

2023年涉密人员保密工作总结 涉密人员管理规定涉密人员保密管理制度(优秀5篇)

总结的选材不能求全贪多、主次不分，要根据实际情况和总结的目的，把那些既能显示本单位、本地区特点，又有一定普遍性的材料作为重点选用，写得详细、具体。相信许多人会觉得总结很难写？下面是小编为大家带来的总结书优秀范文，希望大家可以喜欢。

涉密人员保密工作总结 涉密人员管理规定涉密人员保密管理制度篇一

涉密人员签订保密承诺书，自觉承诺不泄露接触或者知悉的国家秘密信息，有哪些关于涉密人员的管理规定呢？下面本站小编给大家介绍关于涉密人员管理规定的相关资料，希望对您有所帮助。

一、涉密人员负有维护国家秘密安全的责任和保守国家秘密的义务，应自觉遵守有关的法规和制度，接受保密组织的教育和监督。

二、选拔任用涉密人员，要依照机要干部的标准和保密干部专业化要求，进行严格审查，并报上级保密工作部门备案。不得使用临时聘用人员。

三、涉密人员管理由单位组织、人事和保密部门共同实施，并对涉密人员在岗情况每年定期或不定期进行联合检查。对检查中发现不宜留在涉密岗位的，应坚决调离。

四、涉密人员上岗前，必须先参加保密工作部门举办的保密业务培训。 五、涉密人员在岗、离岗和出国(境)前及涉密外

事活动前必须进行保密教育，不断强化政治业务素质。

六、涉密人员必须与单位保密组织签定保密责任书，履行保密责任和保密义务，遵守保密纪律和有关规定。

七、涉密人员辞职、调动，单位应征求上级保密工作部门的意见，并视情况进行脱密期管理。脱密期一般为6个月至3年。

八、涉密人员调动或退休须及时清退个人承办、保管的密件，经有关部门验证无误后，方可予以办理工作调动或退休手续。

九、本制度由市局办公室负责解释。

十、本制度自印发之日起施行。原有规定与本制度不一致的按本制度执行。

第一章 总则

第一条 为保守国家秘密和企业商业秘密，维护国家安全和企业的合法权益，加强在网络维护管理过程中涉及国家和企业保密工作的管理，依据《中华人民共和国保守国家秘密法》，制定本管理办法。

第二条 本管理办法适用于*各单位、各部门及全体员工。

第二章 保密工作基本原则

第四条 *的保密工作由*保密委员会统一领导。保密工作将认真遵循严格管理、严密防范、确保安全、方便工作的原则。

一、不该说的国家秘密和企业商业秘密，绝对不说；

二、不该问的国家秘密和企业商业秘密，绝对不问；

三、不该看的国家秘密和企业商业秘密，绝对不看；

四、不该记录的国家秘密和企业商业秘密，绝对不记录；

五、不准利用工作中的便利条件泄露国家秘密和企业商业秘密；

六、不准在电信业务、公务通信中泄露国家秘密和企业商业秘密；

七、不准在私人交往通信中泄露国家秘密和企业商业秘密；

八、不准在公共场所议论国家秘密和企业商业秘密；

九、不准在非保密本上记录国家秘密和企业商业秘密；

第六条 员工凡泄露国家秘密和企业商业秘密，丢失秘密载体的，视其情节和后果，按照国家相关法律、法则和公司有关规定将给予泄密者行政处分，经济处罚，直至追究法律责任。

第三章 保密组织机构及职责

第七条 成立*保密委员会

一、*保密委员会组成人员

保密委员会主任：

副主任：

委员：

二、*保密工作办公室组成人员(日常办公设在党政办公室)

办公室主任：

副主任：

成员：

第四章 保密工作制度

第八条 *保密工作实行由保密委员会统一领导、分级负责、归口管理、确保安全工作原则。

第九条 建立保密工作责任制，坚持一级对一级负责的精神，逐级签订责任书，把责任分解到部门落实到人。

第十一条 对涉及国家、企业商业秘密的维护管理及维护项目，必须做到事前提出要求，事中加强监督检查，事后验收确认。

第十二条 凡涉密人员严禁使用无线移动电话谈论涉及国家企业要求保密的内容，严禁使用无线互联功能编辑、传送、处理涉及国家企业需保密的文件、资料。严禁涉密人员丢失和损坏涉及国家企业秘密的纸介文件、图纸、资料、影像、磁盘、光盘等。

第十三条 加强对涉密人员的管理，对涉密人员要进行保密培训，使涉密人员掌握必要的保密法律知识，国家相关政策、法规、企业相关制度要求，自觉履行保密责任和义务。

第十四条 对涉及国家，企业秘密的各单位、各部门相关工作人员，要逐级签订保密责任书。

第十五条 严格执行泄密报告制度，不得延误和隐瞒泄密事件。

第五章 保密范围密级及解密

第十六条 涉及国家、集团及北京公司要求保密的所有内容。

第十七条 涉及公司发展规划(包括通信发展规划和网络发展规划)及策略，网络结构和分布情况，新技术、新设备的采用策略等。

第十八条 与通信业务发展策略相配套的管线网络规划、投资规模、成本测算及工程档案、图纸、资料等。

第十九条 维修项目设计(包括总体方案和路由组织)及概预算,项目招投标中的有关评标、选标方案、谈判策略及重大项目合同书内容。

第二十条 通信网络组织,枢纽分布和干线具体路由,通信交换设备、传输设备、终端设备、无线室内覆盖等设备的功能,容量和具体位置,安装及市场占有率等。

第二十一条 未公开的专有技术、技术体制、技术标准、网络结构、工程设计、技术试验结果、关键技术及具有知识产权的软件。

第二十二条 企业人才发展规划、组织编制、人员结构、员工素质、人员信息统计报表、人事档案(如企业高管人员、履历、信息、后备干部情况、考察材料及人事任免事项等),员工职务体系及薪酬。

第二十三条 企业外事活动中的内部通报及内部规定,未公开的对外通信合作计划、协议、协定、各纪录及会议纪要。

第二十四条 维护工作分析会会议资料及各项数据统计及资金计划等。

第二十五条 纪检监察工作中涉及的来信来访、调查、处理过程,未审结公布的案情及诉讼情况、检举人、揭发人、控告人、证人的有关情况。

第二十六条 企业内部办公自动化及业务管理系统中使用的计算机系统的程序指令、数据库及加密方式。

第二十七条 涉及企业商业秘密的领导讲话、文件资料、函件、

传真电报、会议记录、纪要、档案、简报、规章制度、统计报表等。

第二十八条 国家及企业秘密、企业商业秘密等级按文件保密部门要求确定，分为绝密、机密、秘密三个等级。

第二十九条 公司工作中所涉及的国家秘密如需要进行变更和提前解密，必须按国家有关保密规定处理，并做相应文字记载和解密标志。

企业商业秘密的解密可根据情况的变化和企业的利益，由产生秘密的单位确定提前或延期解密，同时要经过上级单位保密部门的同意，并做相应文字记载和解密标志。

第六章 文件资料等涉密载体的保密

第三十条 员工在起草文件时，凡涉及国家秘密或企业商业秘密内容的，均应依照规定，准确标明密级和制作数量，规定发放范围和保管期限。绝密级应编排顺序号。

第三十一条 各部门发出和收到涉密文件资料、磁盘、光盘等秘密载体，均应严格履行登记、签收、编号、清点手续，经管人员要手递手进行传递，并随时掌握其去向。

第三十二条 制发带有密级的文件资料，必须由主管领导制定的专人在企业内部完成；复制秘密和机密级文件资料，必须经主管领导同意，办公室登记方可复制，其复印件按原件密级管理；绝密级文件资料不得复制，如确需复制，则必须经密级制发单位或本单位主管领导批准。

磁介质、光盘等秘密载体的制作应尽可能由业务部门在本企业内部完成。如制作量较大，可在保密部门审查通过的单位制作，其制作场所要符合保密要求，使用电子设备的应当采取防电磁泄漏的保密措施。

制作涉密文件资料、磁盘、光盘等秘密载体过程中所形成的不需归档的材料,应及时销毁。

第三十三条 严格控制涉密内容的知悉范围,阅读和使用秘

密载体应在符合保密要求的办公场所进行;绝密级国家秘密和企业商业秘密只有经过批准的人员才能接触;禁止将涉密文件资料、磁盘、光盘等秘密载体携带出境。如工作需要携带出境的,应按照国家和企业有关保密规定办理批准和携带手续;绝密级文件资料和密码电报不得全文抄录。确因工作需要必须摘抄的,须经有批准权的领导批准,摘抄在保密本上,并妥善保管。

第三十四条 涉密文件资料、磁盘、光盘等秘密载体由党政办公室集中管理,各单位、各部门留存期间必须妥善保管,其他内设机构及经办人不得长期留存。

第三十五条 各单位、各部门要在每年年底,对涉密文件资料、磁盘、光盘等秘密载体统一进行收缴,按规定整理归档或按有关保密规定集中销毁。

销毁秘密载体应经本单位主管领导审核批准,并履行清点、登记手续。纸介质秘密载体可使用碎纸机进行销毁,磁介质、光盘等秘密载体要采用物理或化学方法彻底销毁,确保涉密内容无法还原。

第七章 通信的保密

第三十六条 秘密载体(如:涉密文件资料、磁盘、光盘等)的传递必须由机要人员通过机要渠道进行,不得通过普通邮政渠道或其它渠道进行传递。

缝有韧线的专用信封,并且在封装后,于信封封口及中缝处加盖密封章或加贴密封条。

第三十七条 凡涉密的信息联系必须使用加密通信设施，不得使用无保密措施的通信设备和计算机进行传送；在无保密措施的通信设施中不得谈论国家秘密和企业商业秘密。

第三十八条 计算机系统处理、传递、存储涉密信息时要严格执行《国家保密局计算机信息系统保密管理暂行规定》，涉密计算机或企业办公自动化网必须与外界互联网实行物理断开或设置防火墙。通过互联网与外界进行互联时，要提高网络安全意识，禁止将本单位个人、他人或公共ip 地址泄露给外界。

企业所有计算机均应设置秘密口令，关键数据和软件应该加密。

第三十九条 绝密级国家秘密和企业商业秘密不得通过现代通信及计算机网络进行传递。

第八章 人员、机构变动中的保密

第四十条 各级领导要带头执行国家和企业的有关保密工作规定和工作纪律，在工作变动和办理离退休手续时，要主动把涉及国家秘密和企业商业秘密的各种文件资料、工作笔记、磁盘等移交档案部门处理。

第四十一条 离退休人员个人留存的公务材料、涉及国家秘密和企业商业秘密的文件资料应交原工作单位统一处理。

第四十二条 新员工加入企业时与企业所签订的劳动合同应包括保密条款。

第四十三条 对接触国家秘密或企业商业秘密的员工，在办理调离、辞职、辞退及离退休手续时，必须与单位签订保密协议，承担保密义务，同时要将个人保管的所有秘密载体（如：涉密文件资料、磁盘、光盘等）交还企业。

第四十四条 被撤销或合并的涉密单位，应将秘密载体移交给

承担其原职能的单位或上级主管部门,并履行登记、签收手续。

第九章 附则

第四十五条 全体员工必须认真执行本办法,若发生失、泄密事件应及时向主管领导和本单位保密部门汇报,并积极采取补救措施,将损害降到最低水平。

第四十六条 各部门要认真执行相关规定,认真按照*保密管理工作管理办法的要求抓好保密工作的落实。

第四十七条 本办法由*保密委员会负责解释。

第四十八条 本管理办法自发布之日起执行。

共2页,当前第1页12

涉密人员保密工作总结 涉密人员管理规定涉密人员保密管理制度篇二

xx机关、单位组织涉密人员签定保密承诺书,此次保密承诺书签定活动是为了进一步加强机关涉密人员的保密教育和管理,提高保密意识,强化保密责任,落实涉密人员的保密法律义务,确保国家秘密安全□

1、认真遵守国家保密法律、法规和规章制度,履行保密义务,不提供虚假个人信息,自愿接受保密审查。

2、不违规记录、存储、复制国家秘密信息,不违规留存国家秘密载体;不以任何方式泄露所接触和知悉的国家秘密;未经单位审查批准,不擅自发表涉及未公开工作内容的文章、著述;离岗时,自愿接受脱密期管理,签订保密承诺书。

3、涉密岗位的相关人员要进行保密知识教育，要求涉密人员带头履行承诺，带头学习保密知识，掌握保密技能，真正做到懂保密、会保密、善保密。

4、《保密承诺书》签订后，将建立保密承诺档案，保密承诺执行情况纳入干部年度考核内容，对不履行保密义务的将依法依纪追究责任。

违反以上承诺，自愿承担党纪、政纪责任和法律后果。

承诺人签名：

年 月 日

一、认真遵守国家保密法律法规和本企业保密管理规定，履行保守企业技术、经济及商业秘密的义务。

二、不以个人名义从事与本企业技术、经济和商业秘密相关的咨询和服务等活动，不利用本企业的技术、经济和商业秘密擅自进行生产经营活动，未经批准不会扩大技术、经济和商业秘密知晓范围。

三、个人发表论文、著作或公布信息时，涉及本企业技术、经济和商业秘密的，上报本企业相关专业主管部门进行保密审查，并对技术、经济和商业秘密内容进行妥善处理。

四、不擅自携带涉及本企业技术、经济和商业秘密的信息资料离开工作场所。

五、不以任何方式泄露所接触和知悉的涉密信息。

六、本人因内退、退休、解聘、辞职、解除劳动合同、开除等原因离岗离职时，主动向所在单位交清所有内控文件资料和涉及企业技术、经济及商业秘密的文件、资料、图纸、软

盘以及其它存储介质，不私自带走或复制。

七、自愿接受脱密期管理，本人离开原单位三年内，决不行下列活动：

(一)直接或间接参与组建使用与xx公司拥有相同技术的`新单位。

(二)帮助他人在与xx公司拥有相同技术的领域与xx公司竞争。

(三)在与xx公司经营同类业务的其他单位内任职。

八、若本人违反上述承诺，自愿承担党纪、政纪责任和法律后果。

承诺人签字：

xx公司主管领导签字：

(盖单位公章) 二0xx年 月 日

甲方[]z所、z铂业股份有限公司 地址[]xx-xx

乙方姓名： 身份证号：

1. 本人对在工作中接触到的z铂业股份有限所和公司根据《国家保密法》和行业密级具体范围的规定确定为国家秘密的事项，在离岗后绝不以任何方式向外泄露。

2. 本人承认在z铂业股份有限所和公司工作期间接触、研制国家军工科研项目或军品生产时所产生的任何秘密事项，属国家和z铂业股份有限所和公司所有。

3. 本人已清楚知道因个人的故意或不当行为将导致或可能会触犯《中华人民共和国刑法》中的窃取、刺探、非法提供、非法持有、泄露国家秘密所列之罪行。

4. 本人如违反“离岗保密承诺书”规定的行为，国家有关部门和z铂业股份有限所和公司有权追究本人相关责任。

5. 上述离岗保密承诺书本人已经仔细阅读，对其中的所有内容没有疑义，本人愿为保守国家秘密承担责任自愿签订“离岗保密承诺书”。愿意按承诺书中规定的内容承担保密责任。保密承诺书自本人签订之日起生效。

7. 本保密承诺书一式叁份，人事部门壹份、保密办公室壹份、承诺人壹份。

甲方□z所、z铂业股份有限公司 乙方：

法定代表人或授权代表人(签章)

日期： 日期：

二、 不以任何方式泄露所接触和知悉的国家秘密；

三、 已全部清退不应有个人持有的各类国家秘密载体；

六、 自愿接受脱密期管理，自 年 月 日至 年 月 日服从有关部门的保密监管。

违反上述承诺，资源承担党纪、政纪责任和法律后果。

乙方离开甲方公司后，新的工作单位为： ； 职务： ； 联系方式： 。

承诺人签名：

日期:

涉密人员保密工作总结 涉密人员管理规定涉密人员 保密管理制度篇三

涉密人员上岗应当经过保密教育培训，掌握保密知识技能，对于涉密人员制定了哪些管理规定呢?下面本站小编给大家介绍关于涉密人员保密管理规定的相关资料，希望对您有所帮助。

一、涉密人员应遵守10条保密守则。

(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;

(六)不在私人通讯中涉及秘密;

(七)不在公共场所和家属、子女、亲友面前谈论秘密;

(八)不在不利于保密的地方存放秘密文件、资料;

(九)不在普通电话、明码电报、普通邮局传达秘密事项;

(十)不携带秘密材料游览、参观、探亲、访友和出入公共场所。

一、各科室微机由科室负责人指定专人专管。

三、严格执行《计算机信息系统安全保护条例》，与工作无关的严禁使用。严禁将密码告知无关人员。

四、下班时间专管人员应负责锁机。

五、专管人员对本科室电脑资料妥善保管，未经科室负责人许可，严禁将本单位软件资料打印或拷贝给外单位人员，重要资料必须征得单位主管领导同意，否则追究保管人责任。

一、制订、执行保密法制宣传教育规划，每年对保密普法工作进行布置、检查、总结。

二、每年以创办保密知识宣传栏、开展保密知识竞赛、举办保密讲座、组织观看保密教育录相等形式，提高全体职工的保密安全意识。

三、经常性组织职工学习《保密法》和各项规章制度，做到依法管理，依法治密。

四、各部门应针对岗位特点进行保密安全教育培训，重点对涉密人员加强教育培训，增强整体保密管理素质。

涉密人员保密工作总结 涉密人员管理规定涉密人员保密管理制度篇四

一、认真遵守国家保密法律法规和本企业保密管理规定，履行保守企业技术、经济及商业秘密的义务。

二、不以个人名义从事与本企业技术、经济和商业秘密相关的咨询和服务等活动，不利用本企业的技术、经济和商业秘

密擅自进行生产经营活动，未经批准不会扩大技术、经济和商业秘密知晓范围。

三、个人发表论文、著作或公布信息时，涉及本企业技术、经济和商业秘密的，上报本企业相关专业主管部门进行保密审查，并对技术、经济和商业秘密内容进行妥善处理。

四、不擅自携带涉及本企业技术、经济和商业秘密的信息资料离开工作场所。

五、不以任何方式泄露所接触和知悉的涉密信息。

六、本人因内退、退休、解聘、辞职、解除劳动合同、开除等原因离岗离职时，主动向所在单位交清所有内控文件资料和涉及企业技术、经济及商业秘密的文件、资料、图纸、软盘以及其它存储介质，不私自带走或复制。

七、自愿接受脱密期管理，本人离开原单位三年内，决不进行下列活动：

(一)直接或间接参与组建使用与xx公司拥有相同技术的新单位。

(二)帮助他人在与xx公司拥有相同技术的领域与xx公司竞争。

(三)在与xx公司经营同类业务的其他单位内任职。

八、若本人违反上述承诺，自愿承担党纪、政纪责任和法律后果。

承诺人签字□xxx

涉密人员保密工作总结 涉密人员管理规定涉密人员 保密管理制度篇五

一、涉密人员应遵守10条保密守则。

(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；

(六)不在私人通讯中涉及秘密；

(七)不在公共场所和家属、子女、亲友面前谈论秘密；

(八)不在不利于保密的地方存放秘密文件、资料；

(九)不在普通电话、明码电报、普通邮局传达秘密事项；

(十)不携带秘密材料游览、参观、探亲、访友和出入公共场所。

b科室微机保密管理规定

一、各科室微机由科室负责人指定专人专管。

三、严格执行《计算机信息系统安全保护条例》，与工作无关的严禁使用。严禁将密码告知无关人员。

四、下班时间专管人员应负责锁机。

五、专管人员对本科室电脑资料妥善保管，未经科室负责人许可，严禁将本单位软件资料打印或拷贝给外单位人员，重要资料必须征得单位主管领导同意，否则追究保管人责任。

c保密宣传教育规定

一、制订、执行保密法制宣传教育规划，每年对保密普法工作进行布置、检查、总结。

二、每年以创办保密知识宣传栏、开展保密知识竞赛、举办保密讲座、组织观看保密教育录相等形式，提高全体职工的保密安全意识。

四、各部门应针对岗位特点进行保密安全教育培训，重点对涉密人员加强教育培训，增强整体保密管理素质。

针对当前敌特窃密活动猖獗，内部人员窃密、卖密、无意识泄密案件成上升趋势，涉密人员管理缺乏量化考评和资质认证等问题，必须加强研究涉密人员科学管理的体制机制，考核与评估涉密人员保密能力与素质的评估指标体系与方法，建立针对涉密人员的全程管理信息系统，将涉密人员的政审、保密技能培训、资质认证、经常性的保密教育统一起来；将涉密岗位的设置、涉密人员的选择、培训、使用与保密津贴的发放、人员的调配晋升等关联起来，通过科学化、信息化、系统化的管理确保接触秘密的人受控、可信、可靠。

三是涉密人员社会关系复杂、流动性增加，面临更多主动或被动泄密的诱-惑和陷阱。

我党在革命战争年代以及新中国建设与发展时期保密工作所取得的成功经验告诉我们，加强涉密人员的教育、培训和管理是确保核心秘密安全的基础。在当前这种严峻的形势下，更要采用科学的手段和方法选人、用人，改变涉密人员的教育、培训和任用体制，增强涉密人员的敌情观念和法纪观念，

强化其保密意识，使他们掌握保密技能，真正做到要保密、懂保密、会保密和善保密。

作为世界拥有核心秘密最多的发达国家，美国在涉密人员管理方面可谓经验丰富。在美国任何一个人想要接触秘密，除了必须是美国公民，因工作需要必须接触秘密的前提条件外，还要对其家庭出身、价值取向、心理、爱好、性格、习惯、日常所接触的亲友、消费及犯罪记录等进行全面、系统的审查。只有通过这些审查，并且在签订保密协议、宣誓，经过必要的保密技能培训和保密教育后，才能接触限定范围内的秘密。即使是掌管秘密的部门首长、自己的同事和亲人，也无权获取其不应该知悉的秘密，因为其定期的行为审计和审查，以及对失泄密进行的惩罚是十分严厉的。

德国虽然拥有世界先进的信息技术和管理经验，但是其保密管理仍然注重以人为核心。核心秘密通过人而不是网络传递，接触秘密的人绝对不使用手机等现代通讯设备，严格的涉密人员管理措施和制度确保了国家秘密的安全。

与德国不同的是，美国的国防部门与军队，乃至军工企业、科研院所等大量使用计算机和网络通讯技术传递、处理与利用涉密信息，所采用的保密技术大多是日前成熟的商用安全技术，却很少发生严重的失泄密事件。而我们国家近年来却因网络使用不当或管理不善造成很多严重的失泄密事件。分析原因还是在涉密人员管理上出现了很大漏洞。接触秘密的人保密意识与技能差，保密教育流于形式，保密审查与监督机制落后等，使得我们不敢使用网络但又离不开网络。

2000年前后，我国在军工企业推行“密级项目管理与岗位定密”，即“双定密”工作，取得了显著的成效，不但加强了定密管理，还对如何管好涉密人员提出了有益的思路：必须对涉密人员实行岗位责任制。要根据接触秘密的范围、涉密程度等因素建立界限明晰的涉密岗位，对每个岗位提出明确的岗前保密知识、技能的考核要求，并将涉密人员的保密津

贴与涉密岗位紧密关联起来，使岗位管理成为涉密人员管理的一种有效手段。

类似于银行系统的信用等级评价体系，通过建立涉密人员的可信度评价指标体系，实现对涉密人员身份、地位、工作性质、社会环境、历史表现、性格特征、兴趣爱好、感情稳定性等可能影响其保密意志、立场、信念和执行力的诸多因素的综合考评，对涉密人员的可信度进行跟踪记录，并记入其档案或任职晋级的考核指标中。通过建立这样的管理制度和运行机制，有利于更为系统、全面地考察涉密人员的素质，预防人为因素、主观因素对涉密人员考评带来的负面或不利影响。

（二）

岗位认证的实质是为了加强对保密专职人员、核心岗位涉密人员的教育培训与保密知识、技能的考核。所有接触核心涉密事项或参与核心涉密活动的人员，在上岗前，或者调整岗位时，必须取得相应等级、相应范围的涉密岗位资质证书。通过实施类似于国家计算机等级考试或职称考试的上岗培训模式，将保密教育转变为强制性的、必须落实的一项措施，同时能够保证保密教育的效果。岗位认证可采取分级考核并颁发证书的方式，使之与涉密人员的涉密等级、涉密领域紧密挂钩，并规定一定的有效期（如每五年重新进行一次考核），这样才能将保密教育经常化、制度化。

（三）

责任分离是一种降低偶然或者蓄意泄密风险的方法。应当考虑把某些责任或者责任区的管理权与执行权加以分离，减少对涉密载体、文件、系统或者服务未经授权的访问或者改动的机会。对涉密人员的管理也要充分体现管理（使用）权与监督权相分离的原则。即接触秘密的人员必须受到有效的监督，这种监督不能由接触秘密的人自己履行。现在很多单位

设置的保密专职人员，往往把本单位所有的秘密事项（如移动涉密载体）统管起来，这种做法实际上违背了秘密分割和最少知道原则，管理涉密事项的人如果不可靠，就会造成秘密的完全泄漏。反之，负责监督秘密访问（存取）的人员不能得到秘密，只有这样才能实现有效的相互制约。为了实现这一机制，必须在管理方式和技术手段上加以改进，例如建立移动涉密载体的监管系统。与此类推，对涉密计算机网络、涉密场所等，都要建立健全相应的监管系统，把使用涉密网络和进出核心涉密场所的人员有效管理起来。

（四）

奖惩激励是管理学常用的机制。保密存在风险，保密人员承担着相应的责任，奖惩激励体现的是责权利相结合的原则。对允许接触秘密的人员，按照所允许接触的信息的秘密级别确定相应百分比的附加工资或津贴。国家权力机关、军队相关部门在进行组织变动、编制体制调整、人员晋级晋衔、立功受奖考评时，对涉密人员要在其他同等条件下保留相应的优先权。同样，如果出现失泄密事件，确定责任后，要依据国家、军队的相关法律、法规实施处罚。奖惩激励机制的目的是充分调动人员的积极性，使他们从“要我保密”转变到“我要保密”上来。

综上所述，核心秘密的保密管理必须将涉密人员的管理放在第一位。这是因为获取、利用、处理甚至管理秘密的主体是人。虽然在信息时代可以利用各种先进的保密技术，例如加密技术、身份认证技术、访问控制技术等加强对秘密载体和信息秘密的保密监管与控制，但是，一旦有权限接触秘密的人出现问题，上述所有手段与措施都会功亏一篑。相反，如果能建立有效的涉密人员教育、培训、审查与考核体系，就能极大地弥补技术管理先天存在的不足，降低主动卖密或无意识泄密的风险。