保密资格认定考试题库

**保密办**

**目 录**

[**保密基本知识试题** 3](#_Toc491424515)

[一、填空题（共41题） 3](#_Toc491424516)

[二、判断题（共180题） 7](#_Toc491424517)

[三．单项选择题（共53题） 23](#_Toc491424518)

[四、论述题（共3题） 39](#_Toc491424519)

[五、案例分析题（共4题） 40](#_Toc491424520)

# 保密基本知识试题

（共281题）

# 一、填空题（共41题）

1．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．保守国家秘密的工作，实行**积极防范**、**突出重点**、**依法管理**的方针。

3．加强和改进保密工作的总体要求的基本原则，应坚持**党管保密**、**依法管理**、综合防范、创新驱动。

4．新修订《中华人民共和国保守国家秘密法》自**2010**年10月1日起施行。

5．**中央保密委员会**是党中央统一领导党政军保密工作的领导机构。

6．**国家保密行政管理部门**主管全国的保密工作。

7．**绝密**级国家秘密是最重要的国家秘密，泄密会使国家安全和利益遭受特别严重的损害。

8．各级国家机关、单位对所产生的国家秘密事项，应当按照**国家秘密**及其**密级具体范围**的规定确定密级。

9.定密责任人在职权范围内承担有关国家秘密的**确定**、**变更**和**解除**工作。

10.摘录、引用密件中属于国家秘密的内容，应当以其中**最高密级**和**最长保密期限**作出标识。

11.保守国家秘密是我国公民的一项**基本义务**。

12．涉密人员是指在工作中接触、知悉、管理和掌握**国家秘密**的工作人员。

13.涉密人员上岗前要经过**保密审查**和**培训**。

14.涉密人员脱离涉密岗位必须实行脱密期管理，其中核心涉密人员脱密期为**3**年，重要涉密人员为**2**年，一般涉密人员为**1**年。

15.从事弹道导弹、核武器、军用核动力、核潜艇等装备的核心技术专家脱密期不少于**5**年。

16.涉密人员脱离涉密岗位前，必须清退管理、使用的全部国家秘密载体并签订**保密承诺书**。

17.国家秘密载体保密期限需要延长的，由**原确定密级**和**保密期限**的机关、单位或者上级机关决定。

18.禁止在普通手机通话、发送短信息、社交媒体通信过程中，通过明语或暗语谈论、传递**国家秘密**。

19.不得在连接互联网的计算机上存储、**处理**、**传递**国家秘密信息。

20．不准通过普通邮政、快递等无保密措施的方式传递属于国家秘密的**文件**、**资料**和**其他物品**。

21.涉密人员因公携带**国家秘密载体**外出，应当符合国家保密规定，并采取可靠的保密措施。

22.销毁国家秘密载体，应当采用**物理**或者**化学**的方法彻底销毁，确保信息无法还原。

23.不得在涉密计算机和非涉密计算机上**交叉**使用移动存储介质。

24.**不得**使用普通传真机和一体机传输涉密信息。

25.涉密信息系统不得直接或者间接连接国际互联网，必须实行**物理隔离**。

26.涉密计算机的密级应按照存储和**处理**信息的**最高密级**确定。

27.计算机一旦存储和处理过涉密信息，就应当确定为**涉密计算机**，并粘贴相关密级标识。

28.未经审批的涉密信息系统，在试运行期间不能存储和处理**涉密信息**。

29.未经本单位**信息化**管理部门批准，不得自行对涉密计算机进行格式化并重新操作系统。

30.涉密办公自动化设备现场维修时，应由有关人员全程**旁站**陪同。

31.存储在涉密计算机或者存储介质中的电子文件，只要内容涉密，就应当**标明密级**。

32．机密级涉密计算机的系统登录如采用用户名加口令的方式，则系统口令更换工作不得长于**一周**。

33.绝密级计算机采用**一次性**口令或者**生理特征**身份鉴别措施。

34．符合国家保密要求的涉密计算机屏幕保护程序启动时间要求是不超过**十分钟**。

35.高密级的涉密移动存储介质**禁止**在**低密级**的涉密计算机上使用。

36.携带涉密计算机和存储介质外出应当履行**审批手续**。

37．携带涉密计算机和存储介质外出，带回时应当进行**保密检查**。

38.武器装备科研生产保密资格单位对外发布信息应当进行**保密审查和审批**。

39.机关、单位日常工作中**产生**、**传递**、**使用**和**管理**绝密级或较多机密级、秘密级国家秘密的内设机构称为保密要害部门。

40.保密管理要与涉密科研管理同计划、同部署、同检查、同**总结**、同**奖惩**。

41.刑法第一百一十一条规定，为境外的机构、组织、人员窃取、刺探、收买、非法提供国家秘密或者情报的、处**五年**以上**十年**以下有期徒刑。

# 二、判断题（共180题）

1．国家秘密是关系国家安全的利益，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。（√）

2．一切国家机关、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。（√）

3.单位可以把知悉国家秘密作为一种行政级别待遇，按照行政级别确定国家秘密知悉范围。（×）

4.国家秘密知悉范围内的机关、单位，其有关工作人员不在知悉范围内，但因工作需要知悉国家秘密的，应当经单位负责人批准。（√）

5.国家秘密知悉范围之外的人员，因工作需要确需知悉国家秘密的，应当经本单位负责人同意。（×）

6.单位负责人为本单位的定密责任人，对定密工作负总责。（√）

7.单位对所产生的国家秘密事项，应当按照保密事项范围的规定确定密级，同时确定保密期限和知悉范围。（√）

8.国家秘密变更后，原定密机关、单位应及时在原国家秘密标志附近重新做出国家秘密标志，并书面通知知悉范围内的机关、单位和人员。（√）

9.单位对已定密事项是否属于国家秘密或者属于何种密级有不同意见的，不得向原定密机关、单位提出异议。（×）

10.涉密岗位是指在日常工作中产生、经管或者经常接触、知悉国家秘密事项的岗位。（√）

11.涉密人员在非涉密出版物上发表文章、著作，不得涉及国家秘密。（√）

12.涉密人员禁止向境外期刊等新闻出版机构投寄稿件。（×）

13.涉密人员发表文章、著作凡涉及本单位、本系统业务工作的，应当事先经本单位或上级机关、单位保密审查、审批。（√）

14.涉密载体是指以文字、数据、符号、图形、图像、声音等方式记载国家秘密信息的纸介质、光介质、电磁介质等各类物品。（√）

15.制作涉密载体应当在符合保密要求的场所进行。（√）

16.涉密载体复制件应当加盖复制机关、单位戳记，并视同原件管理。（√）

17.绝密级涉密载体一般不得复制、摘录、引用、汇编，确有工作需要的，必须征得原定密机关、单位或者其上级机关、单位同意。（√）

18.涉密载体可以通过普通邮政、快递等渠道传递。（×）

19.对涉密科研项目文件资料，包括过程文件、电子文档等涉密载体，要进行全面清理、完整归档，个人应根据工作需要自行妥善保管或者销毁。（×）

20.阅读和使用涉密载体应当在符合保密要求的办公场所进行。（√）

21.绝密级涉密载体应当在符合国家保密标准的设施、设备中保存，并指定专人管理。（√）

22.机构撤并时，原机构的涉密载体移交给制发单位时，制发单位不收回的可自行处理。（×）

23.保密要害部门、部位办公场所在采取必要的保密措施后，仍需要对进入的工勤人员严格监督管理。（√）

24.专用手机可以随意带入保密要害部门、部位。（×）

25.未经批准，不得将带有录音、录像、拍照、信息存储功能的设备带入保密要害部门、部位。（√）

26.涉密会议、活动应当按照“谁承办、谁负责”的原则进行管理。（×）

27.重要涉密会议、重大涉密活动组织举办者应在必要时，请保密工作机构对保密工作进行监督和指导，并提供必要的安全保密技术服务保障。（√）

28．保密审查主要是对拟公开发布的信息是否涉及国家秘密进行审查，不需要对是否涉及工作秘密、商业秘密、个人隐私等进行甄别鉴定。（×）

29.在涉密科研项目结题阶段，要加强成果验收、奖项申报、专利申请等工作的保密管理。（√）

30.经严格审批，涉及敏感项目（如军工技术、军贸等）的驻外机构和企业可以雇佣外籍人员。（√）

31.任何组织和个人不得擅自对外提供国家秘密资料。（√）

32.党的纪律处分条例规定，泄露、扩散或者窃取党组织尚未公开事项或者其他应该保密的内容的，情节较重的，给予开除党籍处分。（×）

33.“业务工作谁主管，保密工作谁负责”是保密工作的重要原则。（√）

34.国家秘密的密级分为绝密、机密、秘密三级。（√）

35.绝密级国家秘密是最重要的国家秘密，泄露会使国家安全和利益遭受特别严重的损害。（√）

36.机密级国家秘密是重要的国家秘密，泄露会使国家安全和利益遭受严重的损害。（√）

37. 秘密级国家秘密是一般的国家秘密，泄露会使国家安全和利益遭受损害。（√）

38.保守国家秘密是我国公民的一项基本义务。（√）

39.涉密岗位根据涉及国家秘密的程度分为核心、重要和一般三个等级。（√）

40.承担涉密项目研究、建设、管理任务的岗位应确定为重要涉密岗位。（×）

41.核心涉密岗位是指年产生、处理6件（项）绝密级国家秘密事项的工作岗位。（×）

42.国防科技工业涉密人员是指取得武器装备科研生产单位保密资格的企业事业单位中，在涉密岗位工作的人员。（√）

43．涉密人员应当具有中华人员共和国国籍。（√）

44．涉密人员上岗前要经过保密审查，并接受保密教育培训。（√）

45.经审查合格，进入涉密岗位的人员须按照规定签订保密承诺书，明确享有的权利和应当承诺履行的保密义务。（√）

46.单位应当定期对涉密人员进行复审，核心涉密人员每年复审一次；重要涉密人员每2年复审一次，一般涉密人员每3年复审一次。（×）

47.涉密人员在岗期间，保密工作机构应当会同人事部门、涉密人员所在部门有针对性地对其进行保密教育和检查、考核，对严重违反保密规定的应当及时调离涉密岗位。（√）

48.一般涉密人员与境外人员通婚或者接受境外机构、组织及非亲属人员资助的，事后向单位报告即可。（×）

49.涉密人员本人或其直系亲属拟申请获得境外永久居留权、长期居留权或外国国籍的应当向单位报告。（√）

50.涉密人员离岗后，应当遵守脱密期限规定，核心涉密人员脱密期3年，重要涉密人员脱密期2年，一般涉密人员脱密期1年。（√）

51.涉密人员脱离涉密岗位3年内不得在境外驻华机构或者外商独资企业工作。（×）

52.涉密人员脱密期内不得在境外驻华机构或者外商独资企业工作，但可以为境外组织或者人员提供劳务咨询或者其他服务。（×）

53.涉密人员脱密期内不得在国内中外合资企业工作。（×）

54.涉密人员因私出境应经所在单位同意，还应按照有关规定办理保密审批手续。（√）

55.涉密人员因公出国（境）的，应该按照行政隶属关系、干部（人事）管理权限和外事管理权限履行审批程序。（√）

56.涉密人员脱密期内未经批准可以因私出境。（×）

57．涉密人员离开涉密岗位后，就不再对本人在原涉密岗位上知悉的国家秘密事项承担保密义务。（×）

58.涉密人员脱密期满后，对所知悉的国家秘密同样承担保密责任和义务。（√）

59.出境后可能对国家安全造成危害或者对国家利益造成重大损失的涉密人员，不得批准出境。（√）

60.涉密人员出国（境）期间受到境外机构、组织和人员的礼品馈赠不须向单位报告。（×）

61.涉密单位应当对聘用的保安和临时工进行保密教育培训。（√）

62.在私人交往和通信中不得涉及或泄漏国家秘密。（√）

63.配偶、子女和本人都是涉密人员，互相谈论涉密事项没有关系。（×）

64.各级国家机关、单位对所产生的国家秘密事项，应当按照国家秘密及其密级具体范围的规定及时确定密级。（√）

65.定密工作时指对机关、单位业务活动中所产生的国家秘密事项及时、准确确定其密级、保密期限、知悉范围，并对国家秘密载体做出标志，及时通知应当知悉的机关、单位和人员，并按照规定进行全过程管理的活动。（√）

66.项目定密是指军工单位对从事的武器装备科研生产项目依次进行确定是否涉密以及是何种密级的工作。（√）

67.国家秘密事项范围定得越宽，密级越高，越有利于国家秘密的安全。（×）

68.国家秘密的标识为★，★前标密级，★后标保密期限。（√）

69.纸介质国家秘密载体，其密级和保密期限应在首页（或者封面）标明。（√）

70.涉及国家秘密的地图、图纸、图表在其标题之后或者下方标明密级和保密期限。（√）

71.文件、资料汇编中有密件的，应当对各独立密件的密级和保密期限做出国家秘密标志，并在封面或者首页以其中的最低密级和最短保密期限做出国家秘密标志。（×）

72.摘录、引用密件中属于国家秘密的内容，应当以其中最高密级和最长保密期限做出国家秘密标志。（√）

73.密件的密级和保密期限变更后，应当在原国家秘密标志位置的附近做出新标志，原标志以明显方式废除。（√）

74.在保密期限内解密的密件，应当以能够明显识别的方式标明解密的字样。（√）

75.密品应当在壳体及封面、外包装的显著位置标注国家秘密标志，无法在物品本身标注或者不宜做出国家秘密标志的，应当在密品使用维护说明书中注明密级、保密期限和知悉范围，并提出相应的保密措施。（√）

76.保密工作机构应当组织相关涉密业务部门研究制定本单位《国家秘密事项范围细目》。（×）

77.国家秘密事项的密级和保密期限一经确定，就不能改变。（×）

78.国家秘密的保密期限，除有特殊规定外，绝密级事项不超过20年，机密级事项不超过10年，秘密级事项不超过5年。（×）

79.保密期限需要缩短的，由原确定密级和保密期限的机关、单位或者上级机关决定。（√）

80.保密期限需要延长的，由原确定密级和保密期限的机关、单位或者上级机关决定。（√）

81.单位领导要求继续保密的事项，在领导要求的期限内不得解密。（×）

82.已解密的事项可以对全社会公开。（×）

83.企业的技术成果被确定为国家秘密后，在保密期限内不得擅自解密和对外提供。（√）

84.各级机关和涉密单位编发的内部工作简报都应定为国家秘密。（×）

85.密级的变更包括降低密级或者提高密级。（√）

86.制作国家秘密载体应当按照有关规定标明密级和保密期限，注明发放范围及制作数量，并编排序号。（√）

87.纸介质国家秘密载体应当在本机关、本单位内部文印室或者交保密行政管理部门审查批准的单位制作。（√）

88.国家秘密载体印制资质单位，使用电子方法排版印制或者打印国家秘密载体的，复制完成后其磁盘内的载体内容可以自行删除。（×）

89.收发国家秘密载体，应当履行清点、登记、编号、签收等手续。（√）

90.传递国家秘密载体应当密封包装，装载国家秘密载体的信封或者袋牌上应当标明密级、编号和收发件单位名称。（√）

91.传递国家秘密载体应当通过机要交通、机要通信或者指派专人传递，不得通过普通邮资渠道传递。（√）

92.国家秘密文件、资料可以通过普通邮政“特快专递”传送。（×）

93.不准通过普通邮政、快递传递属于国家秘密的文件、资料和其他物品。（√）

94.记录涉密内容应当使用保密本。（√）

95.单位收到绝密级载体后应当按照规定的范围组织阅读和使用，并对接触和知悉绝密级国家秘密的人员做出文字记载。（√）

96.单位内部复制国家秘密载体应当履行审批手续，复制机密级以上国家秘密载体须经部门或者单位领导批准，加盖复制戳记，视同原件管理，并进行登记。（√）

97.因公出差，且两人同行，可以携带密件到购物、餐饮、娱乐等公共场所。（×）

98.阅读、承办、使用密件，应当在符合保密要求的办公场所进行，严禁擅自携带外出。（√）

99.传阅秘密公文的人员很多，逐人逐份登记很麻烦，有时可以不登记，收回时自己在文件登记本上画个勾就可以。（×）

100.某协作单位工作人员因工作需要借阅协作范围内的绝密级图纸，该单位接待人员电话请示有关领导同意后，就可以为其办理借阅手续。（×）

101.某领导携带涉密U盘参加行业工作会，会议要求报书面材料，因时间紧急，该领导就使用涉密U盘连接营业性场所计算机打印机密级汇报材料，打印完成后作删除处理尚可。（×）

102.某单位进行文件汇编工作时，少量摘抄某涉密文件，经办人员认为该文件汇编册不涉密，可不标注密级。（×）

103.涉密人员参加会议带回的秘密文件、资料，应交本单位文秘部门或档案部门登记、管理。（√）

104.阅读和使用国家秘密载体应当办理登记、签收手续，管理人员应当随时掌握国家秘密载体的去向。（√）

105.传达国家秘密事项时，凡不准纪录、录音、录像的，应当事先申明。（√）

106.不准在普通手机通话中涉及国家秘密。（√）

107.普通手机处于关机状态下，不存在涉密隐患。（×）

108.不得使用普通手机短信传送国家秘密信息。（√）

109.不得使用普通手机中微信、QQ等社交软件谈论、传递国家秘密。（√）

110.不得将普通手机与涉密信息系统连接。（√）

111.不得在保密要害部门、部位使用普通手机。（√）

112.个人因公外出，携带国家秘密载体应当采取严格的保密措施。（√）

113.因工作需要随身携带密件、密品外出时，不得进入购物、餐饮娱乐等公共场所。（√）

114.领导干部为了工作方便，可以将密件带回家中处理。（×）

115.工作人员离开办公场所，应当将国家秘密载体存放在保密设备里。（√）

116.涉密人员在办公场所阅读、承办、使用密件过程中，需要临时离开，无须将密件存放到保密柜中。（×）

117.绝密级秘密载体必须放置在安全可靠的密码保险柜中保存，并有专人管理。（√）

118.销毁国家秘密载体，应当采用物理或者化学的方法彻底销毁，确保信息无法还原。（√）

119.在不解密的情况下，机密级、秘密级国家秘密技术成果可以申请公开专利或者由保密专利转为公开专利。（×）

120.公开报道、出版或者个人接受境外媒体采访涉及国家政治、经济、外交、科技、军事方面内容的，不用事先经过审批。（×）

121.未经批准，严禁公开报道尚属国家秘密的武器装备技术性能指标、科研生产能力、结构布局、产量、发展规划等涉密内容。（√）

122.机关、单位每年应当定期对当年所存国家秘密载体进行清查、核对，发现问题的应当及时向保密工作机构报告。（√）

123.销毁纸介质国家秘密载体应当采用焚毁、化浆等方法处理，使用碎纸机销毁的应当使用符合保密要求的碎纸机，送造纸厂销毁的应当送保密行政管理部门制定的造纸厂销毁，并由销毁单位两人以上押运、监销。（√）

124.U盘上的涉密信息，只要执行删除程序就不可恢复。（×）

125.国家秘密载体不得作为废品出售。（√）

126.已拆除硬盘的涉密计算机，可以赠送给希望小学使用。（×）

127.密品是指直接含有国家秘密信息，或者通过观察、测试、分析等手段能够获取所承载的国家秘密信息的设备和产品。（√）

128.密品的研制、生产、保存和使用单位应当对密品的密级、保密期限、知悉范围、保密要点的内容进行登记，各环节的交接应当登记签收。（√）

129.保密要害部门、部位由各机关、单位确定，报国家或者省、自治区、直辖市保密行政管理部门确认或者备案。（√）

130.保密要害部门、部位应当具备完善可靠的人防、技防、物防措施。（√）

131.涉密场所使用的进口设备和产品应当进行安全技术检测。（√）

132.保密要害部门、部位禁止使用无绳电话和普通手机，未经批准不得带入有录音、录像、拍照、信息存储功能的设备。（√）

133.普通手机关机后可以带入要害部门、部位。（×）

134.涉密电子文档应当标注国家秘密标志，国家秘密标志不能与正文分离。（√）

135.不得在涉密计算机和非涉密计算机上交叉使用移动存储介质。（√）

136.不得使用未采取密码保护的通信系统传输涉密信息。（√）

137.不得将自己使用的涉密计算机和移动存储介质擅自交给他人使用。（√）

138.无线电话不保密，军线电话是保密的。（×）

139．数字移动电话传输的是数字信号，因此是保密的。（×）

140.在保密通信技术比较落后的情况下。允许在单位内部无保密措施的电话中传递国家秘密。（×）

141.电磁信号泄露泄密的方式主要是辐射和传导两种方式。（√）

142.涉密存储介质经文件删除并格式化处理后，仍不得作为非密介质使用。（√）

143.利用现代通信及计算机网络远程传输国家秘密信息，必须采用密码保护措施，并禁止密明混用。（√）

144.涉密信息使用的加密措施应当经过国家密码主管部门批准，在任何地方都可以使用。（×）

145.涉密信息使用的加密措施须经国家密码主管部门批准，并与所保护的信息密级等级相符合。（√）

146.绝密级信息必须加密存储。（√）

147.涉密计算机不得安装使用无线键盘、无线鼠标、蓝牙、红外设备和无线网卡。（√）

148.涉密便携式计算机应当拆除具有无线联网功能的硬件模块。（√）

149.无线联网功能硬件模块无法拆除的计算机禁止作为涉密计算机和信息系统的服务器、用户终端使用。（√）

150.涉密计算机不得安装来历不明的软件和随意拷贝他人文件。（√）

151.涉密计算机和移动存储介质应在保密行政管理部门设立的销毁工作机构或者保密行政管理部门制定的单位销毁。（√）

152.在涉密场所使用的与国家互联网或者其他公共网络连接的计算机不得安装视频、音频等输入装置。（√）

153.不得在连接国际互联网的计算机上存储和处理涉密信息。（√）

154.涉密计算机不得与国际互联网或者其他公共信息网络相连接。（√）

155.确因工作需要，可以使用私人计算机处理涉密文件，但要与国际互联网断开连接，待处理完涉密信息后可与互联网连接。（×）

156.任何单位和个人均不得在国际互联网网络主页、电子公告栏、聊天室、网络新闻组、微博上发布、谈论、张贴、传播国家秘密信息。（√）

157.为节约开支，可以将淘汰的涉密计算机交本单位非涉密部门使用。（×）

158.涉密信息系统不得直接或者间接连接国际互联网，必须实行物理隔离。（√）

159.国家秘密信息不得在与国际互联网连接的计算机和信息系统中存储、处理、传递，但可以在单位内部非涉密单机上存储、处理、传递。（×）

160.召开涉及国家秘密的会议，使用无线扩音、通信设备不能把音量开得太大。（×）

161.对参与国家秘密技术研制的科技人员，有关单位不得因其成果不宜公开发表、交流、推广而影响其评奖、表彰和职称的评定。（√）

162.在对外经济合作中，凡涉及国家秘密的资料未经保密审查和批准，一律不得对外提供。（√）

163.在对外交往与合作中急需提供国家秘密事项的，可以先提供，后补办手续。（×）

164.对外交流中除交流内容与谈判口径外，所提供资料和产品应当经过保密审查。（×）

165.对外公开新闻宣传时，单位代号、真实名称、掩护名称不得同时使用。（√）

166.接收媒体采访，一般不得涉及国家秘密，特殊情况需要涉及国家秘密的，应当办理审批手续。（√）

167.音像制品涉及国家秘密的，应按照涉密资料保管。（√）

168.保密教育和保密提醒是科技交流必须坚持的制度。（√）

169.对外科技交流活动不得涉及国家秘密，确需涉及国家秘密的应当履行审批手续。（√）

170.未经批准，任何单位、部门或者个人均不得到保密要害部门、部位进行采访、照相、录像等活动。（√）

171.使国家秘密被不应知悉者知悉的，属于泄露国家秘密行为。（√）

172.发现国家秘密载体在使用中下落不明，应当在8小时内向本单位保密工作机构报告，向上级报告不应超过24小时。（√）

173.国家秘密载体下落不明，自发现之日起，绝密级载体10日内、机密级、秘密载体60日内查无结果的，按照泄密事件处理。（√）

174.报告泄密事件应当包括被泄露国家秘密的内容、密级、数量及其载体形式、事件发现经过、责任人基本情况、发生的时间、地点及经过。（√）

175.将涉及国家秘密的计算机和计算机信息系统与国际互联网连接，泄露国家秘密的，应立为泄密案件。（√）

176.过失泄露一项绝密级国家秘密的可不予立案，在单位内部处理。（×）

177.违反《中华人民共和国保守国家秘密法》规定，泄露国家秘密的，不够刑事处罚的，可以酌情给予行政处分。（√）

178.以窃取、刺探、收买的方法，非法获取国家秘密的，都应当依据《刑法》追究其刑事责任。（√）

179.发生涉密事件的机关、单位不及时上报或者隐匿不报的，视情节和造成的后果追究有关人员或者领导人的责任。（√）

180.未经相应工作部门批准，不得向境外邮寄密品、密件或者随身携带密品、密件出境。（√）

# 三．单项选择题（共53题）

1.保守国家秘密的工作实行积极防范、突出重点、依法管理的方针，（C）

A.确保国家秘密安全

B.便利各项工作的开展

C.既确保国家秘密安全，又便利信息资源合理利用

D.实事求是

2.（D）主管全国的保密工作。

A.国家安全部门

B.公安部门

C.中央保密委员会

D.国家保密行政管理部门

3.一份文件为秘密级，保密期限是10年，标志形式应当是（C）。

A.秘密10年

B.秘密★

C.秘密★10年

D.秘密●10年

4.重要涉密部门的人员选配，应当坚持（B）的原则，并定期进行考核，不适合的应及时调整。

A.谁选配谁负责

B.先审后用

C.先选后训

D.边审边用

5.涉密人员离岗、离职前，应当将所保管和使用的国家秘密载体全部清退，并（C）

A.登记销毁

B.订卷归档

C.办理移交手续

D.不一定办理移交手续

6.书面形式的涉密载体，应在封面或者首页做出国家秘密标志，汇编涉密文件、资料或摘录、引用属于国家秘密内容的应按照其中（A）标注。

A.最高密级和最长保密期限

B.最高密级和最短保密期限

C.最低密级和最长保密期限

D.最低密级和最短保密期限

7.定密责任人在职权范围内承担有关国家秘密的（D）工作。

A.确定

B.变更

C.解除

D.以上都正确

8.国家秘密确定的基本程序为：在国家秘密产生的同时，由（C）对照保密事项范围提出定密的具体意见，再由定密责任人审核批准。

A.单位领导

B.定密责任人

C.承办人

D.上级机关

9.一般情况下，核心涉密人员脱密期为（A）

A.3年

B.2年

C.1年

D.不超过6个月

10.一般情况下，重要涉密人员脱密期为（B）

A.3年

B.2年

C.1年

D.不超过6个月

11.一般情况下，一般涉密人员脱密期为（C）

A.3年

B.2年

C.1年

D.不超过6个月

12.涉密人员离开原涉密单位，调入其他国家机关和涉密单位的，脱密期管理由（D）负责。

A.原涉密单位

B.调入单位上级管理部门

C.原单位上级管理部门

D.调入单位

13.下列关于涉密载体管理说法错误的是（D）

A.将涉密载体保存在安全保密的场所和部位，并配备必要的保密措施、设备

B.定期清查、核对

C.离开办公场所，将涉密载体存放在保密设备中

D.涉密载体丢失后经查找回的无须报告

14.复制属于国家秘密的文件、资料或者摘录、引用、汇编属于国家秘密内容形成的国家秘密载体，（A）原件的密级、保密期限和知悉范围。

A.不得擅自改变

B.可以根据情况改变

C.应降低

D.应提高

15.印刷、复印等行业在复制国家秘密载体方面，接受县级以上各级政府（C）的指导和监督。

A.公安部门

B.工商部门

C.保密行政管理部门

D.国防科技管理部门

16.印刷、复印等行业的定点复制单位，在复制国家秘密载体时，应当尽量缩短复制时间，对不能当即取走，确需过夜的，须放在安全可靠的（C）内，并派人值班看守。

A.车间

B.仓库

C.文件柜

D.办公室

17.收发国家秘密载体，应当履行（A）手续。

A.清点、登记、编号、签收等

B.交接

C.签字

D.移交

18.下列关于涉密载体销毁管理错误的是（B）

A.自行销毁少量涉密载体的应当使用符合国家保密标准的销毁设备和方法

B.涉密载体销毁的登记、审批记录无须长期保存

C.机关、单位送销涉密载体应当分类封装、安全运送、并派专人现场监销

D.销毁涉密载体应当履行清点、登记、审批手续，并送交保密行政管理部门设立的销毁工作机构或指定的单位销毁

19.下列不符合保密要害部门、部位人员保密管理要求的是（C）

A.上岗前保密审查

B.定期进行在岗保密教育培训

C.未经批准私自出国

D.签订保密承诺书

20.下列关于保密要害部门、部位的说法错误的是（C）

A.需按国家保密标准配备技术防护设备

B.应使用经过保密技术检测的设备和产品

C.在不谈论国家秘密的情况下可使用普通手机

D.经机关、单位保密委员会（领导小组）批准，并登记备案，可以将专用手机带入保密要害部位

21.任何情况下，不得向境外传递（C）国家秘密载体。

A.机密级

B.秘密级

C.绝密级

D.内部

22.变更密级或者解密，应由（B）

A.密件使用单位决定

B.原定密机关、单位决定，也可以由其上级机关决定

C.国家保密行政管理部门指定的单位决定

D.定密责任人直接确定

23.传递绝密级秘密载体，（C）

A.只能通过机要交通递送

B.只能通过机要通信递送

C.必须通过机要交通、机要通信或者派人直接递送

D.只能通过可靠快递

24.领导干部阅办秘密文件、资料和办理其他属于国家秘密的事项，应在（A）内进行。

A.办公场所

B.家中或办公场所

C.咖啡馆

D.图书馆

25.销毁国家秘密载体，应当送（C）设立的销毁工作机构或指定的单位销毁，并由销毁单位派专人押运监销。

A.公安部门

B.上级机关

C.保密行政管理部门

D.造纸厂

26.汇编涉密文件、资料或摘录、引用属于国家秘密内容的应按照其中（A）密级和（）保密期限标注国家秘密标志。

A.最高 最长

B.最高 最短

C.最低 最长

D.最低 最短

27.在境外遇到危及所携带的国家秘密载体安全的紧急情况时，要立即（A）所携带的秘密载体，并及时向本单位的保密部门报告。

A.销毁

B.藏匿

C.邮寄

D.上缴

28.存储国家秘密信息的介质，应按照所存储信息的（A）密级标明密级，并按照相应的密级文件进行管理。

A.最高

B.最低

C.相应

D.不同

29.计算机信息系统的保密管理应试行（C）制，由使用计算机信息系统的单位主管领导负责本单位的计算机信息系统的保密工作，并指定有关机构和人员具体承办。

A.分工负责

B.单位负责

C.领导责任

D.个人责任

30.计算机信息系统的安全保密管理人员应经过严格审查，定期进行（C），并保持相对稳定。

A.考评

B.考试

C.考核

D.测评

31.各单位应对涉密信息系统的工作人员进行（C）的保密培训，并定期进行保密教育和检查。

A.工作中

B.定期

C.上岗前

D.一定

32.涉密信息系统打印输出的涉密文件过程稿，应当按照相应（C）文件进行管理。

A.普通

B.一般

C.密级

D.内部

33.涉密信息系统不得与国际互联网或者其他公共信息网络连接，必须实行（B）

A.防火墙隔离

B.物理隔离

C.逻辑隔离

D.外部隔离

34.存储国家秘密信息的U盘只能在（A）计算机上使用。

A.本单位同一密级或者更高密级的涉密

B.办公用

C.上网用

D.涉密

35.存储过国家秘密的涉密存储介质不能（C）密级使用。

A.提高

B.调整

C.解除

D.更改

36.涉密信息处理场所应当定期或者根据需要进行（B）检查。

A.安全性能

B.保密技术

C.不定期

D.环境

37.绝密级国家秘密技术在保密期限内（B）申请专利或者保密专利。

A.可以

B.不得

C.暂缓

D.根据情况

38.参加涉外活动一般不得携带涉密载体，确需携带机密级、秘密级涉密载体的，要经（C）批准。

A.上级机关

B.保密工作机构

C.机关、单位负责人

D.保密行政管理部门

39.下列关于参加涉密会议、活动人员保密管理要求说法错误的是（A）

A.可自行委托其他人员代替参加涉密会议、活动

B.不得擅自记录、录音、摄像

C.不得使用无线键盘、无线网卡等设备或装置

D.不得将手机带入

40.下列关于涉密会议、活动宣传报道保密管理要求说法错误的是（D）

A.撰写新闻稿件，不得涉及国家秘密

B.会议由新闻通稿或报道口径的，应按照新闻通稿或报道口径报道

C.经会议、活动组织者审批后，可公开报道和播放稿件、录像、图片等

D.有关业务主管部门无须审查公开报道内容

41.下列有关涉密视频会议的保密管理要求说法正确的是（A）

A.会议音频视频资料按照涉密载体管理

B.无须指定专人负责视频会议系统运行维护和音视频录制

C.会议召开时，无须对会场及设施设备进行安全保密检查

D.无须按照涉密网络有关要求建设和管理视频会议系统

42.下列关于涉外活动保密管理要求说法错误的是（D）

A.不得带领国（境）外人员进入涉密场所

B.与国（境）外人员会谈不得涉及国家秘密

C.不得利用国（境）外人员办公设备处理涉密信息

D.在紧急情况下，可以利用国（境）外通信设施进行涉密通信联络

43.违反《中华人员共和国保守国家秘密法》的规定，（B）泄露国家秘密，情节严重的，依照刑法有关规定追究刑事责任。

A．故意

B.故意或者过失

C.过失

D.擅自

44.某领导外出时提包被窃，找回后发现包内钱物丢失，涉密文件完整无缺。这一事件（C）

A.属于涉密事件

B.不应视为泄密事件

C.在不能证明文件未被不应知悉者知悉时，按照泄密事件处理

D.无法定性

45.属于国家秘密的文件、资料或者其他物品下落不明的，自发现之日起，绝密级（A）内，机密、秘密级（）内查无下落的，应当按照泄密事件处理。

A.10日，60日

B.15日，60日

C.10日，30日

D.15日，30日

46.泄密事件查处工作的终结期限为（C）

A.6个月

B.1个月

C.3个月

D.2个月

47.发生泄密事件的机关、单位，应当在发现后（C）小时内，书面向有关保密行政管理部门报告。

A.60

B.48

C.24

D.12

48.向境外组织、机构人员泄露绝密级国家秘密的泄密案件，由（B）组织或者参与查处。

A.省、自治区、直辖市保密行政管理部门

B.国家保密行政管理部门

C.中央国家机关保密部门

D.国防科技工业管理部门

49.过失泄露绝密级（C）件、机密级（）件或者秘密级（）件的，应予立案。

A.1， 2， 3

B.1， 3， 3

C.1， 3， 4

D.3， 2， 1

50.对在定密工作中因玩忽职守、不负责任错定、漏定，致使国家秘密泄露，或者妨碍正常交流，使国家利益造成损失的，应视情节的轻重追究当事人的（A）

A.行政责任

B.刑事责任

C.法纪责任

D.违规责任

51.刑法第一百一十一条规定，为境外的机构、组织、人员窃取、刺探、收买、非法提供国家秘密或者情报的，处（B）

A.十年以上有期徒刑或无期徒刑

B.五年以上十年以下有期徒刑

C.三年以上七年以下有期徒刑

D.三年以下有期徒刑

52.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，故意或者过失泄露国家秘密，情节特别严重的，处（C）

A.十年以上有期徒刑或无期徒刑

B.五年以上十年以下有期徒刑

C.三年以上七年以下有期徒刑

D.三年以下有期徒刑

53.涉嫌故意泄露（C）以上的，应以故意泄露国家秘密罪立案。

A.秘密级国家秘密1项（件）

B.机密级国家秘密1项（件）

C.机密级国家秘密2项（件）

D.秘密级国家秘密2项（件）

# 四、论述题（共3题）

 1.结合自身岗位与业务工作谈一谈如何落实定密工作。

答：（根据实际情况作答）。

 2.请谈一谈对“上网信息不涉密，涉密信息不上网”的理解。

答：（根据实际情况作答）。

 3.你如何看待某些人员泄露甚至出卖国家秘密的行为？

答：（根据实际情况作答）。

# 五、案例分析题（共4题）

 1.在办公室内，一位涉密人员在使用涉密计算机处理机密级信息时，同时用手机和家人通话，是否存在泄密隐患？

答：存在泄密隐患。因为此时手机可以看作一个二次发射机，计算机辐射泄漏发射的涉密信息可以附载到手机信息中再次发射，经过手机的基站还可以再次发射，远远超出安全距离。

 2.在办公室内，有一部地方线电话和一部军线电话，只要谈论涉及武器装备科研生产事项都使用军线电话，是否符合保密要求，为什么？

答：不符合。军线电话是非保密电话。

 3.某单位办公室有涉密计算机和非涉密计算机各一台，因为资金紧张只配备了一台打印机，采用转化开关连接在这两台计算机上使用，是否符合保密要求，为什么？

答：不符合保密要求。因为目前很多打印机都带有存储部件，这些存储部件将存储打印信息的内容，利用转化开关转换后，存储部件可以被访问，信息的内容可以被窃取。

 4.某单位员工为了保证自己的涉密计算机不被病毒感染，定期使用个人U盘从互联网下载最新病毒库然后插入涉密计算机更新病毒库，是否符合保密要求，为什么？

答：不符合保密要求。因为使用个人U盘从互联网下载病毒库时可能被植入特种“木马”程序，当该U盘插入涉密计算机时，在无任何操作和显示的情况下，U盘内的特种“木马”程序会自动按照预先的设计，将涉密计算机中的全部信息复制到U盘中隐藏起来。当该U盘再次插入连接互联网的计算机时，“木马”程序将会将隐藏在U盘上的涉密信息自动发送到互联网上的指定邮箱，造成泄密。