武器装备科研生产单位二级保密资格标准

1 适用范围

1.1 本标准为武器装备科研生产单位二级保密资格审查认定的依据。

2 实施要求

2.1 积极防范，突出重点，严格标准，依法管理。

2.2 业务工作谁主管，保密工作谁负责，促进保密工作与业务工作相融合。

2.3 规范定密，严格按照工作需要控制国家秘密的知悉范围。

2.4 健全保密管理体系，提升系统防范能力。

3 保密责任

3.1 法定代表人或者主要负责人责任

3.1.1 对本单位保密工作负全面领导责任；

3.1.2 贯彻党和国家有关保密工作的方针政策和法律法规，并提出明确落实要求；

3.1.3 了解和掌握单位保密工作情况，及时研究解决保密工作重大问题；

3.1.4 为保密工作提供人力、财力、物力等条件保障；

3.1.5 监督保密工作责任制的落实。

3.2 分管保密工作负责人责任

3.2.1 对本单位保密工作负具体领导责任；

3.2.2 组织研究和部署落实保密工作；

3.2.3 协调解决保密工作中的重点、难点问题；

3.2.4 监督、检查保密工作落实情况；

3.2.5 为保密工作机构履行职责提供保障。

3.3 其他负责人责任

3.3.1 对分管业务范围内的保密工作负直接领导责任；

3.3.2 将保密管理要求融入分管业务工作；

3.3.3 组织制定分管业务范围内的保密管理制度和措施，并督促检查落实；

3.3.4 在分管业务范围内为保密工作开展提供保障。

3.4 涉密部门负责人或者涉密项目负责人责任

3.4.1 对本部门或者本项目的保密工作负直接管理责任；

3.4.2 明确部门或者项目内人员的保密职责，按照工作需要控制国家秘密的知悉范围；

3.4.3 将保密管理要求融入业务工作制度中；

3.4.4 采取具体措施组织落实单位保密工作部署；

3.4.5 开展日常保密教育和监督检查。

3.5 涉密人员责任

3.5.1 对本职岗位保密工作负直接责任；

3.5.2 掌握基本的保密知识、技能和要求；

3.5.3 遵守保密法规制度，履行岗位保密职责；

3.5.4 及时报告泄密隐患，制止违法违规行为。

4 归口管理

单位科研生产、人力资源、信息化、新闻宣传、外事等职能部

门，应当明确职责，结合各自业务工作实际，归口负责业务工作范围内的保密管理工作和相关工作制度制定。

5 保密组织机构

5.1 保密委员会（保密工作领导小组）

5.1.1 单位应当成立保密委员会（保密工作领导小组），保密委员会（保密工作领导小组）为单位保密工作领导机构，应当明确职责并制定工作规则。

5.1.2 保密委员会（保密工作领导小组）由单位负责人和有关部门负责人组成，并明确职责分工。保密委员会（保密工作领导小组）主任（组长）由单位负责人担任。

5.1.3 保密委员会（保密工作领导小组）应当实行例会制度，对保密工作进行研究、部署和总结，重要问题应当及时研究解决。

5.1.4 保密委员会（保密工作领导小组）成员应当每年向保密委员会（保密工作领导小组）报告履职情况。

5.1.5 保密委员会（保密工作领导小组）应当设立办公室，承办日常工作。

5.2 保密工作机构

5.2.1 单位应当设置专门负责保密管理工作的职能部门，独立行使保密管理职能。

单位涉密人员 200 人以下的，可不设立专门部门，但应当确定一个部门履行保密管理职责。

5.2.2 保密工作机构主要职责

5.2.2.1 组织落实保密委员会（保密工作领导小组）工作部署；

5.2.2.2 组织制定保密基本制度，拟制年度保密工作计划，对落实保密工作提出意见建议；

5.2.2.3 监督指导各部门保密工作；

5.2.2.4 组织确定和调整保密要害部门部位；

5.2.2.5 组织开展保密检查；

5.2.2.6 组织查处违反保密法律法规的行为和泄密事件；

5.2.2.7 提出保密责任追究和奖惩建议。

5.3 保密工作机构人员配备

5.3.1 涉密人员 100 人（含）以上的，专职保密工作人员配备不得少于 1 人；涉密人员 100 人以下的，应当配备兼职保密工作人员。

单位应当确定一部门负责人担任保密工作机构负责人。

5.3.2 专职保密工作人员 2 人（含）以上的，应当配备 1 名保密技术管理人员。

5.3.3 保密工作机构人员条件

5.3.3.1 具备良好的政治素质；

5.3.3.2 熟悉保密法律法规，掌握保密知识技能，具有一定的管理能力；

5.3.3.3 熟悉本单位业务工作和保密工作情况；

5.3.3.4 经过保密知识技能培训。

6 保密制度

6.1 保密制度应当全面、规范，具有可操作性，并根据实际情况及时修订。

6.2 单位应当建立保密基本制度，包括保密责任（含归口管理责

任），定密工作，涉密人员，保密教育培训，国家秘密载体，密品，保密要害部门部位，信息系统、信息设备和存储设备，新闻宣传，涉密会议，协作配套，涉外活动，外场试验，保密监督检查，泄密事件报告和查处，考核与奖惩等方面基本要求。

6.3 重大涉密工程或者项目应当制定专项保密制度

6.4 单位各职能部门应当将保密管理要求融入业务工作制度中，并组织落实。

7 保密管理

7.1 定密管理

7.1.1 单位应当根据定密权限依法开展定密工作。

7.1.2 单位应当明确定密程序，制定国家秘密事项范围细目，并根据情况变化及时调整。

7.1.3 单位对产生的国家秘密事项应当及时确定密级、保密期限和知悉范围。

7.1.4 法定代表人或者主要负责人对单位定密工作负总责。法定代表人或者主要负责人可以根据工作需要指定定密责任人，明确定密权限。

7.1.5 定密责任人应当接受定密培训，经考核具备上岗能力。

7.1.6 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。

7.1.7 单位应当每年组织对本单位产生的国家秘密事项进行审核，做好国家秘密变更和解除工作。

7.2 涉密人员管理

7.2.1 单位应当对岗位和人员的涉密等级作出界定。

涉密岗位和人员的涉密等级分为核心、重要和一般三个等级。

7.2.2 涉密人员的涉密等级，应当根据情况变化，及时进行调整。

7.2.3 进入涉密岗位的人员应当通过审查和培训，签订保密承诺书，并定期组织复审。

7.2.4 单位应当对在岗涉密人员进行保密教育培训，每人每年度不少于 15 学时。

7.2.5 涉密人员严重违反保密制度的，应当及时调离涉密岗位。

7.2.6 单位应当每年对涉密人员进行考核，考核不合格的，应当及时调离涉密岗位。

7.2.7 单位应当根据涉密人员的涉密等级，给予相应的保密补贴。

7.2.8 单位应当及时将涉密人员在公安机关出入境管理机构备案。涉密人员出国（境）应当履行审批程序，出国（境）前单位应当对其进行保密教育，返回后及时进行回访。擅自出国（境）或者逾期不归的，单位应当立即向上级机关、单位和有关部门报告。

7.2.9 单位应当对涉密人员的出入境证件实行统一管理。

7.2.10 挂职返聘借调、学习实习人员从事涉密工作以及临时参与涉密业务的，由用人单位按照涉密人员进行管理。

7.2.11 涉密人员离岗离职，应当在离岗离职前清退保管和使用的国家秘密载体、涉密信息设备、涉密存储设备和密品等，并与单位签订保密承诺书，明确应当承担的法律责任和具体脱密期限。单位应当按照有关规定对其实行脱密期管理。

7.3 国家秘密载体管理

7.3.1 国家秘密载体应当相对集中管理，建立台账，做到账物相符，追溯期限不少于 3 年。

7.3.2 国家秘密载体应当按照有关规定作出国家秘密标志，标明密级和保密期限。

7.3.3 制作、收发、传递、使用、复制、保存、维修和销毁国家秘密载体，应当符合有关规定。

7.3.4 单位应当根据工作需要，严格控制国家秘密的知悉范围。持有国家秘密载体或者知悉国家秘密，应当履行审批程序。

7.3.5 机密级(含)以下国家秘密载体应当存放在密码文件柜中，绝密级国家秘密载体应当存放在密码保险柜中。

7.3.6 国家秘密载体的管理和使用，应当禁止以下行为：

7.3.6.1 非法获取、持有国家秘密载体；

7.3.6.2 非法复制、记录、存储国家秘密；

7.3.6.3 买卖、转送或者私自销毁国家秘密载体；

7.3.6.4 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；

7.3.6.5 邮寄、托运国家秘密载体出境；

7.3.6.6 未经有关主管部门批准，携带、传递国家秘密载体出境。

7.4 密品管理

7.4.1 密品应当确定密级，按照国家有关规定作出国家秘密标志，并在有关技术文件中注明。

7.4.2 密品应当建立台账，做到账物相符。

7.4.3 对外形和构造容易暴露国家秘密的密品，在研制、生产、

试验、运输、保存、维修、使用过程中应当对其采取遮挡或者其他保护性措施。

7.4.4 密品禁止通过普通邮政、快递等渠道传递。重要密品运输应当制定安全保密方案，落实安全保密措施，并做好记录。

7.4.5 密品销毁应当履行审批程序，选择符合保密要求的部门、单位、场所进行，指定人员监销。

7.5 保密要害部门部位管理

7.5.1 单位应当按照有关规定确定保密要害部门部位。

7.5.2 保密要害部门应当实行区域隔离，并采取出入口控制、入侵报警、视频监控等技防措施。

7.5.3 保密要害部位应当实行物理防护，并采取出入口控制、入侵报警、视频监控等技防措施。

7.5.4 非授权人员进入保密要害部门部位应当履行审批程序、登记，并采取监督管理措施。

7.5.5 未经批准，不得将具有无线通信功能的设备和具备拍摄、录音等功能的电子设备带入保密要害部门部位。严禁将手机带入保密要害部门部位。

7.5.4 对进入保密要害部门部位的工勤服务人员应当采取相应的保密管理措施。

7.5.6 对进入保密要害部门部位的工勤服务人员应当采取相应的保密管理措施。

7.5.7 涉及保密要害部门部位的工程建设项目要符合安全保密要求，所采取的保密防护措施应当经过单位保密工作机构审核，与

工程建设同计划、同设计、同建设、同验收。

7.6 信息系统、信息设备和存储设备管理

7.6.1 信息系统、信息设备和存储设备包含各类应用系统、服务器、计算机、网络设备、外部设施设备、存储介质、办公自动化设备、声像设备和安全保密产品。

7.6.2 涉密信息系统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系统测评或者风险评估，并经设区的市、自治州级以上保密行政管理部门审查合格，取得《涉及国家秘密的信息系统使用许可证》。许可证涉及事项发生变化时，应当按照有关规定及时报告。申请系统测评或者风险评估的拓扑结构应当与网络实际情况一致。

7.6.3 信息系统、信息设备和存储设备的管理和使用应当符合国家有关保密法律法规和标准要求，禁止以下行为：

7.6.3.1 将涉密信息系统、涉密信息设备和涉密存储设备接入互联网及其他公共信息网络；

7.6.3.2 在未采取防护措施的情况下，在涉密信息系统、涉密信息设备和涉密存储设备与互联网及其他公共信息网络之间进行信息交换；

7.6.3.3 使用非涉密信息系统、非涉密信息设备和非涉密存储设备存储、处理、传输国家秘密信息；

7.6.3.4 在未采取保密措施的有线或者无线通信中传递国家秘密；

7.6.3.5 未经安全技术处理，将退出使用的涉密信息设备、涉密

存储设备赠送、出售、丢弃或者改作其他用途；

7.6.3.6 擅自卸载、修改涉密信息系统、涉密信息设备和涉密存储设备的安全技术程序、管理程序；

7.6.3.7 擅自访问、下载、存储、传输知悉范围以外的国家秘密；

7.6.3.8 擅自扫描或者检测涉密信息系统的网络基础设施、安全保密产品以及应用系统等。

7.6.4 单位应当明确信息化管理部门，负责信息系统、信息设备和存储设备的安全保密管理；指定或者委托具有相应资质的机构（单位）负责信息系统、信息设备和存储设备的运行维护。

7.6.4.1 信息化管理部门应当组织制定由信息安全策略、管理制度和操作规程等组成的信息安全保密管理体系文件，对信息系统、信息设备和存储设备的运行维护工作进行监管，组织对信息系统、信息设备和存储设备的安全保密检查。

7.6.4.2 运行维护机构应当制定运行维护工作制度和操作规程，落实信息系统、信息设备和存储设备的安全保密要求。

7.6.5 涉密信息系统应当配备系统管理员、安全保密管理员和安全审计员（简称“三员”）。未建立涉密信息系统仅使用涉密计算机的单位，至少应当配备涉密计算机安全保密管理员。

7.6.5.1“三员”的配备和权限设置应当相互独立、相互制约，不得兼任或者交叉替代。

7.6.5.2 单位应当组织“三员”参加保密行政管理部门、国防科技工业管理部门，或者保密行政管理部门授权的其他部门组织的培训，具备岗位所要求的专业能力。

7.6.6 信息设备和存储设备应当根据存储、处理、传输信息的最高密级确定涉密等级和责任人，并按规定程序进行变更和调整。

7.6.7 应当建立信息系统、信息设备和存储设备台账，做到信息要素完整、账物相符。涉密信息系统、涉密信息设备和涉密存储设备应当实行全生命周期管理。

7.6.8 信息设备、存储设备应当具有标识，标识的信息要素应当完整，涉密的标明密级，非涉密的标明用途并粘贴保密提醒；涉密信息设备和涉密存储设备中存储的涉密信息应当具有密级标志。

7.6.9 测试、调试、仿真、工控、数控等专用系统或者设备应当明确涉密等级和保护要求，采取管控措施，保证信息流向安全可控。因特殊工作需要，涉密网络与非涉密网络、工业控制系统连接实时进行特定信息交换的，应当制定专门的安全保密方案报国家保密行政管理部门审查。

7.6.10 应当根据工作需要，配备专供外出携带的涉密信息设备和涉密存储设备，并由专人集中管理。携带外出应当履行审批程序，带出前和带回时应当进行保密检查，外出期间应当按照保密要求管理和使用。

7.6.11 涉密信息系统、涉密信息设备和涉密存储设备应当按照规定程序进行维修和报废。维修中应当对存储过涉密信息的硬件和固件采取有效的管控措施，对外来维修人员履行审批程序并全程旁站陪同。

7.6.12 涉密信息系统、涉密信息设备和涉密存储设备使用的安全保密产品、具有安全保密功能的信息设备、虚拟化产品，应当通

过国家相关主管部门授权测评机构的检测。使用中应当按照安全保密要求设置相关策略。涉密信息系统、涉密信息设备、涉密存储设备和传输线路的电磁泄漏发射防护，应当符合国家有关规定和标准要求。

7.6.13 涉密信息系统、涉密信息设备和涉密存储设备，不得具有无线通信功能，不得连接具有无线通信功能的设备。因特殊工作需要采用无线方式接入的，应当采用国家保密行政管理部门检测合格的安全保密设施设备和国家密码管理部门检测合格的密码设备，并制定专门的安全保密方案报国家保密行政管理部门审查。

7.6.14 涉密服务器和涉密计算机重装操作系统、安装或者拆卸软硬件应当履行审批程序；涉密信息系统和涉密信息设备使用的各种软件应当统一管理。

7.6.15 涉密信息系统和涉密信息设备的身份鉴别应当符合有关规定和标准要求

7.6.15.1 应当根据涉密信息系统和涉密信息设备的保护级别，采取相应的身份鉴别方式。

7.6.15.2 用于身份鉴别的物理装置应当参照国家秘密载体的要求严格管控。

7.6.16 涉密信息系统和涉密信息设备应当建立符合有关规定和标准要求的访问控制措施。

7.6.16.1 应当根据国家秘密的知悉范围，实现主体对客体的访问授权。

7.6.16.2 应当采取管理或者技术措施，防止信息设备、存储设

备的非授权接入以及信息的非授权输入输出。

7.6.16.3 多人共同使用一台涉密信息设备或者涉密存储设备时，应当控制每个用户的访问权限，确保涉密信息不被他人非授权访问或者获取。

7.6.17 涉密信息系统、涉密信息设备和涉密存储设备的信息导入导出应当履行审批程序，指定人员负责。

7.6.18 涉密信息系统机房应当确定为保密要害部位，采取符合有关规定和标准要求的安全控制措施。

7.6.19 涉密服务器应当按照有关规定和标准要求严格管控。

7.6.20 应当对涉密信患系统中关键业务数据采取备份措施，并采取技术措施实现备份与恢复中的权限控制；对数据库服务器、磁盘阵列中集中存储的涉密信息，应当采取管理和技术措施，实现安全可控。

7.6.21 应当定期对涉密信息系统、涉密信息设备和涉密存储设备进行审计，并对审计内容进行综合安全分析，形成审计报告，报信息化管理部门和分管业务负责人。

7.6.22 应当定期对涉密信息系统、涉密信息设备和涉密存储设备进行风险自评估，查找脆弱性和威胁，确定风险和隐患，及时采取整改措施，并报信息化管理部门和分管业务负责人。

7.6.23 应当建立互联网接入审批和登记制度，严格控制互联网接入口数量，并采取符合有关规定和标准的监管技术措施。

7.7 新闻宣传管理

7.7.1 涉及武器装备科研生产事项的宣传报道、展览、发表著作

和论文等，应当经合同甲方单位审批。

7.7.2 涉及涉密武器装备科研生产事项的参观、采访，应当按照规定履行审批程序，提出保密要求。

7.8 涉密会议管理

7.8.1 涉密会议应当确定密级，在具备安全保密条件的场所召开。

7.8.2 应当严格控制与会人员范围，对进入会场人员进行身份登记确认。

7.8.3 会议涉密载体发放、清退、保管和销毁应当指定人员负责，履行相关手续。

7.8.4 会议使用的音像等技术设备应当符合保密要求；会议场所禁止带入手机等移动通信工具。未经批准不得将具备拍摄、录音功能的设备带入会议场所。

7.9 外场试验管理

7.9.1 外场试验单位应当制定保密方案，指定保密负责人。试验现场的保密管理工作由牵头单位组织协调，参试人员应当遵守试验现场的保密管理规定。

7.9.2 外场试验数据交换和通信应当采取保密措施。

7.9.3 对涉密载体和密品的管理应当符合安全保密要求。

7.9.4 外场试验牵头单位应当定期对试验现场的保密工作进行检查。

7.10 协作配套管理

7.10.1 分包涉密项目，应当选择具有相应保密资格的单位。《武器装备科研生产许可目录》之外的应急或者短期生产秘密级项目，

选择非保密资格单位的，分包单位应当按照有关保密规定和程序对承制方进行保密审查，签订保密协议，提出保密要求，履行保密监管责任。

7.10.2 严格控制分包项目的涉密内容，不得提供项目研制必需之外的涉密信息。

7.10.3 与协作配套单位签订的合同中，应当有保密条款或者签订保密协议，明确界定合同文本和项目的密级、保密要求和保密责任，并监督执行。

7.10.4 涉及军工单位的涉密信息系统集成、国家秘密载体印制、军工涉密业务咨询服务等业务，应当从取得相关涉密资质的单位中选择。

7.11 涉外管理

7.11.1 对外交流、合作和谈判等外事活动应当制定保密方案，明确保密事项，采取相应的保密措施，执行保密提醒制度。

7.11.2 接待境外人员来访，应当按照有关规定履行审批程序，对来访人员进行身份确认，明确活动区域，采取必要的安全保密防范措施。

7.11.3 对外交流内容、谈判口径、提供资料和产品应当经过保密审查；涉及国家秘密的，应当按照有关规定履行审批程序。

8 监督与保障

8.1 保密检查

8.1.1 单位应当每半年组织一次保密检查；对发现的问题提出书面整改要求，并督促整改。

8.1.2 涉密部门应当每季度进行一次自查，自查及整改情况报单位保密工作机构。

8.1.3 单位应当根据工作情况组织开展专项检查。

8.1.4 单位应当根据日常管理和检查情况，对单位存在的保密风险进行分析，提出改进措施，并督促落实。

8.2 泄密事件查处

发生泄密事件应当按照有关规定及时报告和采取补救措施，并报告查处情况。

8.3 考核与奖惩

8.3.1 保密工作责任落实情况应当纳入绩效考核。

8.3.2 单位应当每年对保密工作成绩突出的部门和个人给予表彰和奖励。

8.3.3 单位应当严格执行保密工作责任追究制度，对违反保密规章制度或者不履行保密责任的给予处罚，并追究相关领导的责任。

8.4 保密工作经费

8.4.1 保密工作经费分为保密管理工作经费和专项保密工作经费。保密管理工作经费用于单位日常保密管理工作；专项保密工作经费用于保密防护设施的建设和设备的配备。

8.4.2 保密管理工作经费应当列入单位年度财务预算，根据工作需要保证足额开支；专项保密工作经费应当按照实际需要予以保障。

8.4.3 保密管理工作经费按照下列标准计算：

核心涉密人员每人每年度 300 元，重要涉密人员 200 元，，一般涉密人员 100 元。

经合计高于20万元的单位，以20万元为保证基数，低于10万元的单位以10万元为保证基数，不足部分按照实际工作需要增补。

8.5 保密工作档案

8.5.1 单位应当建立保密工作档案，由保密工作机构和业务部门按照职责分工分别建立。

8.5.2 档案内容应当完整真实，反映单位保密工作开展实际情况。

8.5.3 保密工作档案应当按照规定保存，保存期限一般不少于3年。