# 网络安全检查自查报告(大全15篇)

来源：网络 作者：深巷幽兰 更新时间：2024-05-11

*在经济发展迅速的今天，报告不再是罕见的东西，报告中提到的所有信息应该是准确无误的。大家想知道怎么样才能写一篇比较优质的报告吗？下面是小编带来的优秀报告范文，希望大家能够喜欢!网络安全检查自查报告篇一一、加强领导，健全组织。在治理乱收费工作中...*

在经济发展迅速的今天，报告不再是罕见的东西，报告中提到的所有信息应该是准确无误的。大家想知道怎么样才能写一篇比较优质的报告吗？下面是小编带来的优秀报告范文，希望大家能够喜欢!

**网络安全检查自查报告篇一**

一、加强领导，健全组织。

在治理乱收费工作中，学校成立了工作领导小组，由郑现春任组长，李汉卫为副组长，部分中层领导为组员。做到学校一把手亲自抓，并指定专人负责这项工作，从组织上和力量上保证了此项工作的顺利开展。

二、加强宣传学习，提高自觉性

为增强全校对开展治理教育乱收费工作重要性和必要性的认识，学校利用各种形式进行动员部署。

1、严格执行上级文件精神，本学年，我校按照教体局的统一要求，保证全校学生免除杂费、学费、、教科书费，大力宣传“两免一补”政策，并认真执行。在开学前召开专题会议，学习“治理教育乱收费”相关文件，把握文件要求，明确各自职责与任务，有序地部署好开学工作。

2、学校根据市区教体局的文件精神，组织教师学习上级关于治理教育乱收费工作的文件、本校治理教育乱收费计划和实施方案，吃透精神，提高认识。在全校班主任工作、学科教师会议上，提出工作的相关要求，并与全体教师签订了《治理乱收费责任状》，要求全体教师必须认真对待，严禁私设项目收费，不得强行向学生推荐教辅用书，严禁私自动员学生订购教辅用书、练习。

3.不自立收费项目，坚持“两免一补”公示制，有计划地使用经费，严肃审批报销手续，坚决杜绝帐外帐、“小金库”、乱收乱支等违纪行为。

三、加强制度建设，规范收费行为

我校在治理教育乱收费工作中，不断加强制度建设，坚持治理乱收费制度。

1.建立乱收费工作责任追究制度，并与各教研组长签订治理教育乱收费工作责任状。

2.严格执行“两免一补”政策。治理教育乱补课、乱办班、乱收费自查报告。治理乱收费工作是学校的一项重要工作，因此，学校对这项工作高度重视。在学期初，学校领导认真学习文件精神，明确自身职责，从思想上提高对开学治理乱收费工作的认识。首先，学校成立了由校长为组长的治理乱收费领导小组，制订了治理乱收费各项规章制度，治理乱收费工作由一把手校长亲自抓。其次，召开专题会议，落实零收费。同时严格按照上级要求，实施“两免一补”政策。开学初，学校对各班进行收费调查，未发现乱收费现象。

四、开展师德师风教育活动，提高教师师德修养水平

**网络安全检查自查报告篇二**

按照汉区宣字〔20xx〕17号《关于在全区开展关键信息基础设施网络安全检查的通知》文件精神要求，我镇高度重视，立即对网络安全工作进行了全面检查，现将自查情况报告如下：

吉河镇网络建设运行以来，一直对安全工作十分重视，成立了专门的网络安全领导小组，积极完善各项安全制度，严格落实有关网络安全的各项管理规定，采取了多种措施防范网络安全事件的发生，近年来未发生安全事故，保障了网络安全、稳定、高效运行，为全镇各项工作的开展奠定了坚实基础。

1、组织管理

我镇高度重视网络安全工作，成立了由主要领导任组长，分管领导任副组长，站所办负责人为成员的网络安全领导小组，领导小组下设办公室，抽调具体工作人员负责办公。召开了由分管领导、网络安全职能部门和重点部门负责人参加的.会议，对上级文件进行了认真学习，对自查工作做了周密部署，确定了自查任务和人员分工，真正做到了领导到位、机构到位、人员到位、责任到位。为确保网络安全工作顺利开展，要求镇全体干部充分认识网络安全工作的重要性，认真学习网络安全知识，都能按照网络安全的各种规定，正确使用计算机网络和各类信息系统。

2、日常管理

针对网络安全工作的特点，结合我镇实际，制定了《网络安全管理办法》、《视频会议管理制度》、《电子政务平台操作系统操作指南》等一系列网络安全制度和规定。网站信息发布由专人负责，并进行登记；杀毒软件和防火墙均为国内产品；网站上传信息前均在本地进行病毒检测；禁止携带移动存储介质进入电子政务平台专用计算机。

3、防护管理

全镇网络设备、服务器等均运转正常。所有网络设备、信息系统等按规定设置高强度密码并定期进行更换；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、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控，认真检查保管系统安全。

4、应急管理

进一步完善了网络安全应急预案，明确了应急处理流程，落实了应急技术支持队伍；对重要文件、数据进行定期自动备份。

5、安全检查

对系统和软件等及时更新补丁；对防病毒软件和防火墙升级病毒代码特征库；定期对网站进行查杀、漏洞扫描、检测和修复。

成立了吉河镇网络安全工作领导小组，全面负责网络安全工作；修订完善了《网络安全管理规定》等一系列制度；新增了2名网络工作人员，充实了技术队伍；开展了网络安全应急处理培训；让网络工作人员定期在网上收听信息安全教育讲座。

通过这次自查，我们也发现了当前存在的一些问题：

1、部分干部网络安全意识不强，日常运维缺乏主动性和自觉性。

2、专业技术人员较少，网络安全知识、技术、经验欠缺。

3、网络安全经费投入不足，软、硬件设备需要进行改善。

4、规章制度尚不完善，未能涉及到网络安全的所有方面。

1、进一步加强对全镇干部和网络工作人员的安全意识教育，提高做好安全工作的主动性和自觉性，增强对网络安全的防范意识。

2、多参加市区和专业机构举办的网络安全技术培训，增强安全防范意识和应对能力，提高工作人员的水平和能力，提高网络安全管理水平。

3、完善网络安全制度，同时安排专人，密切监测，及时发现网络安全隐患。

4、加大投入，继续完善网络安全设施，从边界防护、访问控制、入侵检测、病毒防护等方面建立起全方位的安全体系。

1、市区要经常组织召开专家讲座和座谈会等形式多样的经验交流活动。

2、经常组织网络安全方面的专门培训，增强安全防范意识，提高网络管理人员的\'专业水平。

**网络安全检查自查报告篇三**

按照《xx县x息化工作领导小组办公室关于开展20xx全县网络与信息系统安全检查工作的通知》文件要求，我单位高度重视，立即组织开展全镇范围内的网络与信息系统安全工作。现将自查情况汇报如下：

1、我单位高度重视网络与信息系统安全工作，在党委扩大会议上专门研究部署了此项工作，并成立了信息化与网络安全工作领导小组，明确了镇办公室为信息化与网络安全工作办公室，确定了一名网络与信息系统安全工作管理员，负责日常管理工作。

2、制定下发了《人民政府关于加强信息网络安全保障工作的意见》和《网站的管理维护工作制度》，要求各科室、各部门认真组织学习，充分认识网络和信息安全工作的重要性，能够按照各项规定正确使用网络和各类信息系统，确保我镇网络与信息系统的安全。

结合我镇实际，在日常管理工作中，与各科室、部门签订网络和信息安全工作责任书，并要求各科室、各部门严格按照以下规定执行，确保网络和信息系统的安全。

1、计算机必须设置系统启动密码，密码严禁外泄，避免外部人员登录对本单位计算机网络进行攻击。

2、办公计算机在使用过程中，要定期进行系统备份，以提高突发事件发生时的应对能力。

3、不得随意接入网络设备，避免因擅自接入影响网络和信息系统的正常运行，确因工作需要接入网络设备，必须经信息化与网络安全工作办公室允许方可接入。对于移动存储设备，不得与涉密计算机及政务专网以外计算机共用。

4、所有计算机必须安装防火墙，定期查杀网络病毒，移动存储设备在接入计算机使用前，必须进行杀毒。

5、严格信息系统文件的收发，完善清点、修理、编号、签收制度。

1、安排专人负责我镇的网络安全工作，并积极参加县有关部门组织的网络安全知识培训，提高工作水平。

2、安排专人负责信息系统的管理，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。

3、利用机关干部集中学习，专门组织开展了一次网络与信息安全知识的学习活动。

为切实做好网络与信息系统安全管理工作，确保全镇网络与信息系统安全稳定运行，在8月21日我镇召开的安保工作专项部署会上，镇党委政府对此项工作进行了专门部署，要求各科室、各部门严格按照各项工作部署，扎实做好网络与信息系统安全管理工作，确保此项工作落实到位。

目前，针对我镇的网络与信息安全工作现状，信息化与网络安全工作领导小组定期组织由专业技术人员组成的检查小组到各办公室专项检查网络和信息安全情况，仔细排查信息系统的漏洞和安全隐患，用专用工具查杀木马、病毒，及时加强防范措施，并为计算机安装了正版的杀毒软件和系统软件，有效提高了计算机和网络防范、抵御风险的能力。

1、存在的主要问题

一是由于本单位计算机网络方面的专业技术人员较少，网络安全方面可投入的力量有限。

二是规章制度体系初步建立，可能还不够完善，未能覆盖到网络与信息系统安全的所有方面。

三是遇到计算机病毒侵袭等突发事件时，由于技术力量薄弱，处理不够及时。

2、整改措施

一是要继续加强对本单位工作人员的安全意识教育，提高做好安全工作的主动性和自觉性。

二是安排专人，密切监测，随时随地解决可能发生的信息系统安全事故。

三是要加大对网络线路、计算机系统的及时维护和保养，加大更新力度，确保网络和信息系统正常运行。

**网络安全检查自查报告篇四**

根据市委保密委员会《关于集中开展全市网络清理检查工作的通知》(密〔20xx〕5号)要求，xx市环保局高度重视，重点对文件制发、网络使用、信息发布、网站监督等四个方面工作进行了全面自查。基本情况和自查情况汇报如下：

(一)加强保密工作组织领导。我局将保密工作列入重要议事日程，实行保密工作领导责任制。专门成立了以分管领导为组长，各单位负责人为成员的网络及信息安全工作领导小组，负责网络及信息安全统筹规划和组织协调工作。对保密工作所需设施、设备和经费，我局领导给以充分的重视和支持，保证了日常工作顺利开展。

(二)加强保密工作队伍建设。坚持做到网络及信息安全工作机构健全，安排信息中心负责网络及信息安全具体工作，设有专职网站信息编辑人员和技术维护人员，安全工作队伍基本素质较高，大部分管理人员具备本科以上学历，且都能熟练掌握保密法规和保密技术基础知识，熟悉本单位业务工作和保密工作基本要求。

(三)加强保密教育提高保密意识。局领导对安全保密工作十分重视，时刻强调安全保密工作的重要性，要求做到部署、检查、总结、考核与安全保密工作同步进行。采取多种方式，利用各种机会对干部职工进行经常性的保密教育，除了文件学习，还组织观看保密录像，开展网络及信息安全工作培训，进一步增强职工的安全保密意识，提高做好安全工作的主动性和自觉性。

通过认真学习《中华人民共和国保守国家秘密法》和《保密法实施办法》，切实开展好保密工作的教育与宣传。及时传达贯彻上级安全保密工作会议及有关文件精神，进一步明确保密管理要求。依据《中华人民共和国政府信息公开条例》和《环保部环境信息公开办法(试行)》，认真审核、发布各类政务信息及依申请公开信息。近年来，结合xx市政务信息工作实际，修订完善政府信息公开《指南》、《目录》，健全了主动公开和依申请公开工作机制，补充完善了xx市环保局政府信息发布协调机制、公开保密审查、政府信息公开申请、投诉举报受理和机房设备管理等17项制度。根据安全保密工作需要，制定完善了《xx市环保局网络安全管理制度》、《信息发布审核制度》等22项安全保密工作制度，所有制度编制成册发到各部门遵照执行。

为保证制度落到实处，建立了网络及信息安全工作跟踪检查机制，局网络及信息安全工作领导小组定期通报各单位网络及信息安全工作及制度落实情况，发现问题，及时督促整改，并追究相关人员责任，使网络及信息安全工作真正做到制度化、经常化，切实落实安全保密工作长效机制。

明确保密领导责任和涉密岗位人员责任，落实了“谁主管，谁负责”的工作原则，为做好保密工作打下了良好基础。

局办公室及各业务科室在制作文件或内部资料时严格把关，对涉及国家秘密的文件资料依法定秘，明确密级、保密期限和知悉范围;按知悉范围最小化原则，发放涉密文件资料均根据工作需要，严格控制范围，认真履行登记、签收手续，在资料使用完毕后，均收回并实行专人、专柜管理，严禁擅自复印和转发;对不属于国家秘密但不宜公开的文件资料，标注“内部使用”，明确发放范围，未经单位负责人批准，不得扩大知悉范围;对可以部分公开或一段时间后可公开的文件资料，按文件资料明确的公开时间、内容和方式进行。

20xx年3月，我局整体完成新大楼搬迁，着力加强环境信息化能力建设，按照国家b级标准建设了专业的网络机房。面积达100余平方，采取全封闭式管理，可容纳服务器柜15台，目前架设ibm、浪潮等各类高性能服务器20余台，网络设备50余台，内设两台大功率精密空调，所有设备均连接ups保障停电等紧急情况下的设备安全正常运行。环保局网络接入中国电信百兆带宽，实现各科室、下属事业单位200多个“节点”的联网。为加强网络及硬件设备安全工作，采取以下措施：

1、服务器机房安装门禁系统，管理员通过门禁卡进入服务器房，并做好出入登记。服务器房按照区域划分责任人，负责日常维护管理工作，按制度规定定时检查服务器及防火防盗防雷设备。

2、服务器系统都安装瑞星防火墙和瑞星杀毒软件网络版，防止黑客、病毒入侵，工作计算机需与互联网实行彻底物理隔离，内网机之间尽可能使用内网邮件系统，减少使用移动存储介质;针对网络、服务器系统的安全，采取了有效的安全策略和措施，保障服务器的安全稳定运行，有效地防范了黑客、病毒的攻击。

3、架设vpn及上网行为管理设备。屏蔽存在威胁的网站，杜绝不当操作引起的涉密信息泄露及网络威胁。

4、建立完整的上网记录，禁止处理存储涉密信息和工作秘密信息;加强计算机、服务器及网络设备的密码安全管理工作，按照要求使用复杂性密码，定期进行修改。

5、严格管控移动存储介质，杜绝内外网u盘混用;根据现有关于环保工作的管理规定，尚没有明确的政务和业务归类于涉密范畴。为完善涉密管理机制，防范于未然，我局参照省委保密委员会与市委保密委员会相关文件规定，特设置一套计算机设备，按涉密计算机要求严格管理。

xx市环保网是由我局信息中心技术人员自主开发设计，采用基于asp/环境，结合sql server数据库开发设计，具有网站前后台分离技术，独立页面模板技术、页面全静态生成技术，后台动态管理等技术特点。信息发布及系统维护由专职编辑人员和技术人员负责，网站公开信息经认真核对后由分管领导审核，审核后的信息发布在xx市环保局政府网站。因工作需要，需要在其他网站转载信息的，要求来源于全国性门户网站和专业网站，且在转载其他网站信息前，编辑人员仔细核对，经分管领导审核确认无误后转载信息，确保信息真实性，对涉嫌泄密的信息一律禁止发布并上报有关部门。为应对网站系统突发事件，我局制定一整套完善的应急处理制度，安排专职人员每日定期检查网站访问、网站链接情况，做好日常巡逻和监测工作并做好检查记录，遇到突发事件，技术人员第一时间处置，恢复网站正常访问。

**网络安全检查自查报告篇五**

根据《海口市科学技术工业信息化局关于开展20xx年海口市网络安全检查行动的通知》(海科工信字〔20xx〕236号)要求，我局对网络安全情况进行了自查，现将自查情况汇报如下：

1、我局及时成立了信息安全检查行动小组。由分管领导任组长，办公室主任为副组长，办公室成员为组员的行动小组，负责对局网站检查的排查并填记有关报表、建档留存等工作。

2、信息安全检查小组对照网络与信息系统的实际情况进行了逐项排查、确认，并对自查结果进行了全面的核对、分析，提高了对网络与信息安全状况的掌控。

为加强我局网站的网络安全保护工作，依据《中华人民共和国政府信息公开条例》、《中华人民共和国计算机信息系统安全保护条例》，结合我局实际，制定了《海口市粮食局网络和信息安全事件应急处置和报告制度》、《海口市粮食局网络信息安全责任追究制度》、《海口市粮食局政府信息主动公开制度》、《海口市粮食局政府信息依申请公开制度》、《海口市粮食局政府信息公开工作考核评议制度》、《海口市粮食局政府信息公开工作年度报告制度》、《海口市粮食局政府信息公开责任追究制度》、《海口市粮食局政府信息公开保密审查制度》、《海口市粮食局网站管理制度》。

2、在网站信息处理和人员落实方面规定了栏目的内容及相应的信息提供实行各处室分工负责制。即各处室负责对本网站相应栏目提供内容，处室负责人要对所提交内容的真实性和可靠性进行认真审核，并提交分管领导进行审批。要发布的信息经最终确定后向办公室提供相应电子文档，办公室经办人员负责网站信息的分类、整理、更新、发布。

3、在网上互动及网上办事方面规定了网站所设置的意见箱等互动栏目中群众发布的咨询信息由办公室负责定时接收，并及时提交给相应处室予以解答。

4、在网站涉密信息方面明确了要严格遵守“上网不涉密，涉密不上网”的规定，确保党和国家秘密的绝对安全。

2、20xx年6月，开展信息系统等级测评工作，经评审，确定信息安全测评机构海南正邦信息科技有限公司对我局门户网站进行安全等级测评。

1、我局按照网络安全管理的规定，定期检查本系统内的漏洞、安全缺陷、病毒扫描等，安装了正版杀毒软件、防火墙。为确保网上信息安全，我局制定并严格遵守了保密管理规定，做到了“上网不涉密、涉密不上网”。

2、网站管理人员签订保密工作责任书。网站管理人员对网站也实行密码管理，用户名和开机密码专有且不得外泄。网站所要发布内容一律要通过管理员验证才能够发表、删除、修改。

3、为妥善应对和处置门户网站与信息系统突发事件，立足于最大程度减少安全事件对信息资产造成的损失，结合信息管理实际情况，制定了《网络与信息安全事件应急预案》。

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。今年组织2次信息员培训。增强内部人员的信息安全防护意识，有效提高工作的信息安全防护意识。

在自查过程中我们也发现了一些不足，同时结合我单位实际，今后要在以下几个方面进行整改。

存在不足：一是规章制度体系建立不够完善;二是信息系统安全保护技术力量薄弱;三是信息安全的资金不足;四是我局信息安全专业化服务力量薄弱。

整改方向：一是加强对机关干部计算机水平和网络安全意识教育，提高有关人员做好网络安全工作的主动性和自觉性，同时与信息中心运维人员保持密切联系，加强网站安全措施建设力度，进一步增加网站防篡改、防攻击、防瘫痪能力。二是完善现有网站安全管理制度;三是提高我局信息系统安全防护队伍的技术力量;四是追加信息安全等级保护经费。

**网络安全检查自查报告篇六**

我校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。同时在学校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。

**网络安全检查自查报告篇七**

根据公安部文件，我公司开展了相关工作，对办公电脑、网络安全、信息系统等进行了检查，加强对办公网信息和安全保密的管理，防止出现信息安全隐患及信息安全事故，将信息安全工作标准户、常态化。

网络安全管理工作情况

公司成立了由公司总经理任组长，各科室负责人为成员的领导小组，领导小组下设了办公室，安排网络安全维护工作。二是专门制订网络安全有关规章制度，对网络设备、安全管理、计算机操作人员管理维护责任等各方面都作了详细规定，进一步规范了我公司信息安全管理工作。三是及时对系统和软件进行更新，对重要文件、资源做到及时备份，数据恢复。

公司进一步扩大对网络安全知识培训面，组织信息员和干部职工进行培训，二是切实增强网络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，从而提高人员安全防护意识，三是以制度为根本，在进一步完善网络安全制度的同时，安排专人，完善设施，密切监测，随时随地解决可能发生的网络安全事故。

目前我公司所有网络设备、服务器及网络相关设备均未使用缺省密码，建立了核心网络设备及服务器应急处理预案，我公司所有网络设备及电脑在接入移动存储设备时，均按要求检1测病毒和木马，坚决杜绝病毒和木马在公司内网网络传播，严禁在网络设备及电脑终端上安装盗版软件和与工作无关软件，严禁通过代理访问网络，电脑终端安装防病毒软件和杀毒软件。定时更新网络防火墙的登录密码，及时更新病毒及木马信息，防止外网攻击入侵到公司网络设备及办公网中。建立机房网络设备及服务器档案，保存各网络设备及服务器的配置信息、参数等。

我公司建立信息化管理组织机构，明确信息管理专业负责人和职责，完善信息管理制度，不定期检查运维的日常工作，每年组织信息安全管理培训，尽可能的让公司所有员工都能了解信息安全的重要性，保证日常工作中正确使用办公电脑，使用安全性高的口令并定时更换口令，保护公司的信息财产安全。

定期检查机房内的消防、空调、监控、ups、环境监测、照明、噪音、粉尘、接地等配套设施的工作状态，配套设施的维护、维修、升级、更新、换代等工作有序进行，查看进入机房的登记记录及机房监控，保证机房设备的正常运行。

公司员工访问企业邮箱、移动办公、oa等系统均使用唯一认证身份信息，各系统对所有员工进行权限分配，员工调离工作岗位时各系统权限同步变更。所有管理员账户仅在系统升级或系统维护时使用，禁止多方持有管理员账户。

二、目前存在的问题由于专业技术人员较少，网络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，三是遇到网络病毒侵袭等突发事件处理不够及时有效。

对存储介质的管理还不到位，只是对存储介质的接入和传播进行管理，可能存在一定的网络安全隐患。

网络行为管理及审计工作还不到位，缺少必要的网络硬件设备。

对网络安全基础培训等开展的次数还不够多。

二、下一步计划：

公司今后要建立网络安全机制。建立网络安全协调制度，协调跨部门的网络安全工作;建立重大网络安全事件会商制度，提高网络安全应急反应和处理能力。

公司要搞好网络安全体系建设。开展网络安全风险评估工作。选择部分网络系统，对其安全系统的潜在威胁进行分析评估，发现问题，查找隐患。各网络系统根据实际情况建立和完善安全监控系统，提高网络防范能力，加强网络安全监控和管理。建立网络安全应急处理机制。

公司要加大网络安全的资金投入。切实保障网络安全建设的投入和运行维护费用。加大对网络安全基础设施建设和基础性工作的资金支持力度，不断提高资金的使用效益。

在下一步的工作中，我公司将继续严保网络安全，强化保3密意识，落实管理责任，确保公司信息化工作的正常安全运行。

**网络安全检查自查报告篇八**

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、网络入出口安全、数据安全等。物理安全主要是设施设备的防火防盗、物理损坏等。网络入出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、对我校几大网站平台的帐户、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2024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、二小博客上的贴子，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。

**网络安全检查自查报告篇九**

为了加强我校教育信息网络安全管理，保护信息系统的安全，促进我校信息技术的应用和发展，保障教育教学和管理工作的顺利进行，并配合省公安厅、省教育厅(豫公通220号文件精神，对我校计算机信息系统开展以“反黑客、反破坏、扫黄打非、清理垃圾邮件”为主要内容的安全大检查，净化校园网络环境，不断提高学校计算机信息系统安全防范能力，从而为学生提供健康，安全的上网环境。

为落实“教育部办公厅关于开展网络安全检查的通知”(教技厅函51号)、“教育部关于加强教育行业网络与信息安全工作的指导意见”(教技4号)、陕西省教育厅“关于开展全省教育系统网络与信息安全专项检查工作的通知”(陕教保【20xx】8号)，全面加强我校网络与信息安全工作，校信息化建设领导小组办公室于9月16日-25日对全校网络、信息系统和网站的安全问题组织了自查，现将自查情况汇报如下：

一、学校网络与信息安全状况

本次检查采用本单位自查、远程检查与现场抽查相结合的方式，检查内容主要包含网络与信息系统安全的组织管理、日常维护、技术防护、应急管理、技术培训等5各方面，共涉及信息系统28个、各类网站89个。

从检查情况看，我校网络与信息安全总体情况良好。学

校一贯重视信息安全工作，始终把信息安全作为信息化工作的重点内容。网络信息安全工作机构健全、责任明确，日常管理维护工作比较规范;管理制度完善，技术防护措施得当，信息安全风险得到有效降低;比较重视信息系统(网站)系统管理员和网络安全技术人员培训，应急预案与应急处置技术队伍有落实，工作经费有一定保障，基本保证了校园网信息系统(网站)持续安全稳定运行。但在网络安全管理、技术防护设施、网站建设与维护、信息系统等级保护工作等方面，还需要进一步加强和完善。

二、20xx年网络信息安全工作情况

1.网络信息安全组织管理

按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，学校网络信息安全工作实行“三级”管理。学校设有信息化工作领导小组，校主要领导担任组长，信息化工作办公室设在网教中心，中心主任兼办公室主任。领导小组全面负责学校网络信息安全工作，授权信息办对全校网络信息安全工作进行安全管理和监督责任。网教中心作为校园网运维部门承担信息系统安全技术防护与技术保障工作。各处室、学院承担本单位信息系统和网站信息内容的直接安全责任。

2.信息系统(网站)日常安全管理

学校建有“校园网管理条例”、“中心机房安全管理制度

“、“数据安全管理办法”、“网站管理办法”、“服务器托管管理办法”、“网络故障处理规范”等系列规章制度。各系统(网站)使用单位基本能按要求，落实责任人，较好地履行网站信息上传审签制度、信息系统数据保密与防篡改制度。日常维护操作较规范，多数单位做到了杜绝弱口令并定期更改，严密防护个人电脑，定期备份数据，定期查看安全日志等，随时掌握系统(网站)状态，保证正常运行。

3.信息系统(网站)技术防护

校园网数据中心建有一定规模的综合安全防护措施。

四是全面实行实名认证制度，具备上网行为回溯追踪能力;

五是对重要系统和数据进行定期备份，并建有灾备中心。

4.信息安全应急管理

20xx年制定了《西北农林科技大学网络与信息安全突发事件应急预案》。网教中心为应急技术支持单位，确保网络安全事件的快速有效处置。

5.信息安全教育培训

20xx年派员参加了陕西省信息安全保密培训。暑期处级干部培训安排有信息安全与保密专题，每年组织全校网管员技术培训，增强管理干部和技术人员的安全防范意识，提高技术防护能力。

三、检查发现的主要问题

对照《通知》中的具体检查项目，我校在信息安全工作上还存在一定的问题：

1.安全管理方面：网管员为兼职，投入精力难以保证，部分网管员长时间未登录过自己管理的系统(网站)，无法及时知晓已发生的安全事件。部分系统(网站)日常管理维护不够规范，仍存在管理员弱口令、数据备份重视不够、信息保密意识差等问题(20xx年发生2起个人隐私信息上传网站的事件)。

2.技术防护方面：校园网安全技术防护设施仍不足，如缺少数据中心安全防御系统和审计系统，欠缺安全检测设施，无法对服务器、信息系统(网站)进行安全漏洞扫描与隐患检查。

3.应用系统(网站)方面：个别应用系统(网站)存在设计缺陷和安全漏洞，容易发生安全事故。(经统计20xx年以来14个网站发生安全事故17起，其中11起是因为网站存在技术问题，如安全漏洞或设计缺陷)。

4.信息系统等级保护工作尚未全面开展。

5.部分院(系)管辖的机房或学习室尚未实行认证和审计。

四、整改措施

针对存在的问题，学校信息化领导小组专门进行了研究部署。

1.进一步完善网络信息安全管理制度，规范信息系统和网站日常管理维护工作程序。加强网管员技术培训，提高安全意识和技术能力。

2.继续完善网络信息安全技术防护设施，配备必要的安全防御和检测设备，实行信息系统(网站)安全检测准入制度，从根本上降低安全风险。定期对服务器、操作系统进行漏洞扫描和隐患排查，建立针对性的主动防护体系。

3.针对各级网站建设水平参差不齐问题，学校20xx年引入了站群系统管理平台，目前已将多个部门共计12个网站迁移到站群系统管理平台。今后将加大推进力度，逐步将全部各级网站迁入站群系统管理平台，提高网站技术安全性能。

4.全面开展信息系统等级保护工作，按照新颁布的《教育行政部门及高等院校信息系统安全等级保护定级指南》，完成所有在线系统的定级、备案工作。积极创造条件开展后续定级测评、整改等工作。

5.加强应急管理，修订应急预案，组建以网教中心技术人员为骨干、重要系统管理员参加的应急支援技术队伍，加强部门间协作，做好应急演练，将安全事件的影响降到最低。

6.对院(系)管机房或学习室强制认证和审计。

五、几点建议

3.建议各类网站在适当的时候(最好是改版时)加入学校站群系统管理平台，一旦加入该站群系统管理平台，管理者将无需考虑网站的技术安全及风险，只需考虑网站的信息与内容安全。

坏、扫黄打非、清理垃圾邮件”为主要内容的安全大检查，净化校园网络环境，不断提高学校计算机信息系统安全防范能力，从而为学生提供健康，安全的上网环境。

一、领导重视，责任分明，加强领导

为了认真做好迎检准备工作，进一步提高教育网络信息安全工作水平，促进教育信息化健康发展，我校建立了专门的网络信息安全管理组织，成立了由分管领导、网络管理员组成的计算机网络信息安全管理领导小组。负责制定学校计算机信息系统安全管理的办法和规定，协调处理全校有关计算机信息系统安全的重大问题;负责学校计算机信息系统的建设、管理、应用等工作;负责信息系统安全的监督、事故的调查和处罚。学校网络管理人员要在学校计算机安全管理领导小组的领导下，负责校园网的安全保护工作和设备的维护工作，必须模范遵守安全管理制度，积极采取必要的防范技术措施，预防网络安全事故的发生。

二、完善制度，加强管理

为了更好的安全管理网络，我校建立了健全的安全管理制度：

(一)计算机机房安全管理制度

1、重视安全工作的思想教育，防患于未然。

2、遵守“教学仪器设备和实验室管理办法”，做好安全保卫工作。

3、凡进入机房的人员除须遵守校规校纪外，还必须遵守机房的各项管理规定，爱护机房内的所有财产，爱护仪器设备，未经管理人员许可不得随意使用，更不得损坏，如发现人为损坏将视情节按有关规定严肃处理。

4、机房内禁止吸烟，严禁明火。

5、工作人员必须熟悉实验室用电线路、仪器设备性能及安全工作的有关规定。

6、实验室使用的用电线路必须符合安全要求，定期检查、检修。

7、杜绝黄色、迷信、反动软件，严禁登录黄色、迷信、反动网站，做好计算机病毒的防范工作。

8、工作人员须随时监测机器和网络状况，确保计算机和网络安全运转。

9、机房开放结束时，工作人员必须要关妥门窗，认真检查并切断每一台微机的电源和所有电器的电源，然后切断电源总开关。

(二)操作人员权限等级分配制度

1、校领导统一确定操作人员职能权限。

2、电教组成员负责管理、维修学校所有计算机，出现重大事故应及时报上级领导。

3、教师用户帐号、密码由网络管理员发放，并统一管理。

4、学校计算机管理人员需定期维护计算机软件和数据，重要信息定期进行检查和备份。

5、网络管理员负责校园用户计算机系统能够正常上网，为用户提供日常网络维护服务和日常数据备份。

(三)账号安全保密制度

1、网络用户的账号、密码不得外传、外借。

2、非法用户使用合法用户的账号进入校园网的，追究该帐号拥有者的安全责任。

(四)计算机病毒防治制度

1、学校购买使用公安部颁布批准的电脑杀毒产品。

2、未经许可证，任何人不得携入软件使用，防止病毒传染。

3、凡需引入使用的软件，均须首先防止病毒传染。

4、电脑出现病毒，操作人员不能杀除的，须及时报电脑主管处理。

5、在各种杀毒办法无效后，须重新对电脑格式化，装入正规渠道获得的无毒系统软件。

6、建立双备份制度，对重要资料除在电脑贮存外，还应拷贝到软盘上，以防遭病毒破坏而遗失。

7、及时关注电脑界病毒防治情况和提示，根据要求调节电脑参数，避免电脑病毒侵袭。

(五)安全教育培训制度

1、学校组织教师认真学习《计算机信息网络国际互联网安全保护管理办法》,提高教师的维护网络安全的警惕性和自觉性。

2、学校负责对本校教师进行安全教育和培训，使教师自觉遵守和维护《计算机信息网络国际互联网安全保护管理办法》，使他们具备基本的网络安全知识。

3、校管理中心对信息源接入的骨干人员进行安全教育和培训，使之自觉遵守和维护《计算机信息网络国际互联安全保护管理办法》，杜绝发布违犯《计算机信息网络国际互联网安全保护管理办法》的信息内容。

(六)、事故和案件及时报告制度

1、任何单位和个人不得利用互联网制作、复制、查阅和传播下列信息：

煽动抗拒、破坏宪法和法律、行政法规实施。

煽动颠覆国家政权，推翻社会主义制度。

煽动分裂国家、破坏国家统一。

煽动民族仇恨、民族歧视、破坏民族团结。

捏造或者歪曲事实、散布谣言，扰乱社会秩序。

宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪。

公然侮辱他人或者捏造事实诽谤他人。

损害国家机关信誉。

其他违反宪法和法律、行政法规。

如发现有上述行为，保留有关原始记录，并填写好《安全日志》，在12小时内向上级报告。

2、接受并配合区电教中心和公安机关的安全监督、检查和指导，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。

3、发现有关计算机病毒、危害国家安全、违反国家有关法律、法规等计算机安全案情的，应在12小时以内向上级报告。

4、计算机机房设管理员一名，其职责是每天不定期浏览主页或自己页面，负责领导还应经常巡视操作者，如发现有违反上述规定者应立即制止并报告校园网安全领导小组。

(七)、面对大面积病毒应急处理方案

1、制定计算机病毒防治管理制度和技术规程，并检查执行情况;

2、培训计算机病毒防治管理人员;

3、采取计算机病毒安全技术防治措施;

4、对网站计算机信息系统应用和使用人员进行计算机病毒防治教育和培训;

5、及时检测、清除计算机系统中的计算机病毒，并做好检测、清除的记录;

6、购置和使用具有计算机信息系统安全专用产品销售许可证的计算机病毒防治产品;

7、向公安机关报告发现的计算机病毒，并协助公安机关追查计算机病毒的来源;

8、对因计算机病毒引起的计算机信息系统瘫痪、程序和数据严重破坏等重大事故及时向公安机关报告，并保护现场。

除以上健全的安全管理制度外，我校也认真落实相关安全技术措施，安全基础措施良好拥有完善的安全保护措施，设有学校重要部位值班制度，做到昼夜值班，任何人不得擅自进入微机房。

**网络安全检查自查报告篇十**

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。

**网络安全检查自查报告篇十一**

根据广西壮族自治区网络安全和信息化领导小组办公室《2024年全区网络安全检查工作方案》工作要求，我院开展了相关工作，对办公电脑、网络安全、信息系统等进行了检查，加强对办公专网信息和安全保密的管理，防止信息泄密。现将检查结果汇报如下：

1.我院已采取技术措施（广西高院统一安装360内网认证）对办公内网使用的移动存储（u盘、移动硬盘等）介质管控。办公专网的信息交换基本符合保密相关规定。我院内网电脑均按照高院的要求安装内网安全管理系统，信息的刻入经过病毒或恶意代码检测（内网江民杀毒软件负责检测），刻入由办公室网络管理员负责，以确保光盘刻出的数据不包含工作秘密或其他敏感信息。用于数据交换的光盘均按要求标识标注涉密程度和光盘内容信息。

2．我院目前还没有使用涉密信息办公专网，从宜州市保密局、机要局领取回来的涉密文件均采用纸质化浏览，并做好涉密纸质化文件登记。没有安装涉密信息自动审查系统，办公室会根据宜州市保密局的要求，每年对我院内网电脑扫描排查一次。如发现违规问题，首先将情况汇报院领导办公室主任，其次汇报宜州市保密局和河池市中级人民法院，最后根据上级单位的意见处理相关责任人。我院的死刑统计数据、大案要案审理等涉密数据目前暂未出现上述数据违规上办公专网的情况。3.办公内网与其他网络已经进行物理隔离，每台电脑只允许接入一种网络。因我院禁止办公内网与其他网络进行信息交换，所以不需要制定规范的工作方案。

4.边界安全和信任体系建设基本完善。通过广西高院的360内网认证实现必要的用户身份认证和授权管理等安全防护措施。院内中心机房已经安装了防火墙和入侵检测等安全设备并正确设置发挥效用。

5.办公专网用户接入身份统一使用广西法院综合门户网站的账号和密码，采取了360内网身份认证进行准入控制。办公专网用户访问权限根据需要设置为文秘、院长、庭长、一般干警。

6.负责办公专网运维的公司我院没有外包给其他公司，所以不涉及需要涉密资质的认定，不需要签订保密协议。

7.没有办公专网内擅自安装无线网络、无线鼠标、键盘、摄像头或国家安全保密部门明令禁止安装的硬件或软件。

8.保密工作部门和技术部门负责保密管理的人员配备与担负的职责，按照广西高级人民法院、河池中级人民法院、宜州市保密局、机要局的通知要求设置，并参加过相应的涉密、保密的培训，能够有效的开展办公保密管理工作。

9、我院除旧锐新审判系统外，其他的信息系统都是由上级法院统一委托外包公司进行开发，服务器、数据库都架设在上级法院，由上级法院统一管理，并进行安全评估。

三、目前存在的问题

1、对存储介质的管理还不到位，只是对存储介质的接入和传播进行管理，未配备统一的储存介质销毁工具，可能存在一定的网络安全隐患。

2、对重点检查网络安全宣传教育、领导干部及各级人员网络安全基础培训、网络安全人员专业技术培训等开展的次数还不够多，个别同志网络安全意识还不到位。

下一步计划：

今年来，我院未发生办公专网失泄密事件。在下一步的工作中，我院将继续严格网络安全，强化保密意识，落实管理责任，确保全院信息化工作的正常安全运行。

二〇一五年十月十三日

**网络安全检查自查报告篇十二**

（一）网络安全。我局所有计算机均配备了防病毒软件，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）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”，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。重点抓好“三大安全”排查：一是加强对硬件安全的管理，包括防尘、防潮、防雷、防火、防盗、和电源连接等；二是加强网络安全管理，对我局计算机实行分网管理，严格区分内网和外网，合理布线，优化网络结构，加强密码管理、ip管理、互联网行为管理等；三是加强计算机应用安全管理，包括邮件系统、资源库管理、软件管理等。定期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。

**网络安全检查自查报告篇十三**

根据xxx发[xx]x号文件《开展xx市电子政务网信息安全与网络管理专项检查的通知》文件精神，我局积极组织落实，认真对照，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，对我局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、充实领导机构，加强责任落实

为进一步加强全系统网络信息系统安全管理工作，我局成立了网络与信息系统安全保密工作领导小组，做到分工明确,责任具体到人。安全工作领导小组，组长xxx，副组长xxx，成员有xxx、xxx、xxx。分工与各自的职责如下：xxx副局长为我局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。办公室主任xxx分管计算机网络与信息安全管理工作。xxx负责计算机网络与信息安全管理工作的日常事务，上级教育主管部门发布的信息、文件的接收工作。xxx负责计算机网络与信息安全管理工作的日常协调、督促工作。xxx负责网络维护和日常技术管理工作。

二、开展安全检查，及时整改隐患

1、我局网络中心、办公室、会议室、办事窗口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、网络入出口安全、数据安全等。物理安全主要是设施设备的防火防盗、物理损坏等;网络入出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、对我局几大网站平台的帐户、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，我局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，保证了我局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，我局对外的服务器有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，由于我局领导的高度重视，管理得当，我局从20xx年建立政务办公网到现在，还没有任何黑客攻入内网的记录。

4、强化网络安全管理工作，对所有接入我局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。每周定时对我局门户网站的留言簿、二小博客上的贴子，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，及时向上汇报。6、本期第三周我局在干部职工大会组织人员学习有关信息网络法律法规,提高干部职工合理、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、存在的问题和不足之处

1、由于我局的网络终端300多个点，管理难度大，局里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、我局的服务器共有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、我局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，尽最大努力把我局网络安全工作做到更好，给全局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。

**网络安全检查自查报告篇十四**

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。

**网络安全检查自查报告篇十五**

县人社局：

为了贯彻《职工带薪年休假条例》、《企业职工带薪年休假实施办法》及省、市、县关于落实职工带薪年休假相关文件精神，切实保障职工的合法权益，根据县人社局《关于开展落实职工带薪年休假制度落实情况自查的通知》（扶人社发〔20xx〕162号）文件精神，经镇政府决定对全镇辖区内职工带薪年休假执行情况进行专项检查。现将专项检查情况总结如下：

一、高度重视，周密部署

按照县上文件精神，我镇从切实维护职工权益、构建和谐劳动关系的高度，充分认识开展专项行动的重要意义，立即召开专题会议进行研究，成立xx镇职工带薪年休假专项检查领导小组，镇长任组长，主管劳动保障的副镇长为副组长，成员单位有镇政府办公室、劳保所、派出所、企业办、妇联，领导小组下设办公室，办公室设在镇公共服务中心，副组长兼任办公室主任，并决定从5月28日起至6月5日，对辖区餐饮、加工制造等劳动密集型企业进行一次专项检查。本次专项检查注重宣传教育，采取企业先自查自纠，镇上对辖区内用人单位重点检查，层层分解落实了工作任务，严明了工作纪律，要求各检查人员要深入到一线，检查中不得走过场、走形式，务求实效，从而为专项检查工作的顺利开展打下了坚实的基础。

二、加大宣传，营造氛围

假实施办法》，修订完善用人单位职工带薪年休假有关制度。二是镇上检查人员深入企业与职工交流对话，宣传政策规定，共印发宣传资料500余份，为维护劳动者合法权益营造了良好氛围。

三、做好自查，建章立制

专项检查开展前，我们要求相关用人单位对其职工带薪年休假的情况认真开展自查自纠，对存在的问题要有明确的整改方案，通过与企业工会或职工民主协商，在处理好依法享受带薪休假和保证生产经营正常运转的情况下，建立健全带薪年休假制度。

四、加强督查，依法行政

1、畅通渠道。为使劳动保障违法行为及时得到制止，我们公布了举报投诉电话xxxxxxx，广开信息渠道，及时、准确捕捉各种举报投诉信息。

2，严格执法。检查中充分发挥和依靠各部门的力量，对所辖区域内的餐饮、加工制造等劳动密集型企业的用人单位遵守执行国家工作时间和休息休假制度、职工带薪年休假制度、法定节假日加班工资支付等情况全面排查，检查组针对检查中发现的违法违规问题，限期改正，从而确保此次专项行动收到了实效。此次专项行动，共检查22户企业，涉及职工2355人，在检查中，各企业均能做到年休假的落实，在落实中企业按照自身发展情况，通过夏收假、收秋假及法定节假日分批次休假，但由于企业在生产过程中盈利低的原因，大多数没有做到带薪年休假，为此检查小组及时将企业关于带薪年休假有关政策落实不到位情况予以当面通报，并与企业协商尽快按照政策逐步予以落实。

通过开展此次专项行动，发现我辖区的部分企业单位对职工带薪年休假制度了解的不够，认识还不到位，执行也很不理想，存在问题较为普遍，目前由于岗位少求职者多，多数员工为了保住工作而委曲求全，这个方面投诉举报也很少。在推进职工带薪年休假制度的落实上，还应该着力做好以下几个方面：一是加强宣传，让职工明白带薪年休假制度是法律赋予职工的权利不可侵犯，职工个人也要在追求经济利益的同时，也从自身健康的角度出发，合理安排个人时间，能正确处理好二者之间的平衡。二是企业自律，落实《职工带薪年休假条例》，单位的积极态度是关键，制订相应的制度和规定，做到有章可循。三是加强监督，检查小组在日常巡查和专项检查中应把职工带薪年休假情况作为一项检查内容督促落实，要通过宣传政策、法律、规章制度，让企业和职工明确各自的权利和义务，促使劳动者和企业在民主协商的基础上解决带薪休假方面出现的劳动争议，建立平等的、互相尊重的合作关系，以促进和谐劳动关系的构建，推动社会安定团结。

20xx年6月5日

本文档由028GTXX.CN范文网提供，海量范文请访问 https://www.028gtxx.cn