# 年度网络安全工作总结范文十二篇

来源：网络 作者：尘埃落定 更新时间：2023-11-16

*工作总结（Job Summary/Work Summary），以年终总结、半年总结和季度总结最为常见和多用。就其内容而言，工作总结就是把一个时间段的工作进行一次全面系统的总检查、总评价、总分析、总研究，并分析成绩的不足，从而得出引以为戒的经...*

工作总结（Job Summary/Work Summary），以年终总结、半年总结和季度总结最为常见和多用。就其内容而言，工作总结就是把一个时间段的工作进行一次全面系统的总检查、总评价、总分析、总研究，并分析成绩的不足，从而得出引以为戒的经。下面是小编精心整理的年度网络安全工作总结范文十二篇，仅供参考，大家一起来看看吧。

style=color:#ff0000>年度网络安全工作总结1

       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。

>　　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。

style=color:#ff0000>年度网络安全工作总结2

　　随着新年的临近，一年紧张的工作也到了扫尾的阶段，网络安全工作总结。已经拥有近两年工作经验的我，无论是在工作经验、技术水平、人文交际和自身修养都有了较好的提高，并且学会了一些正确分析以及解决问题的方法的流程，制定日常工作计划以及在相对重要的事情后及时做一些简单的总结，来获取经验等，一些在工作和生活中不可或缺的技能和处事方法，这些经验将会对在以后的工作和生活起到很大的正面作用。总的来说我对自己过去1年的工作过程及结果基本满意。

　　在今年的工作中，在各方面工作不断实践和完成的过程中，还是遇到了一些阻力和困难，但绝大多数都已经克服。

　　在计算机服务器方面，我认真自学了一些服务器知识以补充自己对服务器知识的不足，了解了服务器的基本构架，以及服务器和普通pc机的不同之处，补足了阵列及阵列柜方面的知识，会简单使用hpservernavigator工具盘，并且自己动手安装了一次服务器系统，学会了一些简单的故障判断、恢复和处理手段。

　　在网络方面基本比较熟悉cisco的各个型号设备的功能、配置和一些基本的故障判断、恢复和处理手段。在今年网络整改前夕同同事张亮一起前去武汉网络信息中心进行了网络整改方案的讨论，同时也认真学习了网络信息中心的网络结构，回来后和汤主任、高攀宇老师、张亮，将拿回来的方案与重庆天融信公司的安全工程师们又进行了讨论和修改，这次经历使我网络技术方面又一次获得宝贵的经验，它不但使我了解了更多更广的网络及网络安全知识，同时也对我以前知道却没有过多使用的一些模糊的知识和概念有了重新的认识和理解，使我的网络知识结构得到了强化和补充。只是在后期网络实施整改时，由于参加了江口预报系统的开发没有时间一起参加整改，虽然对大的网络结构拓扑熟悉，但对于一些细节的设备配置却没有能够熟练掌握，这部分知识将在下一年有空余时间时进行补足，工作总结《网络安全工作总结》。

　　在网络病毒方面，基本上可以不依靠杀毒软件，而发现和各种种类的病毒。2023年随着科技的提高和计算机广泛的应用也是病毒广为活跃的一年，一种病毒的多样性也极高的提高了病毒的破坏力和传染能力，基本上来说已经很少再有单纯的单机病毒，基本都有网络特性，就拿蠕虫病毒来说，一些蠕虫病毒除了会广泛感染计算机抢占计算机和网络资源以外，甚至还有黑客工具开后门能力、信息盗窃能力、网络设备攻击以及ddos攻击能力、arp欺骗等等其破坏性已经远远超出了单纯的蠕虫病毒的破坏力，一个多元化的病毒的破坏能力是显而易见的!在2023年我局网络多次受到冲击导致网络瘫痪，而这其中绝大多数冲击还是来自我们网络内部，内网的安全性问题已经迫在眉睫，在多次事故中，通过我们全体网络人员的共同努力下全部及时有效的解决掉，并且没有对我们的水情报讯信息传输的最终结果上，产生任何影响。在多次排查冲击网络病毒工程中，让我摸索出了一条快速排查的方法和套路并在水文网上发表了“水文上游局处理网络arp欺骗故障中的一些经验”一文，同时我也找到了大量的网络管理及分析工具，在对这些工具的熟练过程中极大的提高了我们故障处理的效率，对病毒源判断的准确率，如cisco设备管理助手系列和snifferportable已经成为我们网络必不可少的一部分。

　　在软件开发方面，我利用空余时间写了一些方便日常报讯工作和网络检测的小软件，重写了分中心报文监视及到报时间打印软件，使其更方便使用、理解和修改;写了三峡梯调发报查询软件，提高了我们对发往梯调的报文监视的效率和准确度，使我们可以节省更多的时间来对其他异常故障进行处理;写了网络监视软件，使其可以详细记录网络中断时间，并对网络中断进行实时告警，减轻了对网络监视的负担。在工作时间我参与了“江口水库调度系统”的后台管理部分的开发，并且按时合格的完成了自己的工作。经过上述的工作及学习经验，我感觉自己的软件设计及编写水平有了质的提高，尤其是在参与了“江口水库调度系统”的后台管理部分的开发后，和软件公司的技术人员进行了交流，提高了我对大型软件工程体系的理解，以及重新认识了前期规划设计和编写大量文档的必要性，对数据库的设计及构架的重要性有了重新的理解，在对后台管理这部分编写的时候，对我自身代码编写以及规划等能力也有了很大的提高，尽量使自己编写的代码易读、易修改、加强层次性、减少代码的偶合性，并避免没有效率的重复编写。同时在开发中我也由以前的，使用c#语言开发.net程序的基础上，进而学会了vb语言的编写，并努力使自己摆脱编程语言的束缚，而是去掌握一种编程的思想和理念。“江口水库调度系统”开发的过程对我来说，是一次非常宝贵难得的经验。

　　在自动报讯报文监视方面，我认真尽职的完成了自己的工作，每次发报前都提前到位检查网络，在报文出现问题后或帮助分中心解决问题，或根据分中心需求进行相关操作，从没有因为我个人原因对分中心造成任何损失，2023年3月份以来开始实行新报文编码规则，我熟练掌握了新报文编码格式，以确保能及时的帮助分中心发现报文问题，使其能及时修改保证。

　　在一年的工作中自身还是暴露出一些不足之处，在工作过程中还是会因为经验不足产生一些问题，值得庆幸的是并没有因此而产生严重后果，我的不足简单归纳为以下几点。

　　1.人文交际能里还有待提高。

　　2.服务器知识还需要继续提高。

　　3.英语能力需要加强。

　　4.对所分配的工作还需要更详细有效率的计划安排，从而提高工作效率。.

　　5.对现在网络设备的配置需要更熟练掌握，还需对帧中继等知识进行补充。

　　6.还应加强对网络安全方面知识的学习，不应该一味的在问题发生后解决，而是要学会防范于未然。

　　我将利用新的一年来继续提高自己的技术水平和工作经验，并侧重于改进自己的缺点和不足，同时加强学习充分利用空余时间，为自己“充电”。

　　以上是我对今年的工作总结和认识，在这期间感谢王主任和汤主任以及各位老师，对我们的照顾和教导，无论是在生活上还是在知识上都给了我莫大的帮助，为我们的方方面面都考虑的非常周到，让我可以专心工作毫无后顾之忧，使我最快的融入了水情室这个大集体，我为自己能在这里工作，能为国家作贡献感到自豪!

　　新的一年即将到来，我们又即将迎接新的挑战，出问题是在所难免的，重要的是我们要勇于面对问题、解决问题，而不是一味的拖沓和回避，我将继续提高自己的自身技术水平，更好的发挥计算机的价值，为我们的水文事业服务。

style=color:#ff0000>年度网络安全工作总结3

　　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。

style=color:#006aff>年度网络安全工作总结4

　　我院积极贯彻落实县委网信办《关于做好我县医院网络安全保障工作的通知》要求，我院领导高度重视，立即行动，顺利完成国庆期间网络信息安全工作。现将此项工作总结如下：

　　一>、高度重视，落实责任。

　　我院成立网络安全领导小组，由信息科主任任小组组长，其它各科室主任任副组长和组员。9月21日之前将责任领导、联络员名单、网络安全自查表报送网络安全领导小组办公室，要求组员24小时开机，做好随时反映、报告网络安全问题的准备工作。

　　国庆xx周年9月21日至10月10日期间：

　　1、网络信息安全上报要求24小时监控。

　　2、风险防控制：发现问题，三分钟之内必须断；半小时之内上报网络安全领导小组；无问题，零报告。

　　3、要求各科室每天15：00时之前上报前一天至当日15：00时网络信息安全情况。

　　>二、强化安全防范措施，提高风险防范能力

　　1、对医院办公通信工具OA，进行漏洞修复检查升级。坚决整改用户长期使用默认口令、长期不变口令等问题。

　　2、信息科对医院数据采取分类、备份、加密等措施，严格数据的访问权限，及时发现处置非授权访问等异常情况。

　　3、对医院公共区域的LED屏幕，由专人负责，修改内容需要高强度密码口令。

　>　三、规范流程操作，养成良好习惯。

　　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。

style=color:#ff0000>年度网络安全工作总结5

　　我办网络安全工作在市委市政府的坚强领导下，在市网信办具体指导下，网络安全工作有序开展，各项工作稳步推进，网络安全得到进一步保障。现将具体情况报告如下：

　　>一、基本情况

　　(一)健全组织，明确责任分工。成立网络安全人防领导小组，由办主要领导负责网络安全工作的组织、指导和监督，综合科负责网络安全建设各项具体事务的组织推进和落实，信保中心负责技术保障和运维服务。制定《xx市人民防空办公室网络安全责任制检查考核制度并实施。

　　(二)强化教育，提高思想认识。深刻领会习近平总书记关于网络安全工作的重要批示特别是“四个坚持”重要指示精神的内涵，坚持领导干部带头学习网络安全知识和相关法律，将网络安全学习纳入中心组理论学习，联系工作实际，结合职责和岗位实际，对照《网络安全责任制检查考核制度》，确保指示精神落小落细。市人防办党组定期组织全体职工干部，利用座谈会深入交流学习心得。通过深入浅出的学习讨论，深化全体职工网络安全的思想认识，落实网络安全细节工作。

　　(三)注重末端，强化日常管理。日常网络安全工作管理中，网络安全领导小组强调并检查：网络安全管理：机房安全策略采取防火墙及入侵检测技术。不得私自架设无线WIFI，不得浏览、下载、传播与工作内容无关的网页或网络资源，密码不得使用弱口令，加密文件与明文密码不得同时出现。终端安全管理：办公电脑专机专用，定期查杀病毒，扫描并修复办公电脑漏洞;电子认证证书、移动存储介质等设备需妥善保管。各类信息系统、政务网络及VPN等账号和密码，应妥善保管并定期修改密码。数据安全管理：不得擅自利用职务之便查询、窃取、篡改、删除、拷贝和伪造各类政务信息资源。严格落实保密规定，涉密设备定点专机、专人专用;涉密文件和信息专人专管，不得复印、拍摄、上网。信息发布管理：政府信息公开依托政务外网,严格遵守政府信息公开流程。行政审批结果、行政执法公示涉及个人隐私信息均做屏蔽化处理。

　　(四)提升能力，强化应急演练。落实网络安全值班制度，实行x×xx小时在岗值班，根据《网站值班注意事项和应急处置程序》制度，保障网络安全应急处置准备和建设。2023年x月初根据网络安全部门工作要求在防火墙端封禁境外高危恶意攻击。参加属区网络安全部门组织的网络攻防演练复盘会，学习经验教训，引之为戒并积极准备参加下一次的网络攻防安全演练工作。

style=color:#006aff>年度网络安全工作总结6

　　根据《衡阳市人民政府办公室关于开展全市重点领域网络与信息安全检查的通知》精神，9月10日，由市电政办牵头，组织对全市政府信息系统进行自查工作，现将自查情况总结如下：

　　>一、 网络与信息安全自查工作组织开展情况

　　9月10日起，由市电政办牵头，对各市直各单位当前网络与信息安全进行了一次全面的调查，此次调查工作以各单位自查为主，市电政办抽查为辅的方式进行。自查的重点包括：电政办中心机房网络检修、党政门户网维护密码防护升级，市直各单位的信息系统的运行情况摸底调查、市直各单位客户机病毒检测，市直各单位网络数据流量监控和数据分析等。

　　>二、 信息安全工作情况

　　通过上半年电政办和各单位的努力，我市在网络与信息安全方面主要完成了以下工作：

　　1、 所有接入市电子政务网的系统严格遵照规范实施，我办根据《常宁市党政门户网站信息发布审核制度》、《常宁市网络与信息安全应急预案》、《“中国?常宁”党政门户网站值班读网制度》、《\"中国?常宁”党政门户网站应急管理预案》等制度要求，定期组织开展安全检查，确保各项安全保障措施落实到位。

　　2、 组织信息安全培训。面向市直政府部门及信息安全技术人员进行了网站渗透攻击与防护、病毒原理与防护等专题培训，提高了信息安全保障技能。

　　3、 加强对党政门户网站巡检。定期对各部门子网站进行外部web安全检查，出具安全风险扫描报告，并协助、督促相关部门进行安全加固。

　　4、 做好重要时期信息安全保障。采取一系列有效措施，实行24小时值班制及安全日报制，与重点部门签订信息安全保障承诺书，加强互联网出口访问的实时监控，确保十八大期间信息系统安全。

　　>三、 自查发现的主要问题和面临的威胁分析

　　通过这次自查，我们也发现了当前还存在的一些问题：

　　1、部分单位规章制度不够完善，未能覆盖信息系统安全的所有方面。

　　2、少数单位的工作人员安全意识不够强，日常运维管理缺乏主动性和自觉性，在规章制度执行不严、操作不规范的情况。

　　3、存在计算机病毒感染的情况，特别是U盘、移动硬盘等移动存储设备带来的安全问题不容忽视。

　　4、信息安全经费投入不足，风险评估、等级保护等有待加强。

　　5、信息安全管理人员信息安全知识和技能不足，主要依靠外部安全服务公司的力量。

　　>四、 改进措施和整改结果

　　在认真分析、总结前期各单位自查工作的基础上，9月12日，我办抽调3名同志组成检查组，对部分市直机关的重要信息系统安全情况进行抽查。检查组共扫描了18个单位的门户网站，采用自动和人工相结合的方式对15台重要业务系统服务器、46台客户端、10台交换机和10台防火墙进行了安全检查。

　　检查组认真贯彻“检查就是服务”的理念，按照《衡阳市人民政府办公室关于开展全市重点领域网络与信息安全检查的通知》要求对抽查单位进行了细致周到的安全巡检，提供了一次全面的安全风险评估服务，受到了服务单位的欢迎和肯定。检查从自查情况核实到管理制度落实，从网站外部安全扫描到重要业务系统安全检测，从整体网络安全评测到机房物理环境实地勘查，全面了解了各单位信息安全现状，发现了一些安全问题，及时消除了一些安全隐患，有针对性地提出了整改建议，督促有关单位对照报告认真落实整改。通过信息安全检查，使各单位进一步提高了思想认识，完善了安全管理制度，强化了安全防范措施，落实了安全问题的整改，全市安全保障能力显著提高。

　　>五、 关于加强信息安全工作的意见和建议

　　针对上述发现的问题，我市积极进行整改，主要措施有：

　　1、对照《衡阳市人民政府办公室关于开展全市重点领域网络与信息安全检查的通知》要求，要求各单位进一步完善规章制度，将各项制度落实到位。

　　2、继续加大对机关全体工作人员的安全教育培训，提高信息安全技能，主动、自觉地做好安全工作。

　　3、加强信息安全检查，督促各单位把安全制度、安全措施切实落实到位，对于导致不良后果的安全事件责任人，要严肃追究责任。

　　4、继续完善信息安全设施，密切监测、监控电子政务网络，从边界防护、访问控制、入侵检测、行为审计、防毒防护、网站保护等方面建立起全方位的安全防护体系。

　　5、加大应急管理工作推进力度，在全市信息安全员队伍的基础上组建一支应急支援技术队伍，加强部门间协作，完善应急预案，做好应急演练，将安全事件的影响降到最低。

style=color:#ff0000>年度网络安全工作总结7

　　根据《20\_\_年\_\_国家网络安全宣传周活动实施方案的通知，结合“网络安全知识进校园”的主题，根据实际，根据实际情况，我校开展了“网络安全宣传周”活动。现将活动的开展情况总结如下：

　　1.领导有力，“网络安全宣传周”活动顺利推进。

　　学校成立了领导小组。学校主要领导具体负责指导本次活动的开展，各班班主任具体负责活动的开展，使得“网络安全宣传周”活动稳步开展。

　　2.通过多种渠道，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。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。

　　3.网络安全活动进班，用网要求进一步得到明确。

　　召开“网络安全进校园”主题班会。\_月21日下午，我校分班级召开“网络安全进校园”主题班会，班会是此次活动的主要形式。各班主任围绕主题认真准备，整理班会所需资料，带领全班同学详细学习了网络安全知识，并要求学生将学习到的网络安全常识与家长、朋友分享。

　　通过此次活动，同学们积极参与，认真阅读了关于“网络道德和网络素养”的文章，将其运用到生活中，以便更好的创造和谐的网络环境。

style=color:#006aff>年度网络安全工作总结8

　　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。

>　　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。

style=color:#ff0000>年度网络安全工作总结9

　　2023年以来，我矿的计算机网络管理工作在我矿党政领导的正确领导下，在公司信息中心的关心、帮助、指导和支持下，我矿计算机管理工作取得了有效的进步，oa系统、瓦斯监测、财务系统、供应购销链及煤矿安全等网络系统的安全、稳定运行工作取得了较好成绩。计算机各项管理的工作得以顺利开展，并取得较好效果。现将一年来的计算机管理工作总结如下：

　>　一、制定制度，明确责任

　　我矿共有电脑129台，打印机77台，分布在矿区的办公大楼，综合大楼，救护队各地，分布较散，由于局域网络的全面铺开应用，给我矿网络管理与维护工作带来难处。对此，在我矿党政领导的高度重视和指导下，我矿成立了计算机安全管理领导小组并制定出台了《计算机及网络管理办法》，对计算机的使用和网络的安全管理拟定了详细的规定和法则，坚持专业管理与业余小组管理相结合，落实责任，明确分工，使逢春煤矿的计算机与网络管理在制度上得到了健全，做到了责任落实到个人。

>　　二、加强管理，规范员工行为，提高员工素质

　　为了规范我矿员工使用电脑的行为，我矿每个星期都坚持定时或不定时对电脑进行检查，检查杀毒软件是否升级，电脑是否做到人走关机，电脑上是否安装了游戏等。在雷雨季节时候，我矿更是加强了检查次数，并及时制定了《雷雨季节计算机使用办法》。办法规定：电脑使用者必须做到人走关机并将网线拔出，做好相关防雷措施。

　　在电脑使用上，我矿员工素质参差不齐，2023年3月，我矿遭受了一次因为arp病毒导致全矿网络瘫痪的事故。事后经分析，这次事故是由于一个基层连队的电脑使用不当造成。这让我矿感到：要想让我矿网络长治久安，还得从提高电脑使用者素质抓起。为此，去年，我矿组建了一个电脑培训室，并组织举办了4次计算机安全培训，这4次培训都是针对对电脑知识欠缺的基层连队的队长、书记和机关管理人员而设计；培训课上除了学习《计算机及网络管理办法》以及一些办公自动化软件应用的基础知识，还重点讲解了计算机基础知识、计算机安全相关知识、病毒的防范、处理以及卸载、安装、杀毒软件的等技巧。经过培训，我矿各级管理人员对计算机网络安全意识得到了提高，同时也提高了他们电脑操作和应用水平。

　　另外，我矿在日常的计算机及网络维护过程中，采取现场讲解、指导的方式，如：问题原因出在那里，下次遇见这种情况怎么处理。同时还要求他们人走关机，重要资料不存c盘并备好份等。提高了计算机使用者的业务技能，才能进一步提高计算机使用者的安全意识、防范、处理技能。

>　　三、加强学习，提高自身业务素质

　　计算机是一门很深的学科，技术更新很快，只有不断的学习才能提高自身水平，从矿计算机管理的实际情况出发，我们着重自学了计算机硬件日常保养及维护，以及常用软件使用等。

　　计算机和网络管理最主要的安全问题还是防治病毒的入侵。

　　2023年期间，arp病毒在我矿盛行。后经公司信息中心的老师们指点，我矿学习了利用sniffer4\_70工具进行抓包分析，大大减少了对病毒计算机的盲目性处理。后来，我矿从网络上找到了一款arp防火墙单机版，这款软件能够拦截来自局域网中的arp病毒攻击，也能够抑制感染了病毒的计算机对局域网的发包数量，我矿把这款软件安装在一些经常用u盘的电脑上，这样，一旦我矿有电脑感染了arp病毒，我矿就能在最短的时间内知道并进行处理。

　　但这款软件并不能对感染了病毒的计算机进行杀毒处理，于是，我矿从网上找到了一款专门针对一些arp病毒的杀毒工具，如usbcleaner6.0专杀工具，av终结者-8749木马专杀工具等。有了这些软件工具，有效杜绝了该病毒的进一步蔓延和入侵，确保了我矿计算机的安全运行。

style=color:#006aff>年度网络安全工作总结10

　　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。

style=color:#ff0000>年度网络安全工作总结11

　    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。

style=color:#006aff>年度网络安全工作总结12

      为贯彻落实习近平总书记关于网络安全的重要讲话精神、党中央关于网络安全的决策部署、重要网络安全工作安排部署以及《网络安全法》。今年以来，我单位大力推进单位网络网络安全建设，压实网络安全工作任务，严格主体责任追究，提升网络安全理念，防范化解单位网络安全风险、设备失效风险以及网络链路中断风险，全力保障单位网络安全稳定运行。

>　　一、强化组织领导，健全制度建设

　　为贯彻落实国家关于网络安全相关工作的部署要求。一是中心建立了网络安全工作领导小组，传达和学习习近平总书记和党中央关于网络安全的重要指示精神，贯彻落实上级部门关于网络安全工作的决策部署，加强单位网络安全工作领导，制定《防范化解网络风险工作方案》落实网络安全工作责任，压实防范化解相关工作任务及计划，组织开展应急演练。二是为加强单位网络网络安全管理规范化，进一步保障单位网络安全，对所制定的单位网络相关管理制度及应急预案从提高网络安全性、规范化人员安全操作及处置流程可行有效等方面进行修订完善，规范化单位网络的安全管理。

>　　二、加强安全建设，提升安全理念

>　　（一）加强网络安全监测能力建设

　　在单位网络核心机房测试部署入侵检测系统、流量探针、漏洞扫描及日志服务器等安全监测分析设备。通过设备对电子单位网络进行监测，及时对安全隐患或安全事件进行预警及处置。

　　（二）提升单位网络整体网络安全防护能力。推进单位网络平台工程建设，提升电子单位网络核心机房网络、系统及安全设备，动环，消防，UPS供电及空调等各设备支撑能力，切实降低机房各设备失效概率，进而保障电子单位网络核心机房的安全稳定运行。

　　（三）提升单位网络网络链路健壮性冗余性。一是加快推进单位网络链路升级改造项目建设，建设安全态势感知系统，升级主用链路带宽，提升电子单位网络网络链路主用链路的健壮性；二是加快推进电子单位网络备用链路建设，使电子单位网络链路具备冗余性，降低单位网络网络链路中断风险。

　　（四）加强人员安全教育培训。为着力提升单位网络人员安全管理水平及专业技术知识能力，一是组织单位网络管理部门相关专业技术人员到全国各地多次参加网络安全相关培训，学习国家相关安全标准、安全防护理念以及了解现今安全形势与安全技术。二是通过邀请专业厂商到单位以授课以及技术交流等形式向单位全体专业技术人员进行网络安全培训，提升中心全体人员的安全防范意识及能力。

　　（五）提升信息安全共享机制。与上级主管部门形成单位网络安全信息共享机制，组建安全通报工作联系群，对于所发现的安全隐患及安全漏洞及时通告预警，对于发生的安全事件进行联动处置。

　　（六）完善上报机制。对单位网络安全情况每月向省委网信办进行汇报，发现安全风险或出现安全事件及时向省委网信办汇报，在重大活动期间每日以零报告机制进行安全情况汇报。

>　　三、积极处置网络安全事件，防范化解网络安全风险

　　通过监测数据协助处置了多起网络攻击事件，在事件处置过程中，组织技术力量及时准确封堵源头，有效遏制事件影响的发展趋势，对事件进行持续跟踪监测，直至事件彻底解决，所有事件均未造成重大影响，保障了单位网络安全稳定。

>　　四、保障节假日期间单位网络稳定运行

　　在各节假日前组织对单位网络系统进行安全检查、漏洞扫描及渗透测试，并进行安全加固；对单位网络核心机房空调、消防、UPS供电等设施设备运行情况进行检查，确保机房各设施设备正常运行；组织对单位网络网络链路进行检查，确保网络链路运行情况正常；下发自查通知至各办公室，要求对各自终端进行安全自查，提升单位网络整体安全性、联动处置安全事件的能力及有效性。在节假日期间，组织进行24小时现场值守和应急值守工作，并加强巡查巡检及网络监测力度，全力保障节假日期间的单位网络网络安全、机房安全、链路安全，对突发事件能够随时进行应急响应。保障单位网络在新在节假日期间安全稳定运行，0安全事件发生。

>　　五、下一步工作打算

　　一是提升单位网络安全性。通过我省建设的电子单位网络态势感知系统。形成数据采集、数据分析、预警通告和态势展现等安全监测能力，联动处置网络安全事件，极大提升单位网络安全保障能力。二是促进单位网络安全合规。对单位网络省级平台进行等级保护三级测评，保障单位网络安全合规。三是持续做好各节假日期间安全保障工作。在节日前期做好安全检查发现的安全风险进行预警，监测直至修复，降低安全事件的发生概率。在节日期间24小时监测，对突发安全事件进行人工应急响应，准确溯源及时处置，控制事件发展事态。保障节日期间单位网络安全稳定运行。四是组织开展单位网络应急演练。组织各重要组成单位以及安全服务商开展一次应急演练，检验单位网络安全防护能力及应急预案有效性，提升单位网络管理人员的安全管理能力及安全意识。

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