

# 南京航空航天大学 航空学院 保密自查表/保密自学内容（涉密人员）

（表格更新时间：2019.03.31，制作人：学院保密工作领导小组 张金凤）

受检人	系所	身份	□教职工 □研究生	涉密等级	□一般□重要		
序号	检查内容及要求				结果	问题	整改
<b>（一）重点学习资料：</b>							
1	<ul style="list-style-type: none"> <li>● 《中华人民共和国保守国家秘密法》（2010年10月1日起施行）（见《国防科技工业安全保密“六条规定”解读》（2010.05）附件）；</li> <li>● 《武器装备科研生产单位一级保密资格标准解读》（浅蓝，2017.08）；</li> <li>● 《南航保密工作规章制度汇编》（蓝色，2017.08）；</li> <li>● 《南航涉密人员应知应会及保密考试题库》（绿色，700题，2017.08）；</li> <li>● 《南航信息系统、信息设备和存储设备安全保密策略及操作规程》（橙色，2017.08）；</li> <li>● 《南航国家秘密事项范围细目》（红色，2017.08）；</li> </ul> 如上材料的旧版本作废，尽快返回至院科研办；				□是 □否		
2	熟悉岗位业务中的保密事项，掌握本职岗位的保密职责（《南航保密工作责任制规定》中的保密职责）、涉密人员签订的保密责任书和保密承诺书等内容；				□是 □否		
<b>（二）涉密人员管理要求：</b>							
1	<b>涉密人员申请条件：</b> <ol style="list-style-type: none"> <li>1) 具有中华人民共和国国籍，无境外永久居留权或长期居留许可，且与境外人员（含港澳台）无婚姻关系；</li> <li>2) 拥护《中华人民共和国宪法》，遵纪守法，无违法犯罪记录；</li> <li>3) 作风正派，品行端正，无吸毒、赌博、酗酒等不良嗜好；</li> <li>4) 忠诚可靠，责任心和事业心强；</li> <li>5) 具有涉密岗位要求的工作素质和工作能力；</li> <li>6) 无其他可能影响国家安全利益的倾向；</li> </ol> <b>申请流程：</b> 拟申请/承接/参与涉密项目前，应后至学院科研办接受学院保密教育，领取各类保密学习材料，参加学院保密知识考试（90分及格），通过后填写《南航涉密人员审批表》等材料进行保密审查，签订保密承诺书，参加学校保密教育并通过保密知识考试（80分及格），确定为涉密人员后，方可申请/承接/参与涉密项目； <b>涉密项目较多的项目组可以考虑申请涉密研究生；</b>				□是 □否		
2	<b>保密教育：</b> <ol style="list-style-type: none"> <li>1) 参加学校、学院及上级部门组织的保密法规及保密知识的教育培训，提高保密意识和技能；</li> <li>2) 涉密人员每年接受保密教育时间不少于15学时；</li> <li>3) 因故未参加人员需参加补课；</li> </ol>				□是 □否		
3	<b>系所/项目组保密教育：</b> <ol style="list-style-type: none"> <li>1) 各系所/项目组（含研究生）自行组织开展保密教育活动，学习保密法规及保密知识，提高保密意识和技能；</li> <li>2) 每年至少开展一次，范围、内容、时间、地点自定，填写《南航保密教育培训记录表》交至学院科研办；</li> <li>3) 如需学院现有教育培训资源可至学院科研办借用光盘；</li> </ol>				□是 □否		
4	<b>考核：</b> <ol style="list-style-type: none"> <li>1) 涉密人员逐月考核，根据考核结果发放保密补贴；发放时需提交校内转账支票至学院科研办，重要涉密人员300元/每月，一般涉密人员100元/每月，老师保密津贴必须用横向课题，研究生保密津贴可用纵向课题；不能领取人员需写说明；老师和学生的转账支票需分别开具，标注人名；</li> <li>2) 年终考核填写《南航涉密人员年度考核表》，保密教育学时由学院填写，学时不足的人员参加学院的补课；保密检查次数由学院填写；注意除本人签字外，还需请项目负责人签字；</li> <li>3) 若发现保密违规行为，本月考核不合格，按《南航保密责任考核和奖惩规定》执行；</li> </ol>				□是 □否		
5	<b>复审：</b> 一般涉密人员每5年复审一次，重要涉密人员每3年复审一次，办理变更手续时须进行复审；				□是 □否		

6	<b>出入国（境）管理：</b> 1) 出入境证件（护照、往来港澳通行证、往来台湾通行证）及拥有外籍、境外永久居留权或长期居留许可情况如实上报，包括入密之前获得的； 2) 全部因私出入境证件交人事处统一管理，因公出入境证件交国际合作交流处统一管理； 3) 涉密人员出国（境）（含因公、因私）必须有对应的出国（境）审批表，签订《南航对外科技交流保密承诺书》、《南航因私出国（境）保密承诺书》（正反打印），并接受保密提醒，出国事由应具体准确； 4) 在境外遇到盘问、利诱、威胁或其他异常情况，应及时向驻外使馆报告； 5) 回国7日内上交出入境证件（护照、往来港澳通行证、往来台湾通行证）（因公交国际合作交流处、因私交人事处），并填写《南航出国（境）回访记录表》； 6) 境外机构及个人赠送的服务器、主机、存储阵列及各类移动存储介质需上交上级保密部门检测； 7) 检查时随机抽取个人护照，随机一次使用记录，核查此次出国（境）审批表等材料；	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不涉及		
7	<b>重大事项报告：</b> 如发生失泄密或重大泄密隐患，针对本人利诱、胁迫、渗透、策反行为的，与国（境）外人员通婚、本人、配偶、子女国籍变更或移居国（境）外的，接受国（境）外机构、组织、人员资助的，填写《南航重大事项报告表》；	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不涉及		
8	<b>脱密：</b> 1) 脱密前移交全部的涉密载体和设备，填写《南航脱离涉密岗位审批表》，并签订脱密期保密承诺书，脱密期内严格遵守相关的保密承诺； 2) 一般涉密人员脱密期1-2年，重要涉密人员2-3年； 3) 脱密期内不得擅自出境； 4) 不得到有境外（驻华）机构、组织和外商独资企业工作，不得为境外（驻华）机构、组织及外商独资企业提供劳务、咨询或其他服务； 5) 不得申请外国国籍或者国（境）外永久居留权、长期居留许可； 6) 项目负责人应督促项目组中不再承担涉密项目的涉密人员办理脱密手续，收回其保管的所有涉密载体和设备； 7) 涉密研究生毕业前申请脱密，脱密期1年；原则上只能到各级机关、国防军工企事业单位或者以公有经济为主体的企业就业，学校委托就业单位进行脱密期管理；如需到上述以外单位就业的，应按毕业离校时间提前1年停止涉密工作，并办理脱密手续，在校履行脱密期； 8) 脱密期应遵守涉密人员管理的各项规章制度，对从事涉密工作期间掌握、知悉、管理的国家秘密继续承担相应保密责任；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
(三) 涉密项目管理要求				
1	<b>定密：</b> 1) 做好本项目组内部产生的国家秘密的密级和保密期限的拟定和申请定密工作； 2) 合同/技术协议/任务书/附件等资料封面的密级为文本密级，不是项目密级； 3) 合同/技术协议/任务书/附件等文本签订前务必检查合同保密条款、质量条款、责任条款、知识产权条款、付款条款、售后服务承诺等； 4) 涉密项目定密审批表要明确具体的定密依据和保密要点，知悉范围应明确具体的项目组成员； 5) 严格控制接触和知悉人员的范围； 6) 不得以任何方式泄露国家秘密，不得与无关人员讨论项目的涉密内容； 7) 个别涉密项目下款时会更改主项目负责人，更改后的主项目负责人务必为涉密人员； 8) <b>重点关注：</b> 学科材料、实验室/中心材料等；网站介绍；教师个人介绍；在申报自然科学基金等科研项目时有关本单位、项目组科研基础等情况介绍；各单位、教师个人的年终工作总结报告；教师职称申报材料中科研情况汇报；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
2	<b>归档：</b> 1) 已结题涉密项目及时办理归档，并办理结算/结转手续； 2) 检查时重点检查在研涉密项目全过程闭环管理（申请、评审、签合同、研究、结题、归档等）； 3) 保管好归档证明原件；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
(四) 国家秘密载体（纸质/光盘等）要求： 纸质：秘密级 份，机密级 份，光盘：秘密级 份，机密级 份				
1	<b>专人负责：</b> 项目组应明确专人负责国家秘密载体的收发、传递、归档、保存、移交和销毁等日常	<input type="checkbox"/> 是		

	管理工作;	<input type="checkbox"/> 否		
2	<b>标密、编号:</b> 从外单位带回、购买或自产的国家秘密载体均应进行标密, 并且统一编号;	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
3	<b>闭环管理:</b> 1) 国家秘密载体的收发、刻录、打印、复印、销毁各环节, 均应在《南航科技涉密资料登记本》上进行登记接收/发送; 2) 单位、经办人、时间、份数、页数等信息, 填写完整; 资料名称书写应详细; 不同份数、页数的材料不能合计登记, 不便于核对; 光盘应有唯一性标识的光盘号; 纸质资料不同版本之间应有唯一性标识; 密级标识应写全称; 如未出校, 仅在科研院评审使用, 也需在备注说明, 尤其是打印/复印多份材料, 过一段时间申请销毁, 要说明资料的用途; 为了专家检查时快速找到资料的源头/出处, 建议在登记表备注列增加索引说明; 3) 接收人必须本人签字, 如发送至上级机关, 不方便接收人本人签字的情况才可代签; 4) 纸质发送记录中要依据资料是打印件还是复印件, 填写至打印/复印一列; 5) 依据光盘发送还是拷贝过光盘内容, 填写电子文档复制/发送一列; 6) 每一个流转环节清楚可控, 对尚未办理登记的要进行补办; 7) 可至科研院、机要室、档案馆、印刷厂、学院科研办等核对闭环记录(2012年至今), 可按项目的进展核查闭环记录; 8) 必须由涉密人员办理如上各类手续; 9) 科技涉密资料登记本封面左上角密级为“内部资料”, 右上角为编号, 格式如: 0111-01; 10) 一个项目组可共用一本科技资料交接记录本; 11) 如果同一团队有多本科技资料收发登记, 同一项目资料的收发登到不同登记本上, 不便于核查; 建议: 同一项目资料的收发登记到一本上; 如同一项目资料的收发登到不同老师的登记本上, 应做好标注; 12) 代其他团队办理/收发资料的闭环记录, 建议登到他人的收发登记本上, 否则遗忘后, 双方均不便于核查; 13) 可至学院科研办领取科技资料交接记录本及查询编号; 14) 脱密前交学院科研办归档; 15) 重点检查在研涉密项目申请、评审、签合同、研究、结题、归档等全过程闭环管理, 及各类涉密的学科、实验室/中心的申报、评估、验收等材料; 16) 已结题或验收的涉密项目尽快结题归档; 17) 已作废并不再使用的文件尽快至院科研办办理销毁; 18) 派人发送给上级/甲方资料时, 如不方便携带科技资料收发登记本, 可请对方填写资料交接单;	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
4	<b>借阅:</b> 1) 借阅国家秘密载体, 需经学院领导审批; 2) 借阅后, 及时归还, 禁止向第三方横向传递; 3) 借阅本部门业务以外的国家秘密载体, 须经相应部门的主管领导批准;	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
5	<b>复印:</b> 1) 复印涉密文件资料, 需填写《南航涉密复印受控单》一式两联, 经学院领导审批; 2) 携带《南航涉密复印受控单》第二联、涉密文件资料原件至校印刷厂涉密复印点; 3) 应与印刷厂复印登记本份数一致; 4) 应写清楚用途: 用于复印资料、复印封面; 5) 申请后如未复印, 应返还院科研办; 6) 如携带涉密光盘去印刷厂打印, 应需填写输出审批表; 7) 应由涉密人员到印刷厂去复印; 不能代签字; 8) 由印刷厂复印点人员在复印件每页加盖“此件为复印件、视同原件管理, 严禁复印”章, 在复印件首页右上角加盖复印件发文章, 填写日期、份数及编号, 在《南航涉密复印登记本》上登记, 履行签收手续, 保存第二联; 9) 不得改变其密级、保密期限和知悉范围; 10) 统一编号、登记;	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
6	<b>打印、刻录:</b>			

	<p>1) 打印的页数应为文件 office 软件在页面左下角显示的包括封面、目录、填表说明等的全文页数，不仅是正文的页数，更不能是纸张数；如包含空白页，建议增加备注，写清含几页空白页；</p> <p>2) 打印时登记条形码编号；</p> <p>3) 刻录时要在份数附近写明光盘编号；</p> <p>4) 打印/刻录时要写明材料去处；</p> <p>5) 不能代签字；</p>			
7	<p><b>密码文件柜：</b></p> <p>1) 秘密级和机密级国家秘密载体保管在密码文件柜内；</p> <p>2) 密码文件柜密码设置为 8 位（含）以上；</p> <p>3) 输入密码时如有他人 在场，应用手遮挡；</p>	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
8	<p><b>文件盒：</b></p> <p>1) 国家秘密载体及目录清单应放置在密码文件柜内的标注密级的文件盒内；</p> <p>2) 文件盒可至学院科研办领取；</p> <p>3) 密级标示为“机密★20 年”、“秘密★10 年”、“内部资料 注意保管”；</p> <p>4) 按文件盒内载体的最高密级进行标注；</p>	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
9	<p><b>国家秘密载体目录清单：</b></p> <p>1) 核对个人涉密载体清单及涉密载体的数量，包括资料和光盘，帐物相符；</p> <p>2) 国家秘密载体及目录清单应放置在密码文件柜/保密柜内的标注密级的文件盒内（可来院科研办领取）；</p> <p>3) 登记时间指的是接收时间，而不是表格更新时间；</p> <p>4) 密级标示为“机密★20 年”、“秘密★10 年”、“内部资料 注意保管”；</p> <p>5) 按文件盒内载体的最高密级进行标注；</p> <p>6) 已作废并不再使用的文件尽快至院科研办办理销毁，销毁前必须核查清楚接收记录；</p> <p>7) 目录清单及时更新；</p> <p>8) 每半年提交一份至学院科研办备份；</p>	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
10	<p><b>出校：</b></p> <p>1) 校外发放和传递国家秘密载体，需采用机要通信（校机要室办理）或涉密人员取送方式，不能通过普通邮寄渠道寄运；</p> <p>2) 个人携带国家秘密载体送交、甲方/上级，或通过机要室寄出的环节，均需办理《国家秘密载体出校审批表》；</p> <p>3) 打印资料/刻录光盘至校外汇报后全部带回，也要有出校审批表；</p> <p>4) 表格个人保管备查；</p> <p>5) 秘密级载体学院审批，机密级载体还需校科研院审批；</p> <p>6) 严禁携带国家秘密载体旅游、探亲、访友和出入娱乐场所；</p>	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
11	<p><b>销毁：</b></p> <p>1) 不得擅自销毁国家秘密载体；</p> <p>2) 已作废并不再使用的国家秘密载体应填写《南航国家秘密载体销毁审批表》，经学院领导审批后，携带《南航科技涉密资料登记本》，至学院科研办办理销毁；</p> <p>3) 秘密级载体学院批准，机密级载体还需保密处审查；</p>	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
12	<p><b>个人保密笔记本：</b></p> <p>1) 记录涉密事项使用保密笔记本；</p> <p>2) 入密时发放，确实缺失的可至院科研办签字领取；</p> <p>3) 有编号；</p> <p>4) 个人保管备查；</p> <p>5) 脱密前交学院科研办归档；</p>	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
<b>(五) 密品管理：</b>				
1	<p>1) 密品指通过观察或者测试、分析手段能够获得国家秘密信息的设备或者产品；</p> <p>2) 密品应确定密级，标明密级，并在相关技术文件中注明，建立台账，物帐相符；</p> <p>3) 研制、生产、试验、运输、保存、维修、使用、销毁等过程明确各环节负责人，根据工作需要制定保密方案，并对其采取遮挡或其他保护性措施；</p>	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不 涉及		

	4) 密品的运输应由二人或者以上的专人押运; 在各环节、各岗位的交接影登记签收, 其技术文件不得同其分离, 应一并纳入全过程管理;			
<b>(六) 保密要害部门部位:</b>				
1	1) 涉及要害部门部位的新建、改建工程项目所采取的保密防护措施应当经学校保密处组织的审核, 与工程建设同计划、同设计、同建设、同验收; 2) 安装防入侵警报装置、视频监控系统、电子门禁系统、防盗门窗等技防措施; 3) 配备安全值班人员 24 小时中控室值班; 4) 视频监控存储设备要独立划分区域放置; 5) 设置手机存放柜、密码文件柜; 6) 对于可进出要害部门部位的安全值班、工勤服务人员: 上岗前对其进行保密培训, 对其个人及家庭情况进行审查; 在岗期间进行保密教育; 上岗前填报保密审查表, 签订保密承诺书; 严格控制活动区域和知悉范围; 禁止私自单独出入涉密场所; 离岗前签订保密承诺书; 7) 禁止使用无线移动通信设备(手机、具有无线联网工程的计算机), 禁止带入具有录音、录像、拍照和信息存储等功能的设备(检查录像); 8) 外来人员进入需审批登记, 并专人全程陪同;	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不涉及		
<b>(七) 信息设备——涉密计算机(台式计算机/便携式计算机/涉密数据交换机): 受控号 M-J-_____, <input type="checkbox"/>无此项</b>				
1	<b>信息设备台账分类:</b> ● 服务器、计算机: 服务器、操作终端、台式计算机、便携式计算机、工作站等; ● 网络设备: 交换机、路由器、网关等; ● 外部设备: 打印机、扫描仪、移动光驱、读卡器等; ● 存储设备: 计算机硬盘和固态存储器、移动硬盘、光盘、U 盘、存储卡、记忆棒等; ● 办公自动化设备: 复印机、传真机、多功能一体机、碎纸机、绘图仪等; ● 声像设备: 照相机、摄像机、录音机、录音笔、投影仪等; ● 安全保密产品: 接入控制、单向导入、身份鉴别、访问控制、监控审计、病毒防治、干扰滤波、漏洞扫描等;	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
2	<b>采购:</b> 应在境内采购的国产设备; 购置现货; 建议使用新计算机, 如为旧计算机, 应更换硬盘; 不具有一键恢复功能;	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
3	<b>审批:</b> 应经审批后使用; 因办公室地点调整、责任人调整等原因导致的任何涉密设备信息变更需及时至学院科研办办理变更手续; 物帐相符;	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
4	<b>标贴:</b> 1) 显示器屏幕左上角粘贴警示标识(白底红字: 本计算机为涉密机, 严禁联接互联网!); 2) 机箱正面居中粘贴涉密设备标贴(红色, 含受控号、密级、责任人), 必须打印, 如为手写或不清晰, 尽快报院科研办; 3) 机箱顶端与侧挡板之间粘贴封条(白底红字: 保密封条, 严禁私自开启 受控设备封条), 尽量选择便于识别且不易被意外损坏的位置, 机箱有多个可开启部件时, 应对应粘贴多个封条; 4) 机箱 USB 接口粘贴警告封条(红底白字: 不得接入非授权设备); 5) 如遇之前计算机维修等原因, 封条已破坏的需尽快至院科研办领取新封条粘贴; 6) 部分移动存储设备(如 CF 卡、SD 卡、MS 卡、TF 卡等) 如果无法粘贴标贴或粘贴后影响使用, 可采用不可擦除的标记方式(如激光刻录、不可擦除签字笔等);	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
5	<b>显示器:</b> 1) 不能使用 CRT 显示器, 如必须使用需安装视频干扰器; 2) 不能面对门、窗、走廊等, 不能位于所在建筑物最外围墙壁处, 窗外正面附近无高层建筑; 3) 操作人员离开时应锁定系统或关闭相应的显示器; 4) 仅针对机密级计算机: 安装视频干扰器;	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
6	<b>操作系统:</b> 安装相适应的操作系统及驱动程序;	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
7	<b>补丁:</b> 1) 需在补丁程序发布后 3 个月内安装操作系统补丁、各类应用程序补丁; 2) 部分计算机未升级到 SP3, 请尽快下载升级包升级到 SP3; 3) 系统补丁包下载: window xp sp3 补丁包发布至 2014 年 5 月; window 7 32 位系统补丁包发	<input type="checkbox"/> 是 <input type="checkbox"/> 否		

	<p>布至 2017 年 8 月；window 7 64 位系统补丁包发布至 2017 年 8 月；</p> <p>4) office 软件补丁包：office2003 补丁升级；office2007 补丁升级；</p> <p>5) 下载地址：校信息化处网站/服务资源/系统安全“操作系统及应用软件补丁升级”；</p>			
8	<p><b>应用软件：</b></p> <p>1) 安装的应用软件应在学校批准的《南航涉密计算机软件白名单》内；</p> <p>2) 安装前应进行病毒和恶意代码的查杀；</p> <p>3) 软件白名单可至院科研办查询；</p> <p>4) 安装白名单外软件需履行审批手续；</p>	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
9	<p><b>策略：</b>在安装策略前应使用光盘，不能使用移动存储介质；按学校要求配置安全策略、安装防护软件和安全审计软件系统；不使用时建议关机；</p>	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
10	<p><b>用户策略：</b></p> <p>1) 只有一个合法帐户（名），禁用多余帐户、Guest 帐户；</p> <p>2) 知悉范围不一样的多人共用涉密计算机做好不同用户权限划分，使用各自涉密存储介质处理涉密信息，且涉密信息不得留存计算机本地硬盘上；</p> <p>3) 帐户名使用个性化名称，不应使用默认的 Administrator；</p> <p>4) 登录时不显示上次登录帐户；</p> <p>5) 身份鉴别 5 次失败后，进行登录锁定，锁定时间 30 分钟；</p> <p>6) 方法：点击控制面板/性能和维护/管理工具/计算机管理/本地用户和组/用户：除 Guest 外只有一个管理员用户；点击开始/运行/gpedit.msc/组策略/计算机配置/Windows 设置/安全设置/账户策略/账户锁定策略；</p>	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
11	<p><b>密码策略：</b></p> <p>1) 设置开机密码、系统登陆密码和屏保密码，仅被使用人知悉；</p> <p>2) 密码要求大写字母、小写字母、数字和特殊符号四者中三者及以上混排；</p> <p>3) 不能包含用户的帐户名，不能包含用户姓名中超过两个连续字符的部分；</p> <p>4) 秘密级口令不少于 8 个字符，更换周期不长于一个月，机密级口令不少于 10 个字符，更换周期不长于一周；</p> <p>5) 设置 BIOS 首选启动项为本地硬盘启动，并禁止快速启动选择；</p> <p>6) 去掉“密码永不过期”选项；</p> <p>7) 方法：点击开始/运行/gpedit.msc/组策略/计算机配置/Windows 设置/安全设置/账户策略/账户锁定策略；</p>	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
12	<p><b>杀毒软件：</b></p> <p>1) 瑞星杀毒软件：适用涉密机(含数据交换机)，安装升级：点击下载安装包升级，瑞星软件需先卸载原软件，勾选删除安装目录，并重新启动系统后安装新下载的瑞星安全安装包；</p> <p>2) 下载地址：校信息化处网站/服务资源/系统安全“杀毒软件安装程序、病毒库升级补丁下载（最新版）”；</p> <p>3) 每月进行一次全盘查杀；</p> <p>4) 升级周期不长于 15 天；</p> <p>5) 升级后立即进行全盘查杀病毒；</p> <p>6) 设置为开机查杀；</p> <p>7) 及时清除隔离区和未被删除的病毒，对无法删除的病毒，及时报告信息化处和保密处；</p> <p>8) 查杀日志至少保存三个月；</p> <p>9) 实时防护功能开启；</p> <p>10) 被病毒感染的计算机必须中止信息交换等数据操作，直至病毒清除；</p> <p>11) 如遇节假日或责任人外出，需在节假日或外出前一个工作日和回来后第一个工作日进行病毒库升级和全盘查杀操作；</p> <p>12) 涉密人员可携带涉密优盘至各中转点拷贝最新版杀毒软件升级包进行升级；</p>	<p>升级时间：</p> <p>查杀时间：</p>		
13	<p><b>屏保：</b></p> <p>1) 安装《军工安全保密宣传屏保动画》屏保，可登陆学院网站/保密工作/常用软件进行下载；如屏保无法正常显示，及时报告院科研办；</p> <p>2) 密码设置：右键点击桌面/属性/屏幕保护程序/密码保护，等待时间不超过 5 分钟；</p> <p>3) 恢复登陆时使用密码口令保护；</p>	<input type="checkbox"/> 是 <input type="checkbox"/> 否		

14	<b>配置：</b> 1) 2018年3月之后，涉密计算机要求全部国产产品；信息化处有建议品牌及型号； 1) 使用具有保密资质的红黑隔离电源（电磁泄露防护电源插座）； 2) 红黑电源上不能使用非涉密设备（如：手机）； 3) 可至学院科研办领取，涉密计算机报废时一并上交； 4) 不能连接国际互联网及其它公共信息网； 5) 拆除无线联网功能模块（红外、蓝牙、wifi、无线网卡等）； 6) 禁止使用具有无线功能的外部设备（如手机、无线鼠标、无线键盘、无线网卡、激光笔、无线电话等）；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
15	<b>移动存储介质：</b> 1) 未使用过非涉密移动存储介质； 2) 使用的涉密移动存储介质应经过授权； 3) 低密级计算机不能使用高密级存储介质；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
16	<b>标密：</b> 1) 存储的涉密信息（文档/图表/图形/数据）应有相应密级标识； 2) 在文件首页左上角黑体三号字标注密级标识，如：机密★20年、秘密★10年、内部资料 注意保管； 3) 该文件名及所在各级文件夹名字后面逐层标注[密级标识]，形式如：XXX [秘密★10年]；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
17	<b>存储信息：</b> 1) 存储的涉密信息密级不能高于计算机的密级； 2) 涉密信息数据不存放在系统盘及桌面，关键数据备份； 3) 不得存有超出个人知悉范围的涉密信息（记录或痕迹）； 4) 知悉范围不一样多人共用涉密计算机做好不同用户权限划分，使用各自涉密存储介质处理涉密信息，且涉密信息不得留存计算机本地硬盘上；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
18	<b>维修、变更、报废：</b> 1) 不能擅自拆卸任何硬件设备、重装系统及删除安全日志； 2) 重装操作系统应有相应的审批登记手续； 3) 涉密信息设备维修、变更（主机硬件、密级、责任人、地点、单位、用途、在用状态等）、报废应履行相应的审批登记手续； 4) 报废时应将硬盘、固件、存储介质上交保密处； 5) 如有外单位维修情况，应与外单位维修人员签订维修合同和保密协议，在维修过程中学校运行维护人员和设备责任人全程旁站陪同；其中送外单位维修的，应拆除所有存储涉密信息的硬件和固件，不能拆除的，送至具有涉密数据恢复资质的单位进行维修； 6) 不再使用的涉密计算机硬盘、涉密外部设备的存储芯片等存储硬件和固件，应作涉密载体报废审批；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
19	<b>涉密计算机非涉密信息导入：</b> 1) 使用涉密计算机的“三合一”单项导入装置，申请人填写《南航非涉密信息导入审批登记表》，由学院、部门负责人或项目负责人进行审批； 2) 用于非涉密信息导入的普通U盘必须登记在帐，粘贴受控号并妥善保管；上网机和内部机的U盘不能混用，需要2个登记在账的U盘；或仅有一个连接内部机的在账U盘，将上网机信息导入到内部机，使用内部机的在账U盘； 3) 导入的文件存放于U盘根目录下，每次导入时仅存当次需要导入的信息；同类型文件可打包一个压缩包； 4) 严禁使用非涉密USB接口（绿口）导入涉密信息； 5) 审批同意后，申请人将指定的存有非涉密信息的普通U盘插入“三合一”单项导入装置中通用USB接口（绿口）进行单向导入，计算机自动导入U盘根目录内的文件到指定文件夹，不需要操作； 6) 导入后须对导入信息进行病毒查杀； 7) 相关事项登记在《南航非涉密信息导入审批登记表》上，审批、登记签署完整，一一对应； 8) 导入后将非涉密U盘信息删除；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
20	<b>涉密计算机涉密信息导入流程：</b>	<input type="checkbox"/> 是		

	1) 申请人填写《南航涉密计算机信息导入导出审批表》，由学院领导审批后至导入点（院科研办）； 2) 外部涉密光盘插入涉密中间计算机，核对导入信息与审批是否一致； 3) 对导入信息进行病毒查杀； 4) 涉密U盘连接涉密中间计算机，将光盘内信息直接拷入涉密U盘； 5) 相关事项登记在《南航涉密计算机信息导入导出登记表》上，签收手续完整，一一对应； 6) 外部涉密光盘留存时间超过6个月后，定期销毁；	<input type="checkbox"/> 否		
21	<b>涉密计算机涉密信息导出（打印/刻录）流程：</b> 1) 申请人填写《南航涉密计算机信息导入导出审批表》，由学院领导审批后，携带《南航科技涉密资料登记本》至导出点（院科研办、011、0162）； 2) 涉密U盘连接信息导出计算机，核对导出信息与审批是否一致； 3) 刻录/打印前，应对涉密U盘进行病毒查杀； 4) 相关事项登记在《南航涉密计算机信息导出登记表》/《南航涉密打印机打印登记本》上，签收手续完整，一一对应； 5) 本地硬盘内不能存储涉密文件； 6) 方法：搜索所有硬盘的*.doc、*.xls、*.ppt等文件，逐一打开进行内容检查；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
22	<b>涉密便携式计算机：</b> 1) 拆除无线联网功能硬件模块、摄像头、蓝牙、红外； 2) 未在本机硬盘存储过任何国家秘密信息； 3) 不使用时存放在密码文件柜/保密柜中； 4) 外出前应进行审批，机密级以上还需校科研院审批； 5) 外出前由保密员对便携式计算机及配备的介质进行检查； 6) 外出过程中涉密笔记本由专人妥善保管，不离开控制范围，不带入经营性场所； 7) 借用时同时借用了红黑电源； 8) 使用期间填写使用登记表（使用人、开关机时间、使用地点、使用原因、信息导入导出方式及编号、信息交换情况、信息去向、连接投影仪等）； 9) 外出时，便携式计算机与配备的介质分别保存在不同的控制权限下； 10) 返回后，便携式计算机及配备的介质应及时交还学院科研办；保密员需及时进行检查，清除存储的涉密信息，并在检查表上签字确认； 11) 申请打开光驱临时开放策略的，返回后需及时送交信息化处关闭光驱等临时开放策略； 12) 如至上级汇报工作，由主办单位提供涉密投影仪； 13) 如校内汇报工作，还需同时借用科研院/学院的涉密投影仪，并填写了《涉密投影仪使用记录》；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
<b>（八）信息设备——涉密打印机要求</b> <span style="float: right;">受控号：M-D-____-____，<input type="checkbox"/>无此项</span>				
1	1) 采购：应为在境内采购的国产设备；购置现货；统一编号；建立台账； 2) 标贴：正面居中粘贴涉密设备标贴（红色，含受控号、密级、责任人）； 3) 配置：不能联接互联网等公共信息网络及非涉密不联网计算机或信息系统；不带读卡器、存储功能、无线联网功能模块（红外、蓝牙、wifi等）及网络功能；不能使用一体机；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
<b>（九）信息设备——涉密移动存储介质要求</b> <span style="float: right;">受控号：M-U-0100-____，<input type="checkbox"/>无此项</span>				
1	由学校统一采购、编号、登记、发放、销毁；其中涉密移动硬盘及其他涉密移动存储介质（如涉密相机卡）需履行审批登记手续；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
2	正面居中粘贴涉密设备标贴（红色，含受控号、密级、责任人）；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
3	台帐清楚，型号、序列号准确登记；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
4	严禁连接国际互联网、其他公共信息网或内部非涉密网络；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
5	首次使用时格式化一次后，之后不建议进行格式化；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
6	由专人负责管理，不使用时保存于密码文件柜/保密柜中；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		



7	存储的涉密信息密级不能高于介质本身的密级；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
8	不得存有超出个人知悉范围的涉密信息；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
9	<b>标密：</b> 1) 存储的涉密信息（文档/图表/图形/数据）应有相应密级标识； 2) 在文件首页左上角黑体三号字标注密级标识，如：机密★20年、秘密★10年、内部资料 注意保管； 3) 该文件名及所在各级文件夹名字后面逐层标注[密级标识]，形式如：XXX [秘密★10年]；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
10	携带外出前，彻底清除与当次工作无关的涉密信息；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		

**(十) 涉密场所（存放涉密计算机的办公场所）：**

1	非涉密计算机机箱与涉密计算机机箱、红黑电源、红信号线间隔 $\geq 1$ 米；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
2	涉密设备存放场所应相对独立，并采取有效的安全防盗措施，无关人员不能接触涉密设备及介质，做到防盗、防毁、防火、防潮；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
3	涉密场所严禁使用具有无线功能的通信设备（如无绳电话、无线麦克风、子母电话、对讲机等），不安装无线信号发射装置；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
4	涉密场所内的非涉密计算机或互联网计算机禁止安装、配备和使用摄像头、麦克风等视频、音频输入设备；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
5	涉密场所内的非涉密计算机或互联网计算机禁止启用视频、音频设备（摄像头覆盖、声卡禁用）；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
6	涉密计算机不应与非涉密设备放置于同一金属平台；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
7	涉密场所内不应有非涉密人员办公；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
8	二层楼以下或必要楼层应配有防盗窗；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
9	<b>资料保管：</b> 1) 文件资料分类放置，摆放整齐； 2) 资料、文件、光盘、u盘、移动硬盘等尽量清桌锁柜； 3) 检查办公场所的不带锁的普通柜子（特别是玻璃门柜子），不要存放内部/敏感资料； 4) 内部资料或含敏感信息资料必须保管在带锁不可视的文件柜内或密码文件柜/保密柜内； 5) 每个项目组应配备碎纸机，用于销毁已作废并不再使用的内部资料/敏感信息；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
10	重要涉密场所：不得将手机带入，或手机放入手机屏蔽柜内，或开启手机信号干扰设备；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		

**(十一) 信息设备—非涉密计算机（台式计算机、便携式计算机）受控号：F-J- - ， F-BJ- - ， 无此项**

1	<b>非涉密设备登记：</b> 1) 范围如下：计算机类：台式计算机、便携式计算机、服务器、工作站； 办公自动化设备类：打印机、传真机、复印机、扫描仪、一体机、碎纸机、照相机、摄像机、投影仪； 移动存储介质类：U盘、移动硬盘、相机存储卡、录音笔等； 2) 登记流程：在办理国资处固定资产前，填写《南航非涉密计算机及办公自动化设备登记表》，由各系所保密员/设备管理员发放设备受控号，并发放相应设备标签； 3) 信息更新：由于设备损坏、报废、位置移动、使用人变更等原因产生的任何设备信息变更应及时至各系所保密员/设备管理员更新台账；各系所每3个月向学院科研办提交一次最新台账； 4) 未经登记的计算机及各类存储介质等办公设备不得带入办公场所； 5) 研究生自带计算机应至各系所保密员/设备管理员登记后，方可带入办公场所； 6) 不得将计算机/存储介质/IP地址让他人随意使用，因此发生的保密问题责任自负； 7) 物帐一致；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
---	--	--	--	--

2	机箱正面居中粘贴非涉密设备标贴（蓝色，含受控号、责任人（含学生及导师姓名））；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
3	显示器屏幕左上角粘贴警示标识（上网机：白底黑字，内部机：白底蓝字）；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
4	台帐清楚，硬盘型号、序列号准确登记（使用 IDE 软件查询，可登陆学院网站/保密工作/常用软件进行下载，台帐可至各系所保密员/设备管理员处查询）；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
5	设置系统登陆密码（点击开始/控制面板/用户帐户/管理员/创建密码）；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
6	安装正版杀毒软件及防火墙（建议国产），及时升级（周期不长于 1 个月），并定期查杀病毒、漏洞扫描并修补等（周期不长于 1 个月，点击软件杀毒日志查询）；	升级： 查杀：		
7	安装《军工安全保密宣传屏保动画》屏保（可登陆学院网站/保密工作/常用软件进行下载；密码设置：右键点击桌面/属性/屏幕保护程序/密码保护，等待时间不超过 15 分钟，恢复登陆时使用密码口令保护）；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
8	1) <b>上网机</b> ：不能存储处理涉密信息/内部/敏感信息； 2) <b>内部机</b> ：不能存储处理涉密信息； 3) 不得存有与涉密计算机内涉密文件主要内容相一致的信息（检查中该类情况判定为非密存密）； 4) 敏感材料务必放在内部计算机内； 5) 航空基金、商业秘密、学科材料、实验室等建议书、评估、验收等材料建议存放在内部机； 6) 搜索所有硬盘及电子信箱的*.doc、*.xls、*.ppt 等文件，逐一打开进行内容检查，如发现立即断网、清理，格式化硬盘，并且重装系统；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
9	可将存储的重要文件进行加密（右键点击文件/添加到压缩文件/高级/设置密码/输入密码/再次输入密码确认/加密文件名/确定）；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
10	1) 不能使用过涉密移动存储介质； 2) 不能使用过涉密办公自动化设备；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
11	<b>上网机</b> ：使用的介质可控，并最小化，USB 记录不超过 10 个（点击开始/运行/regedit/HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Enum/USBSTOR 查询介质使用记录）；	USB 个数：		
12	<b>内部机</b> ： 不能连接过互联网（检查联网痕迹）； 上网计算机与内部机之间尽量采取光盘进行传输； 不建议使用任何移动存储介质，确因工作需要的，应最多配备 1 个 U 盘及 1 个移动硬盘，专门用于内部机之间的信息交换、数据备份，该 U 盘/移动硬盘密级为内部，严禁在上网机上交叉使用；	USB 记录 个数：		
13	不能带有无线联网功能模块（红外、蓝牙、wifi、无线网卡等）；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
14	不能使用具有无线功能的外部设备（无线路由器、无线鼠标、无线键盘、无线电话等）；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
	<b>电子信箱</b> ： 1) 不得存有与涉密计算机内涉密文件主要内容相一致的信息（检查中该类情况判定为非密存密）； 2) 不得存有敏感信息； 3) 邮箱密码设置要求：密码长度不少于 8 位，且含有数字、小写字母、大写字母、特殊符号四种中的三种以上混排； 4) 建议：电子信箱经常进行清理，周期不长于一年；	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
15	建议：经常进行重装系统，周期不长于一年（点击开始/运行/cmd/systeminfo/初始安装时间进行查询，如无法查询时可点击 C: /Windows 查看系统文件生成时间）；	系统 安装 时间：		
16	<b>家用计算机</b> ：禁止使用家用计算机、家用移动存储介质处理、存储涉密信息；			
(十二) 信息设备—非涉密移动存储介质（U 盘、移动硬盘、手机卡、相机存储卡等）受控号：F-U- - ， <input type="checkbox"/> 无此				

项			
1	粘贴非涉密设备标贴（蓝色，含受控号、责任人（含学生及导师姓名））；	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
2	1) 台帐清楚，硬盘型号、序列号准确登记； 2) 存储设备一般不超过 3 个；	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
3	未存储、处理涉密/内部/敏感信息；	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
4	仅存储与当次工作相关的信息，并且使用一次格式化一次； 与他人之间的文件交换（公开信息）尽量通过电子邮件/网络；	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
5	未连接涉密计算机或信息系统；	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
6	不将未登记编号的非涉密存储介质带到办公场所；	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
7	<b>非涉密光盘：</b> 可不建立台账，但是操作系统安装、软件安装、病毒库升级、清除工具、检查工具等光盘应当上账；	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
8	<b>手机：</b> 1) 尽量不用高端智能手机； 2) 严禁使用手机等无线通讯设备谈论、存储、传输国家秘密； 3) 不得连接涉密信息设备； 4) 不得在涉密公务活动中开启和使用位置服务功能； 5) 不得使用境外机构、人员赠送的手机； 6) 不得将手机带入重要涉密场所，或手机放入手机屏蔽柜内，或开启手机信号干扰设备； 7) 手机如连接计算机，只能连接上网机； 8) 手机卡视同 U 盘管理；	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
<b>（十三）新闻宣传保密管理：</b>			
1	<b>涉及军工科研生产的宣传报道、接收采访等：</b> 应填写《南航宣传报道保密审批表》，经学院、科研院审查后，宣传部审批，不得涉及国家秘密；	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
2	<b>涉及军工科研生产的报送材料：</b> 应填写《南航报送材料审批表》；	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
3	<b>论文/论著：</b> 1) 公开发表著作和论文都应进行保密审查，不得涉及国家秘密； 2) 研究生导师负责对学生发表的论文及学位论文进行保密审查； 3) 发表前填写《南航公开发表著作或论文审批表》，携带被审查著作/论文至学院科研办审核后，至校保密处办理《南航著作或论文非涉密证明》；	<input type="checkbox"/> 是 <input type="checkbox"/> 否	
4	<b>涉密展览、涉密参观：</b> 1) 应填写《南航涉密展览和涉密参观审批表》进行审批； 2) 选择易于控制和采取保密防反措施的场所进行，专人负责，制定专项安全保密方案； 3) 禁止照相、摄像、记录，禁止携带照相、摄像工程的设备进入； 4) 明确人员范围，做好人员审查登记；	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不涉及	
<b>（十四）涉密会议：</b>			
1	1) 应按照涉及国家秘密的最高密级确定会议密级； 2) 在具备安全保密条件的场所召开，必要时对会议场所采取技术安全保密检查措施； 3) 提前 3 至 7 天填写《南航涉密会议审批表》，指定专人负责保密管理工作，进行全过程管理； 4) 明确参会人员名单，进行身份登记确认； 5) 涉密载体编号后发放、回收，指定专人负责记录； 6) 禁止使用无线话筒； 7) 禁止带入手机、拍摄、录音功能设备，并开启手机信号干扰设备； 8) 发放载体涉及机密级以上国家秘密信息，且参会人员达到 50 人以上，或参会人员达到 100 人以上的秘密级会议，应制定保密工作方案；	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不涉及	
<b>（十五）科研协作配套：</b>			

1	1) 涉密项目的科研协作配套合同的密级应尽量解密成公开或内部; 2) 如无法解密, 外协合同承担方需通过相应级别的武器装备科研生产单位保密资格审查认证; 3) 外协合同应明确文本及项目密级, 明确保密条款或签订保密协议; 4) 不得向外协单位或人员提供必需的技术要求以外的涉密信息;	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不 涉及		
<b>(十六) 涉外活动管理:</b>				
1	<b>接待境外人员来访:</b> 应填写《南航涉外活动审批表》; 对来访人员进行身份确认; 境外人员不得进入存放有涉密设备、资料的办公室及保密要害部门部位等涉密场所;	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
2	<b>涉密人员参加涉外活动:</b> 在国内参加涉外活动或出国(境)参加涉外活动, 签订《南航涉密人员对外科技交流保密承诺书》;	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
3	<b>国际会议:</b> 1) 填写《南航涉外活动审批表》; 2) 填写《南航涉外活动安全保密教育记录》(涵盖参加国际会议的涉密人员); 3) 参会的涉密人员需填写《南航对外科技交流保密承诺书》; 4) 参加国际会议的中外来访人员需登记(单位、姓名、职称、地点、国籍、到达时间、离开时间等);	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
<b>(十七) 外场试验:</b>				
1	1) 应制定保密工作方案, 制定专人负责试验现场的保密管理工作, 应对试验各环节进行保密管理, 并保留过程记录; 2) 选择易于控制、便于采取保密防范措施的场所进行; 3) 参试人员进入现场前应进行保密教育, 遵守现场的保密管理规定; 4) 涉密载体和密品应采取防护措施; 5) 现场苏剧交换影当采取技术措施;	<input type="checkbox"/> 是 <input type="checkbox"/> 否 <input type="checkbox"/> 不 涉及		
<b>(十八) 保密监督检查:</b>				
1	<b>系所保密检查表:</b> 各系所每月开展保密检查, 并填写《航空宇航学院 系所保密工作检查记录表》交至学院科研办;	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
2	<b>保密检查:</b> 定期组织保密检查, 及时发现泄密隐患, 并采取有效的整改措施, 发生泄密事件要及时向学院以及学校保密管理部门报告, 积极协助、配合有关部门的查处工作; <b>检查要求:</b> 项目组负责人负责项目组成员的保密检查, 研究生导师负责本人所带研究生的保密检查, 可安排老师或研究生协助检查, 但计算机内的文件是否为涉密或内部信息最终由项目负责人/研究生导师进行界定; 每个月抽查计算机数量不少于 2 台套, 存储介质不少于 5 只; 一年内所有本人项目组成员/所带研究生的计算机和存储介质被检查次数不少于 1 次;	<input type="checkbox"/> 是 <input type="checkbox"/> 否		
<b>其他问题</b>				
受检人签字: _____ 检查人签字: _____ 时间: 201____. _____. ____ 地点: _____				

**海恩法则:** 每一起严重事故的背后, 必然有 29 次轻微事故和 300 起未遂先兆以及 1000 起事故隐患。

**墨菲定律:** 只要存在发生事故的原因, 事故就一定会发生, 而且不管其可能性多么小, 但总会发生, 并造成最大可能的损失。