晋中学院文件

院字〔2017〕40号

关于印发《晋中学院校园网络安全管理制度》的通知

各教学学院、各部门：

为了加强晋中学院校园网络（简称：校园网，下同）的安全管理，保证校园网的正常运行，充分利用网络资源，合理使用网络信息，提高校园网的运行效益，更好地为教学、科研等提供服务，经2017年9月22日第29次院长办公会研究通过了《晋中学院校园网络安全管理制度》，现印发给你们，请遵照执行。

附件：晋中学院校园网络安全管理制度

晋中学院

2017年9月22日

附件：

晋中学院校园网络安全管理制度

第一章 总则

第一条 为了加强晋中学院校园网络（简称：校园网，下同）的安全管理，保证校园网的正常运行，充分利用网络资源，合理使用网络信息，提高校园网的运行效益，更好地为教学、科研等提供服务，依据国家有关法律法规、国家有关计算机网络安全管理规定和中国教育科研网(CERNET)的有关规定，特制定本网络安全管理制度。

第二条 在本校范围内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本制度。

第三条 学校信息安全领导组为校园网的领导机构，负责统筹协调网络安全工作和相关监督管理工作。信息中心为学校校园网的建设、维护、管理和技术支持机构，其他有关部门依照本制度和其他相关规定，在各自职责范围内负责网络安全保护和监督管理工作。

第四条 使用校园网的所有部门和人员，必须遵守法律、法规和校内各项规定，履行网络安全保护义务，接受学校相关部门的监督。

第五条 学校尽力保障网络的接入，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。任何个人和组织使用网络应当遵守宪法法律，遵

守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第六条 任何个人和部门有权对危害网络安全的行为向学校信息安全领导组、信息中心、保卫部等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章　网络运行安全

第七条 使用校园网络的所有工作人员及用户必须遵守国家、地方的有关法规以及CERNET、晋中学院有关规章制度，严格执行安全保密制度。

拥有网络主机的各部门应按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危

害网络安全行为的技术措施；

（三）采取监测、记录服务器运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

第八条 网络采用实名制，学校为用户办理上网、申请学校邮箱、使用 VPN、网盘、服务器等校内资源的网络接入手续时，用户须经所在部门同意并持合法证件到信息中心办理相关手续，相关表格和资料在信息中心网站下载，用户不提供真实身份信息的，不得为其提供相关服务。

第九条 各部门办理网络接入或主机服务时，应指定专门的管理人员。各部门负责人要对部门内部计算机的网络行为承担主体责任和监督责任。部门没有指定专门管理员的，不得为其提供相关服务。

第十条 任何单位和个人未办理入网手续，不得私自将计算机接入校园网络、盗用校园网络资源；未经学校或信息中心允许，不得在校园内或是楼宇内撕拉乱扯网络光缆和线缆，不得违规使用路由器、交换机、代理服务器等相关设备。

第十一条 任何人不得破坏、损坏网络线路，不得盗窃、挪用、移动网络设备，不得随意变更网络设备的安装位置；学生离校时要对该宿舍网络设备进行检查，如有损坏，予以赔偿；未经允许，不得随意对网络设备进行断电，发生掉电故障，学校相关部门要及时解决。

第十二条 拥有网络主机和虚拟主机的各部门应当制定

网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关部门报告。

第十三条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供帮助。

第十四条 校园网用户必须接受并配合国家有关部门及学校按章依法进行的监督检查，必须接受信息中心对网络系统及信息系统的安全检查，并在需要时提供协助。

第三章 网络信息安全

第十五条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息；依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和秘密严格保密，不得泄露、出售或者非法向他人提供。

第十六条 任何个人和组织应当对其使用网络的行为负责，不得利用网络从事危害国家安全、泄露国家机密等犯罪活动；不得制作、复制和传播有碍社会治安和不健康的、有伤风化的信息；禁止在网络上发布不真实的信息；不得利用

网络进入未经授权的计算机或其他网络设备，不得以虚假身份使用网络资源等。

第十七条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

第十八条 各部门和二级学院发布的信息由各部门进行审核，各部门领导是二级网站的安全责任人，二级学院要严格审核和把关信息的发布。需要在学校主站发布信息时，要提交宣传部审核把关。

第十九条 信息中心和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求有关人员或部门停止传输，采取消除等处置措施，保存有关记录；对来源于校外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第二十条 信息中心应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织相关关键信息基础设施的部门进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的部门之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第二十一条 学校对一些重点部门以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害信息安全、工作开展的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护制度由学校信息安全领导组制定。

第二十二条 根据学校信息安全管理的相关规定，负责关键信息基础设施安全保护工作的部门，分别编制并组织实施本领域的关键信息基础设施安全规划，实施和监督关键信息基础设施运行安全保护工作。

第二十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第二十四条 除本制度第七条的规定外，关键信息基础设施的使用部门还应当履行下列安全保护义务:

（一）设置专门安全管理负责人;

（二）定期对相关人员进行网络安全教育、技术培训和技能考核;

（三）对重要系统和数据库进行容灾备份;

（四）制定网络安全事件应急预案，并定期进行演练;

第四章 监测预警与应急处置

第二十五条 学校建立网络安全监测预警和信息通报制

度。信息中心应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第二十六条 拥有重要数据信息和申请使用虚拟服务器部门，应当建立健全本部门的数据安全管理制度，切实做好本系统数据及虚拟环境的安全防护，并和信息中心签订信息安全责任书，确保自身数据和信息的安全，制定本部门的网络安全事件应急预案，并定期组织演练。

第二十七条 信息中心协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第二十八条 网络安全事件发生的风险增大时，有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门和人员及时收集、报告有关信息，加强对网络安全风险的监测；

（二）组织有关部门和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

（三）向指定范围发布网络安全风险预警，发布避免、减轻危害的措施。

第二十九条 发生网络安全事件，应当立即启动网络安

全事件应急预案，对网络安全事件进行调查和评估，要求主机所有者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向指定范围发布有关的警示信息。

第五章 责 任

第三十条 违反本制度的规定，有下列行为之一者，信息中心可提出警告或停止其使用校园网络；情节严重者，提交学校行政部门或有关司法部门处理；

1. 违反宪法所确定的基本原则的网络行为；

2. 危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的网络行为；

3. 损害国家荣誉和利益的网络行为；

4. 煽动民族仇恨、民族歧视，破坏民族团结的网络行为；

5. 破坏国家宗教政策，宣扬邪教和封建迷信的网络行为；

6. 散布谣言，扰乱社会秩序，破坏社会稳定的网络行为；

7. 散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的网络行为；

8. 侮辱或者诽谤他人，侵害他人合法权益的网络行为；

9. 未经信息中心批准，采用各种手段切断学校、部门或他人网络连接；

10. 通过扫描、侦听、破解口令、安置木马、远程接管、

利用系统缺陷等手段获取他人信息；

11. 冒用他人和信息中心名义从事网上活动。

12. 盗用校园网络资源及他人帐号或地址。

13. 对使用信息炸弹，致使校园网络系统或连网计算机系统发生阻塞、溢出、处理机忙、资源异常消耗、死锁、瘫痪等运行异常的行为；

14. 对收到的境内外反动电子邮件不及时报告信息中心，而继续散发。

15. 对其主机存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时向有关部门报告；

16. 未经批准使用校园网从事经营性活动；

17. 拒绝、阻碍有关部门依法实施的监督检查；

第六章　附　则

第三十一条　本制度下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（四）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第三十二条 如本制度与学校以前制定的相关规定或制度相冲突，按本制度执行，本制度中未尽事宜，按国家或山西省相关规定执行，本制度自发布之日起执行，

第三十三条 本制度由信息中心负责解释。