

一、 保密工作方针、原则和体制

1. 什么是保密工作？ 保密工作就是为维护国家安全和利益，将国家秘密控制在一定范围和时间 内，防止 泄露或被 非法利用 ，由国家 专门机构组织实施的活动。从工作目的看，保密工作包括 预防和打击 窃密泄密活动；从工作过程看，保密工作贯穿国家秘密运行的 全过程 ；从工作方式看，保密工作主要包括 宣传教育、 法制建设、 指导管理、 技术防护、 监督检查 等方面。

2. 保密工作的方针是什么？ 保密法规定，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，即确保国家秘密安全，又便利信息资源合理利用。 法律、行政法规规定公开 的事项，应当依法公开。

3. 保密工作应当坚持哪几项原则？ 保密工作应当坚持 最小化、 全程化、 精准化、 自主化、 法制化 五项原则。

4. 保密工作领导体制是怎样的？ 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， 各级党的保密委员会是党管保密的专门组织。下级保密委员会接受上级保密委员会的指导和监督。

5. 保密工作管理体制是怎样的？ 国家保密行政管理部门主管全国 的保密工作。 县级以上地方各级保密行政管理部门主管 本行政区域 的保密工作。 机关、 单位设立保密工作机构或者指定人员 专门负责本机关和本单位的保密工作。中央国家机关 在其职权范围内，管理或者指导 本系统 的保密工作。

6. 行业系统内上下级单位保密工作管理关系是怎样的？ 业务工作 接受上级业务部门垂直管理 的单位，保密工作以上级业务部门管理为主， 同时接受 地方 保密行政管理部门的指导； 业务工作接受上级业务部门 指导 的单位，保密工作以地方保密行政管理部门管理为主，同时接受上级业务部门的指导。

二、 国家秘密

7. 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。

8. 国家秘密分哪几个等级？ 国家秘密的密级分为绝密、机密、秘密三级。 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； 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； 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。

9. 国家秘密的基本范围包括哪些？ 国家事务 重大决策中的秘密事项； 国防建设和武装力量 活动中的秘密事项； 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； 国民经济和社会发展 中的秘密事项； 科学技术 中的秘密事项； 维护国家安全活动和追查刑事犯罪 中的秘密事项； 经国家保密行政管理部门 确定的其他秘密事项。 政党的秘密事项，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，属于国家秘密。

10. 国家秘密知悉范围确定的原则是什么？ 确定 国家秘密知悉范围 有两个基本原则。一是 工作需要原则 。不应简单地把知悉国家秘密视作一种政治待遇， 或者把行政级别作为确定国家秘密知悉范围的依据。 二是 最小化原则 。能够限定到具体人员的，限定到具体人员；不能限定到具体人员的，限定到机关、单位，由机关、单位限定到具体人员。

11. 扩大国家秘密知悉范围有哪些规定？ 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 经机关、单位负责人批准 。国家秘密 知悉范围之外 的机关、单位及其人员，因工作需要确需知悉国家秘密的， 应当 经原定密机关、单位同意 。原定密机关、单位对扩大知悉范围有明确规定的，应当遵守其规定。扩大国家秘密知悉范围应当作出 详细记录 。

12. 什么是国家秘密标志？ 国家秘密标志是一种 法定 的文字与符号标识，用以表明所标识的物品（载体及设备、产品等） 承载内容属于国家秘密， 并提示其密级和保密期限。 国家秘密标志形式为 “ 密级 保密期限 ”、“ 密级 解密时间 ” 或者 “ 密级 解密条件 ”。

13. 如何做出国家秘密标志？ 书面形式的涉密载体，应在 封面或首页 作出国家秘密标志（地图、图纸、图表在其标题之后或者下方适当位置标注， 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最高密级和最长保密期限标注）；非书面形式的涉密载体，要以能够明显识别的方式予以标注（套、盒、袋等凡有包装的载体在载体包装上标注）；电子文档中含有国家秘密内容的，应作出国家秘密标志，且标志与文档正文不可分离。对不能或不宜作出国家秘密标志的，产生或制作机关、 单位应作出文字记载， 并将其密级和保密期限及时通知知悉范围内的机关、单位或人员。

14. 国家秘密保密期限如何确定？ 机关、单位对所产生的国家秘密，应当按照保密事项范围的规定确定具体的保密期限；保密事项范围没有规定具体保密期限的，可以根据工作需要，在保密法规定的保密期限内确定；不能确定保密期限的，应当确定解密条件。国家秘密的保密期限，除另有规定外，绝密级不超过 30 年，机密级不超过 20 年，秘密级不超过 10 年。

15. 国家秘密保密期限如何计算？ 国家秘密的保密期限，自标明的制发日起计算；不能标明制发日的，确定该国家秘密的机关、单位应当书面通知知悉范围内的机关、单位和人员， 保密期限自通知之日起计算。 一般情况下，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；保密期限在 1 个月以内的，可以规定保密期限为 1 个月或具体规定为多少日。

三、 定密工作

16. 什么是定密？ 定密是指机关、单位依法确定、变更和解除国家秘密的活动。

17. 定密应当坚持什么原则？ 机关、单位定密应当坚持最小化、精准化原则，做到权责明确、依据充分、程序规范、及时准确，既确保国家秘密安全，又便利信息资源合理利用。

18. 定密权是如何规定的？ 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。公安、国家安全机关在其工作范围内按照规定的权限确定国家秘密的密级。

19. 定密权如何申请？ 没有定密权但经常产生国家秘密事项的机关、单位，或者虽有定密权但经常产生超出其定密权限的国家秘密事项的机关、单位，可以向授权机关申请定密授权。 “ 经常 ” 主要是指近三年来年均产生六件以上国家秘密事项的情形。申请定密授权，应当向其上级业务主管部门提出；没有上级业务主管部门的，应当向其上级机关提出。申请定密授权，应当书面说明拟申请的定密权限、事项范围、授权期限以及申请依据和理由。

20. 定密责任人包括哪些人员？ 机关、单位负责人为本机关、本单位的定密责任人，对定密工作负总责。根据工作需要，机关、单位负责人可以指定本机关、本单位其他负责人、内设机构负责人或者其他工作人员为定密责任人，并明确相应的定密权限。

21. 定密责任人的主要职责是什么？ 定密责任人在职责范围内承担有关国家秘密确定、变更和解除工作。具体职责是：审核批准本机关、本单位产生的国家秘密的密级、保管期限和知悉范围；对本机关、本单位产生的尚在保密期限内的国家秘密进行审核，作出是否变更或者解除的决定；对是否属于国家秘密和属于何种密级不明确的事项先行拟定密级，并按照规定的程序报保密行政管理部门确定。

22. 国家秘密如何确定？ 机关、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。

23. 国家秘密确定的依据是什么？ 保密事项范围是确定、变更和解除国家秘密事项的具体标准和依据，由国家秘密范围和国家秘密目录两部分构成。

24. 保密事项范围由谁规定？ 保密事项范围，由国家保密行政管理部门分别会同外交、公安、国家安全和其他中央有关机关规定；军事方面的保密事项范围，由中央军事委员会规定。保密事项范围的规定，应当在有关范围内公布，并根据情况变化及时调整。

25. 国家秘密确定的基本程序是什么？ 国家秘密确定的基本程序是：在国家秘密产生的同时，由承办人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。

26. 哪些事项不得确定为国家秘密？ 需要社会公众广泛知晓或者参与的；属于工作秘密、商业秘密、个人隐私的；已经依法公开或者无法控制知悉范围的；法律、法规或者国家有关规定要求公开的。

27. 国家秘密在什么情况下需要变更？ 当国家秘密确定时所依据的法律法规或者保密事项范围发生变化的，或者国家秘密事项泄露后对国家安全和利益的损害程度发生明显变化的，国家秘密应当及时变更。

28. 国家秘密如何变更？ 国家秘密变更按照国家秘密确定程序进行并作出书面记录。国家秘密变更后，原定密机关、单位应当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。

29. 国家秘密在什么情况下需要解除？ 机关、单位应当定期审核所确定的国家秘密。对保密法律法规或者保密事项范围调整后不再属于国家秘密的，或者公开后不会损害国家安全和利益、不需要继续保密的，应当及时解除。

30. 国家秘密如何解除？ 国家秘密解除主要有两种情形：一是自行解密，即具体保密期限已满、解密时间已到或者符合解密条件的国家秘密事项自行解密；二是提前解密，即机关、单位定期审核所确定的国家秘密事项，不需要继续保密的，应当按照国家秘密确定程序及时解密并作出书面记录。国家秘密解除后，有关机关、单位或者人员应当及时在原国家秘密标志附近做出解密标志，并书面通知知悉范围内的机关、单位和人员。解密的国家秘密事项并不意味着可以公开，需要公开的应当由解密的机关、单位经过审查后作出决定。

31. “不明确”事项的密级如何确定？ 机关、单位对符合保密法的规定，但保密事项范围没有规定的不明确事项，拟定为绝密级的事项和中央国家机关拟定的机密级、秘密级的事项，报国家保密行政管理部门确定；其他机关、单位拟定的机密级、秘密级的事项，报省、自治区、直辖市保密行政管理部门确定。

32. “有争议”事项的密级如何确定？ 机关、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，可以向原定密机关、单位提出异议，由原定密机关、单位作出决定。机关、单位对原定密机关、单位未予处理或者对作出的决定仍有异议的，确定为绝密级的事项和中央国家机关确定的机密级、秘密级的事项，报国家保密行政管理部门确定。其他机关、单位确定的机密级、秘密级的事项，报省、自治区、直辖市保密行政管理部门确定；对省、自治区、直辖市保密行政管理部门作出的决定有异议的，可以报国家保密行政管理部门确定。

33. 定密工作中如何使用保密事项范围？ 使用保密事项范围，首先要准确理解保密事项范围规定中有关条款的含义，并依据本行业、本领域保密事项目录，确定本机关、本单位产生的国家秘密事项的密级、保密期限和知悉范围。同时，对可能产生的其他工作方面的国家秘密事项，需要对照相关领域保密事项范围，不能仅局限于在本行业、本领域保密事项范围中“对号入座”。

四、涉密人员

34. 什么是涉密人员 在涉密岗位（日常工作中产生、经营或经常接触、知悉国家秘密事项的岗位）工作的人员。

35. 涉密人员分为哪几类？ 涉密人员分为核心涉密人员、重要涉密人员和一般涉密人员。

36. 涉密人员应当具备哪些基本条件？ 任用、聘用涉密人员应当按照有关规定进行审查。涉密人员应当具备一定的基本条件，具体来说：具有中华人民共和国国籍；热爱祖国，遵纪守法；政治立场坚定，品行端正，忠诚可靠；具备涉密岗位要求的业务素质和能力。

37. 涉密人员上岗主要有哪些保密要求？ 涉密人员上岗应当经过保密教育培训（每年不少于 4 个学时），掌握保密知识技能，签订保密承诺，严格遵守保密规章制度，不得以任何方式泄露国家秘密。

38. 在岗人员保密承诺书主要包括哪些内容？ 在岗人员保密承诺书内容主要包括：认真遵守国家保密法律、法规和规章制度，履行保密义务；不提供虚假个人信息，自愿接受保密审查；不违规记录、存储、复制国家秘密信息，不违规留存涉密载体；不以任何方式泄露所接触和知悉的国家秘密；未经单位审查批准，不得擅自发表涉及未公开工作内容的文章、著述；离岗时，自愿接受脱密期管理，签订保密承诺书；违反上述承诺，自愿承担党纪、政绩责任和法律后果。

39. 涉密人员离岗，离职主要有哪些保密要求？ 涉密人员离岗、离职应当及时清退个人持有和使用的涉密载体及涉密信息设备，签订保密承诺书，严格脱密期管理等。

40. 离岗人员保密承诺书主要包括哪些内容？ 离岗人员保密承诺书内容主要包括：认真遵守国家保密法律、法规和规章制度，履行保密义务；不以任何方式泄露所接触和知悉的国家秘密；已全部清退不应由个人持有的各类涉密载体；未经原单位审查批准，不得擅自发表涉及原单位未公开工作内容的文章、著述；自愿接受脱密期管理，自 年_月_日至_年_月_日服从有关部门的保密监管；违反上述承诺，自愿承担党纪、政纪责任和法律后果。

41. 涉密人员脱密期为多长？ 涉密人员脱密期，一般情况下，核心涉密人员为 3 年至 5 年，重要涉密人员为 2 年至 3 年，一般涉密人员为 1 年至 2 年。对特殊的高知密度人员，可以依法设定超过上述期限的脱密期。

42. 涉密人员脱密期如何计算？ 涉密人员脱密期自机关、单位批准涉密人员离开涉密岗位之日起计算。

43. 涉密人员脱密期管理主要有哪些要求？ 涉密人员脱密期管理要求主要包括： 明确脱密期限； 与原机关、单位签订保密承诺书，做出继续履行保密义务、 不泄露所知悉国家秘密的承诺； 及时清退所持有和使用的全部涉密载体和涉密信息设备，并办理移交手续；未经审查批准，不得擅自出境；不得到境外驻华机构、组织或者外资企业工作；不得为境外组织人员或者外资企业提供劳务、咨询或者其他服务。

44. 涉密人员脱密期管理由哪些单位负责？ 涉密人员离岗（离开涉密工作岗位，未离开本机关、本单位）的，脱密期管理由本机关、本单位负责。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，脱密期管理由调入单位负责；属于其他情况，由原涉密单位、保密行政管理部门或者公安机关负责。

45. 涉密人员应当报告哪些重大事项？ 涉密人员需报告的重大事项主要有： 发生泄密或者造成重大泄密隐患的；发现针对本人渗透、策反行为的；接受境外机构、组织及非亲属人员资助的；与境外人员结婚的；配偶、子女获得境外永久居留资格或者取得外国国籍的；其他可能影响国家秘密安全的个人情况。

46. 涉密人员出国（境）主要有哪些保密要求？ 涉密人员出国（境）应当严格出国（境）审批制度。确需携带涉密载体出国（境）的应当履行审批程序。涉密人员在境外遇到盘问、利诱、胁迫或者其他重大异常情况的，应当及时报告。

47. 涉密人员发表文章、著作主要有哪些保密要求？ 涉密人员发表文章、 著作不得涉及国家秘密。 凡涉及本系统、本单位业务工作或对是否涉及国家秘密界限不清的， 以及拟向境外新闻出版机构提供报道， 出版涉及国家政治、经济、外交、科技、军事等方面内容的，应当事先经本单位或上级机关、单位审定。向境外投寄稿件，应当按照国家有关规定办理。

48. 涉密人员的权益保障主要有哪些？ 涉密人员享有作为机关、 单位一般工作人员应有的各项权利外， 还有权要求机关、单位为其提供符合保密要求的工作条件，配备必要的保密设施、设备，参加保密业务培训，对本岗位的保密工作提出意见建议，依法享有相应的岗位津贴等。

五、 涉密载体

49. 什么是涉密载体？ 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。

50. 制作涉密载体如何管理？ 制作涉密载体应当由机关、 单位或者经保密行政管理部门保密审查合格的单位承担；制作场所应当符合保密要求，使用电子设备的应当采取电磁泄漏发射防护等措施； 制作过程中形成的不需归档的材料要及时销毁。

51. 复制涉密载体或者摘录、引用、汇编属于国家秘密的内容如何管理？ 机密级、秘密级涉密载体的复制、摘录、引用、汇编，应当按照规定报批， 不得擅自改变原件的密级、 保密期限和知悉范围， 复制件应当加盖复制机关、单位戳记，并视同原件进行管理。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。

52. 收发涉密载体如何管理？ 收发涉密载体应当履行清点、编号、登记、签收手续。

53. 传递涉密载体如何管理？ 传递应当通过机要交通、机要通信或者其他符合保密要求的方式进行，不得通过普通邮政、快递等无保密措施的渠道传递；指派专人传递时，要选择安全的交通工具和交通路线，并采取相应的安全保密措施；设有机要文件交换站的城市，在市内传递机密级、秘密级涉密载体，可以通过机要文件交换站进行。

54. 阅读和使用涉密载体如何管理？ 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；确需在办公场所以外阅读和使用涉密载体的，应当遵守有关保密规定。阅读和使用涉密载体，应当办理登记、签收手续，管理人员随时掌握涉密载体的去向。

55. 保存涉密载体如何管理？ 保存涉密载体应选择安全保密的场所和部位，配备必要的保密设施、设备，同时，应定期清查、核对，发现问题及时报告。离开办公场所，应将涉密载体存放在保密设备中。

56. 携带涉密载体外出如何管理？ 携带涉密载体外出，要采取严格的保密措施，使涉密载体始终处于携带人的有效管控之下。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，要经机关、单位负责人批准。

57. 维修涉密载体如何管理？ 维修涉密载体应由本机关、本单位内部专门技术人员负责。确需外单位人员维修的，要在本机关、本单位内部进行，并指定专人全程现场监督。确需送外维修的，应送保密行政管理部门审查批准的定点单位进行，并在送修前拆除信息存储部件。

58. 销毁涉密载体主要有哪些保密要求？ 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。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。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。涉密载体销毁的登记、审批记录应当长期保存备查。

59. 绝密级涉密载体有哪些特殊保密要求？ 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；未经原定密机关、单位或者上级机关批准，不得复制和摘抄；收发、传递和外出携带，应当指定人员负责，并采取必要的安全措施。

60. 机构撤并时如何移交、清退涉密载体？ 机构撤并时，原机构的涉密载体应根据不同情况，分别移交制发单位、档案管理部门或合并后的新单位。移交时，须履行登记、签收手续。制发单位不收回的，要按规定登记销毁。

六、 计算机及移动存储介质

61. 涉密计算机保密管理主要有哪些要求？ 新购置涉密计算机启用前，应进行保密技术检测。涉密计算机应按照存储、处理信息的最高密级管理，不得接入互联网及其他公共信息网络，不得在未采取防护措施的情况下在互联网及其他公共信息网络之间进行信息交换，不得擅自卸载、修改安全技术程序和管理程序，不得将未经安全技术处理的退出使用的涉密计算机赠送、出售、丢弃或者改作其他用途。

62. 为什么涉密计算机不得接入互联网等公共信息网络？ 涉密计算机接入互联网等公共信息网络，相当于将涉密信息公之于网、扩大知悉范围，且易被境外情报机构植入特种“木马”，实施网络攻击窃密。

63. 为什么涉密计算机安全保密防护软件和设备不得擅自卸载？ 擅自卸载涉密计算机安全保密防护软件和设备会使涉密计算机失去安全保密保障，带来泄密隐患。如，卸载防病毒软件，则易遭受网络攻击窃密；卸载主机监控与审计软件，则不易发现非法操作；卸载保密技术防护专用系统（“三合一”），则不易发现违规外联、介质交叉使用等行为。

64. 涉密计算机为什么不能安装来历不明的软件？ 涉密计算机安装来历不明的软件，特别是从互联网上下载的软件，很可能被境外情报机构捆绑上特种“木马”等间谍窃密程序，有的计算机病毒就是隐藏在软件中，甚至是伪装成杀毒软件进行传播。随意下载安装这些软件，很可能把与软件捆绑在一起的“木马”或计算机病毒等有害程序带到涉密计算机中。

65. 为什么不能将他人的文件、资料随意拷贝到涉密计算机上？ 他人的计算机或 U 盘可能连接过互联网，或被植入特种“木马”间谍窃密程序，或感染了病毒。随意将他人计算机或 U 盘上的文件、资料拷贝到涉密计算机上，极有可能使涉密计算机被植入“木马”间谍窃密程序或感染计算机病毒。

66. 怎样预防和查杀“木马”间谍程序？ 及时更新系统补丁，不接受、不运行来历不明的文件，不点击来历不明的链接，不浏览“诱人”的网页。安装并及时升级专业的“木马”查杀工具，开启实时监控，禁止 U 盘的自动运行。检查系统的自启功能，取消可疑的和不需要程序自启动。将系统启动到安全模式，删除感染“木马”的文件。对于捆绑在系统文件中的“木马”程序，应从其他系统拷贝同名文件覆盖被捆绑了“木马”的文件。

67. 为什么涉密计算机不得使用无线网卡、无线鼠标、无线键盘等无线设备？ 使用无线网卡，涉密计算机可与无线网络连接，会被境外情报机构攻击窃密。使用无线鼠标、无线键盘等无线设备，涉密信息会以无线信号形式传递，极易被他人截获，造成泄密。

68. 涉密计算机如何设置口令？ 秘密级计算机口令长度应不少于 8 位，更换周期不超过 1 个月。机密级计算机口令长度应不少于 10 位，更换周期不超过 1 个星期，也可采用 IC 卡或 USB Key 与口令（长度不少于 4 位）相结合的方式。秘密级、机密级计算机的口令设置，应采用多种字符和数字混合编制。绝密级计算机应采用生理特征等强身份鉴别方式，也可采用 IC 卡或 USB Key 与口令（长度不少于 6 位）相结合的方式。

69. 携带涉密笔记本电脑及其他涉密存储介质外出应当遵守哪些保密要求？ 在一般情况下，不允许携带涉密笔记本电脑及其他涉密存储介质外出。确需携带外出的，要严格履行审批手续，采取有效管理措施，确保涉密笔记本电脑及其他涉密存储介质始终处于有效监控之下。同时，应采取身份证、涉密信息加密等保密技术防护措施。

70. 涉密计算机改作非涉密计算机应当注意哪些问题？ 涉密计算机改作非涉密计算机使用、应当经过机关、单位批准，并采取拆除信息存储部件（如硬盘、内存）等安全技术处理措施。

71. 未经专业消磁的涉密计算机、涉密移动存储介质为什么不能随意淘汰、报废？ 涉密计算机或涉密移动存储介质中的信息作简单删除或格式化处理，难以达到彻底消除信息的目的，仍然可以使用数据恢复技术恢复信息，随意淘汰、报废极易造成泄密。只有经过专业消磁才能彻底消除涉密计算机和涉密移动存储介质中存储的涉密信息，使之无法通过任何技术手段还原。

72. 为什么涉密计算机删除涉密信息后仍不能连接互联网？ 涉密计算机中的涉密信息被删除或格式化后，通过一定的技术手段仍可以复原，连接互联网易造成泄密。

73. 为什么涉密计算机工作时电磁泄漏发射会导致泄密？ 计算机工作时会辐射电磁波，窃密者使用定向天线对准作为窃取目标的计算机在方向搜索信号，然后采用特殊方法过滤掉无用信号，将所需的图像信号放大，计算机显示屏上的图像及信息即可复现，造成泄密。

74. 非涉密计算机保密管理主要有哪些要求？ 严禁使用非涉密计算机存储、处理、传输涉密信息。涉密计算机与非涉密计算机之间进行信息交换，应采取保密防护措施。

75. 为什么涉密场所中连接互联网的计算机不能安装和使用摄像头等音视频输入设备？ 涉密场所是集中制作、使用、存放涉密载体和处理涉密信息的地方，有的涉密载体可能摆放在办公桌上，工作人员的谈话也可能涉及国家秘密。如果涉密场所中连接互联网的计算机安装和使用音频、视频输入设备，极易被窃听、窃照，造成泄密。

76. 私人计算机和移动存储介质为什么不能用于存储、处理涉密信息？ 私人计算机和移动存储介质属于私有财产，无法按照保密规定要求进行管理。同时，私人计算机和移动存储介质往往连接过互联网，存在很大的泄密隐患和安全风险，不能用于存储、处理涉密信息。

77. 为什么移动存储介质不得在涉密计算机和非法涉密计算机之间交叉使用？ 移动存储介质在非涉密计算机上使用时，有可能被植入“木马”程序。当这个移动存储介质又在涉密计算机上使用时，“木马”窃密程序会自动复制到涉密计算机中，并将涉密计算机中的涉密信息打包存储到移动存储介质上。当移动存储介质再次接入连接互联网的计算机时，涉密信息就会被自动发往指定主机，造成泄密。

七、网络

78. 什么是涉密网络？ 涉密网络是指存储、处理国家秘密信息的涉密计算机网络，按照存储、处理国家秘密信息的最高密级分为绝密级、机密级和秘密级。集中存储、处理工作秘密的网络，参照秘密级网络管理。

79. 涉密网络规划建设主要有哪些保密要求？ 涉密网络应当根据存储、处理信息的最高密级确定密级，按照同步规划、同步建设的要求，依据国家保密规定和标准，制定分级保护方案，采取身份鉴别、访问控制、安全审计、密码保护等技术措施。建设完成后，应当由国家保密行政管理部门设立或者授权的保密测评机构进行检测评估，并经设区的市、自治州级以上保密行政管理部门审查合格，方可投入使用。

80. 涉密网络建设承建单位应如何选择？ 涉密网络建设使用单位应在各级保密行政管理部门的指导与监督下，选择具有相应涉密资质的承建单位承担或者参与涉密网络的方案设计与实施、软件开发、综合布线、系统服务、系统咨询、风险评估、屏蔽室建设、工程监理和保密安防监控等。有技术实力的建设使用单位可以按照国家有关保密标准和规定组织自身技术力量自行进行方案设计和实施。

81. 涉密网络运行维护外包单位应如何选择？ 涉密网络运行维护服务外包的，应当选择具有相应涉密信息系统集成资质的单位，签订保密协议，明确保密责任，落实保密管理要求。

82. 涉密网络中使用的设备、软件应满足那些保密要求？ 涉密网络中使用的设备、软件应优先选用国产设备，确需选用进口设备的应进行详细调查和论证，不得选用国家保密行政管理部门规定禁用的设备或部件。涉密网络中的安全保密产品应选用经过国家保密行政管理部门授权的检测机构测评、符合国家保密标准要求的產品，计算机病毒防护产品应选用公安机关批准的国产产品，密码产品应选用国家密码管理部门批准的产品。

83. 涉密信息系统集成资质有哪些等级和种类？ 涉密信息系统集成资质分为甲级和乙级两个等级。甲级资质单位可在全国范围内从事绝密级、机密级和秘密级信息系统集成业务，乙级资质单位可在注册地省（区、市）行政区域内从事机密级、秘密级信息系统集成业务。涉密信息系统集成业务种类主要包括系统、系统咨询、软件开发、综合布线、安防监控、屏蔽室建设、运行维护、数据恢复、工程监理等。

84. 涉密网络运行使用主要有哪些保密要求？ 涉密网络应指定内部人员担任系统管理员、 安全保密管理员、 安全审计员；与互联网及其他公共信息网络实行物理隔离；统一采购、登记、标识、配备信息设备，并明确使用管理责任人；依据岗位职责严格设定用户权限；严格规范文件打印、存储介质使用等行为，严格控制信息输出；加强对用户操作记录的综合分析，及时发现违规或异常行为；将互联网及其他公共信息网络上的数据复制到涉密网络， 应采取病毒查杀、 单向导入等防护措施； 涉密网络建设和运行维护采用外包服务的，应选择具有相应涉密信息系统集成资质的单位，签订保密协议，严格保密管理措施。

85. 涉密网络“三员”的基本职责有哪些？ 系统管理员主要负责涉密网络的日常运行维护工作； 安全保密管理员主要负责涉密网络的日常安全保密管理工作， 包括用户账号管理以及安全保密设备和系统所产生日志的审查分析；安全审计员主要负责对系统管理员、安全保密管理员的操作行为进行审计、跟踪、分析和监督检查，以及时发现违规行为，并定期向涉密网络安全保密管理机构汇报相关情况。

86. 非涉密网络保密管理主要有哪些要求？ 非涉密网络严禁存储、处理、传递涉密信息，发现涉密信息应立即删除并及时报告。不得在互联网及其他公共信息网络或者未采取保

87. 涉密网络与非涉密网络之间的信息交换主要有哪些保密要求？ 在未采取防护措施的情况下， 不得在涉密网络与互联网及其他公共信息网络之间进行信息交换。 确需将互联网及其他公共信息网络上的数据复制到涉密网络中，应采取必要的防护措施，例如，使用一次性光盘刻录下载、设置中间机，或者使用经过国家保密行政管理部门批准的信息单向导入设备。

88. 为什么不能在政府门户网站上登载涉密信息？ 政府门户网站是建立在互联网上的信息发布平台， 在政府门户网站上登载涉密信息，相当于将涉密信息发布在互联网上。

八、 涉密场所声光电磁防护

89. 常见的窃听方式主要有哪些？ 常见的窃听方式主要有有线搭线窃听、无线窃听（包括专门的无线窃听器、手机窃听、智能终端窃听等）、激光探测窃听、定向探测窃听等。

90. 涉密场所防窃听应当采取哪些措施？ 有线窃听，可通过建设专用电话网、采用光纤传输等方式进行防范；无线窃听， 可通过建设电磁屏蔽室等方式进行防范； 激光窃听， 可通过加装能够阻挡激光的遮盖物或安装语音干扰装置等方式进行防范；定向窃听和振动窃听，可通过限制声源大小、实施隔声防护和管道消声、布置声掩蔽装置等方式进行防范。

91. 常见的窃照方式主要有哪些？ 常见的窃照方式主要有间谍卫星窃照、 高空侦察机窃照、 照相器材窃照、手机窃照、专用小型设备窃照等。

92. 涉密场所防窃照应当采取哪些措施？ 间谍卫星、高空侦察机对场所景象、建筑布局结构、 大型设备等的窃照，可采取伪装技术手段进行防范；照相器材、手机、专用小型设备对涉密文件、小型设备等的窃照，可采取出入口控制（门禁）、视频监控手段和微型电子设备监测、金属探测等检查手段进行防范。

93. 常见的电磁泄漏发射方式主要有哪些？ 常见的电磁泄漏发射方式主要有传导发射、 辐射发射、 耦合发射等。

94. 涉密场所电磁泄漏发射防护应当采取哪些措施？ 涉密设备分散、涉密程度高的场所，可采用低泄射计算机进行防护；涉密设备集中、涉密程度高的场所，可采用建设电磁屏蔽室、配置电磁屏蔽机柜的方式进行防护；处理机密级及以下密级信息的设备，可采用配备视频干扰器的方式进行防护。

九、 通信和办公自动化设备

95. 使用普通手机主要有哪些保密要求？ 使用普通手机，不得在通信中涉及国家秘密；不得存储、处理、传输涉及国家秘密的信息；不得连接涉密信息系统、涉密信息设备或者涉密载体；不得存储核心涉密人员的工作单位、职务、红机电话号码等敏感信息；不得在涉密公务活动中开启和使用位置服务功能；在申请手机号码、注册手机邮箱或者开通其他功能时，不得填写禁止公开的涉密单位名称和地址等信息；不得使用未经国家电信管理部门进网许可的手机；不得使用境外机构、境外人员赠送的手机。

96. 使用电话机和传真机等通讯设备主要有哪些保密要求？ 使用普通电话机、传真机不得谈论或传输涉密信息。传真涉密信息，必须使用国家密码管理部门批准使用的加密传真机。加密传真机只能传输机密级和秘密级信息，绝密级信息应送当地机要部门译发。

97. 使用复印机主要有哪些保密要求？ 非涉密复印机不得复印涉密文件、资料。涉密复印件应安放在符合保密要求的场所，指定专人管理，不得与互联网等公共信息网等公共信息网络连接。启用前应进行保密技术检查检测。

98. 使用打印机和扫描仪主要有哪些保密要求？ 非涉密打印机和扫描仪不得打印、扫描涉密文件、资料。涉密打印机和扫描仪不得与互联网等公共信息网络连接，与涉密计算机连接不得采用无线方式。涉密文件、资料打印机应进行审计记录。涉密文件、资料扫描应履行审批程序。

99. 涉密打印机、复印机、扫描仪、多功能一体机等办公自动化设备连入公共信息网络有哪些泄密隐患？ 打印机、复印机、扫描仪、多功能一体机等办公自动化设备具有信息存储功能，一旦接入公共信息网络，可被境外情报机构通过网络远程控制，窃取设备内存储的信息，造成泄密。

100. 涉密存储部件信息消除和数据恢复主要有哪些保密要求？ 涉密存储部件信息消除和数据恢复，应送交保密行政管理部门设立的工作机构或指定的单位进行，并严格履行清点、登记、交接手续。自行消除的，应采用符合国家保密标准的方法和工具，确保涉密信息无法还原。自行恢复的，应采取保密管理措施，确保涉密信息安全。

101. 淘汰、报废涉密办公自动化设备主要有哪些保密要求？ 淘汰、报废涉密办公自动化设备应进行清点、登记，经机关、单位的主管领导批准后，送交保密行政管理部门指定的涉密载体销毁机构销毁。禁止转送、捐赠他人，更不能当作废品出售或随意丢弃。

十、 保密要害部门、部位

102. 什么是保密要害部门、部位？ 保密要害部门，是指机关、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。保密要害部位，是指机关、单位内部集中制作、存储、保管涉密载体的专门场所。

103. 保密要害部门、部位确定应把握哪些原则和标准？ 保密要害部门、部位确定应把握内部确定、分级确定、分级确认和最小化的原则。保密要害部门应根据其产生、传递、使用和管理国家秘密的密级高低和数量多少确定，保密要害部位应视是否为集中制作、存储、保管涉密载体的专门场所而确定。

104. 保密要害部门、部位确定程序是什么？ 中央和国家机关及直属单位保密要害部门、部位由各机关、单位确定，报国家保密行政管理部门确认； 省级机关及直属单位保密要害部门、部位由各机关、单位确定，报所在省（区、市）保密行政管理部门确认，并报国家保密行政管理部门备案；中央和国家机关下属单位和省级以下机关、单位确定保密要害部门、部位，应报中央和国家机关保密工作机构或省（区、市）保密行政管理部门审核确认。

105. 保密要害部门、部位管理要求是什么？ 保密要害部门、部位实行“谁主管，谁负责”的原则，做到严格管理、责任到人、严密防范、确保安全。

106. 保密要害部门、部位人员管理主要有哪些保密要求？ 保密要害部门、部位工作人员上岗前要进行涉密资格审查和保密教育培训，审查合格的应签订保密承诺书，并定期进行在岗保密教育培训和考核，不得擅自离岗离职或因私出国（境）。

107. 保密要害部门、部位办公场所主要有哪些保密要求？ 保密要害部门、部位应当确定安全控制区域，根据周边环境特点和工作需要，采取电子监控、防盗报警等必要的安全防范措施。同时，确定进入人员范围，安装身份鉴别装置，或采取其他控制人员进入的措施，对进入的工勤人员应严格监督管理。

108. 保密要害部门、部位保密技术防护主要有哪些保密要求？ 保密要害部门、部门应按照国家保密标准配备保密技术防护设备，对使用的信息设备特别是进口设备和产品应进行保密技术检查检测。 保密要害部门禁止使用普通手机。保密要害部位禁止带入手机，确需将专用手机带入的，应经机关、单位保密委员会（领导小组）批准，并登记备案。未经批准不得带入有录音、录像、拍照、信息存储等功能的设备。

十一、涉密会议、活动

109. 涉密会议、活动保密管理原则是什么？ 涉密会议、活动应当按照“谁主办，谁负责”的原则进行管理，明确涉密会议、活动各方的保密管理职责。

110. 涉密会议、活动主办单位应采取哪些保密管理措施？ 涉密会议、活动主办单位应当根据会议、活动的内容确定密级，制定保密方案，限定参加人员范围；使用符合国家保密规定和标准的场所、设施、设备；按照国家保密规定管理文件资料、录音录像等涉密载体，涉密文件、资料应统一编号，明确传达范围，需发给与会人员单位的应通过机要交通或机要通信部门寄发； 对参加人员提出具体保密要求。 重大涉密会议、活动应当请保密行政管理部门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。

111. 涉密会议、活动承办单位应采取哪些保密管理措施？ 涉密会议、活动承办单位应按照主办单位要求，提供安全保密的环境、设施和设备，对工作人员进行保密教育，明确工作人员的保密责任并要求其做好保密服务保障工作。

112. 涉密会议、活动驻地宾馆主要有哪些保密要求？ 涉密会议、活动驻地宾馆保密要求主要有：会前对工作人员进行专题保密教育； 会议期间关闭与会人员、工作人员房间互联网接口， 关闭会场区域移动通信信号增强器和无线局域网接入设备； 严禁将会议须知、住房分配表等资料信息透露给无关人员； 与会人员房间电话应做到应允式

接入；商务中心不得承接涉密文件、资料复制、打印、传真等业务；工作人员不得打听会议内容，不得在会场逗留，不得向无关人员透露会议、活动信息；在会场、餐厅等公共场所发现会议文件、资料应及时交会议主办方，严禁留存、翻看、拍照、摄录、复制、传抄。

113. 参加涉密会议、活动的人员应注意哪些保密事项？ 参加涉密会议、活动的人员应遵守保密纪律和保密要求，不得擅自委托其他人员代替参加会议，不得擅自记录、录音、摄像，不得使用无线键盘、无线网卡等无线设备或装置。绝密级、机密级会议、活动场所禁止带入手机，确需将专用手机带入的，应经过机关、单位保密委员（领导小组）批准，并登记备案。对于举办地点、参加人员需要严格保密的涉密会议、活动，参加人员及随行人员不得携带手机前往。秘密级会议、活动场所禁止使用普通手机。

114. 参加涉密会议、活动领取的涉密文件、资料应如何使用保管？ 参加涉密会议、活动领取的涉密文件、资料和其他涉密载体应当妥善保管。注明“会后收回”或不允许由参加人员带回的文件、资料，应及时交还会议文件管理人员，不得擅自转借、传抄、摘抄、复印、扫描；允许带回的文件、资料，应及时交单位机要人员登记保存，个人不得留存。

115. 涉密会议、活动场所主要有哪些保密要求？ 涉密会议、活动应在符合保密要求的场所进行。会场及设施、设备应经保密技术检查检测。会场内应加装移动通信和无线网络屏蔽设备。携带、使用录音、录像设备应经主办单位批准。不得使用对讲机、无绳电话、无线话筒、无线键盘、无线网卡等无线设备或装置，不得使用不具备保密条件的电视电话会议系统。

116. 宣传报道涉密会议、活动应注意哪些事项？ 撰写新闻稿件应当认真遵守询问出版保密规定和会议保密要求，不得涉及国家秘密。会议、活动提供新闻通稿或报道口径的，应按照新闻通稿或报道口径报道。凡是公开报道、播放的稿件、图片、录像片、录音带等，应请有关业务主管部门或涉密会议、活动组织者审查批准。

117. 涉密视频会议主要有哪些保密要求？ 涉密视频会议除遵守涉密会议、活动保密管理一般要求外，应按照涉密网络有关要求建设和管理视频会议系统，指定专人负责视频会议系统运行维护和音视频录制，会议召开时应断开所有不参会会场的视频会议设备和网络连接，并对参会会场及设施设备进行安全保密检查，会议音视频资料应按照涉密载体管理。

十二、 政府信息公开保密审查

118. 保密审查的原则是什么？ 保密审查应坚持“先审查、后公开”和“一事一审”的原则。

119. 保密审查工作的要求是什么？ 建立健全信息公开保密审查机制，严格审查责任和程序，明确审查机构。审查工作应由领导分管，部门负责，专人实施。保密审查工作人员应强化保密意识，熟练掌握保密审查工作有关法律法规。

120. 保密审查内容是什么？ 保密审查主要是依据国家秘密的基本范围和保密事项范围对拟公开发布的信息是否涉及国家秘密进行审查，也包括依据相关法律法规对是否涉及工作秘密、商业秘密、个人隐私等进行甄别鉴定，以确认拟发布的信息是否可以公开。

121. 保密审查方式有哪些？ 保密审查方式主要分为目录审查和信息审查。目录审查是对本机关、本单位制定的信息公开目录进行审查，信息审查是对拟公开的具体信息进行审查。

122. 保密审查程序是什么？ 对拟公开政府信息进行保密审查，应由承办单位提出具体意见，经机关、单位指定的保密审查机构审查后，报机关、单位有关负责同志审批。未经审查和批准，不得对外公开发布政府信息。

123. 在保密审查过程中对是否属于国家秘密的不明确事项如何处理？ 在保密审查过程中对是否属于国家秘密的不明确事项，应当报送保密保密行政管理部门审查确定，涉及业务工作的应当听取业务主管部门的意见。遇有可能涉及国家安全、公共安全、经济安全和社会稳定的重大拟公开事项，应与有关部门协调会商。

124. 保密审查特殊情况如何处理？ 对已解密的不属于本机关、本单位产生的国家秘密事项，需要公开的，应当经原定密机关、单位同意；对仍在保密期限内的国家秘密，需要公开的先由原定密机关、单位或其上级机关依法解密，再进行保密审查确定；对保密期限届满的国家秘密，需要公开的仍应进行保密审查确定。

125. 政府网站发布信息对网站管理部门和承办单位主要有哪些保密要求？ 网站管理部门应建立政府信息发布登记制度，承办单位应向网站管理部门提供保密审查机构的审查意见和机关、单位负责同志的审批意见，网站管理部门要做好相应记录备查。

十三、 专项保密工作

126. 涉密经济数据管理主要有哪些保密要求？ 知悉人员应当作出保密承诺，不得向知悉范围之外的任何单位、个人提供涉密数据或者可据以推断涉密数据的统计资料，不得以“预测”等方式变相提供涉密数据。报送、交换涉密数据应严格履行清点、登记、编号、签收手续，复制涉密数据应经主管领导批准。接受新闻单位采访、参加学术活动、出席会议或者发表研究文章时，不得涉及涉密数据及相关信息。

127. 国家统一考试主要有哪些保密要求？ 命题人员和内部工作人员应强化保密意识，签订保密承诺书。命题工作应采取入闱工作形式，原始试题应在安全保密的场所和设备中存放并由两人专门保管。考试试卷应在定点印制单位印制；运送应通过机要渠道或使用可靠的交通工具，由两人以上专门押送，并严格履行交接查验手续；封存场所应采取必要的安全保密措施，24小时两人守卫。以电子信息形式进行考试的，应严格计算机、网络和移动存储介质的保密管理，并采取必要的安全保密防范措施。

128. 涉密测绘成果资料管理主要有哪些保密要求？ 涉密测绘成果资料一律由测绘管理部门提供。借领涉密测绘成果资料应严格履行审批程序。复制涉密测绘成果资料须经省级以上测绘行政管理主管部门批准。递送涉密测绘成果资料应由机要部门寄送或由两人以上携带押运。

129. 涉密科研项目管理主要有哪些保密要求？ 涉密科研项目下达单位和承担单位应做好科研项目全过程保密管理。在项目立项阶段，项目下达单位应做好项目原始定密工作，选择具有相应保密资格的承担单位，与项目承担单位签订保密协议；项目承担单位应做好项目密级分解工作，与协作配套单位签订保密协议。在项目研究阶段，项目承担单位应制定项目各个环节保密制度，采取保密措施、落实保密责任，组织参研人员签订保密承诺书，加强涉密科研项目文件、资料管理，完善涉密科研场所人防、物防、技防等措施。在项目结题阶段，应明确对评审人员的保密要求，加强成果验收、申报奖项、申请专利等工作的保密管理。

130. 涉密工程管理主要有哪些保密要求？ 涉密工程应经本机关、本单位主要负责人审核批准后，报保密行政管理部门审查。申报单位（或者代建单位）、承建单位应当建立或者指定专门工作机构，负责涉密工程保密管理工作；制定保密管理方案，明确保密要素和关键部门、部位，明确保密责任和人员分工；签订保密协议；建立涉密文

件、资料和图纸，涉密信息系统，涉密人员以及保密要害部门、部位等方面的保密制度；落实法律法规或者规范性文件规定的其他保密措施。

131. 保密重点领域主要有哪些保密要求？ 外交、政法、科技、教育、金融、能源资源、测绘、军工等重点领域业务主管部门应认真履行本行业保密管理指导职责， 会同国际保密行政管理部门制定本领域保密事项范围并定期审查，建立保密工作联动机制；重点领域各机关、单位应制定保密管理相关制度和措施，在加强国家秘密管理的同时，做好涉及国家经济命脉、能源资源安全和社会公共安全的商业秘密、工作秘密管理。

132. 保密重点区域主要有哪些保密要求？ 保密重点区域应经保密行政管理部门批准，建立保密、公安、国家安全、工业和信息化、工商、国防科工、军队等部门协作机制，加强信息通报交流、联合检查、周边环境综合治理等工作，强化保密技术防护设施设备配备、保密宣传教育培训，做好窃密泄密事件应急处置工作，切实维护国家秘密安全。

十四、涉外活动

133. 涉外活动主要有哪些保密要求？ 涉密活动不得带领国（境）外人员进入涉密场所和涉密部门、部位。与国（境）外人员会谈不得涉及国家秘密。出入国（境）外驻华组织、机构和国（境）外人员驻地或陪同国（境）外人员活动不得携带涉密载体。 遇有国（境）外人员要求提供有关涉密信息的应予以拒绝， 并及时向机关、 单位报告。不得利用国（境）外通信设施进行涉密通信联络，不得使用国（境）外人员办公设备处理涉密信息。

134. 驻外机构和企业保密管理主要有哪些要求？ 严格驻外机构和企业派出人员政审，加强工作人员日常保密教育培训和保密管理。涉及敏感项目（军贸、军工技术项目等）驻外机构和企业原则上不许雇用当地或外籍人员，确因工作需要雇用的应进行严格审批。 办公场所应配备必要的保密设施、 设备，场所设备应定期进行保密技术检查检测。涉密载体应严格按照有关保密规定管理。

135. 因公出国（境）团组保密管理主要有哪些要求？ 因公出国（境）团组实行“谁派出谁负责、谁组团谁负责”，坚持内外有别、专人负责、全程管理、确保安全的原则。团组出国（境）前应对在国（境）外期间涉密活动的组织管理作出安排，明确保密管理措施。派出机关、单位应对出国（境）人员进行保密教育。使用计算机处理涉密信息应在我驻外使（领）馆屏蔽室内或符合安全保密要求的场所进行。 召开涉密或者重要敏感事项的会议应在我驻外使（领）馆、驻外机构或符合安全保密要求的场所进行。确需出国（境）携带或在国（境）外制作、复制、使用、保管涉密载体的，应严格按照涉密载体有关保密管理规定执行。

136. 对外提供国家秘密资料主要有哪些保密要求？ 任何组织和个人不得擅自对外提供国家秘密资料。确需提供的应确定范围， 进行保密审查并进行必要的技术处理， 报有审批权限的部门批准， 并按照政府间保密协定或根据有关保密法律法规，与接受方签订保密协议，要求其承担保密义务。

137. 涉密载体携运出国（境）主要有哪些保密要求？ 确因工作需要携运涉密载体出国（境），须交由外交信使或者国家保密行政管理部门核准的单位和个人携运。 目的地不通外交信使或者外交信使难以携运的， 确因工作需要，需自行携运机密级、秘密级载体出国（境）的，应严格履行审批手续，并使涉密载体始终处于有效控制之下。不得携运绝密载体出国（境），不得把密件夹放在托运的行李中托运。携运出国（境）的涉密载体，凡可以由我国驻外使（领）馆或驻外机构代为保存的，应当尽快交其代为保存；不能交使（领）馆保存的，应当采取严格的保密管理措施。

138. 国家秘密技术出口主要有哪些保密要求？ 国家秘密技术出口应根据不同密级分别报有关主管部门审查批准。秘密级技术按照行政隶属关系报省（区、市）、计划单列市科技工作主管部门或者国务院有关主管部门审查批准，并报国家科技部门备案； 机密级技术按照行政隶属关系报省（区、市）、计划单列市科技工作主管部门审查后，报国家科技部门审批；绝密级技术禁止出口，特殊情况需要出口的，由省（区、市）、计划单列市科技工作主管部门或者国务院主管部门提出申请，经国家科技部门审查后，报国务院批准。

139. 任用、聘用的国（境）外人员接触、知悉国家秘密主要有哪些保密要求？ 任用、聘用的国（境）外管理人员、科研人员在工作中确需接触、知悉我国国家秘密的，按照“谁主管，谁负责”和“一事一批”原则，报国务院有关主管部门或者省（区、市）、人民政府有关主管部门批准。机关、单位任用、聘用国（境）外人员的，根据有关保密法律法规，与拟接触、知悉国家秘密的国（境）外人员签订保密协议，要求其承担保密义务。机关、单位应指定专门机构和人员对保密协议执行情况进行经常性的监督检查， 发现违反保密协议的情形或存在威胁国家秘密安全行为，应立即采取有效措施。

十五、保密工作责任制

140. 保密工作责任制主要有哪些？ 保密工作责任制主要有：领导干部保密工作责任制，机关、单位保密工作责任制，涉密人员保密工作责任制、保密行政管理部门工作责任制等。

141. 领导干部保密工作责任制有哪些？ 领导干部保密工作责任制主要有：带头遵守保密纪律；学习掌握保密知识技能；履行保密工作领导责任；自觉接受保密监督、检查和考核；严格管理亲属子女和身边工作人员等。

142. 机关、单位保密工作责任有哪些？ 机关、单位保密工作责任主要有：贯彻落实党和国家保密工作方针政策和保密法律法规；建立保密工作机构并指定人员负责保密工作；提供人力、财力、物力保障；将保密工作情况纳入考核体系；配合保密行政管理部门严肃查处泄密事件；对下级单位的保密工作进行指导和监督等。

143. 涉密人员保密工作责任有哪些？ 涉密人员保密工作责任主要有：严格遵守保密法律法规、规章制度；自觉接受保密教育培训；依法保管和使用涉密载体及设施、设备；制止和纠正违反保密规定的行为；接受保密监督检查；发现泄密隐患或泄密行为及时报告，并积极采取补救措施等。

十六、保密违法违纪责任

144. 保密法规定的 12 种严重违规行为是什么？ 保密法规定的 12 种严重违规行为是：非法获取、持有国家秘密载体；买卖、转送或者私自销毁国家秘密载体；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；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；非法复制、记录、存储国家秘密；在私人交往和通信中涉及国家秘密；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；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；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；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；擅自卸载、修改涉密信息系统的安全技术程序、管理程序；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。

145. 刑法对泄露国家秘密的犯罪有哪些规定？ 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；情节特别严重的，处十年以上有期徒刑

刑或者无期徒刑；情节较轻的，处五年以下有期徒刑、拘役、管制或者剥夺政治权利。第二百八十二条规定，以窃取、刺探、收买方法，非法获取国家秘密的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利；情节严重的，处三年以上七年以下有期徒刑。非法持有属于国家绝密、机密的文件、资料或者其他物品，拒不说明来源与用途的，处三年以下有期徒刑、拘役或者管制。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，情节严重的，处三年以下有期徒刑或者拘役；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。

146. 最高人民检察院关于故意泄露国家秘密罪的立案标准是什么？ 涉嫌下列情形之一的，应以故意泄露国家秘密罪立案：泄露绝密级国家秘密 1 项（件）以上的；泄露机密级国家秘密 2 项（件）以上的；泄露秘密级国家秘密 3 项（件）以上的；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；通过口头、书面或网络等方式向公众散布、传播国家秘密的；利用职权指使或者强迫他人违反保守国家秘密法的规定泄露国家秘密的；以牟取私利为目的泄露国家秘密的；其他情节严重的情形。

147. 最高人民检察院关于过失泄露国家秘密罪的立案标准是什么？ 涉嫌下列情形之一的，应以过失泄露国家秘密罪立案：泄露绝密级国家秘密 1 项（件）以上的；泄露机密级国家秘密 2 项（件）以上的；泄露秘密级国家秘密 3 项（件）以上的；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连接，泄露国家秘密的；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；其他情节严重的情形。

148. 公务员泄露国家秘密和工作秘密应受到哪些行政处分？ 公务员泄露国家秘密、工作秘密、造成不良后果的，给予警告、记过或者记大过处分；情节较重的，给予降级或者撤职处分；情节严重的，给予开除处分。

149. 机关、单位违反保密法规定，有关人员应受到哪些行政处分？ 机关、单位违反保密法规定，发生重大泄密案件的由有关机关、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；不适用处分的人员由保密行政管理部门督促其主管部门予以处理。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。

150. 共产党员泄露党和国家秘密应当受到哪些党纪处分？ 党的纪律处分条例规定，丢失秘密文件资料或者泄露党和国家秘密，情节较轻的，给予警告或者严重警告处分；情节较重的，给予撤销党内职务或者留党察看处分；情节严重的，给予开除党籍处分。在保密工作方面不负责任，致使发生重大失泄密事故，造成或者可能造成较大损失的，对负有主要领导责任者，给予警告或者严重警告处分；造成或者可能造成重大损失的，对负有领导责任的，给予撤销党内职务处分。