目 录

保密知识问答

保密知识问答

1.什么是国家秘密？

国家秘密是关系国家安全和利益，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。

2.什么是工作秘密？

工作秘密，是机关、单位在履行职能过程中产生或者获取的，不属于国家秘密，但泄露后会妨碍机关、单位正常履行职能或者对国家安全、公共利益造成不利影响的内部敏感事项。

3.国家秘密的基本范围？

下列事项泄露后可能损害国家在政治、经济、国防、外交等领域的安全和利益的，应当确定为国家秘密:

（1）国家事务重大决策中的秘密事项;

（2）国防建设和武装力量活动中的秘密事项;

（3）外交和外事活动中的秘密事项以及对外承担保密义务的秘密事项;

（4）国民经济和社会发展中的秘密事项;

（5）科学技术中的秘密事项;

（6）维护国家安全活动和追查刑事犯罪中的秘密事项;

（7）经国家保密行政管理部门确定的其他秘密事项。

4.哪些事项不能确定为工作秘密？

（1）依法应当确定为国家秘密的;

（2）党内法规、法律、行政法规、规章和国家有关规定明确要求公开的;

（3）需要社会公众广泛知晓或者参与的;

（4）已经依法公开或者不可控制知悉范围的。

5.国家秘密分为哪几个等级？

国家秘密分绝密、机密、秘密三个等级。

“绝密”是最重要的国家秘密，泄露会使国家的安全和利益遭受特别严重的损害。

“机密”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。

“秘密”是一般的国家秘密，泄露会使国家的安全和利益遭受损害。

6.什么是国家秘密标志？

国家秘密标志，是指标记在国家秘密载体上，表明其内容涉及国家秘密的一种法定的文字与符号标识。国家秘密的标志由密级、标志符号、保密期限（或解密条件）三部分组成。完整的国家秘密标志的内容为：“密级★保密期限（解密条件）”。“★”为标志符号，密级在标识符号★前标注，保密期限（或解密条件）在标志符号★后标注。

7.工作秘密标志是什么？

工作秘密没有法定专属标志，确定为工作秘密的载体一般在其明显部位以“内部”、“内部事项 注意保管”等方式作出提示。

8.国家秘密与工作秘密的区别？

（1）法律特征不同。

“国家秘密”的法律特征有三点:

①关系国家的安全和利益的事项。

②依照法定程序确定。

③在一定时间内只限一定范围的人员知悉。

“工作秘密”其含义包括两点:

①除国家秘密以外的，在公务活动中不得公开扩散的事项。

②一旦泄露会给本机关、单位的工作带来被动和损害。

（2）权利主体不同。

“国家秘密”的权利主体是“国家”，作为国家秘密唯一拥有的特定主体。

“工作秘密”以本机关、单位为拥有主体。

（3）确定程序不同。

“国家秘密”强调要经过法定程序确定，并且在《保密法》中规定了一套极为严格的确定程序。

“工作秘密”由各机关、单位自行确定

（4） “秘密”的标志不同。

国家秘密有专属标志，分为三个等级，同时又原则地规定了区分三个密级的标准。三个不同的等级如何在密件或密品上标志也有专门的规定。

工作秘密没有法定的专属标志，不分等级、一般以“内部文件”“内部事项”等方式作出提示。

（5）一旦泄露危害的对象不同。

“国家秘密”一旦泄露危害的是国家的安全和利益。

“工作秘密”一旦扩散或公开，会给本机关工作造成被动和损害。

（6）一旦泄露所承担的法律责任不同。

“国家秘密”一旦被泄露，除了要承担行政责任外，构成犯罪的还应承担刑事责任。

“工作秘密”一旦泄露，要承担行政责任，受到行政处分。

9.什么是定密责任人？

定密责任人是指机关、单位负责国家秘密确定、变更和解除工作的专门人员。保密法关于定密责任人的规定表明，定密责任人分为法定定密责任人和指定定密责任人两类。法定定密责任人是指机关、单位负责人，对本机关、本单位定密工作负总责。指定定密责任人是指由法定定密责任人通过授权程序指定的履行定密责任人职责的其他人员。

10.什么是定密权限？

定密权限也就是确定国家秘密密级的权限，是指对不同密级国家秘密确定资格的授权与限制。修订后的保密法改变了以往任何机关、单位都可以确定任何密级的做法，设定了定密权限制度和授权定密制度。即中央国家机关、省级机关及其授权的机关、单位可以确定绝密级、机密级和秘密级国家秘密；设区的市、自治州一级的机关及其授权的机关、单位可以确定机密级和秘密级国家秘密。具体的定密权限、授权范围由国家保密行政管理部门规定。

11.什么是派生定密？

派生定密是指机关、单位在执行上级机关、单位或者办理其他机关、单位确定的国家秘密事项时，对在执行中所产生的文件、资料需要定密的，直接根据所执行或者办理的国家秘密事项的密级、保密期限和知悉范围进行确定。

12.为什么说保守国家秘密是全体工作人员的义务？

《宪法》第五十三条规定：“中华人民共和国公民必须遵守宪法和法律，保守国家秘密……”《宪法》第五十四条规定：中华人民共和国公民有维护祖国的安全、荣誉和利益的义务，不得有损害祖国的安全、荣誉和利益的行为。”《保密法》第三条规定：“一切国家机关、武装力量、政党、社会团体、企业事业单位和公民都有保守国家秘密的义务。”因此，保护国家秘密是所有工作人员的义务。

13.涉密人员应当遵守哪些保密管理规定？

（1）严格遵守涉密载体保密管理规定;

（2）严格按照涉密信息保密要求，传输、储存、处理涉密信息;

（3）组织、参与涉密会议时应当遵守有关的保密要求;

（4）不得在社会交往、接受采访或涉外活动中涉及国家秘密;

（5）不得在私人通信及公开发表的文章、著作、讲演中涉及国家秘密;

（6）不得与亲友、无关人员谈论国家秘密;

（7）外出访问、考察等活动中不得擅自携带涉密载体，确因工作需要携带的，须按规定办理审批手续，并采取严格的保密措施;

（8）发生泄密事故时，应立即采取补救措施并及时向所在单位报告;

（9）不得隐瞒泄密事故;

（10）自觉接受保密教育和保密监督检查。

14.落实领导干部保密工作责任制有哪些具体要求?

（1）应将各级领导干部落实保密工作责任制的情况，纳入领导干部民主生活会和领导干部年度考核内容。凡履行保密工作领导责任不力的，不得提拔使用。

（2）主要领导干部对本单位保密工作负有全面领导责任，分管保密工作的领导对本单位保密工作负有组织领导责

任，分管有关业务工作的领导对所分管业务工作范围内的保密工作负有直接领导责任。

（3）对认真履行保密工作职责、为保守国家秘密做出显著成绩和突出贡献的领导干部，依照有关规定予以表彰或奖励。

（4）对单位存在重大泄密隐患或发生泄密事件负有主要领导责任的领导干部，视情节轻重，按照党纪政纪规定分别给予警告、严重警告、撤销党内职务、留党察看或开除党籍处分。

（5）对玩忽职守、拒不履行保密工作领导职责，造成严重泄密后果的领导干部，要依法追究法律责任。

15.保密管理工作应遵循哪些基本原则？

（1）坚持党委统一领导保密工作的原则；

（2）“归口管理、分级负责”的原则；

（3）“谁主管，谁负责”的原则；

（4）坚持依法管理的原则；

（5）保密管理与业务管理结合的原则；

（6）管理与服务相结合的原则。

16.对涉密人员的管理有哪些要求？

（1）涉密人员上岗前应接受单位及有关部门的审查，与单位签订涉密人员保密承诺书，接受相应的上岗教育培训，经考试合格后，方可上岗。

（2）涉密人员的日常管理、教育由所在单位和保密工作部门负责；单位应定期对涉密人员进行考核监督，并根据在岗工作表现进行奖惩。

（3）涉密人员调整工作岗位时，应经过单位保密工作部门审核和批准，遵守脱密期管理有关要求。

（4）涉密人员脱离涉密岗位，应履行批准手续，与单位签订保密承诺书，按照脱密期制度进行管理。

17.什么是脱密期管理？

脱密期管理，是指涉密人员因辞职、解聘、调动等原因离开涉密岗位，在一定期限内对从业和出境方面进行的必要限制。主要内容包括:

（1）从业限制。涉密人员在脱密期内不得到境外驻华机构、组织或外商独资企业工作，不得为境外组织或人员提供劳务、咨询等服务。

（2）出境限制。涉密人员在脱密期内出境，必须经有关机关审查批准，不得擅自出境。

（3）期限要求。涉密人员的脱密期限由单位根据其涉密程度确定。核心涉密人员的脱密期为 2～3 年，重要涉密人员的脱密期为 1～2 年，一般涉密人员的脱密期为 6 个月～1 年。

18.什么是涉密载体？涉密载体有哪些种类？

单位涉密载体主要有以文字、数据、符号、图形、图像、视频和音频等方式记载国家秘密信息的纸介质、磁介质、光

介质及半导体介质等各类物品。

纸介质涉密载体是指以文字、图形、符号、等书面形式记录国家秘密信息的介质，如国家秘密文件、文稿、档案、电报、信函、图纸及其它图文资料等。

磁介质涉密载体是以磁性物质记录国家秘密的载体，如记录国家秘密信息的计算机硬盘、移动硬盘、软盘以及录音带、录像带等。

光介质涉密载体是以光信号记录国家秘密信息的载体，如光盘。半导体介质涉密载体是以电子器件存储国家秘密信息的载体，如U盘、存储卡等。

密品是直接含有国家秘密信息的设备、产品等。这类载体有的可以通过外观观察获得国家秘密信息，有的则需要通过一定手段进行测试、分析获得国家秘密信息。

19.单位制作涉密载体有哪些保密要求？

制作涉密载体包括起草涉密文件、资料和印刷、制作国家秘密载体。

（1）起草涉密文件、资料的过程稿、送审稿、讨论稿、修改稿、征求意见稿等，都要严格按照秘密文件、资料保密管理规定妥善保管，不能随意丢弃。

（2）涉密文件、资料一经产生，应当严格履行定密程序，确定密级和保密期限。

（3）制作涉密文件、资料应注明发放范围、制作数量和

编排顺序号。需要委托印刷厂印制的，应送保密行政管理部门确定的涉密载体定点复制单位印制。禁止将涉密文件、资料委托非定点单位印制。

（4）印制过程中的废页、废料、残页、残料、校对稿、胶片、胶版等，需要保存的，应当按照国家秘密载体保密管理规定妥善保管；不需要保存的，应当按规定销毁，不能随意处置，不得作为废品出售。

（5）使用磁、光、半导体等介质拷贝、刻录国家秘密信息，应当在单位内或国家保密行政管理部门确定的定点单位进行，并在适当位置做出国家秘密标志，不能托交其他社会单位或无关人员刻录、制作。

（6）严格按照批准的数量制作，承办人员及其他任何人不能多制、私留涉密载体。

20.单位收发、传递国家秘密载体有哪些保密要求？

收发人员要按照保密规定核对、登记涉密载体，严格按照规定的知悉范围收发密件，并掌握国家秘密载体的流转情况。

（1）收发国家秘密载体，应履行登记、编号、签收手续，签收时必须逐件清点、核对。

（2）密件包装应当由单位的机要保密人员或有关专门人员拆封。

（3）接收密件，及时在收文（件）登记簿上登记。分发

密件要严格分发范围，遵守相关规定。

（4）注意检查信封、袋、套密封是否完好无损，确认未被拆开，才能接收。如发现问题，应当立即将情况报告单位主管领导和发文（件）单位处理。

（5）检查签收单上的登记与涉密实物是否相符，如果不相符，不能接收，同时要及时告知发文（件）单位，并要求投递人员弄清原因。

（6）传递、运输国家秘密载体必须交由机要交通、机要通信部门，不得通过普通邮政邮寄或交给无关人员捎带；确需自行传递、运输的，要选择安全的交通路线和交通工具，采取严密的保密措施。设有机要文件交换站的城市，在本市区内传递机密级、秘密级秘密载体，可以通过机要文件交换站进行。

21.复制涉密载体有哪些保密要求？

（1）绝密级国家秘密涉密载体原则上禁止复制，因工作需要确需复制的，必须经原制发机关、单位或其上级机关批准。复制上级机关下发或其他机关单位制发的机密级，秘密级载体，也应当经制发机关批准。

（2）复制制发机关、单位允许复制的国家秘密载体，应当经本机关、本单位的主管领导批准并履行审批手续。

（3）复制国家秘密载体，不得改变其密级、保密期限和知悉范围；

（4）复制国家秘密载体，应当履行登记手续；复制件应当加盖复制单位、单位复印戳记，并视同原件管理。

（5）复制涉密载体应在本单位内部进行；需要送外单位复制的，应交由保密行政管理部门确定的定点单位复制；

（6）复制过程中形成的中间材料，包括文件、资料的草稿、废稿、废页等，应当妥善保管。不需要保存的，应按规定及时销毁。

22.借用涉密载体有哪些保密要求？

有一些国家秘密事项需要有关单位、科室和人员在一段时间内长期使用、随时查询并遵照执行，可以由科室借用暂时保管，但应当遵守下列保密规范:

（1）借用涉密载体的单位、科室和人员应当符合该项国家秘密事项知悉范围的规定，并经单位主管领导批准，办理借用登记手续。

（2）借用涉密载体应当由借用单位、科室指定专人保管，在符合保密要求的文件柜中保存，没有保存条件的随用随借，当天归还。绝密级涉密载体不得在借用单位和科室留存。

（3）借用的涉密载体在使用完毕后应当及时清退，并办理清退手续。

23.传阅涉密文件应遵守哪些保密要求？

（1）不横传文件。文件应由专人传送，阅办部门不得互相横传文件。

（2）传阅时间不应过长。经办人员应根据文件内容和知悉范围，及时、迅速传阅、办理，不得拖延，事后应在办文单上签字或写明办理经过及结果。

（3）传阅部门不应过多。传阅文件应遵守主要领导、主管领导、主管部门先阅和急用先阅的规则。

24.怎样保存涉密载体?

（1）涉密载体必须在符合国家保密标准的密码文件柜内保存。绝密级涉密载体应当在专库密码保险柜内保存。

（2）离开涉密场所时，应当将涉密载体存放在密码文件柜内，并关锁门窗。

（3）个人不得私自保存涉密载体。确因工作需要，个人持有涉密载体，须经主管领导批准，使用完毕后应当及时清退。

（4）保密工作部门以及涉密单位每年应定期对当年所存涉密载体进行清查、核对，发现问题及时上报。

25.携带涉密载体外出有哪些保密要求?

（1）确因工作需要携带的，应经保密工作部门批准，采取严格保护措施，使载体始终处于有效监控之内。

（2）原则上应避免携带绝密级涉密载体外出。确因工作需要携带的，必须经单位保密工作部门主管领导批准，并严密封装，至少应有两人同行，并做好涉密载体的签收、回收工作。必要时应及时销毁。

（3）参加涉外活动时，不得携带涉密载体。确需携带机密级、秘密级涉密载体的，应经单位保密工作部门主管领导批准，并采取严格保密措施。

26.个人是否可以留存涉密载体?

确因工作需要留存涉密载体的，应在单位办理相关借用手续，用完后要及时归还。严禁个人长期留存涉密载体。

27.维修涉密载体应当遵守哪些保密规定?

涉密计算机、U盘、移动硬盘等涉密存储设备，带有存储功能的打印机、传真机等涉密办公自动化设备，照相、录像、录音等涉密数码设备，是国家秘密的重要载体。这些涉密载体维修时应当遵守如下保密规范:

（1）机关、单位有维修能力的应当尽可能自行维修;

（2）请人上门维修时，应当有懂技术的人员现场监督，禁止打开涉密文档，数据需要备份的应当使用本机关、本单位设备;

（3）确需送外维修的，应当到保密行政管理部门审查批准的定点单位或部门进行，并在送修前拆除信息存储部件;

（4）确需送经销商或厂商售后服务维修的，应当拆除存储部件或进行专业销密；不能拆除或销密的，应当派人现场监修，维修时需要备份的，应自带备份盘。

28.什么是涉密计算机、涉密移动存储介质、涉密信息系统?

涉密计算机是指处理涉及国家秘密信息的计算机。

涉密移动存储介质是指用于记录、存储国家秘密信息的，可以携带、移动的各种介质载体。主要包括硬盘、软盘、磁带等磁介质载体，CD、DVD 光盘等光介质载体，U 盘、存储卡等半导体介质载体。

涉密信息系统是指由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对涉密信息进行采集、加工、存储、传输等的人机系统。

29.购置用于处理涉密信息的计算机要注意什么问题？

（1）原则上应选购国产计算机。如需选购进口计算机及设备，要选购经国家有关主管部门检测认可和批准的设备产品。

（2）购买时要随机选购，不要事先预订。一旦选定，要当即购买并提货，以防被安装窃密装置。

（3）不要选购带有无线键盘、无线鼠标、无线网卡等具有无线互联功能的计算机。如果已经购买并准备用于处理涉密信息的，使用前必须拆除具有无线互联功能的硬件模块，无法拆除的，应将硬件关闭。

（4）计算机在使用前要由有关部门进行专门的安全保密技术检测，确认不存在泄密风险和安全隐患后，再用于处理涉密信息。

上述要求同样适用于购买其他涉密办公设备。

30.存放、使用涉密计算机的环境有哪些保密要求？

（1）涉密场所必须采取安全防护措施，涉密计算机存放地点必须安装防盗门窗。

（2）涉密计算机应尽可能放置在独立房间；确受条件所限，需要与非涉密计算机共用房间的，应尽可能与不连接互联网的非涉密计算机放置在同一房间；涉密计算机应当远离互联网及其它公共信息网络接口。

（3）涉密计算机与非涉密计算机不得放置在同一个金属平台上。

（4）涉密计算机主机与非涉密计算机之间的直线距离，应符合有关保密规定。

（5）涉密计算机电磁辐射必须符合国家保密标准，辐射超过限值的，必须安装防辐射干扰器。涉密计算机必须使用具有滤波功能的电源插座。

（6）应妥善摆放涉密计算机，使其在工作时他人不易看见屏幕内容；涉密计算机屏幕不得正对向门口、窗口；如果朝向门口、窗口，要采取相应的保密措施。

（7）涉密计算机不得连接公共网络。

（8）涉密计算机不得连接手机、MP3、数码相机、摄像机、iPod、扫描仪、电纸书等非涉密设备。

（9）涉密计算机（含便携式计算机）不得使用无线互联设备。具有无线互联功能的硬件模块应在使用前拆除。

（10）涉密计算机及同房间的非涉密计算机不得使用音频视频输入装置。

（11）进入使用涉密计算机的场所不得使用无线通信设备。

31.电信通信存在哪些泄密隐患？

（1）通信设备电磁泄密。通信设备，包括电话机、传真机、交换机等，工作时会产生电磁波，通信信号会被辐射到数百米之外，利用相关技术设备就可以接收通信信号并还原通信内容。

（2）网络串音泄密。相邻线路之间因各种原因产生串音。

（3）无线传输泄密。微波、短波、超短波等无线信道广泛用于通信传输，所传输的信号暴露在空中。只要有相应的接收设备，选择合适的位置，就可接收并还原通信内容。

（4）程控交换机泄密。如果计算机被植入“木马”间谍程序，程控交换机就会将通信信息发送给窃密者。

32.办公自动化设备存在哪些泄密隐患？

办公自化设备主要有计算机及其辅助设备、其它的办公设备及办公辅助设备，如打印机、扫描仪、光盘刻录机、投影仪、碎纸机、复印机、多功能一体机等。

办公自动化设备的泄密隐患主要有:

（1）存储功能的泄密隐患。打印机、复印机、扫描仪等办公自动化设备的数字化程度日益提高，这些设备在工作中，

会将处理的信息存储在内置的存储器中，当这些设备维护、修理、报废时，其他人员可通过调换或取走存储器获取所存储的信息。

（2）在办公自动化设备内安装窃密装置。有关部门技术检测发现，从国外进口的传真机、碎纸机、复印机等设备内，有的被安装了窃密装置。使用这些设备时，窃密装置会自动将处理的信息转换为电子信号发射出去，特别是新一代的多功能一体机，集复印、打印、扫描、传真功能于一体，可以直接接入互联网。当多功能一体机连接互联网时，处理的信息会自动传输到境外数字信息中心。数码复印机配置的大容量硬盘，有的容量高达上百个G，具备长期保存大量数据的功能，如果管理不当造成泄密，后果无法想象。

33.手机在使用中存在哪些泄密隐患？

（1）手机在通话状态下失泄密。手机通信是一个开放的电子通信系统，只要有相应的接收设备，就能够截获任何时间、任何地点、任何人的通话信息。

（2）手机在待机状态下失泄密。在待机状态下，手机与通信网络保持不间断的信号交换并产生电磁频谱，人们很容易利用侦察监视技术发现、识别、监视和跟踪目标，并且能对目标进行定位，从中获得有价值的情报。一些手机具有隐蔽通话功能，可以在不振铃、也没有任何显示的情况下由待机状态转变为通话状态，从而将周围的声音传递出去。

（3）手机在关机状态下泄密。手机在关机状态的泄密有两种情况，一种情况是使用者关闭手机，持有特殊仪器的人员，仍可遥控打开手机的话筒，窃听话筒有效范围内的任何谈话。另一种是，有的手机制造过程中在芯片中植入接收和发送功能。这种手机虽然没有开机或不是待机状态，但只要有电池，手机上的接收装置就能将其有效范围内的话音信息接收到，并发送出去。

（4）淘汰的旧手机导致失泄密。旧手机里的信息虽经删除，但仍可以通过特种技术恢复。淘汰的涉密手机应作为涉密载体，采用专业技术进行销密。

34.我国对互联网的保密管理有哪些基本要求？

互联网的保密管理，实行“控制源头、归口管理、分级负责、突出重点、有利发展”的原则。

（1）涉及国家秘密的计算机信息系统，不得直接或间接地与公共网络相连接，必须实行物理隔离；

（2）涉及国家秘密的信息，包括在对外交往与合作中经审查、批准与境外特定对象合法交换的国家秘密信息，不得在连接互联网的信息系统中存储、处理和传递；

（3）用户不得利用电子邮件传递、转发或抄送国家秘密信息，互联单位、接入单位对其管理的邮件服务器用户，应当明确保密要求，完善管理制度；

（4）上网信息的保密管理实行“谁上网，谁负责”的原

则，凡向联网的站点提供或发布信息，包括对网站信息的扩充或更新，须经保密审查;

（5）凡在互联网上开设电子公告系统、聊天室、网络新闻组的单位和用户，应由有关主管部门审批，明确保密要求和责任，加强监督和检查;

（6）严格限制从互联网向涉密信息系统复制数据，确需复制的，应当严格按照国家有关保密标准执行，例如，通过设立“中间机”来进行，并采取严格的技术防护措施;

（7）互联单位与接入单位，应当把保密教育作为信息技术培训的主要内容。互联单位与接入单位、接入单位与用户所签订的协议和用户守则中，应当明确规定遵守国家保密法律、不得泄露国家秘密的条款。

35.信息公开要遵守哪些保密要求？

（1）应当建立健全信息公开的保密审查机制。

（2）应坚持“谁公开、谁审查、事前审查、全面审查和依法审查”的原则。

（3）重点审查拟公开信息是否是涉及国家秘密、商业秘密、工作秘密、个人隐私等。

36.单位发布新闻要注意哪些保密问题？

（1）新闻发布会的相关材料要经保密审查，防止涉密信息公开。

（2）新闻发言人现场发布信息、介绍情况、表述意见时，

不得披露涉密信息。

37.工作人员接受采访、投寄稿件和著书立说应注意哪些保密问题?

（1）不得涉及国家秘密。

（2）不得涉及工作秘密、商业秘密和他人的隐私。

38.个人发表稿件、论文应注意哪些保密问题?

发表稿件、论文时不得涉及国家秘密内容，也不得涉及机关、单位的工作秘密、商业秘密和他人隐私。涉及本单位以及本本行业、本系统业务工作的，在投寄前，应当提交本机关、本单位有关部门进行保密审查，并经本机关、本单位领导批准。

39.为什么不能随意公开工作中的“敏感信息”?

机关、单位产生的信息中，除公开信息和国家秘密、商业秘密、个人隐私等保密信息外，还存在着大量介于两者之间又不能随意公开的信息，这些信息被称为敏感信息或工作秘密信息。敏感信息虽然不是国家秘密，但一旦泄露会给工作带来被动和的损害，并且这些信息中有许多是构成国家秘密的基础信息，此类信息的集合就属于国家秘密。正是因为敏感信息不好界定公开或者保密，容易出问题，所以需要特别注意此类信息的管理，明确敏感信息的范围和确认原则，加强敏感信息的保密审查，做好信息公开与保密的平衡。

40.组织涉密会议、活动要注意哪些保密问题?

（1）制定涉密会议、活动保密方案和保密须知，制定并落实保密工作应急处理措施。确定会议内容的密级，对于机密级以上的会议，单位保密工作部门须全程参与。

（2）明确涉密会议、活动保密工作的组织领导、明确保密工作责任人及工作职责和监督措施。

（3）选定符合保密要求的场所，对承接涉密会议、活动的服务单位规定保密责任，签订保密协议书。非涉密人员与涉密会议人员不能混住同一场所。

（4）对各种设施、设备、环境、应急保障措施等进行保密技术检查。

（5）按照会议所涉及国家秘密密级、知悉范围的要求，审定参加会议的人员。参加涉及绝密级内容的会议代表和会务工作人员，由主办部门限定到具体人，并规定不能由其他人员代替参加会议。严格执行会议签到制度。

（6）涉密会议和活动期间，禁止使用无线话筒和其他不符合国家保密标准要求的音响设备。

（7）不得携带手机进入涉密会议和活动场所或使用信号干扰器。

（8）未经批准，禁止带入具有摄录功能的设备。

（9）明确涉密载体管理要求，明确会议内容传达范围。

（10）对涉密会议和活动全过程进行保密监督检查。

41.如何管理涉密会议文件、资料和其他涉密载体?

（1）会议前，涉密文件、资料和其他涉密载体要按照涉密管理要求统一登记、编号。发给与会人员的涉密载体，要严格履行登记签收手续，注明是否会后收回等。

（2）休会期间，需要收回的涉密文件、资料和其他物品，要明确专门人员集中清理收回和妥善保管。

（3）会议结束后，注明“会后收回”的，要及时收回，不能让与会人员自行带走。

（4）允许与会人员自带的涉密文件、资料和其他物品，要明确规定使用后及时交单位保密室保管，个人不得留存，并向与会人员所在单位发出会议涉密文件、资料和其他物品清单，要求单位按照清单如数收回。

（5）明确规定涉密会议内容的传达范围。

（6）不允许与会人员自带的涉密文件、资料和其他物品，如需发给与会者单位的，应通过机要交通或机要通信部门寄发。

（7）在离开会议驻地前，要对会议驻地进行全面检查，防止文件、资料和其他物品遗留在会议驻地。

42.宣传报道涉密会议和活动有哪些保密要求？

（1）对不能公开报道的涉密内容做出明确规定。

（2）凡是拟公开报道、播放的稿件、图片、录像片、录音带等，要由会议主办单位负责人进行保密审查。

（3）统一对外宣传报道口径。为防止会议内容因宣传报

道而泄密，必要时应统一组织新闻发布会。

（4）会议组织者在会议开始前要对与会记者进行保密教育，明确提出会议新闻报道的保密要求。

43.涉密会议与会人员应遵守哪些保密规定？

（1）会议期间需与会外进行通信联系的，不得在通信联系中涉及会议内容;

（2）会议明确规定不准记录和录音的，不得擅自记录、录音；不准摘录、摘抄秘密文件、资料内容，不得擅自复印会议文件、资料;

（3）允许由会议代表自己带回单位的文件，回单位后应立即送交单位文件保管部门登记保存，不得由个人保存会议文件。携带秘密文件、资料返回单位途中，不得办理无关事项，以防文件丢失被盗。

（4）会议工作人员要切实履行职责，加强会议的保密管理，将会议文件、资料发给会议代表时要登记，需要集中管理的文件，会议休会期间要及时收回。会议结束时，应将涉密会议文件统一收回，允许与会代表带回的，需要发给有关单位的，应按携带国家秘密载体的有关规定执行。

44.有境外人员参加的学术交流与合作活动应注意哪些保密问题？

（1）在有境外人员参加的学术交流与合作活动中，要严格执行保密规章制度和外事工作规定，对在教学、科研、生

产中产生的国家秘密事项，未经审批，不得对外交流。

（2）对来校讲学或访问的境外人员，涉及到国家秘密事项时，交流单位应拟定专项保密工作方案，划定参观范围，统一介绍口径。

45.如何做好试卷保密室的管理工作？

国家教育考试保密室是存放处于保密状态的试题、试题答案和评分参考的要害部位，必须由专人负责管理。

（1）国家教育考试试卷保密室必须设在楼房的第二层（含第二层）以上，房间必须是钢混（或砖混）结构的套间，具备防盗、防火、防潮、防鼠功能，配备铁门、铁窗、铁柜和报警设备。套间的外屋供值班巡逻人员使用，配备专用电话，内屋用于存放试卷，内外屋之间须安装防盗门，保证外屋可观察到内屋情况。

（2）各学科（项目）的试题及其它相关材料须放入和归档在不同保密柜内，保密柜钥匙及密码由学科（项目）负责人和保密员分别保管，两人同时在场方可开启。不得转交他人或相互替代保管钥匙及密码。

（3）工作人员进入保密室领取保密材料，须经有关领导同意，并严格履行登记手续。

（4）保密室内配备消防设备，注意防火防潮，严禁吸咽。

（5）保密室使用期间的监控资料在考试结束后由教育考试机构至少保存半年。

46.发现国家秘密可能泄露或已经泄露应采取什么措施？

（1）拾得他人遗失的国家秘密文件、资料等，及时送交本单位保密工作部门，当地保密行政管理部门，或当地公安机关；

（2）发现他人出售或收购国家秘密文件、资料等，立即进行制止，并报告当地保密行政管理部门或学校保密工作部门；

（3）发现他人在不适当的场合传播、谈论国家秘密时，立即劝阻；

（4）发现盗窃国家秘密文件、资料时，应将行为人连同物证一并交由当地公安机关，或向当地公安机关及时举报。

（5）个人发生泄密事件，应立即将事件的具体情节如实报告学校保密工作部门。需由公安机关立案的，同时向案发地点的公安机关报案；立即采取补救措施，避免或减轻损害后果。

47.造成泄露国家秘密的主要原因有哪些？

（1）有法不依，有章不循；

（2）思想麻痹，保密观念淡薄；

（3）缺乏保密知识和技能；

（4）保密管理措施不到位；

（5）保密防范和保密检查技术落后或缺乏。

48.个人违反保密法律法规行为有哪些种类？

保密法第四十八条规定的个人违反保密法律法规行为共有12种类型。个人有其中任何一中行为，无论是否造成泄密，都要依法给予处分；构成泄密犯罪的，要依法追究刑事责任。这些行为分别是：

（1）非法获取、持有国家秘密载体的；

（2）买卖、转送或者私自销毁国家秘密载体的；

（3）通过普通邮政、快递等无保密措施的渠道传递国家秘密载体的；

（4）邮寄、托运国家秘密载体出境，或者未经有关主管部门批准，携带、传递国家秘密载体出境的；

（5）非法复制、记录、存储国家秘密的；

（6）在私人交往和通信中涉及国家秘密的；

（7）在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递国家秘密的；

（8）将涉密计算机、涉密存储设备接入互联网及其他公共信息网络的；

（9）在未采取防护措施的情况下，在涉密信息系统与互联网及其他公共信息网络之间进行信息交换的；

（10）使用非涉密计算机、非涉密存储设备存储、处理国家秘密信息的；

（11）擅自卸载、修改涉密信息系统的安全技术程序、

管理程序的;

（12）将未经安全技术处理的退出使用的涉密计算机、涉密存储设备赠送、出售、丢弃或者改作其他用途的。

49.为什么在保密检查工作中要特别强调责任追究?

责任追究是检查工作的重要内容。保密检查的目的不是处理人，但不能回避处理人。对于相关人员的处理，要根据违规情节、后果和造成的影响等，区分情况，严格责任追究，借以惩前毖后、治病救人。

责任认定和追究的标准：一是确定是否泄密；二是认定泄密行为；三是确定责任人要承担的政纪、党纪责任；四是如果达到最高人民检察院立案标准的，要向检察院进行案件移交。各单位应按照上述标准，认真进行责任追究，不能重责轻罚，轻责不罚。

50.《行政机关公务员处分条例》规定公务员泄密将会受到何种处分?

《行政机关公务员处分条例》第二十六条规定：泄露国家秘密、工作秘密，或泄露因履行职责掌握的商业秘密、个人隐私，造成不良后果的，经予警告、记过或记大过处分；情节较重的，给予降级或撤职处分；情节严重的，给予开除处分。

51.刑法对涉及国家秘密的犯罪行为有什么样的规定?

《中华人民共和国刑法》第三百九十八条规定：国家机

关工作人员违反保守国家秘密法的规定，故意或过失泄露国家秘密，情节严重的，处三年以下有期徒刑或拘役；情节特别严重的，处三年以上七年以下有期徒刑。非国家机关工作人员犯前款罪的，依照前款的规定酌情处罚。

52.泄密犯罪的判定标准是什么？

《最高人民检察院关于渎职侵权犯罪案件立案标准的规定》，规定了国家机关工作人员或者非国家机关工作人员违反保密法、泄露国家秘密，情节严重，涉嫌犯罪的立案标准。

故意泄露国家秘密是指故意使国家秘密被不应知悉者知悉，或故意使国家秘密超出了限定的接触范围，情节严重的行为。

故意泄露国家秘密涉嫌下列情形之一的，应予立案：

1.泄露绝密级国家秘密1项（件）以上的；

2.泄露机密级国家秘密2项（件）以上的；

3.泄露秘密级国家秘密3项（件）以上的；

4.向非境外机构、组织、人员泄露国家秘密，造成或者可能造成危害社会稳定、经济发展、国防安全或者其他严重危害后果的；

5.通过口头、书面或者网络等方式向公众散布、传播国家秘密的；

6.利用职权指使或者强迫他人违反国家保守秘密法的规定泄露国家秘密的；

7. 以牟取私利为目的泄露国家秘密的;

8. 其他情节严重的情形。

过失泄露国家秘密是指因过失泄露国家秘密，或遗失国家秘密载体，致使国家秘密被不应知悉者知悉或超出了限定的接触范围，情节严重的行为。

过失泄露国家秘密案（第三百九十八条）

过失泄露国家秘密涉嫌下列情形之一的，应予立案:

1. 泄露绝密级国家秘密 1 项（件）以上的;

2. 泄露机密级国家秘密 3 项（件）以上的;

3. 泄露秘密级国家秘密 4 项（件）以上的;

4. 违反保密规定，将涉及国家秘密的计算机或者计算机信息系统与互联网相连接，泄露国家秘密的;

5. 泄露国家秘密或者遗失国家秘密载体，隐瞒不报、不如实提供有关情况或者不采取补救措施的;

6. 其他情节严重的情形。