

温州市保密知识竞赛题库

(以下题目及答案仅供参考)

一、单选题

1、新修订《中华人民共和国保守国家秘密法》共有（ C ）。

A、五章三十四条 B、五章三十五条 C、六章五十三条

2、新修订《中华人民共和国保守国家秘密法》于(C)由第十一届全国人民代表大会常务委员会第十四次会议通过。

A、2010年1月1日 B、2010年10月1日 C、2010年4月29日

3、2010年____，第十一届全国人大常委会第十四次会议审议通过了新修订的《中华人民共和国保守国家秘密法》，自2010年____起实施。（B）

A、4月29日，8月1日

B、4月29日，10月1日

C、5月9日，10月1日

4、新《保密法》规定，国家秘密的保密期限，除另有规定外，绝密级不超过____年，机密级不超过____年，秘密级不超过____年。

(C)

A、五十，三十，二十 B、二十，十，五 C、三十，二十，十

5、涉密计算机安装从互联网下载或来历不明软件存在的泄密隐患主要是：（A）

A、被植入“木马”窃密程序 B、死机 C、盗版危害

6、新《保密法》第三条规定任何（C）的行为，都必须受到法律追究。

A、泄露国家秘密 B、窃取国家秘密 C、危害国家秘密安全

7、涉密计算机及相关设备存储数据的恢复，必须到（B）进行。

A、销售单位 B、国家保密行政管理部门批准的涉密数据恢复资质单位 C、原生产单位

8、处理涉密信息的计算机、传真机、复印机等办公自动化设备应当在单位内部进行维修，现场有专门人员监督，严禁维修人员读取或复制涉密信息；确需送外维修的，应当（A）。

A、拆除涉密信息存储部件 B、对涉密信息存储部件进行加密处理 C、将涉密信息删除

9、涉密信息系统是指由计算机及其相关和配套设备、设施构成的，按照一定的应用目标和规则存储、处理、传输（A）信息的系统或者网络。

A、国家秘密 B、工作秘密 C、商业秘密

10、涉密信息系统建设使用单位应当按照系统处理国家秘密信息的（C）确定系统密级，并按相应密级的涉密信息系统防护要求进行保护和管理。

A、最低密级 B、大多数文件的密级 C、最高密级

11、集中存储、处理工作秘密的信息系统和信息设备，参照（C）级信息系统和信息设备管理。

A、绝密 B、机密 C、秘密

12、新《保密法》第四条规定，法律、行政法规规定公开的事项，应当（ A ）。

A、依法公开 B、以公开为原则公开 C、经保密审查后公开

13、关于新《保密法》中定密权限的说法，不正确的是：（ B ）

A、确定国家秘密的密级，必须遵守定密权限

B、除公安机关和国家安全机关外，县（处）一级机关未经授权，只能确定机密级和秘密级国家秘密事项。

C、设区的市、自治州一级的机关及其授权的机关、单位可以确定绝密级以外的国家秘密事项。

14、国家机关和涉密单位的涉密信息系统投入使用前应经过（ B ）审查批准。

A、本单位保密工作机构 B、保密行政管理部门 C、主管领导

15、涉密信息设备改作非涉密信息设备使用或淘汰处理时，应当（ C ）。

A、删除涉密文件 B、格式化存储部件 C、将涉密信息存储部件拆除

16、涉密信息系统的保密设施、设备应当与系统_____。（ C ）

A、同步规划，同步建设，同步维护

B、同步规划，同步运行，同步维护

C、同步规划，同步建设，同步运行

17、涉密信息系统应当严格设定用户权限，按照_____和_____的原则，控制涉密信息知悉范围。（ C ）

A、最高密级防护 最大授权管理

B、最低密级防护 最小授权管理

C、最高密级防护 最小授权管理

18、甲涉密单位面临搬迁，大量涉密计算机和移动存储介质亟待寄运。正确的做法有：（C）

A、将涉密计算机和移动存储介质通过中国邮政挂号和保价邮寄方式寄运

B、在不指派专人全程监管的情况下委托搬家公司搬运

C、通过机要交通渠道寄运

19、传递涉密载体的做法不正确的是：（B）

A、在市内传递机密级和秘密级涉密载体，通过机要文件交换站进行，也可以派专人送达

B、传递涉密载体，可由收件机关、单位的任一工作人员签收

C、寄往市外的涉密载体，要通过机要交通或机要通信部门传递

20、下列关于绝密级载体管理，说法不正确的是：（B）

A、传递涉密载体要通过机要交通或机要通信部门

B、禁止携带绝密级涉密载体外出

C、禁止携带绝密级载体参加涉外活动

21、以下不属于涉密移动存储介质的是：（A）

A、涉密台式计算机

B、涉密移动硬盘、涉密光盘

C、涉密优盘或存储卡

22、在涉及国家秘密岗位工作的人员，按照涉密程度分为_____，实行分类管理。（A）

A、核心涉密人员，重要涉密人员，一般涉密人员

B、核心涉密人员，一般涉密人员，非涉密人员

C、重要涉密人员，一般涉密人员，非涉密人员

23、制订保密技术发展规划、计划、政策、措施，制订保密技术装备体制标准，并督促有关部门配备达标。这是（ B ）的职责。

A、各级党委保密委员会 B、各级政府保密工作部门 C、中央国家机关保密工作机构

24、中央国家机关在其职权范围内，（ B ）本系统的保密工作。

A、监督或管理 B、主管或指导 C、检查或督促

25、国家秘密是关系（ A ），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。

A、国家的安全和利益 B、国家的经济安全和政治利益 C、国家的安全和民族的利益

26、国家秘密及其密级的具体范围，由国家保密行政管理部门分别会同外交、公安、国家安全和（ B ）规定。

A、其他有关部门 B、其他中央有关机关 C、国务院其他有关部门

27、机关、单位应当对工作人员进行（ C ），定期检查保密工作。

A、岗位培训 B、警示教育 C、保密教育

28、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（ C ）。

A、给予警告处分 B、进行批评教育 C、给予行政处分

29、根据《中华人民共和国保守国家秘密法》的有关规定，关于政党的秘密事项的正确表述是(C)。

A、政党的秘密事项经保密工作部门确认后，属于国家秘密事项

B、政党的秘密事项与国家秘密性质不同，不属于国家秘密事项

C、政党的秘密事项符合保密法有关规定的，属于国家秘密

30、国家秘密的密级分为(A)。

A、绝密、机密、秘密三级 B、绝密和机密两级 C、秘密和机密两级

31、(C)以上地方各级保密行政管理部门在其职权范围内，主管本行政区域保守国家秘密的工作。

A、省级 B、市级 C、县级

32、县级以上国家机关和涉及国家秘密的单位，根据实际情况设置(A)或者指定人员，管理本机关和本单位保守国家秘密的日常工作。

A、保密工作机构 B、管理工作机构 C、业务指导机构

33、国家秘密及其密级的具体范围，应当在(B)公布。

A、社会范围内 B、有关范围内 C、机关、企事业范围内

34、对某一事项是否属于国家秘密和属于何种密级有争议的，由国家保密工作部门或者省、自治区、(C)的保密工作部门确定。

A、地市 B、县(区) C、直辖市

35、国家秘密事项的保密期限需要延长的，由(C)决定。

A、原确定密级的保密期限的机关、单位决定

B、原确定密级的保密期限的机关、单位的上级机关决定

C、原确定密级和保密期限的机关、单位或者其上级机关决定

36、对于国家秘密保密期限已满而未收到原定密机关、单位延长保密期限通知的，该项国家秘密可以（ A ）解密。

A、自行 B、由上级机关 C、由保密工作部门

37、对绝密级的国家秘密文件、资料和其它物品，非经（ A ）批准，不得复制和摘抄。

A、原确定密级的机关、单位或者其上级机关
B、原确定密级的机关、单位的上级机关或上级保密工作部门
C、原确定密级的机关、单位

38、违反《中华人民共和国保守国家秘密法》的规定，过失泄露国家秘密，情节严重的，应当（ A ）。

A、追究刑事责任 B、进行批评教育 C、给予党纪、政纪处分

39、国家秘密的保密期限，除有特殊规定外，（ C ）。

A、绝密级事项不超过二十年，机密级事项不超过十年，秘密级事项不超过五年

B、绝密级事项不超过十年，机密级事项不超过五年，秘密级事项不超过一年

C、绝密级事项不超过三十年，机密级事项不超过二十年，秘密级事项不超过十年

40、为境外的机构、组织、人员窃取、刺探、收买、非法提供国家秘密的，依法追究（ B ）。

A、行政责任 B、刑事责任 C、经济损失

41、涉密人员出境，应当经过（ C ）的批准。

A、公安机关 B、保密工作部门 C、批准、任用涉密人员的主管部门

42、绝密级国家秘密，（ A ）才能接触。

A、经过批准的人员 B、省、军级以上人员 C、机关工作人员

43、对外交往与合作中需要提供国家秘密事项的，应当按照（ B ）提供。

A、合同规定 B、规定的程序事先经过批准后 C、协议

44、根据《保密法》和《保密法实施办法》，（ B ）主管全国的保密工作。

A、国家保密工作机构 B、国家保密局 C、国务院

45、县以上地方各级政府的保密工作部门，在上级保密工作部门的指导下，依照保密法律、法规和规章管理（ A ）的保密工作。

A、本行政区域 B、所属各级政府 C、本区机关单位

46、下列哪一事项不应当确定为国家秘密（ B ）。

A、国务院总理视察工作的行程安排

B、省长视察工作的行程安排

C、国家主席出访活动安排

47、秘密载体经管人员离岗、离职前，应当将所保管的秘密载体（ A ）。

A、全部清退并办理移交手续

B、部分清退并办理移交手续

C、全部清退可以不办理移交手续

48、各机关、单位对所产生的国家秘密事项，应当依照保密范围的规定及时确定密级，最迟不得超过(A)。

A、10 日 B、20 日 C、30 日

49、传递秘密载体，应当包装密封；传递秘密载体的信封或者袋牌上应当标明(C)。

A、密级 B、密级和编号 C、密级、编号和收发件单位名称

50、某机关工作人员因工作需要携带秘密载体外出，其下述做法中正确的是(A)。

A、采取保护措施，使秘密载体始终处于自己的有效控制之下

B、报经本机关主管领导批准后，独自携带绝密级文件外出

C、报经本机关主管领导批准后，二人共同携带绝密级文件外出参加涉外活动

51、各级国家机关、单位对所产生的国家秘密事项，应当按照(B)确定密级。

A、保密法律法规的规定 B、国家秘密及其密级具体范围的规定 C、本机关单位的保密规定

52、对是否属于国家秘密和属于何种密级有争议的，由(C)确定。

A、国家保密工作部门 B、省、自治区、直辖市的保密工作部门 C、国家保密工作部门或者省、自治区、直辖市的保密工作部门

53、属于国家秘密的文件、资料和其他物品，由确定密级的(C)标明密级。

A、办公室 B、主要承办人 C、机关、单位

54、国家秘密事项的密级确定以后，确定密级的机关、单位的上级机关发现不符合保密范围规定的，应当(B)。

A、及时自行采取措施予以纠正 B、及时通知确定密级的机关、单位纠正

C、及时通知有关保密工作部门采取措施予以纠正

55、出现下列哪种情况时，保密期限内的国家秘密事项可由确定密级的机关、单位及时解密。(A)

A、从全局衡量公开后对国家更为有利的

B、离保密期满不足 1 个月的

C、对经济发展有利的

56、情况紧急时，保密期限内的国家秘密事项可以由确定密级的(C)直接解密。

A、本机关、单位 B、国家保密工作部门 C、上级机关

57、对于上级机关或者有关保密工作部门要求继续保密的事项，在所要求的期限内(C)。

A、自行解密 B、可以解密 C、不得解密

58、各机关、单位确定密级、变更密级或者决定解密，应当由(A)提出具体意见交本机关、单位的主管领导审核批准。

A、承办人员 B、负责人 C、保密工作部门

59、复制属于国家秘密的文件、资料和其他物品，或者摘录、引用、汇编属于国家秘密的内容，(A)。

A、不得擅自改变原件的密级 B、视情况需要可以改变密级

C、既可以保留原件的密级，也可以改变原件的密级

60、任用、聘用的境外人员因工作需要知悉我国国家秘密的，应
照（ C ）的原则，报有关机关批准。

A、“谁主管，谁负责” B、“一事一批” C、“谁主管，谁
负责”和“一事一批”

61、在对外交往与合作中，通过正当渠道提供国家秘密时，应当
以一定的形式要求（ B ）义务。

A、双方承担保密 B、对方承担保密 C、如期归还的

62、对外提供涉及经济、科技和社会发展方面的国家秘密时，批
准机关应当向（ B ）通报有关情况。

A、级政府的保密工作部门 B、同级政府的保密工作部门
C、省、自治区、直辖市政府的保密工作部门

63、召开涉及国家秘密内容的会议时，主办单位应当采取相应的
保密措施，下面哪一项措施是错误的（ B ）。

A、具备安全条件的会议场所 B、使用无线话筒
C、依照保密规定使用会议设备和管理会议文件、资料

64、有下列哪种表现的，有关机关单位依照保密法给予奖励
（ C ）

A、在保密岗位工作 B、捡到文件资料上交保密工作部门
C、对泄露或者非法获取国家秘密的行为及时检举

65、发生泄密事件的机关、单位，应当迅速查明（ B ），及时采
取补救措施，并报告有关保密工作部门和上级机关。

A、主要、次要责任者，及一切涉密者

B、被泄露的国家秘密的内容和密级、造成或者可能造成危害的
范围和严重程度、事件的主要情节和有关责任者

C、事件属于敌我矛盾或人民内部矛盾，及处理上采用法律手段或行政手段的根据

66、对单位存在重大泄密隐患或发生失泄密事件负有主要领导责任的党政领导干部，视其情节轻重，按照干部管理权限应当给予(C)处分。

A、警告、严重警告、撤销党内职务

B、警告、严重警告、撤销党内职或者留党察看

C、警告、严重警告、撤销党内职务、留党察看或者开除党籍

67、凡泄露国家秘密尚不够刑事处罚的，有关机关、单位应当依照规定并根据被泄露事项和行为的具体情节，给予(C)。

A、批评教育

B、党纪处分

C、行政处分

68、凡泄露国家秘密尚不够刑事处罚的，哪种情形应当从重给予行政处分(B)。

A、丢失国家秘密文件资料没有造成损害后果的

B、以谋取私利为目的泄露国家秘密的

C、过失泄露 1 份秘密级文件资料危害不大的

69、泄露绝密级国家秘密，情节特别轻微的，可以酌情(B)行政处分。

A、免予

B、从轻给予

C、从重给予

70、以下行为不属于《中华人民共和国保守国家秘密法》及其实施办法规定的“泄露国家秘密”的是(B)。

A、使国家秘密被不应知悉者知悉的

B、不应知悉国家秘密者被动知悉国家秘密的

C、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

71、不适用《保密法》和《保密法实施办法》的事项是（ A ）

A、机关、单位的内部事项 B、国家秘密 C、政党中涉及的国家秘密

72、机关、单位公开发布信息应当遵循（ C ）。

A、“谁公开，谁审查”原则 B、事前审查原则和依法审查原则
C、A 和 B

73、机关单位产生的国家秘密事项，应当依照国家关于国家秘密及其密级具体范围的规定（ C ）。

A、标明密级 B、进行管理 C、确定密级和保密期限

74、对是否属于国家秘密和属于何种密级不明确的事项，有关机关单位应当及时申请确定，接到申请的上级主管部门或保密工作部门，应当在（ A ）日内作出批复。

A、30 B、20 C、10

75、在书面形式的密件中，下面标志方法不正确的是（ B ）

A、秘密★长期 B、★秘密 C、机密★5 年

76、收发属于国家秘密的文件、资料及其他物品，应当由（ C ）负责，并且应当逐件、逐页清点，履行签收登记手续。

A、单位工作人员 B、办公室工作人员 C、指定的专人

77、机关、单位确定保密要害部门部位应坚持（ C ）的原则。

A、最小化 B、分级确定 C、分级确定和最小化

78、（ A ）以下单位不得汇编国家秘密文件、资料。

A、县级 B、市级 C、厅级

79、秘密级文件、资料及其他物品，可以由（ A ）传递。

A、专人护送 B、普通邮政 C、机要部门

80、绝密级文件、资料在哪种情况下可以携带（ B ）。

A、本单位办公室负责人批准，且两人同行，共同负责

B、本单位主管领导人批准，且两人同行，共同负责

C、本单位主管领导人批准，一人携带并负责

81、泄密责任者对行政处分或者处罚决定持有异议时，可以要求对作出的行政处分或者处罚（ B ）。

A、进行改正 B、进行复议 C、进行听证

82、销毁秘密文件、资料应当造册登记，且必须经（ B ）审批。

A、县级以上单位主管领导 B、本单位主管领导 C、保密工作部门

83、公务员法规定，公务员应当履行（ C ）的义务：

A、保守业务秘密 B、保守商业秘密 C、保守国家秘密和工作秘密

84、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，情节较轻的，处（ B ）有期徒刑、拘役、管制或者剥夺政治权利。

A、五年以上 B、五年以下 C、十年以下

85、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，情节特别严重的，处（ C ）或者无期徒刑。

A、二十年以上有期徒刑 B、十五年以上有期徒刑 C、十年以上有期徒刑

86、行政机关应当建立健全政府信息公开发布（ B ），明确审查的程序和责任。

A、定人定责机制 B、保密审查机制 C、领导审查机制

87、行政机关在公开政府信息前，应当依照《中华人民共和国保守国家秘密法》以及其他法律、法规和国家有关规定对拟公开的政府信息进行（ A ）。

A、审查 B、送审 C、自查

88、新闻出版单位采访涉及国家秘密的会议或其他活动，应当经（ A ）批准。

A、主办单位 B、上级新闻主管部门 C、保密工作部门

89、国家秘密文件、资料及其他物品，应当存放在有利于安全保密的地方，并配备必要的（ B ）。

A、安全保卫人员 B、保密防范设施 C、监控设施

90、国家秘密文件、资料应当按照（ C ）的规定定期清查、清退。

A、保密部门 B、机关单位 C、制发机关

91、机构撤销、合并时，原机构的国家秘密文件、资料及其他物品，应当根据不同情况，分别移交给有关单位。下列移交做法不对的是（ C ）。

A、移交给制发机关和合并后的新单位

B、移交给承担其原职能的单位

C、移交给保密部门

92、任用管理国家秘密文件、资料及其他物品的专职人员，应当遵循（ A ）的原则，并在上岗前进行保密教育。

A、先审查后使用 B、先使用后审查 C、边使用边审查

93、在销毁国家秘密过程中，以下哪种做法不对（ A ）。

A、将解密的国家秘密文件作为废品出售

B、销毁秘密文件应当在销毁前登记造册并经领导批准

C、销毁国家秘密应当二人以上监销并以不能恢复为标准

94、公开出版发行的报刊、书籍、影视作品，不得涉及（ B ）。

A、政府信息 B、国家秘密 C、个人资料

95、举办各种公开性展览，在展出前应当由（ C ）对展品和说明进行保密审核。

A、文化部门 B、保密部门 C、主管部门

96、发生向境外机构、组织、人员泄露国家秘密的，有关机关、单位应当在发现后的（ B ）向相应的保密工作部门或机构报告。

A、12 小时之内 B、24 小时之内 C、48 小时之内

97、机关、单位发生泄密事件时，应当及时调查处理，同时报告（ C ）。

A、市保密局 B、自治区保密局 C、当地保密工作部门

98、国家秘密事项变更密级不能标明密级的，有关单位应当及时将变更密级的决定通知（ A ）的人员。

A、接触范围内 B、机关单位内 C、行政区域内

99、下列属于密件的是（ B ）。

A、发至省军级的国务院文件 B、标明了密级的未公布的县级领导班子调整意见 C、党内有关资料、材料、党刊、工作简报

100、一国家机关工作人员违反保密规定，携带秘密文件回家，途中文件不慎被盗不能追回。此人的行为属于（ B ）

- A、故意泄露国家秘密行为 B、过失泄露国家秘密行为
C、故意和过失泄露国家秘密行为

101、《保密法》在总则中规定了保守国家秘密的义务，下列表述中正确的是（ A ）。

A、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

B、一切国家机关、武装力量和政党都有保守国家秘密的义务

C、一切社会团体、企业事业单位和公民都有保守国家秘密的义务

102、《保密法》立法的依据是（ A ）

A、《宪法》 B、《刑法》 C、《行政法》

103、在政府信息公开的过程中，行政机关不得公开涉及国家秘密、商业秘密、个人隐私的政府信息。即使在特定情况下，也不可以公开（ C ）

A、涉及商业秘密的政府信息 B、涉及个人隐私的政府信息

C、涉及国家秘密的政府信息

104、《保密法》第三章规定，在有线、无线通信中传递国家秘密的，（ B ）。

A、必须经有关领导批准 B、必须采取保密措施 C、必须经过保密部门批准

105、不属于《保密法》调整范围的是（ B ）

A、国家秘密 B、工作秘密 C、科学技术中的国家秘密事项

106、有权给予泄密责任人行政纪律处分的是（ A ）

- A、责任人所在的机关、单位 B、同级保密工作部门
C、同级国家安全工作部门

107、凡是向国际互联网的站点提供或发布信息，都必须经过
(A)。

- A、保密审查批准 B、保密部门批准 C、上级机关批准

108、涉及国家秘密的计算机信息系统，不得(C)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。

- A、直接地 B、间接地 C、直接或间接地

109、涉及(A)的信息，不得在国际联网的计算机信息系统中存储、处理、传递。

- A、国家秘密 B、绝密级国家秘密 C、机密级国家秘密

110、在管理曾经存储处理过国家秘密信息的计算机媒体的过程中，下列做法不正确的是 (B)。

- A、没有降低密级使用 B、不能使用时可以自行销毁
C、需要维修时应保证所存储的国家秘密信息不被泄露

111、涉密计算机信息系统选用的硬件设备，应尽量选用国产机型，必须使用国外产品时，在安装和启用前，应当由 (A) 进行保密性能检查。

- A、所在地同级保密工作部门 B、自治区国家保密局
C、本单位保密工作部门

112、涉密计算机信息系统经过 (C) 后方可投入使用。

- A、保密检查 B、保密测试 C、申报审批

113、行政机关对政府信息不能确定是否可以公开时，应当依照法律、法规和国家有关规定报有关主管部门或者 (B) 确定。

A、上级保密工作部门 B、同级保密工作部门 C、自治区国家保密局

114、（ A ）同志曾指出：“必须十分注意保守秘密，九分半不行，九分九也不行，非十分不可。”

A、毛泽东 B、周恩来 C、朱德

115、1988 年 9 月 5 日颁布的《中华人民共和国保守国家秘密法》是由（ B ）通过的。

A、全国人民代表大会 B、全国人民代表大会常务委员会
C、全国人民代表大会委员长会议

116、个人参加会议带回的涉密文件资料应（ B ）。

A、由个人妥善保管 B、交保密室登记、管理 C、自行销毁

117、《中华人民共和国刑法》规定：违反保守国家秘密法规，故意或过失泄露国家军事秘密，情节特别严重的，处（ C ）以下有期徒刑。

A、三年 B、五年 C、五年以上十年

118、汇编涉密文件资料，其密级（ C ）进行标识。

A、应按多数文件的密级 B、至少应按机密级 C、应按所采用文件资料的最高密级

119、存储涉密信息的硬盘、软盘、光盘、磁带等介质，应当按照（ C ）划定秘密等级，并按照涉密载体安全保密要求进行管理。

A、存储涉密信息的数量 B、使用者的身份 C、存储信息的最高密级

120、传递绝密级秘密载体，（ C ）。

A、只能通过机要交通递送 B、只能通过机要交通、机要通信传递 C、只能通过机要交通、机要通信传递或者派专人直接递送

121、中央保密委员会 《党政领导干部保密工作责任制的规定》中所指的党政领导干部是指在党和国家机关担任（ A ）的干部。

A、县处级以上含县处级 B、县处级以上不含县处级
C、司局级以上含司局级

122、国家秘密是关系国家的安全和利益，依照（ B ）确定，在一定时间内只限一定范围的人员知悉的事项。

A、法律规定 B、法定程序 C、有关法规规章

123、《印刷、复印等行业复制国家秘密载体暂行管理办法》中所指的国家秘密载体，特指依法确定为国家秘密事项，标有密级的（ A ）。

A、文件、资料、图表、书刊 B、文件、资料、图表、书刊及电磁信息载体 C、文件、资料、图表、书刊及音像制品

124、国家秘密是在一定时间内只限（ C ）知悉的事项。

A、县处级以上领导干部 B、共产党员 C、一定范围的人员

125、凡是向国际互联网的站点提供或发布信息，都必须经过（ A ）的审查批准。

A、本部门 B、保密部门 C、本部门的上级机关

126、《保密法》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（ B ）的义务。

A、党和国家工作秘密 B、国家秘密 C、企业商业秘密

127、某国家机关工作人员，未经批准，私自留存国家秘密文件，他的行为属于(A)行为。

- A、违反保密规定的
- B、非法持有国家秘密的犯罪
- C、违反国家机关工作人员职业道德的

128、复制绝密级秘密载体，应当经(A)批准。

- A、密级确定机关、单位或者其上级机关
- B、密级确定机关、单位的上级机关或上级保密工作部门
- C、本机关、单位领导

129、国家秘密事项的密级需要变更时，一般(C)。

- A、只能由确定密级的机关、单位及时变更
- B、只能由上级机关直接变更
- C、由原确定密级和保密期限的机关、单位决定，也可以由其上级机关决定

130、泄密案件查处工作的基本程序包括(A)。

- A、立案、调查和处理
- B、立案、处理和执行
- C、调查、处理和检查

131、根据《行政机关公务员处分条例》的相关规定，泄露国家秘密、工作秘密，或者泄露因履行职责掌握的商业秘密、个人隐私，造成不良后果且情节严重的，给予(C)。

- A、警告、记过或者记大过处分
- B、降级或者撤职处分
- C、开除处分

132、根据《关于国家秘密载体保密管理的规定》，制作秘密载体，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，(B)。

A、绝密级、机密级、秘密级的都应编排顺序号

B、绝密级、机密级的应编排顺序号

C、秘密级的应编排顺序号

133、紧急情况下，传递国家秘密信息(B)。

A、可以使用普通传真机

B、可以使用经国家密码管理委员会批准使用的商用密码传真机

C、不能使用普通传真机或商用密码传真机

134、某工作人员外出执行任务时手提包被窃，后又找回，发现包内的钱物丢失，文件袋里的涉密文件完整无缺。这一事件(C)。

A、不应视为泄密事件 B、属于违纪行为

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

135、某文件标明“绝密★”，表示密级为绝密，保密期限为(A)。

A、30年 B、20年 C、长期

136、在任何情况下，都禁止将(A)级秘密载体携带出境。

A、绝密 B、机密 C、秘密

137、我市某单位有一份涉密文件要寄往杭州，应通过(C)传递。

A、挂号信 B、邮政特快专递 C、机要通信

138、对外经济合作中所提供资料的保密工作，由(B)具体负责。

A、业务主管机关 B、对外经济合作项目的主办单位

C、保密工作部门

139、国家秘密载体保密管理的原则是(C)。

A、领导负责进行管理 B、各处室严格进行保管

C、严格管理、严密防范、确保安全、方便工作

140、新闻、出版工作者工作中接触的国家秘密事项，非经（ B ）同意，不得擅自公开发表。

A、保密部门 B、主管部门 C、同级人民政府

141、新闻出版保密审查，实行（ C ）的制度。

A、送审 B、自审 C、自审与送审相结合

142、涉密会议的保密工作，主要包括会议保密工作方案的制订，会议过程中各项保密措施的落实，对会议有关人员的保密管理，以及会议（ A ）的选择等。

A、场所和设备 B、人员 C、时间

143、《中国共产党纪律处分条例》规定：“丢失秘密文件资料或泄露党和国家秘密，情节较重的，给予（ C ）处分”。

A、警告或严重警告 B、开除党籍 C、撤销党内职务或留党察看

144、泄密事件查处工作应当坚持（ A ）和依法办事的原则。

A、实事求是 B、求真务实 C、突出重点

145、对保密期限内的国家秘密事项，根据情况变化，可以及时解密的是（ C ）。

A、该事项泄露后对国家的安全和利益损害程度发生明显变化的

B、因工作需要，原接触范围需作较大改变的

C、该事项公开后无损于国家的安全和利益或从全局衡量公开后对国家更为有利的

146、以下关于国家秘密和商业秘密的表述，错误的是（ C ）。

A、国家秘密关系国家的安全和利益；而商业秘密仅仅是涉及权利人经济利益和竞争优势的信息

B、国家秘密未经法律授权的机关审查批准，任何人不得擅自对外提供或转让；而商业秘密只要不损害他人权利或公共利益，是可以随意转让的

C、国家秘密有可能转化成商业秘密，而商业秘密是不可能转化成国家秘密的

147、机关、单位内部集中制作、存储、保管国家秘密载体的专用、独立、固定场所，应确定为（ B ）。

A、保密要害部门 B、保密要害部位 C、重点涉密岗位

148、召开涉密会议，禁止使用（ A ）。

A、无线话筒 B、有线话筒 C、加密电视电话会议设施

149、对外提供资料的保密审批原则是（ C ）。

A、国家保密局统一管理，统一审批

B、各级保密部门统一管理，省级以上保密部门审批

C、业务主管部门归口管理，分级审批

150、在对外经济合作工作中，原则上不能对外提供绝密级国家秘密资料，确需对外提供的，必须报请（ C ）。

A、省级有关业务主管部门审批，或者由省级有关业务主管部门审核后报请省国家保密局审批

B、国务院有关业务主管部门审批，或者由国务院有关业务主管部门审核后报请国家保密局审批

C、国务院有关业务主管部门审批，或者由国务院有关业务主管部门审核后报请国务院审批

151、涉密计算机信息系统应当由(B)单位承建。

A、计算机信息系统集成资质

B、具有涉密计算机信息系统集成资质的

C、省级公安机关认定的

152、处理涉及国家秘密信息的计算机信息系统,(B)。

A、未处理国家秘密信息时可以上国际互联网

B、严禁上国际互联网和其他公共网络

C、加“防火墙”后可以上国际互联网

153、携带涉密笔记本电脑和移动存储介质外出,应当办理携带外出审批手续,并经主管领导批准,报(A)。

A、单位保密组织备案 B、国家安全局 C、保密局

154、计算机信息系统国际联网的保密管理,实行(C)的原则。

A、控制源头、归口管理 B、分级负责、突出重点

C、控制源头、归口管理、分级负责、突出重点、有利发展

155、在涉密信息系统中用于保障涉密信息安全的软件,必须采用经(C)推荐或认可的产品。

A、公安部门 B、国家安全部门 C、国家保密部门

156、各级机关、单位发生重大泄密事件,在向其主管部门报告的同时,应直接向(B)报告。

A、同级保密部门 B、国家保密局 C、上级保密部门

157、处理、存储机密级、秘密级的移动存储介质,应存放在(A)中。

A、密码保险柜 B、铁质密码文件柜 C、铁质文件柜

158、涉密信息系统投入运行后，还要进行有针对性的(B)。

A、保密教育 B、保密技术专项检查 C、保密审批

159、处理(A)信息的计算机，要采用低泄射的信息设备，或安装使用经国家保密部门批准使用的电磁干扰器。

A、秘密级或机密级 B、工作秘密 C、商业秘密

160、销毁涉密笔记本电脑和移动存储介质，在履行审批和备案手续后，可到保密部门指定的(C)进行销毁。

A、国家秘密载体定点复制单位 B、废品收购站点

C、国家秘密载体定点销毁单位

161、“保守国家秘密”是(A)的一项基本义务。

A、每个公民 B、国家公务员 C、领导干部

162、发生泄密事件的机关、单位，应当在发现后(A)内，书面向保密工作部门或机构报告；泄密事件的查处终结期一般为()。

A、24 小时，三个月 B、36 小时，一个月 C、48 小时，两个月

163、重点涉密人员是指掌握、知悉、使用、管理(B)的人员。

A、秘密级以上国家秘密(含秘密级) B、机密级以上国家秘密(含机密级) C、绝密级以上国家秘密(含绝密级)

164、绝密级国家秘密文件、资料和其他物品(B) 办理《中华人民共和国国家秘密载体出境许可证》。

A、可以 B、不得 C、视具体情况

165、《刑法》规定，情节严重的过失泄露国家秘密是一种(B)

行为。

A、错误 B、犯罪 C、过失

166、任何单位或个人不得在进入国际互联网的计算机或网络中存储、处理、传递涉及（ A ）的信息，计算机信息系统国际联网信息保密管理实行（ ）的原则。

A、国家秘密，谁上网谁负责 B、工作秘密，网管中心负责
C、商业秘密，网站负责

167、经管国家秘密事项的专职人员出境，国务院有关主管机关认为将对国家安全造成危害或者对国家利益造成重大损失的，（ B ）批准出境。

A、可以 B、不得 C、视具体情况

168、复制属于国家秘密的文件、资料，应当由（ C ）批准，并且（ ）保密期限。

A、保密部门；需重新制定 B、上报机关批准；需重新计算
C、密级确立机关、单位或其上级机关；不得改变其原件的

169、“保密工作需慎之又慎”，是（ A ）对保密工作的重要批示。

A、毛泽东 B、邓小平 C、江泽民

170、属于国家秘密的文件、资料和其他物品，由（ A ）标明密级。

A、确定密级的机关、单位 B、保密工作部门 C、确定密级的机关、单位的上级机关

171、按《保密法》规定，在有线、无线通信中传递（ B ）的，必须采取保密措施。

A、工作秘密 B、国家秘密 C、股市行情

172、国家秘密及其密级的具体范围，由（ A ）分别会同外交、公安、国家安全和其他中央有关机关规定。

A、国家保密行政管理部门 B、国家安全部门 C、中央办公厅

173、对是否属于国家秘密和属于何种密级不明确的事项由（ B ）确定。

A、本单位保密委员会 B、省、自治区、直辖市或其上级保密行政管理部门 C、单位一把手

174、复制属于国家秘密的文件、资料或摘录、引用、汇编属于国家秘密的内容形成的秘密载体，（ 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、可以改变

175、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

176、收发秘密载体，应当履行（ A ）手续。

A、清点、登记、编号、签收等 B、交接 C、签字

177、涉密人员、秘密载体管理人员离岗、离职前，应当将所保管的秘密载体全部清退，并（ C ）。

A、登记销毁 B、订卷归档 C、办理移交手续

178、违反《保密法》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

179、涉密机关单位违反《关于国家秘密载体保密管理规定》造

成泄密隐患的，由其（ C ）发出限期整改通知书。

A、所在行政区域的保密工作部门

B、所在系统的上级保密工作机构

C、所在行政区域的保密工作部门或所在系统的上级保密工作机构

180、目的地不通外交信使或外交信使难以携运的，确因工作需要，需要自行携运机密、秘密级国家秘密文件、资料和其它物品出境的应当向有关（ C ）申办《国家秘密载体出境许可证》

A、公安部门 B、海关 C、保密工作部门或保密工作机构

181、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（ A ）内，机密、秘密级（ ）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

182、泄密事件查处工作的终结期限为（ C ）。

A、六个月 B、一个月 C、三个月

183、国家工作人员在外地执行公务中发生泄密事件的，应当及时向当地（ C ）报告。

A、保密局 B、主管机关 C、保密局或公安机关

184、实行对外科技交流保密提醒制度的机关、社会团体、企事业单位应当（ B ）对执行情况至少进行一次自查，发现问题及时纠正。

A、每六个月 B、每年 C、每三个月

185、对是否属于国家秘密和属于何种密级有争议的，在未确定前，应按（ C ）进行管理。

A、绝密级 B、机密级 C、最高密级

186、涉及多部门共同查处的泄密事件，由当地（ B ）组织、协调。

A、政府 B、保密局 C、公安机关

187、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工作部门报告。

A、销毁 B、藏匿 C、邮寄

188、以下关于工作秘密的表述，正确的是（ B ）。

A、工作秘密的概念最早是在《反不正当竞争法》中提出的

B、工作秘密是涉及机关单位的公务活动和内部管理的事项

C、工作秘密属于国家秘密的范畴，所以是不能公开的

189、对在定密工作中因玩忽职守、不负责任造成错定、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

190、涉密信息处理场所应当按照国家的有关规定，与境外机构驻地、人员住所保持（ C ）的安全距离。

A、300 米 B、1000 米 C、相应

191、计算机信息系统的保密管理应实行（ C ）制。

A、分工负责 B、单位负责 C、领导负责

192、计算机信息系统的系统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

193、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

194、计算机信息系统应采取相应防（ C ）泄露的保密措施。

A、信息 B、密级资料 C、电磁信息

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

A、普通 B、一般 C、密级

196、《科学技术保密规定》中规定，“我国独有、受一定自然条件因素制约，并社会效益或者经济效益很大的传统工艺，”应确定为（ B ）事项。

A、内部 B、秘密级 C、机密级

197、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

198、国家科技秘密保密期限届满需要继续保密的，可以做出延长保密期限的决定，并在保密期限届满前（ B ）日通知有关单位和个人。

A、15 B、30 C、45

199、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、报刊杂志 B、广播电视 C、新闻出版

200、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 ）部门的指导和监督。

A、公安部门 B、工商部门 C、保密工作

201、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

202、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

203、存储过国家秘密信息计算机媒体不能（ B ）密级使用。

A、提高 B、降低 C、解除

204、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

205、不为公众所知悉，能为权利人带来经济利益，具有实用性并经权利人采取保密措施的技术信息和经营信息是（ B ）。

A、国家秘密 B、商业秘密 C、工作秘密

206、销毁秘密文件、资料要履行（ C ）手续。

A、清点 B、交接 C、审批、登记

207、向境外组织、机构或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、直辖市保密工作部门

B、国家保密工作部门

C、中央机关保密工作部门

208、新修订的《中华人民共和国保守国家秘密法》是第十一届

全国人民代表大会常务委员会（ C ）会议通过的

A、第十二次 B、第十三次 C、第十四次

209、新闻出版的保密工作，要坚持（ A ）的方针。

A、既保守国家秘密又有利于新闻出版工作正常进行

B、自审和送审相结合

C、新闻出版单位与业务部门共同负责

210、1995 年 1 月，国家保密局会同有关部门，依据（ B ）的规定制定并发布了《科学技术保密规定》。

A、《保密法》和《科学技术保密条例》 B、《保密法》和《科学技术进步法》
C、《保密法》及其《实施办法》

211、叛逃罪是指国家机关工作人员或掌握国家秘密的国家工作人员在（ A ），叛逃境外或在境外叛逃，危害国家安全的行为。

A、履行公务期间，擅离岗位 B、境外旅游 C、出国探亲

212、县以上各级人民政府的保密工作部门是（ B ）。

A、各级党委的办事机构 B、各级人民政府的职能机构

C、非常设机构

213、处理秘密级、机密级信息的系统，系统安全保密管理人员应当定期审查系统日志并作审查记录，审查周期不得长于（ C ）。

A、一周 B、15 天 C、一个月

214、国家秘密技术在国内转让，应当经（ B ）批准。

A、技术完成单位 B、技术完成单位的上级主管部门

C、保密工作部门

215、为了加强对国家秘密载体复制活动的管理，国家对印刷、复印等行业实行向（ C ）注册备案的制度。

A、上级业务主管部门 B、工商行政管理部门 C、政府保密工作部门

216、到本机关、单位自办的定点复制单位复制国家秘密载体，其准印手续，由（ C ）确定。

A、本机关、单位自行 B、本机关、单位自行 C、本机关、单位的保密工作机构自行

217、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（ B ）的规定确定密级。

A、行业规定 B、密级具体范围 C、法律规定

218、机关、单位对国家秘密事项确定密级时，应当根据情况确定（ C ）。

A、保密时间 B、保密范围 C、保密期限

219、具有国家秘密内容的会议和其他活动，主办单位应当采取（ A ），并对参加人员进行保密教育，规定具体要求。

A、保密措施 B、安全措施 C、安全保卫措施

220、未经有关主管部门（ B ），禁止将属于国家秘密的文件、资料和其他物品携带、传递、寄运至境外。

A、同意 B、批准 C、授权

221、任用经管国家秘密事项的专职人员，应当按照（ A ）和人事主管部门的规定予以审查批准。

A、国家保密工作部门 B、组织部门 C、公安部门

222、机关、单位应当对工作人员进行保密教育，（ A ）检查保密工作。

A、定期 B、不定期 C、定时

223、县以上地方各级政府的保密工作部门，在上级保密工作部门的指导下，依照保密法律、法规和规章（ B ）本行政区域的保密工作。

A 监督 B、管理 C、检查

224、涉及国家秘密的机关、单位，应当进行经常性的（ A ），落实各项保密措施，使所属人员知悉与其工作有关的保密范围和各项保密制度。

A、保密教育和检查 B、保密教育 C、保密检查

225、接触国家秘密事项的人员或者机关、单位的范围，由（ A ）的机关、单位限定。

A、确定密级 B、保密部门确定 C、上级确定

226、对泄露国家秘密尚不够刑事处罚，有下列情节之一的，应当从重给予行政处分：（ A ）；以谋取私利为目的泄露国家秘密的；泄露国家秘密危害不大但次数较多或者数量较大的；利用职权强制他人违反保密规定的。

A、泄露国家秘密已造成损害后果的

B、泄露国家秘密未造成损害后果的

C、多次泄露国家秘密已造成损害后果的

227、（ A ）是指违反保密法律、法规和规章的下列行为：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。

A、泄露国家秘密 B、泄密事件 C、窃密事件

228、涉密机关、单位收到秘密载体后，由（ B ）根据秘密载体的密级和制发机关、单位的要求及工作的实际需要，确定本机关、

单位知悉国家秘密人员的范围。

A、领导 B、主管领导 C、分管领导

229、保存秘密载体，应当选择（ C ）的场所和部位，并配备必要的保密设备。

A、独立 B、安全 C、安全保密

230、发生泄密事件的机关、单位的保密工作机构应当尽快向上级主管机关的保密工作机构和当地（或同级）政府的（ C ）报告，并立即进行查处工作。

A、公安部门 B、国家安全部门 C、保密工作部门

231、计算机信息系统联网应当采取系统访问控制、数据保护和系统（ C ）等技术措施。

A、保密技术 B、保密技术检查 C、安全保密监控管理

232、为确保涉密信息安全保密，应当严格禁止从互联网或其他公共信息网络直接向涉密计算机拷贝信息。如果确因工作需要拷贝的，可以先将要拷贝的资料刻录到（ B ）中，再通过该移动存储介质将拷贝的资料复制到涉密计算机上。

A、空白优盘 B、空白光盘 C、空白移动硬盘

233、涉密人员是指（ A ）国家秘密的人员。

A、掌握、知悉和管理 B、知悉 C、管理

234、国家保密局《关于加强保密工作依法行政的意见》指出，保密工作部门是政府主管保密工作的（ B ），其一切管理行为都必须依法行政。

A、工作部门 B、职能部门 C、办事机构

235、有效保护经济和科技领域的国家秘密是强化保密管理的重要内容，（ B ）和国有企业、科研院所要在管好国家秘密的基础上，把本行业、本单位的工作秘密和商业秘密以及传统工艺秘诀管住管好。

A、各级保密工作部门 B、经济、科技主管部门 C、党政机关

236、密级鉴定工作，是指（ B ）。

A、办案机关对其办理的案件中涉嫌涉及国家秘密事项作出的鉴别和认定

B、保密工作部门按照管辖范围，应办案机关的提起对其办理的案件中涉嫌涉及国家秘密事项作出的鉴别和认定

C、保密工作部门对其办理的案件中涉嫌涉及国家秘密事项作出的鉴别和认定

237、以下关于书面形式的国家秘密密件的密级和保密期限的标志的表述中正确的是（ A ）。

A、在封面（或首页）的左上角表明密级和保密期限

B、在封面（或首页）的右上角表明密级和保密期限

C、在封面（首页）的左上角表明密级、右上角表明保密期限

238、省、自治区、直辖市保密工作部门进行密级鉴定，涉及（ B ）的，密级鉴定书应当报国家保密局备案。

A、行政案件 B、刑事案件 C、民事案件

239、密级鉴定应当以（ A ）作为依据。

A、被鉴定材料泄露时适用的保密范围的规定、有关保密法规及有效的密级变更和解密证明

B、鉴定机关鉴定时适用的保密范围的规定、有关保密法规及有效的密级变更和解密证明

C、办案机关提交被鉴定材料时适用的保密范围的规定、有关保密法规及有效的密级变更和解密证明

240、有关部门对密级鉴定的鉴定结论有争议的，可以（ C ）。

A、提请上级保密工作部门裁定，国家保密局的鉴定结论和裁定为最终结论

B、提请上级保密工作部门裁定，上级保密工作部门的鉴定结论和裁定为最终结论

C、提请上一级保密工作部门裁定，国家保密局的鉴定结论和裁定为最终结论

241、密级鉴定工作中所指的涉嫌涉及国家秘密事项，不包括（ A ）。

A、对标有国家秘密标志但已超过保密期限的文件、资料和其它物品是否仍然属于国家秘密以及属于何种密级，需要作出鉴别和认定的事项

B、对未标有国家秘密标志的文件、资料和其它物品是否属于国家秘密以及属于何种密级，需要作出鉴别和认定的事项

C、对标有国家秘密标志的文件、资料和其它物品的真伪，及其是否在保密期限内，是否变更密级或解密

242、根据《国家秘密技术出口审查暂行规定》，国家秘密技术是指关系到国家的安全和利益，依照有关保密的法律、法规的规定，划分为秘密级、机密级和绝密级的（ C ）。

A、发明、科技成果和传统工艺技术 B、发明、科技成果和专利技术 C、发明、科技成果和关键性技术

243、中央保密委员会《党政领导干部保密工作责任制的规定》是根据（ C ）制定的。

A、《中华人民共和国保密国家秘密法》

B、《中华人民共和国加强新形势下保密工作的决定》

C、《中华人民共和国保守国家秘密法》和《中共中央关于加强新形势下保密工作的决定》

244、实行保密工作依法行政，就是要严格依照法律、法规、规章所赋予保密工作部门的（ B ）等职权开展保密工作。

A、审批、决定、检查、处罚、裁决

B、审批、决定、检查、处罚、建议

C、审批、决定、检查、处罚、处分

245、根据《印刷、复印等行业复制国家秘密载体暂行管理办法》的规定，哪些企业和个人不得承担复制国家秘密载体的业务？

（ C ）

A、机关创办的内部印刷厂 B、国有企业 C、外商投资企业

246、“机密”级国家秘密是重要的国家秘密，泄露后会造成什么后果？（ C ）

A、使国家的安全和利益遭受特别严重的损害 B、使国家的安全和利益遭受损害 C、使国家的安全和利益遭受严重的损害

247、《刑法》规定：国家机关工作人员在履行公务期间，擅离岗位，叛逃境外或者在境外叛逃，危害中华人民共和国国家安全，情节严重的，处什么徒刑？（ C ）

A、处三年以上七年以下有期徒刑 B、处七年以上十五年以下有期徒刑 C、处五年以上十年以下有期徒刑

248、新形势下的保密工作要实行专门工作与群众路线、（ C ）相结合，依法管理国家秘密。

A、保密部门与党的领导 B、保密部门与其他部门
C、保密部门与业务部门

249、中央指出，要加强保密教育，使保密教育制度化、经常化、规范化，把保密教育纳入普法与（ C ）的教学内容。

A、各种党校、干校 B、各种普通、成人高等教育
C、各级党校、行政学院和其他干部培训机构

250、根据《中华人民共和国刑法》的有关规定，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（ B ）有期徒刑。

A、三年以下 B、三年以上七年以下 C、七年以上十年以下

251、在我国境内居住、工作的外国公民，应当按照什么规定，承担保守我国国家秘密的义务？（ B ）

A、国际惯例、根据条约、协定及合同
B、保密法律法规、根据条约、协定及合同
C、保密法律法规、国际惯例、协定及合同

252、中央《决定》要求，地方（ A ）人民政府，根据实际

情况设置保密工作机构，在其职权范围内主管本行政区域保守国家秘密的工作。

A、县级（含县）以上 B、地（市）级以上 C、各级

253、中央保密委员会《党政领导干部保密工作责任制的规定》中所指导的党政领导干部，是指在党和国家机关担任县（处）级以上（含县处级）领导职务的干部，包括在（ A ）担任相当县（处）级的党政负责人。

A、社会团体、事业单位以及国有大、中型企业

B、社会团体、事业单位 C、各种社会团体、企事业单位

254、保密工作部门要加强对同级政府各部门保密工作机构的业务（ A ）。

A、指导和监督 B、管理和协调 C、指导和协调

255、涉及国家秘密的计算机信息系统的建设，必须与保密设施的建设同步进行，报经（ A ）审批后，才能投入使用，未经保密审批的计算机信息系统不得处理国家秘密信息。

A、地（市）以上保密部门 B、县（市）以上保密部门

C、地（市）以上公安部门

256、涉及国家秘密的计算机信息系统的集成资质单位由（ B ）审定。

A、公安机关 B、保密部门 C、国家安全机关

257、省直各单位涉密信息系统的审批工作由（ C ）负责。

A、省直各单位保密组织 B、所在地（市）的保密局

C、省保密局

258、自治州、市、地区国家保密局负责（ A ）涉密信息系统的审批。

- A、同级和下级机关、单位
- B、同级机关、单位
- C、本单位

259、地（市）级以上各级保密局审批本行政区域内的涉密信息系统。跨区域的涉密信息系统由（ B ）审批。

- A、各所在地的保密局
- B、上一级保密局
- C、各单位保密组织

260、涉密信息系统的建设单位应制定《涉密信息系统安全保密方案》，并报经有审批权限的省、自治州、市、地区国家保密局（ C ）。

- A、备案
- B、存查
- C、审定

261、以下关于工作秘密和商业秘密的描述中，错误的是（ C ）。

- A、各级国家机关是产生工作秘密的主体
- B、企业、事业单位或其他社会团体大多数产生的是商业秘密
- C、工作秘密属于国家秘密，而商业秘密不属于国家秘密

262、涉密信息系统处理多种密级的信息时，应按（ C ）进行防护。

- A、少数信息的密级
- B、多数信息的密级
- C、信息的最高密级

263、涉密信息系统采用的安全保密设备原则上必须选用国产设备，在无相应国产设备时可选用经（ A ）批准的国外设备。

- A、国家主管部门
- B、保密部门
- C、信息产业部门

264、处理（ C ）信息的涉密信息系统的中心机房的门控系统

应采用 IC 卡或生理特征（如指纹、声音、视网膜等）进行身份鉴别，并配备电视监视系统。

A、秘密级 B、机密级 C、绝密级

265、处理绝密级信息的涉密计算机系统当身份鉴别尝试次数连续达到（ A ）次后，系统应自动通知安全保密管理人员，并锁定该用户账号，只有安全管理员有权恢复或重建该账号，且将有关信息生成审讯事件。

A、3 次 B、5 次 C、7 次

266、处理（ B ）信息的涉密信息系统，访问应当按照用户、信息类别控制。

A、机密级、绝密级 B、秘密级、机密级 C、绝密级

267、处理（ C ）信息的涉密信息系统，访问应当控制到单个用户、单个文件。

A、秘密级 B、机密级 C、绝密级

268、处理绝密级信息的涉密信息系统，系统安全保密管理员应当定期审查系统日志并作审查记录，审查记录不得更改、删除。审查周期不得长于（ C ）。

A、一个月 B、半个月 C、一周

269、处理（ A ）信息的涉密信息系统，系统应当能够检测并记录侵犯系统的事件和各种违规操作，并能及时告警。

A、绝密级 B、机密级 C、秘密级

270、处理（ B ）信息的涉密信息系统中使用的信息设备，可采取安装电磁干扰设备的措施，进行电磁泄漏防护。

A、机密级、绝密级 B、秘密级、机密级 C、绝密级

271、处理（ C ）信息的涉密信息系统中使用的信息设备，应采取电磁屏蔽的措施，进行电磁泄漏防护。

A、秘密级 B、机密级 C、绝密级

272、涉密信息系统中的秘密信息应有密级标识，密级标识（ A ）与正文分离。

A、不能 B、不一定 C、必须

273、使用计算机信息系统的单位的（ B ）负责本单位的计算机信息系统的保密管理工作。

A、分管领导 B、主管领导 C、网络安全保密人员

274、违反《计算机信息系统保密管理暂行规定》，由保密部门和保密机构（ C ）。

A、拆除、没收设备 B、没收设备、并处罚款 C、责令其停止使用，限期整改

275、与普通印制单位不同，承担一切国家秘密文件资料印制的印制单位，必须持有（ C ）。

A、《特种经营许可证》 B、《印刷经营许可证》

C、《国家秘密载体复制许可证》

276、保管秘密载体的工作人员离开办公场所，应当将秘密载体（ A ）。

A、存放在保密设备里 B、存放在私人抽屉 C、随身携带

277、推广应用国家秘密技术，应当选择（ C ）进行，有关人员均负有保守国家秘密的义务。

A、技术力量雄厚的单位 B、国有企业单位 C、有相应保密条件的单位

278、任用经管国家秘密事项的专职人员，应当按照（ C ）的规定予以审查批准。

A、国家保密工作部门 B、人事主管部门 C、国家保密工作部门和人事主管部门

279、涉密计算机安装从互联网下载或来历不明软件存在的泄密隐患主要是：（ A ）

A、被植入“木马”窃密程序 B、死机 C、盗版危害

280、复制和传递涉密电子文档，应当严格按照复制和传递（ B ）纸质文件的有关规定办理。

A、秘密级 B、同等密级 C、内部

281、涉密计算机及相关设备存储数据的恢复，必须到（ B ）进行。

A、销售单位 B、国家保密行政管理部门批准的涉密数据恢复资质单位 C、原生产单位

282、处理涉密信息的计算机、传真机、复印件等办公自动化设备应当在单位内部进行维修，现场有专门人员监督，严禁维修人员读取或复制涉密信息；确需送外维修的，应当（ A ）。

A、拆除涉密信息存储部件 B、对涉密信息存储部件进行加密处理 C、将涉密信息删除

283、涉密信息系统是指由计算机及其相关和配套设备、设施构成的，按照一定的应用目标和规则存储、处理、传输（ A ）信息的系统或者网络。

A、国家秘密 B、工作秘密 C、商业秘密

284、《中华人民共和国保守国家秘密法》由第十一届全国人民代表大会常务委员会第十四次会议修订通过，自（ B ）起施行。

A、2010 年 8 月 1 日 B、2010 年 10 月 1 日 C、2010 年 12 月 1 日

285、国家秘密及其密级的具体范围，由国家保密行政管理部门分别会同（ C ）和其他中央有关机关规定。

A、外交、国防、公安 B、国防、国家安全、司法
C、外交、公安、国家安全

286、为了解定密权责不清等问题，定密责任人首次写入了修订的《保密法》中，其中明确规定：机关、单位负责人及其指定的人员为定密责任人，负责（ C ）。

A、本机关、本单位的国家秘密审核、确定和落实工作
B、本机关、本单位的国家秘密确定、执行和督查工作
C、本机关、本单位的国家秘密确定、变更和解除工作

287、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（ B ）国家秘密。

A、绝密级、机密级和秘密级 B、机密级和秘密级
C、秘密级

288、机关、单位对外交往与合作中需要提供国家秘密事项的，应当（ C ）。

A、报本机关、本单位负责人批准
B、报原定密机关、单位批准
C、报国务院有关主管部门批准或者省、自治区、直辖市人民政府

府有关主管部门批准

289、某单位举办涉密会议，有一相关人员将手机关机后带入会场，该行为（ B ）。

A、没有违反相关规定，不存在泄密隐患

B、违反了相关规定，存在泄密隐患 C、纯属个人行为

290、根据国家保密规定，处理机密级信息的系统口令长度不得少于（ B ）位，且口令更换周期不得长于（ ）天。

A、8，30 B、10，7 C、12，3

291、传真国家秘密文件、资料，必须使用机要部门批准使用的加密传真机，其中（ C ）的信息不能通过加密传真机传输，应送当地机要部门译发。

A、绝密级、机密级和秘密级 B、绝密级和机密级

C、绝密级

292、根据《科学技术保密规定》中的相关条例，我国独有、不受自然条件因素制约、能体现民族特色的精华，并且社会效益或者经济效益显著的传统工艺应该划分成（ B ）科学技术秘密。 A、绝密级 B、机密级 C、秘密级

293、公众信息网保密管理基本原则是（ C ）。

A、控制源头、归口管理、分级负责、突出重点

B、加强检查、明确责任、分级负责、突出重点

C、控制源头、加强检查、明确责任、落实制度

294、在涉密信息系统的安全管理应当采取（ C ）的原则。

A、最高安全 B、相应安全 C、适度安全

295、电子政务网络由政务内网和政务外网构成，政务内、外网

之间应实行（ A ），政务外网与互联网之间实行（ ）。

- A、物理隔离；逻辑隔离
- B、逻辑隔离；物理隔离
- C、逻辑隔离；逻辑隔离

296、泄露国家秘密已经人民法院判处刑罚的以及被依法免于起诉或者免于刑事处罚的，应当（ A ）行政处分。

- A、从重给予
- B、从轻给予
- C、免于

297、按照《保密法》及其《实施办法》的规定，各机关、单位按有关保密范围“对号入座”地确定密级之后，（ B ）。

- A、需要报当地保密工作部门审批
- B、不需要报同级或上级保密工作部门审批
- C、需要报同级或上级保密工作部门审批

298、与香港、澳门特别行政区和台湾地区联网的计算机信息系统的保密管理，（ B ）。

- A、部分适用《计算机信息系统国际联网保密管理规定》
- B、参照《计算机信息系统国际联网保密管理规定》执行
- C、不适用《计算机信息系统国际联网保密管理规定》

299、定点复制单位不按规定张挂《国家秘密载体复制许可证》（简称《许可证》）的，县级以上政府的保密工作部门应当责令其立即张挂，对拒不执行的（ B ）。

- A、罚款 1000 元
- B、吊销其《许可证》
- C、吊销其营业执照

300、当属于国家秘密的文件、资料或其他物品下落不明时，认定构成泄密事件的时限是（ B ）。

- A、绝密级 30 年，机密级 20 年，秘密级 10 年

B、绝密级 10 日内，机密级、秘密级 60 日内

C、绝密级 24 小时内，机密级、秘密级 1 个月内

301、销毁纸介质秘密载体，送造纸厂销毁的，应当送（ C ）
销毁，并由送件单位 2 人以上押运和监销。

A、个体造纸厂 B、国有造纸厂

C、保密工作部门指定的厂家

302、《国家秘密载体复制许可证》由（ C ）统一印制。

A、市保密局 B、省保密局 C、国家保密局

303、阅读和使用秘密载体，应当（ B ）。

A、向管理人员索取，无需办理手续

B、办理登记、签收手续 C、根据实际情况灵活处理

304、紧急情况下向相关单位传递涉密资料时，可通过（ C ）
方式进行。

A、传真机 B、加密电子邮件 C、专人专车

305、以下哪种做法不符合保密规定？（ B ）

A、采用焚毁、化浆方法销毁纸介质秘密载体。

B、使用能碎成条状的碎纸机销毁纸介质秘密载体。

C、送保密工作部门指定的厂家销毁，并由二人以上押运和监销。

D、采用物理或化学的方法销毁磁介质、光盘等秘密载体。

306、涉密信息系统采用的口令，应由大小写英文字母、数字、
特殊字符中的（ B ）组成。

A、任何一种 B、两种以上 C、三种以上 D、四种全
部

307、军事禁区 and 属于国家秘密不对外开放的其他场所、部位，

应当采取保密措施，除依照国家有关规定经过批准外，(A) 对外开放或者扩大开放范围。

- A、不得擅自决定 B、可以自行决定 C、只能限定时段
D、也可视情适当

308、保密工作历来是党和国家的一项重要工作。革命战争年代，保密就是 (A)，和平建设时期，保密就是 ()。

- A、保生存、保胜利；保安全、保发展 B、保生存、保安全；保胜利、保发展
C、保胜利、保发展；保生存、保安全

309、关于国家秘密及其密级的具体范围的规定，应当 (C) 公布。

- A、向社会 B、在党政机关 C、在有关范围内

310、做好科学技术保密工作应当依靠 (C)。

- A、单位的保密工作部门 B、单位的保密工作人员
C、广大科技工作者

311、《国家公务员暂行条例》规定，国家公务员必须“保守国家秘密和工作秘密”。这是国家公务员的 (B)。

- A、纪律 B、义务 C、责任

312、互联网及其他公共信息网络运营商、服务商违反《保密法》相关规定的，由 (C) 按照各自职责分工依法予以处罚。

- A、保密部门、公安机关
B、保密部门、公安机关、信息产业主管部门
C、公安机关或国家安全机关、信息产业主管部门

313、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

314、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、企事业单位和公民

315、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

316、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

317、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

318、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

319、国家秘密的保密期限届满的，自行(C)

- A、变更 B、公开 C、解密

320、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

321、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

322、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式的涉密载体，(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

323、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

324、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

325、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，并派值班看守。

A、车间 B、仓库 C、文件柜

326、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

327、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

328、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指定的单位决定

329、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

330、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

331、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

332、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

333、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

324、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

325、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、人员住所保持(C)的安全距离。

A、300 米 B、1000 米 C、相应

326、计算机信息系统的保密管理应实行(C)，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，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

327、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

328、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

329、计算机和信息系统应采取相应的(C)泄漏的保密措施。

A、信息 B、密级资料 C、电磁

330、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

331、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

332、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

333、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

334、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

335、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

335、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

336、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

337、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

338、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，泄密事件处理

339、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(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

340、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

341、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

342、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

343、过失泄露绝密级()件机密级()件或秘密级()件的，应予立案。(C)

A、1，2，3 B、1，3，3 C、1，3，4

344、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

二、不定项选择题

1、使用手机的主要泄密问题和隐患是(ABCDE)。

A、通话中谈论涉密事项 B、发送涉密短信

C、拍摄涉密照片 D、带入核心涉密场所 E、录音涉密电话

2、针对手机的窃密手段是(ABCDE)。

A、窃听通话内容 B、窃听周围动静

C、远程控制开机和收发 D、测定手机位置 E、拦截手机短信息文字

3、国外情报机关依托电子监控系统，能够有效拦截(ABCDE)等电子信息达 95%。

- A、普通无线电话 B、普通有线电话 C、互联网电子邮件
D、手机短信 E、普通传真

4、我国目前可以传递国家秘密信息的通信渠道，主要有（AD）。

- A、点对点的加密通信系统
B、业务系统、行业建立的计算机或者传真机加密通信系统
C、各级政府建立的电子政务内网
D、全国机要系统的密码通信和加密传真系统
E、经批准使用的商用密码加密系统

5、目前我国手机市场上推出的多功能手机，已经具备的信息收集功能包括（ABCDE）。

- A、拍照和录像 B、录音 C、拷贝资料 D、下载文件
E、收听广播和电视

6、屏蔽手机可以达到这样几种防窃密的作用，包括（ABCDE）。

- A、防遥控 B、防定位 C、防窃听 D、防窃照
E、防电磁辐射

7、将手机带入核心涉密场所，会产生（ABCD）等危害后果。

- A、窃听 B、窃照 C、定位 D、录音、录象 E 拷贝文件

8、间谍手机具备的窃密功能，包括（ABCDE）。

- A、窃听通话内容 B、窃听现场动静 C、遥控对象手机
D、窃取手机存储的资料 E、对所窃听的内容进行录音

9、要使手机不涉密，必须做到（ABCDE）。

- A、不得带入涉密场所 B、不谈论秘密事项 C、不编发含有涉密内容的短信息 D、不对涉密内容进行拍照或者录音

E、不在手机中存储和拷贝涉密事项

10、屏蔽手机的主要方法，包括（ABCD）。

A、安装手机干扰器 B、携带手机进入屏蔽室 C、将手机放进屏蔽袋 D、将手机放进屏蔽箱 E、取下手机电池

11、存储载体通常包括（ABCDE）。

A、计算机硬盘 B、光盘 C、U 盘 D、移动硬盘
E、其他存储电子设备

12、使用涉密存储载体必须做到四个统一，即（ABDE）。

A、统一采购 B、统一登记 C、统一销毁 D、统一标识 E、统一管理

13、涉密计算机的登陆口令不能单由数字组成，且存储秘密级信息的登陆要求（A），存储机密级信息的登陆要求（D），存储绝密级信息的登陆要求（E）。

A、口令长度不少于八位，更换周期不得长于一个月
B、口令长度不少于六位，更换周期不得长于一个月
C、口令长度不少于六位，更换周期不得长于一年
D、口令长度不少于十位，更换周期不得长于一周
E、使用指纹、密钥等可靠的身份识别方式登陆

14、涉密计算机最主要的泄密隐患通常发生在（ABCDE）、淘汰换装等环节上。

A、选型采购 B、分类标识 C、安全防护 D、输入输出 E、维护维修

15、严禁存储载体公私混用的主要目的是（ABCE）。

A、避免将办公用存储载体错带回家造成失控

B、避免在属于私人的存储载体上拷贝上涉密信息变成涉密载体

C、避免涉密信息通过非涉密载体扩散

D、避免私用存储载体传播有害的计算机病毒

E、避免办公用的涉密存储载体误操作连接在互联网上造成泄密

16、登记涉密存储载体应当包括以下主要内容，即（ABCDE）。

A、购买日期 B、载体类别 C、所涉最高密级 D、序

列编号 E、领用人签名及日期

17、维修涉密存储载体应当采取这样一些保密措施（ABCD）。

A、在保密工作部门批准定点单位维修

B、由经保密资格审查合格的人员从事维修工作

C、将涉密计算机硬盘取下后再行维修

D、在涉密单位派人监管的情况下维修

E、严禁直接将涉密存储载体连接在互联网上实施下载应用软件

18、目前国外使用高灵敏度专用接受设备可在（E）距离上接收并还原计算机电磁辐射的信息，因此处理绝密信息必须使用符合国家标准低辐射计算机，处理机密和秘密信息必须使用符合国家标准低辐射计算机，处理机密和秘密信息必须使用符合国家技术要求的电磁泄露干扰设备。

A、200 米 B、400 米 C、600 米 D、800 米

E、1000 米

19、登记涉密计算机硬盘序列号和做出密级标识的目的是（ABCDE）。

A、防止涉密存储载体被调包 B、防止涉密存储载体被盗

C、防止涉密存储载体遗失 D、防止涉密存储载体随意出售

或转让 E、防止涉密存储载体通过不安全渠道传递等

20、国家对计算机信息系统的安全保护等级分为（A）。

- A、绝密、机密、秘密 B、国家秘密、工作秘密、商业秘密
- C、一级、二级、三级 D、一级、二级、三级、四级、五级
- E、特别级、普通级

21、由于网络存在（ABCDE）等危险，因此必须与互联网等公共网络实行物理隔离。

- A、木马遥控 B、黑客窃密 C、引擎搜索 D、“后门”入侵
- E、屏幕抓取

22、维护和维修涉密计算机及其网络，必须严格采取（BCDE）等保密防范措施。

- A、在本单位内部场所进行
- B、送保密部门定点维修单位进行
- C、指定专人全过程监督
- D、严禁维修人员读取和复制涉密信息
- E、拆除涉密信息存储部件后送出维修

23、为防范涉密计算机及其网络内部攻击和窃密，必须采取（ABCDE）等保密措施。

- A、设置八位以上的登陆口令 B、定期更换登陆口令
- C、根据工作需要设置访问权限 D、安装符合要求的审计系统 E、安装非法接入或接出的报警系统

24、确保“涉密信息不上互联网，上互联网信息不涉密”，必须对审查上网信息采取（ABCDE）等科学的管理办法。

- A、建立专门审查队伍 B、统一保密审查标准

C、规范保密审查程序 D、落实保密审查责任

E、实行泄密“一票否决制”

25、各机关单位加强对计算机信息系统的安全和保密管理，必须落实（ABCDE）等保障措施。

A、有一名主要领导负责计算机信息系统的安全和保密管理

B、确保必要的经费投入

C、指定一个工作机构具体负责计算机信息系统安全和保密综合管理

D、各部门内设机构应当指定一名信息安全保密员

E、建立健全计算机信息系统安全和保密管理制度

26、涉密网络及其计算机终端，严禁使用含有无线互联网功能的（ABCDE）等设备。

A、无线网卡 B、无线鼠标 C、无线键盘 D、蓝牙

E、红外

27、计算机网络的防病毒措施应当包括（ABCDE）等。

A、安装防病毒软件 B、定期升级和更新杀毒软件

C、及时更新操作系统补丁程序

D、不安装、运行、使用与工作无关的软件

E、不随意开启来路不明的电子邮件

28、为防范木马“摆渡”应当采取（ABCDE）的安全保密措施。

A、不在涉密计算机及其网络和非涉密计算机及其网络间交叉使用移动存储

B、不在非涉密计算机及其网络中使用涉密移动存储设备

C、将互联网上的信息复制到处理内部信息的系统时，应当采取

严格的技术防范措施，查杀病毒、木马等恶意代码，严防病毒等传播

D、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

E、不使用移动存储设备从涉密计算机向非涉密计算机复制数据，确需复制的应当采取严格的保密措施

29、加强对计算机使用人员的保密管理，应当落实（ABCDE）等的措施。

A、开展经常性的保密教育培训，提高计算机使用人员的安全保密意识和技能

B、与重点岗位的计算机使用人员签订安全保密责任书，明确安全保密要求与责任

C、加强计算机使用人员执行相关保密制度的情况进行监督检查

D、严肃查处计算机使用人员的违规和泄密行为

E、计算机使用人员离岗离职，应当及时取消其计算机信息系统访问权限，收回计算机、移动存储设备等相关物品

30、对录有秘密级以上公文的（ABCD）等应按同密级的公文管理。

A、计算机磁盘 B、光盘 C、磁带 D、U 盘

31、根据《保密法实施办法》对外经济合作提供国家秘密文件、资料需要具备以下哪些条件（ABDE）。

A、对方以正当理由和途径要求提供 B、根据平等互利的原则

C、根据利大于弊的原则

D、事先呈报有相应权限的国家主管部门批准

E、通过一定形式要求对方承担保密

32、传递秘密载体所用的信封或袋牌应当标明（ACD）。

A、收发件单位 B、密件清单 C、密级 D、编号

33、国家秘密载体是指以（ABCD）方式记载国家秘密信息的各类物品。

A、文字 B、图形与图像 C、数据与符号 D、视频与音频

34、收发秘密载体，应当履行（ABCD）等手续。

A、签收 B、登记 C、编号 D、清点

35、销毁秘密载体，应当（ABCD）。

A、履行清点手续 B、经本单位主管领导批准
C、履行登记手续 D、确保信息无法还原

36、根据《关于国家秘密载体保密管理的规定》，制作秘密载体应（ABCD）。

A、标明密级 B、标明保密期限 C、注明发放范围
D、注明制作数量

37、涉密单位收到秘密载体后，由主管领导根据（ABC）确定本单位知悉该国家秘密人员的范围。

A、秘密载体的密级 B、制发单位的要求
C、工作的实际需要 D、个人偏好

38、因工作需要携带秘密载体外出（境内），应（AC）。

A、采取必要的保护措施
B、在住宿外出时交由宾馆总台妥善保存
C、使其处于携带人的有效控制之下
D、经单位领导批准后可携带绝密级秘密载体参加涉外活动。

39、涉密计算机中的硬盘需要销毁的，应将硬盘进行专业的销密处理，确保信息无法还原。下列处理措施中仍存在泄密隐患的是（AC）。

- A、删除硬盘中的涉密信息 B、将硬盘物理损坏
- C、在 DOS 下将硬盘格式化
- D、使用符合国家保密标准的设备完全擦除硬盘信息

40、报刊、（ABCD）的出版和发行应当遵守有关保密规定，不得泄露国家秘密。

- A、书籍 B、地图 C、图文资料 D、声像制品

41、在公开的科学技术展览、新闻出版、（ABCD）等活动中，不得涉及国家科学技术秘密。

- A、讲学 B、进修 C、考察 D、合作研究

42、信息安全保密的中心任务是：确保信息的（ABCDEF）。

- A、保密性 B、电磁泄漏发射防护 C、完整性
- D、可用性 E、运行安全 F、抵赖性

43、处理绝密级信息的系统中心机房应（ACD）。

- A、配备警卫人员 B、有效的密码式电子门控系统
- C、IC 卡 D、电视监视系统

44、涉密计算机口令字的设置要根据计算机所处理的涉密信息的密级决定，其中处理机密级信息的计算机所设置的口令应符合的条件为（ACD）。

- A、长度不得少于 10 个字符 B、长度不得少于 8 个字符
- C、应采用字母、数字、特殊字符组合
- D、更新周期不能超过一周

E、更新周期不能超过一个月

45、涉及国家秘密的信息，不得在国际联网的信息系统中（ABCD）。

A、存储 B、处理 C、传输 D、发送

46、系统分析应包含主要几方面内容（ABCDEF）。

A、系统的资源 B、用户、网管人员 C、电磁环境

D、应用系统 E、物理环境 F、网络结构

47、涉密系统应具有对（ABCDE）进行统一管理的安全保密管理系统。

A、网络用户 B、信息类别 C、网络资源

D、管理人员 E、安全保密产品

48、安全保密性能检测的内容包括（ABCE）。

A、系统的安全漏洞 B、网络的安全漏洞

C、私自上互联网 D、嵌入式隐患

E、安全保密强度

49、安全保密产品应具有（BC）认证许可的产品才可应用于涉密系统或重要的信息系统中。

A、科技部 B、公安部 C、保密局 D、信息产业部

50、涉密人员、秘密载体管理人员离岗、离职前，应当（AC）。

A、将所保管的秘密载体全部清退

B、将所保管的涉密载体全部销毁

C、办理移交手续 D、作为自己的劳动成果个人留存一份

51、涉密计算机使用过程中，下列行为存在泄密隐患的是（ABC）。

A、连接手机 B、连接有线电视

C、连接私人 MP3、数码相机

52、确因工作需要，从互联网及其他公共信息网络上将所需数据复制到涉密计算机及网络，下列方式符合保密要求的是（BC）。

A、直接使用优盘

B、使用国家保密行政管理部门批准的信息单向导入设备

C、将要拷贝的资料刻录到空白光盘中，再通过光盘将资料复制到涉密计算机上

53、根据《保密法实施办法》，以下情形应当从重给予行政处分的有（ABCD）。

A、泄露国家秘密已造成损害后果的

B、以牟取私利为目的泄露国家秘密的

C、泄露国家秘密危害不大但次数较多或者数量较大的

D、利用职权强制他人违反保密规定的

54、传递属于国家秘密的文件、资料和其他物品的方法，不准通过（ABC）。

A、普通邮政传递 B、电子邮件传递 C、明码电报传递

55、下列法律法规和章程中对公民和特定公民群体的保密责任和义务作出了规定的有（ABCDEFG）

A、《中华人民共和国宪法》

B、《中华人民共和国保守国家秘密法》

C、《中华人民共和国刑法》

D、《中华人民共和国国家安全法》

E、《中华人民共和国公务员法》

F、《最高人民检察院关于渎职侵权犯罪案件立案标准的规定》

G、《中国共产党章程》

56、公民履行好保密义务应做到（ABCDEF）

A、发现窃密、泄密、违反保密规定等情况时及时向有关部门举报、劝阻和制止

B、拣拾到国家秘密载体时及时上缴，不得私自扩散、留存

C、遵守保密规定，对知悉的国家秘密不得在公众网络、公开报刊、信件等载体上发布、谈论和传播

D、不得非法获取或者非法持有国家秘密 E 不得为境外机构、组织和人员窃取、刺探、收买以及非法提供国家秘密

E、提高保密意识，不该看的不看、不该听的不听、不该记录的不记、不该说的不说

F、对于有机会接触国家秘密的亲朋好友进行提醒

57、《保密法》适用于一切（ABCDEF）

A、国家机关 B、武装力量 C、政党 D、社会团体

E、企事业单位 F、公民

58、国家秘密三个基本组成要素是（ABC）

A、关系国家安全和利益 B、依照法定程序确定

C、在一定时间内只限一定范围人员知悉

59、需要确定为国家秘密的有：（ABCDEFGH）

A、危害国家政权的巩固和防御能力

B、影响国家统一、民族团结和社会安定

C、损害国家的政治、经济利益

D、影响国家领导人、外国要员的安全

E、重要的安全保卫工作

F、使保护国家秘密的措施的可靠性降低或失效

G、削弱国家的经济、科技实力

H、使国家机关依法行使职权失去保障

60、制定《保密法》的宗旨是（ABC）

A、为了保守国家秘密 B、维护国家的安全和利益

C、保障改革开放和社会主义建设事业的顺利进行

61 不符合涉密计算机信息系统应用要求的是(ABD)

A、超越系统密级处理信息

B、用没有保密防范措施的传真机传输涉密文件资料

C、网络终端未连接非涉密网络

D、系统无安全保密措施

62、符合保密组织机构建设要求的是(ABC)

A、组织机构健全 B、坚持例会并有完整记录

C、组织机构发挥了组织协调、检查、指导作用

D、长期无领导分管

63、不符合涉密计算机管理要求的是(AC)

A、未安装防病毒软件 B、安装了违规上互联网监管软件

C、无有效身份认证 D、严禁使用无线鼠标、键盘

64、领导干部应当履行的保密工作职责有(ABCD)

A、选配保密干部从事日常的保密管理工作

B、有计划地开展保密宣传教育工作

C、对涉密的通信采取保密技术防范措施

D、对涉密会议、活动采取保密措施

65、党政领导干部执行了保密工作责任制的有(ABD)

A、工作有部署、有检查、有总结

B、组织机构健全、职责明确

C、人员变动调整不及时

D、能研究、解决和落实保密重大问题

66、书面形式的密件，在封面的（A）标明密级和保密期限；地图、图纸、图表在其标题之后或者（D）标明密级和保密期限。

A、左上角 B、右上角 C、上方 D、下方

67、阅读国家秘密文件时不符合要求的是(ACD)

A、让非指定阅读的人员一起阅读

B、在有保密保障的场所进行

C、用自己的名字登记完后传给其他人看

D、擅自存留国家秘密文件

68、通信系统是由交换设备、传输设备和终端设备组成的，泄密隐患主要有（ABCD）

A、有线传输线路辐射泄密 B、网络串音泄密

C、无线传输泄密 D、通信设备电磁泄漏发射泄密

69、使用手机的主要泄密隐患是（ABC）

A、通话中谈论涉密事项

B、在待机状态下带入重要涉密会议

C、在关机状态下带入重要涉密会议

D、在进入重要涉密场所前将电池取出

70、推行保密工作标准化管理的指导思想是：（ABC）

A、遵循“积极防范、主动作为、夯实基础、创新突破”的要求，坚持国家秘密、工作秘密、商业秘密齐抓共管

B、着力加大宣传教育培训力度，着力增强技术防范能力，着力提升检查督查水平

C、加快保密工作转型升级，努力实现“全领域覆盖、全过程监管、全方位服务”

71、涉密计算机使用过程中，下列哪些行为存在泄密隐患：
(ABC)

A、连接手机 B、连接有线电视 C、连接 MP3、数码相机等私人存储介质。

72、确因工作需要，从互联网及其他公共信息网络上将所需数据复制到涉密计算机及网络，下列哪些方式符合保密要求：(BC)

A、直接使用优盘 B、经保密行政管理部门批准使用的信息单向导入设备 C、使用一次性刻录光盘

73、关于涉密计算机身份鉴别方式，下列哪些做法符合保密规定：
(ABC)

A、秘密级计算机口令设置长度不少于 8 位，更换周期不超过 1 个月

B、机密级计算机采用 IC 卡或 USB Key 与口令相结合的方式，且口令长度不少于 4 位；如仅使用纯口令方式，则长度不少于 10 位，更换周期不超过 1 个星期

C、绝密级计算机采用生理特征（如指纹、虹膜等）等强身份鉴别方式

74、涉密计算机不得使用下列哪些设备：(ABC)

A、无线键盘 B、无线鼠标 C、无线网卡

75、下列哪些行为不符合涉密移动存储介质保密管理要求：(AC)

- A、通过普通邮局邮寄
- B、统一登记、编号，按密件保管
- C、随意交由他人使用

76、确因工作需要，经批准携带涉密笔记本电脑及移动存储介质外出，下列哪些做法不符合保密要求：（ABC）

- A、交由知悉范围以外的人员代为保管
- B、交由宾馆代为保管
- C、留在宾馆房间写字台抽屉内

77、淘汰处理的涉密存储介质和涉密计算机、传真机、复印机等设备的信息存储部件，不正确的做法是（BC）。

- A、送交保密行政管理部门销毁工作机构销毁
- B、进行格式化后赠送或改作其他用途
- C、卖给废品回收单位

78、依法确定工作秘密事项，必须同时具备以下（ ）条件。（ABC）

- A、公开后可能危及国家安全、公共安全、经济安全和社会稳定的
- B、不会产生《保密法实施办法》第四条所规定的 8 种危害情况和程度的
- C、属于机关公务活动和内部管理中产生的事项

79、将手机带入涉密场所，存在下列哪些泄密隐患：（ABC）

- A、暴露涉密目标的地点
- B、相关涉密图像被窃照
- C、周围的涉密话音被窃听

80、以下涉密信息系统的属性发生变更时，机关、单位必须及时向保密行政管理部门报告的是：（ABC）

- A、密级变更
- B、主要业务应用变更
- C、系统不再使用

81、如何限定国家秘密的知悉范围：（ABC）

A、应当根据工作需要限定在最小范围

B、能够限定到具体人员的，限定到具体人员；

C、离退休等知悉范围以外的人员，因工作需要知悉国家秘密的，应当经过机关、单位负责人批准。

82、以下国家秘密载体保密管理不正确的是：（BC）

A、起草涉密文件、资料的过程稿、送审稿、讨论稿等，都应按照密级文件管理规定妥善保管，不能随意丢弃

B、未经批准携带国家秘密载体出境

C、涉密文件经过密封包装后，可采用中国邮政专属的 EMS 快递服务传递

83、以下关于保密行政管理部门对机关、单位保密工作开展情况监督管理的说法正确的是：（ABC）

A、保密行政管理部门发现机关、单位存在泄密隐患的，应当要求其采取措施，限期整改；

B、对存在泄密隐患的设施、设备、场所，应当责令停止使用；

C、对严重违反保密规定的涉密人员，应当建议有关机关、单位给予处分并调离涉密岗位；

84、刑法对泄露国家秘密有哪些规定：（AC）

A、违反国家规定，侵入国家事务、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或拘役

B、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，处十年以上有期徒刑；情节较轻的，处五年以下有期徒刑或拘役

C、违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行的，后果严重的，处五年以下有期徒刑或拘役

三、判断题

1、使用无线通信工具不安全，会泄密；使用有线通信工具比较安全，一般不会泄密。(×)

2、目前，使用从国外进口的手机不安全，有可能被设置后门；使用国产手机比较安全，一般不会设置后门。(×)

3、将手机关机后就不会再发生泄密问题了。(×)

4、只要在核心涉密场所安装并打开了手机屏蔽设备，就可以将手机带入该涉密场所了。(×)

5、只有连接互联网的计算机感染病毒或者受到黑客攻击，手机是不会感染病毒和受到黑客攻击的。(×)

6、不在有线电话机的线路上搭线，照样可以通过放大通信线路中的“串音”和采取语音频谱筛选的办法达到窃听某特定对象通话内容的目的。(√)

7、更换了手机通讯卡，并不影响对该手机持有者所在位置的准确判定。(√)

8、用手机发送的短信息即便将其删除了，也无法使这些短信息在其相应的服务器中彻底消除。(√)

9、遥控别人的手机将其变成窃听器，使可以在不知不觉中进行。(√)

10、被安装了后门的手机进行窃照并向外发送信息，必须由手机的持有人在现场操作。(×)

11、严禁将涉密存储载体接入互联网等公共网络或者在具有无线联网功能的计算机上使用。(√)

12、现代万能开锁器能够开启所有传统结构的弹子门锁，因此弹子锁的防盗门基本不防盗。(√)

13、“一次涉密，终身涉密”在各类存储载体中并不具有普遍性。
(×)

14、必须将涉密存储载体上所有涉密信息全部删除后，才能够在互联网上使用。(×)

15、淘汰下来的涉密计算机进行格式化处理后，才能够出售或者支援外单位使用。(×)

16、涉密存储载体上的秘密信息，即便覆盖多次，也可以通过“超导量子干涉器件”将其还原出最早存储在上面的涉密信息。(√)

17、不能够使用存储载体在涉密网络与互联网等各种非涉密网络之间交叉使用，双向下载或拷贝信息。(√)

18、涉密存储载体不能够在非涉密计算机信息系统上使用，而非涉密存储载体却可以在涉密计算机信息系统上有限制地使用。(×)

19、销毁涉密存储载体应当先清除载体中的信息，再采用物理或化学的方法彻底销毁，确保信息无法还原。(√)

20、采购进口的办公设备未经严格技术检查、检测，不得在保密要害部门部位使用，但碎纸机和复印机可以例外。(×)

21、政务内网是涉密网络，不能将党政机关的内部网络接入政务内网，但是经过审批可以接入政务外网。(×)

22、严格涉密计算机接入互联网，但是经过审批可以接入内部计算机网络。(×)

23、严禁同一台计算机既与互联网相连接，又处理国家秘密信息。
(√)

24、涉密会议、活动应当按照“谁主办，谁负责”的原则，明确涉密会议、活动各方的保密管理职责。(√)

25、涉密网络可以处理内部信息，内部网络不能处理涉密信息。
(√)

26、移动存储载体不得在涉密网络与非涉密网（包括内部网络、互联网等）之间交叉使用，双向下载、拷贝信息。(√)

27、移动存储载体在接入本单位涉密网络或者内部网络之前，都应当查杀病毒、木马等恶意代码。(√)

28、通过计算机网络远程传输国家秘密信息，必须使用经中央密码领导小组批准使用的加密系统。(√)

29、各机关单位对计算机信息系统的安全和保密管理，必须坚持“谁主管谁负责，谁运行谁负责”的原则。(√)

30、内部网络与互联网可以物理隔离，也可以逻辑隔离；涉密网络与互联网必须物理隔离。(√)

31、长期经管国家秘密的专职人员，一贯忠于职守、确保国家秘密安全的，其所在机关、单位、上级机关或者当地政府应当依照规定予以奖励。(√)

32、宣传报道和新闻出版的保密审查由宣传部负责，按照《新闻出版保密规定》执行。(√)

33、因工作需要携带涉密载体外出，要经本机关、本单位主管领导批准。(√)

34、阅读秘密公文只可在办公室或阅文室进行，可以横向传阅。

(×)

35、因公出国人员行前须到国家安全、保密部门接受保密审查和保密教育，应自觉地遵守保密纪律和法律法规。(√)

36、一切国家机关、武装力量、政党、社会团体、企事业单位和公民都有保守国家秘密的义务。(√)

37、机密级国家秘密是指泄露会使国家的安全和利益遭受特别严重的损害的国家秘密事项。(×)

38、对绝密级的国家秘密文件、资料和其他物品，非经原确定密级的机关、单位或者其上级机关批准，不得复制和摘抄。(√)

39、以谋取私利为目的或利用职权强制他人违反保密规定以致泄露国家秘密但又不够刑事处罚的，可以酌情给与行政处分。(×)

40、不属于国家秘密的其他秘密或者机关、单位的内部事项，可以参照适用保密法及其实施办法。(×)

41、制作秘密载体，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，编排好顺序号。(×)

42、纸介质秘密载体只能在本机关、单位内部文印室印制。(×)

43、因工作需要确需携带秘密级秘密载体出境的，应当按照有关保密规定办理批准和携带手续。(√)

44、销毁秘密载体，应当确保秘密信息无法还原。(√)

45、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他公共信息网相联接，必须实行物理隔离。(√)

46、计算机信息系统国际联网的保密管理，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。(√)

47、不得使用明码或者未经中央有关机关审查批准的密码传递国

家秘密。(√)

48、特殊情况下经批准可以通过普通邮政或非邮政渠道传递秘密载体。(×)

49、所谓重点涉密人员，只要是指各级党政机关县处级以上领导干部。(×)

50、国家工作人员或者其他公民发现国家秘密已泄露或者可能泄露时，应当立即采取补救措施并及时报告有关机关、单位。(√)

51、对于我国特有的动、植物资源，为防止不法分子私自携带出境，应当将其定为国家秘密进行保护。(×)

52、根据新修订的《保密法》，县、乡一级机关、单位没有原始定密权，享有定密权的单位也不是人人都有定密权。(√)

53、新修订的《保密法》规定，机关、单位负责人及其指定的人员为定密责任人，负责本机关、本单位的国家秘密确定、变更和解除工作。(√)

54、涉密载体是指以文字、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、光盘以及半导体介质等各类物品。(√)

55、经过本机关、单位主管领导批准，可以携带绝密级秘密载体参加涉外活动。(×)

56、新修订的《保密法》规定，将集中制作、存放、保管国家秘密载体的专门场所确定为保密要害部门。(×)

57、派生定密，是指根据其他单位产生的国家秘密而产生的新的国家秘密。派生的国家秘密的密级和保密期限要与原载体的相一致。(√)

58、对于不涉及国家秘密的党委会议记录和民主生活会议记录是可以公开的。(×)

59、国家秘密在解密后就可以对社会完全公开。(×)

60、《保密法》规定凡是关系到国家安全和利益的信息都要进行保密。(×)

61、处理绝密级信息的涉密系统，应按照用户类型、信息类别进行访问控制。(×)

62、对于涉密的机关、单位来讲，涉密载体故障导致涉密数据泄密的后果可能不仅仅限于巨大的经济损失，严重的可能威胁到国家安全。(√)

63、各机关、单位销毁秘密载体，应当到保密工作部门批准的销毁国家秘密载体定点单位进行销毁，不得向个体商贩、废品收购单位出售秘密载体。(√)

64、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。(√)

65、设区的市、自治州一级的机关及其授权机关、单位可以确定机密级和秘密级国家秘密。(√)

66、保密技术是对保护国家秘密安全的所有技术手段的统称。主要分为保密防范技术和保密检查技术两大类。(√)

67、对于“情节严重的”泄密行为，若是属于故意泄密，则应当追究行为人的刑事责任；若是属于过失泄密，则应当给予相应的行政处分，而不再追究行为人的刑事责任。(×)

68、泄露机密级国家秘密，情节轻微的，可以酌情从轻给予行政处分，也可以免于行政处分。(√)

69、秘密载体的保密管理，根据相关规定，遵循严格管理、严密防范、确保安全、方便工作的原则。(√)

70、收发秘密载体，应当履行清点、登记、编号、签收等手续。(√)

71、绝密级秘密载体只能通过派遣专人传递或由机要交通传递，而不能由机要通信传递。(×)

72、国家工作人员在对外交往中，应当严格遵循内紧外松，内外有别，既保守秘密，又有利于对外交往的原则。(√)

73、泄密事件已经调查清楚，已经采取必要的补救措施，对泄密责任者已经作出处理，发生泄密事件的机关或单位已经采取了加强保密工作的措施，即可终结该项泄密事件的查处工作。(√)

74、“物理隔离对涉密系统的一项基本要求，基本含义是涉密系统与公众信息网之间，没有任何光、电以及实体传输通道。(√)

75、保密检查是指保密工作部门或机关、单位的保密工作机构依据保密法规的规定，通过一定的组织形式和方法，对涉密的机关、单位履行保密职责和义务的情况进行调查了解、监督评价、指导服务的一种行政执法活动。(√)

76、政府门户网站是建立在互联网上的信息发布平台，对拟在政府门户网站上登载的信息应严格遵守信息公开保密审查制度，确保涉密信息不上网。(√)

77、国家秘密范围是指国家秘密这一概念所确指对象的总和。(√)

78、在《保密法》颁布实施以前，我国规定国家秘密的保密期限统一为三十年。(×)

79、国家秘密事项的保密期限届满，没有接到上级保密工作部门

的通知，不能自行解密。(×)

80、国家秘密、工作秘密、商业秘密都属于《保密法》调整的范围。(×)

81、国家秘密的密级分为“绝密”、“机密”、“秘密”、“内部”四级。(×)

82、涉密单位的工作人员向公众散布、传播国家秘密的行为是过失泄露国家秘密。(×)

83、按照规定应当清退的秘密载体，应如数清退。已自行销毁的，应提供两人以上的监销记录。(√)

84、国家秘密载体不需要保存的可以作为废品出售。(×)

85、涉密机关、单位收到绝密级秘密载体，必须按照规定的范围组织阅读使用，并对接触和知悉绝密级秘密载体内容的人员做出文字记载。(√)

86、国家工作人员或者其他公民发现国家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有关机关、单位。(√)

87、涉密机关、单位的保密工作机构对本机关、单位执行《关于国家秘密载体保密管理的规定》负有指导、监督、检查的职责。(√)

88、利用必要的加密手段，可以在互联网上用电子函件传递、转发或抄送国家秘密信息。(×)

89、国家秘密应当根据需要，限于一定范围的机关干部接触。(×)

90、国家秘密在无线通信中传递，就确保了它的安全。(×)

91、不属于国家秘密的，不应标为国家秘密文件、资料。(√)

92、凡因过失泄露国家秘密，都不应追究刑事责任。(×)

93、打印输出的涉密文件应按相应密级的文件进行管理。(√)

- 94、安全保密设备可以采用市场上有售的设备。(×)
- 95、绝密级的系统应有系统、设备等的备份和应急恢复措施，重要的数据应异地备份。(√)
- 96、安全域与安全域之间不必用安全保密设备进行隔离和访问控制。(×)
- 97、审计系统的审计不一定完整记录所有操作。(×)
- 98、涉密系统不直接国际互联网，但可以间接联网。(×)
- 99、涉密系统处理多种密级的信息时，按一般密级进行防护。(×)
- 100、涉密系统只要选用成熟的操作系统。(×)
- 101、泄露国家秘密已经人民法院判处刑罚的，不再从重给予行政处分。(×)
- 102、属于国家科学技术秘密的民用科学技术，一律不得定为绝密级国家秘密。(×)
- 103、为了加强对国家秘密载体复制活动的管理，国家对印刷、复印等行业实行向政府保密工作部门申请许可的制度。(×)
- 104、绝密级国家秘密技术在保密期限内可以申请专利或者保密专利，但须经国家科委批准。(×)
- 105、接触国家秘密事项的人员或者机关、单位的范围，应当根据工作的需要限定在最小范围。(√)
- 106、业务工作管到哪里，保密工作也要管到哪里，是党政领导干部保密工作责任制对各级党政领导干部作出的规定。(√)
- 107、国家秘密文件在公共场所丢失后，凡在一个月內能够找回的，就不应视为泄密。(×)
- 108、被有关中央国家机关确定保密期限为"长期"的国家秘密事

项，非经该机关或其授权的机关作出解密的决定，其他机关、单位应当对此长期采取保密措施，不得擅自决定解密。(√)

109、属于国家秘密的设备或者产品，在确定密品的密级和保密期限的同时，应当明确保密要点。(√)

110、涉密机关、单位收到绝密级秘密载体后，必须按照规定的范围组织阅读和使用，并对接触和知悉绝级秘密载体内容的人员做出文字记载。(√)

111、国防科技成果国家秘密是指以国防为目的或主要目的的科学研究和开发活动中产生的具有国家秘密属性的科学技术成果。(√)

112、保密期限在 1 年及 1 年以上的，以年计；保密期限在 1 年以内的，以月计。(√)

113、国家秘密主要产生于党政机关，企事业单位产生的秘密均不属于国家秘密。(×)

114、对邮寄或非法携带国家秘密文件、资料和其他物品出境的当事人，海关可根据有关规定视情处以罚款；对情节严重，构成犯罪的，依法移送司法机关处理。(√)

115、计算机信息系统存储、处理、传递、输出的涉密信息要有相应的密级标识，密级标识必须与正文分离。(×)

116、科学技术保密工作的重点是确保重要国家科学技术秘密的安全，民用科学技术不应确定为国家秘密。(×)

117、根据《保密法》和《刑法》的规定，泄露国家秘密罪的定罪应考虑主观因素，故意泄密构成犯罪，过失泄密不构成犯罪。(×)

118、因泄露国家秘密所获取的非法收入，应当予以没收并上交国家保密局。(×)

119、接待境外人员参观国家科学技术秘密事项，应当由接待单位按照行政隶属关系报省、自治区、直辖市的科技主管部门或者中央国家机关各部门的科技主管机构审查批准。(√)

120、1951年6月8日，中央人民政府政务院发布了《中央人民政府政务院保守国家机密暂行条例》，这是我国第一部有关规范保密工作的法规。(√)

121、制作秘密载体过程中形成的不需归档的材料，应当及时销毁。(√)

122、各级机关、单位发生重大泄密事件，在向其主管部门报告的同时，还应直接向国家保密局报告。(√)

123、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。(√)

124、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。(√)

125、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。(√)

126、"业务工作谁主管，保密工作谁负责"是保密工作的重要原则。(√)

127、国家秘密的密级分为绝密、机密、秘密三个等级。(√)

128、绝密级国家秘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。(√)

129、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。(√)

130、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。(√)

131、保守国家秘密是我国公民的一项基本义务。(√)

132、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。(√)

135、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。(×)

136、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。(√)

137、涉密人员应当具有中华人民共和国国籍。(√)

138、涉密人员上岗前要经过审查和批准，并接受保密教育培训。(√)

139、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。(√)

140、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。(√)

141、涉密人员与境外人员通婚或者接受境外机构，组织资助的应当向单位报告。(√)

142、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。(√)

143、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。(√)

144、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。(×)

145、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。(×)

146、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。(√)

147、涉密人员脱密期内可以因私出境。(×)

148、涉密人员脱密期满后，可以不再履行保密责任和义务。(×)

149、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。(×)

150、涉密人员脱密期满后，对所知悉的国家秘密仍然要承担保密责任和义务。(√)

151、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。(√)

152、涉密单位应对聘用的保安和临时工进行保密教育培训。(×)

153、不准在私人交往和通信中泄露国家秘密。(√)

154、配偶，子女和本人都是涉密人员，互相谈涉密事项没有关系。(×)

155、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准确定密。(√)

156、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。(√)

157、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。

(√)

158、保密范围定得越宽，密级越高，越有利于国家秘密的安全。

(×)

159、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级工作小组审定。(√)

160、国家秘密的标志为★，★前标密级，★后标保密期限。(√)

161、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。(√)

162、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。(√)

163、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。(×)

164、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。(√)

165、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。(√)

166、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。(√)

167、国家秘密事项的密级和保密期限一经确定，就不能改变。(×)

168、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，秘密事项不超过 5 年。(×)

169、国家秘密事项的保密期限届满即自行解密。(√)

170、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。(√)

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

172、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。(×)

173、已解密的事项可以随意公开。(×)

174、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。(√)

175、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。(×)

176、密级的变更包括降低或者提高密级等级。(√)

177、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。(√)

178、纸介质涉密载体应当在本机关，位内部文印室或委托保密工作机构定点的单位制作。(√)

179、国家秘密定点复制单位，使用电子方法排版印制或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。(×)

180、收发涉密载体，应当履行清点、登记、编号、签收等手续。(√)

181、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、编号和收发件单位名称。(√)

182、传递涉密载体应当通过机要交通、机要通信或指派专人传递；不得通过普通邮政渠道传递。(√)

183、国家秘密文件，资料可以通过普通邮政"特快专递"传送。(×)

184、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。(√)

185、记录涉密内容应当使用保密本。(√)

186、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。(√)

187、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。(×)

188、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。(×)

189、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。(√)

190、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。(×)

191、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。(×)

192、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材料，作删除处理。(×)

193、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。(×)

194、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。(√)

195、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。(√)

196、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。(√)

197、不准在普通手机通话中涉及国家秘密。(√)

198、普通手机处于关机状态下，不存在涉密隐患。(×)

199、不得使用普通手机短信传送国家秘密信息。(√)

200、不得将普通手机与涉密信息系统连接。(√)

201、不得在涉密场所使用普通手机。(√)

202、个人因公外出，携带秘密载体应当采取严格的保密措施。(√)

203、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。(√)

204、领导干部为了工作方便，可以将密件带回家中处理。(×)

205、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。(√)

206、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。(√)

207、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。(√)

208、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。(×)

209、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。(×)

210、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。(√)

211、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。(√)

212、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。(√)

213、U 盘上的涉密信息，只要执行了删除程序就不可恢复了。(×)

214、涉密载体不得作为废品出售。(√)

215、密品是指直接含有国家秘密信息的设备或者产品。(√)

216、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。(√)

217、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。(√)

218、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。(√)

219、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。(√)

220、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。(√)

221、普通手机关机后可以带入要害部门、部位。(×)

222、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。(√)

223、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。(√)

224、不得使用未采取密码保护的通信系统传输涉密信息。(√)

225、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。(√)

226、无线电话不保密、军线电话是保密的。(×)

227、数字移动电话传输的数字信号，因此是保密的。(×)

228、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。(×)

229、电磁信号泄漏泄密的方式主要是辐射和传导两种方式。(√)

230、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。(√)

231、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。(√)

232、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。(×)

233、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。(√)

234、绝密级信息必须加密存储。(√)

235、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。(√)

236、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。

(√)

237、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。(√)

238、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。

(√)

239、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。(√)

240、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。(√)

241、不得在上国际互联网的计算机上处理和存储涉密信息。(√)

242、涉密计算机不得与国际互联网络或其他公共网络相连接。

(√)

243、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。(×)

244、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。

(√)

245、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。(×)

246、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。(√)

247、国际秘密不得在与国际互联网连接的计算机和信息系统中

处理、存储、传递，但可以在单位内部非涉密计算机上处理、存储、传递。(×)

248、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。(×)

249、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。(√)

250、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。(√)

251、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。(×)

252、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。(√)

253、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。(√)

254、音像制品涉及国家秘密的，应按涉密资料保管。(√)

255、保密教育和保密提醒是科技交流必须坚持的制度。(√)

256、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。(√)

257、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。(√)

258、使国家秘密被不应知悉者知悉的，属于泄露国家秘密行为。(√)

259、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。(√)

260、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、秘密级载体 60 日内查无结果的，按泄密事件处理。(√)

261、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。(√)

262、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，应予以立案。(√)

263、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。(×)

264、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。(√)

265、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。(√)

266、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。(√)

267、未经相关保密工作部门批准，不得向境外邮寄密品密件或随身携带密品密件出境。(√)

268、保密工作标准化管理旨在将标准化管理理念引入全市党政机关、涉密单位保密工作，建立明确的保密工作目标评价标准和可控管理程序，实现保密管理的科学化、规范化和制度化。(√)

269、为安全起见，出差时可以将涉密计算机及其移动存储介质放在行李中托运。(×)

270、计算机硬盘、优盘等存储部件的信息，即使经一般数据删除或格式化处理后，仍可以通过技术手段将其中的涉密信息予以恢复。（√）

271、禁止携带绝密级涉密载体参加涉外活动或出境。（√）

272、处理过涉密信息的多功能一体机不得与普通电话线相连接。（√）

273、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，可以在与互联网连接的信息系统中存储、处理。（×）

274、严禁将私人存储介质和具有存储功能的电子设备带入核心和重要涉密场所。（√）

275、具备信息存储功能的电子设备都具有“一次涉密，终生涉密”的特性。（√）

276、涉密会议场所应该选用比较安全的无线话筒。（×）

277、严禁使用私人移动存储介质存储涉密文件、信息。（√）

278、执行和使用保密范围的正确方法是条款对照与属性判定相结合。（√）

279、国家秘密的密级、保密期限和知悉范围的变更，由原定密机关、单位决定，也可以由其上级机关决定。（√）

280、绝密级国家秘密载体未经原定密机关、单位或者其上级机关批准，不得复印。（√）

281、机关、单位违反保密法规定，对应当定密的事项不定密，或者对不应当定密的事项定密，造成严重后果的，由有关机关、单位依法对直接负责的主管人员和其他直接责任人员给予处分。（√）

282、办理涉嫌泄露国家秘密案件的机关，需要对有关事项是否属于国家秘密以及属于何种密级进行鉴定的，由国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门鉴定。（√）

四、填空题

1、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。

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、不准在私人交往和通信中泄露国家秘密。不准在公共场所谈论国家秘密。

4、国家秘密分为绝密、机密、秘密三个等级。

5、涉密信息系统的保密设施、设备应当与系统同步规划，同步建设，同步运行。

6、涉密信息系统应当严格设定用户权限，按照最高密级防护和最小授权管理的原则，控制涉密信息知悉范围。

7、在对外交往与合作中需要提供国家秘密事项的，应当按照规定的程序事先经过批准。

8、具有属于国家秘密内容的会议和其他活动，主办单位应当采取保密措施，并对参加人员进行保密教育，规定具体要求。

9、国家工作人员或者其他公民发现国家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有关机关、单位；有关机关、单位接到报告后，应当立即作出处理。

10、未经有关主管部门批准，禁止将属于国家秘密的文件、资料和其他物品携带、传递、寄运至境外。

11、移动存储介质不得在涉密计算机 和 非涉密计算机 之间交叉使用。

12、涉密场所中连接互联网的计算机不得配备、安装、使用视频 和 音频 输入设备。

13、不得在非涉密 办公网络和连接互联网 及其他公共信息网络的计算机上存储、处理和传输涉密信息。

14、信息系统存储、处理、传递、输出的涉密信息要有相应的密级 标识，该标识不能与正文分离。

15、处理国家秘密信息的单台计算机，应当根据所处理信息的最高密级，按照相应 级别涉密信息系统的有关要求进行了保护和管

理。

16、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。

17、国家机关和涉密单位按照“谁 主管 谁负责、谁 使用 谁负责”的要求，负责本机关、单位信息系统和信息设备使用保密管理工作。

18、涉密信息系统的规划、设计、建设、维护应当按照国家保密规定和标准要求进行，选择 具有涉密信息系统集成资质的单位 承担。

19、涉及国家秘密的信息系统，不得直接或间接地与 互联网 及其他 公共信息网络 连接，必须实行 物理隔离 。

20、任何组织和个人不得擅自改变涉密信息系统的安全保密 防护措施。

21、涉密信息系统应当严格设定用户权限，按照 最高 密级防

护和最小授权管理的原则，控制涉密信息知悉范围。

22、国家机关和涉密单位采购安全保密产品应当选用经过国家保密行政管理部门授权检测机构检测、符合国家保密标准要求的产品。

23、磁介质、光盘等秘密载体应当在本机关内或单位审查批准的单位制作。

24、涉密信息设备使用人员、管理人员离职、离岗时，机关、单位应当收回其使用、管理的涉密信息设备，及时取消有关涉密信息系统的访问授权。

25、保密要害部门部位使用进口设备和产品，应进行安全技术检查。

26、销毁密件实行2人以上的销毁制度。

27、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。

28、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期限作出标志。

29、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。

30、保守国家秘密是我国公民的一项基本义务。

31、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。

32、涉密人员上岗前要经过保密审查和培训。

33、涉密人员脱离期届满的，对其知悉的国家秘密仍负有保密

义务。

33、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。

34、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。

35、外聘工勤服务人员 不得接触 国家秘密

36、“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。

37、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。

38、不准 在私人交往和通信中泄露国家秘密。

39、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。

40、销毁磁介质、光盘等秘密载体,应当采取 物理或化学 的方法彻底销毁,确保信息无法还原。

41、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。

42、计算机口令在网络中必须 加密 存储和传输

43、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 。

44、涉密计算机的密级应按处理和存储信息的 最高 密级确定。

45、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

- 46、在涉密工作区域，禁止使用 无标志的存储介质。
- 47、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
- 48、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。
- 49、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。
- 50、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。
- 51、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。
- 52、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。
- 53、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。
- 54、高密级的移动存储介质禁止在 低密级 的计算机上使用。
- 55、携带涉密计算机和存储介质外出应当履行 审批 手续。
- 56、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。
- 57、单位通过互联网发布信息应当进行 保密审查。
- 58、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。
- 59、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。

五、问答题

1、 什么是保密？

答：保密”，是指国家、公民、法人或社会组织对关系自身安全和利益，公开后会对自身利益造成损害的秘密信息，控制其知悉范围，对其采取保护措施，保障其安全的一种保护行为。在人类社会发展的进程中，自“秘密”产生后，就有了“保密”的行为，小至个人、家庭，大到组织、政党、国家，为了维护其秘密信息，都需要“保密”。

2、 什么是保密工作

答：保密工作是指按照国家《保密法》的规定，为保守国家秘密而进行的工作。

我们党和国家的保密工作主要包括以下几方面：一是由各级党委、党组织保密委员会实施的领导和决策工作；二是由各级政府保密工作部门实施的保密管理工作；三是由各级党政军机关及国有企事业单位内的保密工作机构实施的保密管理工作；四是由具体业务部门承担的、渗透在各项业务工作中的保密工作。

7、 什么是国家秘密载体？

答：国家秘密载体是指以文字、数字、图像、声音等方式记载国家秘密信息的纸介质、磁介质、光盘等各类物品。

国家秘密和载体之间既相互联系又有区别。国家秘密必须借助一定的载体来存储和传递。国家秘密是一种特殊的信息，载体是它的存在形式。二者不能等同。

8、 什么是国家秘密？

答：国家秘密是关系到国家的安全和利益，依照法定程序确定，在一定时间内只限于一定范围的人员知悉的事项。

9、国家秘密具有哪些特征？

答：国家秘密具有三个特征：一是本质特征。即国家秘密必须同国家的安全和利益密切相关。二是程序特征。即国家秘密必须依照国家的法律、法规所规定的程序确定。三是时空特征。即国家秘密必须而且能够在一定时间内限定一定范围的人员知悉。

10、国家秘密事项在什么情况下解密？

答：国家秘密事项在下列三种情况下解密：1、保密期限届满即自行解密，不需履行解密手续。2、经主管机关、单位正式公布后，即视为解密。3、在保密期限内，由于情况变化，不需继续保密的，原确定密级的机关、单位或其上级机关可以决定解密。

11、什么是保密要害部门和部位？

答：单位内部业务工作中经常或大量涉及机密级（含）以上国家秘密的部门，确定为保密要害部门。集中存放保管机密级（含）以上国家秘密载体的场所，涉及机密级（含）以上国家秘密的研制生产试验场所，确定为保密要害部位。

12、什么是国家秘密载体？

答：国家秘密载体是指以文字、数据、符号、图形、图象、声音等方式记载国家秘密信息的纸介质、磁介质等各类物品。磁介质载体包括计算机硬盘、软盘、光盘和录音带、录像带等。

13、《国家公务员暂行条例》对国家公务员的保密义务有哪些规定？

答：1、不该说的国家秘密不说；2、不该问的国家秘密不问；3、不该看的国家秘密不看；4、不该记录的国家秘密不记录；5、不在私人交往中涉及国家秘密；6、不在公共场所办理、谈论属于国家秘密

的事项；7、不在没有保密保障的地方和设备中存贮、处理国家秘密信息和载体；8、不通过普通电话、明码电报、普通邮局、计算机公用网和普通传真递送、传输国家秘密信息和载体；9、不携带密件、密品参观、游览和探亲访友。

14、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、涉及绝密级国家秘密的保密要害部门部位要安装电视监控系统，门控系统，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。

15、“上网不涉密，涉密不上网”保密要求的含义是什么？

答：“上网不涉密”指的是严禁在接入国际互联网的计算机上处理、存储、传输涉密信息。“涉密不上网”指的是处理涉密信息的计算机在任何时候都不得直接或间接接入任何公共网络国际互联网。需要特别指出的是，不能理解为“上网的时候不涉密，涉密的时候不上网”。

16、党政机关人员信息安全保密注意事项？

答：1、涉密信息 and 数据必须按照保密规定进行采集、存储、处理、传递、使用和销毁；2、计算机信息系统存储、处理、传递、输出的涉密信息要有相应的密级标识，密级标识不能与正文分离；3、国家秘密信息不得在与国际网络联网的计算机信息系统中存储、处理、传递；4、任何单位和个人不得在电子公告系统聊天室、网络新闻组上发布、谈论和传播国家秘密信息；5、使用电子函件进行网上信息交流，应当遵守国家有关保密规定，不得利用电子函件传递、转发或抄送国家秘密信息；6、涉密信息处理场所应当根据涉密程度和

有关规定设立控制区，未经管理机关批准无关人员不得进入；7、任何单位和个人发现计算机信息系统泄密后，应及时采取补救措施，并按有关规定及时向上级报告；8、涉密系统的身份认证应当符合以下要求：口令应当由系统安全保密管理人员集中产生供用户选用，并有口令更换记录，不得由用户产生。

17、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。