

保密基本知识试题

(共 238 题)

一、填空题 (共 46 题)

1. 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。
2. 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。
3. 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作出标志，并在封面或者首页以其中的最高密级和最长保密期限作出标志。
4. 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志。
5. 保守国家秘密是我国公民的一项基本义务。
6. 涉密人员是指因工作需要，接触、知悉、管理和掌握国家秘密的人员。
7. 涉密人员上岗前要经过保密审查和培训。
8. 因私出国（境）的重要涉密人员须经军工集团公司或省级国防科技工业管理部门审批。
9. 涉密人员脱密期届满的，对其知悉的国家秘密仍负有保密义务。
10. 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3-5年，重要涉密人员为2-3年，一般涉密人员为1-2年。
11. 涉密人员脱离涉密岗位必须清退所保管的涉密载体、签订保密承诺书以后，才能办理手续。
12. 外聘工勤服务人员不得接触国家秘密。
13. “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。
14. 保密期限需要延长的，由原确定密级和保密期限的机关、单位或者其上级机关决定。
15. 不准在私人交往和通信中泄露国家秘密。

16. 不准在普通手机通话和发送短信中涉及国家秘密。
17. 不准将普通手机与涉密计算机（涉密信息系统）连接。
18. 不准将普通手机带入涉密场所。
19. 不得在互联网上用电子邮件传送国家秘密信息。
20. 不准通过普通邮政、快递、物流方式传递属于国家秘密的文件、资料
和 其他物品。
21. 个人因公外出，应把所携带涉密载体（秘密载体）存放在保密设备里。
22. 销毁磁介质、光盘等秘密载体，应当采用物理或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. 计算机口令在网络中必须加密存储和传输。
26. 涉密系统不得直接或间接连接国际互联网，必须实行物理隔离。
27. 涉密计算机的密级应按处理和存储信息的最高密级确定。
28. 计算机一旦存储和处理过一份涉密信息，就应当确定为涉密计算机，并粘贴相关密级标志。
29. 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。
30. 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装操作系统。
31. 在涉密工作区域，禁止使用无标志的存储介质。
32. 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。
33. 存储在涉密计算机或存储介质中的电子文件，只要内容涉密，就应当标明密级。
34. 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，则系统口令更换周期不得长于一周。
35. 处理秘密级信息的涉密计算机系统口令长度不得少于8个字符。
36. 处理机密级信息的涉密计算机系统口令长度不得少于10个字符。
37. 绝密级计算机采用智能卡或 USBkey 结合口令或生理特征身份鉴别措施。

38. 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 10 分钟。

39. 高密级的移动存储介质禁止在 低密级的计算机上 使用。

40. 涉密移动存储介质禁止在 涉密计算机 和 非涉密计算机 上交叉使用。

41. 携带涉密计算机和存储介质外出应当履行 审批手续。

42. 携带涉密计算机和存储介质外出工作，带回时应当进行 保密检查。

43. 单位通过互联网发布信息应当进行 保密审查。

44. 严禁将用于处理国家秘密信息的具有打印、复印、传真等多功能的一体机与 普通电话线 连接。

45. 机密级国家秘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。

46. 秘密级国家秘密是 一般 的国家秘密，泄露会使公家的安全和利益遭受损害。

二、判断题（对下列各题，正确的打“√”，错误的打“×”。共 143 题）

1. 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。（√）

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护国家秘密的义务。（√）

3. 保守国家秘密的工作的方针是积极防范、突出重点、依法管理，既确保国家秘密安全又便利信息资源合理利用。（√）

4. “业务工作谁主管，保密工作谁负责”是保密工作的重要原则。（√）

5. 国家秘密的密级分为绝密、机密、秘密三个等级。（√）

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

7. 机密级国家秘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。(✓)

8. 秘密级国家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。(✓)

9. 保守国家秘密是我国公民的一项基本义务。(✓)

10. 涉密岗位根据涉及国家秘密的程度分为核心（绝密级）、重要（机密级）、和一般（秘密级）三个等级。(✓)

11. 核心涉密岗位是指产生、管理、掌握或者经常处理绝密级或较多机密级事项的工作岗位。(×)

12. 涉密人员是指因工作需要，合法接触、知悉、管理和掌握国家秘密的人员。(✓)

13. 涉密人员应当具有中华人民共和国国籍。(✓)

14. 涉密人员上岗前要经过审查和批准，并接受保密教育培训。(✓)

15. 经审查合格，进入涉密岗位的人员须按规定签订保密责任书或承诺书，承担相应的保密责任。(✓)

16. 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不适合继续在涉密岗位工作的应当及时调离涉密岗位。(✓)

17. 涉密人员与境外人员通婚或接受境外机构、组织资助的应当向单位报告。(✓)

18. 涉密人员本人或者直系亲属获得境外永久居留权以及取得外国国籍的应当向单位报告。(✓)

19. 涉密人员离岗后，应当遵守脱密期管理规定，核心涉密人员脱密期 3~5 年，重要涉密人员脱密期 2~3 年，一般涉密人员脱密期 1~2 年。(✓)

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

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

22. 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。（ √ ）

23. 涉密人员脱密期内可以因私出境。（ × ）

24. 涉密人员脱密期满后，可以不再履行保密责任和义务。（ × ）

25. 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。（ × ）

26. 涉密人员脱密期满后，对所知悉的国家秘密任然要承担保密责任和义务。（ √ ）

27. 对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。（ √ ）

28. 涉密单位应对聘用的保安和临时工进行保密教育培训。（ × ）

29. 不准在私人交往和通信中泄露国家秘密。（ √ ）

30. 配偶、子女和本人都是涉密人员，互相谈涉密事项没有关系。（ × ）

31. 各个国家机关、单位对所生产的国家秘密事项，应当按照国家秘密及密级具体范围的规定及时确定密级。（ √ ）

32. 定密工作是指对机关、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，并对国家秘密载体作出标志，及时通知应当知悉的机关、单位和人员，并按规定进行全过程管理的活动。（ √ ）

33. 项目定密是指军工单位对承担的武器装备科研生产项目依法进行确定密级、保密期限、知悉范围和作出国家秘密标志的工作。（ √ ）

34. 保密范围定得越宽，密级越高，越有利于国家秘密的安全。（ × ）

35. 定密和变更密级的程序是项目承办人依据密级范围提出初始意见，部门领导审查签字后报主管领导审批，对把握不准的可由单位定密工作小组

审定。(√)

36. 国家秘密的标志为★，★前标密级，★后标保密期限。(√)

37. 纸质载体的密件，其密级和保密期限应在首页（或者封面）标明。(√)

38. 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。(√)

39. 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作出标志，并在封面或者首页以其中的最低密级和最短保密期限作出标志。(×)

40. 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志。(√)

41. 密件的密级和保密期限变更后，应当在原标志位置的附近作出标志，原标志以明显方式废除。(√)

42. 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。(√)

43. 国家秘密事项的密级和保密期限一经确定，就不能改变。(×)

44. 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。(×)

45. 国家秘密事项的保密期限届满即自行解密。(√)

46. 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。(√)

47. 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。(√)

48. 单位领导要求继续保密的事项，在所要求的期限内不得解密。(×)

49. 已降密的事项可以随意公开。(×)

50. 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。(√)

51. 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。
(×)
52. 密级的变更包括降低或者提高密级等级。(√)
53. 制作涉密载体应当依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。(√)
54. 纸介质涉密载体应当在本机关、单位内部文印室或委托保密工作机构定点的单位制作。(√)
55. 国家秘密定点复制单位，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。(×)
56. 收发涉密载体，应当履行清点、登记、编号、签收等手续。(√)
57. 传递涉密载体应当密封包装，装载涉密载体的信封或袋牌上应当标明密级、编号和收发单位名称。(√)
58. 传递涉密载体应当通过机要交通、机要通信或者指派专人传递；不得通过普通邮政渠道传递。(√)
59. 国家秘密文件、资料可以通过普通邮政“特快专递”传送。(×)
60. 不准通过普通邮政传递属于国家秘密的文件、资料和其他物品。
(√)
61. 记录涉密内容应当使用保密本。(√)
62. 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作出文字记载。(√)
63. 单位内部复制涉密载体应当履行审批手续，复制机密级以上涉密载体须经部门或单位领导批准，加盖复制戳记，视同原件管理，并进行登记。
(×)
64. 因公出差，且两人通行，可以携带密件到购物、餐饮、娱乐等公共场所。(×)

65. 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。（√）

66. 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了。（×）

67. 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。（×）

68. 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，该领导使用涉密 U 盘连接营业性场所计算机打印了机密级汇报资料，作删除处理。（×）

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

70. 个人参加会议带回的秘密文件、资料，应交本单位文秘部门登记、管理。（√）

71. 阅读和使用涉密载体应当办理登记、签收手续，管理人员应当随时掌握涉密载体的去向。（√）

72. 传达国家秘密事项时，凡不准记录、录音、录像的，应当事先申明。（√）

73. 不准在普通手机通话中涉及国家秘密。（√）

74. 普通手机处于关机状态下，不存在泄密隐患。（×）

75. 不得使用普通手机短信传送国家秘密信息。（√）

76. 不得将普通手机与涉密信息系统连接。（√）

77. 不得在涉密场所使用普通手机。（√）

78. 个人因公外出，携带秘密载体应当采取严格的保密措施。（√）

79. 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。（√）

80. 领导干部为了工作方便，可以将密件带回家中处理。（ × ）
81. 工作人员离开办公场所，应当将涉密载体存放在保密设备里。（ √ ）
82. 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。（ √ ）
83. 销毁磁介质、光盘等密秘载体，应当采用物理或化学的方法彻底销毁，确保信息无法还原。（ √ ）
84. 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。（ × ）
85. 公开报道、出版或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。（ × ）
86. 未经保密工作机构审查批准，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。（ √ ）
87. 机关、单位每年应当定期对当年所存涉密载体进行清查、核对，发现问题的应当及时向保密工作机构报告。（ √ ）
88. 销毁纸介质涉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国家保密标准的碎纸机，送造纸厂销毁的应当送保密行政管理部门指定的造纸厂销毁，并由销毁单位两人以上押运、监销。（ √ ）
89. U 盘上的涉密信息，只要执行了删除程序就不可以恢复了。（ × ）
90. 涉密载体不得作为废品出售。（ √ ）
91. 密品是指直接含有国家秘密信息的设备或者产品。（ √ ）
92. 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。（ √ ）
93. 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备案。（ √ ）

94. 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。(√)
95. 涉密场所使用进口设备和产品的应当进行安全保密技术检测。(√)
96. 涉密场所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。(√)
97. 普通手机关机后可以带入要害部门、部位。(×)
98. 涉密电子文档应当标注密级标志，密级标志不能与正文分离。(√)
99. 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。(√)
100. 不得使用未采取密码保护的通信系统传输涉密信息。(√)
101. 不得将自己使用和保管的涉密计算机和移动存储介质擅自交给他人使用。(√)
102. 无线电话不保密，军线电话是保密的。(×)
103. 数字移动电话传输的是数字信号，因此是保密的。(×)
104. 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。(×)
105. 电磁信号泄漏泄密的方式主要是辐射和传导两种方式。(√)
106. 涉密存储介质经文件删除格式化处理后，仍不得作为非密介质使用。
(√)
107. 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，禁止密明混用。(√)
108. 涉密信息使用的加密措施经过国家密码主管部门批准后，在任何地方都可以使用。(×)
109. 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。(√)
110. 绝密级信息必须加密存储。(√)

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

112. 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。(√)

113. 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。(√)

114. 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。(√)

115. 涉密计算机和移动存储介质未经国家指定的专业销密点销密, 不得自行淘汰处理。(√)

116. 在涉密场所使用的与国际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。(√)

117. 不得在上国际互联网的计算机上处理和存储涉密信息。(√)

118. 涉密计算机不得与国际互联网络或其他公共网络相连接。(√)

119. 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。(×)

120. 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、网络新闻组上发布、谈论、张贴、传播国家秘密信息。(√)

121. 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。
(×)

122. 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。(√)

123. 国家秘密不得在国际互联网连接的计算机和信息系统中处理、存储、传递, 但可与在单位内部非涉密计算机上处理、存储、传递。(×)

124. 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。(×)

125. 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、表彰和职称评定。(√)

126. 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。(√)

127. 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。(×)

128. 对外公开宣传报道时, 单位代号、真实名称、掩护名称不得同时使用。
(√)

129. 接受新闻媒体采访, 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。(√)

130. 音像制品涉及国家秘密的, 应按涉密资料保管。(√)

131. 保密教育和保密提醒是科技交流必须坚持的制度。(√)

132. 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。(√)

133. 未经批准, 任何单位、部门或个人均不得到重要涉密场所进行采访、照相、录像等活动。(√)

134. 使国家秘密被不应知悉者知悉的, 属于泄露国家秘密行为。(√)

135. 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。(√)

136. 涉密载体下落不明, 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, 按泄密事件处理。(√)

137. 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。(√)

138. 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, 应予立案。(√)

139. 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。(×)

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

141. 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。（√）

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

143. 未经相关保密工作保密批准，不得向境外邮寄密品密件或随身携带密品密件出境。（√）

三、单项选择题（下列各题中只有一个正确答案。共 43 题）

1. 国家秘密是关系国家安全和利益，（ B ），在一定时间内只限一定范围的人员知悉的事项。

- A. 根据实际需要确定
- B. 依照法定程序确定
- C. 按照领导的意图确定

2. 一切国家机关、武装力量、政党、社会团体、（ C ）都有保守国家秘密的义务。

- A. 国家公务员
- B. 共产党员
- C. 企业事业单位和公民

3. 保守国家秘密的工作实行积极防范、突出重点、依法管理，（ C ）的方针。

- 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

4. 各级机关、单位对产生的国家秘密事项，应当按照（ C ）及时确定密级。

- A. 保密法实施办法

- B. 保密规章制度
 - C. 国家秘密及其密级具体范围的规定
5. 一份文件为机密级，保密期限是 10 年，应当标注为（ C ）。
- A. 机密 10 年
 - B. 机密★
 - C. 机密★10 年
6. 某文件标注“绝密★”，表示该文件保密期限为（ A ）。
- A. 30 年
 - B. 20 年
 - C. 长期
7. 国家秘密的保密期限届满的，自行（ C ）。
- A. 变更
 - B. 公开
 - C. 解密
8. 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
9. 涉密人员离岗、离职前，应当将所保管和使用的涉密载体全部清退，并（ C ）。
- A. 登记销毁
 - B. 订卷归档
 - C. 办理移交手续
10. 复制属于国家秘密的文件、资料或摘录、引用、汇编属于国家秘密内容形成的涉密载体，（ 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. 可以改变

11. 制作涉密载体，应当依照有关规定（ A ），注明发放范围及制作数量，涉密载体应当编排顺序号。

- A. 标明密级和保密期限
- B. 提出管理要求
- C. 认真进行核对

12. 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

13. 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

14. 收发涉密载体，应当履行（ A ）手续。

- A. 清点、登记、编号、签收等
- B. 交接
- C. 签字

15. 任何情况下，不得向境外传递（ C ）秘密载体。

- A. 机密级
- B. 秘密级
- C. 绝密级

16. 变更密级或解密，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制定的单位决定

17. 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、机要通信或派人直接递送

18. 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
- C. 现场

19. 销毁涉密载体，应当送（ C ）指定的厂家销毁，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

20. 销毁秘密文件、资料要履行（ C ）手续，并由两名以上工作人员到指定场所监销。

- A. 清点
- B. 交接
- C. 审批、登记

21. 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

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

- A. 最高
- B. 最低
- C. 相应

23. 涉密场所应当按照国家有关规定经相关部门的安全技术检测，与境外机

构、人员所住保持（ C ）的安全距离。

- A. 300 米
- B. 1000 米
- C. 相应

24. 计算机信息系统的保密管理应实行（ 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. 领导负责

25. 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

26. 各单位保密工作机构应对计算机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

27. 计算机和信息系统应采取相应的防（ C ）泄漏的保密措施。

- A. 信息
- B. 密级资料
- C. 电磁

28. 计算机信息系统打印输出的涉密文件，应当按相应（ C ）文件进行管理。

- A. 普通
- B. 一般
- C. 密级

29. 涉密计算机信息系统不得与国际互联网或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

30. 存储国家秘密信息的 U 盘只能在（ A ）计算机上使用。

- A. 本单位同一密级或更高密级的涉密
- B. 办公用
- C. 上网用

31. 存储过国家秘密的信息介质可以（ A ）密级使用。

- A. 提高
- B. 降低
- C. 解除

32. 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

33. 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

34. 新闻出版单位和提供信息的单位，应当根据国家保密法规，建立健全（ C ）保密审查制度。

- A. 报纸杂志
- B. 工商部门
- C. 新闻出版

35. 违反《中华人民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. 故意或过失

C. 过失

36. 发生泄密事件应当迅速查明（ B ），及时采取补救措施，并报告保密行政管理部门和上级领导机关。

A. 主要、次要责任者

B. 被泄露国家秘密的内容和密级、造成或者可能造成的危害、事件的主要情节和有关责任者

C. 事件属于什么性质

37. 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. 属于泄密事件

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，按泄密事件处理

38. 属于国家秘密的文件、资料或其他物品下落不明的，自发现之日起，绝密级、机密或秘密级分别在（ A ）内查无下落的，应当按泄密事件处理。

A. 10 日，60 日

B. 15 日，60 日

C. 10 日，30 日

39. 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

40. 发生泄密事件的机关、单位，应当在发现后的（ 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

41. 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

42. 过失泄露绝密级（ C ）件、机密级（ C ）件或秘密级（ C ）件的，应予立案。

- A. 1, 2, 3
- B. 1, 3, 3
- C. 1, 3, 4

43. 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

四、简答题（共 6 题）

1. 涉密人员应遵守的计算机管理“十个不得”内容是什么？

答：（1）涉密计算机不得连接互联网；

（2）涉密计算机不得使用无线键盘和无线网卡；

（3）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；

（4）涉密计算机和涉密移动存储介质不得让他人使用、保管或办理寄运；

（5）未经专业销密，不得将涉密计算机和涉密移动介质淘汰处理；

（6）涉密场所中连接互联网的计算机不得安装、配备和使用摄像头等视频、音频输入设备；

（7）不得在涉密计算机和非涉密计算机之间交叉使用移动存储介质；

（8）不得在互联网上存储、处理涉密信息；

（9）不得使用普通传真机、多功能一体机传输、处理涉密信息；

（10）不得通过手机和其他移动通信工具谈论国家秘密、发送涉密信息。

2. 涉密计算机信息系统安全保密四方面要求是什么？

答：包括四个方面：物理安全、运行安全、信息安全保密、安全保密管理。

3. 什么是保密要害部门、部位？

答：单位内部业务工作中涉及绝密级或较多机密级、秘密级国家秘密的部门

为保密要害部门。单位内部集中制作、存放、保管国家秘密载体的专门

场所为保密要害部位。

4. 保密要害部门、部位防护措施有哪些？

答：（1）保密要害部门部位要有安全保密隔离措施，并安装防盗报警装置；

（2）涉及机密、绝密级国家秘密的保密要害部门部位还要安装电视监控

系统，门禁系统，采用 IC 卡或生理特征身份鉴别，并配备警卫人员；

（3）存放国家秘密载体要配备密码文件柜，存放绝密级国家秘密载体要

配备密码保险柜。

5. 重要涉密会议应采取哪些主要保密措施？

答：大型或重要涉密会议应当在内部场所召开；确需在外部场所召开的，主

办部门应当制定保密工作方案，征询保密工作机构的意见；对会议现场

进行安全保密技术检查；对参加会议的人员要登记备案；对会议人员和

服务人员要进行保密教育；按规定使用手机干扰器、低辐射扩音设备、防辐射屏幕装置，不得使用无线话筒。

6. 什么是泄露国家秘密的行为？

答：泄露国家秘密行为是指违反保密法律法规和规章制度，使国家秘密被不应知悉者知悉；使国家秘密超出了限定的接触范围，而不能证明未被不应知悉者知悉的行为。