理安全主要是设施的防火防盗、物理损坏等。网络出入口安全是指光纤接入防火墙—路由器—核心交换机及内网访问出去的安全，把握好源头。数据安全是指对校园网的数据备份、对不安全的信息进行处理上报、对信息的过渡等。信息中心有独立的管理制度，如网络更新登记、服务器资源、硬盘分布统计资料、安全日志等，便于发现问题，既时查找。

3、对我校几大网站的帐户、口令等进行了一次专门的清理检查，对弱口令进行等级加强，并及时将应用软件更新升级，我校是电信光纤专线接入互联网，采用思科硬件防火墙作为入口的第一道防线，然后是接入路由器，最后接入核心交换机，保证了我校网络接入互联网的几道很重要的过滤。网络中心服务器的杀毒软件是正式版本，能定时进行升级更新，每天对系统进行补丁升级，消除可能存在的一切安全隐患，我校对外的服务器有2台（FTP服务器、WEB服务器），FTP服务器只对外开放端口21，其余端口全部关闭。同样WEB服务器只开放端口80，其余端口全部关闭，在方便师生使用的同时，要保障网络的绝对安全，由于我校领导的高度重视，管理得当，我校从20_年建立校园网到现在，还没有任何攻入内网的记录。

4、强化网络安全管理工作，对所有接入我校核心交换机的计算机设备进行了全面安全检查，对操作系统存在漏洞、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。

5、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。每周定时对我校站的留言簿、二小博客上的帖子，留言进行审核，对不健康的信息进行屏蔽，对于反映情况的问题，备份好数据，及时向学校汇报。

6、本期第三周我校在教职工大会组织老师学习有关信息网络法律法规，提高老师们合理、正确使用网络资源的意识，养成良好的上网习惯，不做任何与有关信息网络法律法规相违背的事。

7、严格禁止办公内网电脑直接与互联网相连，经检查未发现在非涉密计算机上处理、存储、传递涉密信息，在国际互联网上利用电子邮件系统传递涉密信息，在各种论坛、聊天室、博客等发布、谈论国家秘密信息以及利用QQ等聊天工具传递、谈论国家秘密信息等危害网络信息安全现象。

三、存在的问题

1、由于我校的网络终端300多个点，管理难度大，学校没有多余的经费来购买正版杀毒软件，现在使用的是伪版的或者免费版本的杀毒软件，这给我们的网络安全带来了一定的风险。

2、我校的服务器共有5台，但我们没有一套网络管理软件，平时全靠人工手动去管理，管理难度大，所以平时难免有忘补丁升级的时候，这难免也存在一定的安全风险。

3、在学校，网管员不能专职来搞网络管理，一般都还要兼一个人的工作量，所以在网络管理上的精力有限，在网络管理、资源整理，安全日志记录上还有待于进一步提高。

总之，在后面的工作中，针对我们的不足及问题，努力整改，在现有的基础上，尽最大努力把我校网络安全工作做到更好，给全校师生提供一个安全健康的网络环境。也殷切期望相关领导给我们指点迷津，谢谢。

春节后网络保障工作总结13

作为一名人力资源和社会保障局的工作人员，我按照各项标准严格要求自己，认真完成领导交办的工作任务和本职工作，团结同事、虚心学习，创新工作方法，逐步提高自身素质，现将20xx年的主要工作总结如下。

一、加强学习、提高自身素质，工作中涉及的法律、法规都需要烂熟于心，针对这一问题，我利用工作闲暇时间努力自学有关人力资源和社会保障的各项法律、法规，相关政策，做到准确掌握法律、法规的使用尺度，确保调节改工作的合理性。

二、做好本职工作，完善各项技能，集中精力投入到了人力资源就业工作中来。

20xx年，全国就业形势严峻，尤其是高校毕业生，报考机关事业单位的人越来越多，这也加大了我们的工作，也要求我们更加认真细心工作，做到高效、准确、及时。

本着公开平等竞争的原则，及时公布各类招聘信息，认真审核各项资料，确保工作零失误，切实做到为人民服务。

三、做好各项档案资料的建立、健全。

完善档案管理制度，认真按照要求和政策贯彻工作。

在完成本职工作同时，我积极配合办公室的其他同志，加班加点建立健全各项档案，并顺利通过xx管委会考核组的考核。

今年，我在自己的岗位上，做了一些工作，也取得了些成绩，但这离不开领导、同事的关心与帮助，离领导、同事的要求还有很大差距，这主要表现在主动学习还不够，有时工作欠仔细、缺乏耐心，缺乏创新工作的本领，创造的成果还不多等方面。

在今后的工作中，我将努力改善和弥补，完善自身各项素质，力争在20xx年工作再上新台阶。

春节后网络保障工作总结14

北京冬奥会将于20_年2月4日至20日举办，北京冬残奥会将于20_年3月4日至13日举办。北京冬奥会、冬残奥会（以下简称“北京冬奥会”）是我国重要历史节点的重大标志性活动，是展现国家形象、促进国家发展、振奋民族精神的重要契机。为做好20_年北京冬奥会期间网络安全保障工作，根据XX网办发〔20_〕XX号文件要求，防范化解各类网络安全风险隐患，织密织牢XX网络安全防护网，保障XX网络安全运行平稳，制定方案如下。

一、总体要求 采取有力措施，切实加强网络安全防护，坚决防范网络安全重大风险和事件，严密防范敌对势力开展网络攻击破坏，为保障北京冬奥会顺利举办营造安全平稳的网络环境。

二、重点任务（一）加强网络安全防护管理。严格落实国家关于加强党政机关网站安全管理的相关要求，围绕针对党政机关重要信息系统、关键信息基础设施的篡改攻击、大规模拒绝服务

—2—攻击、钓鱼邮件攻击、勒索病毒攻击、供应链攻击、数据窃取泄露等突出现实威胁，责任部门进一步采取切实有效措施，加强网络安全防护管理，严密防范敌对势力攻击滋扰。

(二) 加强关键信息基础设施保护。组织开展关键信息基础设施网络安全监督检查，确保关键信息基础设施不发生重大网络安全事故。同时推进各区县科协、学会（协会、研究会）、企事业科协等基层科协组织做好关键信息基础设施安全保护工作，保障电信网和公共互联网持续安全稳定运行。

(三) 推进网络安全隐患排查。全面梳理 XX 系统资产设备、网络结构、网络边界、应用软件、业务流程、数据流等，加强对包含大量敏感信息和公民隐私信息、直接影响党政机关运转，以及事关国计民生、社会稳定与国家安全的业务系统的安全风险评估，及时发现问题并整改。

(四) 开展网络安全检查。加强公共互联网威胁专项治理，常态化组织网络安全检查。各区县科协、学会（协会、研究会）、企事业科协等基层科协组织开展网络安全专项检查，及时消除风险隐患，提高风险防范应对能力。

(五) 强化应急演练。完善网络安全事件应急预案，明确网络安全事件应急指挥机构、工作流程，组织开展网络攻防实战演练或以事件处置为核心的应急演练，做好相关人员

网络安全教育培训，提高网络安全意识和应急响应处置水平。并统筹组织好各区县科协应急处置准备和应急能力建设情况。

(六) 做好安全防范和应急准备。北京冬奥会期间，加强应急值守，畅通联络渠道，关键岗位、关键时间节点安全 7*24 小时在岗值班。发生或可能发生网络安全事件时，按照应急预案及时开展应急响应处置或应对准备。发生重大网络安全事件时，按程序第一时间报告，并加强舆情应对。

(七) 开展互联网保密检查。组织对本单位及各区县科协互联网攻击窃密和互联网上发布、储存、处理、传输涉密信息等违法行为进行实时监测和有效处置，严密防范失泄密情况发生。

三、工作要求 (一) 加强组织领导，压实工作责任。各区县科协、学会（协会、研究会）、企事业科协等基层科协组织要充分认识做好 20_ 年北京冬奥会网络安全保障工作的重要性和紧迫性，严格落实《党委（党组）网络安全工作责任制实施办法》要求，部署好网络安全保障工作，定期听取汇报，协调解决重大问题。各单位要抓好具体落实，明确职责要求，层层分解任务，压实主体责任，把责任落实到部门、岗位和个

—4— 人，做到领导到位、责任到位、机构到位、人员到位、经费到位和措施到位。

(二) 把握时间节点，扎实推进工作。XX 各部门要明确时间表、路线图，倒排工期，严格按照各时间节点完成任务。XX 宣传部要发挥统筹协调作用，组织做好网络安全检查工作，避免不必要的检查和交叉重复检查，全面掌握全 XX 系统网络安全检查结果与网络安全状况。

(三) 强化督导协调，严格落实责任。XX 宣传部会同各部门重点做好督导评估和跨部门协调，并将网络安全保障工作及时通报相关单位和部门。强化督导问责，对发生《XX 市党委（党组）网络安全工作责任制实施办法》第十八条所规定情形的，网络安全工作责任制落实不力且造成严重后果的，依照规定严肃问责。

XXX 局 20_ 年 11 月 28 日

春节后网络保障工作总结15

新的一年来临了，首先对春节值班的同事说声辛苦了，是他们的工作换取了大部分同事能够安全安心回家过个好年。下面对春节值班的一些情况做个总结。

> 基站保障：

本次春节保障历时 7 天，共计处理主设备故障 11 次，传输故障 3 起，温度告警 4 起，动力配套设备故障 42 起，发电 35 起。故障处理明细详见春节基站日报。

一：发电

春节期间长期发电情况是比较好的，基本上是完成了移动对长期发电站点的保障时间 8：00-23：00 之间不允许有退

服现象。几个长期发电的基站占了春节保障工作较大的比重，可以说保障任务较重。能够顺利的完成保障任务，得益于春节放假前保障准备工作，特别是发电值班人员的提前落实和单独安排。

二：故障

春节期间故障点可分为3类

- (1) 基站跳电现象比较多
- (2) 基站传输断发生率比较高
- (3) 载频故障发生比较频繁

1、基站跳电现象主要站点集中在农村比较潮湿的地区，但值班人员仍是第一时间对基站进行送电，春节过后将对这些基站进行空开更换。

2、传输故障时比较常见的故障，值班人员都能在第一时间进行处理跟踪。

3、载频故障多发的原因可能是春节期间话务量剧增，导致载频的承受能力导致损坏，值班人员仍然是当天进行了更换恢复。

三：重要事件

在2月7日，有工程部领导路过学前路和内环交界处发现在锦江之星楼顶有2个拉线塔其中有一个有倾斜的现象，我们值班人员第一时间赶到了现场，发现饭店楼顶并不是移动铁塔而是联通和电信的，并在第一时间通知了移动管理员。

四：通过这次春节保障可以总结春节基站告警处理的几个注意点

1、基站在业主单位的，春节期间业主可能会拉电，这类基站需要放假前提前和业主联系，尽量不要拉电。如果业主必须拉电，则需要和移动传输部门确认该基站传输是否需要跳纤，避免单个基站的断电给整个传输环网带来影响。

2、春节期间需要长期发电的基站，提前落实好发电人员单独安排值班表。另外对于长期发电的基站需要关注蓄电池的支撑时间，提前增加电池容量可以减轻节日发电值班人员的工作量。

3、春节保障除了人员的保障外，备品备件的提前准备也非常重要，没有备件就无法展开抢修工作。

4、春节期间除了值班人员值班外，回家的业务负责人和队长需要保持通讯畅通，便于值班人员抢修联系，保障迅速有效地开展抢修工作。

>室分保障：

20xx年2月2日至2月8号共发生36故障。其中监控故障12起、传输故障13起、投诉4起、网优工单2起、其他1起、TD故障4起。值班人员共处理好13起故障，剩余23起故障是由于工厂、商店放假拉电所引起。

>准备措施及问题的解决：

1、过年期间由于业主放假等特殊性质，监控故障、传输故障发生率较高并且处理难度大，对有室外覆盖的设备，涉及到放假拉电的及时和业主沟通，尽量春节期间给设备供电。

2、值班期间内的4起投诉，值班人员对投诉站点进行详细测试，并同网优人员一同对投诉站点进行勘察，耐心为投诉人解决，并解释原因，大部分投诉人表示理解。

假日期间值班人员坚持每天按平时工作时间到办事处集合，没有因私事临时请假，司机也积极配合，人员和车辆全

部坚守岗位，没有因个别原因对此次值班产生负面影响。今后将加强节假日值班人员，要求全体人员保持通讯畅通，确保及时有效的解决故障。

>集团施工保障：

为了保证春节期间的集团施工工作的布置、落实与安全，让部门员工度过一个欢乐、祥和的春节，努力确保期间的工作安全、有序、到位，集团施工主要进行了如下安排：

一、节前召开春节期间工作会议

1月30日下午在金置电脑广场一楼会议室，会上传达假期期间的安全工作要求，并对假期间工作进行安排与分工。

二、春节期间安全值班工作

春节期间值班人员的名单上报给监理单位与移动公司，确定信息联络员（7x24小时），务必保证相关人员通信畅通。

三、春节期间施工特殊要求

1、对于在春节期间停工的工程，尽快提交停工报告，交由监理单位，由监理单位及时

汇总并由移动公司存档。

2、节间如有特殊要求施工，负责人必须加强假期安全检查与指导工作，对下属的项目部及工地进行全面检查，对发现的工程项目安全隐患应及时整改，确保春节期间工程现场及工程材料等安全；

3、春节期间施工现场必须加强对工程现场的巡检工作，涉及有工程施工的现场，需提前通知监理人员到场进行监理；春节期间，施工单位要严格控制施工时间，遇暴雪、冰雹等恶劣天气需停止一切室外作业。

四、春节期间具体施工情况

假期间员工安全值班，无施工，无报修通知。

春节后网络保障工作总结16

为进一步做好先锋系列网站网络安全工作，根据文件要求开展先锋系列网站网络安全全面自查工作，现将我街道工作开展情况总结如下：

一、积极组织，明确分工。

二、强化学习，树立标杆。

重点温习《宣州先锋网络体系信息安全管理办法》、《关于做好当前几项重点工作的通知》及区宣传思想工作交流中分享的《“新中国成立__周年”，这18种不规范表述请注意！》等相关内容，针对政治术语尤其是涉及到党和国家主要领导的姓名、职务，党的最新理论成果等准确表述及撰写工作报告、信息时应如何正确表达，怎么样合理组织语言文字，形成结构最优且连贯流畅文本做出标准，并要求全体机关工作人员以此为范本严格按照要求编撰工作信息、审查信息内容。

三、全面自查，获有成效。

街道协助各村对先锋系列网站发布的信息进行全面、细致、严谨排查，对照梳理相关要求及标准，认真核查各类工作信息内容并立即改正发现的错误。目前排查出问题若干，成效明显，其中：

1、1篇图片新闻只存在标题无内容，对此立即查阅相关资料并补充工作内容；

- 2、主题活动报告类7处措辞不规范，现均将“纪念”改为“庆祝”，“建国”改为“新中国成立”；
- 3、部分村“本地概况”、“领导班子”栏未及时更新，导致职责分工不明确且相关数据出现错误，目前已根据实际更正相关信息，并切实加强网站维护与管理；
- 4、文本排版及分布问题2处，1处文字字体不统一，1处图片未上传成功；
- 5、3篇空白文档，已删除；
- 6、8处错别字、6处语法错误均已改正。

另，各村均对网站密码进行修改，增加密码安全系数。

春节后网络保障工作总结17

为进一步提高财政网络安全管理，不断增强网络信息的安全性，区财政局近期对全局财政专网和互联网网络进行了安全自查。

自查重点从机房设备管理、内外网分离管理、“双微”管理和个人计算机管理使用等四个方面开展，按照“谁主管谁负责、谁运行谁负责”的原则和“谁使用、谁管理、谁负责”的要求，对财政业务系统和计算机逐个进行自查，并结合正在进行的财政专网计算机杀毒软件升级工作同步开展，确保检查能真正发现问题和薄弱环节。对在自查发现的U盘使用不规范、电脑未设密码、业务软件密码简单或使用默认密码等网络信息安全意识不强的问题及时进行了整改和教育，印发了铜印财发《铜川市印台区财政局》，制定完善了制度机制。

通过此次检查和整改，进一步加强了全局网络安全工作，增强了网络信息管理和使用人员的安全意识，推进网络安全工作规范化、制度化和常态化，提高了全局网络的安全水平。

春节后网络保障工作总结18

为进一步做好先锋系列网站网络安全工作，根据文件要求开展先锋系列网站网络安全全面自查工作，现将我街道工作开展情况总结如下：

一、积极组织，明确分工。

二、强化学习，树立标杆。

重点温习《宣州先锋网络体系信息安全管理办法》、《关于做好当前几项重点工作的通知》及区宣传思想工作交流中分享的《“新中国成立70周年”，这18种不规范表述请注意！》等相关内容，针对政治术语尤其是涉及到党和国家主要领导的姓名、职务，党的最新理论成果等准确表述及撰写工作报告、信息时应如何正确表达，怎么样合理组织语言文字，形成结构最优且连贯流畅文本做出标准，并要求全体机关工作人员以此为范本严格按照要求编撰工作信息、审查信息内容。

三、全面自查，获有成效。

街道协助各村对先锋系列网站发布的信息进行全面、细致、严谨排查，对照梳理相关要求及标准，认真核查各类工作信息内容并立即改正发现的错误。目前排查出问题若干，成效明显，其中：

- 1、1篇图片新闻只存在标题无内容，对此立即查阅相关资料并补充工作内容；
- 2、主题活动报告类7处措辞不规范，现均将“纪念”改为“庆祝”，“建国”改为“新中国成立”；
- 3、部分村“本地概况”、“领导班子”栏未及时更新，导致职责分工不明确且相关数据出现错误，目前已根据实际更正相关信息，并切实加强网站维护与管理；

- 4、文本排版及分布问题2处，1处文字字体不统一，1处图片未上传成功；
- 5、3篇空白文档，已删除；
- 6、8处错别字、6处语法错误均已改正。

另，各村均对网站密码进行修改，增加密码安全系数。

春节后网络保障工作总结19

20_年网络安全宣传周活动方案（一）

为进一步普及网络安全知识，增强网络安全意识，营造安全、健康、文明的网络环境，保障师生在网络空间的合法权益，切实维护国家网络安全，根据《xx省教育厅办公室关于组织开展20_年网络安全宣传周有关活动的通知》精神，决定在全市中小学校开展20_年网络安全宣传周活动，现将有关事项通知如下：

一、活动时间20_年9月5日至9月11日。

二、活动主题和总体要求 今年网络安全宣传周主题为“网络安全为人民、网络安全靠人民”。各校要围绕活动主题，深入学习贯彻网络强国战略思想，学习贯彻全国网络安全和信息化工作会议上的重要讲话精神，通过组织动员广大师生广泛参与，深入宣传国家网络安全工作取得的重大成就，宣传贯彻《网络安全法》及相关配套法规，普及网络安全意识和防护技能，营造健康文明的网络环境，共同维护国家网络安全。

三、活动内容 1.举办网上网络安全宣传进校园讲座。

在9月8日校园日活动当天，省教育厅将邀请网络安全领域专家通过教育广场(xx)开设一期网络安全专题讲座。讲座重点围绕宣传网络安全相关法律法规及普及如何防范网络诈骗等知识。讲座内容将制作成视频资源通过教育广场供师生点播学习。各校要组织师生在网络安全

宣传周期间特别是校园日当天观看学习。

2.制作形式多样的宣传作品。

在校园内张贴网络安全知识海报、宣传活动网页和网络安全有关文章，发放宣传材料;开展网络安全问卷调查、组织网络安全测试，发送网络防范提醒等;通过校园网络、广播、宣传栏、微博、微信等多渠道介绍网络安全知识，引导和带动师生全面了解和积极参与，扩大宣传教育的覆盖面，增强师生网络安全意识和防范意识。

3.利用网络安全宣传专栏进行宣传活动。

依托网络安全宣传专栏，重点宣传贯彻网络强国战略思想，宣传贯彻全国、全省网络安全和信息化工作会议精神;宣传国家、我省网络安全工作取得的重大成就;深入宣传《网络安全法》及相关配套法规，普及网络安全知识，提升师生网络安全意识和防护技能。

4.进行网络安全隐患排查。

对机房设备和网站及其他信息系统的安全状况进行自查，排查可能存在的安全隐患，同时对机房计算机、办公室计算机进行安全排查，重点检查涉密文件的处理方式是否符合规范，软件和硬件是否符合国家有关要求。

四、活动要求 1.各校要高度重视网络安全宣传周活动，成立网络安全宣传周活动工作小组，根据本校实际情况，制订切实可行的网络安全宣传周工作方案，积极组织师生参与宣传教育活动，充分调动学生的积极性、主动性和创造性。各校还要积极创造条件，在9月8日校园日当天开展网

络安全宣传进校园、进课堂等活动。

2.各校要紧紧围绕活动主题，积极运用校内外宣传媒体特别是新媒体方式，报道宣传周有关活动，播放网络安全公益广告，推介网络安全作品，提升宣传效果，营造安全上网、依法上网的良好氛围。

3.各校要以宣传周为契机，加强与网信、公安等部门协作，探索建立青少年学生网络安全教育长效机制;要推动相关内容纳入新生教育、课程教育和课外实践活动，完善网络安全教育工作体系，切实增强教育实效。

4.各学校在组织该项活动开展过程中，注意保存相关音频、视频、图片和文字等资料，切实做好该项工作总结。

20_国家网络安全宣传周活动方案（二）

一、活动主题 网络安全为人民，网络安全靠人民 二、活动时间 9月5-11日，其中9月8日为教育主题日。

三、活动安排（一）举办全校大学生网络安全知识竞赛 9月5日至10月31日，各系组织学生参加“全国大学生网络安全知识竞赛”，通过网络答题方式普及网络安全知识。激发学生学习和网络安全知识兴趣，提升网络安全防护技能。

竞赛网址：xxx 任务单位：院团委

（二）开展网络安全教育专题活动 1.网站宣传 在学院网站首页开辟网络安全专题，发布相关安全知识、法律法规及学院相关活动，并组织相关资料供广大师生下载使用。

负责部门：党委宣传部 2.设计网络安全宣传橱窗、电子标语及摆放宣传板 在学校×区设计放置宣传橱窗，×区主干道及学生主要活动区域发送电子宣传标语、摆放宣传板，积极营造网络安全文化氛围。

任务部门：党委宣传部 3.微信推送 通过学校微信面向全校师生进行网络安全信息推送。

任务部门：党委宣传部 4.校园广播宣传 活动期间，校园广播站广播有关网络安全的常识，提高师生网络安全意识。

任务部门：党委宣传部 5.团日主题班会 各系部根据实际情况，组织开展“网络安全宣传周”团日教育活动，以视频、实例、线上线下互动交流等方式，组织学生学习和网络安全知识，提升网络安全意识。

任务部门：学生处、院团委 四、工作要求

1.高度重视，加强组织领导。举办网络安全周活动是贯彻落实中央关于网络安全和信息化战略部署的重要举措，各系部要高度重视，组织师生积极参与宣传教育活动，充分调动学生的积极性、主动性和创造性，推动活动形成声势。

2.突出主题，注重工作实效。要紧紧围绕活动主题，将网络安全教育与学生思想政治教育、文明校园建设、维护校园稳定等工作有机结合，提升工作的针对性与实效性，营造校园安全上网、依法上网的良好氛围。

3.加强协作，建立长效机制。以安全周为契机，探索建立青少年学生网络安全教育长效机制。推动相关内容纳入新生教育、课程教育、团日活动和课外实践活动，完善网络安全教育工作体系，切实增强教育实效。

4.严守规定，务实高效。要坚决贯彻执行中央八项规定有关要求，严格按照勤俭节约、务实高效原则，着力在活动实效上下功夫，严禁铺张浪费、大讲排场和各种形式主义。

20_年国家网络安全宣传周活动方案（三）

为增强校园网络安全意识，增强广大师生网络安全意识，提高网络安全防护技能，夯实文明建设基础，传播文明风尚，弘扬文明精神，扎实推进社会主义核心价值观体系建设，特制定xx中学校园网络安全宣传周活动方案：

一、活动主题

“网络安全伴我行”

二、活动时间

20_年9月5---9月11日三、组织机构为搞好“20_年国家网络安全宣传周活动”组织工作，确保该项工作在学校的顺利实施，学校成立了“网络安全宣传周”活动工作领导小组：

组长：xx 副组长：xx 成员：xx 四、活动内容

1.国旗下讲话 利用9月6日周一升旗仪式,宣传网络安全活动的方案、活动的要求,引导和带动师生全面了解和积极参与，扩大宣传教育的覆盖面，增强师生网络安全意识和防范意识。

2.网站宣传?

在学校网站首页开辟网络安全专题，发布相关安全知识、法律法规，并组织相关资料供广大师生下载学习使用。

3.开展网络安全知识进课堂活动

宣传周期间，全校利用班会和读报时间统一安排各班学习《学生网络安全教育》。

4.召开网络安全知识主题班会

在全校各班召开“网络安全伴我行”主题班会,讨论宣传网络安全知识，提高学生网络安全意识，增强识别和应对网络危险的能力。

5.校园广播站

利用校园广播站,设置专栏节目，在全校范围内反复宣传网络安全知识。

五、工作要求

1.高度重视，加强组织领导 举办网络安全周活动是贯彻落实中央关于网络安全和信息化战略部署的重要举措，学校要高度重视，组织师生积极参与宣传教育活动，充分调动学生的积极性、主动性和创造性，推动活动形成声势。

2.突出主题，注重工作实效 要紧紧围绕活动主题，将网络安全教育与学生思想政治教育、文明校园建设、维护校园稳定等工作有机结合，提升工作的针对性与实效性，营造校园安全上网、依法上网的良好氛围。

3.加强协作，建立长效机制 以安全周为契机，探索建立青少年学生网络安全教育长效机制。推动相关内容纳入新生教育、课程教育，完善网络安全教育工作体系，切实增强教育实效。

4.严守规定，务实高效。

要坚决贯彻执行中央八项规定有关要求，严格按照勤俭节约、务实高效原则，着力在提高活动实效上下功夫，严禁铺张浪费、大讲排场和各种形式主义。

网络安全宣传周活动方案(四) 一、活动主题：网络安全为人民，网络安全靠人民

普及网络安全知识，旨在提高我校全体师生网络安全自我保护意识，提升网络安全问题甄别能力。

二、活动时间：9月5日至9月11日 三、活动内容 以“净化网络环境，安全使用网络”为目标，统一使用“国家网络安全宣传周”活动标识，普及基本的网络知识，使广大师生员工增强网络安全防范意识，提高网络安全防护技能。

四、活动形式 1、标语宣传 在我校LED

滚动屏循环滚动“网络安全为人民，网络安全靠人民”等网络安全宣传标语。

2、消息推送 通过办公系统、邮件系统等推送网络安全宣传周相关精神和网络安全手册等。

3、开办专栏 在我校网络服务站点上开辟“网络安全”专栏，普及基本的网络知识，使广大师生员工增强网络安全防范意识，提高识别和应对网络安全威胁的能力。

- 4、视频短片 通过校园网及有线电视网络播放网络安全的相关视频。
- 5、安全培训 面向我校各部门的网络管理员进行网站安全防护专项培训，提高我校二级站点的安全防护能力。
- 6、网络协会 加强对网络协会的安全培训，通过网络协会面向学生普及网络安全知识。
- 7、活动总结 现代教育技术中心 网络安全宣传周活动方案（五）

为了进一步增强全区教育系统网络安全意识，提高网络安全防护技能，按照x省教育厅办公室《关于开展x省教育厅系统网络安全宣传周活动的通知》要求，区教体局决定在全区教育系统开展网络安全宣传周活动。现将有关事项通知如下：

一、活动目的 目前，全区各中小学、幼儿园全部达到了光纤网络校校通，实现了网络校园全覆盖，部分学校还建设了无线网络应用环境。为进一步推动我区教育网络建设，提升教育网络安全教育管理水平，深入开展网络安全宣传周活动，培养广大师生绿色上网、文明上网意识和良好习惯，增强师生网络安全防护能力，加强网络安全教育宣传，强化各项管理措施，全面构建全区教育系统文明、安全、和谐的网络环境。

二、组织机构 为了搞好本次活动，区教体局成立了网络安全宣传周活动领导小组：

组长：xx 副组长：xxx xxx

成员：各乡镇(街道)教育助理员;各中小学校长、幼儿园园长。

三、活动主题 本次活动主题为“网络安全知识进校园”，旨在提高青少年网络安全自我保护意识，提升其网络安全问题甄别能力。

四、活动时间 20_年9月5日至11日。

五、活动内容 开展网络安全宣传周活动，旨在引导广大师生和家长正确认识互联网，依法管理和使用互联网，自觉抵制网络危害，远离网络违法犯罪陷阱，带动全社会共同营造良好的网络环境。各学校通过开展形式多样的网络安全宣传活动，积极倡导师生文明上网、安全上网、绿色上网，大力宣传涉网案件防范基本知识，使广大师生成为积极参与活动、主动教育宣传、坚决抵制恶习、养成良好上网习惯的网络安全践行者，使学校率先成为我区文明、安全、和谐的网络育人基地。

- 1、学习网络安全方面的相关政策、法规、文件，了解目_络安全方面的动态信息。
- 2、召开学校网络安全工作会，总结本校在网络安全维护工作方面所采取的措施和取得的成效。
- 3、采用多种形式进行网络安全宣传，普及基本的网络安全知识，使教师、学生增强网络安全防范意识，具备识别和应对网络危险的基本能力。

六、活动形式

各学校可结合各自实际情况，充分利用校园网络、电子屏、板报、校刊、手抄报等多种媒体，采用专题会议、主题班会、演讲比赛、安全征文等多种形式，开展网络安全主题宣传活动。本次网络安全宣传周活动建议采取以下形式开展：

- 1、悬挂网络安全宣传横幅。

各学校应在宣传活动期间在本单位人流量较多的场所悬挂横幅，横幅内容为“共建网络安全，共享网络文明”。

- 2、开办网络安全宣传专栏。

各学校应在本单位宣传栏上开辟一个网络安全宣传专栏，结合黑板报、手抄报等多种形式，编写一期网络安全黑板报，对网络安全相关知识进行宣传。

3、举办网络安全宣传讲座。

各学校可根据本单位情况，邀请网络安全方面的专家为师生开办一期专题讲座;或利用“班班通”设备收看一场网络安全宣传片;或在“校园电视台”组织一次网络安全讲座或广播;或组织各班召开一次网络安全主题班会，学习网络安全相关知识。

4、开展网络安全知识竞赛。

为调动师生的积极性，各学校应组织师生开展网络安全知识竞赛或测试，竞赛内容应紧扣本次活动主题。

5、发放网络安全宣传传单。

各学校应制作电子版或纸质版网络安全宣传传单，采取“致家长、学生一封信”、开展网络安全问卷调查等方式，向学生及其家长发放，

引导和带动师生、家长全面了解和积极参与本次活动。

七、活动要求 1、本次活动时间紧、任务重。各乡镇要认识到新形势下网络安全进校园工作的紧迫性，认认真真、扎扎实实地组织学校开展此项活动。要落实专人负责，尽快制定活动方案，安排部署该项工作，确保网络安全宣传活动走进每一所学校。

2、各学校要高度重视此次宣传活动，落实工作责任。要结合活动主题，认真组织有关人员全面准备宣传内容。要精心谋划、创新形式开展系列宣传教育活动，提前做好每项活动的人员、时间安排。要动员和组织广大师生和家长积极参与，各个学校要按照活动计划，分阶段、分层次推进网络安全宣传活动，让每一名在校师生都普遍接受一次网络安全教育。

同时，各校要开展一次清理清查活动，全面掌握学校网络设备、网络接入点、上网计算机的管理情况(特别是无线接入点的管理)，了解师生网络安全防范基本信息。各校要认真查找薄弱环节，不断完善管理措施，改进宣传教育方法，全面提升网络安全管控能力，并建立长效机制。

春节后网络保障工作总结20

根据《关于开展xx区政务信息系统网络安全专项整治工作的通知》文件精神，区xx局党委高度重视网络安全工作，强化网络安全管理，按照“健全机制，狠抓落实”的工作思路，大力开展网络安全自查自纠、整改加固等网络安全防护工作，取得良好成效。现将我局网络安全整治情况总结如下：

一、加强组织领导，健全安全机制 为了加强对网络安全专项整治行动的组织领导，确保本次专项行动的顺利开展，我局通过局委会议讨论，结合我局工作实际，确定了分管网络安全的局领导为主要责任人，综合科为统筹责任部门，具体负责规划、指导、协调全局网络安全整治行动，各相关科室相互配合的工作机制。局党委十分重视网络安全补缺维稳工作，要求各科室要积极主动，开展信息系统底数的全面排查，将网络安全专项整治作为一项重要内容纳入科室日常工作当中，落细落小落实，常抓不懈。

二、加强学习宣传，增强安全意识

面对形势日益严峻的网络安全问题，我局充分认识到网络安全工作的极端重要性和紧迫性，深入开展网络安全理论

知识学习，积极组织引导各相关业务科室人员打破学习理念上的定性思维和惯性模式，采取“自学+集中学”的学习形式将网络安全理论知识与实际操作充分融合，突出理论学习的实用性，加强网络安全理论学习宽度；结合每周二晚“知行学堂”制度，由上至下，领导干部带头学，加强网络安全理论知识学习长度；创新宣传、学习载体，采用微信群、QQ群、钉钉群等互联网客户端完成线上学，各支部集中学习等方式实现线下学，加强网络安全理论知识学习广度。截至目前，共完成《网络安全等级保护条例》《_网络安全法》等多项法规学习，支部集中学习x次。

通过全局党员领导干部的努力，我局及时建立了网络安全维护工作机制，广泛普及了基础网络安全知识，修补了单

位网络系统安全漏洞，切实提高了网络安全防护质量。但同时也暴露出部分工作人员掌握信息不全面、学习主动性不强、学习碎片化等问题。下一步，我局将进一步理顺关系，严格按照网络安全防护工作相关要求，加强信息共享和力量整合，以更高热情确保网络安全保障常态长效。

春节后网络保障工作总结21

在今后的'工作中，乡将进一步加大对干部职工的教育培训力度，力争不出现网络安全事件。希望上级部门加大对乡镇网络安全的支持力度，落实经费保障，以便更好的开展工作。

为进一步提高财政网络安全管理，不断增强网络信息的安全性，区财政局近期对全局财政专网和互联网网络进行了安全自查。

自查重点从机房设备管理、内外网分离管理、“双微”管理和个人计算机管理使用等四个方面开展，按照“谁主管谁负责、谁运行谁负责”的原则和“谁使用、谁管理、谁负责”的要求，对财政业务系统和计算机逐个进行自查，并结合正在进行的财政专网计算机杀毒软件升级工作同步开展，确保检查能真正发现问题和薄弱环节。对在自查发现的U盘使用不规范、电脑未设密码、业务软件密码简单或使用默认密码等网络信息安全意识不强的问题及时进行了整改和教育，印发了铜印财发《铜川市印台区财政局》，制定完善了制度机制。

通过此次检查和整改，进一步加强了全局网络安全工作，增强了网络信息管理和使用人员的安全意识，推进网络安全工作规范化、制度化和常态化，提高了全局网络的安全水平。

为进一步做好先锋系列网站网络安全工作，根据文件要求开展先锋系列网站网络安全全面自查工作，现将我街道工作开展情况总结如下：

春节后网络保障工作总结22

为贯彻落实国家网络安全宣传周活动，响应教育上级部门的号召，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，现将我校网络安全教育工作总结如下：

一、通过多种渠道的宣传方式，提升全校学生的网络安全意识。

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。

二、通过组织学习及参与网络安全知识竞赛深刻了解网络安全教育的重要性。

认真计划并组织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。在此活动中，同学们纷纷展现出了较高的积极性，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。”

三、开展“网络安全精彩一课”教育活动。

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，主讲人李霏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。

春节后网络保障工作总结23

园区：2月2日至2月8日春节放假期间共发生3起故障，其中互联网故障2起、数据专线故障1起。2起互联网故障均是反映某国外网站打不开，原因是由于上端数据链路出口出现问题，更改链路路由后客户恢复正常。1起数据专线故障是由于客户端停电后再开电造成传输设备吊死，重启传输设备后恢复正常。三起故障发生后我部人员第一时间与客户取得联系并及时帮客户恢复业务，并没有因为放假期间而耽误客户故障抢修。

吴江：2月2日到2月8日春节期间共处理8起故障，其中集团集户5起，小区宽带3起。

集团客户报障分别为3家话吧和2家合作厅，具体信息如下：3家话吧故障原因为客户端路由器及设备电源问题所引起的故障。2家合作厅的故障分别是基站板卡吊死及客户端PDH设备坏所引起的故障。2月2日到2月8日春节放假期间共处理小区故障3起，放假期间共装机7部。故障发生后，我们值班人员都及时的帮客户恢复了业务，保证了客户业务的正常运营。在此，我们向春节期间仍旧坚持在工作岗位上的同事表示崇高在敬意。

昆山：春节7天假期，昆山工维共处理故障16起。按工单划分为：

有工单6起，无工单10起；按故障发生日期划分为：2月2日2起，2月3日2起，2月4日3起，2月5日1起，2月6日3起，2月8日5起。其中2月2日大润发故障为第三方施

工造成客户光缆中断，因客户使用移动业务时间较长，查不到路由图纸，路面管道井盖上停放汽车较多，部分井盖打不开，无法查清光缆走向，故障处理时长较长，其他均为一般故障，均在2小时之内处理完毕。

春节后网络保障工作总结24

一、加强网络安全认真部署师生网络安全意识

为切实抓好这次活动，中心校召开小学校长会，对整个网络信息安全宣传活动作了详细的布置，明确了人员的职责，会后下发了《中心小学网络信息安全宣传周活动计划》。要求各校充分利用各种会议、活动、课堂等有效形式，在全校广泛宣传 and 普及网络安全的法律、法规政策和相关知识，强化全校师生对网络安全教育工作的参与意识和责任意识。

二、精心组织狠抓落实

为确保宣传周活动不走过场，达到预期效果，全校各部门强化措施，狠抓落实，确保了活动取得实效。成立了以校长组长的宣传活动领导小组，全面负责本次宣传活动的方案拟定、工作部署、组织协调等工作。中心校班子成员各负其责，全力配合学校做好本次宣传周的活动。

三、形式多样内容丰富

- 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。

四、效果明显深入人心

- 1、经过这次活动，全校师生对网络安全教育有了新的认识。一是对网络安全教育工作支持重视多了，二是教师和学生亲自参与多了。
- 2、教师和学生的网络安全意识明显提高。

春节后网络保障工作总结25

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