中共池州学院委员会办公室文件

党办字〔2014〕6号

关于印发池州学院涉密和非涉密计算机保密管理制度等八项制度的通知

各部门、各单位:

为进一步加强信息化条件下的保密工作，杜绝泄密隐患，确保国家和学校秘密的安全，促进网络信息系统安全应用、高效运行，根据《中华人民共和国保守国家秘密法》和国家保密局《计算机信息系统保密管理暂行规定》、《计算机信息系统国际互联网保密管理规定》要求，结合我校实际，特制定《池州学院涉密和非涉密计算机保密管理制度》等八项规章制度，现印发给你们，请认真贯彻执行。

特此通知

附件:

1. 池州学院涉密和非涉密计算机保密管理制度
2. 池州学院涉密和非涉密移动存储介质保密管理制度
3. 池州学院涉密网络安全保密管理制度

4. 池州学院非涉密网络安全保密管理制度

5. 池州学院涉密计算机维修更换报废保密管理制度

6. 池州学院涉密载体销毁管理制度

7. 池州学院在公共信息网络上发布信息保密管理制度

8. 池州学院公文传输网络保密管理制度

中共池州学院委员会办公室

2014 年 12 月 16 日

附件 1:

池州学院涉密和非涉密计算机保密管理制度

为进一步加强我校涉密和非涉密计算机保密管理工作，杜绝泄密隐患，确保国家秘密的安全，促进网络信息系统安全应用、高效运行，根据《中华人民共和国保守国家秘密法》，结合我校实际，特制定本制度。

第一条　现代教育技术中心负责全校计算机网络的统一建设和管理，维护网络正常运转，各部门、各单位未经批准不得擅自在校系统网络上安装其他设备。

第二条　涉密计算机严禁直接或间接接入国际互联网（外网）等公共信息网络。非涉密计算机严禁直接或间接接入政务内网。

第三条　涉密计算机主要用于处理涉密业务，不得处理国家秘密信息。非涉密计算机严禁存储、处理、传递和转载国家秘密信息。涉密计算机必须与国际互联网（外网）实施物理隔离。

第四条　坚持“谁主管谁负责、谁运行谁负责、谁使用谁负责”的原则，加强对计算机使用人员的保密教育和管理，提高计算机使用人员的保密观念，增强防范意识，自觉执行有关规定。

第五条　未经部门或单位领导批准和授权，个人使用的计算机不得交由非本岗位工作人员操作。

第六条　不得使用移动存储设备在涉密和非涉密计算机间复制数据。确需复制的，应当利用中间计算机进行转存处理，并采取严格的保密措施，防止泄密。

第七条　国家秘密信息输出实行严格的登记、审批手续，特别是对国家秘密信息输出的范围、数量和介质要有明确的记载，确保国家秘密信息可控。

第八条　不得安装、运行、使用与工作无关的软件。

第九条　使用电子邮件进行网上信息交流，应当遵守国家有关

保密规定，不得利用电子邮件传递、转发或抄送国家秘密信息。

第十条　为防止病毒造成严重后果，对外来移动存储介质、软件要严格管理，原则上不允许外来移动存储介质、软件在本单位计算机上使用。确因工作需要使用的，事先须进行防（杀）毒处理，证实无病毒感染后，方可使用。

第十一条　接入网络的计算机严禁将计算机设定为网络共享，严禁将机内文件设定为网络共享文件。

第十二条　为防止黑客攻击和网络病毒的侵袭，接入网络的计算机一律安装杀毒软件，并要定时对杀毒软件进行升级。

第十三条　涉及国家秘密信息的计算机设备出现故障，应送至市保密局审查合格的定点单位进行维修，学校保密委员会派人员在现场负责监督，保证存储的国家和学校秘密信息不被泄露。

第十四条　涉密计算机不再继续使用时，须经单位领导批准，并在履行清点、登记手续，进行技术处理后将硬盘及时销毁，一律不得进行捐赠或当作废品出售。

第十五条　各部门、各单位发现计算机系统泄密后，应及时向学校保密委员会报告，并采取补救措施。

第十六条　涉密计算机信息在打印输出时，打印出的文件应当按照相应密级文件管理，打印过程中产生的残、次、废页应当及时销毁。

第十七条　对不按规定管理和使用涉密计算机，造成泄密事件的，依法依规追究责任，构成犯罪的移送司法机关处理。

第十八条　本制度由学校保密委员会办公室负责解释。

附件 2:

池州学院涉密和非涉密移动存储介质保密管理制度

为进一步加强我校涉密和非涉密移动存储介质保密管理工作，杜绝泄密隐患，确保国家秘密的安全，根据《中华人民共和国保守国家秘密法》，结合我校实际，特制定本制度。

第一条　本规定所称移动存储介质，是指移动硬盘、软盘、优盘、光盘、磁带、存储卡及其他具有存储功能的各类介质。

第二条　校保密办负有建立健全使用、复制、转送、携带、移交、保管、销毁等制度以及对各部门、各单位执行本制度的监督、检查职责。校保密委员会界定涉密与非涉密移动存储介质及涉密笔记本电脑，并由校保密办登记造册。

第三条　各部门、各单位须指定专人负责涉密笔记本电脑和涉密移动存储介质的日常管理工作。涉密笔记本电脑、涉密移动存储介质必须妥善保存，日常使用由使用人员保管，暂停使用的交由指定的专人保管。

第四条　涉密笔记本电脑、涉密移动存储介质只能在本单位内使用，严禁在互联网外网上使用。确因工作需要携带涉密笔记本电脑、涉密移动存储介质外出，须报保密办批准，并履行相关手续和采取严格的保密措施。严禁将涉密笔记本电脑、涉密移动存储介质借给外单位使用。

第五条　非涉密笔记本电脑、移动存储介质不能与涉密笔记本电脑、移动存储介质相混用，严禁将私人笔记本电脑、移动存储介质带入本单位内使用。

第六条　涉密笔记本电脑、移动存储介质需要维修时，必须由市保密局审查合格的定点单位进行维修,并将废旧的存储介质收回。涉密移动存储介质在报废前，应进行信息清除处理。

第七条　涉密笔记本电脑硬盘、涉密移动存储介质的销毁，须

经校保密委员会批准，并送交市国家保密局统一销毁，各部门、各单位不得擅自销毁。禁止将涉密移动存储介质作为废品出售。

第八条　对不按规定管理和使用涉密笔记本电脑和涉密移动存储介质造成泄密事件的，依法依规追究责任。

第九条　本制度由学校保密委员会办公室负责解释。

附件 3:

池州学院涉密网络安全保密管理制度

为进一步加强我校计算机信息保密管理工作，杜绝泄密隐患，确保国家秘密的安全，根据《中华人民共和国保守国家秘密法》,结合我校实际，特制定本制度。

第一条　本规定所称的涉密计算机及涉密网络是指处理、存储和传输涉密信息的单机、笔记本电脑、涉密信息系统及涉密网络等。

第二条　校保密委员会对各部门、各单位执行本规定负有指导、监督、检查职责。各部门、各单位主要负责人对部门、单位执行本规定情况负有指导、监督、检查职责。

第三条　涉密计算机投入使用前，须进行必要的安全检查，不允许进行各种形式的有线及无线的网络连接，不允许使用无线功能的键盘鼠标进行操作。

第四条　涉密计算机应为专人专用,用户应定期修改登录密码,登陆密码必须由数字、字符和特殊字符组成。秘密级计算机设置的密码长度不能少于 8 个字符，密码更换周期不得多于 30 天；机密级计算机设置的密码长度不得少于 10 个字符,密码更换周期不得超过 7 天；涉密计算机需要分别设置 BIOS、操作系统开机登录和屏幕保护三个密码。秘密级计算机设置的用户密码由使用人自行保存，严禁将自用密码转告他人，因工作需要确需转告，应请示校保密委员会同意；机密级计算机设置的用户密码须登记造册，并将密码本存放于保密柜内，由所在部门和单位负责人管理。

第五条　涉密人员因工作变化、调动等原因需要开始或停止使用涉密计算机及涉密网络的，应报校保密办备案登记，同时提交书面申请由校保密委员会主任批准后再由网络管理人员开通或关闭相应权限。

第六条　涉密计算机及涉密网络所在的场所，必须采取必要的安全技术防护措施，并指定专人进行日常管理，严禁无关人员进入

该场所。

第七条　涉密计算机及涉密网络设备需要维修时，须到市保密局审查合格的定点单位进行维修。涉密计算机等设备送修前须将涉密存储部件拆除并妥善保管。涉密存储部件出现故障，如不能保证安全保密，必须按涉密载体予以销毁。

第八条　禁止将涉密计算机转为非涉密环境使用，禁止进行公益捐赠或销售。

第九条　报废、销毁涉密设备应当严格履行审批、清点、登记手续，送至市保密局审查合格的定点单位进行销毁，各部门、各单位不得擅自销毁涉密设备。

第十条　管理人员违反本规定，情节较轻的，应责令改正，给予批评教育；情节严重，造成泄露机密的，按照有关保密规定给予责任人党纪政纪处分；构成犯罪的，移交司法机关依法追究刑事责任。

第十一条　本制度由学校保密委员会办公室负责解释。

附件 4:

池州学院非涉密网络安全保密管理制度

为进一步加强我校计算机信息保密管理工作，杜绝泄密隐患，确保国家秘密的安全，根据《中华人民共和国保守国家秘密法》,结合我校实际，特制定本制度。

第一条　计算机操作人员必须遵守国家有关法律、法规及学校制定的各项规章制度，严格执行安全保密规定，任何人不得利用计算机从事违法活动。

第二条　网络系统由现代教育技术中心负责运行、维护与管理，各部门、各单位不得私自连接任何网络，不得损坏、拆卸、移动和侵占网络设施和线路。

第三条　除现代教育技术中心外，其他部门、单位不得以任何方式登录进入局域网节点、服务器等设备进行修改、设置、删除等操作。

第四条　各部门、各单位必须严格使用由现代教育技术中心按计算机使用人分配的 IP 地址,现代教育技术中心对入网计算机进行登记、备案。严禁私自修改 IP 地址等网络系统配置。

第五条　具有互联网访问权限的计算机访问互联网及其他网络时，严禁浏览、下载、传播、发布违法违规信息。严禁接收来历不明的电子邮件。

第六条　计算机操作人员未经领导批准，不得对外提供内部信息和资料以及用户名、口令等内容。

第七条　网络设备必须安装防病毒工具，并具有漏洞扫描和入侵防护功能，以进行实时监控，定期检测。

第八条　计算机操作人员对计算机系统要经常检查,防止漏洞。严禁通过电子邮箱、QQ 等网上传递涉密文件，磁盘、光盘、U 盘等存贮介质要由相关责任人编号建档，严格保管。除需存档和必须保

留的副本外，计算机系统内产生的文档应及时删除，在处理过程中产生的样品等必须销毁。

第九条　对重要数据要定期备份，定期复制副本以防止因存储工具损坏造成数据丢失。备份工具可采用光盘、移动硬盘、U 盘等方式，并妥善保管。

第十条　计算机操作人员调离时应将有关材料、档案、软件移交给其他工作人员，调离后对需要保密的内容要严格保密。接管人员应对系统重新进行调整，重新设置用户名、密码。

第十一条　对于违反本规定发生泄密事件的，将视情节轻重追究责任。

第十二条　本制度由学校保密委员会办公室负责解释。

附件 5:

池州学院涉密计算机维修更换报废保密管理制度

为进一步加强我校计算机信息保密管理工作，杜绝泄密隐患，确保国家秘密的安全，根据《中华人民共和国保守国家秘密法》,结合我校实际，特制定本制度。

第一条　涉密计算机发生故障时，应向校保密委员会提出维修申请，经批准后，到市保密局审查合格的定点单位进行维修。涉密计算机进行维修时，须保证所存储的涉密信息不被泄露，对涉密信息应采取涉密信息转存、删除、异地转移存储媒体等安全保密措施。无法采取上述措施时，安全保密人员和该单位涉密计算机系统维护人员必须在维修现场，对维修人员、维修对象、维修内容、维修前后状况进行监督并做详细记录。

第二条　各涉密部门、单位将本部门、本单位设备的故障现象、故障原因、扩充情况记录在设备的维修档案记录本上。

第三条　凡需外送修理的涉密设备,必须经校保密委员会批准,并将涉密信息进行不可恢复性删除处理后方可实施。

第四条　校保密委员会指定专人负责涉密计算机软件安装和设备维护工作，严禁使用者私自安装计算机软件和擅自拆卸计算机设备。

第五条　需报废的涉密计算机由校保密办安排专人负责定点销毁。

第六条　本制度由学校保密委员会办公室负责解释。

附件 6:

池州学院涉密载体销毁管理制度

为进一步加强我校涉密载体销毁管理工作，确保国家秘密的安全，根据《中华人民共和国保守国家秘密法》，结合我校实际，特制定本制度。

第一条　本规定所称国家秘密载体，是指以文字、数据、符号、图形、视频、音频等方式记载、存储国家秘密和工作秘密信息的纸介质、磁介质及半导体介质等各类物品。

第二条　国家秘密载体除正在使用或按照有关规定留存、存档外，应当及时予以销毁。销毁工作要指定专人负责，不定期将需销毁载体进行登记、造册并经校保密委员会主任签字后，派 2 人以上送至市国家保密局指定地点统一销毁。

第三条　涉密载体的销毁范围:

（一）日常工作中不再使用的涉密文件、资料;

（二）淘汰、报废或按照规定不得继续使用的处理过涉密信息的计算机、移动存储介质、传真机、复印机等通信和办公设备;

（三）涉密会议和涉密活动清退的文件、资料;

（四）领导干部和涉密人员离岗（退休、调离、辞职、辞退等）时清退的秘密文件、资料;

（五）已经解密但不宜公开的文件、资料;

（六）经批准可复制使用的涉密文件、资料的复制品;

（七）其他需要销毁的涉密载体。

第四条　禁止未经批准私自销毁国家秘密载体；禁止非法捐赠或转送国家秘密载体；禁止将国家秘密载体作为废品出售；禁止将国家秘密载体送市保密局审查合格的定点单位以外的单位销毁。

第五条　对违反上述规定的涉密人员或秘密载体的管理人员，情节轻微的，给予批评教育；情节严重，造成重大泄密隐患的，报

市国家保密局处理。

第六条　对玩忽职守、滥用职权，造成涉密载体流失、失控，泄漏国家秘密的人员，视情节轻重，依法给予处分或追究刑事责任。

第七条　本制度由校保密委员会办公室负责解释。

附件 7:

池州学院在公共信息网络上发布信息保密管理制度

为进一步加强我校计算机信息网上发布保密管理工作，杜绝泄密隐患，确保国家秘密的安全，根据《中华人民共和国保守国家秘密法》，结合我校实际，特制定本制度。

第一条　在公共信息网络上发布的信息是指经学校主要领导或分管领导审核批准，提供给信息发布部门，向社会公开、让公众了解和使用的信息。

第二条　校园网或其他公众信息网站发布信息保密管理坚持“谁发布、谁负责”的原则。凡向校园网或其他公众信息网站提供或者发布信息，必须经过保密审查批准，报校保密委员会审批。提供信息的部门、单位应当按照一定的工作程序，完善和落实信息登记、保密审核制度。

第三条　除新闻媒体已公开发表的信息外，各部门、各单位提供的上网信息应确保不涉及国家秘密。

第四条　严禁利用网站、网页上开设的电子公告系统、聊天室、论坛等发布、谈论和传播国家秘密信息。

第五条　禁止网上发布信息的基本范围:

（一）标有密级的国家秘密。

（二）未经有关部门批准的，涉及国家安全、社会政治和经济稳定等敏感信息。

（三）未经制文单位批准，标注有“内部文件（资料）”和“注意保存”（保管、保密）等警示字样的信息。

（四）认定为不宜公开的内部办公事项。

第六条　保密工作分管领导应履行的职责:

（一）定期对网络管理人员进行保密法规、保密纪律、保密常识教育，增强信息保密观念和防范意识，自觉遵守并执行有关保密

规定。

（二）建立健全上网信息保密管理制度，落实各项安全保密防范措施。

（三）发现国家秘密网上发布的，立即采取补救措施，并及时向有关部门报告。

（四）定期或不定期向校保密委员会汇报网上发布信息保密管理情况。

第七条　校保密委员会应履行的职责:

（一）指导、监督各部门、各单位网上发布信息的保密管理工作。

（二）协助参与涉及多个部门、单位拟发布信息的保密审查。

（三）向省国家保密局报告网上发布信息保密审查中的重要情况。

（四）负责对网上发布信息进行经常性保密监督检查，发现问题，立即采取补救措施，查明原因，并及时向省国家保密局报告。

（五）协助有关部门对违反规定造成网上泄密的事件依法进行查处。

第八条　提供信息发布的部门、单位应履行的职责:

（一）对拟发布信息是否涉及国家秘密进行审查。

（二）对已发布信息进行定期保密检查，发现涉密信息的，立即采取补救措施，查清泄密渠道和原因，并及时向校保密委员会报告。

（三）接受上级机关和省国家保密局的监督检查。

第九条　违反本规定，对网上发布信息保密审查把关不严，导致严重后果或安全隐患的，按照规定严肃查处。

第十条　现代教育技术中心负责运行和维护，由各部门、各单位指定人员负责进行网页内容的更新工作,发布的信息必须经部门、单位主要负责人初审，校主要领导或分管领导审核批准。

第十一条　本制度由校保密委员会办公室负责解释。

附件 8:

池州学院公文传输网络保密管理制度

为进一步加强我校无密级公文传输网络操作保密管理工作，杜绝泄密隐患，确保国家秘密的安全，根据《中华人民共和国保守国家秘密法》，结合我校实际，特制定本制度。

第一条　网络公文传输实行专人管理，管理人员要切实强化计算机及网络保密意识，要牢固树立保密工作无小事意识，从讲政治的高度，充分认识加强计算机及网络保密工作的重要性，一手抓计算机及网络应用，一手抓网络保密和安全保障。

第二条　网络公文传输的计算机必须专机专用，其他人员不得随便使用。

第三条　局域网内的用于网络公文传输的计算机严禁启用文件夹共享项。

第四条　网络公文传输的计算机要安装防火墙软件和定期防病毒软件对计算机查杀病毒。

第五条　严禁使用因特网上的电子邮件系统发送依申请公开的学校公文信息，严禁利用公文传输网传输密级文件。

第六条　对收到的公文要采取必要防护措施并及时转存到软盘或其他存储体上。

第七条　凡在计算机及网络保密方面出现问题的，将追究主要人员的责任。

第八条　本制度由校保密委员会办公室负责解释。