鲁中高校字〔2019〕48号

山东中医药高等专科学校
关于印发《网络信息安全管理条例》
的通知

各部门：

《山东中医药高等专科学校网络信息安全管理条例》已经学校研究通过，现印发给你们，请认真抓好贯彻落实。

山东中医药高等专科学校

2019年2月26日

山东中医药高等专科学校
网络信息安全管理条例

为进一步加强校园网络信息安全的管理，规范学校各级网站建设，保证网络安全，把校园网建设成为广大师生进行交流的平台、教育和学习的阵地、宣传学校事业发展的窗口。根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》以及《山东省计算机信息系统安全管理办法》的规定，结合我校实际情况，特制定本条例。

第一章　总则

第一条　方针：

（一）坚持“业务为主、安全为重，预防为先、综合防范，统筹兼顾、科学管理”的总体方针，实现网络信息系统安全的可控、能控、在控。

（二）依照信息安全的总体防护策略，落实信息系统安全等级保护等各项安全制度。通过对网络信息系统的全面梳理、全面诊断和全面加固，掌握现状、找准问题、制订措施、有效改进。

第二条　目标：

使已识别的信息资产满足信息安全的各项要求，包括法律法规、用户与相关方和组织业务要求。具体目标包括：

（一）由操作和管理流程原因，造成严重后果的信息泄漏事件为零；造成学校主要业务中断时间累计不超过 4 h/年； 引起学

校主要业务中断事件发生次数不超过2次/年；严重影响网络与信息系统可用性的事件不超过1次/年；

（二）信息安全事件发生时，以损失最小化、恢复时间最短化、避免再次发生为工作目标；

（三）保护信息免受各种威胁的损害，确保信息系统持续、稳定、可靠运行；

（四）对整个网络信息安全管理制度体系及信息安全工作本身做出持续性改进。

第三条 信息安全管理体系

（一）物理安全管理体系：机房要选择合适的物理位置，对进出人员执行必要的访问控制。机房内部必须划分区域管理，并部署基础防护系统和设备等。

（二）网络安全管理体系：要求网络中主要设备必须进行双机热备，且除接入交换机链接工作终端的线路外，其他线路必须进行双线冗余；在保证整体网络带宽充足的基础上，需划分地址段进行网络管理，并突出优先级；网络边界处必须部署防火墙、IPS等安全设备；网络设备必须开启相应的日志审计功能等。

（三）主机安全管理体系：要求系统登陆必须进行身份标识和鉴别，系统管理用户身份标识应确保其唯一性，避免共享账户的存在；口令应有复杂度要求并定期更换，且必须及时删除多余的、过期的账户；系统必须启用登录失败处理功能；对服务器进

行远程管理时，必须采取必要的防窃听措施；必须开启日志审计功能，并安装统一管理的防恶意代码产品等。

（四）应用安全管理体系：要求登录应用系统必须进行两种或两种以上的复合身份验证，并保证应用系统用户的唯一性；应用系统必须开启身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数，且必须开启日志审计功能；应用系统存储用户信息的设备在销毁、修理或转其他用途时，必须清除内部存储的信息是否牵涉泄密等。

（五）数据安全管理体系：要求业务应用数据和设备配置文档都必须进行备份，并保证数据及传输过程的完整性。必须使用专业备份设备和工具，进行加密数据的传输和存储。进行异地备份时，必需利用通信网络将关键数据定时批量传送至备用场地。

第四条 重要原则、标准和符合性要求

学校在建立和管理信息安全管理体系时，必须符合相关法律法规和合同的要求。

第五条 校园网络信息系统是指由校园计算机网络设备、服务器、网络线缆、客户端、软件、电子数据所构成的为校园网络应用而服务的硬件和软件的集成系统。

第六条 校园网络信息是指在校园网内由学校、各部门建立的各类网站、应用信息系统等的所有信息。

第七条 网络信息安全管理，应当保障计算机网络设备和配套设施的安全，保障信息的安全和运行环境的安全，保障网络系统的正常运行，保障软件和信息系统的安全运行。

第八条 校园网用户指所有接受我校网络接入服务、使用校园网络资源、设施设备和数据的教职员工、学生及其他人员。

第九条 校园网用户必须严格遵守国家有关法律法规和学校有关规章制度，严格执行安全保密制度，接受并配合有关部门的教育、管理、监督和检查，不得制作、复制、使用和传播有害、违法或违反社会公德的信息、数据和软件等。

第二章 网络信息安全管理机构

第十条 学校成立网络信息安全工作领导小组。下设领导小组办公室,办公室设在教育技术中心，行使日常管理职能。

第十一条 校园网络信息系统管理按照“谁主管谁负责、谁运行谁负责、谁使用谁负责”的原则，明确责任，突出重点，保障安全。各部门负责人是第一责任人。

第三章 网络使用权与用户

第十二条 校园网用户要增强网络安全意识,经常更换账号密码，不把账号密码借给他人使用。严禁非法获取、破解、盗用他人网络身份、账号密码和 IP 地址等行为。

第十三条 在校园内和学校拥有的网络系统中，安装、拆卸和

改变网络服务设施（包括服务器、交换机、路由器等硬件设施及软件和数据库系统等），必须事先经网络信息安全工作领导小组办公室进行安全性技术审查并批准后方可进行采购和实施。

第十四条 校园网用户在遭到黑客、病毒、木马攻击或发现非法使用迹象、违规行为和有害信息等可能危害网络安全的现象时，应立即断电、断网并及时上报网络信息安全工作领导小组办公室予以及时处理。

第四章 网络设施与资源安全

第十五条 涉及校园网络信息系统的工程建设应当严格遵守有关标准和规范，妥善保护网络设施的安全。

第十六条 加强校园拓朴结构、网络设备和线路信息保密工作，需要查看或更改网络线路、交换机等网络设施的硬件结构、连接和参数配置的，须经网络信息安全工作领导小组办公室批准。

第十七条 域名、IP 地址和带宽资源由网络信息安全工作领导小组办公室统一分配指定，任何人不得擅自变更、盗用。

第十八条 严禁在校园网内使用和传播来历不明、可能引发病毒或木马传染的软件和文件。外来光盘、U 盘、移动硬盘和存储卡等移动存储介质使用前必需进行病毒和木马查杀后，方可使用。

第十九条 非网络管理人员进入网络中心机房必须由网络管理员现场全过程陪同，网络设备调整须由网络管理员操作。

第二十条 严禁任何部门和个人破坏校园网络设施和设备，

危害网络运行安全。

第五章　信息安全

第二十一条　校园网各类信息系统必须每天由各信息系统管理员扫描并修复服务器漏洞、定期查杀病毒，以防止系统中的重要信息文件通过漏洞或病毒程序扩散传播，造成重大泄密事故。

第二十二条　系统管理员以及版面管理员必须每天浏览、监测各信息系统及网站的信息发布情况，发现版面内有不良内容或问题必须立即删除或屏蔽，并及时上报网络信息安全工作领导小组办公室进行处理，保证信息系统健康运行。

第二十三条　任何人不得非法和越权获取、复制、传播、发布和篡改非本人职权内的业务信息及他人的私人信息。

第二十四条　具有信息系统的单位责任人应责成信息系统管理员定期对部门所属的信息系统进行安全检查，检查内容包括：

（1）安全责任落实情况，重点检查信息系统及网站管理员落实情况；

（2）安全防范措施落实情况，重点检查信息系统及网站的身份认证、访问控制、防篡改、防病毒、防攻击等安全技术措施的有效性；

（3）应急机制建设情况，重点检查信息系统及网站出现问题后的应急预案制定、落实情况，应急技术支持队伍建设情况，重大信息安全事故处置情况，以及重要数据及业务系统的备份情

况；

（４）安全隐患排查及整改情况，重点检查对安全事故、防范措施、设备设施等方面存在的漏洞和薄弱环节的排查情况，分析产生问题和隐患的原因，研究和落实整改措施等；

（５）安全形势及安全风险评估，深入、系统地分析外部安全形势和内部防范措施的有效性，全面评估信息系统及网站的安全风险状况，提出整改意见。

第二十五条 任何部门和个人都必须遵守《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》以及《山东省计算机信息系统安全管理办法》的规定。任何人不得利用校园网危害国家安全、泄露国家秘密；不得侵犯国家的、社会的、集体的利益和公民的合法权益；不得从事违法犯罪活动等。

第二十六条 不得利用校园网制作、复制、查阅和传播下列信息：

（1）煽动抗拒、破坏宪法和法律、行政法规实施的；

（2）煽动颠覆国家政权，推翻社会主义制度的；

（3）煽动分裂国家、破坏国家统一的；

（4）煽动民族仇恨、民族歧视，破坏民族团结的；

（5）捏造或者歪曲事实，散布谣言，扰乱社会秩序的；

（6）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，

教唆犯罪的；

（7）公然侮辱他人或者捏造事实诽谤他人的；

（8）损害国家机关信誉的；

（9）其他违反宪法和法律、行政法规的。

第二十七条 不得从事下列危害计算机信息网络安全的活动：

（1）未经允许，进入计算机信息网络或者使用计算机信息网络资源的；

（2）未经允许，对计算机信息网络功能进行删除、修改或者增加的；

（3）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加的；

（4）故意制作、传播计算机病毒等破坏性程序的；

（5）其他危害计算机信息网络安全的。

第二十八条 专用、涉密的计算机和服务器不得接入公共网络。

第六章 系统管理员

第二十九条 各信息系统必须明确责任人和系统管理员，同时将责任人和系统管理员的电话（手机）报网络信息安全工作领导小组办公室备案；如果人员发生变动，需及时上报、更新备案内容。

第三十条 学校内各信息系统的管理工作不得交由学生或兼职人员代管。

第三十一条 系统管理员应严格遵守岗位规范和职业道德，保护系统和信息安全，不得借职务之便为自己或协助他人非法或非授权获取、传播、复制和篡改数据。

第三十二条 系统管理员不得擅自查阅非系统管理所需信息，特殊情况需要查阅或修改时，须同时获得网络信息安全工作领导小组办公室和该应用系统主管部门负责人的书面许可。

第三十三条 系统管理员需要对系统信息、安全配置、软件参数等数据定期妥善备份保存。

第三十四条 系统管理员账号密码要定期更换。

第七章 违规处理

第三十五条 发现用户存在违法违规行为的，网络管理员和系统管理员应中断其联网权限和服务，并按违规行为有关规定进行处理。

第三十六条 校园网用户的违规行为，依情节轻重由网络信息安全工作领导小组（提请学校）给予下列处理：

（一）情节轻微、未造成后果的，责令立即改正并记录在案；

（二）情节较严重、对网络安全造成轻微后果的，立即中断涉及计算机的网络服务，对当事人进行通报批评；

（三）情节严重、造成网络安全事故的，对涉及的计算机予

以关停整顿，责成部门负责人和当事人写出书面检查，由学校给予相应纪律处分；

（四）情节严重、涉嫌违法犯罪的，交由公安部门处理。

第八章　其他

第三十七条　本条例自颁布之日起施行。与本条例有冲突的有关文件同时废止。

山东中医药高等专科学校办公室　　2019 年 2 月 26 日印发