第九篇

信息图书

信息管理中心工作职能、职责

信息管理中心工作职能

一、根据学校发展战略制定信息化工作规划。

二、负责编制学校信息化建设年度预算，并负责信息化项目的建设。

三、负责学校局域网的运行、维护和管理，制定局域网的维护管理细则和操作章程，制定相关作业计划并实施。

四、负责计算机及周边设备和网络设备的采购、维护和管理。建立完善的设备档案，定期进行保养维护。

五、负责学校各信息系统的管理，确保正常使用。负责学校信息化建设应用系统的规划、运行、维护和管理以及业务的推广和用户的指导、培训及技术支持。

六、与各个业务部门协调配合，参与制定学校各类管理制度和业务流程，保证其能通过信息管理平台实施。

七、负责编制计算机和信息系统应用的使用手册和培训教材，不定期组织培训，提高学校计算机应用和网络办公的水平。

八、完成学校领导交办的其他工作任务。

信息管理中心主任工作职责

一、负责信息管理中心的日常管理工作，负责组织制定学校信息化总体建设规划和分期建设计划以及经费预算。

二、建立和完善信息化建设和管理的各项规章制度，实现管理的规范化和制度化。

三、负责学校网络体系的总体规划和设计，根据学校信息化规划，结合学校的实际情况逐步拓展信息系统管理范围和深度。进行系统新需求的调研并提出解决方案。对信息化建设项目提出具体技术要求，并控制进度和质量，负责协调实施过程中遇到的问题。

四、与各业务部门参与学校各类管理制度和业务流程的制定，保证其能通过信息管理平台实施。

五、定期对业务数据进行检查，保证数据的规范性、完整性、合理性。

六、负责学校网络安全策略的规划。

七、负责组织信息管理中心人员进行业务学习，不断提高其工作能力和业务水平。

八、积极主动配合、协助学校其他部门的工作完成领导临时交办的任务。

行政干事工作职责

一、负责学校校园网的管理与维护，记录网络安全运行情况，处理网络故障及突发事件。

二、协助主任建设、管理、更新学校网站。

三、管理维护学校多媒体教室的多媒体教学设备。

四、管理学校网络中心机房。

五、协助主任管理维护各办公室办公用计算机设备。

六、负责校报的电子编辑排版工作。

七、负责学校各种活动的录像工作，并及时整理存档音像资料。

八、完成领导、主任交办的其他工作。

信息管理中心工作管理规定

为了进一步规范学校信息安全工作，满足业务发展和监管机构对学校信息安全保障工作的要求，构建安全、稳定、持续运行的信息安全保障体系，根据《中华人民共和国计算机信息系统安全保护条例》《河南省计算机信息系统安全保护管理办法》等有关规定，结合学校实际，制定本规定。

第一章　人员安全管理规定

第一条　操作人员必须爱护电脑设备，保持办公室和电脑设备的清洁卫生。

第二条　操作人员必须懂得正确操作和使用计算机，加强计算机知识的学习。

第三条　不得让任何无关的人员使用自己计算机，不要擅自或让其他非专业技术人员修改自己计算机系统的重要设置。

第四条　严禁利用计算机系统上网发布、浏览、下载、传送反动、色情及暴力的信息。

第五条　严格遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》，严禁利用计算机非法入侵他人或其他组织的计算机信息系统。

第六条　计算机各终端用户应保管好自己的用户账号和密码。严禁随意向他人泄露、借用自己的账号和密码；严禁不以真实身份登录系统。计算机使用者更应定期更改密码、使用复杂密码。

第七条　每年度对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训，并对相关人员进行考核，并记录相关成绩。

第八条　规范人员的录用过程，对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核，对从事关键岗位的人员签署保密协议。

第九条　人员离岗过程中，应及时终止离岗员工的所有访问权限，收回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备，应办理严格的调离手续。

第二章　系统建设管理

第十条　安全方案设计

应以书面的形式描述对系统的安全保护要求、策略和措施等内容，形成系统的安全方案。

应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的详细设计方案。

应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施。

第十一条　产品采购和使用

应确保安全产品采购和使用符合国家的有关规定。

应确保密码产品采购和使用符合国家密码主管部门的要求。

应指定或授权专门的部门负责产品的采购。

第十二条　自行软件开发

应确保开发环境与实际运行环境物理分开。

制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则。

应确保提供软件设计的相关文档和使用指南，并由专人负责保管。

第十三条　外包软件开发

应根据开发要求检测软件质量。

应确保提供软件设计的相关文档和使用指南。

应在软件安装之前检测软件包中可能存在的恶意代码。

应要求开发单位提供软件源代码，并审查软件中可能存在的后门。

第十四条　工程实施

应指定或授权专门的部门或人员负责工程实施过程的管理。

应制定详细的工程实施方案，控制工程实施过程。

第十五条　测试验收

应对系统进行安全性测试验收。

在测试验收前应根据设计方案或合同要求等制定测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告。

应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

第十六条　系统交付

应制定系统交付清单，并根据交付清单对所交接的设备、

软件和文档等进行清点。

应对负责系统运行维护的技术人员进行相应的技能培训并对培训过程进行记录表格记录（附件 2《项目交付培训记录表》）。

应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档。

第十七条　安全服务商选择

应确保安全服务商的选择符合国家的有关规定。

应与选定的安全服务商签订与安全相关的协议，明确约定相关责任。

应确保选定的安全服务商提供技术和服务承诺，并要求与安全服务商签署保密协议。

第三章　办公用计算机上网的使用管理

第十八条　各系、部上网的计算机，必须装有杀毒软件，并注意及时升级。

第十九条　各系、部应使用由信息管理中心所分配的 IP 地址，不得随意更改为其他的 IP 地址。如果私自更改，给其他部门计算机上网使用造成影响及由此带来的一切相关责任，由违规部门全部承担。

第二十条　出现不能上网的情况，先自行检查计算机是否正常，在排除“使用不当”“系统问题”“病毒影响”等问题后，再与信息管理中心联系，信息管理中心只负责检测网络线路是否畅通。

第二十一条　以前绑定 IP 并登记过的计算机，在点击

IE 浏览器时出现提示“您不是合法的网络用户”，请不要自行处理，应与信息管理中心取得联系后进行解决。

第二十二条　每个部门被核准上网的计算机只有一个合法的 IP 地址，如果由于工作需要，确有新的未核准登记的计算机加入互联网，请先报校领导审批，再由信息管理中心统一分配新的合法 IP 地址方可接入互联网，通过其他方法接入互联网均被视为非法用户。

第二十三条　出现私自改动计算机 IP 地址或者使用未经核准的计算机接入互联网的情况，将会暂停该部门的计算机接入互联网，待问题解决并由校领导批示后方可重新开通。如果改动期间给相关部门的工作造成影响，都将由违规部门负全部责任。

第二十四条　各部门保存重要数据以及重要或机要文件的计算机，严禁接入互联网，以免造成泄密、数据丢失等不可挽回的严重后果。

第四章　机房管理

第二十五条　出入管理

（一）严禁非机房工作人员进入机房，凡因设备安装调试等原因需要进入机房的，应填写机房登记表（附件 3《人员出入机房登记表》），在机房操作期间，机房人员应全程陪同。

（二）进入机房人员应遵守机房管理制度。

（三）进入机房人员不得携带任何易燃、易爆、腐蚀性、强电磁、辐射性、流体物质等对设备正常运行构成威胁的物

品。带出物品需填写物品出门证（附件 4《物品出门证》），并经图书馆与信息管理中心同意后方可带出。

第二十六条　安全管理

（一）操作人员随时监控中心设备运行状况以及各网点运行情况，确保其安全高效运行，发现异常情况应立即按照预案规程进行操作，并及时上报和详细记录。

（二）非机房工作人员未经许可不得擅自上机操作和对运行设备及各种配置进行更改。

（三）严格执行密码管理规定，对操作密码定期更改，超级用户密码由系统管理员掌握。

（四）机房工作人员应恪守保密制度，不得擅自泄露中心各种信息资料与数据。

（五）中心机房内严禁吸烟、喝水、吃食物、嬉戏和进行剧烈运动，保持机房安静。

（六）每学期对机房内设置的消防器材、机房火灾自动报警系统、监控设备进行检查和维护，以保证其有效性。

（七）路由器、交换机、防火墙、服务器及存储等关键设备，须放置计算机机房内，不得自行配置或更换，更不能挪作他用。

第二十七条　操作管理

（一）机房管理人员定期对机房基础设施进行巡检包括服务器、网络设备、空调、UPS、监控等设备的运行指示灯、CPU、内存、硬盘、应用程序等进行检查，机房温度须保持为：20℃-25℃，机房湿度保持为：40％RH～70％RH。机房

管理人员须认真、如实、详细填写机房基础设施巡检记录表（附件 5《机房基础设施巡检记录表》）、（附件 6《机房温湿度记录表》）及（附件 7《机房基础设施维护表》）以备后查。

（二）严格按照每日预制操作流程进行操作，对新上业务及特殊情况需要变更流程的应事先进行详细安排并书面报负责人批准签字后方可执行；所有操作变更必须有存档记录。

（三）每周对机房环境进行清洁，以保持机房整洁；每月进行一次大清扫，对机器设备吸尘清洁。

（四）严格按规章制度要求做好各种数据、文件的备份工作。应用系统定期或按需进行本地和异地备份。所有重要文档定期整理装订，专人保管，以备后查。

第二十八条　运行管理

（一）中心机房和开发调试机房隔离分设。未经负责人批准，不得在中心机房设备上编写、修改、更换各类软件系统及更改设备参数配置。

（二）各类软件系统的维护、增删、配置的更改，各类硬件设备的添加、更换必须经负责人书面批准后方可进行；必须按规定进行详细登记和记录，对各类软件、现场资料、档案整理存档。

（三）为确保数据的安全保密，对各业务单位、业务部门送交的数据及处理后的数据都必须按有关规定履行交接登记手续。

（四）部门负责人应定期与不定期对制度的执行情况进行检查，督促各项制度的落实，并作为人员考核之依据。

第五章　介质管理

第二十九条　介质定义

介质是指在信息化建设当中留存的纸质文档和购买的应用软件的光盘、U 盘，移动硬盘等。

第三十条　介质管理和使用

（一）介质由专人统一管理，分类标记并存放在介质保管柜后统一登记（附件 8《介质归档登记表》）。

（二）按国家标准《电子计算机机房设计规范》的要求，介质存放的条件为:

项目	纸质介质	U盘		移动硬盘		光盘
		已记录	未记录	已记录	未记录	
温度°C	5～40	18～28	0～40	18～28	0～40	13～20
相对度%	30～70	20～80	20～80	20～80	20～80	20～45
磁场强度A/m		<3200	<3200	<4000	<4000	<4000

（三）个人需要使用时、需凭批准手续到介质管理员处登记，填写介质借用登记表（附件 9《介质借用登记表》），归还时也需在介质借用表上签字确认归还。保管人员应每月对登记介质和借用表核对。

（四）对存储介质的购置、分发、使用、维修、废弃、销毁等各个环节、都应认真重视，做好防泄密工作。重要的资料至少应有两种存储介质的数据存储设备。

（五）工作人员工作时使用的光盘、硬盘、U 盘等存储

介质，不得随意给外人使用，不得带出办公场所。

（六）对已损坏的光盘、硬盘、U盘等存储介质，不得随意丢弃，应交专人统一处理。

第六章　网络安全管理

第三十一条　遵守国家有关法律法规，严格执行安全保密制度，不得利用网络从事危害国家安全、泄露国家秘密等违法犯罪活动，不得制作、浏览、复制、传播反动及黄色信息，不得在网络上发布反动、非法和虚假的消息，不得在网络上谩骂攻击他人，不得在网上泄露他人隐私。严禁通过网络进行任何黑客活动和性质类似的破坏活动，严格控制和防范计算机病毒的侵入。

第三十二条　网络安全管理员主要负责全单位网络（包含局域网、广域网）的系统安全性。

第三十三条　良好周密的日志审计以及细致的分析经常是预测攻击，定位攻击，以及遭受攻击后追查攻击者的有力武器。应对网络设备运行状况、网络流量、用户行为等进行日志审计，审计内容应包括事件的日期和时间、用户、事件类型、事件是否成功等内容，对网络设备日志须保存60天以上。

第三十四条　网络管理员察觉到网络处于被攻击状态后，应确定其身份，并对其发出警告，提前制止可能的网络犯罪，若对方不听劝告，在保护系统安全的情况下可做善意阻击并向主管领导汇报。

第三十五条　网络设备关键策略配置的更改，各类硬件

设备的添加、更换前需经过技术验证，策略更改前后做好备份。

第三十六条　定期对网络设备进行漏洞扫描并进行分析、修复，网络设备软件存在的安全漏洞可能被利用，所以定期根据厂家提供的升级版本进行升级。

第三十七条　用户通过学校内网访问互联网需进行身份验证，开户需要填写《郑州医药健康职业学院校园网络入网申请表（个人）》。

第三十八条　对关键网络设备和关键网络链路需进行冗余，以保证高峰时的业务需求，以消除设备和链路出现单点故障。

第三十九条　IP 地址为计算机网络的重要资源，计算机各终端用户应在信息科的规划下使用这些资源，不得擅自更改。另外，某些系统服务对网络产生影响，计算机各终端用户应在信息科的指导下使用，禁止随意开启计算机中的系统服务，保证计算机网络畅通运行。

第七章　主机系统安全管理

第四十条　对主机上的每个操作系统用户和数据库用户进行审计，审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等，并保护审计记录，避免受到未预期的删除、修改或覆盖等。对主机设备日志须保存三个月。

第四十一条　任何用户不得进入未经许可的计算机系

统更改系统信息和用户数据。

第四十二条　对操作系统盘区/文件进行访问权限的配置，关闭/禁用不需要服务如：远程桌面服务、Computer Browser、Task scheduler、Error reporting service、Remote Registry 等。

第四十三条　各部门定期对本部门主机系统进行备份使之能在发生故障时进行恢复。对关键设备须进行设备冗余，以满足业务高峰期的需求及消除设备单点故障。

第四十四条　检查用户账号，停止不需要的账号和组，停用 guest 等账号，建议重命名 administrator。

第四十五条　设定终端接入方式、对网络地址范围等进行限制，对终端登入用户数量进行限定，对终端连接的空闲时间进行限定。

第四十六条　主机系统登入用密码应是数字、字母和特殊符号的结合体，密码更新周期为 30 天。如果给定的口令超过 90 天，则必须锁定账号。严禁重新使用口令，强制密码历史为 3。用户登入失败三次自动锁定 15 分钟以上。

第四十七条　系统管理员察觉到系统处于被攻击状态后，应确定其身份，并对其发出警告，提前制止可能的网络犯罪，若对方不听劝告，在保护系统安全的情况下可做善意阻击并向主管领导汇报。

第四十八条　对主机及存储设备进行关机、重启、断电等操作时一定得安装设备的操作说明，对于主机设备按照先关闭操作系统再断电源顺序，对于存储设备先关闭与之相连

的设备，再关闭存储设备系统，最后断电的顺序，以保证设备、数据的安全。

第四十九条　定期对主机系统进行漏洞扫描，补丁升级，升级前做好备份，并对补丁进行安全性测试。

第八章　恶意代码防范

第五十条　应在单位网络配置计算机网络病毒防治产品，其生产单位应具有《计算机信息安全专业产品销售许可证》，其病毒防治能力应达到公安部规定的合格或以上水平。

第五十一条　各部门应有较强的病毒防范意识，定期进行病毒检测，发现病毒立即处理并通知信息管理部门或专职人员。

第五十二条　各工作计算机必须进行安全配置及杀毒软件的安装。各计算机终端用户应定期对计算机系统、杀毒软件等进行升级和更新，并定期进行病毒清查，不要下载和使用未经测试和来历不明的软件、不要打开来历不明的电子邮件、以及不要随意使用带毒 U 盘等介质。

第五十三条　任何人不得制造、传播计算机病毒、不得故意输入计算机病毒及其有害数据危害网络安全。发现病毒，及时报告，及时处理。

第五十四条　定期检测恶意代码进行分析，并记录分析情况。

第五十五条　定期进行系统漏洞扫描和风险评估，发现系统漏洞要按风险等级制定解决方案并组织实施。

第五十六条　应用系统投产前，必须进行系统安全配置

检测和漏洞扫描，安装最新补丁包，关闭不需要的端口。

第九章　数据备份

第五十七条　根据需要定期对的重要数据制作异地备份，离线数据应做好分类标识，确保系统一旦发生故障时能够快速恢复。

第五十八条　离线数据的备份、恢复、转出、转入的权限都应严格控制。严禁未经授权将数据备份出系统，转给无关的人员或单位；严禁未经授权进行数据恢复或转入操作。

第五十九条　离线备份的数据必须指定专人负责保管，由系统管理员按规定的方法同数据保管员进行数据的交接。交接后的备份数据应在指定的数据保管室或指定的场所保管。

第六十条　离线备份数据资料保管地点应有防火、防热、防潮、防尘、防磁、防盗设施。

第六十一条　定期对备份的使用现状进行检查，每学期抽取部分数据测试恢复，以检验备份是否有效。

第六十二条　服务器未做好备份前不得删除任何硬盘数据。对重要的数据应准备双份，存放在不同的地点；对采用磁性介质或光盘保存的数据，要定期进行检查，定期进行复制，防止由于磁性介质损坏而使数据丢失。

第十章　应急预案

第六十三条　为提高我校处置校园网络与信息安全突发公共事件能力，形成科学、有效、反应迅速的应急工作机

制，确保重要计算机信息系统的实体安全、运行安全和数据安全，最大限度地减轻网络与信息安全突发公共事件的危害，保障国家和人民生命财产的 安全，保护公众利益，维护正常的经济、政治、社会秩序，促进社会的和谐发展。

第六十四条　根据《中华人民共和国计算机信息系统安全保护条例》《计算机病毒防治管理办法》《河南省网络与信息安全应急预案》《郑州市突发公共事件总体应急预案》《郑州医药健康职业学院校园计算机网络管理办法》《郑州医药健康职业学院信息化建设管理办法》等有关法规、规定，制定本预案。

第六十五条　网络安全突发事件是指自然灾害、事故灾难和人为破坏引起的网络与信息系统的损坏。

（一）自然灾害是指地震、台风、雷电、火灾、洪水等。

（二）事故灾难是指电力中断、网络损坏或者是软件、硬件设备故障等。

（三）人为破坏是指人为破坏网络线路、通信设施，黑客攻击、病毒攻击等事件。

第六十六条　工作原则和要求

（一）积极防御、综合防范。立足安全防护，加强预警，重点保护基础信息网络；从预防、监控、应急处理、应急保障环节，在管理、技术、人才等方面，采取多种措施，充分发挥各方面的作用，共同构筑网络与信息安全保障体系。

（二）明确责任、分级负责。按照“谁主管谁负责、谁运营谁负责”以及“条块结合、以条为主”的原则，建立和完善安全责任制、协调管理机制和联动工作机制。

（三）以人为本、快速反应。网络与信息安全突发公共事件发生时，要按照快速反应机制，及时获取充分而准确的信息，跟踪研判，果断决策，迅速处置，最大程度地减少危害和影响。

（四）依靠科学、平战结合。加强技术储备、规范应急处置措施与操作流程，实现网络与信息安全突发公共事件应急处置工作的科学化、程序化与规范化。树立常备不懈的观念，定期进行预案演练，确保应急预案切实可行。

第六十七条　组织机构及职责

（一）学校成立校园网络与信息安全事件应急处置领导小组，全面负责和统一指挥校园网络与信息安全重大突发事件的应急处置工作。领导小组组长由主管信息安全工作的副校长担任，小组成员由办公室、保卫处、人事处、教务处、学生处、团委、财务处、信息管理中心、基建处、后勤保障处等部门主要负责人组成。

领导小组的工作职责为研究制订本校网络与信息安全应急处置工作的规划、计划和政策，协调推进本校校园网与信息安全应急工作体系建设；发生网络与信息安全突发公共事件后，决定启动本预案，组织应急处置工作。

（二）信息管理中心作为职能部门，负责校园主干网络与主要信息系统安全事件的预防、监测、报告和应急处置，负责对学校其他部门主管的网络信息系统的安全防护情况进行日常检查、指导和督促。

第六十八条　应急处置程序

（一）应急预防

1.机房:

定期检查信息管理中心机房电源、空调、UPS、发电机等设备的运行情况。

做好机房防漏、防火、防盗设施的安全检查。

重大自然灾害天气、重要节假日安排人员值班。

2.应用系统:

做好系统服务器、SAN 存储等关键设备日常检查，定期进行安全管理和评估。

做好操作系统、应用系统、数据库系统等软件的恢复准备，关键性的应用服务应以双机冗余、双机热备等形式提高系统的强健性。

做好应用系统和数据库数据的异机或异地备份。

做好应用系统日常运行维护，并根据需要调整安全策略，进行安全监察和评估，及时发现和解决安全隐患。

3.网络安全:

对网络安全设备进行日常巡检，以确保正常运行。

定期检查安全设备的运行日志和统计报表，并根据运行情况调整安全策略。

4.校园一卡通:

做好系统服务器等关键设备日常检查，定期进行安全管理和评估。

做好操作系统、应用系统、数据库系统等软件的恢复准备，关键性的应用服务应以双机冗余、双机热备等形式提高系统的强健性。

做好应用系统和数据库数据的异机或异地备份，数据库

数据的备份应做到可实时备份，实时恢复。

做好应用系统日常运行维护，并根据需要调整安全策略，进行安全监察和评估，及时发现和解决安全隐患。

（二）启动预案

1.突发事件发生后，信息管理中心应进行先期应急处置工作，立即采取措施控制事态，并将事件上报校园网络与信息安全事件应急处置领导小组。任何原因导致校园网络、应用中断超过30分钟的，应采用各种手段如网上发布通知、电话通知等告知相关部门和用户。

2.领导小组核实相关情况后，裁定具体故障类型和级别，根据相应情况启动预案。

（三）应急处置

1.机房断电：常规停电，水电中心应提前2个工作日通知信息管理中心。突发的断电，水电中心应在第一时间通知信息管理中心，并尽快回复供电。其中：

断电两小时以内的，安排人员值班，以确保断电及来电后发电机、UPS及空气开关等正常工作。

断电两小时至六小时的，安排人员值班，关闭不重要的应用系统的服务器，以节约UPS电能，确保重要应用不间断运行，并在来电后，启动被关闭的服务器，检查运行情况。

断电六小时以上的，相关设备管理人员到机房值守，做好数据备份后，按正确操作顺序，关闭各服务器、SAN存储设备、交换机、路由器、防火墙等网络设备。来电后经确认供电平稳正常后，再依次开机，检查各软硬件设备的运行情况，确保校园网络的通畅。

2.校园主干网络故障:

因电信、教科网线路故障导致学校网络出口中断的，应立即联系相应管理机构，确认故障原因和时长，督促其尽快恢复，同时在信息门户上发布通知告知用户。

因核心网络设备如交换机、路由器、防火墙等故障导致校园主干网络中断的，应立即联系硬件供货商进行更换或维修，同时启用备用设备，导入最新的备份配置，尽快恢复网络通讯。

校内主干光纤因各种原因（如鼠咬、野蛮施工等）毁损的，应立即联系光缆熔接单位进行施工恢复，同时将情况报告给领导小组和相关责任部门。事后按照损坏程度进行相关的索赔。

3.服务器故障：服务器故障后应立即与设备管理人员联系进行报修工作，其中:

非关键硬件组件故障的，应先进行数据备份，再更换故障组件，确认无误后重新启动服务器运行服务;

关键硬件组件、操作系统、应用系统故障的：如重启无效，应立即联系相关管理人员、软硬件厂商维护人员对服务器及应用系统进行检查，同时，有冷（热）备服务器的，立即启动备份服务器，否则，应立即申请服务器进行重新部署安装，以最新的备份数据启动应用服务。

因软件设计缺陷、设计漏洞等引起的故障，应通知相关软件公司研发部门在期限内查明原因，解决问题。

4.存储设备故障：存储设备故障后应立即与设备厂家售后工程师联系，根据故障情况分别进行:

相关应用系统管理人员采用异机备份数据先恢复应用系统运行。

存储设备对故障组件进行更换，做好数据恢复工作。

5.黑客入侵或计算机病毒爆发：校园网络上出现黑客攻击或计算机病毒爆发行为，任何人员都有义务向信息管理中心报告。信息管理中心立即启动应急响应，切断受攻击计算机与网络的连接，停止一切操作、保护现场，并上报有关领导：

安全管理人员应立即查找入侵踪迹，分析入侵方式和原因，根据对入侵事件的分析，组织相关人员对内部网计算机整改，防止黑客用同样的手段再次入侵其他系统。安全管理员检查确定无安全隐患后，才可将受攻击计算机重新连接网络，或启用备份计算机来恢复应用。

安全管理人员做好记录，保护现场，进行日志收集等工作。如果能追查到攻击者的相关信息，可以对其发出警告，必要时可以采取进一步的行动，乃至采取法律手段。根据破坏程度，经有关领导同意后，上报公安部门。

安全管理人员根据攻击行为或病毒爆发行特征，在校园网出口安全设备、行为管理设备、核心交换机、汇聚层交换机上建立相关访问控制条目，关闭相关端口通讯，以阻断病毒传播。

被入侵或感染病毒的服务器或计算机应在断网后检查操作系统、应用软件系统的漏洞，查杀病毒和木马，经清理整顿后，修改系统、应用、数据库等管理员的账号密码后，方可接入网络重新运行。

6.校园一卡通系统故障：服务器端出现故障后应立即与设备管理人员联系进行报修工作，同时迅速通知需要应用到校园一卡通系统的各个部门，包括后勤、图书馆、机房等。

关键硬件组件、操作系统、应用系统故障的：如重启无效，应立即联系相关管理人员、软硬件厂商维护人员对服务器及应用系统进行检查，同时，立即启动备份服务器，以最新的备份数据启动应用服务。服务器端运行后，通知需要应用到校园一卡通系统的各个部门，测试各应用端服务运行是否正常。

校园一卡通系统发生故障，导致其他应用系统不能正常工作时，如是可短时间暂停服务的，先暂停服务，待系统恢复正常后，再开始服务。

如是不可暂停的服务，其中：

餐厅 POS 机不能正常工作时，系统将由智能通讯控制器接管，迅速通知各餐厅说明情况，同时立即组织人员进行抢修。必要时对餐厅的所有 POS 机进行脱机工作，待系统恢复正常后，进行数据回收。当 POS 机无法进行脱机以及 UPS 电源故障时，迅速通知各餐厅准备备用菜票，或者临时性现金交易。

其他 POS 机不能正常工作时，则进行脱机工作，待系统恢复正常后，进行数据回收。

对接的应用系统，可进行手动操作的，暂时进行手动操作；需进行收费交易的，暂时进行现金交易。

（四）事后评估

在应急处置工作结束后，信息管理中心要迅速采取措施，

抓紧抢修，维护受损的基础设施，减少损失，尽快恢复正常工作。统计各种数据，查明原因，对事件造成的损失和影响以及恢复重建能力进行分析评估，认真制定恢复重建计划，并迅速组织实施，并将善后处置的有关情况上报上级领导。

信息管理中心将损失情况汇总统计后，根据具体情况制订设施、设备、软件、服务等项目的紧急采购方案上报学校负责采购的责任部门，由学校统一进行紧急采购。

应急处置领导小组就应急工作体系和工作机制存在的问题，修正和完善应急预案，提高应急处置能力。

（五）其他

本预案由校园网络与信息安全事件应急处置领导小组负责解释，自印发之日起施行。

第十一章　附　则

第六十九条　本制度适用于郑州医药健康职业学院内部各部门计算机信息系统。

第七十条　本制度根据时效性和适用性，定期评审，及时补充修改并记录（附件 1《管理制度评审记录》），逐渐完善。

第七十一条　本制度自印发之日起施行。

学校图书馆管理规定

为规范学校图书馆管理工作，更好地服务学校教育、教学和科研工作，发挥学校图书的最大效益，制定如下规定。

一、图书管理员要认真学习管理业务知识，做好图书管理工作，为教育教学服务。

二、图书管理员在新书到室后，要及时做好验收、登记、编目、排架等工作，以加速书刊资料的流通。

三、图书馆需建立图书总括登记、个别登记和注销登记三个账册，做到帐物相符。

四、图书馆要逐步实现自动化管理，建立图书和期刊数据库。利用网络实现网上查询、借阅、统计、账册打印等工作。

五、图书分类应使用国家标准《中国图书馆分类法》；期刊分类应使用《中国图书馆分类法期刊分类表》。图书著录应以国家标准《普通图书著录规则》为依据；期刊著录应以国家标准连续出版物著录规则为依据。

六、严格执行图书借阅制度。根据教学和学生的需要建议学校及时添置图书。

七、对于珍贵文献、资料要妥善保存，非经领导同意不得外借，对于破损书籍应及时修补，延长使用寿命。

八、做好图书室、阅览室卫生整洁工作，并督促读者保持室内安静。

九、认真制订书刊资料的选购标准，使之结构合理、复本量适当，不断提高藏书质量。对于内容陈旧、过时不宜流

通、借阅率不高、复本量过大和破损无法整修的图书要定期剔除，及时注销。

十、教工调离、学生休学、退学和毕业离校，均需主动还清全部书刊，并交回借书证，否则，不予办理离校手续。

教师阅览室管理规定

阅览室是广大教职工读书看报的场所，为保证阅览室的正常开放，特制定如下制度:

一、讲究卫生，不得在室内吃东西、随地吐痰、乱丢杂物。

二、爱护书刊，不准在书刊上乱涂乱画，损坏书刊的，照价赔偿。

三、书刊看完后，放回原处，摆放整齐。

四、保持室内安静，不准大声喧哗。

五、不准私自拿书刊离开阅览室，否则按偷窃论处。

六、管理人员必须按要求定期开放，每天做好书刊的清点工作，对室内所有书刊要登记入册，分类编号摆放整齐。

七、保持室内清洁，每天打扫一次。

学生阅览室阅览规定

为规范学生阅览室的管理，提高书刊的使用寿命，特制定如下制度。

一、学生持借阅卡均可进学生阅览室阅览。学生阅览室为开架阅览，每次限阅一本，取书时将借阅卡放在原书位置，阅览完毕，将书放回原处，取走借阅卡。

二、学生阅览室书、刊严禁携出室外，自带书、刊及书包等放在指定场所，不准带入室内。

三、遵守公共秩序，讲究文明礼貌。室内不得大声喧哗、打闹，保持安静。

四、保持室内清洁，不乱扔杂物，不随地吐痰，不在室内吃东西。

五、自觉爱护书刊，取放有序，不准任意涂抹、撕页，否则按有关规定给予处罚。

六、服从工作人员的管理，遵守阅览规则。

七、阅览室按时开放，满足学生阅览需要。

图书借阅规定

图书流通工作是图书馆日常工作的一个重要组成部分，直接关系到学校图书管理质量和效率，为规范此项工作，特制定如下制度:

一、图书馆对师生实行开架借阅，读者可先在学校内网上查询图书信息，记下索书号，然后再到图书馆借书。这样可避免盲目性，节约时间。

二、入室借书，个人物品不得带入书库。

三、工具书、大型成套书只供查阅，一般不予外借。

四、办借书手续之前，读者要仔细察看书中有无缺页和污损，如发现图书已有损坏，应及时告知图书管理人员。否则，还书时发现问题，由还书者承担一切责任。

五、学生凭借阅卡入室借书。每次可借 2 本，借期为 20 天。教师每次可借 10 本，所借图书非教学用书须在一个月内归还，教学用书学期结束归还。

六、对借书逾期不还者，视其时间长短，情节轻重给予批评教育或罚款甚至停止借阅。

七、爱护图书，保持图书的整洁、完好，不准在图书上标点、画线、涂改、撕剪或污损，妥善保管，以免遗失。如有违反，按有关规定给予处罚。

八、开架图书未办理借阅手续，不能以任何理由将图书携出室外，违者按偷窃处理。

九、借阅卡只供本人使用，不得转借，若有丢失，应立即到图书室挂失，如发现无冒借情况，可予补发。挂失前借出的图书由借者本人负责。

图书遗失和损坏赔偿规定

为切实加强学校图书资产的管理，保证书刊的广泛流通和图书资料的完整，特制定以下规定:

一、本馆借阅的图书、杂志、资料，必须严加爱护，不得卷折、涂写、答题、污损、撕页或遗失，如有发生按本规定处理。

二、遗失图书，原则上是以相同版的原书赔偿；如不能赔偿原版者，则由遗失者去校财务部门付款赔偿，凭收据注销借书记录。

（一）一般图书按现价的两倍赔偿；工具书按现价的三倍赔偿；其余使用价值高、不易购到的书籍，按现价的五倍赔偿。

（二）成套多卷本图书，如遗失其中一本或一本以上，则按整套图书现价的两倍赔偿。

三、污损图书按下列情况处理:

（一）损坏严重、影响图书内容完整及使用保存的图书，应购原版本书赔偿，无法偿还原书按本制度第二条规定处理。

（二）污损或损坏图书封面，一般图书赔偿 50 元；精装本图书赔偿 100 元。

（三）污损书刊内容，但不影响阅读和保存，按书刊原价的 10%-30%赔偿。

（四）污损书内的机读条形码，赔偿 50 元。

四、损坏图书已按原版书赔偿者，被损图书经注销后可归赔偿者所有；如无法购到原版图书而按损坏图书原价赔偿

者，则损坏图书归图书馆处理。

五、读者履行赔偿手续后，事后若能找回原书又无污损，可持收据去校财务部门退回赔偿费。

六、若故意污损图书者，除按本章制度赔偿外，视其情况提交校有关部门批评教育。

七、读者遗失书刊或污损书刊未照章赔偿前暂停图书借阅。

图书清点、剔除管理规定

随着科学技术的迅速发展，知识老化现象日益加速，为提高图书馆的藏书质量和工作效率，在藏书达到一定规模时，也要相应地剔除相当数量的旧书:

一、剔除范围:

（一）图书内容已陈旧过时的。

（二）流通率不高的。

（三）没有现实意义的。

（四）复本过多的。

（五）图书内容与本馆任务不相适应的。

（六）破烂不堪和残缺不全已没有参考价值的。

二、剔除的方法:

（一）根据图书借阅记录决定图书去留。

（二）把准备剔除的图书打印成清单，向学校师生征求意见，以达到兼听则明，防止片面性。

（三）将剔除的图书清单报校领导批准。

（四）在财产登记和目录上予以注销。

三、处理办法:

（一）组织交换，互通有无。

（二）组织调拨，支持基层。

（三）组织出售，削价处理。

（四）报废。

四、剔除总结:

每次图书剔除工作结束后，必须有书面小结，将剔除计

划、领导批示、剔除清单、处理情况、 处理日期、经办人等记录在案，存档备查。

附件：1.管理制度评审记录

2.项目交付培训记录表

3.出入机房登记表

4.物品出门证

5.机房基础设施巡检记录表

6.机房温湿度记录表

7.机房基础设施维护表

8.介质归档登记表

9.介质借用登记表

10.郑州医药健康职业学院校园网络入网申请表（个人）

11.应急预案培训记录

附件 1

管理制度评审记录

安全管理制度名称			
版本号		评审时间	
评审地点			
参加评审人员			
评审意见:			
分管领导意见: 签名 日期			

附件 2

项目交付培训记录表

培训时间		主讲	
培训地点		培训方式	
培训课题			
项目名称			
参加培训人员:			
培训内容:			
记录人		审核人	

附件 3

出入机房登记表

日期	姓名	单位	进机房时间	进机房原因	出机房时间	陪同人签字

附件 4

物品出门证

存根			
物品名称		数量	
带出人单位			
带出人姓名		联系电话	
批准人姓名		批准人部门	
备注:		信息管理中心 签章	

物品出门证			
物品名称		数量	
带出人单位			
带出人姓名		联系电话	
批准人姓名		批准人部门	
信息管理中心签章		备注:	

附件 5

机房基础设施巡检记录表

检查时间：　　年　　月　　日

检 查 项 目	检　查　情　况	异常情况记录
服务器	运行情况：□正常　　□异常	
数据库	运行情况：□正常　　□异常	
存储	运行情况：□正常　　□异常	
防火墙	运行情况：□正常　　□异常	
路由器	运行情况：□正常　　□异常	
核心交换机	运行情况：□正常　　□异常	
身份验证设备	运行情况：□正常　　□异常	
行为管理设备	运行情况：□正常　　□异常	
UPS 电源	运行情况：□正常　　□异常	
柴油发电机	运行情况：□正常　　□异常	
空调设备	运行：□正常　　□异常 送风：□正常　　□异常	
灭火器	情况：□正常　　□异常	
系统安全	高危漏洞□　低危漏洞□	
数据备份	是否可用□	

检查员签字：

附件 6

机房温湿度记录表

（　　年　　月）

适宜温度范围：　20℃ － 25℃　　相对湿度范围 ：　40 － 70 %

日期	温度	湿度	是否需要进行调整	记录员

附件 7

机房基础设施维护表

部门		时间	
维护设备名称			
设备故障原因:			
设备维护结果:			

维护人签名:　　日期:

附件 8

介质归档登记表

序号	介质名称	介质类型	存放位置	归档日期	介质管理员	备注

附件 9

介质借用登记表

序号	介质名称	数量	介质类型	使用目的	使用天数	借出时间	借出人签名	接收人签名	归还时间	归还人签名	接收人签名	备注

附件 10

郑州医药健康职业学院校园网络入网申请表（个人）

申请人姓名		所属部门	处（学院）
身份证号		联系电话	
用 户 名	（学生为学号，教工为姓名全拼）		

1. 个人用户凭身份证和郑州医药健康职业学院工作证或郑州医药健康职业学院学生证实名入校园网。
2. 用户自备并自主管理、维护入网用的终端设备及相应软硬件。
3. 校园网络用户可以按级别访问校园网络上的相应网络资源。
4. 网络用户必须遵守国家有关互联网络的法律法规和学校有关校园网络管理的规章制度，严禁任何危险校园网络安全的行为。
5. 用户必须妥善保管自己的账号和密码，自行承担账号被他人使用所造成的损失或影响。密码遗忘或被盗的用户可凭个人有效证件到网络中心申请密码修改。
6. 用户应当做好防毒防黑措施，网络中心有权将妨碍网络安全的计算机从校园网上断开。
7. 本表一式两份，用户与网络中心各持一份。

请选择相关服务：（在下面相应的“□”内打勾） 初始密码由网络中心填写

□ Internet 访问： 初始密码（ ）

8. 采用账户管理的方式，用户凭本人用户名和密码可以在任意一台校园网络接入计算机上访问 Internet。
9. 按学校相关文件规定采用“限额免费，超额收费”的计费方式。
10. 缴费：采取先缴费后使用的办法，用户账户余额为零或为负值时将无法登录计费服务器。用户可以到网络中心主页上查询本人的账户使用情况。
11. 任一账户同一时间内只能在一台校园网络接入计算机上使用。网络使用完毕应及时注销以停止计费。死机后应立即重启后进行注销操作。
12. 用户未经网络中心许可擅自出售、出让账号或建立代理服务利用自己的账号对他人提供网络服务的，网络中心有权终止服务，并有权追缴相关费用及追究相关责任。

用户同意上述条款签字：_____ ____年____月____日

网络中心意见：

□ 申请成功，将于一个工作日内开通服务。

□ 由于 _____申请失败。

工作人员签字：

年 月 日

附件 11

应急预案培训记录

培训名称			
培训时间		培训地点	
培训方式		使用资料	
主讲人		主办单位	
参加人员姓名			
培 训 内 容			