

中共济宁学院委员会办公室文件

济院党办[2009]25号

关于印发网络、计算机、存储介质 保密管理规定的通知

各部门、各单位：

为进一步加强和规范我校涉密计算机、涉密网络和涉密移动存储介质的保密管理，防止工作中敏感信息（工作秘密）外泄，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》和保密工作的有关法律、规定，结合我校实际，特制定《涉密和非涉密计算机保密管理规定》《涉密计算机维修、更换、报废保密管理规定》《网络保密管理规定》《校园网络发布信息保密管理规定》《移动存储介质保密管理规定》一系列相关的规定。现印发给你们，望你们认真贯彻执行。

中共济宁学院委员会办公室

2009年10月5日

涉密和非涉密计算机保密管理规定

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，根据《中华人民共和国保守国家秘密法》，结合我校实际，制定本规定。

1. 学校保密工作领导小组负责对全校计算机的保密工作进行指导、协调、监督和检查。各部门负责本部门的计算机的保密管理使用，遵循“业务谁主管，保密谁负责”的原则，明确制度，分清职责。

2. 国家秘密信息和工作中的敏感信息(工作秘密)不得在与国际互联网联网的计算机上存储、处理、传递。涉密的计算机必须与国际互联网断开，实行专人负责，专机专用，在使用、管理、维护等方面要严格区别于非涉密计算机，禁止混用、乱用。

3. 凡是上国际互联网的信息要经单位负责人审查、审批，做到涉密的信息不上网，上网的信息不涉密，坚持“谁上网，谁使用，谁负责”的原则，加强上网人员的保密教育和管理，提高上网人员的保密观念，增强防范意识，自觉执行有关规定。

4. 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和工作中的敏感信息(工作秘密)。

5. 凡涉及国家秘密信息的计算机设备的维修，应保证储存的国家秘密不被泄露，到保密工作部门指定的维修点进行维修，并派技术人员在现场负责监督。

6. 学校涉密计算机实行申报登记制度。凡是拟用于处理国家秘密信息或工作中敏感信息(工作秘密)的计算机必须向学校保密工作领导小组办公室申报、登记、审定,并由学校保密办报市国家保密局备案。

7. 涉密计算机只能使用涉密移动存储介质,非涉密计算机只能使用非涉密移动存储介质,不能交叉使用。

8. 涉密的计算机在打印输出信息时,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、废品应当及时销毁。

9. 在发现计算机系统泄密后,应及时采取补救措施,并应及时报学校保密办,由学校保密办负责报市国家保密局。

10. 工作人员不按规定管理和使用涉密和非涉密计算机造成泄密事件的,将按《中华人民共和国保守国家秘密法》和保密工作的有关规定追究责任,构成犯罪的将移送司法机关处理。

11. 本规定由学校保密工作领导小组办公室负责解释。

12. 本规定自发文之日起执行。

涉密计算机

维修、更换、报废保密管理规定

1. 涉密计算机系统进行维护检修时，须保证所存储的涉密信息不被泄密，对涉密信息应采取涉密信息转存、删除（专业清除软件）、异地转移存储媒体等安全保密措施。无法采取上述措施时，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。

2. 涉密计算机的使用单位应将设备的故障现象、故障原因等情况都记录在案。

3. 凡需外送修理的涉密计算机，必须经分管领导和学校保密工作领导小组办公室批准，到保密工作部门指定的维修点进行维修，并在现场负责监督。

4. 涉密计算机更换时，必须报学校保密工作领导小组办公室登记，经单位负责人同意，再由学校保密办报市国家保密局备案后方可实施。被更换的涉密计算机须用专用清除工具将机器内涉密信息清除，待市国家保密局再次检查后方可变更为非涉密计算机。

5. 涉密计算机的报废由学校保密办负责，首先办理涉密计算机的报废手续，经主要领导批准后，到市国家保密局指定的销毁点销毁或送交市国家保密局统一销毁，各单位不得擅自销毁。

6. 本规定自发文之日起执行。

网络保密管理规定

1. 计算机涉密网络的日常使用、维护由使用单位具体负责，应遵守国家有关保密规定，明确保密要求、完善管理制度。

2. 国家秘密信息或内部敏感信息（工作秘密）不得在与国际互联网联网的计算机中存储、处理、传递。

3. 凡是上国际互联网的信息要经单位主要领导审查，做到涉密的信息不上网，上网的信息不涉密。坚持“谁上网谁负责”的原则。要建立信息保密审查领导责任制。

4. 加强对上网人员的保密教育和管理，提高上网人员的保密观念。增强防范意识，自觉执行有关保密工作规定。

5. 使用电子邮件进行网上信息交流，要遵守保密规定，不得利用电子邮件传递、转发或抄送国家秘密信息和内部敏感信息（工作秘密）。

6. 在发现上网计算机系统泄密后，应及时采取补救措施，并及时向分管领导和学校保密工作领导小组办公室报告，由学校保密办报市国家保密局。

7. 工作人员不按规定管理和使用涉密和非涉密计算机造成泄密事件的，将按《中华人民共和国保守国家秘密法》和保密工作的有关规定追究责任，构成犯罪的将移送司法机关处理。

8. 本规定由学校保密工作领导小组办公室负责解释。

9. 本规定自发文之日起执行。

校园网络发布信息保密管理规定

1. 学校校园网信息发布管理实行“谁发布谁负责”的原则。上网信息不得有违反国家法律、法规和涉及国家秘密、内部敏感信息（工作秘密）的内容。

2. 学校网站各栏目的信息应由信息发布部门分管领导签字、审核，若有与其他部门相关的信息，也应经其他部门同意，方可发布。重大信息需经学校主要领导审核。

3. 校园网论坛、聊天室等应由主办单位明确专人负责监管，并在论坛、聊天室等明显位置注明保密要求，网络管理员要对所发布的信息进行实时审查、监控，对敏感信息要及时采取有效的控制措施。

4. 各系、部门要明确专人负责本部门信息发布工作，确保所发布的信息均经过审查、审批，不涉及国家秘密和内部敏感信息（工作秘密）。对上网的信息事先要进行审查，对是否属于涉密信息把握不准的，要及时请示。

5. 信息发布采取责任追究制度，凡是将不准或未经批准的信息进行发布的系、部门，将追究分管领导和具体责任人的责任，造成泄密的将按《中华人民共和国保守国家秘密法》和保密工作的有关规定追究责任，构成犯罪的将移送司法机关处理。

6. 党委（校长）办公室、党委宣传部、安全保卫处及其他相关职能部门指定人员对校园网信息巡查，发现不良信息应及时做好记录并通知网络中心，网络中心在做好相关记录和备份后，应立即删除。对于一些重大事件，要及时上报学校领导和上级主管部门。

7. 本规定自发文之日起执行。

移动存储介质保密管理规定

为加强和规范涉密和非涉密移动存储介质的管理,确保国家秘密的安全,防止工作中敏感信息(工作秘密)外泄,根据《中华人民共和国保守国家秘密法》和保密工作的有关法律、规定,结合我校实际,制定本规定。

1. 移动存储介质分为涉密和非涉密两类。各单位拟用于处理国家秘密信息的移动存储介质必须向学校保密工作领导小组办公室进行申报、登记,经审批后,方能投入使用,并按其所涉及的秘密等级(绝密、机密、秘密)进行管理。凡未存储国家秘密的移动存储介质属非涉密移动存储介质。存储工作中敏感信息(工作秘密)的移动存储介质按有关保密规定按涉密移动存储介质进行管理。

2. 各单位必须指定专人负责本单位涉密移动存储介质的日常管理工作,涉密移动存储介质必须妥善保存,严禁将涉密移动存储介质借给他人使用。

3. 涉密移动存储介质不能在连接国际互联网的计算机上使用。非涉密移动存储介质不能在涉密计算机上使用,杜绝交叉使用。

4. 非涉密移动存储介质禁止以任何形式存储、传输涉及国家秘密和内部敏感信息(工作秘密)。

5. 涉密移动存储介质需要送外部维修时,必须到保密工作

部门指定的具有保密资质的单位进行维修。涉密移动存储介质在报废时，应进行信息清除处理，无法清除处理的交学校保密办。

6. 涉密移动存储介质的报废、销毁变更为非涉密存储介质的，须报学校保密工作领导小组办公室登记、注销，经主要领导批准后，到市国家保密局指定的销毁点销毁或送交市国家保密局统一销毁。不得擅自销毁。

7. 工作人员不按规定管理和使用涉密移动存储介质造成泄密事件的，将按《中华人民共和国保守国家秘密法》和保密工作的有关规定追究责任，构成犯罪的将移送司法机关处理。

8. 本规定由学校保密工作领导小组办公室负责解释。

9. 本规定自发文之日起执行。

主题词：机要工作 保密 规定

济宁学院党委办公室

2009年10月5日印发

(共印50份)