# 网络安全自查阶段工作计划(27篇)

来源：网络 作者：青苔石径 更新时间：2024-02-09

*网络安全自查阶段工作计划1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：>...*

**网络安全自查阶段工作计划1**

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、加强领导，深化意识

(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。

(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。

>二、健全机制，落实责任

(一)抓好制度的完善

通过认真学习《\_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《\_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。

(二)抓好制度的落实

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。

>三、加强管理，规范程序

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。

(一)加强文件制发的管理

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。

(二)加强网络及硬件设备的管理。

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。

**网络安全自查阶段工作计划2**

为进一步加强和改进街道网络安全工作，落实党管意识形态原则，牢牢掌握网络安全工作的领导权、主动权，明确党工委领导班子、干部的网络安全工作责任，根据上级文件要求结合我街道实际制定本方案实施。

一、领导小组

组长：

副组长

成员：

王慧街道宣传文化办公室副主任

同时，各社区要相应成立网络安全工作组，全面负责社区网络安全具体工作。

二、工作职责

1.负责贯彻落实上级网络工作的部署和要求，依据“谁使用、谁主管、谁负责”的原则，加强网络安全工作的领导，落实工作责任。

2.严格落实滨河街道党员干部新媒体使用管理制度，确保网络安全运行。

3.负责开展网络安全的工作检查。

4.负责统筹、协调本单位的网络安全事件应急工作，并配合上级主管部门做好网络安全相关应急处置工作。

领导小组下设办公室，办公室设在宣传文化办，办公室主任由王慧兼任，负责网络安全相关事务工作，领导小组人员如有变动，由有关人员自行接替，不再另文通知。

三、工作目标

全面落实《自治区各级党委（党组）网络安全工作责任制实施细则》，牢牢掌握网络安全工作领导权、管理权、话语权，确保网络空间更加明朗，让党的声音成为网络空间最强音，形成共同防范社会风险、共同构筑同心圆的良好局面，切实巩固党的执政根基，维护国家政治安全和\_安全。

四、工作任务

（一）加强网络安全统筹部署

加强网络安全领导小组的统筹领导，贯彻落实《自治区各级党委（党组）网络安全工作责任制实施细则》，研究上级网信部门网络安全重要会议精神，对街道社区网络安全工作作出部署。

（二）推进网络安全学习教育

组织中心组成员积极学习《网络安全和信息化政策汇编》，开设网络安全知识讲堂，充分利用街道社区微信公众号和居民群用好网言网语。

（三）强化网络安全宣传教育

重视社区文化建设，开展丰富多样的网络安全教育宣传活动，提高辖区居民网络安全意识，营造良好的社会氛围。

五、保护措施

（一）深入贯彻落实《网络安全法》

进一步完善相关网络安全有关制度和标准规范。持续推进网络安全监测预警通报机制，建立常态化的通用软件安全评估机制。

（二）加强系统数据安全防护能力

研究制定网络安全应急预案，建立数据分级保障的工作机制，加强数据全生命周期管理。开展数据安全专项自查行动，全面排查个人信息保护存在的安全隐患。

（三）建立常态化的网络安全保障机制

**网络安全自查阶段工作计划3**

>一、信息安全自查工作组织开展情况

1、成立了信息安全检查行动小组。由站长、书记任组长，相关科室（车间）负责人、信息技术科全体人员为组员负责对全站的重要信息系统全面排查并填记有关报表、建档留存。

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、梳理、分析。整改，提高了对全站网络与信息安全状况的掌控。

>二、网络与信息安全工作情况

1、8月2日前开展网络语信息系统的自查工作部署。

1）组织成立了网络与信息安全检查工作小组，由站长、书记任组长，相关科室（车间）负责人、信息技术科全体人员为组员。

2）研究制定自查实施方案，根据系统所承担的业务的独立性、责任主体的独立性、网络边界的独立性、安全防护设备设施的独立性四个因素，对客票发售与预订系统、旅客服务系统、办公信息系统进行全面的梳理并综合分析。

2、8月6日前对客票发售与预订系统、旅客服务系统、办公信息系统的基本情况进行逐项排查。

1）系统安全基本情况自查

客票发售与预订系统为实时性系统，对车站主要业务影响较高。目前拥有IBM服务器2台、cisco路由器2台、cisco交换机13台，系统均采用windows操作系统，灾备情况为系统级灾备，该系统不与互联网连接，防火墙采用永达公司永达安全管控防火墙。

旅客服务系统为实时性系统，对车站主要业务影响较高。目前拥有HP服务器13台、H3C路由5台、H3C交换机15台，系统采用linix操作系统，数据库采用SQLServer，灾备情况为数据灾备，该系统不与互联网连接，安全防护策略采用按照使用需求开放端口，重要数据均采用加密防护。

办公信息系统为实时性系统，对车站主要业务影响一般。目前拥有IBM服务器1台、cisco路由器1台、cisco交换机2台，系统采用windows操作系统，数据库采用SQLServer，灾备情况为数据灾备，该系统不与互联网连接，安全防护策略采用按照使用需求开放端口，重要数据均采用加密防护。

2）安全管理自查情况

人员管理方面，指定专职信息安全员，成立信息安全管理机构和信息安全专职工作机构。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》。

资产管理方面，指定了专人进行资产管理，完善了《资产管理制度》、《设备维修维护和报废管理制度》，建立了《设备维修维护记录表》。

存储介质管理方面，完善了《存储介质管理制度》，建立了《存储介质管理记录表》。

运行维护管理方面，建立了《客服系统维护标准》、《运行维护操作记录表》，完善了《日常运行维护制度》。

3）网络与信息安全培训情况

制定了《太原站网络与信息安全培训计划》，20xx年上半年组织信息安全教育培训2次，接受信息安全培训人数20人，站单位中人数的5%。组织信息安全管理和技术人员参加专业培训10人次。

**网络安全自查阶段工作计划4**

学校领导高度重视校园网络安全与信息安全工作，校网络与信息安全工作领导小组对学校网络安全建设、信息系统和网站的安全问题组织了自查，现将主要情况汇报如下：

>一、学校网络与信息安全工作情况

本次检查内容主要包含网络与信息系统安全的管理机构、规章制度、设施设备、网站和信息运行情况、人技防护、队伍建设等5个方面，同时从物理安全差距、网络安全差距、主机安全差距、应用安全差距、数据安全及恢复差距等5个方面对主机房和14个信息系统、1个网站进行等级保护安全技术差距分析，通过差距分析，明确各层次安全域相应等级的安全差距，为下一步安全技术解决方案设计和安全管理建设提供依据。

从检查情况看，我校网络与信息安全总体运维情况良好，未出现任何一起重大网络安全与信息安全事件(事故)。近几年，学校领导重视学校网络信息安全工作，始终把网络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;管理制度较为完善，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;加强对学生网络宣传引导教育，日常重视微信、微博、QQ群的管理，提倡争当“绿色网民”;工作经费有一定保障，网络安全工作经费纳入年度预算，在最近一年学校信息化经费投入中，网络建设与设备购置费用约占，数字资源与平台开发费用约占，培训费用约占，运行与维护费用约占，研究及其他费用约占，总计投入占学校同期教育总经费支出的比例约，基本保证了校园网信息系统(网站)持续安全稳定运行。

1.网络信息安全组织管理

xx年学校成立网络与信息安全工作领导小组，校主要领导担任组长，网络与信息安全工作办公室设在党委工作部，领导小组全面负责学校网络信息安全工作，教育技术与信息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，对全校网络信息安全工作进行安全管理和监督责任。各部门承担本单位信息系统和网站信息内容的直接安全责任。xx年，由于人事变动，及时调整网络安全和信息安全领导小组成员名单，依照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，明确各部门负责人为部门网站的具体负责人，建立学校网络信息员队伍，同时，还组建网络文明志愿者队伍，对网络出现的热点问题，及时跟踪、跟帖、汇报。

2.信息系统(含网站)日常安全管理

学校建有“校园网络系统安全管理(暂行)条例”、“学生上网管理办法“、“校园网络安全保密管理条例(试行)”、“校园网管理制度”、“网络与信息安全处理预案”、“网上信息监控制度”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。日常监控对象包括主要网络设备、安全设备、应用服务器等，其中网络中的边界防火墙、网络核心交换机和路由器、学校门户网站服务器均纳入重点监控。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

学校网络信息安全前期的防控主要是基于山石防火墙、深信服防火墙及行为管理软件，xx年为加强校园网络安全管理，购置了“网页防篡改、教师行为管理、负载均衡”等相关安全设备，xx年二月中旬完成校园信息系统(含网站)等级保护的定级和备案，并上报宁德市网安支队。同时，按二级等保要求，约投资110万元，完成“网络入侵防御系统、网络安全审计系统、运维审计-堡垒机系统、服务及测评及机房改造(物理安全)”等网络安全设备的采购工作，目前，方案已经通过专家论证。

xx年4月-6月及xx年3月对网站系统进行安全测评，特别对系统层和应用层漏洞扫描，发现(教务管理系统、教学资源库)出现漏洞，及时整改，并将结果上报省教育厅、省网安大队、宁德市网安支队。同时，对各防火墙软件7个库进行升级，对服务器操作系统存在的漏洞及时补丁和修复，做好网站的备份工作等。

4.网络信息安全应急管理

xx年学校制定了《宁德职业技术学校网络与信息安全处理预案》、《宁德职业技术学校网络安全和学生校内聚集事件应急处置预案》。教育技术与信息中心为应急技术支持单位，在重大节日及敏感时期，采用24小时值班制度，对网络安全问题即知即改，确保网络安全事件快速有效处置。

>二、检查发现的主要问题

对照《通知》中的具体检查项目，我校在网络与信息安全技术和安全管理建设上还存在一定的问题：

1.由于学校信息化建设尚处于起步阶段，学院数据中心建设相对薄弱，未建成完善的数据中心共享体系，各应用系统的数据资源安全及灾备均由相关使用部门独自管理。同时，网络安全保障平台(校园网络安全及信息安全等级保护)尚在建设中。

2.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、信息保密意识较差等问题;学校子网页网管员为兼职，投入精力难以保证，而且未取得相应资格证书;由于经费问题，个别应用系统未能及时升级，容易发生安全事故。

3.目前尚未开展网络安全预案演练，还未真正组建一支校内外联合的网络安全专家队伍，未与社会企业签订应急支持协议和完成应急队伍建设规划。

>三、整改措施

针对存在的问题，学校网络与信息安全工作领导小组专门进行了研究部署。

1.全面开展信息系统等级保护工作。按照相关《通知》要求，xx年8月底全面完成网络安全保障平台建设，根据系统在不同阶段的需求、业务特性及应用重点，采用等级化与体系化相结合的安全体系设计方案，形成整体的等级化的安全保障体系，同时根据安全技术建设和安全管理建设，保障信息系统整体的安全。

2.完善网络安全管理制度。根据等级保护要求,进行信息安全策略总纲设计、信息安全各项管理制度设计、信息安全技术规范设计等，保障信息系统整体安全。

3.加强网络安全队伍建设。加强网络安全应急队伍建设，组建校内外专家联同的网络安全专家队伍，与社会企业签订应急支持协议和完成应急队伍建设规划，提升网络安全应急队伍业务素质;加强网管员技术培训，提高安全意识和技术能力;加强学校网络安全主题宣传教育活动，加强校园微信、微博、QQ群、辅导员博客、易班、百度贴吧的建设管理，提升师生文明素养、争做文明使者，构建积极、健康、文明的校园网络环境;在特殊敏感时期加强网络舆情监控，发现问题及时处理并上报，有效防止网络事件的发生;切实做好网络安全应急演练，在演练中完善应急预案，降低网络安全事件风险的发生;建立网络安全责任追究制度，依据责任追究制度对发生的网络安全事件(事故)进行追责，同时将网站安全工作的执行情况纳入到年度考核指标。

4.经费保障。教育信息化是国家信息化和社会信息化的重要内容，是教育面向社会发展的一项重要任务，也是当前教育发展的一个重要课题。在“十三五”示范性现代高等职业院校建设期间，学校的信息化建设任务相当繁重，必须以《国家教育信息化十年发展规划(20xx-20xx年)》为指导，依据《职业院校数字校园建设规范》(教职成函[xx]1号)等要求，按照“顶层设计、统一标准、数据共享、应用集成、硬件集群、一站式服务”的规划建设理念，加大力度深入推进“数字宁职”建设。目前，学校制订了“校园信息化建设五年规划”，总经费投资862万元，其中网络安全预投资180万元，以确保网络安全装备的维护和更新需要。

**网络安全自查阶段工作计划5**

越来越多的商务楼开始采用宽带网FTTB(光纤到楼)方式，向租户提供Internet接入服务。大楼物业向租户提供100M以下带宽，供商务楼用户采用共享或独享带宽的方式接入Internet。

入户的每条线路仅可供一台电脑上网，无法实现局域网共享一条线路同时上网。从技术角度而言，用户必须要投入路由器设备进行网络地址翻译(NAT)，才可以实现局域网共享上网；由于入户的线路另一端都直接连在大楼的主干交换机上，因而造成大楼内部这一开放的网络环境存在很大的安全隐患：

大楼内各公司的计算机直接或间接通过本公司的交换机或集线器连接到主干交换机上。这样，就使得大楼所有租户的计算机在物理链接都处在同一个局域网内；

大楼内部的个别用户可以通过更改IP等简单手段轻松进入其他用户的网络，查看或窃取数据，甚至进行网络破坏活动；

对于在本地搭建网站，设立E-Mail、DNS和FTP等Internet应用服务器的用户，由于拥有固定不变的静态IP地址，因此网络更容易受到来自外部的恶意攻击和入侵。

那么，如何保护公司的数据安全呢？

方案简述：

大厦内使用宽带资源的公司在其内部交换机与大厦交换机之间加装防火墙产品后，用户可以直接通过防火墙产品迅速建立高速上网通道，并对此通道进行安全管理与安全控制，可以方便有效地满足客户的上网需要，同时伴随着安全需求，而且无需再投入昂贵的路由器设备，降低了用户的网络建设门槛。

防火墙放置于大厦楼层交换机与各公司交换机或集线器之间，使防火墙成为控制公司内部网络访问Internet的唯一通道，可以保证该公司整个网络的安全。

**网络安全自查阶段工作计划6**

衡量一个学校信息化水平高低的重要标志之一就是是否有一支掌握现代教育技术的师资队伍。努力建设一支掌握现代教育技术的师资队伍是学校信息化建设的重中之重。为适应信息社会对学校教育管理工作的新要求，加强对学校网站、网络的管理，提升教师教育信息技术能力，为各项教学竞赛活动提供技术支持与保障，经学校研究决定，成立网络安全和信息化指导小组。为保证相关工作的开展正常、有序、高效，特制定本方案。

一、领导小组

组长副组长

成员：学校其他行政成员

二、技术团队

1.网络安全与保障小组：

（组长）、

2.信息技术支持组：

（组长）、\_\_

三、工作职责

1.网络安全与保障组：负责管理学校网站、QQ群，保障各教学楼、综合楼办公室、电脑教室、录播教室网络的正常顺畅运行。

2.信息技术支持组：保障学校监控系统、广播系统的正常运行；对学校新、旧多媒体教室和广播室的正常运行，以及学校大型活动提供技术和设备支持；对参加远程培训的教师提供相关技术支持。

3.网络安全与保障组和信息技术支持组所有成员，共同负责对学校教师进行信息技术能力提升培训，带头参与信息技术能力展示或竞赛，为学校教师参与各级各类教学研讨、展示、竞赛活动提供技术支持，制作授课课件或背景视频、音频、图片等。

4.技术团队组长应定期或不定期对本组成员进行业务培训、组织团队成员进行技术交流，促进团队成员技术水平的提高。

四、工作方式

1.技术团队成员利用课余时间为学校老师提供技术支持。特殊情况需要调课或占用上课时间的，须报教务处批准。

2.每次活动所需技术支持，原则上由参加活动的教师本人按本年级（六年级除外）→本教研组（六年级除外）→信息技术支持组其他成员（六年级除外）→网络安全与保障组其他成员及六年级团队成员的顺序主动申请；也可按照双方自愿原则提供技术支持。

3.大型集中活动或其它特殊情况需由学校指派专人提供技术支持的，按学校指定的人员和方式提供技术支持。

五、奖罚措施

1.技术团队成员为学校教师根据学校安排参与的各级各类教学研讨和竞赛活动提供技术支持和保障，学校按如下标准给予奖励：参赛教师获国家级二等奖及以上，奖励课件、视频制作人100元/次（多人合作则分享奖金，下同）；市级一（特）等奖、省级二等奖及以上，奖励80元/次；县级一（特）等奖及以上，奖励60元；校级一（特）等奖及以上，奖励40元/次；校级二等奖及以下或未获奖、未评奖的，每次奖励（补助）30元。

**网络安全自查阶段工作计划7**

>一、安装安全的无线路由器。

这个设备把你网络上的计算机连接到互联网。请注意：不是所有路由器都是天生一样的。至少，路由器需要具有以下三种功能：

（1）支持最不容易被的密码；

（2）可以把自己隐藏起来，防止被网络外面未经授权、过于好奇的人看见；

（3）防止任何人通过未经授权的计算机进入网络。本文以Belkin International公司生产的路由器为例。它和其他公司生产的类似路由器广泛应用于如今的网络中。它们的设置过程非常相似。本文推荐的一些方法适用于这类设备。请注意：款式较老或价格较低的路由器可能提供不了同样的功能。

>二、选择安全的路由器名字。

可以使用生产厂商的配置软件来完成这一步。路由器的名字将作为广播点（又叫热点），你或试图连接至路由器广播区范围之内的无线网络的任何人都看得见它。不要把路由器的品牌名或型号（如Belkin、Linksys或AppleTalk）作为其名字。那样的话，黑客很容易找出路由器可能存在的安全漏洞。

同样，如果把你自己的姓名、住址、公司名称或项目团队等作为路由器的名字，这无异于帮助黑客猜出你的网络密码。

你可以通过这个办法来确保路由器名字的安全：名字完全由随机字母和数字或者不会透露路由器型号或你身份的其他任何字符串组成。

>三、定制密码。

应当更改路由器出厂设置的默认密码。如果你让黑客知道了所用路由器的型号，他们就会知道路由器的默认密码。而如果配置软件提供了允许远程管理的选项，就要禁用这项功能，以便没有人能够通过互联网控制路由器设置。

>四、隐藏路由器名字。

选择了一个安全的名字后，就要隐藏路由器名字以免广播，这个名字又叫服务集标识符（SSID）。

一旦你完成了这了步，路由器就不会出现在你所在地区的路由器广播列表上，邻居及黑客因而就看不见你的无线网络。以后你照样可以广播信号，而黑客需要复杂的设备才能确定你有没有无线网络。

>五、限制网络访问。

**网络安全自查阶段工作计划8**

根据xx网络与信息安全信息通报中心关于切实加强网络安全保障工作的通知精神，为进一步推动我中心网络建设，提升网络安全教育管理水平，培养广大干部职工绿色上网、文明上网意识和良好习惯，增强干部职工网络安全防护能力，保护人民群众信息和财产安全，根据我单位实际，特制定网络安全教育培训方案如下：

>一、指导思想

突出“网络安全为大家，网络安全靠大家”活动主题，深入开展“网络安全”宣传教育活动，提升广大干部职工绿色上网、文明上网意识和网络安全防护能力，全面加强法治网络教育宣传，强化各项管理措施，全面构建文明、安全、和谐的网络环境。

>二、目标任务

重要批示精神和总体国家安全观，通过开展形式多样的网络安全宣传活动，加强干部职工网络安全教育，提倡文明上网、安全上网、绿色上网，大力宣传涉网案件基本知识，实现网络宣传单位和社会的互利共赢，使广大干部职工养成积极参与活动、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。

>三、组织机构及成员职责

为了切实搞好网络安全教育培训工作，决定成立网络安全教育培训工作领导小组：

组长：x

副组长：x

成员：x

领导小组下设办公室，设在xx办公室，由xx兼任办公室主任，并具体负责日常事务工作。

按照“谁主管谁负责、谁使用谁负责”和“一把手”负总责的原则，落实网络安全主体责任，建立健全领导责任追究机制。组长xx对网络安全管理负总责，各副组长及各成员根据自己所管辖工作职责范围对其范围内的\'网络安全负总责，各具体使用人员对网络安全负直接责任。

>四、教育培训内容及形式

通过宣传栏、LED字幕频、单位QQ群、单位微信群，科室会议、单位集中会议（每年至少保证一次以上开展网络安全教育培训）等多种形式开展网络安全教育培训，其教育培训内容：

（一）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。

（二）召开网络安全工作会，总结通报本单位网络安全维护工作方面所采取的措施和取得的成效，以及当\_络安全重点注意防范事项。

（三）组织观看网络安全宣传片，普及基本的网络安全知识，使广大干部职工增强网络安全防范意识，具备识别和应对网络风险的基本能力。

（四）通过开展网络教育培训，动员和组织广大干部职工积极参与，正确认识和使用网络，自觉抵制有害、低俗的信息，提高网络安全防范能力，远离网络陷阱，确保人民群众信息及财产安全。

**网络安全自查阶段工作计划9**

学校平安问题不停是我园最为关注和看重的工作之一，也是各项工作的首要任务。我园在上级教导部门的领导下，在各平安部门的指导下，结合本园平安工作的实际环境，依照上级部门揭橥的各类平安会议精神，坚持以隐患险于明火，警备重于泰山为指针，认真贯彻落实上级各有关要求，全面增强学校平安教导，通过齐抓共管，营造氛围，切实保障师生平安，维护幼儿园正常的教导教授教化秩序。现将平安工作进行自查并总结陈诉请示如下：

>一、增强领导

落实专人负责学校平安的日常治理工作，进一步明确各级平安组织和责任人的职责、责任以及学校平安工作的任务，和每个岗位的每个人员签定了平安责任书、层层落实责任，包管了各项工作真正落到实处。

>二、从建章立制入手

树立健全了学校平安宁期反省和日常警备相结合的治理制度，树立了平安反省记录的制度，突法变乱和平安工作应急预案以及平安值班，防火防灾，食堂卫生平安等规章制度，使学校平安工作有章可循，违章必究，不留盲点。

>三、具体工作

从讲政治的高度，把学校平安工作作为头等大事，多次强调，逢会必讲，匆匆使全体教职员工充分认识到平安工作的`紧张性，和幼儿园工作的特殊性。

1、各班幼儿责任落实到每个班主任，增强日常的工作监管和巡查，发明平安隐患，实时申报，即使处置惩罚，实时整改。

2、增强门卫挂号制度，来园来访必须挂号，方可进入幼儿园。

3、增强园内设施的巡查，大型玩具按期进行平安反省，并作好记录，而且大型玩具四周都有有警示标志，确保各人事事平安。总部主楼后墙面面砖有局部脱落的现象，目前抓紧进行修补，该路段已经全部封闭，已无人进出。为增强学校设施平安，今年暑期对操场上原铁制的玩具调换成了木制的器具，增加了平安系数;幼儿茅厕走道铺设了防滑的垫子，走道加涂了防滑的液体，幼儿园的通道危险处，也有提醒标志，走廊、过道、操场不连任何杂物，给幼儿让出流动的平安空间，为幼儿创设更平安的情况;对某些电路进行改造，对松动破损开关、插座重新安装，对破损窗子、玻璃实时进行补缀，确保师生平安;

4、增强学校食堂卫生平安工作，加大反省力度。贯彻落实教导部、\_(14号令)的实施细则。把好食品进货关、验收关，增强对食品从业人员的专业知识培训，做好食品进货、验收、留样等台帐记录工作，食堂工作人员严格依照各类操作流程和规章制度进行食品操作，同时，树立食品卫生监督步队，由保健室按期反省，学校全体教职员工进行监督。

5、在幼儿的一日运动中，除了为幼儿创设平安的情况之外，在平时的运动中也渗透平安教导的内容，由教师设计和组织各类相符幼儿年龄特点的运动，匆匆使幼儿控制一些基础的自我掩护的意识，加强幼儿的平安意识，确保幼儿在园的平安。

**网络安全自查阶段工作计划10**

为进一步落实安全隐患排查的各项工作，有效控制各类事故的发生，促进安全生产状况持续稳定好转。根据上级文件精神及要求，结合我公司所属的项目部实际，现就开展安全生产隐患排查治理工作，制定本实施方案。

>一、工作目标

在开展安全生产隐患排查治理专项行动，全面排查治理项目部事故隐患，狠抓隐患整改工作，推动安全生产职责制和职责追究制的落实，完善安全生产规章制度，建立健全隐患排查治理及重大危险源监控的长效机制，强化安全生产基础，提高安全管理水平，坚决杜绝事故的发生。

>二、组织领导

组长：

副组长：

成员：

>三、排查资料

1.安全生产法律法规、规章制度、规程标准的贯彻执行状况；

2.安全生产职责制建立及落实状况；

3.高危行业安全生产费用提取使用执行状况；

4.企业安全生产重要设施、装备和关键设备、装置的完好状况及日常管理维护、保养状况，劳动防护用品的配备和使用状况；

5.危险性较大的特种设备和危险物品的存储容器、运输工具的完好状况及检测检验状况；

6.对存在较大危险因素的生产经营场所以及重点环节、部位重大危险源普查建档、风险辨识、监控预警制度的建设及措施落实状况；

7.事故报告、处理及对有关职责人的职责追究状况；

8.安全基础工作及教育培训状况，个性是企业主要负责人、安全管理人员和特种作业人员的持证上岗状况和生产一线职工(包括农民工)的教育培训状况，以及劳动组织、用工等状况；

9.应急预案制定、演练和应急救援物资、设备配备及维护状况；

10.对项目周边或作业过程中存在的易由自然灾害引发事故灾难的危险点排查、防范和治理状况等。

>四、职责分工

按照上级文件要求，结合我项目部实际，对全生产隐患排查治理工作领导小组成员职责分工如下：

（一）颜景波组长为该项工作第一职责人，对该项工作全面负责。同时负责安全生产法律法规、规章制度的执行状况；安全生产职责制建立、落实状况；安全生产费用提取、使用状况；事故报告、处理状况。

（二）高玉岩主要负责项目部的安全检查状况；重大危险源的风险辨识、监控预警制度的建设及措施落实状况；对作业过程存在的易由自然灾害引发事故灾难的危险点排查、防范和治理状况。安全生产重要设施、装备和关键设备、装置的完好状况及日常管理维护保养状况；危险性较大的特种设备和危险物品的存储容器、运输工具的`完好状况及检测状况；应急救援物资、设备配备及维护状况；劳动保护用品的配备和使用状况。

（三）刘忠锋主要负责重大危险源普查建档状况；应急预案制定、演练状况；安全基础工作及教育培训状况。

（四）工作小组成员既要职责分工，各自负责；又要相互配合，团结协作。

>五、工作步骤

第一阶段：动员部署阶段。项目部立即建立健全领导小组和工作机构。召开专门会议，按文件要求实施意见，制订项目部实施方案。针对排查治理工作的要求，细化任务，分清职责，明确专门机构和人员负责此项工作，全面动员，深入开展安全生产隐患排查整治行动。

第二阶段：自查整改阶段。各项目部是安全生产隐患排查治理的职责主体。要把自查整改贯穿于整治全过程，结合项目工作要求和此次安全生产隐患排查治理工作的资料，认真组织开展事故隐患排查整治工作。对排查出的事故隐患，按照事故隐患的等级进行登记，建立事故隐患信息档案，并按照职责分工实施监控治理；对排查出的重大事故隐患，及时向有关部门报告。

自查整改阶段分三个重要时点，一是项目部以建立事故排查基础台帐为该项工作主要任务，自查自纠，重点整改安全通病。二是以“平安工地”认真做好施工现场安全隐患排查工作，做到横向到边，竖向到底，不留死角，确保生产、安全工作双达标。三是切实做好项目扫尾工作，确保项目全过程无事故。

第三阶段：总结验收阶段。项目部根据公司安全生产隐患排查治理督查验收工作状况及项目部自身工作状况，对组织开展隐患排查治理工作的先进个人予以奖励。

**网络安全自查阶段工作计划11**

按照省\_《关于积极配合公安机关网络安全执法检查及加快推进省属企业等级保护备案工作的通知》文件要求，深入贯彻落实国家网络安全等级保护制度，全面提升网络安全保障能力和防护水平，特制定以下工作方案。

>一、加强组织领导，全面部署网络安全自查整改工作。

集团公司所属各单位是网络安全的责任主体，要加强网络安全工作管理，建立\_一把手\_主管机制，推进“谁主管谁负责，谁运维谁负责，谁使用谁负责”的管理原则，进行层层分解，落实到具体部门、具体负责人。涉及关键信息基础设施的所属各单位，要落实网络安全主责机构，严格按照国家关键基础设施相关法律法规开展网络安全防护工作。

>二、加强安全管理，有效防范重大网络安全事件。

要建立健全网络安全工作规章制度，落实安全管理责任。强化网络安全培训工作，提升网络安全人才的配置能力，提高网络安全保障的专业化、规范化、集约化水平。加强网络安全、系统安全、数据安全等相关安全管理工作，减少网络安全事件的发生，保障各类信息系统平稳运行。同时要定期开展网络安全监督与检查工作，及时纠正管理漏洞，发现安全隐患，有效防范重大网络安全事件的发生。

>三、开展等保测评，全面分析面临的安全威胁和风险。

各单位要加快推进网络安全等级保护备案工作，依法履行网络安全保护义务。按照国家网络安全等级保护制度的`要求，委托《全国等级保护测评机构推荐目录》推荐的测评机构对网站、关键信息基础设施等信息系统，依法开展网络安全等级测评及备案。严格按照《网络安全法》中网络安全等级保护制度的要求，履行安全保护义务，提高风险抵御能力。

>四、明确重点对象，开展关键信息基础设施保护工作。

明确重点防护对象，按照关键信息基础设施保护有关要求，采取有效措施保护关键信息基础设施运行安全及数据安全，做到安全技术措施与关键信息基础设施同步规划、同步建设、同步使用。重视工控系统安全，提高核心信息系统安全可控程度。坚持管理和技术并重，做好识别、防护、监测、预警、响应、处置等环节的技术支撑和管理衔接，提高技术水平，切实增强关键信息基础设施的保护能力。

>五、开展自查工作，增强网络安全防范意识。

全面开展网络安全自查工作，以防攻击、防病毒、防篡改、防瘫痪、防泄密为重点，深入查找薄弱环节，及时核查整改。自查内容主要包括网路安全基础设施、边界安全、关键基础设施、工业控制系统、数据中心、门户网站、网上综合应用平台、移动APP业务系统等。要深刻认识到网络安全工作的重要性、复杂性和艰巨性，进一步增强责任感和使命感,按照全面排查风险、增强重点防护、实时发现预警、强力有效处置、确保平稳运行的工作目标，抓好网络安全工作。

>六、建立联动机制，快速应对各类突发网络安全事件。

积极完善本单位网络安全监测预警和信息通报联动机制，出现安全事件后各单位应及时上报集团公司科技与信息化管理部，加强协作沟通，提高网络与信息安全突发性危害事件的防范和应急处理能力, 形成科学、有效、快速反应的联动机制。同时结合本单位实际情况制定完善应急机制和应急预案，定期组织开展应急演练，做好信息系统管理和运维工作，提高服务保障人员的应急处置能力。

>七、狠抓贯彻落实，严格把握网络安全工作。

要求为全面摸清集团公司关键信息系统网络安全保护状况，排查网络风险，落实网络安全责任，提高网络安全保障能力和防护水平，各单位务必全面梳理，检测排查并督促整改网络安全重大漏洞、隐患、风险和突出问题。届时陕西省公安厅将会组织开展网络安全技术抽查检查和现场执法抽查检查，并组织实施网上远程技术检测和渗透测试，各单位应积极配合公安机关开展现场执法检查。

各单位要在x月x日前完成网络安全自查工作，重点对自查工作的组织开展情况、网络安全等级保护和信息通报等重点工作开展情况、当\_络安全方面存在的突出问题以及下一步网络安全工作计划等进行总结，并将网络安全执法检查自查表及总结报送集团公司科技与信息化管理部。

**网络安全自查阶段工作计划12**

衡量一个学校信息化水平高低的重要标志之一就是是否有一支掌握现代教育技术的师资队伍。努力建设一支掌握现代教育技术的师资队伍是学校信息化建设的重中之重。为适应信息社会对学校教育管理工作的新要求，加强对学校网站、网络的管理，提升教师教育信息技术能力，为各项教学竞赛活动提供技术支持与保障，经学校研究决定，成立网络安全和信息化指导小组。为保证相关工作的开展正常、有序、高效，特制定本方案。

>一、领导小组

组长：

副组长：

成员：学校其他行政成员

>二、技术团队

1.网络安全与保障小组：

组长：

副组长：

2.信息技术支持组：

组长：

副组长：

>三、工作职责

1.网络安全与保障组：负责管理学校网站、QQ群，保障各教学楼、综合楼办公室、电脑教室、录播教室网络的正常顺畅运行。

2.信息技术支持组：保障学校监控系统、广播系统的正常运行；对学校新、旧多媒体教室和广播室的\'正常运行，以及学校大型活动提供技术和设备支持；对参加远程培训的教师提供相关技术支持。

3.网络安全与保障组和信息技术支持组所有成员，共同负责对学校教师进行信息技术能力提升培训，带头参与信息技术能力展示或竞赛，为学校教师参与各级各类教学研讨、展示、竞赛活动提供技术支持，制作授课课件或背景视频、音频、图片等。

4.技术团队组长应定期或不定期对本组成员进行业务培训、组织团队成员进行技术交流，促进团队成员技术水平的提高。

>四、工作方式

1.技术团队成员利用课余时间为学校老师提供技术支持。特殊情况需要调课或占用上课时间的，须报教务处批准。

2.每次活动所需技术支持，原则上由参加活动的教师本人按本年级（六年级除外）→本教研组（六年级除外）→信息技术支持组其他成员（六年级除外）→网络安全与保障组其他成员及六年级团队成员的顺序主动申请；也可按照双方自愿原则提供技术支持。

3.大型集中活动或其它特殊情况需由学校指派专人提供技术支持的，按学校指定的人员和方式提供技术支持。

>五、奖罚措施

1.技术团队成员为学校教师根据学校安排参与的各级各类教学研讨和竞赛活动提供技术支持和保障，学校按如下标准给予奖励：参赛教师获国家级二等奖及以上，奖励课件、视频制作人100元/次（多人合作则分享奖金，下同）；市级一（特）等奖、省级二等奖及以上，奖励80元/次；县级一（特）等奖及以上，奖励60元；校级一（特）等奖及以上，奖励40元/次；校级二等奖及以下或未获奖、未评奖的，每次奖励（补助）30元。

**网络安全自查阶段工作计划13**

>一、活动宗旨

提高同学们的网络安全意识，在加强网络安全知识学习的同时，营造一种浓厚的学习氛围。较好地发挥学生的\'特长，丰富学生的课余生活和提高同学们学习计算机网络的热忱。

>二、活动组织

1.活动总负责：xxx

2.活动策划：xxx

3.活动时间：10月25日下午7点

4.活动地点：综合楼308

5.活动对象：信息工程系08级全体学生

>三、活动内容

1.网络计算机的使用技巧

2.预防网络诈骗

3.网络道德

4.网络与法律

>四、注意事项

1.每个班级每个同学在本班负责人的组织下不得迟到，须在讲座前10分钟入指定点，迟到5分钟则不 得入内。

2.讲座过程中不允许大声喧哗，走动，交头接耳，听歌，玩手机。

3.学生到场后，依次入座，由本协会成员维持会场纪律。

4.讲座结束后，由本协会会员安排下依次退场，每部就本次的讲座各写一份总结。

**网络安全自查阶段工作计划14**

根据《\_办公厅关于开展重点领域网络与信息安全检查行动的通知》（国办函〔20xx〕102号）文件精神，我公司对信息安全情景进行了自检自查，现将情景汇报如下：

>一、信息安全自查工作组织开展情景

1、8月7日成立了信息安全检查领导小组，由副总裁张轩宏任组长，办公室主任冯涛、信息化办公室主任高玉磊任副组长，信息化办公室李普阳、鲁宁、马茜、陈超为组员，负责对全公司的重要信息系统全面排查并填记有关报表、建档留存。

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

>二、信息安全工作情景

8月13日信息安全检查行动小组对金蝶k3系统的情景进行逐项排查。

1、系统安全基本情景自查

金蝶k3系统为实时性系统，对公司主要业务影响较高。目前拥有dell服务器5台、tp-link路由器1台、feixun路由器5台、fast交换机10台，系统均采用windows操作1系统，灾备情景为系统级灾备，该系统不与互联网连接，防火墙采用amaranten管控防火墙。

2、安全管理自查情景

人员管理方面，指定专职信息安全员，成立信息安全管理机构和信息安全专职工作机构。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》。

资产管理方面，指定了专人进行资产管理，完善了《资产管理制度》、《设备维修维护和报废管理制度》，建立了《设备维修维护记录表》。

存储介质管理方面，完善了《存储介质管理制度》，建立了《存储介质管理记录表》。

运行维护管理方面，建立了《客服系统维护标准》、《运行维护操作记录表》，完善了《日常运行维护制度》。

3、网络与信息安全培训情景

制定了《河南丰太信息安全培训计划》，20xx年上半年组织信息安全教育培训2次，理解信息安全培训人数20人，占公司总人数的，组织信息安全管理和技术人员参加专业培训1人次。

4、信息安全应急管理

我公司制定了本年度信息安全应急预案，对可能发生的各类信息安全事件做到心中有数，对重点业务计算机经常备份数据，本年度没有发生信息安全事故。

>三、自查发现的主要问题

1、安全意识不够，需要继续加强对公司员工的信息安全意识教育，提高做好安全工作的主动性和自觉性。

2、规章制度体系初步建立，但还不完善，未能覆盖到信息系统安全的所有方面。

3、设备维护、更新还不够及时。

>四、改善措施与整改

根据自查过程中发现的不足，同时结合我公司实际，将着重对以下几个方面进行整改：

1、加强公司职工信息安全教育培训工作，增强信息安全防范和保密意识。

2、要创新完善信息安全工作机制，进一步规范办公秩序，提高信息工作安全性。

3、不断加强计算机信息安全管理、维护、更新等方面的资金投入，及时维护设备、更新软件，以做好信息系统安全防范工作。

**网络安全自查阶段工作计划15**

>一、机构健全，责任明确

多年来，我院领导高度重视信息安全管理工作，成立了信息安全小组《关于调整和充实技术信息网络化工作领导小组成员的通知》(拉检发xxx号)，建立了网络信息安全工作制度，明确了信息安全主管领导和管理人员，按照“谁主管、谁负责”的原则，全面落实工作职责。

>二、制度健全，管理严格

我院制定补充修订了计算机信息系统安全保密相关制度的同时，建立健全了《拉萨市检察机关保密规定》、《拉萨市检察系统计算机信息系统安全保护条例》、《拉萨市检察系统机房管理办法》、《第三方来访人员进入计算机机房管理办法》等制度，严格信息保密管理，实行“涉密不上网，上网不涉密”，坚持“谁发布，谁负责”的原则。定期或不定期对工作人员进行安全和保密意识教育培训，制定了日常考核监督制度，确保管理监控到位。

>三、做好网络信息安全防范工作，加强网络技术管理

1、定期检查，增强防护。我院技术人员定期对电脑、网络进行检查、维护，采取了防篡改、防病毒、防攻击、防瘫痪、防泄密等技术措施，安装了防病毒软件，能够及时更新和修复系统漏洞。对计算机、移动存储设备等实行严密的安全防护措施，有效地保障了网络和系统安全，防范了病毒的攻击。

2、措施得力，防止泄密。本院涉密计算机采用加密、口令等技术措施，防止黑客盗用我院信息及非法侵入我院计算机系统进行破坏。存贮于计算机设备中的保密信息，无关人员不得私自调阅。

3、责任明确，消除隐患。对日常办公电脑和专用电脑实行专机专用，专人负责，责任落实到具体操作人员，力争把隐患消除在源头，有效保障了我院计算机信息系统安全。

4、合理使用硬件设备，软件设置规范，保障设备良好运行状态。每台终端机都安装了防病毒软件，系统相关设备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定，单位硬件的运行环境符合要求，防雷地线正常，防雷设备运行基本稳定，没有出现雷击事故;ups运转正常。网站系统安全有效，暂未出现任何安全隐患。

5、通讯设备运转正常。我院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。

6、建立台账，规范设备维护。我院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、提高干警计算机技能，使全体干警意识到计算机安全保护的重要性。

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。

7、按网站安全要求进行网管工作。

一是使用专属权限密码登陆后台;

二是上传文件提前进行病毒检测;

三是网站分模块分权限进行维护，定期进后台清理垃圾文件;四是网站更新专人负责。

8、多项制度确保计算机网络安全。实行网络专管员制度、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。同时我院结自身情况制定计算机系统安全自查工作制度，做到三个确保：

一是系统管理员定期检查机房计算机、服务器系统，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;

三是定期组织全院人员学习有关网络知识，提高计算机使用水平，确保预防。

>四、存在的问题及整改措施

通过自查，目前，我院网络运行存在以下几点不足：

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。

针对目前我院网络安全方面存在的不足，将从以下几方面进行整改：

1、进一步加强本院干警计算机操作技术、网络安全技术方面的培训，强化本院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、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。

3、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，为我院网络的稳定运行提供硬件保障。

4、在以后的工作中，我们将继续加强计算机安全意识教育和防范技能训练，让干警充分认识到计算机涉密案件的严重性。人防与技防结合，确实做好单位的网络安全工作。

**网络安全自查阶段工作计划16**

>一、加强领导，成立了网络与信息安全工作领导小组

为进一步加强全局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，由局长任组长，下设办公室，做到分工明确，责任具体到人。确保网络信息安全工作顺利实施。

>二、我局网络安全现状

我局的统计信息自动化建设从一九九七年开始，经过不断发展，逐渐由原来的小型局域网发展成为目前与国家局、自治区局以及县区局实现四级互联互通网络。网络核心采用思科7600和3600交换机，数据中心采用3com4226交换机，汇集层采用3com4226交换机、思科2924交换机和联想天工ispirit1208e交换机，总共可提供150多个有线接入点，目前为止已使用80个左右。数据中心骨干为千兆交换式，百兆交换到桌面。因特网出口统一由市信息办提供，为双百兆光纤。与自治区\_采用2兆光纤直联，各县区\_及三个开发区\_采用天融信虚拟专用网络软件从互联网上连接进入到自治区\_的网络，入口总带宽为4兆，然后再连接到我局。横向方面，积极推进市\_与政府网互联，目前已经实现与100多家市级党政部门和12个县区政府的光纤连接。我局采用天融信硬件防火墙对网络进行保护，采用伟思网...

**网络安全自查阶段工作计划17**

为了加强我校网络安全管理，保护系统的安全，促进我校网络技术的应用和成长，保障教育教学和管理工作的顺利开展，并配合教育局的要求，对我校计算机系统开展安全大检查，净化校园网络环境，不断提高学校计算机系统安全防范能力，从而为教师和学生提供健康，安全的上网环境。

>一、领导重视，责任分明，加强领导

为了认真做好工作，进一步提高教育网络安全工作水平，促进学校网络健康成长，我校建立了计算机网络安全管理领导小组。名单如下：

组 长：陈新春

成 员：徐东 帅志、扬倪仨

>二、校园网络安全使用情况

学校网络设备主要是光纤接收器、路由器、交换机等。学校现有办公用计算机6台，一个网络教室有计算机24台，一个多媒体电子教室有计算机1台。安全方面的措施主要有：采用固定IP地址，每台机子都安装金山杀毒软件。定期查杀病毒等。

>三、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、遵循“计算机教室管理办法”，做好安全保卫工作。

3、凡进入机房的人员除须遵循校规校纪外，还必须遵循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、计算教室使用的用电线路必须符合安全规定，定期检查、检修。

6、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。

7、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。

8、机房开放完毕时，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)计算机病毒防治制度

1、每台电脑都安装杀毒软件。

2、未经许可证，任何人不得携入软件使用，防止病毒传染。

3、建立备份制度，对重要资料除在电脑贮存外，还应拷贝到光盘上，以防遭病毒破坏而遗失。

4、及时注意电脑界病毒防治情况和提示，根据规定调节电脑参数，避免电脑病毒侵袭。

(三)事故和案件及时报告制度

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，保留有关原始记录，并及时向上级报告。

(四)面对病毒应急处理方案

1、制定计算机病毒防治管理制度和技术规程。

2、培训计算机病毒防治管理人员;

3、对网站计算机资讯系统应用和使用人员开展计算机病毒防治教育和培训;

4、定期检测、清除计算机系统中的计算机病毒，并做好检测、清除的记录;

5、购置和使用正规的计算机病毒防治产品。

**网络安全自查阶段工作计划18**

坚持科学发展观，充分发挥学校网络的技术指导的管理职能，强化服务意识、责任意识、发展意识，巩固我校教育信息化成果，不断完善信息化建设水平，大力推进教育现代化进程，科学、规范、高效抓管理，求真、务实、优质育人才，努力争创教学示范学校，办优质教育，特制订以下计划：

>一、网络管理与建设

1、采取切实可行的措施，加强对校园网的管理，继续完善相关规章制度，落实各项管理措施，确保学校网络安全畅通。学校要继续完善相关的网络制度，杜绝网络信息安全事故的发生，确保网络畅通，更好的服务与教育教学工作。采取积极可行的措施，在保证网络畅通的情况下，杜绝教师上网聊天、打扑克、玩游戏等不良现象的发生。管理员及全体教师都要深入研究网络应用问题，充分发挥网络的作用，提高教育教学质量。

2、网络防毒。加强对教师信息技术的培训力度，使教师学会使用杀毒软件进行计算机病毒的查杀，确保学校网络畅通。基本上解决网络病毒在我校计算机上的传播，保证网络不因病毒而导致堵塞、停网等现象的发生。

>二、网站建设

加强学校校园网网站建设和应用力度，使其服务于教学、服务于德育、服务于管理;服务于学生、服务于教师、服务于社会。管理员要不断学习相关业务知识，不断提高自己的业务能力，树立服务于教学的思想，管好用好学校网络。

>三、信息技术使用与培训工作

加强信息技术知识的培训与应用。学校将组织专人进行不同层次的`培训班，加强培训指导，教师要将学习走在前头，自觉地学。

**网络安全自查阶段工作计划19**

>一、活动主题和总体要求

今年国家网络安全宣传周主题为“网络安全为人民，网络安全靠人民”。各单位要围绕活动主题，深入学习贯平网络强国战略思想，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，普及网络安全知识，提升网络安全意识和防范技能，营造健康文明的网络环境，共同维护国家网络安全。

>二、活动内容

（一）举办大学生网络安全知识竞赛

各学院分别组织开展“全国大学生网络安全知识竞赛”（9月3日至10月31日）“全国大学生网络安全知识答题闯关”（9月10日至9月18日）活动，通过网络答题方式，普及网络安全知识，各地各高校要组织高校学生积极参与竞赛，激发学生学习网络安全知识兴趣，提升网络安全防护技能。

知识竞赛网址：

答题闯关网址：

（二）开展网络安全宣传体验活动

网络管理与信息服务中心要结合实际情况，组织开展多种形式的网络安全宣传活动，通过发放宣传单，展板展示等形式，让学生了解网络安全知识，提高学生网络安全意识，增强网络安全防护技能等。并与xx州网信办及州公安局网侦支队联系，结合实际情况通过实地参观的形式提高网络工作人员的网络安全意识，增强工作技能。

（三）举办网络安全教育主题日活动

各单位要把9月18日网络安全教育主题日作为加强师生网络安全教育的有利契机，结合实际认真制定活动方案，设计组织形式活泼、内容丰富、时效性强的主题班会活动、集中开展网络安全宣传教育引导，切实提高师生，特别是广大青少年学生的网络素养。

>三、工作要求

（一）举办网络安全周活动是学习贯平网络强国战略思想的.重要举措，各单位要高度重视，组织师生积极参与此次教育活动，充分调动学生的积极性、主动性和创造性。

（二）各单位要紧紧围绕活动主题，宣传部做好校内外宣传活动，网络中心和保卫处加强与网信、公安等部门的联系，开展好案例讲解、实地参观等活动，学生处要推动相关内容纳入新生教育，切实增强教育实效。

**网络安全自查阶段工作计划20**

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、加强领导，明确责任。为确保我校网络安全管理工作顺利开展，学校成立了校长任组长，其他领导为成员的网络信息安全管理工作领导小组，全面负责该工作的实施与管理。实行信息安全保密责任制，切实负起确保网络与信息安全的责任。严格按照“谁主管、谁负责”、“谁主办、谁负责”的原则，落实责任制，明确责任人和职责，细化工作措施和流程，建立完善管理制度和实施办法，确保使用网络和提供信息服务的安全。

2、健全制度，强化管理。建立健全了一系列的学校网络安全管理规章制度。包括：《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。通过制度的制定与实施，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。学校组织全体教职工学习了上级有关网络安全的文件，制定和完善了各项网络安全管理制度，组织师生学习网络安全管理常识，营造了网络安全管理氛围。

二、加强教师队伍建设，建立起了一支相对稳定的网络安全管理队伍

1、网上内容的发布全部由网络管理员完成，工作人员素质高、专业水平好，有强烈的责任心和责任感。网络所有信息发布之前都经分管领导审核批准。及时利用微信公共平台发布学校热点新闻，报道及时，内容丰富。学校校园内目前已经实现wifi上网，教师无论在办公室，操场上都可以利用移动电子设备畅游网海，而且我校的网络安全稳定。学校领导对网络的管理、网络的安全极为重视,经常性地听取教师们的意见和建议。为了维护网络安全稳定的运行，学校实名上网制度，对每一个端口实行固定IP地址，实名上网不是为了监控教师，而是为了维护网络的安全、稳定运行，共同维护好我们的网络。

2、加大教师培训力度。为了使培训落到实处,不流于形式,学校领导每次都到亲临现场组织安排，现在我们的老师都能较熟练掌握教室电教设备的使用，能够通过网络平台进行办公，能从校园网站、远教IP资源和教育信息网获取相关教学资料，通过培训教师的信息知识和技能有了一定的提高。使全体教师了解计算机的有关操作与应用，也使青年教师更好地将电教媒体服务于教学，从而促进了学校现代化教育的有效开展。

三、提高安全责任意识，切实做好计算机维护及其病毒防范措施

由于学校计算机的不断增多，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。但目\_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，要求各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。防止电脑内重要信息出现泄密或造成重大影响事件。

四、大力开展文明上网，安全上网等宣传教育

**网络安全自查阶段工作计划21**

>一、建立健全网络和信息安全管理制度

各单位要按照网络与信息安全的有关法律、法规规定和工作要求，制定并组织实施本单位网络与信息安全管理规章制度。要明确网络与信息安全工作中的各种责任，规范计算机信息网络系统内部控制及管理制度，切实做好本单位网络与信息安全保障工作。

>二、切实加强网络和信息安全管理

各单位要设立计算机信息网络系统应用管理领导小组，负责对计算机信息网络系统建设及应用、管理、维护等工作进行指导、协调、检查、监督。要建立本单位计算机信息网络系统应用管理岗位责任制，明确主管领导，落实责任部门，各尽其职，常抓不懈，并按照“谁主管谁负责，谁运行谁负责，谁使用谁负责”的原则，切实履行好信息安全保障职责。

>三、严格执行计算机网络使用管理规定

各单位要提高计算机网络使用安全意识，严禁涉密计算机连接互联网及其他公共信息网络，严禁在非涉密计算机上存储、处理涉密信息，严禁在涉密与非涉密计算机之间交叉使用移动存储介质。办公内网必须与互联网及其他公共信息网络实行物理隔离，并强化身份鉴别、访问控制、安全审计等技术防护措施，有效监控违规操作，严防违规下载涉密和敏感信息。严禁通过互联网电子邮箱、即时通信工具等处理、传递、转发涉密和敏感信息。

>四、加强网站信息审查监管

各单位通过门户网站在互联网上公开信息，要遵循涉密不公开、公开不涉密的原则，按照信息公开条例和有关规定，建立严格的审查制度。要对网站上的信息进行审核把关，审核内容包括：上网信息有无涉密问题；上网信息目前对外是否适宜；信息中的.文字、数据、图表、图像是否准确等。未经本单位领导许可严禁以单位的名义在网上信息，严禁交流传播涉密信息。坚持先审查、后公开，一事一审、全面审查。各单位网络信息审查工作要有领导分管、部门负责、专人实施。

>五、组织开展网络和信息安全清理检查

各单位要在近期集中开展一次网络安全清理自查工作。对办公网络和门户网站的安全威胁和风险进行认真分析，制定并组织实施本单位各种网络与信息安全工作计划、工作方案，及时按照要求消除信息安全隐患。各单位要加大网络和信息安全监管检查力度，及时发现问题、堵塞漏洞、消除隐患；要全面清查，严格把关，对自查中发现的问题要立即纠正，存在严重问题的单位要认真整改。

各单位要从维护国家安全和利益的战略高度，充分认识信息化条件下网络和信息安全的严峻形势，切实增强风险意识、责任意识、安全意识，进一步加强教育、强化措施、落实责任，坚决防止网络和信息安全事件发生，为召开营造良好环境。

**网络安全自查阶段工作计划22**

按照自治区信息化领导小组下发的《关于20xx年我区开展重点领域信息安全检查工作的通知》（内信领办字[20xx]15号）文件精神，内蒙古自治区民政厅结合自身情况，认真组织自查，取得预期效果，现将检查结果报告如下：

>一、重点网络与信息系统基本情况

正式运行中的业务应用系统包括：自治区最低生活保障信息系统、自治区婚姻登记信息系统、自治区优待抚恤信息系统、自治区社会团体信息系统、自治区五保供养信息系统及自治区城乡医疗救助信息系统等6个主要业务信息系统，由信息中心负责日常保障和维护。

从应用系统的实时性、服务对象、连接互联网、数据集中、灾备情况来看，以上6个业务信息系统全部采用实时交互、逻辑强隔离措施连接互联网、省级数据集中、数据级灾备模式运行。

从网络硬件构成情况来看，中心机房配置有30台服务器、2台小型机、2部路由器、1台隔离网闸、3台负载均衡设备等。

>二、整体安全状况的基本判断

从总体来看，各类业务信息系统上线运行以来，严格遵照有关规章制度的要求、完善各项安全防范措施、加强信息安全工作人员教育培训、信息安全风险得到有效降低，应急处置能力得到显著提高，切实保障了业务信息系统安全、稳定，高效运行。

>三、发现的主要问题

（一）专业技术人员队伍薄弱，网络与信息系统安全保障工作可投入的人力物力有限。

（二）处于规章制度体系建立初期，尚未能覆盖网络与信息系统安全保障工作的各个方面。

（三）当遇到计算机病毒大规模集中爆发、恶意侵袭信息系统等突发事件时，应急处理能力未得到实践检验。

>四、 薄弱环节及整改情况

（一）安全保障预算资金和技术人员缺乏的问题已提请厅领导审批。

（二）在实际工作中不断发现问题、解决问题，修订各类规章制度。

（三）不定期开展数据恢复演练，密切监测，检验各项应急预案的可操作性和实际有效性，随时预防发生的信息系统安全隐患。

>五、意见和建议

随着现代信息技术日新月异的发展，新的、不可预测的信息安全漏洞和安全隐患将层出不穷。建议每年组织一些系统的信息安全技术培训，有针对性地提高安全防范水平和安全可控能力，预防和减少重大信息安全事件的发生。

**网络安全自查阶段工作计划23**

一、活动宗旨

提高同学们的网络安全意识，在加强网络安全知识学习的同时，营造一种浓厚的学习氛围。较好地发挥学生的特长，丰富学生的课余生活和提高同学们学习计算机网络的热忱。

二、活动组织

1.活动总负责：\_\_

2.活动策划：\_\_

3.活动时间：10月25日下午7点

4.活动地点：综合楼308

5.活动对象：信息工程系08级全体学生

三、活动内容

1.网络计算机的使用技巧

2.预防网络诈骗

3.网络道德

4.网络与法律

四、注意事项

1.每个班级每个同学在本班负责人的组织下不得迟到，须在讲座前10分钟入指定点，迟到5分钟则不得入内。

2.讲座过程中不允许大声喧哗，走动，交头接耳，听歌，玩手机。

3.学生到场后，依次入座，由本协会成员维持会场纪律。

4.讲座结束后，由本协会会员安排下依次退场，每部就本次的讲座各写一份总结。

**网络安全自查阶段工作计划24**

我局对网络信息安全系统工作一直十分重视，成立了专门的领导组，建立健全了网络安全保密责任制和有关规章制度，由局信息中心统一管理，各科室负责各自的网络信息安全工作。严格落实有关网络信息安全保密方面的各项规定，采取了多种措施防范安全保密有关事件的发生，总体上看，我局网络信息安全保密工作做得比较扎实，效果也比较好，近年来未发现失泄密问题。

>一、计算机涉密信息管理情况

今年以来，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）实行了与国际互联网及其他公共信息网物理隔离，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。我局配备了防病毒软件、网络隔离卡，采用了强口令密码、数据库存储备份、移动存储设备管理、数据加密等安全防护措施，明确了网络安全责任，强化了网络安全工作。

二是信息系统安全方面实行领导审查签字制度。凡上传网站的信息，须经有关领导审查签字后方可上传；二是开展经常性安全检查，主要对SQL注入攻击、跨站脚本攻击、弱口令、操作系统补丁安装、应用程序补丁安装、防病毒软件安装与升级、木马病毒检测、端口开放情况、系统管理权限开放情况、访问权限开放情况、网页篡改情况等进行监管，认真做好系统安全日记。

三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，没有出现雷击事故；UPS运转正常。网站系统安全有效，暂未出现任何安全隐患。

>四、通讯设备运转正常

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。

>五、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、提高员工计算机技能。同时在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。

>六、网站安全

我局对网站安全方面有相关要求，一是使用专属权限密码锁登陆后台；二是上传文件提前进行病素检测；三是网站分模块分权限进行维护，定期进后台清理垃圾文件；四是网站更新专人负责。

>七、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。

>八、安全教育</st

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！