

村级保密工作实施方案(模板5篇)

无论是个人还是组织，都需要设定明确的目标，并制定相应的方案来实现这些目标。方案的制定需要考虑各种因素，包括资源的利用、时间的安排以及风险的评估等，以确保问题能够得到有效解决。下面是小编为大家收集的方案策划范文，供大家参考借鉴，希望可以帮助到有需要的朋友。

村级保密工作实施方案篇一

按照xx精神，我办严格按文件要求对我办的计算机保密工作进行了自查，特汇报如下：

一、加强组织领导，为保密工作供给组织保障

作为基层党政机关，我办长期把机关保密工作作为一项重要工作常抓不懈。本着“控制源头、加强检查、明确职责、落实制度”的指导思想，成立了由街道纪检书记任组长，办公室主任等为成员的安全保卫保密工作领导小组，党政办公室负责承办日常保密工作。

二、办事处计算机保密管理情景

我办共有计算机9台，其中涉密计算机1台，非涉密计算机8台。我办所有电脑都配备了杀毒软件，能定期杀毒与升级。对于涉密计算机的管理，明确了一名分管领导具体负责，并指定专人从事计算机保密管理工作。对于非涉密计算机的管理，都设置了开机密码，并能作到定期更换，同时明确非涉密单机不得处理涉密信息。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，严禁携带存有涉密资料的磁介质到上网的计算机上加工、贮存、传递处理文件。到目前为止，我办未发生一齐计算机泄密事故。

三、提高保密水平，进取落实保密工作

1、以宣传教育为主导，强化保密意识

为加强计算机及其网络的保密管理，防止计算机及其网络泄密事件发生，确保国家秘密信息安全，在计算机网络管理人员以及操作计算机的领导干部、涉密人员中强化计算机保密安全意识，我办结合工作实际，对干部职工进行了业务培训，学习并熟悉公文异常是“三密”（绝密、机密、秘密）文件处理保管规定及内务等工作要求，组织学习了《基层单位内勤岗位职责》，进一步规范了职责。

2、以制度建设为保障，严格规范管理加强制度建设，是做好计算机保密管理的保障。

为了构筑科学严密的制度防范体系，不断完善各项规章制度，规范计算机及其网络的保密管理，我办主要采取了以下几项措施：一是认真贯彻执行上级保密部门文件的有关规定和要求，不断增强依法做好计算机保密管理的本事；二是制定《创新街道办事处涉密计算机及网络管理制度》；三是严格涉密信息流转的规范性，弥补管理上存在的空挡；四是针对信息发布中存在的不规范等问题，及时制定涉密信息发布审查制度，要求对上网信息严格审查、严格控制、严格把关，从制度上杜绝泄密隐患，做到“上网信息不涉密、涉密信息不上网”。

3、以督促检查为手段，堵塞管理漏洞

为了确保计算机及其网络保密管理工作各项规章制度的落实，及时发现计算机保密工作中存在的泄密隐患，堵塞管理漏洞，我办十分重视对计算机及其网络保密工作的督促检查，采取自查与抽查相结合，常规检查与重点检查相结合，定期检查与突击检查相结合等方式，对计算机及其网络管理制度的落实情景、涉密网络的建设和使用情景以及涉密计算机、涉密

网络采取的管理和防范措施的落实情景进行检查。今年以来，我办对全办计算机及其网络的情景进行了进行了一次全面检查，经过检查，查找计算机保密工作中存在的管理漏洞，并整改到位。经过自查，我办的计算机保密工作能做到制度到位、管理到位、检查到位，但也存在必须的问题，主要是计算机防范技术有待学习提高。

村级保密工作实施方案篇二

文件、资料打印装订完成后，由办公室盖印后按发文范围分送局领导，相关单位、科室，存档。

1、机关人员要严格遵守《保密法》的规定，牢固树立保密观念，严守党和国家机密。

2、妥善保管各种文件、资料。无特殊情况，文件不出室；离开办公室时，桌上不得存放文件；下班后，文件柜和办公桌要上锁；不得带文件旅游、参观、探亲、访友或出入公共场所及闹市区。

3、严禁私自向废品收购部门或个人出售文件、材料和内部资料、刊物、书籍等。各种文件、资料统一由办公室处理。

4、加强涉密信息传输的保密管理，涉密计算机严禁上国际互联网，严禁在使用普通电话时谈论国家秘密事项，严禁在互联网上用电子邮件传递国家秘密信息。

5、有关科室对重要涉密会议和重大涉密活动要明确保密范围，妥善保管相关资料，并做到在任何场合不谈论涉密事项。

6、对重要会议内容和群众涉案事项的情况不得在任何场合泄漏，如发生丢失、泄密事件，将按有关规定追究当事人责任。

7、机关印章由专人管理，用印必须经领导签字批准。

浏览更多的相关制度文章，请您[登陆](#)

村级保密工作实施方案篇三

为保守国家和机关秘密，维护本单位的安全和利益，保障各项事业的顺利进行，特制定本制度：

(一)对上级部门发来的秘密文件资料和机关制定的秘密文件，由专人负责收发和存档，并在规定范围内进行传阅。传阅密件应当使用专用文件夹，要有登记签收手续，不得横向传阅，阅办人阅后应及时将密件退回。

(二)借阅、查询密件必须经主管领导批准后，在机要室内进行，查询人要在登记本上签字后方可查阅。绝密级文件、资料和密码电报不得抄录、复印、拍照、录像等，因工作需摘抄的，要履行审批手续；摘抄时只能抄录有关内容，不得抄录日期和编号。

(三)机关各业务科室、职能部门领导干部开会、学习带回的文件，一律由本科室兼职保密员负责登记、整理，按时间要求归档。

(四)各科室印制密件必须严格遵守保密制度，确保密件及印制过程中的安全。印制密件，必须按批准份数印制，不得多印、私留，印制中的校样、半成品、印板、废品等应当按规定及时销毁，需要保留的软盘、光盘等应当按密件管理，妥善保管，密件印好后，应当及时送到交办的单位。

(五)绝密级文件不得复印，确因工作需要复印的，须经主管领导同意，并经制发机关批准。复印件要视同原件密级进行管理。绝密级文件不得通过传真机传输。

(六)对绝密的机关秘密文件、资料或其它物品，必须采取以下保密措施：非经原确定密级的机关、单位或上级批准，不

得复制和摘抄;收发、传递和外出携带,须由指定人员担任,并采取必要的安全措施;在设备完善的保险装置中保存。

(七)不准在公共场所谈论本人所掌握的国家、单位秘密,不准在私人交往中泄露国家、机关秘密。对外提供涉及本单位经济、社会发展方面的秘密,批准人员应向本单位保密领导小组通报有关情况。严禁在无保密装置的有线、无线电话及私人通信中涉及国家秘密。

(八)本机关涉及国家秘密的计算机信息系统不得直接或间接地与国际互联网或其它公共信息网络相连接,必须加强管理,并加强对《计算机信息系统国际互联网保密管理规定》的学习。

(九)机关各科室购买软盘、计算机及维修计算机须由党政办公室严格把关,存有保密数据和文件的软盘一律不得带回家或各科室相互借用。

(十一)严格控制各项国家秘密和知悉范围,因工作需要扩大知悉范围的,须经领导批准。

(十二)本制度由保密领导小组负责解释。

1、严格办案保密纪律,认真执行纪检监察机关办案保密规定,进一步建立和落实办案保密工作纪律及其责任制。加强对涉案材料、办案用计算机、移动存储设备(u盘、软盘、移动硬盘等)、密码传真机、手机的管理。

2、对信访举报件由信访室实行统一登记,集中管理。

3、切实加强对领导同志批示件的管理,个人不得保存领导同志的批示件。

4、严格遵守“四不准”。不准打听、了解不属于自己职责范

围内的信访举报情况和案件情况;不准传播案情或者向案件当事人和其他涉案人员及其亲友传递消息;不准泄露、扩散有关举报材料、私自向被举报人透露举报人的情况和举报材料的内容;不准未经批准,擅自在新闻媒体上披露正在查处的案件情况。

1、所有秘密文件、有关汇报材料的打印,都必须按照领导批准的发送范围计算印刷份数,不得擅自多印多留。打印过程中形成的清样、废纸,应及时销毁。复印、翻印、摘录秘密文件必须经过批准,并将复印、翻印件同正本文件一样保管。

2、对各个渠道收到的密件,由专人负责进行登记、签收、传阅、借阅、销毁,无关人员不得拆封。由领导亲启的信访件只能由领导本人拆阅。

3、秘密文件传阅由专人传递,并严格限制在规定的范围之内,不得扩大。文件传阅夹内的文件不得拆散、取出。传递人员要随时掌握其流向,传阅完毕后及时清点收存。

4、严格秘密文件借阅登记,规定借阅时间,控制“密级”文件阅知范围,特别是对标有“密级”文件的外借,须经分管机关的副书记批准。

5、下发、批转秘密文件和涉案材料(领导批示件、批转信访件等),要严格登记制度,集中管理。

1、根据“上网不涉密、涉密不上网”的要求,各室用于文字处理的计算机必须做到专机专用,一律不准直接或间接与其他机关网、国际互联网连接。非本委局机关工作人员严禁使用本单位计算机。严禁在上互联网的计算机存储、制作、传递、使用涉密文件、信息、数据以及内部资料。

2、便携式计算机必须专人保管,不得横传或将其放置在未加保密措施的地方。使用人更换时必须做好交接手续。

3、不得在计算机硬盘中存贮机密级以上文件，秘密级文件必须采取加密措施。

4、在处理涉密文件、信息时，不得有无关人员在场。

5、处理有涉密信息的计算机必须设置开机密码，涉密文件必须在文中标明密级，密级与正文不得分离。

6、存贮有涉密文件、信息的移动存贮设备(软盘□u盘、移动硬盘等)必须标明密级，并按同级密件属性进行保管和传输，同一移动存贮设备中存有不同密级文件的，按其存贮最高密级文件标密级;存贮过涉密文件的移动存贮设备，即使已删除文件或格式化，仍需按其密级进行保管和传输，严禁将其带出机关或办案点。

7、信息网的公文传输(邮件)仅限于纪检监察机关内部传输信息、文件、通知、报表、材料和数据等。

8、涉密载体、涉密设备或配件的维护、更换、维修由办公室负责，事先必须进行消磁处理，严禁私自拿出单位维修。请外单位技术人员到机关维修或维护涉密计算机或网络，必须登记并有专人监督。

9、涉密载体、涉密设备或配件(计算机、软盘等)的报废，需书面报请委局保密领导小组批准，由办公室处理，不得随意处置或丢弃。涉密存贮设备的销毁由办公室实施，在委局保密领导小组监督下实行不可恢复性销毁。

1、文印室属委局机关保密重地，应控制进入文印室人员。室内工作人员要谨慎处理各类文件、材料，注意保存原件和安全保密工作。计算机、复印机、激光打印机、轻印刷设备维修人员进入文印室要进行严格监督。

2、密码机发生故障或出现异常，要立即停止使用，并向分管

领导和省纪委办公厅总控室报告，由省纪委负责解决；与密码机相接的计算机出现故障需维修时，一定要将密码机取下，移出另存并删除带有国家机关和机关工作秘密的文件后，单独请人维修。

3、非工作时间或机房内无人时，报警器要处在良好的工作状态。密码设备操作人员每天下班、节假日要做好密码设备的安全检查工作，保证各种设施的完好、到位。

委局所有印章必须明确专人管理，严格履行审批手续，按要求登记备案。纪委、监察局印章、纪委机关党支部委员会印章由办公室保管，使用由分管机关副书记审批。纠风办印章由纠风室保管。县纪委、监察局(含纠风办)印章使用涉及重大事项的报书记签批。各室印章使用管理由各室驻室常委负责。

第一章总则

第一条为规范和加强学校保密工作，根据《中华人民共和国保守国家秘密法》、《中华人民共和国保守国家秘密法实施办法》等国家有关法律法规和中共国家民委党组印发《关于贯彻落实中共中央关于加强和改进保密工作的意见的工作方案》的通知(x发〔xx〕x号)精神，结合学校实际，制定本规定。

第二条保密工作是维护国家安全和利益的重要手段，保守国家秘密是每一个公民的基本职责和应尽的义务。全校师生员工要不断增强保密意识，严格遵守国家的各项保密法律法规和学校保密管理制度，确保国家秘密安全，杜绝失泄密事件发生。

第三条学校保密工作遵循统一领导、分级负责、积极防范、突出重点、依法管理的原则，既要确保党和国家秘密的安全，又要便利学校各项工作的开展。

第二章 保密机构

第四条 学校设立保密委员会，在上级保密部门的指导和学校党委的领导下，负责贯彻落实党的保密工作方针政策及国家有关保密法律法规，研究部署学校保密工作，组织审定学校保密规章制度，审查审批学校保密工作重要事项，指导、协调、监督各单位保密工作等。

第五条 学校保密委员会办公室(以下简称“保密办”)设在学校办公室，负责贯彻落实学校保密委员会有关保密工作的任务和要求，组织开展保密宣传教育以及涉密人员的保密教育、培训;负责涉密文件、资料的接收、保管、传阅、使用、归档、销毁等工作。

第六条 各分党委(党总支、直属党支部)书记，各职能部门和教辅单位主要负责人是本单位保密工作第一责任人，负责本单位的保密工作，并指定专人负责本单位日常保密工作和保密文件、资料(含复印涉密文件)的领取、保管、清退等工作。

第三章 保密事项范围

第七条 保密范围包括上级机关及有关单位发给学校的秘密文件、电传、资料等。国家秘密的密级分为“绝密”“机密”“秘密”三级。

第八条 学校工作中涉及下列事项应按照有关国家秘密及其密级的具体规定执行：

(一) 中央领导人来校视察及来访的高级别外宾未公开的活动安排；

(三) 向上级及有关部门报送的不宜公开的重要情况和问题；

(四) 有关组织、人事、教学和科研等工作中的秘密事项；

- (五) 涉及学校要害部门、要害部位的秘密事项；
- (六) 涉及国防科研项目的秘密事项；
- (七) 处理重大政治、刑事案件的秘密事项；
- (八) 全国各类考试和学校考试试题(卷)及标准答案要点；
- (九) 其他需要保密的项目。

第四章定密工作

第九条定密工作是指学校依法对工作中所产生或派生的国家秘密事项确定密级、保密期限和限定接触范围，对在保密期限内的国家秘密变更密级、变更保密期限和变更接触范围或者解密工作的总称。

第十条凡学校各单位在日常工作中产生或派生的各种属于国家秘密的纸介质、光介质、电磁介质、图片资料、音像等，或属于国家秘密但尚未形成一定载体的事项，均应纳入定密范围。

第十一条凡涉及国家秘密事项的单位和个人，应及时根据定密工作程序规定，由承办人提出具体意见，部门主管领导同意，报学校保密委审批，确定涉密事项的保密等级、保密期限和接触范围。

第五章涉密人员管理

第十二条涉密人员是指因工作需要，在教学、科研、生产、管理等工作中，经常接触、知悉和掌握国家秘密事项岗位工作的人员。按照其掌握国家秘密重要程度划分为核心、重要和一般涉密人员。

第十三条涉密人员应具有良好的政治素质和品行，组织人事

部门应会同保密部门依据相关保密规定对拟进入涉密岗位人员进行岗前审查，各单位应严格按照相关保密规定对涉密人员进行保密教育、管理和检查。

第十四条涉密人员上岗前应经过保密教育培训，掌握保密知识技能，签订保密承诺书，自觉接受保密教育和保密监督检查，严格遵守有关保密法规和规定，不泄露、不传播国家秘密和工作秘密，保障其所涉及的秘密事项的安全。

第十五条涉密人员离岗离职时应提前做好调整安排，实行脱密期管理制度。涉密人员在脱密期内，应当按照规定履行保密义务，签订保密承诺书，不得违反规定就业，不得以任何方式泄露国家秘密。

第六章文件、资料保密

第十六条国家秘密文件、资料是指记录有国家秘密信息的载体（以下简称涉密文件）。内部件是指不属于国家秘密，但不宜公开的内部资料 and 文件。

第十七条学校党政涉密文件的收发、登记、传阅、保管、归档、销毁等工作，由学校保密办直接管理。各单位应指定专人负责本单位涉密文件、资料的收发、登记、保管、传递、移交等工作。内部件应当作为内部事项管理，不得擅自公开。

第十八条涉密文件的制作、收发、传递、承办、借阅、复制、保管、清退、移交、销毁等各个环节，均要严格遵守有关保密规定。

第十九条向校外传递涉密文件应通过机要传递。确因工作急需随身携带机密、秘密级文件、资料或密品时，须经保密委主任批准，方可办理登记手续；携带绝密级文件、资料时必须两人以上；不准携带涉密文件、密品出入公共场所和办理私事。

第二十条承办涉密文件必须及时办理，工作调动或退休时，个人承办的涉密文件必须及时清退。涉密文件阅读需要在机要文件阅文室进行，阅文时要严格遵守有关保密规定。

第二十一条密级文件、资料原则上不准复制，确因工作需要，经批准后复印，复印件视同原件一样管理。

第二十二条保密办负责全校密件以及内部件的销毁工作。由保密办具体组织实施，其他单位或个人不得随意销毁，更不得当作废品出售。涉密文件的销毁由保密办直接送成都市涉密载体销毁中心统一销毁。

第二十三条通过非公开渠道或特殊手段获得的涉密文件，其密级、保密期限和接触范围，按提供该密件的部门的要求确定，或由最初使用该密件的部门、单位确定。

第七章 涉外活动保密管理

第二十四条各项涉外活动，应在批准的范围内进行。对尚未批准对外开放的部位或项目确需对外开放时，应报保密办审核，经上级主管部门审批同意方可开放。

第二十五条在对外交往和合作中涉及到国家秘密事项时，有关业务部门应会同保密办事先拟订安全保密方案，规定保密纪律。保密办应对执行情况进行监督和检查。

第二十六条参加外事活动不准携带涉密文件、密品。确因工作需要携带时，须经学校保密委员会主任批准，保密办备案，并妥善保管，不得遗失。

第二十七条涉密人员因公出境，由各单位主要负责人、国际合作与交流处、保密办等按规定进行保密审查，并对涉密人员进行保密提醒教育；涉密人员因私出境，按规定履行审批手续。

第八章办公设备和网络管理

第二十八条本规定所称办公设备是指计算机及存储介质、打印机、传真机、复印机、扫描仪、碎纸机、照相机、摄像机等具有信息存储和处理功能的设备。

第二十九条未经加密的办公自动化设备，均不得传输、储存涉及国家秘密内容的信息、文件、资料。

第三十条涉密计算机必须与互联及其他公共信息网络物理隔离，并设置开机密码、用户密码、屏幕保护密码。严禁在涉密与非涉密计算机之间交叉使用移动存储介质。

第三十一条存储国家秘密信息的电子载体，应按所存储信息的最高密级标明密级，并按相应密级的文件进行管理。存储在计算机信息系统内的国家秘密信息应当采取保护措施。存储涉密信息的便携式计算机应同涉密文件一样管理。

第三十二条计算机信息系统的保密应实行单位领导负责制。各单位建立网络信息发布审查机制，遵循涉密不公开、公开不涉密、谁公开谁负责的原则。

第三十三条存储或存储过国家秘密信息的计算机信息系统的维修应以不泄露国家秘密为原则。当计算机出现故障，厂家上门维修时，管理人员必须到场监督。如需送出维修，必须对硬盘拆卸进行封存保管后，方可送出维修。

第三十四条存储过国家秘密信息的电子载体不能降低密级使用，不再使用的电子载体应及时销毁，严禁将涉密办公设备赠送、出售、丢弃或者改作其他用途。维修涉密计算机、制作涉密光盘、销毁涉密电子载体必须在本单位内部进行或到四川省国家保密局指定单位，非定点单位不得承担上述三项工作。

第三十五条各单位要严格敏感资料数据信息在线传输管理，加强手机使用保密管理，严禁通过各类网络传媒、论坛，互联网电子邮箱□qq□微博、微信等即时通信工具，网盘、云盘等网络存储服务，普通手机、固定电话等谈论、处理、传输国家秘密或内部敏感资料数据信息，防止发生失泄密现象。

第九章保密要害部门(部位)管理

第三十六条保密要害部门应当是各单位内部涉及重要国家秘密事项的最小行政单位或其绝大多数内设部门涉及重要国家秘密事项的行政单位或涉及绝密级项目和重要国家秘密事项的单位。保密要害部位应当是存放、保管国家秘密载体、密品的专用、独立、固定场所。

第三十七条保密要害部门(部位)的确定，由保密办按照有关规定提出初步意见报校保密委员会通过，并报有关上级部门备案。

第三十八条学校组织人事部门要做好保密要害部门(部位)调入人员的审查工作，对不适宜在保密要害部门(部位)工作的人员及时调离。保密办协助组织人事部门做好保密要害部门(部位)人员调入和调离工作。

第三十九条学校保密委员会对保密要害部门(部位)的保密工作要经常进行检查和监督，并指导保密要害部门(部位)制定保密防范措施，开展保密教育。

第四十条保密要害部位(部门)实行“谁主管、谁负责”的原则，主要领导要切实担负保密工作责任，对本单位人员进行经常性的保密教育和检查，配备必要的保密防范设施与装置。要把保密工作与业务工作同计划、同部署、同检查、同总结、同奖惩；结合本业务工作制定相关保密管理规定，并建立严格的保密工作责任制。

第十章宣传报道和涉密会议管理

第四十一条拟公开宣传报道、展出的事项，主(承)办单位的领导负责保密审查。凡属国家秘密事项，除经上级主管业务部门和保密工作部门批准外，不准利用公开的报刊、广播、电影、电视、录像、展览等进行宣传报道。

第四十二条内部宣传报道和展览，不得涉及绝密、机密级事项，涉及秘密事项须经学校保密委员会审查同意，进行非密化处理后，才能宣传和展出。

第四十三条召开涉密的党政及其他会议，主办单位要根据会议的涉密情况，规定与会人员范围，明确保密要求。

第四十四条其他重要的涉密会议，主办单位会同保密部门共同做好安全保密工作。会议密件应有专人管理，会议结束时要认真清理清退。密件传递、携带按本规定第十三条办理。

第四十五条凡召开涉密会议，不准使用无线话筒和手机，不准使用非保密本记录涉密内容，不准将涉密内容向无关人员泄露或擅自扩大传达范围。涉密会议不得录音，如需录音，须经会议主管领导批准。大型涉密会议应使用移动通信干扰器。

第十一章奖惩

第四十六条凡严格遵守保密法纪及保密制度，保密工作有突出成绩者；凡能及时纠正他人违反保密制度行为，堵塞失、泄密漏洞，避免党和国家利益遭受损失者；凡坚决同出卖党和国家秘密的行为作斗争，为保护党和国家秘密的安全做出突出贡献者，学校对单位及个人给予先进表彰和奖励。

第四十七条各单位发现、发生失泄密事件，应立即采取补救及防范措施，将损失限制在最小，并第一时间向学校保密委

员会报告。学校保密委员会发现失泄密事件，应立即调查处理，并将有关情况及时向上级主管单位和相关保密管理部门报告，同时及时评估失泄密影响及后果，积极采取补救、防范措施，依法追究直接责任人的失泄密责任。

第四十八条保密工作纳入各单位以及教职工年终考核内容之中。对违反保密法律法规和本规定，故意或过失泄露国家秘密的，不严格执行失泄密报告制度或故意隐匿不报，以致影响查处工作和及时采取补救措施的，将视情节轻重，给予相应处分，并追究有关领导和人员的责任。构成犯罪的，移交有关部门依法追究刑事责任。

第十二章附则

第四十九条本规定由学校保密办负责解释。

第五十条本规定自印发之日起实施。

保密工作规章制度范本

第一条总则

1. 为保守公司秘密，维护公司权益，特制定本制度。
2. 公司秘密是关系公司权力和利益，依照特定程序确定，在一定时间内只限一定范围的人员知悉的事项。
3. 公司附属组织和分支机构(包括办事处)以及职员都有保守公司秘密的义务。

第二条保密范围

1. 公司重大决策中的秘密事项。
2. 产品研发、产品生产情况、新产品代理情况。

3. 公司尚未付诸实施的经营战略、经营方向、经营规划、经营项目及经营决策。
4. 公司内控文件和制度、流程、收发文。
5. 合同、协议、意见书及可行性报告、主要会议记录。
6. 公司财务预决算报告及各类财务报表、统计报表。
7. 公司所掌握的尚未进入市场或尚未公开的各类信息。

第三条 保密级别

1. 公司秘密的密级分为“绝密”、“机密”、“秘密”三级。

绝密是最重要的公司秘密，泄露会使公司的权力和利益遭受特别严重的损害，机密是重要的公司秘密，泄露会使公司的权利和利益遭受到严重的损害；秘密是一般的公司秘密，泄露会使公司公司的权益和利益遭受损害。

2. 公司秘级的确定：

(1) 公司经营发展中，直接影响公司权益和利益的重要决策文件资料为绝密级；

(2) 公司的规划、财务报表、统计资料、重要会议记录、公司经营情况为机密级；

(3) 公司人事档案、合同、协议、职员工资性收入、尚未进入市场或尚未公开的各类信息为秘密级。

第四条 保密措施

1. 属于公司秘密的文件、资料和其它物品的制作、收发、传递、使用、复制、摘抄、保存和销毁，由总经理、或总经理

委托专人执行;采用电脑技术存取、处理、传递的公司秘密由行政部负责保密。

2. 对于密级文件、资料和其他物品，必须采取以下保密措施：

(1) 未经董事长或总经理批准，不得复制和摘抄；

(2) 收发、传递和外出携带，由指定人员担任，并采取必要的安全措施；

(3) 在设备完善的保险装置中保存。

3. 属于公司秘密的设备或者产品的研制、生产、运输、使用、保存、维修和销毁由公司指定专门部门负责执行，并采取相应的保密措施。

4. 对外交往合作中需要提供公司秘密事项的，须经总经理批准。

5. 具有属于公司秘密内容的会议和其他活动，主办部门应采取下列保密措施：

(1) 选择具备保密条件的会议场所；

(3) 依照保密规定使用会议设备和管理会议文件；

(4) 确定会议内容是否传达及传达范围。

6. 不准在私人交往和通信中泄露公司秘密，不准在公共场所谈论公司秘密，不准通过其他方式传递公司秘密。

第五条 责任与处罚

1. 出现下列情况之一者，给予警告，并扣发工资100元以上500元以下；

- (1) 泄露公司秘密，尚未造成严重后果或重大经济损失的；
- (2) 违反本制度规定的秘密内容的；
- (3) 已泄露公司秘密但采取补救措施的。

2. 出现下列情况之一的，予以辞退、赔偿经济损失或追究刑事责任：

- (1) 故意或过失泄露公司秘密，造成严重后果或重大经济损失的；
- (2) 违反本保密制度规定，为他人窃取、刺探、收买或违章提供秘密的；

第六条本规定自签订之日起生效。

根据公司201x年保密工作计划的总体部署，在公司董事会用心指导和大力支持之下，公司保密工作领导小组强化落实各项工作，圆满完成20xx年公司的保密工作总体目标，全年无泄密事件发生。为进一步提升思想认识，强化管理，突出重点，完善措施，推动保密工作向规范化更上一个台阶，迎接国家保密局的针对公司保密资格的全面检查[]201x年公司保密工作将严格执行《中华人民共和国保守国家秘密法》及《中华人民共和国国家保密法实施办法》，围绕“加强保密制度的全面落实”和“推动保密教育的深化”两条主线，努力做好保密工作，构建保密安全工作的长效机制。

201x年是母公司冲刺的关键一年，作为体现公司软实力的一个重要方面，要充分认识保密工作的重要性，高度重视保密工作，继续把保密工作作为公司内部的一件大事来抓。继续坚持法人代表总负责制和保密工作目标管理原则，按照目标管理考核资料进行任务分解并且落到实处，让保密工作成效与绩效紧密挂钩[]201x年工作实践来看，保密工作与生产工作

同计划、同落实、同检查同考核成效明显□201x年需要继续坚持和细化。各涉密部门要分工有协作，尽其职责，加强部门领导的首要负责制，充分发挥保密工作领导小组的作用，加强涉密工作的指导和管理检查。

为使保密工作更加规范化、制度化，结合公司生产实际状况，进一步修订完善公司保密工作各项规章制度，增强制度的可操作性，做到涉密事项有章可循、有据可查。重点抓好保密宣传教育、电子信息系统安全、涉密人员培训等工作制度的健全和落实，抓好保密载体收发、登记、保管、清退、销毁等环节，堵塞各种失泄密漏洞，进一步完善各项规章制度和职责，建立健全档案管理各项规章制度和涉密人员岗位职责。

保密宣传教育是公司保密工作的一项基础性工作，从过去来看，我公司的保密教育尽管在规范化和制度化方面取得可喜成效，但也存在不足和需要改善的地方，比如：培训形式较为单一，主要以授课的形式；涉密人员考试成绩很高，但意识还有薄弱环节。因此在新的一年里，公司高度重视并认真抓好工作落实，增强针对性、注重实效性，在保密形势教育、保密法制宣传教育和保密技术支持教育等三大传统项目的基础上，增加警示教育、爱国主义教育的比重，用心探索宣传教育的新形式，采取多种形式，多种措施，多种方法，。探索在日常工作生产之余的保密教育培训，增设相关的杂志、报纸、宣传资料便利放置点，让保密教育走到员工身边。

为适应涉密信息系统分级保护管理的需要，切实加强对计算机信息系统的安全保密技术培训。进一步规范涉密计算机和上网计算机的管理，对计算机网络系统严格执行国家保密局《计算机信息系统保密管理暂行规定》和《计算机信息系统国际联网保密管理规定》，加强互联网管理，要坚持实行物理隔离，做到计算机信息系统涉密管理由专人负责。在涉密计算机的显著地方粘贴保密警示用途标识。

保密工作的最终目的是保障涉密产品生产、储运的顺利进行，我们将紧紧围绕这条主线任务做好涉密载体的保密工作。我公司的涉密载体主要有涉密光盘、样品、特种原材料和涉密成品，以及流转过程中构成的涉密文档。工作中要做好秘密文件的管理，继续完善密件和重要文件登记制度，实行专人保管，专柜保存，确保涉密资料、信息的安全。严格管理密级文件的制作、传递、使用、复制、保管和销毁工作，执行涉密文件资料严格签收制度，严格控制流向，从根本上消除涉密文件的泄密隐患。

20xx年全公司会继续强化经营资料的规范化管理，改变过去资料存放散乱、流转无序的不良习惯，作为保密资料要更强化这方面的管理，各部门集思广议改善保密方法和检查方式方法。对涉密载体的生成、保存和流转开展定期不定期展开检查，在检查过程中要轻形式、重实质，重点关注留痕的及时性，对检查中存在的问题及时整改，到达资料存放有序的目的。

总之□201x年，我公司将继续加大对保密工作的督查力度，推动各项保密工作任务的落实。严格执行泄密报告制度，严肃查处泄密事件，认真自查自纠，清除涉密隐患，切实增强职工的保密意识，建设一支保密意识强，保密技能过硬的涉密人员队伍，适应保密形势的不断发展，杜绝泄密事件发生。

1. 不准将国家的一切秘密文件私自带到公共场所；
2. 不准将秘密文件、密码电报等带出办公室；
3. 不准将秘密文件横传、积压或请人代交；
4. 不准将秘密文件等私自给无关人员阅览；
5. 不准利用工作之便，私抄和复制秘密文件等；

6. 不准泄露由于工作之便获悉的秘密事项。

为切实加强我局保密管理工作，根据《中华人民共和国保守国家秘密法》（以下简称《保密法》）和相关法律法规的规定，特修订我局保密工作制度：

1. 上级下发的涉密文件、资料，一律由保密办公室专人领取登记，按规定程序办理；开会带回的涉密文件、资料，应先交由办公室登记后，再按规定程序办理。

2. 严格按照涉密文件确定的阅读范围，专人送阅读对象阅办，并办理阅办手续，不得横传或由他人代为传递，不得擅自扩大涉密文件的阅读范围。

3. 涉密文件、资料应由保密人员负责统一管理，存放于安全保密的场所，并配备必要的保密设备。

4. 借阅涉密文件、资料，须经分管保密工作的领导同意，在保密人员处办理借阅手续，用后及时退还，清销借阅登记。

5. 涉密文件、资料一般不得复印、复制，确因工作需要的，须经分管保密工作的领导批准同意后，才能复印、复制。对复印、复制的份数要进行登记，涉密文件复印件按原件要求管理。

6. 涉密文件、资料的销毁，必须造册逐一登记，经领导签字后，由办公室交市保密办统一销毁，任何个人不得擅自销毁。各处室或机关工作人员不得长期保存和私自销毁秘密文件、资料。

1. 涉密计算机不得直接或间接与互联网相连，只允许单机形式进行工作，并由专人负责，实行“一人一机”管理。

2. 涉密计算机均应设置密码，密码的设置，均应遵循不易破

译的原则，如：不采用与自己姓名、出身年月、电话号码等有关的文字或数字作密码，不得把密码告诉他人，也不要把密码写在纸上，并应经常更换密码。

3. 涉密信息的查询、修改、删除等处理只能在涉密计算机上进行，不得与非涉密计算机进行涉密信息的传输。禁止在非涉密计算机上处理、存储、传输涉密信息。

4. 含有涉密信息的各类存储介质，如u盘、光盘等，列入保密管理范畴，由专人保管，并做好记录。实行备份生成、存储、借用、销毁全过程的管理。

5. 凡涉及国家秘密信息的计算机设备的维修，应保证储存的国家秘密信息不被泄露，并到保密部门指定的维修点进行维修。

6. 涉密计算机信息在打印输出时，打印出的文件应当按照相应密级文件管理，打印过程中产生的残、次、废页应当及时销毁。

7. 未按规定管理和使用涉密计算机造成泄密事件的，要依法依规追究相关责任。

1. 严格遵守《保密法》和《计算机信息系统国际联网保密管理规定》，切实加强和规范网络保密管理及网络信息安全保护工作。

2. 加强上网信息和上报信息保密工作和网络信息安全的法律、法规和知识宣传教育，增强工作人员的网络安全及信息保密意识和责任意识。工作人员要严格遵守国家有关保密规定，不得利用电子邮件传递转发或抄送秘密信息。

3. 按照“分管领导负总责、处室负责人具体抓”的原则，切实加强对上网信息保密工作的领导。上网信息工作责任实行

三级负责制：即分管信息工作的领导对本部门信息发布、资源提供负总责；相关处室负责人对初审工作负责；信息拟定人员对提供的信息负直接责任。

4. 定期对网络及信息保密安全进行检查，及时消除安全隐患，切实杜绝涉密和有害信息的传播。一旦发现网上失泄密事件或违反保密规定的行为，要及时采取有效的补救措施，并报告保密部门。

5. 实行严格的上网信息审批制度，按照“谁提供谁负责”和“谁上网谁负责”的原则，坚持“信息提供人员自审，相关业务处室初审和分管领导审签，特别重要信息由一把手审签”的原则，切实加强对互联网上网信息和上报信息的保密管理，严防涉密信息上网，确保上网信息安全。未经审批的信息一律不得上网发布。

1. 自觉遵守保密法律法规，严守党和国家秘密。

2. 秘密文件、资料应在办公场所内使用，使用完后应及时将秘密文件、资料交办公室保管，不得横向传阅使用或留存。

3. 不得擅自携带秘密文件、资料外出。确因工作需要的，应当经分管保密工作的领导批准，并采取严格的安全保密措施。

4. 在私人通信和公开发表的文章中，不得涉及国家秘密。

5. 不在非保密笔记本上记录党和国家秘密事项。记有秘密事项的保密笔记本必须严格保管，不得丢失，用完后交保密办统一保管、销毁。

6. 传递涉密信息，应通过机要渠道；禁止使用普通电话、明码传真、手提电话等传递秘密事项。

7. 不得在公共计算机信息系统中存储、处理、传递涉密信息

和内部资料。不得擅自销毁秘密文件、资料，确需销毁时，要按要求的办理。

8. 发现有泄密情况时，应当及时报告。

第一章总则

第一条根据《中华人民共和国保守国家秘密法》、《中华人民共和国保守国家秘密法实施办法》及省、市有关规定，结合我单位实际，制定本制度。

第二条单位保密工作领导小组是我单位的保密工作领导机构，在市委、市政府保密工作委员会和保密局的指导下，依照国家保密法规、省市保密规章制度及本制度，负责检查、督促我单位的保密工作。

第三条保密工作要贯彻党中央以经济建设为中心，坚持突出重点，积极防范，确保安全，便利工作的方针，该保密的坚决保住，该公开的坚决公开，发挥保密工作的服务和保障作用，为经济建设和改革开放服务。

第二章保密范围和秘密等级

第四条国家秘密是关系国家的安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项。单位保密范围主要包括：

(一) 上级保密部门或上级其它部门下发的国家秘密载体；

(二) 其它经市委、市政府研究应该保密的事项。

第五条密级划分。根据秘密事项的重要程度、接触范围和失密后的危害大小，将密级划分为绝密、机密、秘密三个等级。

(二) 机密级。是重要的国家秘密，泄露会使国家的安全和利

益遭受严重的损害；

范围，又不宜公开的事项，应作为内部事项妥善管理。

第七条下列事项不属于国家秘密，但应当作为内部事项管理，不得扩散：

(二) 各种内部规章、制度、管理措施、内部文件、资料及印章；

(三) 单位主要领导的电话号码、家庭住址及其它有关资料。

第三章 保密领导机构和职责

第八条单位设立保密工作领导小组，具体领导和指导我单位保密工作。第九条单位保密工作领导小组的主要职责是：

(一) 贯彻执行党和国家及省市有关保密工作的方针、政策、法规、指示；

(四) 建立保密岗位责任制；

(五) 制定保密工作计划，做好保密宣传和教育；

(六) 对涉及国家秘密的保密要害部位及涉密计算机系统，采取保密技术防范措施；

(七) 监督和检查保密工作落实情况，指导并组织追查失、泄密事件；

(八) 研究和改进保密工作，努力解决保密工作存在的问题；

(九) 向保密委员会和保密局汇报我单位保密工作情况，完成上级交办的事项。

第十条单位配备专(兼)职保密员，主要任务是：

(二)负责本单位保密检查工作；

(三)向单位保密工作领导小组汇报保密工作情况。

第四章各项保密规定

第十一条全体干部职工应遵守的保密规定

(一)不该说的秘密绝对不说；

(二)不该问的秘密绝对不问；

(三)不该看的秘密绝对不看；

(四)不该记录的秘密绝对不记录；

(五)不在非保密本上记录秘密事项；

(六)不在私人通信中涉及秘密事项；

(七)不在公共场所和家属、子女、亲友面前谈论秘密事项；

(八)不在不具备保密条件的地方存放秘密文件、资料和物品；

(九)不在普通电话、手机、传真、明码电报及普通邮件中传递或谈论秘密事项；

(十)不携带秘密文件、资料、物品等游览、参观、探亲、访友和出入公共场所。

第十二条定密工作责任制

(一)单位保密工作领导小组负责对本单位公文、会议记录、

计算机存储介质等的定密、变更、解密工作进行指导、监督和审查。审查工作必须定期进行，将重点涉密部门的文件资料列为重点审查对象，发现有漏定或错定密级的必须及时加以提醒和纠正，情况较重、屡教不改的必须严肃批评教育或按有关规定予以必要的处分。

(二)公文拟稿时要依法定密。各部门具体承办人员要根据“谁发文、谁定密”的原则，确定工作中产生的事项是否属于国家秘密。对属于国家秘密的，应当拟定密级，并提出定密依据交由单位办公室审核。

(三)单位办公室必须确定专人对拟定的公文内容进行审核，同时在文稿审批单密级栏内拟定密级，如属国家秘密事项，则按所需保密等级定为“秘密”、“机密”或“绝密”，并依据《国家秘密保密期限规定》确定保密期限；如系公开事项，则定“无密”；如属内部事项，则定“内部”，不得使之处于空白。区分的标准和依据是《国家秘密及密级具体范围的规定》。

(五)文件密级一经确立，其传递、核稿、签发、盖印、封发、保管、清退、移交、销毁等各个环节，均必须履行严格的登记手续，并按照文件规定的级别、范围进行传递。

第十三条载体和密品管理制度

(一)各类文件、资料(包括纸介质、光介质、电磁介质等载体)的管理必须由单位保密工作领导小组指定专人负责。

(二)查阅涉密文件、资料(包括纸介质、光介质、电磁介质等载体)，只准在保密室(或档案室)内查阅。查阅时原则上不能复制，确因工作需要复制的，必须经原制发机关、保密局和单位保密工作领导小组批准，并按规定办理审批手续由专人复制。复制后的涉密文件、资料(包括纸介质、光介质、电磁介质等载体)必须严格登记，标明复制单位、份数和日期。复

制件按原件的同等要求严格管理，阅办后按规定立卷、归档或清退。

(三) 传阅涉密文件、资料(包括纸介质、光介质、电磁介质等载体)须经单位保密工作领导小组指定专人负责，未经批准不得擅自扩大阅读范围;阅读涉密文件要在办公室进行;外出递送涉密文件过程中，不准办理与递送文件无关的事，且必须两人同行，必要时采取安全保护措施;借用涉密文件、资料须经主要领导批准，并于借用当天退回。

(四) 传递涉密文件、资料(包括纸介质、光介质、电磁介质等载体)，不准用普通邮件邮寄，不准用没有加密设施的办公设备传输秘密文件。

(五) 涉密文件、资料(包括纸介质、光介质、电磁介质等载体)必须放在有保密设施的文件柜内，并经常检查保密情况;管理人员在工作调动或退休时，必须把自己经管的涉密文件、资料(包括纸介质、光介质、电磁介质等载体)全部移交，并认真办理移交手续。

(六) 各类文件、资料(包括纸介质、光介质、电磁介质等载体)应当定期清查、清退。如有涉密文件、资料(包括纸介质、光介质、电磁介质等载体)，除制发机关规定清退时限的须按时清退外，其它的一般每季度向保密局清退一次。需销毁的废旧文件、资料(包括纸介质、光介质、电磁介质等载体)须由单位办公室统一送到上级保密部门指定的地点进行销毁，任何人未经批准不得擅自处理。

第十四条 计算机信息系统保密制度

(一) 计算机信息系统应用、管理人员必须严格执行国家保密局《计算机信息系统保密管理暂行规定》、《计算机信息系统国际互联网保密管理规定》的规定，确保国家秘密信息安全。

(二) 计算机信息系统应用、管理人员未经批准，严禁对外提供内部信息和资料以及用户名、口令等内容；计算机系统要经常检查，防止漏洞，禁止通过网络传递涉密文件，严禁涉密软件、光盘□u盘、移动存储介质等在涉密与非涉密计算机之间交叉使用。

(三) 计算机应用、管理人员使用具有互联网访问权限的计算机访问互联网及其它网络时，严禁浏览、下载、传播、发布违法信息和涉及国家秘密的信息；严禁接收来历不明的电子邮件，利用电子邮件传递、转发或抄送国家秘密信息；当发现国际互联网计算机信息网络中有涉及国家秘密信息时，应当立即向上级保密部门报告。

(四) 计算机信息系统应用、管理人员要定期备份重要数据，复制副本以防止因存储工具损坏造成数据丢失。备份工具可采用专用光盘、硬盘□u盘等方式，并妥善保管。

(五) 计算机信息系统应用、管理人员调离时应将有关材料、档案、软件移交给其他工作人员，调离后对需要保密的内容要严格保密。接替人员应对系统重新进行调整，重新设置用户名、密码。

(六) 涉密专用计算机系统应当采取有效的保密措施，严防泄密、窃密；所采取的保密措施应与所处理信息的密级要求相一致。

(七) 涉密专用计算机系统的机房应当按照国家的有关规定，与境外机构驻地、人员住所保持相应的安全距离，并定期进行保密技术检查。

(八) 涉密专用计算机系统一般不允许他人参观和提供对外服务，因特殊情况接待外来人员，要履行审批手续，并明确接触的范围和内容，未经批准无关人员不得进入机房。

(九)涉密专用计算机系统不得直接或间接地与国际互联网或其它公共信息网络相连接，必须实行物理隔离。

(十)涉密计算机的维修应由本单位人员在本单位范围内进行，并确保涉密信息在维修过程中不被泄露；不具备自行维修涉密计算机的，应当委托保密部门认定的涉密计算机维修定点单位进行维修。

(十一)涉密计算机在维修过程中，不得随意下载、复制或自行处理涉密文件、资料；因维修必须下载、复制或以其他方式处理的，须经单位保密工作领导小组批准，不得擅自保存和扩大涉密信息知悉范围。

(十二)有机密级以上国家秘密信息的计算机原则上不送定点单位维修，应请定点单位派专人到本单位维修，并指定专人全程监督，确保国家秘密信息安全。

(十三)需要更换、报废的涉密计算机，必须彻底清除涉密信息，不能自行清除涉密信息的，应当委托定点单位清除，没有彻底清除涉密信息的计算机，不得擅自处理和另作他用。

(十四)需购置涉密计算机，必须满足国产标准，同时是国家保密局、公安部、安全部认定的产品。

(十五)涉密计算机委托给非定点单位维修，由此导致泄密事件的，将按照有关保密法律法规严肃处理。

第十五条公开发布信息保密管理制度

(四)在无密级的报刊、资料、书籍中不得转载秘密文件、资料；

(五)出国人员未经授权，不得擅自接受境外新闻媒介的采访、邀请等各种旨在获取我国情报信息的活动；在非自愿的情况下，

遇到国外新闻记者或有关人员的采访时，应以外交辞令应对或婉拒。

第十六条会议工作保密制度

(四) 与会人员一律关闭所携通讯工具；

(九) 会议结束后，要对会议场所、住所进行保密检查，不得有文件、笔记本等遗漏。

第五章奖励与惩处

第十七条凡有下列表现之一的集体或个人由上级保密部门或本单位依照规定给予奖励或表扬：

(一) 在危急情况下，保护国家秘密安全者；

(二) 对泄露或盗取国家秘密的行为进行斗争或及时检举者；

(三) 发现他人泄密或可能泄密时，立即采取措施，从而避免或减轻损害程度者；

(四) 在保密工作中做出重要贡献或取得重要科研成果者；

(五) 一贯忠于职守，从事保密工作事迹突出者。

第十八条凡泄露国家秘密尚不够刑事处罚的，根据情节轻重，按照干部(职工)管理权限，给予行政处分。

第十九条对泄露国家秘密尚不够刑事处罚，但具有下列情况之一的，应从严从重给予行政处分：

(一) 泄露国家秘密造成严重后果者；

(二) 以谋取私利为目的故意泄露国家秘密者；

(三) 虽然泄密情节较轻，但多次泄密或泄密数量较大者；

(四) 利用职权强制他人违反保密规定，从而造成损害国家利益者。

第二十条泄露国家秘密，情节轻微，认错态度好的，可以酌情从轻或免予行政处分。

第六章附则

第二十一条本制度未尽事宜，依照《中华人民共和国保守国家秘密法》、

《中华人民共和国保守国家秘密法实施办法》及省、市有关规定执行。第二十二条本制度由单位单位保密工作领导小组负责解释。

第二十三条自发布之日起执行。

为加强我局保密工作的管理，保守国家机密，维护国家利益和安全，做到“内外有别”、“既便于工作又确保秘密”，现根据国家、省、市有关法律和规定，结合本局实际，制定本制度。

一、人力资源和社会保障工作中的国家秘密，是指关系国家的安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项。

二、人力资源和社会保障工作中国家秘密及其密级的具体范围：

（一）绝密级事项

1. 各类人事录用考试的试题、试卷（含备用卷）、答案；

3. 含有“绝密”内容的密码电报；
4. 引进国外智力工作中的有关涉外政策和经济技术资料。

（二）机密级事项

1. 省、市人民政府管理的干部档案、汇总名册；
2. 尚未出台的工资改革和调整；
3. 尚未公布的全国童工案件查处情况及统计数据；
4. 尚未公布的重大社会敏感政策的调整意见；
5. 全国企业职工集体上访和罢工等重大突发事件的综合情况；
6. 国务院各部门及各省、自治区、直辖市的企业工资调整政策、调整方案；
7. 社会保险基金被挤占挪用和违规动用的重大案件及案件举报人的有关情况；
8. 参加国际劳工组织会议及其他重要国际会议的计划、对策；
9. 非绝密级内容的密码电报；
10. 涉外活动中需要保密的事项。

（三）秘密级事项

1. 市人民政府管理的干部（公务员）的考察材料及未公布的任免、调动事项；
2. 国家机关和事业单位人员计划和工资总额计划；

3. 尚未公布的干部（公务员）录用计划、考试方案及候选人名册；
4. 尚未公布的军队转业干部安置方案和接收安置计划；
5. 尚未出台的企事业单位专业技术职务（含任职资格）的评审事宜及有关统计资料；
6. 副科级以上干部（公务员）档案及考察材料，科级以上公务员的档案及考察材料；
7. 干部调动和录用的审批材料；
8. 享受国家特殊津贴人员材料，国家和省级突出贡献专家的推荐选拔材料；
9. 尚未公布的考试成绩、统计数字和分析情况；
10. 尚未出台的调整机关、事业单位工作人员和离退休、退职人员生活待遇的方案；
11. 尚未公布的失业率、社会保险基金收支预测和计划数据；
12. 反映全国企业工资分配宏观状况的调查资料和统计数据。

三、人力资源和社会保障工作中的下列事项不属于国家秘密，应作为工作秘密管理，不得擅自扩散：

- （一）一般干部的档案；
- （二）人才交流机构代管的人事档案及出境人员的政审材料；
- （五）职业技能鉴定国家题库试题和答案；
- （六）本局在工作中不宜公开的其他工作事项。

四、人力资源和社会保障工作中涉及其他部门或行业的国家秘密事项，应按国家有关主管部门的保密范围确定密级。

五、为加强对保密工作的领导，确定保密工作领导小组成员。局长任组长，分管办公室局领导任副组长，其它局领导及各科室、单位负责人任领导小组成员。

六、认真执行《保密法》，牢固树立保密意识，严守党和国家秘密。

七、严格有密级的文件、资料（下称密件）的登记和交接手续，阅后及时退还，不自行在科室、单位间横传。

八、不擅自翻印、复制密件及内容，不自行扩大阅读范围。确因工作需要复印密件的，须严格履行审批手续，并对复印份数实行保密监督和登记备案。查阅密件档案，须办理审批和登记手续。

九、涉密载体由局办公室定期统一收取销毁。

十、定期进行保密教育和保密检查，总结经验，堵塞漏洞，发现问题，及时处理。

十一、严格遵守国家工作人员保密“十不”规定：1. 不该说的秘密，绝对不说；2. 不该问的秘密，绝对不问；3. 不该看的秘密，绝对不看；4. 不该记录的秘密，绝对不记录；5. 不在非保密本上记录秘密；6. 不在私人通信中涉及秘密；7. 不在公共场所和家属、子女、亲友面前谈论秘密；8. 不在不利于保密的地方存放保密文件、资料；9. 不在普通电话、明码电报、普通邮局传达秘密事项；10. 不携带秘密材料游览、参观、探亲、访友和出入公共场所。

十二、处理、保存重要信息的计算机，必须采取相应的安全保密防护措施，切实消除泄密隐患，并限专人操作，所有信

息的传递必须经主管领导同意。涉密计算机信息系统应采取有效的保密措施，配置合格的保密专用设备，防止泄密、窃密事件的发生。

十三、上网信息的保密管理应坚持“谁上网，谁负责”的原则。凡向国际互联网的站点提供或发布信息，必须通过保密审查批准。涉及国家秘密的信息，不得直接或间接与国际互联网或其它公共信息网络相联接，必须实行物理隔离，或采取相应的防电磁信息泄密的保密措施。

十四、使用政府协同办公系统的计算机不得处理、保存和传输涉密信息。

十五、严格实行《保密工作领导责任追究制》，发生失泄密事件，追究相关责任人和负责人的责任。

村级保密工作实施方案篇四

1、1为保守公司秘密，维护公司权益，特制定本制度。

1、2公司秘密是关系公司权力和利益，依照特定程序确定，在必须时间内只限必须范围的人员知悉的事项，包括但不限于技术秘密和其他商业机密。技术秘密是指不为公众知悉、能为企业带来经济利益、具有实用性并且企业采取保密措施的非专利技术和技术信息。技术秘密包括但不限于：技术方案、工程设计、电路设计、制造方法、配方、工艺流程、技术指标、计算机软件、数据库、研究开发记录、技术报告、检测报告、实验数据、试验结果、图纸、样品、样机、模型、模具、操作手册、技术文档、相关的函电，等等。其他商业秘密，包括但不限于：客户名单、行销计划、采购资料、定价政策、财务资料、进货渠道等。

1、3公司全体职员都有保守公司秘密的义务。接触到企业商业秘密的高级员工，例如：管理人员、技术人员、财务人员、销售人员、秘书等对保守公司秘密负有个性化的职责。

1、4公司保密工作，实行既确保秘密又便利工作的方针。

2保密范围和密级确定

2、1公司秘密包括本制度第1、2项规定的范围以及下列秘密事项：

1) 公司重大决策中的秘密事项。

2) 公司尚未付诸实施的经营战略、经营方向、经营规划、经营项目及经营决策。

3) 公司内部掌握的合同、协议、意见书及可行性报告、主要会议记录。

4) 公司财务预决算报告及各类财务报表、统计报表。

5) 公司所掌握的尚未进入市场或尚未公开的各类信息。

6) 公司职员人事档案，工资性、劳务性收入及资料。

7) 其他经公司确定应当保密的事项。

一般性决定、决议、通告、通知、行政管理资料等内部文件不属于保密范围。

2、2公司秘密的密级分为“绝密”、“机密”、“秘密”三级。

绝密是最重要的公司秘密，泄露会使公司的权益和利益遭受个性严重的损害；

机密是重要的公司秘密，泄露会使公司权益和利益遭受到严重的损害；

秘密是一般的公司秘密，泄露会使公司的权益和利益遭受损害。

2、3公司秘级的确定：

1) 公司经营发展中，直接影响公司权益和利益的重要决策文件、技术资料为绝密级；

2) 公司的规划、财务报表、统计资料、重要会议记录、公司经营状况为机密；

3) 公司人事档案、合同、协议、职员工资性收入、尚未进入市场或尚未公开的各类信息为秘密级。

2、4属于公司秘密的文件、资料，应当依据本制度规定标明密级，并确定保密期限。保密期限分永久、长期、短期，一般与密级相对应，特殊状况外标明。保密期限届满，自行解密。

3公司保密措施

3、1属于公司秘密的文件、资料和其他物品的制作、收发、传递、使用、复制、摘抄、保存和销毁，由办公室或主管副总经理委托专人执行；采用电脑技术存取、处理、传递的公司秘密由电脑部门负责保密。

3、2对于密级文件、资料和其他物品，务必采取以下保密措施：

1) 非经总经理或主管副总公司批准，不得复制和摘抄；

2) 收发、传递和外出携带，由指定人员担任，并采取必要的

安全措施；

3) 在设备完善的保险装置中保存。

3、3属于公司秘密的设备或者产品的研制、生产、运输、使用、保存、维修和销毁，由公司指定专门部门负责执行，并采用相应的保密措施。

3、4在对外交往与合作中需要带给公司秘密事项的，应当事先经总经理批准。

3、5具有属于公司秘密资料的会议和其他活动，主办部门应采取下列保密措施：

1) 选取具备保密条件的会议场所；

2) 根据工作需要，限定参加会议人员的范围，对参加涉及密级事项会议的人员予以指定；

3) 依照保密规定使用会议设备和管理会议文件；

4) 确定会议资料是否传达及传达范围。

3、6不准在私人交往和通信中泄露公司秘密，不准在公共场所谈论公司秘密，不准透过其他方式传递公司秘密。

3、7公司工作人员发现公司秘密已经泄露或者可能泄露时，应当立即采取补救措施并及时报告综合管理部；综合管理部接到报告，应立即作来源理。

3、8出现下列状况之一者，予以辞退并酌情赔偿经济损失：

1) 故意或过失泄露公司秘密，造成严重后果或重大经济损失的；

2) 违反本保密制度规定，为他人窃取、刺探、收买或违章带
给公司秘密的；

3) 利用职权强制他人违反保密规定的。

3、9公司与全体员工签订《员工保守商业秘密协议书》，
《员工保守商业秘密协议书》以书面形式签订，协议附后。

3、10在保密合同有效期限内，员工应履行下列义务：

1) 严格遵守本企业保密制度，防止泄漏企业技术秘密；

2) 不得向他人泄漏企业技术秘密；

3) 非经公司书面同意，不得利用该技术秘密进行生产与经营
活动，不得利用技术秘密进行新的研究和开发：

3、11对高级员工实行“竞业限制”制度，限制管理人员、技
术人员、财务人员、销售人员、秘书等高级员工的以下行为：

1) 自行设立与本公司竞争的公司；

2) 就职于本公司的竞争对手；

3) 在竞争企业中兼职；

4) 引诱企业中的其他员工辞职；

5) 引诱企业的客户脱离企业；

6) 在离职后，与企业进行竞争的其他行为。

3、12涉及公司商业秘密的合作、代理、交易合同或协议，均
需设置“保密条款”，对合同对方增设保密义务。“保密条
款”应当包含以下资料：

- 1) 明示合同所涉及的需要保密的商业秘密范围；
- 2) 合同对方以及合同对方的任何员工、代理人均受保密条款的约束；
- 4) 受约束的保密义务人不可将内含保密信息的资料、文件、实物等携带出保密区域；
- 6) 不相关的员工不可接触或了解商业秘密；
- 7) 保密信息应当在合同终止后交还；
- 8) 保密期限在合同终止后仍然持续有效；
- 9) 违反保密义务的，应当承担明确的违约职责。

4附则

本制度的解释权属于综合管理部。

本制度自发布之日起施行。

村级保密工作实施方案篇五

一、全校工作人员必须严格执行有关保密规定，严守党和国家的秘密，自觉做到不该说的秘密绝对不说，不该知道的秘密绝对不问，不该看的文件绝对不看。

二、机要室是重要涉密部门，无关人员不得随意进入，因工作需要进入的，不得随意翻阅秘密文件和材料。

三、机关来文，由专人统一处理，其他人员不得随意拆封。秘密文件、资料由机要室登记、编号。需送校领导传阅的文件，由机要人员负责运转。各处室秘密文件、资料的传阅和

保管，由处室指定专人负责。秘密文件、资料不得随意复印、摘录、引用和外传，密码电报由机要人员随送、随收，不得在机要室以外存放。

四、使用电传、传真电话传送国家秘密文件资料，必须严格遵守密来密复、明来明复的规定。

五、需要销毁的文件、资料，应统一送交校办公室，经领导批准后，由省国家保密局统一销毁。任何单位或个人不得自行销毁；严禁向废品收购部门出售秘密文件、资料。