上海船研所涉密信息系统

安全保密管理制度

舰船自动化分所

二〇一五年八月

目录

一、信息安全保密方针

积极防范、突出重点，既确保国家秘密不失密、不泄密，又便利各项工作的开展

二、目的和依据

为了加强对上海船研所涉密信息系统的安全保密管理，确保国家秘密信息的安全，更好地为改革开放和经济建设服务，根据《中华人民共和国保守国家秘密法》、《中华人民共和国计算机信息系统安全保护条例》、《涉及国家秘密的信息系统分级保护管理规范》、《上海船舶运输科学研究所保密管理体系文件》以及其他相关规定要求制定管理规定。

三、总体目标

安全保密规定制定的总体目标是建立上海船研所涉密信息系统的安全保密管理机构、安全保密管理制度、安全技术管理制度及安全人员培训管理制度，从制度上切实保障上海船研所涉密信息系统的安全保密性。按照统筹规划、统一标准、分级管理、促进发展的原则，对上海船研所涉密信息系统进行安全科学地组织、建设和管理。通过制定和完善与本系统有关的政策及规章制度，依据相关法律及有关规定，统一管理本系统的安全保密工作。

上海船研所涉密信息系统安全保密管理规定

第一章　总则

第一条　上海船研所涉密信息系统的正常运行是依靠各相关部门工作人员来具体保障实施的，是信息系统安全的主体，也是系统安全管理的对象。为了确保上海船研所涉密信息系统的安全、稳定运行，特制定本管理规定。

第二条　本规定适用于上海船舶运输科学研究所舰船分所所有在编职工及临时聘用人员。

第二章 安全保密策略

第三条　成立专门的安全保密管理组织负责规划上海船研所涉密信息系统的信息安全保密策略，建立文档化的安全保密管理体系，监视体系的运行并对体系进行持续改进。

第四条　根据信息系统所处理的信息最高密级确定信息系统以及安全域的保护等级，由上海船舶运输科学研究所保密委员会办理审核并报上海市保密局审核批准。根据应用情况变化，上海船舶运输科学研究所将重新确定系统保护等级，按相应等级要求调整保护措施，上报审批。

第五条　上海船研所涉密信息系统的方案设计和实施委托获得上海船研所涉密信息系统集成资质和工程监理单项资质的单位承担。

第六条　上海船研所涉密信息系统工程建设将根据具体情况划定保密范围，并制定相应的保密措施和保密控制流程，对涉密人员范围进行严格控制；按照 BMB18-2007 的要求组织实施工程监理。工程

施工结束后由国家保密部门授权的系统测评机构对上海船研所涉密信息系统进行安全保密检测，经过主管保密工作部门的审批后开通运行。

第七条 对投入运行的上海船研所涉密信息系统建立包含人员管理、物理环境和设施管理、设备与介质管理、运行与开发管理和信息保密管理等多方面的管理制度，并组织人员定期、不定期地从制度涉及的各方面进行日常管理检查，并组织进行风险自评估工作，对各项安全保密管理制度进行审核与完善。

第八条 如系统环境或应用发生重大改变时，将重新进行安全保密方案评审与测评工作。

第九条 对各类安全保密测评与保密检查过程中形成的相关文档、有关数据、记录和评估报告按照密级划分的有关规定进行定密，并按照相应的涉密文件管理办法进行管理。

第十条 信息系统要害部位严格执行治安保卫管理制度，对上海船研所涉密信息系统机房进行标识；对出入上海船研所涉密信息系统机房进行控制，由专门的人员负责日常保密管理工作；实施包括门禁、视频监控、报警等在内的要害部位安全防范措施，对外来人员访问核心机房的要害部位严格实行人员陪同等控制措施。

第十一条 禁止使用具有无线互联功能的设备处理涉密信息，禁止在处理涉密信息的设备上使用无线键盘、无线鼠标及其他无线互联的外围设备，禁止在涉密场所连接互联网的设备上配备、安装和使用摄像头等视频输入设备，禁止将具有存储功能的自带设备接入上海

船研所涉密信息系统。

第十二条 对涉密场所实行节假日周边巡视制度；每晚至少二次对舰船分所 17 号楼周围巡查，从防灾、防盗和防失泄密方面，重点对水电气切断情况、门窗关闭情况、涉密介质和涉密设备的保管情况以及单位人员滞留情况等方面进行巡防巡查。

第十三条 对基础保障设施进行定期检测检修，以保护供电和通信的正常，通过警示，防止线缆被施工等原因意外破坏，并将系统内所有线路线缆的布置图进行整理汇编，以备查看。

第十四条 放置上海船研所涉密信息系统网络和计算机设备的屏蔽机柜按相应建设标准和规范进行建设，部署各项电磁泄漏防护措施，并落实机房与设备维护管理制度，为网络和计算机设备提供安全的运行环境。

第十五条 对各类涉密设备采购设备实行归口管理，由指定部门进行统一购置、统一标识、统一发放；在具有资质的单位和经国家主管部门批准的范围内，采取邀标、竞争性谈判、单一来源采购和询价的方式进行采购。系统中使用的安全保密产品应选用国产设备，各类产品获得国家保密工作部门批准。由专人负责对供货方交付的货物进行验收，验收时严格核对产品型号、数量、配置、检测证书。

第十六条 对上海船研所涉密信息系统相关资产依据存储和处理的信息进行分级管理，通过识别、分类、标记、授权、报废和销毁等手段，管理所有信息系统相关资产，落实信息系统相关资产的使用单位、使用地点和责任人，保持信息系统相关资产完整、可用。

第十七条 加强上海船研所涉密信息系统相关涉密人员（包括内部员工和外来人员）的信息安全保密管理，明确岗位信息安全保密职责，与涉密岗位人员签署保密协议，落实人员聘用、在岗和离岗等安全保密控制。在上海船舶运输科学研究所现有培训体系中加入信息安全保密培训，通过信息安全保密培训和各种形式的信息安全保密教育活动，不断提高上海船研所涉密信息系统涉密人员的信息安全保密意识和能力。对涉密人员从日常表现、对外提供资料和对外学术交流、外出、出国（境）、本人及配偶和子女是否具有外国国籍以及境外长久或永久居留权等实行保密监管。对遵守保密规定，完成工作任务中表现突出或成绩优异的人员予以表彰奖励；对于违反保密规定的人员，给予批评教育；情节严重的，给予行政处分；构成犯罪的应依法追究刑事责任。

第十八条 加强外来人员访问上海船研所涉密信息系统的管理，通过保密要求知会、安全域管理控制、携带物品限制、旁站陪同控制，以及访问控制、审计等措施，防止外来人员危害上海船研所涉密信息系统安全。

第十九条 定期对系统内安全保密设备的安全策略规则进行审核，对系统内软件安装进行集中管理，严禁用户私自安装，根据系统规模、用户数量变化的情况进行风险评估、及时调整系统的保护策略。并根据系统的变化情况，及时更新系统文档资料，使之与实际状况保持一致。

第二十条 上海船研所涉密信息系统的变更应得到严格控制，

通过变更管理流程，保证每个信息系统变更在实施之前都被正确的识别、定义、评估和审批，确保信息系统变更不会对上海船研所涉密信息系统正常运行造成严重影响。

第二十一条 在组织开发用于处理涉密信息的业务应用系统时，从身份鉴别、访问控制和安全审计等几个方面进行安全保密功能的同步开发。要求开发、测试业务应用系统所使用的网络环境和设备与系统实际运行环境、设备物理分离，并禁止使用实际涉密信息作为测试数据。

第二十二条 对重要的信息和信息系统进行备份，进行定期的备份测试验证，保证各种备份信息的保密性、完整性和可用性，确保所有重要信息系统和重要数据在故障、灾难后及其它特定要求下进行可靠的恢复。

第二十三条 按上海船研所涉密信息系统照相关资产管理策略，对可移动介质的登记、移动、外出携带、保管、报废、处置进行严格的控制，防止存储有涉密数据的介质遭受未授权使用、移动、丢失或损毁，造成重要数据的泄漏。

第二十四条 对上海船研所涉密信息系统与外部之间信息的交换进行控制，介质或硬拷贝形式的信息交换由专人携带，确保安全。

第二十五条 依据《中华人民共和国保守国家秘密法》及《中华人民共和国保守国家秘密法实施办法》，确定系统中涉密信息的密级和保密期限。对系统中产生、存储、处理、传输、归档和输出的信息及其存储介质进行相应的密级标识，对系统中涉密信息总量进行分

类统计，定期将情况汇总，并根据秘密级信息数量或含量增多时，考虑调整系统防护措施。

第二十六条 加强上海船研所涉密信息系统的授权管理和访问控制。建立用户标识和鉴别机制，以及安全的授权管理制度，并落实授权责任人。按照“按需可知”的原则，通过功能和技术配置，对上海船研所涉密信息系统应用系统、数据等实施访问控制。

第二十七条 加强涉密信息安全保密日常安全保密管理，包括系统口令管理、无人值守设备管理、屏幕保护管理等，促使上海船研所涉密信息系统涉密人员的日常工作，符合上海船研所涉密信息系统涉密信息安全保密策略和制度要求。

第二十八条 建立健全异常事件处理机制，制定事件响应应急预案，并定期进行测试和演练，加强对事件监测、报告与处理，由专人负责整个灾难现场和灾难恢复过程中的安全保密工作，并按照数据保护的要求妥善处理涉密介质和涉密设备。通过对事件的总结评估，从技术与管理两方面进行改进，提高对异常事件处置的能力。

第二十九条 对重要信息系统的系统日志、故障日志、审计日志、管理员与操作员日志等进行监控和定期分析，监控信息系统运行，为信息系统审计提供依据。

第三十条 上海船研所涉密信息系统与其他网之间实施物理隔离，通过部署相应的技术设施防止违规外联。对上海船研所涉密信息系统实施网络访问控制、审计、入侵检测等技术防范措施，以满足系统控制的要求。

第三十一条　　在上海船研所涉密信息系统内统一部署网络防病毒软件，并进行病毒库的统一更新，防范恶意代码对上海船研所涉密信息系统和网络的影响。通过强化恶意代码防范的管理措施，如加强介质管理，严禁擅自安装软件，加强人员安全意识教育，定期进行恶意代码检测等，提高上海船研所涉密信息系统对恶意代码的防范能力。

第三十二条　　定期采用技术手段对系统的运行情况和用户操作行为进行安全保密法规、保密标准符合性方面的检查，确保系统符合保密标准的要求。

第三章　安全保密组织管理

第三十三条　　信息系统安全管理机构的职能

（一）信息系统安全管理机构负责与信息安全有关的规划、建设、投资、人事、安全政策、资源利用和事故处理等方面的决策和实施。

（二）信息安全管理机构应根据安全需求建立各自信息系统的安全策略、安全目标。

（三）根据国家信息系统安全的有关法律、法规、制度、规范建立和健全有关的实施细则，并负责贯彻实施。

（四）建立和健全本系统的系统安全操作规程。

（五）确定信息安全各岗位人员的职责和权限，建立岗位责任制。

（六）审议并通过安全规划，年度安全报告，有关安全的宣传、教育、培训计划。

（七）对已证实的重大的安全违规、违纪事件及泄密事件进行处

理。

第三十四条　　计算机安全保密管理人员职责

（一）保密委员会职责

1、对保密工作负全面领导责任。

2、保证国家保密工作法律、法规、方针、政策在的贯彻执行。

3、为保密工作提供组织及财力、物力的保障。

4、定期听取保密工作汇报，掌握保密工作重要情况。

5、对重要保密工作事项提出明确要求，采取有效措施解决保密工作中的重大问题。

（二）保密委员会办公室职责

1、对保密工作负组织领导责任。

2、贯彻执行国家保密工作法律、法规、方针、政策和上级机关保密工作指示精神，对保密工作进行决策和部署。

3、保证保密委员会办公室及其工作人员能够切实履行职责。

4、每年不少于2次召开保密委员会例会，对保密工作进行研究、部署和总结。

5、及时组织、协调重大保密工作，解决重要问题，查处泄密事件。

6、及时听取保密工作汇报，督促检查保密工作落实情况。

7、按有关规定审批保密工作有关事项。

8、及时向法定代表人报告保密工作重要情况和泄密事件。

（三）其他领导职责

1、对分管业务工作范围内的保密工作负直接领导责任。

2、结合业务工作实际提出保密工作要求，督促检查落实情况。

3、布置重大涉密、涉外工作任务，要求保密委员会办公室进行保密管理和监督。

4、了解掌握业务工作中的保密工作重点、国家秘密事项和涉密人员的基本情况。

5、按有关规定审批保密工作有关事项。

6、及时与分管保密工作领导沟通保密工作重要情况。

（四）舰船分所主管领导职责

1、对本部门保密工作负主要领导责任。

2、了解掌握有关保密工作法规、保密规章制度并贯彻执行。

3、了解掌握上海船研所涉密信息系统全保密管理要求并督促检查。

4、结合本部门实际提出保密工作要求，督促检查落实情况。

5、定期听取保密工作汇报，了解掌握本部门保密工作重点、国家秘密事项和涉密人员的基本情况。

6、负责对本部门中各项信息系统安全保密工作授权范围内的使用授权与审批管理工作。

7、掌握上海船研所涉密信息系统重要口令。

8、及时向领导报告保密工作重要情况和泄密事件。

（五）舰船分所所在部门分管保密工作领导职责

1、对本部门保密工作负组织领导责任。

2、了解掌握有关保密工作法规、保密规章制度并贯彻执行。

3、了解掌握上海船研所涉密信息系统安全保密管理要求并根据管理细则进行贯彻执行。

4、建立、健全保密组织，保证保密组织能够切实履行职责。

5、每季度召开一次保密工作例会，传达上级保密工作精神，结合实际研究、部署保密工作，督促检查保密工作和规章制度落实情况。

6、每逢法定节假日前，组织保密防范检查，落实保密安全措施。

7、了解掌握本部门保密工作重点、国家秘密事项和涉密人员的基本情况。

8、及时向本部门主要领导和保密委员会办公室报告保密工作重要情况和泄密事件。

（六）上海船研所涉密信息系统所在部门其他副职领导职责

1、对分管业务工作范围内的保密工作负直接领导责任。

2、了解掌握有关保密规章制度并贯彻执行。

3、了解掌握上海船研所涉密信息系统安全保密管理要求并根据管理细则进行贯彻执行。

4、结合业务工作实际提出保密工作具体要求和措施，督促检查落实情况，做到保密工作与业务工作“五同时”。

5、配合保密组织开展工作，保证保密管理措施在分管业务工作范围内贯彻落实。

6、了解掌握分管业务工作范围内的保密工作重点、国家秘密事项和涉密人员的基本情况，结合业务工作实际对涉密人员进行教育。

7、及时与本部门分管保密工作领导沟通保密工作重要情况。

（七）保密委员会办公室专职保密人员职责

1、了解国家保密法律、法规、方针、政策，熟悉保密规章制度和本部门保密管理规定并贯彻实施。对上海船研所涉密信息系统进行保密要求方面的指导。

2、督促检上海船研所涉密信息系统的各项安全保密管理规定的执行情况。

3、根据上级部署，对上海船研所涉密信息系统落实保密宣传教育、不定期进行保密防范检查和隐患整改等工作。

4、对涉密事项落实保密安全措施，建立相应的基础资料登记、汇总和备案工作。

5、及时向本部门分管领导提出保密工作建议，报告重要情况和泄密事件。

6、完成本部门分管领导和保密委员会办公室交办的工作任务。

（八）上海船研所涉密信息系统管理员保密工作职责

1、负责上海船研所涉密信息系统中各项系统维护管理工作，并提供相应的维护记录。

2、负责上海船研所涉密信息系统中各项安全保密技术措施的检查、记录工作。

3、负责涉密计算机审计日志的查看、记录、汇报工作。

4、及时与部门领导和本部门领导汇报系统中出现的各种安全保密问题。

5、负责对上海船研所涉密信息系统进行定期备份、登记管理等工作。

6、对上海船研所涉密信息系统产生介质，按照涉密介质的管理要求配合介质管理员做好相关的管理工作。

7、负责上海船研所涉密信息系统的病毒管理工作。

8、负责上海船研所涉密信息系统的防病毒软件的安装、升级、日常检测等各项工作。

9、负责对上海船研所涉密信息系统中出现的病毒进行各项扫描、清除、隔离、记录、汇报等管理工作。

（九）上海船研所涉密信息系统安全保密管理员工作职责

1、执行涉密介质的领用、登记台帐管理、借用、销毁等工作。

2、执行USBKey的领用、登记台帐管理、借用、销毁等工作。

3、负责涉密资料的打印和刻录光盘等的登记、管理工作，定期汇总记录并备案。

4、负责对涉密计算机（包括笔记本电脑）实行定密、上报审批表、贴标密级标识等保密措施。

5、负责信息系统安全日志分析工作。

6、负责信息安全设备运行维护、策略管理等工作。

7、负责信息安全事件处理、上报工作。

8、定期向领导汇报保密工作情况。

（十）上海船研所涉密信息系统安全审计员工作职责

1、负责对系统管理员、保密管理员的操作行为进行审计跟踪分析和监督检查，负责审计日志的分析工作，负责各类审计异常事件的上报、协助处理工作。

2、了解国家保密法律、法规、方针、政策，熟悉本单位保密规章制度和本部门保密管理规定并贯彻实施。对上海船研所涉密信息系统进行保密要求方面的指导。

3、督促检查上海船研所涉密信息系统的各项安全保密管理规定的执行情况。

4、根据上级部署，对上海船研所涉密信息系统落实保密宣传教育、不定期进行保密防范检查和隐患整改等工作。

5、对涉密事项落实保密安全措施，建立相应的基础资料登记、汇总和备案工作。

6、及时向领导提出保密工作建议，报告重要情况和泄密事件。

（十一）涉密计算机设备管理人员安全保密职责

1、熟悉有关计算机安全保密管理规定，负责对本部门计算机人员实行保密教育。

2、负责本部门的安全保密日常管理工作以及与保密办的日常联络。

3、执行部门涉密文件打印、光盘刻录操作及相关登记工作。

4、负责对涉密计算机（包括便携式电脑）实行定密、上报审批表、贴标密级标识等保密措施。

5、负责对涉密计算机和涉密介质（包括磁盘、光盘、活动硬盘、

U 盘和磁带等）管理人员、存放地点和存放要求的规范管理和督促检查。

6、负责涉密计算机的干扰器配置管理。

7、监督检查涉密计算机内存储的涉密文件和目录文件的密级标识。

8、熟悉上海船研所涉密信息系统安全保密管理所涉及的计算机相关的保密管理内容。

9、负责对计算机、U 盘和活动硬盘的规范管理和规范使用。

10、对本部门中使用的笔记本电脑进行专项督促检查，对存在的保密隐患实施整改措施，发现问题及时纠正。

11、核对本涉密计算机为有固定资产编号并经保密办登记审批的计算机。

12、负责涉密计算机的维修协调工作。

13、按保密要求配合相关人员对相关计算机进行保密措施的落实。

14、按保密要求配合相关人员对计算机系统（包括非涉密计算机）进行相应的保密检查。

15、及时向本部门安全保密管理员沟通有关计算机安全保密管理问题。

（十二）部门打印负责人保密工作职责

1、负责对打印内容进行涉密检查，确保没有打印涉密信息。

2、定期对打印日志进行审查，确保没有涉密信息打印。

第四章 机构及职责

第三十五条 上海船舶运输科学研究所一贯重视信息安全管理工作。根据“统一领导、层层落实、外防内审、保障有力”的安全组织建设原则，成立了三级安全保密责任机构，确保安全对象和目标明确、管理与技术并重、全面与重点并举。

（一）舰船分所安全保密领导小组

舰船分所由分所领导牵头由5人组成的安全保密领导小组（见表1），每季度定期对上海船研所涉密信息系统安全保密进行规划和检查，对上海船研所涉密信息系统的重大事项进行决策，其职责是：

(1) 批准安全保密策略

(2) 批准安全保密责任分工

(3) 批准安全保密安全考核指标

(4) 制订安全事故报告流程

(5) 检查安全保密制度执行

(6) 安全保密体系的重大事宜决策

表1 舰船分所保密领导小组名单

角色	职务	姓名	联系电话
领导小组组长	分所所长	曹建明	58856638-2416
领导小组成员	研究开发部主任	张欢仁	58856638-2772
领导小组成员	综合计划部主任	黄国强	58856638-2488
领导小组成员	综合计划部技术总监	毛奇林	58856638-2888

角色	职务	姓名	联系电话
领导小组成员	系统工程部副主任	张兴龙	58856638-2521

（二）安全保密应急响应小组

安全保密应急响应小组(见表2)负责对涉密系统突发安全事故的紧急响应和系统恢复，该小组在安全事件发生时，按照报告制度向有关领导汇报的同时，采取一切必要手段处理安全事故，并与上级部门和有关安全专业机构合作，在合适的情况下进行事故的分析和取证。

表2 安全保密应急响应小组

角色	职务	姓名	联系电话
组长	分所所长	曹建明	58856638-2416
副组长	综合计划部主任	黄国强	58856638-2488
组员	研究开发部主任	张欢仁	58856638-2772
组员	综合计划部技术总监	毛奇林	58856638-2888
组员	系统工程部副主任	张兴龙	58856638-2521
组员	保密管理员	柴婉儿	58856638-2403
组员	系统管理员	张晓慧	58856638-2965
组员	安全审计员	耿琪	58856638-2938

对安全保密应急响应小组人员采取了严格的管理措施，确保政治可靠、技术过硬，并组织对他们进行技术培训。

对使用者应定期进行安全培训，保证每人每年的安全培训不少于1小时，要求他们有强烈的安全意识，并将安全目标落实到人；当其离岗或调动时采取全面的安全保护措施，如立即更换密码、进行文档和介质回收。

（三）安全人员

安全人员应包括：安全审计员、安全保密管理员、系统管理员，分别负责系统的运行、安全保密和安全审计工作，这三类安全保密管理职责必须由不同人员担当。具体职责分派如下：

- 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，并定期向保密领导小组汇报相关情况；
- 安全保密管理员主要负责系统的日常安全保密管理工作，包括用户账户管理以及安全保密设备和系统所产生日志的审查分析；
- 系统管理员主要负责系统的日常运行维护工作。

上海船研所涉密信息系统物理环境和设施管理规定

第一章　周界安防管理制度

第一条　职责

（一） 保密委员会办公室负责提出周界安防的各项需求，组织安全风险评估工作。

（二） 所有关部门负责落实各项安防技术措施的落实，落实人员值守、巡逻，报警响应等各项保卫工作。

第二条 周边监控

（一） 应对周边环境情况（如可疑人员、安全距离变化）进行监控，如环境发生重大变化，应及时与保密委员会办公室沟通，调整防护方案。

（二） 保密委员会办公室两年组织一次针对物理入侵等方面的安全风险评估，并根据评估结果及时调整系统的防护方案。

第三条 周界安防

（一） 每月对周界安防设备进行检测、维修，保证设备的正常使用；

（二） 所门卫值班室，对舰船分所周界和重点部门安防情况进行监控，并有专人 24 小时值班。

第四条 出入控制

（一） 对需要访问涉密机房的人员需要由系统管理员或安全保密员用钥匙开启大门后方可进入；

（二） 外部来访人员应进行登记，填写会客登记单，由前台向其核实身份，并查验相关证件后方可放行，人员离开时应交回有会见人签字后登记单；

（三） 携带物品出门必须出示相关证明，经查验无误后方可放行。

第五条 安全巡防巡查

（一） 节假日办公大楼实行值班制度，由值班巡查人员负责对重要区域进行安全巡防巡查；

（二） 巡查人员每晚至少对舰船分所周边巡查二次，并填写巡查记录。

第二章 保密要害部门、部位保密管理制度

第六条 确定保密要害部门、部位的标准

（一） 本所内部业务工作中经常出现或大量涉及国家秘密的部门，应当确定为保密要害部门。

（二） 集中存放、保管秘密级以上国家秘密载体的场所，应当确定为保密要害部位。

（三） 直接含有国家秘密信息的设备或产品，通过观察或者测试、分析手段能够获得该设备或产品的国家秘密信息，应当确定为涉密设备或产品。

第七条 确定保密要害场所及涉密设备的程序

符合上述确定标准的拟定保密要害部门、部位及涉密设备的部门，应当履行审批程序，及时报保密委员会办公室审核。

第八条 保密要害部门、部位防护措施的基本要求

（一） 保密要害场所须进行密级标识。

（二） 保密要害场所须有安全保密隔离措施，并安装防盗门窗。

（三） 涉及国家机密级事项的保密要害场所须安装门禁系统。

（四） 严禁无关人员进入或参观。

第九条 保密要害部门、部位的管理要求

（一）加强对保密要害部门、部位保密管理工作的领导，保密办负责保密工作的协调、指导、督促、检查工作。舰船分所要有专门分

管保密工作的领导，负责本单位日常保密管理工作，配合本单位保密部门共同做好保密安全工作。

（二）舰船分所应当按照国家保密法规和本所有关要求，制订和完善保密要害部门、部位各项管理规定，报保密办备案。

（三）涉及保密要害部门、部位的工程项目建设，应当做到工程项目建设与保密技防措施同计划、同预算、同建设、同验收，并在工程项目施工前及时将保密技术防护措施实施方案报保密办审核，并经所领导经批准后再予以实施；工程项目竣工后应当及时通知保密办主管部门一同参与工程验收，以确保保密技防设施、设备质量可靠，安全运行。

（四）保密要害部门、部位应当完善保密防护措施，并且指定分管领导具体负责此项工作，认真履行职责，严格保密管理制度，严格保密防范措施，严肃保密工作纪律。有关保密设施、设备的选用、维护、管理，必须按照有关规定执行，以保证保密设施、设备质量可靠、安全运行。

（五）保密办负责指导、协调和监督保密要害部门、部位及涉密设备、产品的保密管理工作，严格遵照国家保密法规和本所的有关规定，落实人防、技防、物防“三位一体”的保密防护措施，健全和完善各项保密管理制度，形成运行有效的保密管理体系。

（六）舰船分所应当加强对涉密人员的教育和管理，对进入、调整、调离（辞职）涉密岗位的工作人员按规定履行审核报批手续。

（七）外单位人员、确因工作需要，进入保密要害部门、部位的，本单位接待部门应当办理有关审批手续，并派人陪同，在经审批确定的区域、范围内进行工作，不得擅自更改工作内容和涉及范围。

（八）保密要害部门、部位中对于手机等无线通信和定位终端设备的使用，应严格按照有关规定确定是否需要安装和使用防止手机等无线通信和定位终端设备泄密的设施。

（九）严禁对涉密产品、实物进行摄影、摄像。确因工作需要摄影、摄像的，应当办理有关审批手续。

（十）严禁无关人员进入保密要害部门、部位，接触涉密产品和设备。

（十一）要加强保密安全巡防检查工作，发现问题时要及时整改，并自觉接受保密办、所办公室专项工作的检查和指导。

（十二）因涉密情况的变化，需要撤销保密要害部门、部位的，部门应提交申请报告，报所保密办公室，由所保密委员会报上海市保密局，审批同意后方可撤销。

第十条 无线、多媒体产品使用管理规定

（一） 禁止使用具有无线互联功能的信息设备处理涉密信息，凡用于处理涉密信息的信息设备应拆除具有无线联网功能的硬件模块。

（二） 用于处理涉密信息的信息设备禁止使用无线键盘、无线鼠标及其他无线互联的外围设备。

（三） 禁止在涉密场所连接互联网的信息设备上配备、安装和使用摄像头等视频输入设备。

（四） 在涉密场所内谈论涉及国家秘密事项时，对具有音频输入功能并与互联网连接的信息设备采取关机断电措施。

第三章 保障设施

第十一条 对于保密要害部门、部位中的设施、设备应定期进行检测检修，发现问题的应按照上海船研所涉密信息系统涉密设备管

理规定的有关要求进行维修或更换。

第十二条 上海船研所涉密信息系统的通信电缆要使用专用光缆、专用双绞线。光电转换及接线部分要注意屏蔽，接线盒要加锁并设置在易受控制的部分(如电视监控范围内)。

第十三条 应严密保护本单位接入光纤、光电转换器等设备的正常运转和网络的畅通，发生网络运行异常应及时上报所主管部门进行排除。所主管部门应经常性对光纤线路进行巡查以确保线路线缆的正常运行。重要线路线缆埋放地点应设有明显警示装置，防止被施工等原因意外破坏。

第十四条 应对系统内所有线路线缆的布置图进行整理汇编，作为技术资料进行存档，以备查看。

上海船研所涉密信息系统机房管理规定

上海船研所涉密信息系统机房包含：屏蔽机柜、楼层设备间等。上海船研所涉密信息系统的主机房是位于 17 号楼 2 层机房里，是上海船研所涉密信息系统核心设备存放的地方。为保障整个上海船研所涉密信息系统的正常运行和机房的安全保密，特制定如下制度：

1、机房管理人员和上机人员必须遵守国家有关法律、法规，认真执行机房管理制度、安全保密制度等各项规章制度，机房管理人员应认真地做好本职工作，保障系统正常、安全、可靠地运行。

2、涉密机房、配线间的门应当保持关闭，机柜应上锁。钥匙应由机房管理员与主管领导掌握。

3、机房钥匙及设备机柜钥匙由机房管理人员集中保管，未经允许不得转让他人。严禁无关人员进入上海船研所涉密信息系统机房，集成方或开发、维护人员进入机房必须有信息部门人员在场。参观机房须有关领导批准并办理登记手续。进入机房须填写“涉密机房出入登记表”。

4、机房内所有设备应严格管理，专机专用，未经允许不得挪作他用，严禁在服务器等设备上擅自运行外来的光盘等存储介质，使用外来的光盘等存储介质应严格进行病毒检测后方可使用。

5、机房保持 7x24 小时运行，确因管理维护需要进行关机重启，由系统管理员进行操作，操作完成后应填写“涉密信息系统设备开关登记表”。

6、为确保上海船研所涉密信息系统运行安全，涉密系统三员负

责机房的日常巡视工作。负责对涉密机房内的网络设备、PC 服务器、安全设备等每天 2 次进行巡查，确保网络系统、安全系统正常运行，并填写“涉密机房巡查表”。

7、机房内维修工作由部门负责进行，维修工作需在机房管理员的陪同下进行，工作完毕需要填写“涉密信息系统设备维护记录表”。机房内服务器设备的硬盘发生故障，应送市国家保密局指定的单位进行消磁处理。

8、除日常值班巡查工作以外，在涉密机房内进行的各项重要操作（包括对 PC 服务器、路由器以及所有安全设备的操作、涉密文件访问授权设置、安全审计、病毒防范、信息备份、涉密介质制作、储存等），由保密办指定专人进行，上述操作均应在保密管理员的监督下完成，操作完毕后操作人员应填写“涉密信息系统重要操作情况记录表”。

9、上海船研所涉密信息系统机房内设备情况、机器性能、网络地址、使用程序及业务处理范围等情况，未经允许一律不准对外传播、解答。机房内所有设备要制定严格的符合安全保密要求的口令，口令由系统管理员严格管理、定期更换，不准转告他人。

10、上海船研所涉密信息系统管理员应每季度查看各项安全保密设备相关记录，发现异常应填写“涉密信息系统异常事件汇报处理单”，并立即上报。

11、机房内严禁存放易燃易爆物品，严禁使用明火或吸烟，消防器材应固定位置存放，不得随意挪动。机房内的空调、消防、防

盗报警设备要有专人负责，定期检查、维护，确保设备正常。

12、机房内所有设备的电源插座、信号连接线严禁擅自连接。

13、上机人员请自觉保持机房整洁，不乱扔纸屑和杂物，严禁将食物、茶水带入机房。

附件 1：

涉密机房出入登记表

日期	人员	事由	进入时间	离开时间	备注

附件 2：

涉密信息系统设备开关机登记表

日期	时间	设备名称	开机/关机/ 重启	执行 人员	值班人	情况	备注

附件 3：

涉密机房巡查表

序号	日期	检查人员	检查项目（正常打 √，异常打×）						进入时间	离开时间	备注
			电源	交换机	服务器	保密柜	空调	其它			
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

附件 4：

涉密信息系统设备维修记录表

日期	报修部门	报修人	型号	维修事宜	维修单位	维修人	确认人

附件 5：

涉密信息系统重要操作情况记录表

日期	内容	操作人	确认人

附件 6：

涉密信息系统异常事件汇报处理单

汇报人：	日期：
异常情况描述	
事件分析	
建议采取行动	
领导批示： 签名： 日期：	
处理结果	
  签名： 日期：	
领导批示： 签名： 日期：	

注：异常状况包括审计日志异常，病毒警报，发现入侵行为等各种安全事件，描述时应写明分析的依据。

上海船研所涉密信息系统机房设备管理规定

上海船研所涉密信息系统机房设备包括：网络设备、安全设备、服务器和机房配套设备（UPS、空调、灭火器、防盗报警系统等），它们是整个上海船研所涉密信息系统计算机机房的核心组成，对整个网络系统、应用系统的正常运行起到重要作用，特此制定如下设备管理规定：

一、网络设备（交换机、路由器）

1、网络设备检查、维护每月进行一次，原则上必须由部门系统管理员进行，确有需要由系统集成商或维修人员进行设备操作时，必须有部门系统管理员在场，并征得主管领导同意。

2、网络设备检查、维护要做好记录工作，进行严格登记，同时做好配置更改的备份工作。

3、网络设备检查、维护操作日志及运行日志由系统管理员定期导出，并审阅处理。

4、网络设备出现故障要立即报告主管领导，并及时通知系统集成商或有关单位进行故障排除，不得拖延，故障解决要有文档记录。

二、服务器设备

1、服务器设备检查、维护每月进行一次，必须由部门系统管理员进行，确有需要由系统集成商或维修人员进行设备操作时，必须有部门系统管理员在场，并征得主管领导同意。

2、所有服务器设备检查、维护要做好记录工作，进行严格登记，

同时做好配置更改的备份工作。

3、服务器设备要设定严格的操作及安全审计策略，对设备操作及运行安全进行记录审计，运行日志及审计记录由安全审计员定期审阅处理，导出备份。

4、服务器设备的数据由系统管理员定期备份，严格管理。

5、服务器设备出现故障要立即报告主管领导，并及时通知系统集成商或有关单位进行故障排除，不得拖延，故障解决要有文档记录。

三、机房配套设备

1、UPS 设备

（1）机房 UPS 设备日常运行检查、维护每月一次，必须由相关技术人员进行；UPS 设备厂方维护每年一次，UPS 电池放电每三个月放电一次，由厂方进行。

（2）检查巡查时，如发现 UPS 工作不正常，应及时报告主管领导，并联系 UPS 厂家，不得耽误。

2、空调设备

（1）空调设备日常运行检查、维护每月进行一次，要及时查看空调设备（包括室外机）是否能正常启动；制热、制冷、加湿、新风功能是否正常，并作日常记录。每半年清洁室外机一次。

（2）如空调设备工作不正常，应及时报告主管领导，并联系空调维护单位进行解决，不得耽误。

3、消防设备

（1）消防设备日常检查、维护每月进行一次，要定期检查机房

消防设备是否正常工作，并作好运行情况记录。

（2）如机房消防设备工作不正常，应及时报告主管领导并联系消防维护单位予以解决，不得耽误。

4、防盗报警设备

（1）要定期（每月一次）检查机房防盗报警设备是否正常工作，并作好运行情况记录。

（2）如机房防盗报警设备工作不正常，应及时报告主管领导并进行报修。

上海船研所涉密信息系统机房安全保密设备管理规定

上海船研所涉密信息系统机房中安全保密设备如入侵检测、网络安全审计，病毒防杀、漏洞扫描是确保涉密计算机系统安全运行的主要技术设备和措施，使用、维护和管理好这些设备对整个涉密网络系统的安全保密和正常运行起到重要作用，为此特制定以下规定：

1、为了更好地保障网络系统的安全性，必须建立每月一次的安全设备日常运行维护检查制度，对安全设备运行记录表中发现的问题进行汇总整理，保障系统安全设备的正常运行。

2、建立每周一次对网络病毒防杀系统病毒库升级，全网统一查杀及病毒事件的定期检查及汇总制度，查看病毒防杀系统事件日志、记录系统发现病毒情况及统一升级情况，保障网络病毒防杀系统的有效运行。

3、建立每二周一次的网络入侵检测系统和网络安全审计系统的定期数据分析、处理和汇总上报制度，对“鹰眼”网络入侵检测系统和网络安全审计系统进行定期检查维护，以保障网络安全事故的及时发现、处理和及时上报。

4、建立每月一次的系统安全漏洞扫描定期检查制度，以及时纠正系统可能存在的安全漏洞及安全隐患。

5、建立每月一次系统数据备份及恢复的定期检查制度，结合日常备份的制度，检查备份措施的执行情况，备份介质的管理情况。

上海船研所涉密信息系统涉密设备管理规定

上海船研所涉密信息系统涉密设备包括网络设备、服务器、安全设备和机房配套设备等，它们是整个计算机信息系统的核心组成，对整个网络系统、应用系统的正常运行起到重要作用。为了加强对涉密设备的管理特制定本规定。

第一章 设备采购与选型

第一条 保密设备的购置原则

（一）系统中使用的安全保密产品应选用国产设备，非安全保密产品应充分考虑国家安全保密需要，优先选择国产设备；在选用国外设备时，应进行详细调查和论证，不得选用国家保密工作部门禁用的设备或附件，必要时应对选用的国外产品进行安全保密检测；

（二）计算机病毒防护产品应获得公安机关批准，密码产品应获得国家密码管理部门批准，其他安全保密产品如身份鉴别、访问控制、安全审计、入侵检测和电磁泄漏发射防护等产品应获得国家保密工作部门批准。

（三）涉密设备的供货方应有完备的资质证明；长期供货和代理维修应签订保密协议，保证设备的使用安全与维修安全。

（四）严禁外资企业和国（境）外背景的机构、组织及其人员参与系统的建设与管理，系统集成与系统服务、安全保密产品的采购，不得进行公开招标，应在具有资质的单位和经国家主管部门批准的范围内，采取邀标、竞争性谈判、单一来源采购和询价的方式进行；

（五）涉及到招标的采购项目，应对招标资料进行严格保密审查，

并采取必要的保密措施，如招标项目采用代号、最终用户采用化名等。

（六）涉密设备的添置、维修、报废、停止使用，应履行有关审批手续，并报主管部门审核备案。

（七）涉密设备应进行严格验收。

第二条 涉密设备的审批准入程序

（一）涉密设备及保密防护设施、设备的添置、维修、报废、停止使用，履行有关审批手续，并报保密委员会办公室审核备案，经过统一标识与配置后方可投入运行。

（二）禁止将与互联网以及其他公共信息网络连接的办公自动化设备（如复印机、电话传真打印一体机等）接入系统。

第二章 涉密设备的管理

第三条 上海船研所涉密信息系统中涉密设备要注意设备保养和用电安全，定期对设备进行检查，及时消除隐患。

第四条 对所有设备均应建立项目齐全、管理严格的购置、移交、使用、维护、维修、报废等登记制度，并认真做好登记及检查工作，保证设备维护管理工作正规化。

第五条 每六个月应对存储涉密信息的设备和存储介质的数量、用途等进行清查核对和登记，并将结果报保密委员会办公室进行备案，如发现问题应及时向上级部门报告。

第六条 舰船分所负责涉密网的管理、维护及升级工作。涉密网计算机密码由涉密责任人员输入，保密员监管。涉密计算机出现故障，应

及时向保密办报告，本部门技术人员不能检修的,由保密办统一安排定点维修。

第七条 禁止使用部门和个人擅自挪动、拆除保密防范设施、设备。确因工作需要，应当由有关部门报经所保密部门批准，并采取临时性的保密防护措施，确保安全保密，万无一失。

第八条 涉密设施、设备的使用应建立相应的管理制度，严格使用程序和操作规定。对于重要的保密设施、设备应由专职管理人员负责管理和使用，并认真落实各项保密措施，切实做好安全防范工作。

第九条 安全保密设备与介质应由专人负责对供货方交付的货物进行验收，验收时应对产品型号、数量、配置、检测证书等进行严格核对。查验供应商提供的相关检测证书原件，以验证其真实性。

第十条 涉密设施、设备的使用管理人员必须严格遵守保密纪律，不得泄露有关涉密信息，不得擅自携带涉密设备外出。

第十一条 配备保密防护措施的部门、部位应当按要求开启使用。

第十二条 上海船研所涉密信息系统中，每台（套）设备的使用均应制定专人负责并建立详细的运行日志记录、备份制度。

第十三条 由设备责任人负责设备的使用登记，登记内容应包括运行起止时间、累计运行时数及运行状况等。

第十四条 设备责任人应保证设备在其出厂标称的使用环境（如温度、湿度、电压、电磁干扰、粉尘度等）下工作。

第十五条 一旦设备出现故障，责任人应立即如实填写故障报告，通知有关人员处理。

第十六条 上海船研所涉密信息系统接入设备管理

（一）上海船研所涉密信息系统计算机，应放置在配备了相关物理安全防护设施的场所，放置场所必须安装铁门、铁栅栏窗和防盗报警装置。上海船研所涉密信息系统计算机必须使用专用屏蔽双绞线和屏蔽接头。

（二）上海船研所涉密信息系统计算机显示器等显示输出设备，不得面对门窗摆放，防止显示输出内容被非授权获取。

（三）连接上海船研所涉密信息系统的计算机原则上应选用国产计算机。便携机（笔记本电脑）不得作为上海船研所涉密信息系统信息点接入设备。

（四）禁止在上海船研所涉密信息系统计算机上使用具有无线互联功能的设备（如无线键盘、无线鼠标及其它无线互联的外围设备）处理涉密信息。

（五）放置上海船研所涉密信息系统计算机的涉密场所，若同时还放置有连接互联网的信息设备，则连接互联网的信息设备上禁止配备、安装和使用摄像头等视频输入设备。

（六）上海船研所涉密信息系统计算机必须专机专用，禁止安装、运行与工作无关软件。

（七）用于打印上海船研所涉密信息系统信息的具有打印、复印、传真等多功能的一体机，禁止与普通电话线连接。

上海船研所涉密信息系统计算机设备管理规定

第一章　总则

第一条　涉密计算机设备是指经保密办公室审批并登记备案的计算机设备。

第二条　涉密计算机的保密工作贯彻“谁保管，谁负责”的原则，保管者负有直接的保密责任。

第三条　本制度适用于涉密计算机系统的使用、维护、保密等工作。

第二章　涉密计算机设备使用管理

第四条　上海船研所涉密信息系统使用授权、审批的管理

（一）建立、使用涉密的计算机信息系统必须实现与内网及外网的物理隔离，涉密网不得通过其他任何途径接入社会公众网。涉密网的建设应当根据国家的有关规定，落实管理和技术防范措施，并向国家保密工作部门进行相应的报批、实施及验收工作。

1、　禁止使用具有无线互联功能的信息设备处理涉密信息，凡用于处理涉密信息的信息设备需拆除具有无线联网功能的硬件模块；

2、　禁止在处理涉密信息的信息设备使用无线键盘、无线鼠标及其他无线互联的外围设备；

3、　禁止在涉密场所连接互联网的信息设备上配备、安装和使用摄像头等视频输入设备；

4、　在涉密场所内谈论涉及国家秘密事项时，应对具有音频输入功能并与互联网连接的信息设备采取关机断电措施；

5、 涉密计算机的使用者，必须经过分所领导审批，填写“涉密计算机设备领用审批表”，通过审批涉密人员才能使用该涉密计算机。

6、 每台涉密计算机的操作人员为该涉密计算机的责任人，负责该计算机的安全使用，协助安全保密管理员做好保密工作。如因岗位调动等原因，涉密计算机责任人需要变更，必须作好涉密计算机责任人变更手续，填写“计算机设备信息变更登记表”。

7、 由系统管理员对涉密计算机系统内软件安装实行集中管理，严禁用户私自安装非合法授权的软件系统，应填写“涉密计算机重装系统、软件申请表”。

8、 涉密计算机设备由各部门根据信息部门推荐的配置型号统一购买，并且向相关部门进行统一报备。报备内容为：涉密计算机的编号、硬件序列号、系统启用日期、配置和责任人的登记。应填写“涉密网络计算机台帐” 。

9、 除有特殊应用的涉密计算机（如专门涉密打印），其余涉密计算机严禁带有打印机、扫描仪等外接输入输出设备。打印涉密文件的有关规定参见《涉密文件打印管理制度》。

10、 严禁在计算机上处理涉及绝密级及机密级国家秘密事项。严禁越级处理各类信息但可以降级使用。亦即，不得在秘密级计算机内处理机密信息但可以处理非密信息，不得在非密计算机内处理涉密信息但在涉密计算机内可以处理非密信息，而在机密级计算机内可以处理秘密及非密信息。

11、 严禁涉密计算机联入国际互联网或非涉密局域网。

12、 涉密计算机应和非涉密计算机分开，涉密计算机所在场所应有防止非法进入的物理措施，作好涉密计算机所在场所的安全、防盗工作。

13、 不满足安全距离要求的涉密计算机（终端）应加装视频干扰器，在工作时间应打开视频干扰器，防止信息被窃取。

第三章　涉密计算机设备口令管理

第五条　口令的长度要根据信息系统处理国家秘密信息的密级决定。涉及国家机密级信息的口令不应少于十个字符（或五个汉字）；涉及国家秘密级信息的口令不应少于八个字符（或四个汉字）。口令变更频率根据访问等级确定，机密级 7 天更换一次，秘密级 30 天更换一次。

第六条　若采用人工输入口令字方式，使用者应记住自己的口令字，不应把它记载在不保密的媒介物上，严禁将口令字贴在终端上。输入的口令字不应显示在显示终端上。

第七条　强度特别高的访问控制应使用一次性口令机制。

第八条　口令策略由系统管理员利用操作系统的机制强制设定，设定的策略在计算机登记表中进行备案。涉密计算机用户应保存相关系统日志，以备检查。

第四章　涉密计算机设备监督检查

第九条　将不定期组织有关管理部门对上海船研所涉密信息系统的使用、维修、报废、销毁等情况进行监督检查，并对存在的隐患落实整改措施。

第十条 涉密计算机所属部门每季度应对其使用、管理等情况进行一次检查，发现问题要及时纠正，信息化主管部门等相关技术部门作相应的技术支持。

第五章 涉密计算机设备维修管理

第十一条 涉密计算机一旦设备出现故障，设备管理员应立即如实填写“涉密计算机设备维修记录表”，按规定的故障保修流程处理。涉密计算机需要外出维修，需要拆除所有可能存储过涉密信息的硬件和固件后，方可外出维修。如存储过涉密信息的硬件和固件损坏需恢复，必须到具有上海船研所涉密信息系统数据恢复资质的单位进行维修。

第十二条 涉密计算机因故障需送外修理，必须经部门主管领导批准，由日常执行部门卸下硬盘交部门专人保管。送修由日常执行机构负责，申请维修的部门应指定专人陪同，并在修理现场进行监督，当场取回，严禁失控。请外单位人员上门修理的，事先必须经部门主管领导批准，设备管理员必须做好被修涉密计算机的安全保密工作，修理时指定陪同者必须在场。

第六章 涉密计算机设备报废管理

第十三条 涉密计算机设备损坏后不得自行报废或销毁，需交还至上海船研所涉密信息系统主管部门日常执行机构处理。

第十四条 保密管理员定期将损坏的涉密计算机设备硬盘集中，填写“涉密载体销毁清单”，经部门领导批准后，交保密办进行统一销毁。

第十五条 涉密计算机设备硬盘的销毁工作由保密办归口负责。

第十六条 拟销毁的涉密计算机设备硬盘要登记造册，两人核对、两人监销。

第十七条 涉密计算机设备硬盘要使用相应有效手段消除涉密信息。

第十八条 涉密计算机设备硬盘销毁必须确实达到涉密信息彻底销毁且不可恢复。

第七章 涉密计算机设备接入管理

第十九条 为了保障上海船研所涉密信息系统基础网络和重要信息系统的安全运行，规范网络管理部门及网络平台使用部门的行为，以管理促安全，积极防御、综合防范，制定本管理办法。本管理办法适用于上海船研所涉密信息系统涉密信息点的申报、接入、管理。

（一）涉密点设置工作：

上海船研所涉密信息系统根据工作需要进行申报。同时满足国家保密标准BMB17-2006《涉及国家秘密的信息系统分级保护技术要求》、BMB20-2007《涉及国家秘密的信息系统分级保护管理规范》的要求及规范设置涉密点，包括涉密终端技术及管理上的各相关要求。

1. 涉密点连通：

涉密点只有通过安全保密测评通过后，方可开通。开通后应严格遵守国家保密局上海船研所涉密信息系统相关保密规定。

2．未经测评通过的涉密信息点一律不得使用，相关交换机端口由系统管理员设置关闭状态，线路与交换机物理断开。

附录 A

计算机设备领用审批表

设备编号		密级	□非密 □秘密 □机密	责任人 使用人	
固定资产号		类别	□台式 □单机 □便携式 □网络终端	品牌型号	
其它配置					
设备系列号 服务标签		IP 地址		使用地点 （房间号）	
硬盘序列号				购置日期	
MAC 地址				操作系统 安装日期	
主要配置				启用日期	
安装软件	□标配　□见备注　□其它			打印端口	□开启　□关闭
管理员签字	签字：　　日期：				
领用人签字	签字：　　日期：				
领导审批意见	签字：　　日期：				
备注说明					

附录 B

计算机设备信息变更登记表

设备编号		密级	☐非密 ☐秘密 ☐机密
固定资产号		类别	☐台式 ☐单机 ☐便携式 ☐网络客户端
变更内容			
日期	变更内容	变更前	变更后	管理员签字

附录C

涉密电脑重装系统、软件申请单

申 请 人		所在部门	
申请理由			
电脑编号		安装时间	
重装系统（勾）		安装软件（勾）	
需安装工作软件			
部 门 意 见			
信息化管理组			
备 注			

附录 D

涉密计算机设备维修登记表

编号：

申请部门		申请人	
设备编号		设备型号	
资产编号		密级	
申请日期		保修期情况	
故障现象			
涉密处理记录			
处理人		年　　月　　日	
维护工作记录			
维护人		年　　月　　日	
申请部门验收意见			
响应速度： 完工速度： 完工质量：			
验收人		年　　月　　日	

附录 E

涉密网络计算机台账

序号	设备编号	设备名称	设备类型	品牌型号	主要配置	硬盘序列号	MAC 地址	IP 地址	网络端口编号	责任人	密级	使用人	使用地点	启用日期	系统安装日期	使用情况	备注

附录F

涉 密 载 体 销 毁 清 单

编号

序号	文件编号	介质类别	名称	编制	日期	份数	页数	密级	销毁原因	备注

批准人：　　监销人：　　销毁人：　　销毁日期：　　年　　月　　日

第八章　便携式计算机保密管理制度

第二十条　总体原则

a)根据《中华人民共和国保守国家秘密法》、国家保密局《计算机信息系统保密管理暂行规定》，制定本规定。

b)便携式计算机的保密工作贯彻“谁保管，谁负责”的原则，保管者负有直接的保密责任。

第二十一条　便携式涉密计算机购置管理

(一) 便携式计算机必须在境内公有制计算机商店购买，严禁在境外购买。

(二) 便携式计算机须由相关主管部门统一购置，其余部门不得自行购买便携式计算机。

第二十二条　便携式涉密计算机使用管理

(三) 凡处理涉密信息的便携式计算机定义为涉密便携机，不处理涉密信息的便携式计算机为非涉密计算机。

(四) 便携式计算机在发放前应对便携式计算机的编号、硬件设备、系统、软件和责任人进行登记，涉密便携式计算机应在保密办备案并进行密级标识，贴标工作。

(五) 如因岗位调动等原因，便携式计算机责任人需要变更，必须作好便携式计算机责任人变更手续，填写“涉密计算机信息变更登记表”。

（六）便携式计算机中软件的安装，由部门系统管理员负责，由所技术部门做相应技术支持。严禁安装任何未经许可的软件、系统。严禁使用来源不明的软盘、光盘等存储介质。

（七）禁止非涉密便携式计算机以任何形式处理涉密信息。

（八）涉密便携式计算机应由专人妥善保管。

（九）凡借用涉密便携式计算机人员或部门应事先填写《涉密电脑及附属设备借用申请单》，说明借用原因，经保管者清点、处理机内文件，并经所在部门领导同意后，由安全保密管理员登记、涉密检查后方可借出，严禁将自己保管的便携式计算机私自转借他人，见附录H。

（十）安全保密管理员应做好借用及外携记录的登记保管工作。

（十一） 借用便携式计算机使用完毕后应及时归还。归还时保管者与借用者需共同检查计算机使用情况，包括使用期间保密情况和计算机完好情况，见附录I。

第二十三条 便携式涉密计算机报废、清理管理

（一）便携式计算机的报废、清理按计算机固定资产管理办法进行管理，内部硬盘按照涉密介质管理有关规定执行。

第二十四条 便携式涉密计算机维修管理

（一）维修管理参见本制度中涉密计算机维修管理。

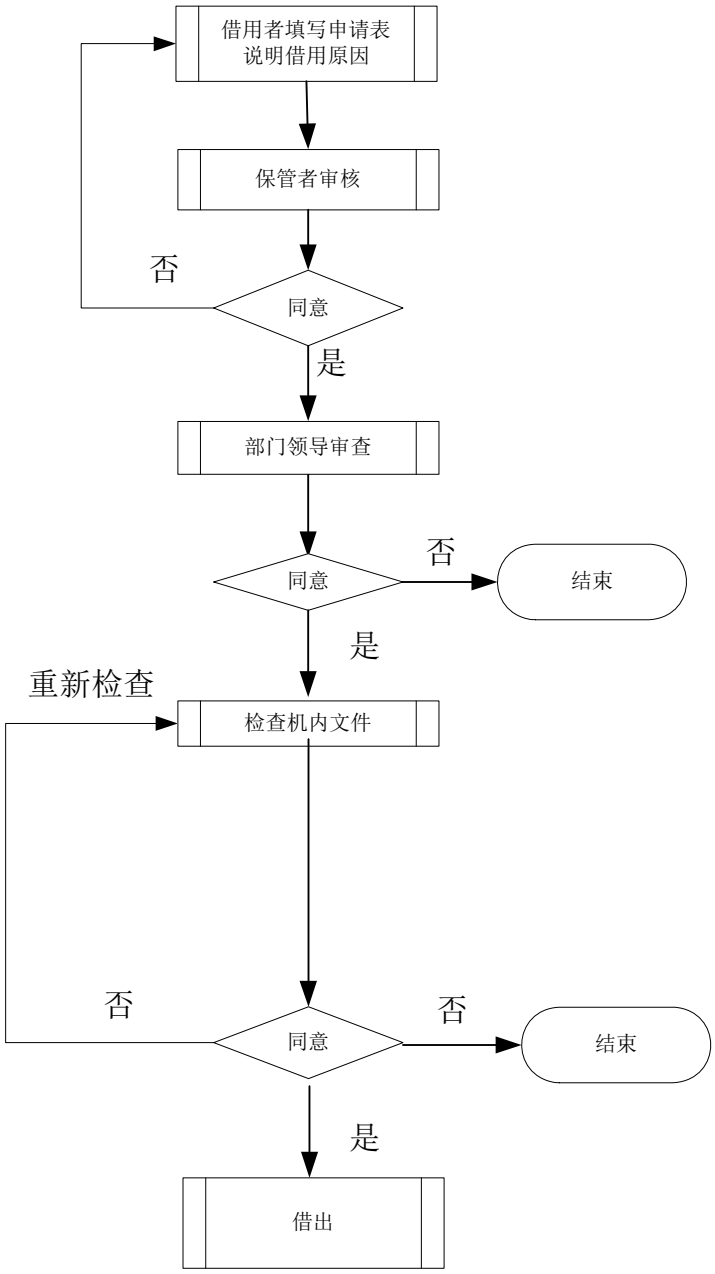
附录 1：

涉密电脑及附属设备借用申请单

<table>
<tr><td>申请人</td><td></td><td>所在部门</td><td></td><td>工号</td><td></td></tr>
<tr><td>申请理由</td><td colspan="5"></td></tr>
<tr><td>借用日期</td><td></td><td>估计归还日期</td><td colspan="3"></td></tr>
<tr><td colspan="6">借用设备如下：</td></tr>
<tr><td>设备名称</td><td></td><td>设备编号
保密编号</td><td></td><td>密级</td><td></td></tr>
<tr><td>配置情况</td><td colspan="5"></td></tr>
<tr><td>附件说明</td><td colspan="5"></td></tr>
<tr><td colspan="6">借用人签字（含日期）：</td></tr>
<tr><td colspan="6">部门领导意见：</td></tr>
<tr><td colspan="6">综合计划部领导意见：</td></tr>
<tr><td colspan="6">分所领导意见：</td></tr>
<tr><td colspan="6">备注说明：</td></tr>
<tr><td>归还情况描述</td><td colspan="5">口设备整洁　口配置齐全　口系统良好　口使用信息已清除
其它说明：</td></tr>
<tr><td>实际归还日期</td><td colspan="2"></td><td>核实人</td><td colspan="2"></td></tr>
</table>

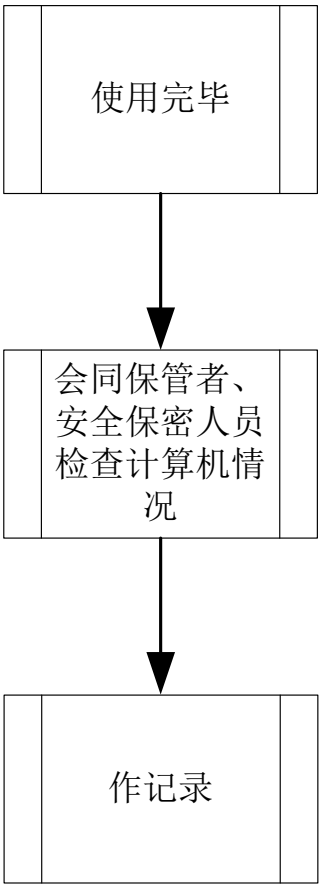
附录：

便携式计算机借用审批流程



附录：

归还流程



上海船研所涉密信息系统涉密载体管理规定

在上海船研所涉密信息系统中，存储涉密信息的介质(含磁盘、磁带、光盘和 U 盘等)，定义为计算机信息系统的涉密载体。依照国家安全保密主管部门的规定要求，在上海船研所涉密信息系统中，涉密介质要严格管理，特制定本规定。

第一条 上海船研所涉密信息系统计算机存储涉密信息的存储介质（U 盘、移动硬盘、光盘、软盘等)，应按存储信息的最高密级表明密级，并按密级文件进行管理，见附录 A。

第二条 涉密 U 盘、涉密移动硬盘、涉密光盘、涉密软盘，应由使用部门统一购置、履行领用手续、登记造册并由专人统一管理，涉密介质应当与非密介质分开保管，涉密介质应放置于铁质密码柜中。禁止使用私人磁介质存储涉密信息。

第三条 应建立涉密移动存储设备使用管理制度，禁止在涉密计算机和非涉密计算机之间交叉使用 U 盘、移动硬盘等移动存储设备。

第四条 存储过涉密信息的存储介质不得降低密级使用，无保存价值的涉密介质应当报领导批准后销毁，并做好销毁记录。

第五条 涉密存储介质维修及数据恢复，必须在市国家保密局定点单位（具有上海船研所涉密信息系统数据恢复资质的单位）进行。禁止将涉密介质交由非定点单位处理。

第六条 在上海船研所涉密信息系统计算机上打印输出涉密文件，应按有关规定严格执行，并按相应密级文件进行管理。不得擅自拷贝涉密信息。

第七条 进入上海船研所涉密信息系统的涉密信息，应当根据国家保密局会同中央、国家机关有关部门制定的《国家秘密及其密级具体范围的规定》，确定并标明密级。

第八条 未经部门领导审批，不得在上海船研所涉密信息系统中擅自发布涉密信息。绝密级及机密级的信息不得进入上海船研所涉密信息系统。

第九条 因工作需要，将非上海船研所涉密信息系统上的数据拷贝至上海船研所涉密信息系统计算机，须经领导批准后采取先行查杀病毒、木马，刻录光盘后单向导入方式。

第十条 上海船研所涉密信息系统计算机上的非涉密信息未经批准不得拷贝至非涉密计算机。上海船研所涉密信息系统涉密计算机上的高密级信息不得拷贝至低等级信息系统。

第十一条 涉密介质携带离开本单位规定。

（一）不得私自携带涉密存储介质离开本单位。

（二）特殊情况携带涉密存储介质离开本单位须履行保密审批。

（三）携带涉密介质出差要采取可靠的安全措施，两人以上同行的要明确主次责任。

（四）携带涉密介质出差应用专车到机场、车站、码头接送。

（五）携带数量较多的机密级涉密介质，乘火车可乘软卧席，乘飞机轮船可相当于火车软卧的同等舱位。

（六）禁止将涉密介质携带到不具备保密条件的场所 （如医院、列车、飞机、轮船等处）阅办；禁止携带涉密介质外出旅游、探亲访友、参加外事活动等。

（七）涉密介质丢失，使用人员应立即上报部门及保密办，保密办应按照规定要求对事件进行处置。

（八）对于归还的涉密介质应进行信息删除处理。

第十二条 涉密介质要按存放时间进行报废更新,软盘报废更新周期不长于6个月，光盘报废更新周期不长于1年，报废更新要经专业技术人员鉴定,报废更新前要做好新的备份转存,并做好报废介质登记记录。报废介质要按照涉密介质销毁规定进行严格销毁。

第十三条 涉密介质不得降低密级使用和记录非密信息,无保存价值的涉密介质要报领导批准后销毁，必须送上海市国家保密局指定地点销毁，并作好销毁记录。

第十四条 涉密介质的维修应到上海市国家保密局指定的地点进行维修或消磁，确保所有存储的涉密信息不被泄露。

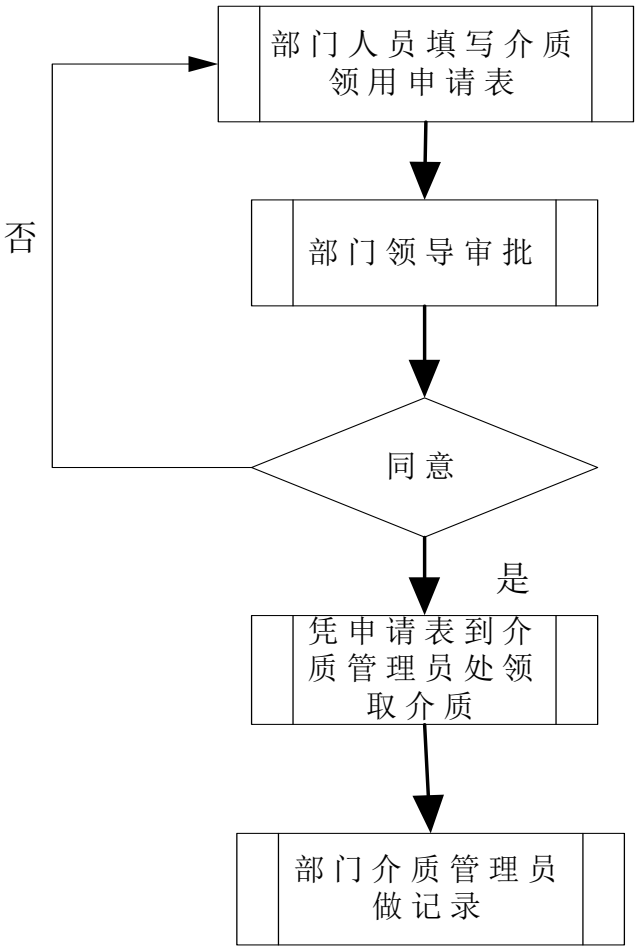
附录 A：

移动存储介质借用登记表

借用日期	借用人	借用原因（内容）	U 盘编号	归还日期	备注

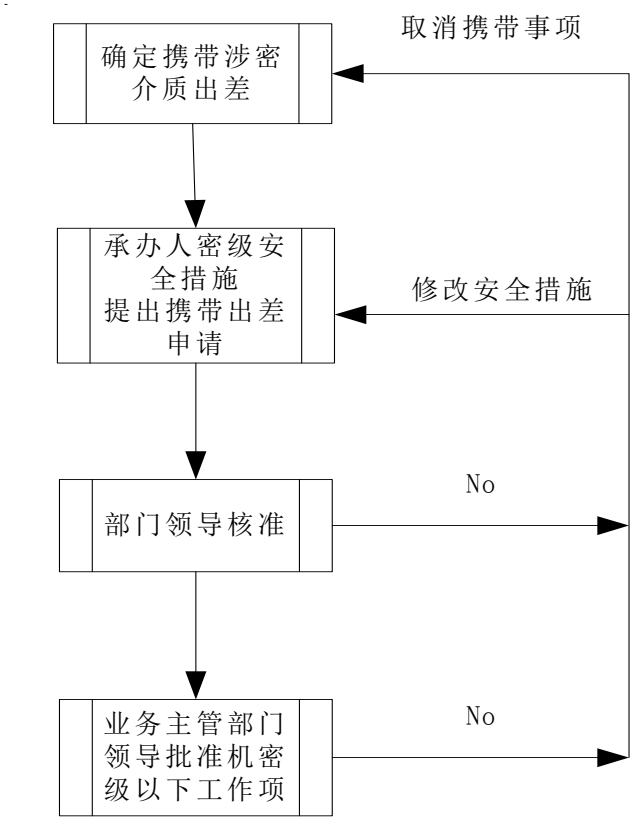
附录 B

涉密介质使用流程



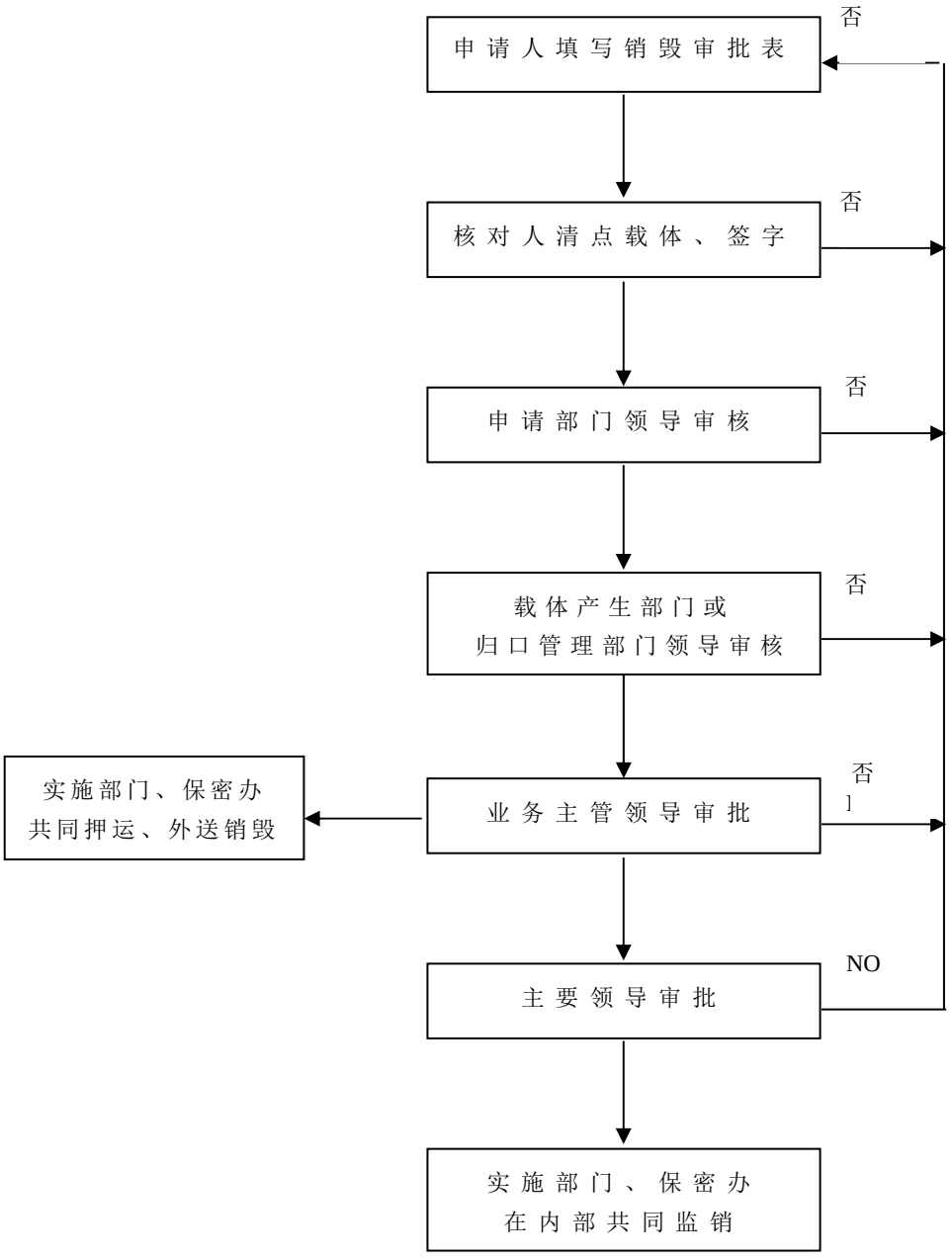
附录C

携带涉密载体出差保密审批程序



附录 D

涉密载体销毁审批流程图



上海船研所涉密信息系统分级保护管理规定

第一条 系统定级

（一）上海船研所涉密信息系统按照所处理信息的最高密级，由低到高划分为秘密、机密和绝密三个等级，上海船研所涉密信息系统最高密级为秘密级。

（二）当上海船研所涉密信息系统处理信息的密级和应用情况发生变化时，上海船舶运输科学研究所将根据上海船研所涉密信息系统相关文件，重新组织确定系统保护等级，并按相应等级要求调整保护措施。

第二条 方案设计

（一）上海船研所涉密信息系统建设在上级主管部门与安全保密日常执行机构的指导和监督下，选择具有相应涉密资质的承建单位承担上海船研所涉密信息系统的方案设计与实施、综合布线、系统服务、系统咨询、屏蔽、工程监理和保密安防监控等。

（二）上海船研所涉密信息系统集成资质分为甲级、乙级和单独三种，上海船研所涉密信息系统建设使用单位应按照下列原则选择相应的承建单位：

1、 上海船研所涉密信息系统或安全保密技术要求较高的上海船研所涉密信息系统，优先选择甲级资质单位。

2、 上海船研所涉密信息系统建设使用单位在选择乙级资质单位时，选择本省、自治区、直辖市所辖行政区域内的乙级资质单位；

3、 军工系统集成单项资质单位只能在所属军工集团内承接上海船研所涉密信息系统集成业务；

4、 上海船研所涉密信息系统的软件开发、综合布线、系统服务、系统咨询、风险评估、工程监理、数据恢复和保密安防监控等单项业务，选择具有单项资质的单位承担。

（三）上海船研所涉密信息系统建设使用单位和承建单位依据分级保护方案设计指南、BMB17-2006、BMB20-2007、BMB23-2007 进行系统方案设计。在方案设计前，首先进行风险评估，根据评估结果确定采取的保护措施，增强分级保护的针对性。具体步骤如下：

1、 根据系统定级，确定系统保护所应达到的基本要求；

2、 结合系统实际进行风险评估，对部分保护要求做适当调整；

3、 按照最终确定的保护要求，采取具体的保护措施。

（四）上海船研所涉密信息系统方案涉及阶段的风险评估由建设使用单位组织自身技术力量开展或委托具有相应资质的单位承担。

（五）确定为秘密级的信息系统，根据上海船研所涉密信息系统重要性、系统中涉密信息的数量和含量、信息系统的重要程度和建设使用单位对信息系统的依赖程度等因素，确定是否选择 BMB17-2006 中的保护要求。

（六）上海船研所涉密信息系统中相同等级的不同安全域，根据风险评估结果采取不同的保护措施；系统中不同等级的安全域，应按照相应等级的保护要求进行保护。

（七）处理涉密信息的单台计算机，根据所处理信息的最高密级，按照相应等级上海船研所涉密信息系统的有关要求进行保护和管理。

（八）上海船研所涉密信息系统投入使用前有关风险评估、方案设计、方案评审论证、工程监理和系统测评等所需经费，系统建设使用单位须在系统规划时按照一定比例统一纳入系统建设经费预算予以解决。

（九）系统设计方案由上海船研所涉密信息系统建设使用单位、办公室、保密办、信息化主管部门组织审查论证，聘请保密工作部门人员以及保密专家参与方案评审论证，在系统总体安全保密性方面加强指导，严格把关。

第三条 工程实施

（一）在进行工程前，应选择具有涉密工程监理单项资质的单位在安全保密控制、质量控制、进度控制、成本控制、合同管理和文档管理六个方面加强监督检查。

（二）在工程实施时，办公室、保密办、信息化主管部门、上海船研所涉密信息系统工程监理、上海船研所涉密信息系统建设单位将根据工程的具体情况划定保密范围，制定相应的保密措施和保密控制流程，严格控制接触涉密信息的人员范围。

（三）在工程实施期间，办公室、保密办、信息化主管部门、上海船研所涉密信息系统工程监理、上海船研所涉密信息系统建设单位将按照 BMB18-2007 的要求组织工程监理。

第四条 系统测评

（一）上海船研所涉密信息系统建设使用单位在系统工程施工结束后，应上级保密工作部门提出申请，由国家保密工作部门授权的系统测评机构对上海船研所涉密信息系统进行安全保密测评，系统全面地验证

所采取的安全保密措施能否满足安全保密需求和安全目标，为上海船研所涉密信息系统审批提供依据。

（二）上海船研所涉密信息系统建设使用单位应按照国家保密工作部门授权的系统测评机构的要求，提交测评所需的必要资料。

第五条 系统审批

（一）国家对上海船研所涉密信息系统投入运行实行行政审批制度。上海船研所涉密信息系统建设使用单位在系统投入使用前，应按照上海船研所涉密信息系统审批管理办法的规定进行审批，通过审批后方可投入使用。未经保密工作部门的审批，上海船研所涉密信息系统不得投入运行。

（二）国家保密局负责审批中央和国家机关各部委及其所属单位、国防武器装备科研生产一级保密资格单位的上海船研所涉密信息系统；省（自治区、直辖市）保密局负责审批省直机关及其所属单位、国防武器装备科研生产二、三保密资格单位的上海船研所涉密信息系统；市（地）级保密局负责审批市（地）直机关及其所属单位、县直机关所属单位的上海船研所涉密信息系统。

（三）上海船研所涉密信息系统通过国家保密工作部门授权的系统测评机构的安全保密测评后，其建设使用单位应通过保密办按照上海船研所涉密信息系统审批管理规定的要求，向负责审批的保密工作部门提出投入运行前的审批申请，并报送相关材料。

第六条 日常管理

（一）上海船研所涉密信息系统经过审批投入运行后，应严格按照上海船研所涉密信息系统分级保护管理规范的相关要求，明确安全保密管理策略，组建相应安全保密管理机构，设置安全保密管理人员，落实保密管理制度。

（二）上海船研所涉密信息系统应从人员管理、物理环境与设施管理、设备与介质管理、运行与开发管理和信息保密管理五个方面进行日常安全保密管理。

（三）上海船研所涉密信息系统经过审批投入运行后，建设使用单位应至少每年进行一次风险自评估工作，分析由于系统需求及技术与管理因素变化而新出现的安全威胁，动态调整安全策略，适时补充和完善技术与管理措施，以使系统保持与等级要求相一致的防护水平。风险自评估过程中形成的有关数据、记录和评估报告，应及时定密并按照相应密级文件进行管理。

第七条 测评与检查

（一）系统投入运行后，秘密级、机密级信息系统应每两年至少进行一次安全保密测评或保密检查；绝密级信息系统应每年至少进行一次安全保密测评或保密检查。

（二）上海船研所涉密信息系统投入运行后的安全保密测评，由负责该系统审批的保密工作部门组织系统测评机构进行，以检验系统安全保密措施的有效性和对环境变化的适应性。当系统环境或应用发生重大改变时，应及时进行方案论证和安全保密测评，并采取相应的补充保护措施。

（三）上海船研所涉密信息系统投入运行后的保密检查，由保密工作部门的保密技术检查机构承担，进行有针对性的保密监督检查，发现问题、堵塞漏洞、消除隐患。

（四）安全保密测评和保密检查过程中形成的有关数据、记录和评估报告，应及时定密并按照相应密级文件进行管理。

第八条 系统废止

（一）上海船研所涉密信息系统不再使用时，应通过保密办向负责该系统审批的保密工作部门备案，并按照设备与介质使用保密规定妥善处理涉及国家秘密信息的设备、产品、介质和文档资料。

（二）对需要报废处理的涉密设备和涉密介质，应统一由保密办组织进行信息消除和载体销毁处理，所采用的技术、设备和措施应符合相关标准和规定，防止失泄密事件的发生。

上海船研所涉密信息系统运行与开发管理规定

第一章　职责

第一条　安全保密管理机构职责

（一）安全保密管理机构指由办公室、保密办及其它管理部门组成的各负其责的管理体系。

（二）负责信息系统开发管理过程的各项安全保密审批工作

（三）负责信息系统安全保密的指导监督工作

（四）负责组织信息系统的立项审查和验收。

（五）负责信息系统各项安全保密功能审核工作

第二条　信息系统使用部门职责

（一）负责提出信息系统安全保密需求。

（二）落实信息系统开发中的安全保密管理。

（三）负责信息系统运行过程中的岗位操作信息安全管理。

第三条　信息系统维护部门职责

（一）负责识别对信息系统进行变更的需求，提出变更申请。

（二）负责按照《信息系统任务单》实施变更，并做相应记录。

第二章 运行开发工作程序

第四条　立项阶段

（一）信息系统安全需求的识别

信息系统使用部门在项目立项阶段提出信息系统功能需求（包含系统的容量需求）时，要通过调研、风险评估等手段识别存在的各种

安全风险，并依据信息安全管理相关规定，提出信息系统安全需求，作为信息系统整体功能需求的一部分。在开发用于处理涉密信息的业务应用系统时，应按照BMB17-2006中8.3“信息安全保密要求”的规定，从身份鉴别、访问控制和安全审计等几个方面进行安全保密功能的同步开发。

（二）容量管理

新建、扩建、改造信息系统的设计方案中应含有系统容量需求分析，容量需求除满足系统自身需求外，还需考虑未来业务发展、信息处理能力的提升以及技术发展趋势，报安全保密管理机构审查。

（三）立项审查

信息系统使用部门于每年第三季度向所主管部门申报上海船研所涉密信息系统立项计划，所主管部门组织对立项计划进行审查。

第五条 设计阶段

设计单位根据下达设计委托书，针对信息系统安全需求，完成相应的信息安全技术方案的设计，作为信息系统整体设计方案的一部分。涉密信息的信息系统应按照国家保密部门相关标准规定进行设计，并组织专家评审。

上海船研所涉密信息系统设计方案评审由所主管部门组织，评审时应考虑以下因素：

1） 对信息系统安全需求理解的准确性；

2） 风险控制的合理性；

3） 系统容量设计的合理性；

4） 技术设计和施工组织两方面的安全性；

5） 对项目建设过程中可能存在的安全风险和处理办法；

6） 与国家相关法律、法规、标准、本单位信息安全有关规定的符合性。

第六条 购买、开发、集成阶段

安全保密管理机构在合同签订时应对承建单位做出以下要求：

1） 保守国家秘密的责任和义务；

2） 保守本单位商业秘密的责任和义务；

3） 保护知识产权的责任和义务；

4） 使用本单位信息处理设施的信息安全责任和义务。

（一）购买信息系统产品

各部门涉密人员不得自行安装信息系统软件，须向相关部门提出申请，经过保密办批准后，由相关部门统一购买，在购买信息系统产品前，所主管部门与信息系统使用部门应对其产品进行测试。拟采购产品的安全功能若不能满足要求，应考虑选择其他供应商或采取相应的控制措施。购买信息系统产品，所采取的信息安全措施包括：

1) 应选购国家认可登记的正版商业软件；

2) 应选购通过国家信息安全测评认证的信息安全产品;涉及国家秘密的信息系统应使用国家保密单位批准的信息安全产品；

3) 应要求软件产品供应厂家对以下软件安全性相关内容作出明确商业承诺,必要时信息系统实施单位应对所购买的软件产品进行安全性测试，形成安全测试报告。软件安全性相关内容包括：

a）软件产品应具有时间安全性，到期不出现锁死、自毁等对计算机信息系统造成损害的情况；

b）软件不应含有病毒、后门等恶意代码；

c）软件产品应对用户输入数据进行验证，以减少用户输入错误的风险和预防包括缓冲区溢出和代码注入等攻击；

d）软件产品应对软件输出数据进行验证，以确保对所存储信息的处理是正确的且是安全的。

（二）自行开发或委托开发

新建、扩建、改造、技术进步信息系统的承建单位必须按照上海船研所涉密信息系统安全管理要求进行开发。

涉及国家秘密的信息系统承建单位必须按照国家保密部门相关标准规定进行系统开发。

应将开发、测试系统与运行系统分离，避免开发和测试活动对运行系统的稳定和安全造成影响。

在信息系统开发过程中，信息系统使用部门要对开发过程进行安全控制与管理。包括：

1）在委托开发过程中，信息系统使用部门应加强开发过程中的安全管理和监控，重点考虑资质、许可证、代码所有权和知识产权；审核工作质量和访问权限，代码质量和安全功能达到合同要求。特殊情况应测试恶意代码和特洛伊木马。

2) 信息系统使用单位应要求承建单位在所开发的信息系统内设计实现了安全控制措施，确保信息在系统中得到了正确处理。控制措施包括：

a) 系统应对用户输入数据进行验证，以减少用户输入错误的风险和预防包括缓冲区溢出和代码注入等攻击；

b) 系统应对内部处理中的数据完整性进行验证检查，防止正确输入的数据被硬件错误、程序故障所损坏；

c) 必要时，应保护系统内所传输的消息的真实性和完整性；

d) 系统应对输出数据进行验证，以确保对所存储信息的处理是正确的且是安全的。

3) 在发生变更时,信息系统使用部门应严格对开发过程中的变更进行控制。

4) 在开发过程中，信息系统使用部门应采取控制措施，减少信息泄露的可能性，重点考虑：规范开发过程中的通信行为，以减少第三方从这些行为中推断信息的可能性;在现有法律或法规允许的情况下，定期监视个人和系统的活动；监视计算机系统的资源使用；防止非授权的网络访问；对程序源代码的防护管理；

5) 信息系统使用部门应要求承建单位对程序源代码进行管理与控制。程序源代码应集中保存在代码库中,对代码库实施安全保护。保护措施主要包括：建立程序源代码和源程序库管理规范；对访问源程序库人员进行授权管制；程序列表应保存在安全的环境

中；建立对源程序库所有访问的审核日志；维护和拷贝源程序库应受严格的限制；

6）测试数据的管理。信息系统使用部门对于开发过程中涉及的测试数据，例如使用本部门离线的数据进行测试时，应考虑安全性选择、保护和控制。在测试数据选择过程中，应避免使用包含个人信息或其它敏感信息的运行数据库用于测试，禁止使用涉密信息作为测试数据。其控制措施包括：运行信息每次被拷贝到测试系统时应有独立的授权；测试完成后，应立即从测试系统中清除运行信息或进行授权访问控制；记录运行信息的拷贝和使用日志；

7）信息系统安全整体测试。信息系统使用单位组织信息系统承建单位在离线测试环境下对所开发信息系统进行安全测试。测试内容包括系统所提供安全功能的测试，以及系统自身安全性的测试。系统安全功能测试依据系统安全需求进行。经过测试确认并经过验收后，方可转入正式运行环境，并组织评估测试结果的安全符合性。

（三）系统集成

新建、扩建、改造、技术进步信息系统的承建单位必须按照本单位信息系统安全管理要求进行系统集成。

涉及密信息的信息系统承建单位必须按照国家保密部门相关标准规定进行系统集成。

在信息系统集成过程中，信息系统使用单位要对集成过程进行安全管理与控制。其措施包括：

1) 审核所集成产品的许可证、知识产权；

2) 审核集成工作质量，安全功能集成达到合同要求；

3) 检查承建方人员是否按合同要求,正确使用自带或本单位的信息处理设施；

4) 检查承建方是否对系统初始配置进行了修改；

5) 检查系统集成测试对现有系统运行造成的影响和处理办法；

6) 选择有资质的监理方对工程进行监理。

第七条 系统试运行与上线阶段

信息系统使用部门负责进行信息系统离线试运行，在试运行阶段结束时由信息系统使用部门会同信息系统承建单位编写系统试运行总结报告，经验收通过后提交系统上线申请，报所保密办审批。

系统应由国家保密局许可的第三方测评机构进行测评，按照国家制定的安全标准和本单位安全管理规定，对信息系统进行安全测评，其测评报告中需明确说明系统对安全要求与安全措施满足的情况。测评报告应作为试运行总结报告的组成部分。

所保密办对试运行总结报告与上线申请进行审批，审批通过的信息系统转入正式上线运行。

第八条 系统验收阶段

信息系统正式上线运行一段时间后，所主管部门会同信息系统使用单位、承建单位，根据合同中规定的信息安全有关条款进行验收。

验收时，承建单位应按照本单位工程项目管理要求提交竣工验收文档，并对验收文档中以下内容进行重点审查：

1) 性能和计算机容量符合设计要求；

2) 系统安全保密功能和系统自身安全性达到合同要求；

3) 具备故障恢复程序以及应急预案；

4) 新系统对本单位总体信息系统安全保密性影响的说明；

5) 新系统的用户操作手册。

第九条 信息系统运维阶段

（一）所主管部门每半年组织对上海船研所涉密信息系统内安全保密设备的安全策略规则进行审核。并根据系统规模、用户数量变化的情况进行风险评估、及时调整系统的保护策略。

（二）保密办每半年组织一次系统的运行情况和用户操作行为进行安全保密法规、保密标准符合性方面的检查。

（三）根据系统的变化情况，上海船研所涉密信息系统的管理人员应及时更新系统文档资料，使之与实际状况保持一致。

（四）后期维护或升级服务人员需要对系统操作访问时，应对其权限进行限制，禁止其访问涉密信息；

（五）应由专人对进入现场进行后期维护或升级的服务人员全程陪同，禁止其将具有存储功能的自带设备接入系统。

（六）信息系统使用部门应保证对信息系统操作做到：定地点、定岗位、定职责，并制订相应的操作规程和配套的管理制度。岗位操作人员上岗前必须经过本所或本所专业部门组织的专业知识培训，能正确地使用本岗位操作功能。

（七）信息系统维护部门应制定系统维护规程，安排维护人员，维护人员应及时报告维护过程中发现的异常现象和故障，对系统容量进行监控，对系统资源进行定期清理，并做好设备检修、调试记录。

（八）信息系统使用部门定期对信息系统使用中的安全管理情况进行检查，检查内容包括：

1) 岗位操作人员是否按操作规程要求，及时、正确录入数据，是否在终端设备上从事与本岗位不相关的工作；
2) 信息系统维护人员是否严格按照维护规程进行了操作和维护，系统维护日志是否真实、完整；
3) 是否擅自拆除、迁移终端设备，卸载系统软件和应用软件，在终端设备上安装和使用与本岗位业务无关的任何软件，在终端上安装和使用盗版软件；
4) 信息系统出现故障时是否得到了及时报告和处理。
5) 信息系统维护单位是否对系统运行软件的版本进行严格控制。

上海船研所涉密信息系统变更与控制管理规定

第一章　职责

第一条 安全保密管理机构职责

（一）负责对信息系统变更申请的审批。

第二条 信息系统使用单位职责

（一）负责识别对信息系统进行变更的需求，提出变更申请。

第三条 信息系统维护单位职责

（一）负责识别对信息系统进行变更的需求，提出变更申请。

（二）负责按照《信息系统任务单》实施变更，并做相应记录。

第二章 工作程序

第四条 变更申请的提交

信息系统使用部门、信息系统维护部门负责识别具体的变更需求（如范围、可交付成果、时限、组织等），填写《信息系统任务单》，必要时附相关资料，报保密办公室审批。

第五条 变更申请的审核

（一）由信息系统使用单位、信息系统维护部门的信息主管领导对本部门提交的《信息系统任务单》进行审批，审批通过后报保密办。

（二）保密办公室对上报《信息系统任务单》中变更内容的安全性进行审核。

（三）对重大的信息系统变更，或者流程变更，由安全保密管理机构职责、信息系统使用部门、信息系统维护部门、计算机专家组成员对变更申请进行进一步审查。可以从以下方面进行审查：

1、变更需求的详细描述；

2、可以选择的变更方式；

3、变更所需的成本及带来的利益；

4、变更的风险，至少应包括变更对业务、系统带来的影响，对原有安全措施以及数据完整性的影响；

5、变更的建议和计划。

（四）保密办对《信息系统任务单》形成正式审查意见。对于审批通过，需要立项解决的信息系统变更，由信息系统使用单位向保密办提出立项申请，按相关程序执行。对于审批通过，不需要立项解决的信息系统变更，由主管部门批准后对《信息系统任务单》进行统一编号，并转使用部门进行组织实施。

第六条 变更的实施

（一）使用部门接到《信息系统任务单》批复后，立即组织实施变更。

（二）在实施变更的过程中，应保证变更有具体的变更实施进度计划和资源使用计划。

（三）在正式运行的系统上实施变更前，还应考虑以下控制措施：

1、确保执行变更的时候不会对业务造成较大或以上的影响；

2、对变更的内容做完整的测试和检查，确保变更不会出现非预期的情况；

3、在正式运行的系统上进行数据备份，确保在变更失败时不会损失重要数据；

4、预先确定返回流程，在变更失败或发生非预期事件后，能够从变更流程中返回。

（四）对操作系统和应用软件的变更实施过程，应考虑以下控制措施：

1、维护所有软件更新的版本控制；

2、确保在每个变更完成之后更新系统配置文件，并将旧文件归档；

3、必要时，确保对用户操作手册作合适的更新。

第七条 变更结果的评估和报告

在完成变更后，应对变更的实施情况和结果进行记录和评估，填写《信息系统任务单》中相应内容。评估内容包括以下方面：

1、变更计划执行的情况；

2、变更过程中出现的非预期情况；

3、变更后系统的安全现状；

4、变更实施结果。

5、完成变更后，将《信息系统任务单》反馈到保密办公室，由保密办将变更执行情况进行备案。

附录 1：

信息系统任务单

系统名称：

编号：

系统名称		提出部门		提出人		提出时间		联系电话	
提出原因及理由									
工作内容									
涉及到相关系统或程序									
提出部门领导审批意见				审批日期		要求完成时间			
任务涉及单位审批意见									
保密办审批意见		审批日期		完成时间		完成单位			
办公室领导审批（重大任务）									
具体工作责任人				预计完成时间		实际完成时间			
完成任务情况说明									
验收人意见		验收人		验收日期		程序上线日期			
其它补充说明									

备注：任务主要含：新增或修改程序、修改数据、数据提供、数据转移或备份、批次作业调整、密码初始化、系统接入（IP 分配）等。（实施单位在验收确认后的 2 个工作日内将此单反馈到主管部门存档）

上海船研所涉密信息系统操作系统、数据库及应用软件安全保密管理规定

上海船研所涉密信息系统计算机中操作系统、数据库及应用软件是整个计算机信息系统重要组成部分，对整个系统正常运行起到重要作用，特制定如下规定：

1、上海船研所涉密信息系统中，所有服务器设备及接入终端的操作系统均要安装正版软件，严禁使用测试版和盗版软件。

2、正版软件安装后，须使用可靠检测软件或手段进行安全测试，了解其脆弱性，并根据脆弱性程度采取措施，进行系统补丁及安全优化，使风险降至最小。

3、操作系统要设置安全策略和口令修改策略。要建立用户身份验证、访问权限控制等保密防御机制和安全事件的审计机制。操作系统安全日志应定期审查备份。

4、上海船研所涉密信息系统中各类数据库必须采用正版数据库软件，数据库中要建立用户身份鉴别、访问权限控制和数据库审计等安全保密保障措施。

5、上海船研所涉密信息系统应用软件要使用正版软件，开发商要确保软件中使用第三方软件的合法性。

6、应用软件要建立用户身份认证、访问权限控制等安全保密保障措施。

上海船研所涉密信息系统信息保密管理规定

为了进一步加强对上海船研所涉密信息系统中涉密信息的生成、存储、查看、传输、复制、备份、归档、销毁的管理，特制定本规定。

第一条 上海船研所涉密信息系统各类信息均应按照有关现行规定确定级。

第二条 在上海船研所涉密信息系统中涉密信息的发布要经安全保密主管部门严格审批，审批后由涉密信息专业维护人员发布，并做好信息发布记录等级。未经主管领导审批，任何人不得在上海船研所涉密信息系统中擅自发布涉密信息，违反规定者将按泄漏相应密级文件规定处理。

第三条 应认真做好上海船研所涉密信息系统各类涉密信息的管理工作，每周对涉密信息总量进行统计并做好相关记录。

第四条 上海船研所涉密信息系统密级标识规范

（一）凡在上海船研所涉密信息系统内存贮、处理、传递、输出的涉密信息均应标识密级。

（二）涉密电子文件应按照密级设定与变更的有关规定设定密级。

（三）设定密级后的文件应在存贮文件名和文件首页上标明相应的密级标识。

（四）标识后的涉密文件应进行加密存储，并设置口令进行保护。在未配备统一购置的加密软件情况下，采用 ZIP 中的加密功能对各文件进行压缩并加密，压缩完成后应将源文件删除。

第五条 涉密信息的查看须严格按照上海船研所涉密信息系统统一管理规定。系统中需严格按照用户等级界定用户可查看的涉密信息密级，任何用户不得越权查看高于其权限等级的涉密信息。

第六条 涉密信息不得异地传输，不准将涉密信息在非涉密网络及不安全网络上传输和发布。

第七条 涉密信息的复制需经分所领导审批，必须填写“涉密资料打印审批表”或“涉密信息输出审批和管理登记表”，未经审批，任何人不得擅自复制涉密信息，涉密信息复制须做好登记记录。

第八条 涉密信息备份、归档、销毁应严格按照有关规定执行。

第九条 涉密文件打印管理制度

（一）所有涉密文件在部门指定地点进行打印。

（二）涉密文件严禁在非涉密计算机上打印。

（三）上海船研所涉密信息系统中涉密文件的打印必须填写“涉密资料打印审批表”，经部门领导审批同意后交保密管理员负责打印并登记管理。

（四）打印出的涉密文件按照涉密载体有关的管理制度进行管理。

第十条 涉密载体保密管理

（一）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、磁介质、光盘、胶片等各类物品。磁介质载体包括计算机硬盘、软盘、优盘和录音带、录像带等。

（二）本制度适用于负责制作、复制、收发、传递、使用、保存和销毁涉密载体的所有部门和个人（以下统称涉密部门、个人）。

（三）涉密载体由该载体所在部门负责管理。涉密载体的保密管理，应当遵循严格管理、严密防范、确保安全、方便工作的原则。

（四）涉密部门应当指定政治上可靠、具备相关专业知识的专门人员负责本部门涉密载体的日常管理工作，在管理中应当严格执行国家有关法律、法规和保密规定，加强指导、监督和检查，确保国家秘密安全。

第十一条 上海船研所涉密信息系统授权管理

（一）上海船研所涉密信息系统为内部采集、存贮、处理、传递国家秘密信息的专用系统。

（二）上海船研所涉密信息系统中的每个用户都设有独立的帐号。上海船研所涉密信息系统将对帐号进行统一管理，根据一定的要求设置分组（科室）。如人员发生变更，（岗位调动，调离）应由使用部门的安全保密管理员及时通知系统管理员更改分组。分组信息应进行登记应交使用部门安全保密管理员进行备案。

（三）在网络管理过程中，若发现有未进行安全共享设置的密级文件，经安全保密管理员确认后，有权将该涉密文件删除。

（四）安全保密管理员要对系统的各级访问权限进行严格管理，不得泄漏各类密码口令，监督系统管理员对各级访问控制权限的设置。

（五）系统管理员定期应将所有用户的账户信息及权限分配表打印成册，交保密管理员备案，分管安全保密的领导应组织审查权限列表，发现异常情况，及时向系统安全保密管理机构进行汇报。

附件 1

涉密资料打印审批表

申请人姓名		申请日期		
申请打印内容				
序号	涉密资料名称	密级	打印份数	张/份
申请理由				
领导审批	年　月　日			
申请人收到涉密资料签字	年　月　日			
资料最好归属				

附件 2

资料外送印刷申请单

申请部门		申请人		申请日期	
印刷单位		涉密资质		□有 □无	
序号	资料名称	份数/页数		密级	
1					
2					
3					
4					
5					
6					
资料印刷后接收人签字					
申请部门领导意见					
技术审核意见					
保密安全管理员意见(是否需要交所保密办审核)					
综合计划部领导意见					

附件 3

上海船舶运输科学研究所
资料交接回执单

移交单位		接收单位			
序号	资　料　名　称		密级	类型	数量
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
时　间		地　点			
移交方签名		接收方签名			
备注					

注：1.“类型”一栏填写图纸、文件、光盘。

2.若为外寄材料，请在备注栏中注明接收方的联系方式，并请接收单位签字后寄回或传真至我单位。

3.本表一式两份，移交方、接收方各执一份。

附件 4

涉密信息输出审批和管理登记表

<table>
<tr><td>输出涉密信息内容</td><td colspan="5"></td><td>密级</td><td></td></tr>
<tr><td>输出形式</td><td colspan="2">□复印 □刻录 □外发</td><td colspan="2">介质名称 X 份数</td><td colspan="3"></td></tr>
<tr><td>申请部门</td><td colspan="2"></td><td>申请人</td><td colspan="2"></td><td>申请日期</td><td></td></tr>
<tr><td>介质编号</td><td colspan="7"></td></tr>
<tr><td colspan="8">申请输出理由：</td></tr>
<tr><td colspan="8">部门领导或指定负责人意见：
年 月 日</td></tr>
<tr><td colspan="8">输出承办人签名、确认输出载体是否已标密：
年 月 日</td></tr>
<tr><td colspan="8">申请人收到签字：
年 月 日</td></tr>
<tr><td rowspan="2">过程和末尾控制记录及管理</td><td colspan="3">清理记录</td><td>外发</td><td>销毁</td><td>存档</td><td>其他办理</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>责任人签 名</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>备注</td><td colspan="7"></td></tr>
</table>

上海船研所涉密信息系统泄露国家秘密事件监测、报告、查处规定

第一条 本制度所称泄露国家秘密事件是指使国家秘密被不应知悉者知悉，或者超出限定的知悉范围，而不能证明未被知悉者知悉的事件(下称泄密事件)。

第二条 上海船研所涉密信息系统应急响应小组应根据需求目标，制定应急响应策略，进行评审和演练，筹备所需资源，并将预案分发给相关人员。

第三条 由上海船研所涉密信息系统使用单位，系统管理员对运行安全事件和泄密事件进行监测、报告和预处理，由系统管理员、保密管理员、审计管理员通过对网络审计日志、入侵检测记录、主机审计日志、各项记录的分析实现对上海船研所涉密信息系统事件的监测，发现异常应及时向部门领导、保密办汇报，进行快速处置。

第四条 发生灾难事件，应由保密办负责整个灾难现场和灾难恢复过程中的安全保密管理工作，部门领导、系统管理员、保密管理员协助进行涉密介质和涉密设备的处置，保护国家密的安全。

第五条 发生泄密事件后，部门应当及时向保密办公室报告，不得隐瞒或自行处理后再报，执行一事一报制度。保密办公室负责向保密委员会报告。

报告内容为：被泄露秘密事项的内容、密级、数量及其载体形式；泄密事件的发现过程；泄密事件发生的时间、地点及经过；泄密事件造

成或可能造成的危害；泄密责任人的基本情况；已进行的查找工作情况；拟采取的补救措施。

上报时间要求：机密级事项应当在 8 小时内上报；秘密级事项应当在 24 小时内上报。

第六条 保密办公室按照国家保密局的有关规定，向上海市国家保密局报告，执行一事一报制度。

第七条 部门向保密办公办报告后，应当及时采取补救措施，积极配合保密办公室组织力量进行追查，努力挽回或减少泄密造成的损失。

第八条 泄密事件查清后，发生泄密部门的保密分会根据查证情况，对事件的当事人按照《保密工作奖惩制度》有关规定，向保密办公室提交书面处理建议，保密办公室提出处理意见，报保密委员会审批，由保密委员会对泄密事件的有关责任人员作出处理决定。

第九条 每一泄密事件的查处工作的终结期限为 3 个月。保密办公室负责将泄密事件的发生、发现过程，泄密事件已经或可能造成的危害，造成泄密事件的主要原因，采取的补救措施和对事件有关责任人员的查证处理情况，书面上报上级保密委员会和上海市国家保密局。

第十条 应针对发生的异常事件，进行综合分析，查找原因，从技术和管理两个方面加以改进。

上海船研所涉密信息系统性能检查制度

第一条 为确保计算机信息系统的安全保密性能有效，每半年上海船舶运输科学研究所将组织一次针对上海船研所涉密信息系统的安全检查。

第二条 安全保密管理制度要求以及安全保密方案设计的要求。

第三条 由保密办牵头，部门配合。

第四条 上海船研所涉密信息系统的检查范围包括：上海船研所涉密信息系统，包括网络、服务器、客户端、安全设备、防病毒软件、屏蔽机柜计算机信息系统，以及涉密介质等各项上海船研所涉密信息系统相关的内容。

第五条 上海船研所涉密信息系统安全保密性能检查将通过记录审查、日志分析、配置查看、客户端抽查、人员问询等方式进行。

第六条 检查具体内容包括：涉密信息管理、介质管理、机房管理、涉密计算机管理、打印输出控制、安全审计、系统备份、病毒防范等各项运行安全保密措施的执行情况。

第七条 保密办负责各项记录的审查、人员问询工作。

第八条 信息化技术人员负责上海船研所涉密信息系统检查涉及技术方面的各项检查、检测工作。

第九条 使用部门负责保证检查工作的顺利进行。

第十条 各项检查的结果包括：合格、不合格两种，由各检查小组提交，最终在保密办进行汇总。

第十一条 检查不合格的应根据有关要求限期进行整改，对于

检查中发现严重违反本规定的现象将依照本保密管理制度的规定进行处罚。

附件 1

上网行为控制设备审计记录表

日期	人员	设置策略	网页审计	USB 审计	邮件审计	全盘杀毒	硬盘清理	备注

附件 2

涉密信息系统审计记录表

日期	人员	审计软件					三合一审计		windows 审计		chinasec 审计		备注
		网络审计	打印审计	文件审计	硬件审计	日志审计	台数	人员	台数	人员	台数	人员	

注：正常打 √，异常打×。

附件 3

杀毒软件漏洞补丁更新记录表

日期	人员	瑞星	江民	系统补丁	备注

上海船研所涉密信息系统使用管理规定

第一章 总 则

第一条 为加强对上海船研所涉密信息系统的使用管理，确保上海船研所涉密信息系统的安全、稳定、高效、可靠运行，根据《中华人民共和国计算机信息系统安全保护条例》、《涉及国家秘密的信息系统分级保护管理规范》、《上海船舶运输科学研究所保密管理体系文件》以及其他相关规定要求，制定本规定。

第二条上海船研所涉密信息系统主要用于传输、处理、储存秘密及以下信息，该网络在物理上与公众网实施完全隔断，属于涉密网。

第三条 保密办为上海船研所涉密信息系统管理牵头部门，所部其它有关部门根据各自工作职能，协同配合，共同做好上海船研所涉密信息系统的管理工作。

第四条 本规定适用于与上海船研所涉密信息系统相关所有设备。

第二章 组织人员管理

第五条 应当严格对上海船研所涉密信息系统计算机的安全保密管理，确定一名部门负责人分管上海船研所涉密信息系统的保密管理工作（原则上由本所主管保密工作的领导担任）。

第六条 使用部门，在本部门保密小组及分管领导的领导下，具体负责上海船研所涉密信息系统保密管理工作，承担安全保密制度的制定、日常执行情况的检查及其他涉及安全保密方面的工作，并明确

责任人。

第七条 上海船研所涉密信息系统系统管理员和保密管理员负责设备的日常维护和操作使用，应当按照《上海船舶运输科学研究所保密管理体系文件》的要求，坚持先审查后录用的原则，并报保密办备案。

第八条 上海船研所涉密信息系统使用人员要加强学习，增强安全保密意识，自觉接受密码专业知识和技术培训，禁止无关人员操作上海船研所涉密信息系统计算机。对不适宜在机要岗位工作的人员应及时调整。

第九条 上海船研所涉密信息系统管理人员要保持相对稳定，必须保证时时有人在岗，对工作调动和离职人员应履行相关手续并做好销密工作。

第三章 设备管理

第十条上海船研所涉密信息系统延伸点的涉密计算机，应放置在配备了相关物理安全防护设施的场所，放置场所必须安装铁门、铁栅栏窗和防盗报警装置。上海船研所涉密信息系统计算机必须使用专用屏蔽双绞线和屏蔽接头。

第十一条 上海船研所涉密信息系统计算机显示器等显示输出设备，不得面对门窗摆放，防止显示输出内容被非授权获取。

第十二条 上海船研所涉密信息系统服务为重要设备，使用部门不得擅自开启上海船研所涉密信息系统服务器机箱，无关人员不得接触服务器及网络控制设备。

第十三条 连接上海船研所涉密信息系统的计算机原则上应选用国产计算机。便携机（笔记本电脑）不得作为上海船研所涉密信息系统信息点接入设备。

第十四条 禁止在上海船研所涉密信息系统计算机上使用具有无线互联功能的设备（如无线键盘、无线鼠标及其它无线互联的外围设备）处理涉密信息。

第十五条 放置上海船研所涉密信息系统计算机的涉密场所，若同时还放置有连接互联网的信息设备，则连接互联网的信息设备上禁止配备、安装和使用摄像头等视频输入设备。

第十六条 上海船研所涉密信息系统计算机必须专机专用，禁止安装、运行与工作无关软件。

第十七条 用于打印上海船研所涉密信息系统信息的具有打印、复印、传真等多功能的一体机，禁止与普通电话线连接。

第四章 上海船研所涉密信息系统新增接入点

第十八条 上海船研所涉密信息系统不得擅自增加接入点。

第十九条 确因工作需要，需增加上海船研所涉密信息系统接入点，应履行以下工作程序：

1、 需增加接入点的应填写《上海船研所涉密信息系统新增接入点申请表》报所保密办公室。

2、 保密办公室确认新增接入点是否具备相关技术条件。

3、 具备相关技术条件的，由保密办确认新增接入点放置场所是否满足涉密设备物理环境安全的要求、新增接入点计算机硬件设备是

否符合涉密计算机使用管理要求。

4、 所保密办根据有关要求，指导使用部门对新增接入点计算机进行联网配置及安全设置，并报保密局备案。

第五章 上海船研所涉密信息系统接入点移址

第二十条 确因工作需要，需对上海船研所涉密信息系统接入点进行移址，应履行以下工作程序：

1、 需移动上海船研所涉密信息系统接入点的，应填写《上海船研所涉密信息系统接入点移址申请表》报保密办。

2、 保密办审核是否具备移址的技术条件。

3、 具备相关技术条件，由保密办确认移位新址是否满足涉密设备物理环境安全的要求。

4、 由保密办指导相关单位实施移址工作。

5、 移址工作结束后，保密局再次确认移位新址的物理环境安全，并由保密局组织认定。

6、 认定通过后，正式开通使用。

第六章 上海船研所涉密信息系统计算机更换

第二十一条 使用单位如需更换上海船研所涉密信息系统计算机应履行以下工作程序：

1、 填写《上海船研所涉密信息系统计算机更换申请表》报保密办。

2、 保密办确认上海船研所涉密信息系统接入点物理环境安全

是否符合相关要求、更新的计算机硬件设备是否符合涉及计算机使用管理要求。

3、 对拆除的计算机存储介质（硬盘）进行检查，明确存储过涉密信息的存储介质不得降低密级使用。

4、 保密办根据有关规定的要求，指导更换部门对更新的上海船研所涉密信息系统计算机进行联网配置及安全设置。

5、 更新的涉密计算机，原则上由使用部门自行解决。

第七章 联网规定

第二十二条上海船研所涉密信息系统与国际互联网实行物理隔离，禁止上海船研所涉密信息系统计算机、网络设备与互联网有任何形式的连接。

第二十三条 上海船研所涉密信息系统计算机不得擅自与其他内部工作网络相连。

第八章 涉密存储介质和信息管理

第二十四条 上海船研所涉密信息系统计算机存储涉密信息的存储介质（U 盘、移动硬盘、光盘、软盘等），应按存储信息的最高密级表明密级，并按密级文件进行管理。

第二十五条 涉密 U 盘、涉密移动硬盘、涉密光盘、涉密软盘，应由使用单位统一购置、履行领用手续、登记造册并由专人统一管理。涉密介质应当与非密介质分开保管，涉密介质应放置于铁质密码柜中。禁止使用私人磁介质存储涉密信息。

第二十六条 应建立涉密移动存储设备使用管理制度，禁止在上海船研所涉密信息系统涉密计算机和非涉密计算机之间交叉使用 U 盘、移动硬盘等移动存储设备。

第二十七条 存储过涉密信息的存储介质不得降低密级使用，无保存价值的涉密介质应当报领导批准后销毁，并做好销毁记录。

第二十八条 涉密存储介质维修及数据恢复，必须在市国家保密局定点单位（具有上海船研所涉密信息系统数据恢复资质的单位）进行。禁止将涉密介质交由非定点单位处理。

第二十九条 在上海船研所涉密信息系统计算机上打印输出涉密文件，应按有关规定严格执行，并按相应密级文件进行管理。不得擅自拷贝涉密信息。

第三十条 进入上海船研所涉密信息系统的涉密信息，应当根据国家保密局会同中央、国家机关有关部门制定的《国家秘密及其密级具体范围的规定》，确定并标明密级。

第三十一条 未经本单位领导审批，不得在上海船研所涉密信息系统中擅自发布涉密信息。绝密级及机密级的信息不得进入上海船研所涉密信息系统。

第三十二条 因工作需要，将非上海船研所涉密信息系统上的数据拷贝至上海船研所涉密信息系统计算机，须经领导批准后采取先行查杀病毒、木马，刻录光盘后单向导入方式。

第三十三条 上海船研所涉密信息系统计算机上的非涉密信息未经批准不得拷贝。

第十一章 涉密事件报告查处制度

第三十四条 接入上海船研所涉密信息系统计算机一旦发生泄密事件，应立即报告保密工作部门并及时采取补救措施，切断泄密源头，控制泄密范围。隐瞒不报的将从严处罚。

第三十五条 对违反有关规定，造成泄密事件的行为，将依据《中华人民共和国保守国家秘密法》、《中国人民共和国保守国家秘密法实施办法》进行处理。

第三十六条 对泄密事件负有主要领导责任者，有关部门将根据《中国共产党纪律处分条例》第 138 条的规定，进行处理。

第三十七条 故意或过失泄露国家秘密，泄露国家秘密数量达到立案标准的，检察机关将根据最高人民检察院《关于渎职侵权犯罪案件立案标准的规定》予以立案；情节严重的，根据《刑法》第 398 条的规定，追究当事人刑事责任。

第十二章 附 则

第三十八条对 接入上海船研所涉密信息系统的计算机进行安全配置，并定期更换口令。使用部门不得擅自降低安全配置强度及擅自更改配置项目。

第三十九条 机房内的屏蔽机柜，应确保设备和信息安全。

第四十条 应建立健全上海船研所涉密信息系统、涉密存储介质使用管理制度。

第四十一条 本规定自发布之日起试行

附件 1：

涉密信息系统新增接入点申请表

申请部门：　　填表日期：

<table>
<tr><td rowspan="10">申请部门填写</td><td>本部门现有接入点数量</td><td colspan="2"></td></tr>
<tr><td>拟增加接入点数量</td><td colspan="2"></td></tr>
<tr><td>拟增加接入点物理位置</td><td colspan="2"></td></tr>
<tr><td>拟增加接入点责任人</td><td colspan="2"></td></tr>
<tr><td>拟增接入点计算机情况（品牌、型号、硬件配置、是否有无线互联设备）</td><td colspan="2"></td></tr>
<tr><td>拟新增接入点原因</td><td colspan="2"></td></tr>
<tr><td>填表人：</td><td colspan="2"></td></tr>
<tr><td>联系电话：</td><td>手机：</td><td></td></tr>
<tr><td colspan="3">部门意见：

签字：　　日期：</td></tr>
<tr><td rowspan="2">审核部门填写</td><td>分所领导意见</td><td colspan="2">年　　月　　日</td></tr>
<tr><td>备注</td><td colspan="2"></td></tr>
</table>

附件 2

涉密信息系统接入点移址申请表

申请部门：　　填表日期：

<table>
<tr><td rowspan="9">申请部门填写</td><td colspan="2">现接入点位置</td><td colspan="4"></td></tr>
<tr><td colspan="2">现接入点责任部门及责任人</td><td colspan="4"></td></tr>
<tr><td colspan="2">现接入点 IP 地址</td><td colspan="4"></td></tr>
<tr><td colspan="2">拟移新址具体位置</td><td colspan="4"></td></tr>
<tr><td colspan="2">新址接入点责任部门及责任人</td><td colspan="4"></td></tr>
<tr><td>移址原因</td><td colspan="5"></td></tr>
<tr><td>填表人</td><td></td><td>联系电话</td><td></td><td>手机</td><td></td></tr>
<tr><td colspan="6">部门意见：

签字：　　日期：</td></tr>
<tr><td rowspan="2">审核单位填写</td><td>分所领导意见</td><td colspan="5">年　　月　　日</td></tr>
<tr><td>备注</td><td colspan="5"></td></tr>
</table>

附件 3

涉密信息系统计算机更换申请表

申请部门：　　填表日期：

<table>
<tr><td rowspan="9">申请单位填写</td><td>申请部门</td><td colspan="2"></td><td>填表日期</td><td colspan="2"></td></tr>
<tr><td colspan="3">需更换的接入点计算机情况（品牌、型号、硬件配置）</td><td colspan="3"></td></tr>
<tr><td colspan="3">需更换接入点 IP 地址</td><td colspan="3"></td></tr>
<tr><td colspan="3">更新的计算机情况（品牌、型号、硬件配置、有否无线互联设备）</td><td colspan="3"></td></tr>
<tr><td>更换原因</td><td colspan="5"></td></tr>
<tr><td>填表人</td><td></td><td>联系电话</td><td></td><td>手机</td><td></td></tr>
<tr><td colspan="6">部门意见：

签字：　　日期：</td></tr>
<tr><td rowspan="2">审核部门填写</td><td>分所领导意见</td><td colspan="5">年　　月　　日</td></tr>
<tr><td>备注</td><td colspan="5"></td></tr>
</table>

附件 4

光盘输出登记表

输出日期	姓 名	拷贝内容	介质数量	拷贝趋向	光盘归还日期	光盘编号	备注

附件 6

移动存储介质借用登记表

借用日期	借用人	借用原因（内容）	U 盘编号	归还日期	备注

附件 7

涉密计算机信息导入申请单

申请部门		申请人		申请日期	
导入计算机类型	□台式机 □便携机	导入涉密计算机编号		导入信息密级	□非密 □秘密 □机密
信息导入介质	□光盘 □非涉密 U 盘 □涉密 U 盘 □电子邮件 □互联网 □外部门 介质编号： 其它说明：				
信息内容					
信息用途					
领导审批					
备注	非密信息由部门领导审批，涉密信息由总负责领导审批				

附件 8

涉密会议记录表

会议名称：

<table>
<tr><td>会议主持
单　位</td><td></td><td>会议召开地点</td><td></td></tr>
<tr><td>会议赴止
日　期</td><td colspan="3"></td></tr>
<tr><td>会议内容
涉密等级</td><td colspan="3">绝密　□　　机密　○　　秘密　□</td></tr>
<tr><td>会议资料
发放情况</td><td colspan="2">发出　　份</td><td>收回　　份</td></tr>
<tr><td>与会人员
范　围</td><td colspan="3"></td></tr>
<tr><td rowspan="3">保
密
责
任
分
工</td><td colspan="3">资料管理责任人签字：

年　　月　　日</td></tr>
<tr><td colspan="3">服务人员审查责任人签字：

年　　月　　日</td></tr>
<tr><td colspan="3">主办单位领导签字：

年　　月　　日</td></tr>
<tr><td colspan="4">需要说明的问题：</td></tr>
</table>

附件9

上海船舶运输科学研究所
涉密事项定密审批表

<table>
<tr><td>部门</td><td></td><td>承办人</td><td></td><td>填报日期</td><td></td></tr>
<tr><td>项目名称</td><td colspan="2"></td><td>项目代号</td><td colspan="2"></td><td>密级</td><td></td></tr>
<tr><td colspan="4">涉密事项名称</td><td>拟定密级</td><td>拟 定
保密期限</td><td>控制范围</td></tr>
<tr><td colspan="4"></td><td></td><td></td><td></td></tr>
<tr><td colspan="4"></td><td></td><td></td><td></td></tr>
<tr><td colspan="4"></td><td></td><td></td><td></td></tr>
<tr><td colspan="4"></td><td></td><td></td><td></td></tr>
<tr><td colspan="4"></td><td></td><td></td><td></td></tr>
<tr><td>项目负责人
审核意见</td><td colspan="7">签名： 日期：</td></tr>
<tr><td>部门领导
审核意见</td><td colspan="7">签名： 日期：</td></tr>
<tr><td>所定密责任
人审核意见</td><td colspan="7">签名： 日期：</td></tr>
</table>

上海船研所涉密信息系统涉密文档管理规定

上海船研所涉密信息系统涉密文档是指工作中所有包含涉密内容描述的文档资料。鉴于涉密文档的重要性，特制定以下管理规定：

1、涉密文档记录了系统内的涉密信息，为管理人员、操作人员、用户之间的技术交流提供了交互的媒体，必须重视涉密文档的建立与保存。

2、涉密文档须按密级进行管理，涉密文档分为秘密级文档和一般文档。

秘密级文档是国家秘密级信息的涉密文档。

一般文档是指非涉密文档和规则制度等。

3、上海船研所涉密信息系统中，涉密文档的使用、管理须做到：借阅、复制涉密文档要履行相应的手续，包括申请、审批、登记、归档等必要环节，并明确各环节当事人的责任和义务。

4、对秘密级文档应考虑双份以上的备份，并存放于异地。

5、对报废的涉密文档，要有严格的销毁、监视销毁的措施。

6、应明确执行涉密文档管理制度的责任人。

上海船研所涉密信息系统安全审计管理规定

为了保证上海船研所涉密信息系统安全可靠的运行，防止有意或无意的操作错误，防止和发现计算机犯罪案件，就必须利用对上海船研所涉密信息系统的安全审计方法，对上海船研所涉密信息系统的运行状态进行详尽的审计，并保存审计记录和审计日志，从中发现问题，调整安全策略并以此降低安全风险，特制定以下规定：

1、通过在系统上安装国家保密机关认可的安全审计软件，对系统进行安全性监控，以便及时发现网络存在的安全漏洞或恶意的攻击。安全检测工具可以为安全网络提供对网络和系统攻击的敏感性，从而实现动态和实时的安全控制。

2、在系统日常管理中，要定期对系统日志文件等进行检查，并对用户登录情况进行检查，以尽早发现潜在的非法侵入。

3、上海船研所涉密信息系统计算机中要有详细系统日志，记录每个用户的每次活动（访问时间、地址、数据、程序、设备等）以及系统出错和配置修改等信息。

4、系统安全保密管理人员要定期审查系统日志并做好审查记录，审查周期不得长于一个月，同时保证系统核心日志的定期备份。

上海船研所涉密信息系统病毒防杀管理规定

上海船研所涉密信息系统中须防范各种计算机病毒的侵入，确保整个系统的正常运行，特制定如下规定：

1、在上海船研所涉密信息系统中所有计算机资源都要受到防病毒软件的保护。由系统外部带入的信息介质（包括光盘、软盘、 U 盘等）必须经过专门的病毒防范检查、杀毒后才能在上海船研所涉密信息系统中使用。

2、配备正版网络病毒防杀软件，与有关计算机安全检测部门保持经常性联系，加强病毒防范监管力度。

3、各终端用户安装统一的防病毒软件，要负责防病毒软件的运行，不得关闭。如果用户受到系统中运行的防病毒软件发出的任何警告，则要立即停止使用系统，并且与系统管理员联系。

4、各终端用户不得自行卸掉统一安装的病毒防杀软件，不得自行安装其它类型的病毒防杀软件。

5、系统管理员要负责定期更新病毒库，始终保持防病毒软件为最新版本。各终端用户通过网络自动升级病毒特征码，如果发现自己的防病毒软件没有及时更新，要及时与系统管理员联系。

6、定期汇总、分析病毒发生情况，研究防范对策及采取有效措施。

7、建立定期升级网络病毒库的机制，全网统一查杀及病毒事件的定期检查及汇总制度，查看病毒防杀系统事件日志、记录系统发现病毒情况及统一升级情况，保障网络病毒防杀系统的有效运行。

上海船研所涉密信息系统数据备份与恢复管理规定

上海船研所涉密信息系统中，数据的安全性极为重要，特制定下列规定：

1、要定期由专人承担系统中关键数据的安全备份，系统备份数据由专人管理。

2、对于一些重要的数据及资料，一定要做到定时备份。

3、对于备份资料要妥善保管，并做好自动恢复计划，对于无法自动恢复的，要制定出人工恢复计划。

4、要做好系统应急恢复盘，确保在系统出现异常或崩溃的情况下，能够在最短的时间内进行恢复。

上海船研所涉密信息系统安全与应急事故处理规定

第一章 安全事故处理规定

（一） 此处所指的安全事故包括黑客入侵、病毒入侵、涉密资料泄漏、安全设备故障设备丢失等事故。

（二） 发生安全事故后，当事人和管理员必须马上向部门和保密办报告备案，并记录在案。

（三） 系统管理员和安全管理人员需要定期对进入系统的有害信息及时控制并删除，不得传播。

（四） 发现下列危害计算机信息网络安全的活动的人员，应及时阻断处理并上报保密办备案。

（五） 发现下列危害计算机信息网络安全活动的人员：

1) 未经允许进入计算机信息网络或者使用计算机信息网络资源；

2) 未经允许对计算机信息网络功能进行删除、修改或者增加；

3) 未经允许对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加；

4) 故意制作、传播计算机病毒等破坏性程序的；

5) 其他危害计算机信息网络安全的活动。

（六） 应该做好记录并立即向安全保密管理员和保密办报告，由安全保密日常执行机构进行处理。

（七） 发现病毒后，需要及时断开网络防治病毒扩散和进一步的

损害找出毒源，清除病毒，并对全网进行检查；如果遇到不能处理的病毒，则需要上报主管部门并联系杀毒厂商由专业人员处理。

（八） 发生黑客入侵行为后，应及时断开网络，立刻上报安全保密日常执行机构，检查并保存系统日志，找出系统漏洞，如果不能自行处理，需要同专业厂商联系，由专业人员处理；上报主管部门备案，必要时上报公安机关立案侦查。

（九） 系统设备发生故障，应及时备份数据，并及时请专业人员维修或更换以保证系统正常安全的运行。

（十） 发生数据丢失或损坏等事故后，应及时利用备份系统恢复数据，同时要保存并检查系统日志，找出事故原因；如果不能恢复的重要数据则需要专业人员进行数据恢复工作。

（十一） 发生严重安全事故后，应积极接受并配合公安机关的安全监督、检查，如实向公安机关提供有关安全保护的信息、资料及数据文件，协助公安机关查处该安全事故背后的违法犯罪行为。

第二章 应急事故处理规定

上海船研所涉密信息系统应急反应是建立在技术与管理两个层面上的。技术层面上要解决系统、数据库、应用软件系统和网页的预警与应急反应的问题；管理层面上要解决网络安全管理的问题，从管理上保证安全技术有效的实现，确保用户能及时得到网络预警提示并采取应急措施，恢复被破坏的系统的正常运行。

从技术层面及管理层面综合实现应急事故的体系框架，可如下图所示：

在系统中建立完备的事故应急响应处理流程，包括以下几点：

（1） 系统用户发现系统运行可疑现象后，应立即报告本部门安全保密管理员；

（2） 安全保密管理员应尽可能采取相应措施保护现场，并在一小时内向应急响应小组进行报告，同时报本部门安全主管领导；

（3） 应急响应小组应在二小时内确定现象的性质，并采取措施，收集现场数据，避免严重安全后果的发生，同时，对于安全事故，要上报信息安全领导小组；

（4） 安全保密领导小组根据事故的性质，向相应的主管部门进行报告。

（5） 汇报完毕，将事故定性之后，接到上级指示，对于被破坏的系统和数据，采取可行的措施进行恢复，使之重新正常运行。

上海船研所涉密信息系统三合一系统保密管理制度

总则

（1） 根据《中华人民共和国保守国家秘密法》、国家保密局《计算机信息系统保密管理暂行规定》，制定本规定。

（2） 三合一系统的保密工作贯彻“谁保管，谁负责”的原则，保管者负有直接的保密责任。

（3） 本制度适用于三合一系统的保密管理。

三合一系统购置管理

（4） 三合一系统必须在境内保密制定渠道购买。

（5） 三合一系统须由相关主管部门统一购置，其余部门不得自行购买三合一系统。

三合一系统使用管理

（6） 三合一系统在发放前作好应作对三合一系统的编号、硬件设备、软件和责任人的登记，涉密三合一系统应在保密办备案并进行密级标识，贴标工作。

（7） 如因岗位调动等原因，三合一系统硬件责任人需要变更，必须作好三合一系统责任人变更手续。

（8） 三合一系统中软件的安装，由部门系统管理员负责，由技术部门做相应技术支持。严禁安装任何未经许可的软件、系统。严禁使用来源不明的软盘、光盘等存储介质。

（9） 涉密三合一硬件系统应由专人妥善保管。

（10） 安全保密管理员应做好借用及外携记录的登记保管工作。

三合一系统报废、清理管理

（11） 三合一系统的报废、清理按计算机固定资产管理办法进行管理，内部硬件按照本制度中涉密介质管理有关规定执行。

三合一系统维修管理

（12） 维修管理参见本制度中的《上海船研所涉密信息系统涉密设备管理制度》维修管理。