南京航空航天大学 航空学院 保密自查表/保密自学内容（非涉密人员）

（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		单位		身份	□教职工 □博士生 □硕士生 □其 他

序号	检查内容及要求	检查结果	问题	整改
保密管理要求				
1	非涉密设备登记： **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； **登记流程：**在办理国资处固定资产前，填写《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； **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/设备管理员更新台帐；各系所每 3 个月向学院科研办提交一次最新台账；	□是□否		
2	未纳入学校固定资产的信息设备不得带入办公场所；	□是□否		
3	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；	□是□否 □不涉及		
4	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； 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； 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》；	□是□否		
5	参加学校、学院及上级部门组织的各类保密法规及保密知识的教育培训，提高保密意识和技能；	□是□否		
6	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； 检查要求:课题组负责人负责课题组成员的保密检查，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课题组负责人/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；一年内所有本人所带研究生的计算机和存储介质被检查次数不少于 1 次；	□是□否		
7	不得处理涉密项目，不得进入涉密场所，不得存储、处理涉密信息，不得持有国家秘密载体，不能向涉密人员打听涉密项目内容；不能办理涉密计算机的信息输入、涉密载体的收发、刻录、打印、复印、销毁等环节；	□是□否		
8	**资料保管：** 1．文件资料分类放置，摆放整齐； 2．资料、文件、光盘等尽量清桌锁柜； 3．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； 4．每个课题组应配备碎纸机，用于销毁已作废并不再使用的内部资料/敏感信息； 5.办公场所保持环境整洁；	□是□否		
9	**涉密人员申请条件：** 1）具有中华人民共和国国籍，在中华人民共和国境内居住，且与境外人员（含港澳台）无婚姻关系； 2）拥护《中华人民共和国宪法》，遵纪守法，无违法犯罪记录，未曾受过刑事处罚； 3）作风正派，品行端正，无吸毒、赌博、酗酒等不良嗜好； 4）忠诚可靠，责任心和事业心强； 5）具有涉密岗位要求的工作素质和工作能力； 6）无其他可能影响国家安全利益的倾向； 7）无严重违反保密规定被调离涉密岗位的情况； 8）愿意遵守保密规章制度； **申请流程：**拟申请/承接/参与涉密项目前，应先至学院科研办接受学院保密教育，领	-		

	取各类保密学习材料，填写《涉密人员审批表》等材料进行保密审查，签订保密承诺书，参加学校保密知识考试，通过后确定为涉密人员，方可申请/承接/参与涉密项目；**涉密项目较多的课题组可以考虑申请涉密研究生；**			
非涉密计算机（含台式计算机、便携式计算机）受控号：F-J-　　-　　，F-BJ-　　-　　，□无此项				
1	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））；	□是□否		
2	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）；	□是□否		
3	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）；	□是□否		
4	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）；	□是□否		
5	安装正版杀毒软件及防火墙，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）；	升级时间： 最近查杀时间：		
6	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）；	□是□否		
7	上网机：不能存储处理涉密信息/内部/敏感信息； 内部机：不能存储处理涉密信息； （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）；	□是□否		
8	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）；	□是□否 □不涉及		
9	不能使用过涉密移动存储介质；	□是□否		
10	不能使用过涉密办公自动化设备；	□是□否		
11	上网机：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 记录个数：		
12	内部机：与上网计算机之间严禁交叉使用移动存储介质，必须采取光盘进行传输； 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）；	□是□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）；	□是□否		
15	建议：电子信箱经常进行清理，周期不长于一年；	-		
16	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：		
17	建议：配备台式内部机（不上网非涉密台式计算机）；	-		
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-　　-　　，□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））；	□是□否		
2	台帐清楚，硬盘型号、序列号准确登记；	□是□否		
3	未存储、处理涉密/内部/敏感信息（搜索所有*.doc、*.xls、*.ppt 等文件，逐一打开进行内容检查，如发现立即清理，进行擦除及格式化）；	□是□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；	□是□否		
5	未连接涉密计算机或信息系统；	□是□否		
6	手机如连接计算机，只能连接上网机； 手机卡视同 U 盘管理；	□是□否 □不涉及		
7	不将未登记编号的非涉密存储介质带到办公场所；	□是□否		
8	存储设备一般不超过 3 个；	□是□否		
其他问题				

受检人签字：　　检查人签字：　　时间：201　.　.　　地点：