网络中心规章制度

安阳学院信息系统管理制度

一、为了保证本院信息系统的正常运行，完成系统各项应有功能，保证各系统数据、资料的安全性、有效性、完整性，特制定本管理制度。

二、学院任何单机版信息系统的使用、维护及系统数据的安全保护由本部门负责承担；学院其它网络版信息系统的使用、维护及系统数据安全保护由网络中心负责承担。相应部门必须有专人负责信息系统的使用、维护及安全保护。

三、为了各系统数据的安全性，运行信息系统的计算机原则上不得与因特网直接进行联接。特别需要提供远程网上查询的系统与因特网进行联接时应该有完善的安全防范办法，同时不得将原始数据直接与因特网联接。

四、信息系统的使用实行严格的权限分散管理制度。严禁任何非授权人员管理、操纵运行信息系统的计算机。信息系统的使用人员分为系统管理人员和应用人员，明确系统管理人员、应用人员的权限和操作范围。各信息系统的系统管理人员视本系统大小确定一个人或一个管理小组，人员名单由负责部门的主管推荐，并报经院长批准。应用人员名单及对相应信息系统的使用权限由使用该系统的部门主管确定，并报网络中心备案。

五、信息系统管理人员负责为应用人员分配系统的使用权限；并定期及时进行系统数据备份（本地备份和异地备份）；当

发生数据错误时，应该及时恢复；应该定期对所管理之信息系统的安全状况进行检查，发现问题及时处理。

六、信息系统管理人员应该熟悉本部门所使用信息系统的各项功能，熟练完成信息系统提供的各项功能，并能够及时排除软、硬件故障。信息系统应用人员应该熟悉本系统的各项功能，能够严格按照信息系统提供的功能正确进行操作，完成相关工作。

七、不得在运行信息系统的计算机上使用、浏览任何与系统无关的程序、游戏、文档等资料；不得使用任何不明来历的光盘、U 盘等外部存储设备；不得制造、复制、传播任何色情、暴力、迷信等有害资料及计算机病毒。

八、信息系统的管理和应用人员须做好各自系统软、硬件的防火、防水、防盗等安全工作。

九、信息系统的使用人员应对系统的各类数据、资料严格保密。如有违反规定泄漏学院机密者，按绩效考核制度从严惩处。

十、信息系统核心部分的技术人员调离时，必须移交全部技术手册、文档、资料；信息系统管理人员调离时，必须确认系统数据的有效性、完整性，并由接管人更换信息系统的有关口令和密钥。信息系统应用人员调离时，应移交有关的技术手册、文档、资料和相关业务。

十一、本制度适用于学院内的所有信息系统。

十二、本制度自发布之日起执行，修正时亦同。

安阳学院信息系统安全保密制度

信息系统的安全保密工作是保证数据信息安全的基础，同时给全校的信息安全保密工作提供了一个工作指导。为了加强我校信息系统的安全保密管理工作，根据上级要求，结合我校的实际情况，现制定如下制度。

第一章 总则

第一条 安阳学院校园网和各类信息系统的服务对象是学校教学、科研和管理机构，全校教职工和学生。

第二条 我校内任何部门及个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、社会、集体利益和个人的合法权益，不得从事违法犯罪活动。

第三条 未经批准，任何单位或个人不得将校园网及各类信息系统延伸至校外或将校外网络引入至校园内。未经批准，任何数据业务运营商或代理商不得擅自进入安阳学院内进行工程施工，开展因特网业务。

第四条 各部门应按照国家信息系统等级保护制度的相关法律法规、标准规范的要求，落实信息系统安全等级保护制度。

第五条 各部门要规范信息维护、信息管理、运行维护等方面的工作流程和机制，指定专人负责系统运行的日常工作，做好用户授权等管理服务工作。

第二章 数据安全

第六条 本制度中的数据是指各类信息系统所覆盖的所有数据，包括教务系统、财务系统、图书馆系统、一卡通系统以及学校网站等网站和系统的所有数据。

第七条 各部门要及时补充和更新管理系统的业务数据，确保数据的完整性、时效性和准确性。

第八条 保证各系统相关数据安全。各部门和系统管理人员，要对自己所管理的数据负责，保证数据安全，防止数据泄漏。

第九条 学校数据信息主要用于教学、科研、管理、生活服务等，申请数据获取的单位有义务保护数据的隐秘性，不得将数据信息用于申请用途外的活动。

第十条 未经批准，任何部门和个人不得擅自提供信息系统的内部数据。对于违反规定、非法披露、提供数据的单位和个人，应依照相关规定予以处罚。

第三章 信息安全

第十一条 任何部门和个人不得利用校园网及各系统制作、复制、传播和查阅下列信息：

（一）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。

（二）损害国家荣誉和利益的。

（三）煽动民族仇恨、民族歧视，破坏民族团结的。

（四）破坏国家宗教政策，宣扬邪教和封建迷信的。

（五）散布谣言，扰乱社会公共秩序，破坏国家稳定的。

（六）散步淫秽、色情、暴力、凶杀、恐怖或者教唆犯罪的。

（七）侮辱和诽谤他人，侵害他人合法权益的。

（八）含有国家法律和行政法规禁止的其他内容的。

（九）煽动抗拒、破坏宪法和法律、法规实施的。

第十二条 未经批准，任何个人和部门不能擅自发布、删除和改动学校网站和系统信息。凡发布信息，必须经过严格审核。

第十三条 校园网用户必须自觉配合国家和学校有关部门依法进行的监督、检查。用户若发现违法有害信息，有义务向学校有关部门报告。

第十四条 学校内部所有人员上网均需实名制，并执行严格的实名备案制度。一经发现上述本制度禁止信息，要尽快查处，情节严重者交由公安机关。

第四章 网站安全

第十五条 学校网站是学校的门户，学校网站信息安全是至关重要的。安阳学院网站已按照相关部门要求备案。

第十六条 凡上线网站，安阳学院实行网站备案，未经备案的网站，学校一律停止该网站的运行。

第十七条 各部门网站信息发布严格实行信息发布审核登记制度，发现有害信息，应当在保留有关原始记录后，及时予以删除，并在第一时间向学校办公室和网络中心报告。发现计算机犯罪案件，要立即向公安机关网警部门报案。

第十八条 学校办公室、网络中心负责对学校网站进行监督、检查。对于存在安全隐患的网站，网络中心有权停止其对外服务。

第五章 其他

第十九条 违反本管理规定的，视情节轻重采用以下其中一种或多种处理措施：

（一）批评整改。

（二）报相关部门领导处理。

（三）移交公安、司法部门处理。

第二十条 本规定由网络中心负责解释。

第二十一条 本规定自公布之日起生效。

网络中心

2017 年 9 月 28 日

安阳学院信息系统数据管理办法

第一章　总则

第一条 安阳学院信息系统数据作为学校的无形资产和战略资源，应纳入学校统一管理范畴，实现信息系统数据的统一管控，提高数据质量和数据的利用效率，提供安全、完整、统一的数据服务，为学校教学、科研、管理提供信息服务和技术保障。

第二条 本办法所指的信息系统与《中华人民共和国计算机信息系统安全保护条例》中的信息系统定义一致：由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。包括范围是：学校各类型的管理信息系统、网站、教学资源系统、用户服务系统等。

第三条 本办法所指的数据是指各类信息系统所覆盖的相关数据，包括但不限于：管理信息系统产生的业务数据、网站数据、教学资源（含多媒体视频、图片、课件等）、用户服务支持系统产生的数据。

第四条 信息系统数据管理是指利用信息系统对数据进行采集、录入、运维、存储、归档、应用的过程以及制定数据标准、数据安全策略和实施数据审核的管理。

第五条 信息系统数据管理应遵循以下原则：

（一）统一规范原则。信息系统采集和处理的数据，应符合信息系统所要求的特定数据标准。

（二）全程管控原则。建立数据从采集、处理到维护的全过程管控体系，重点把好数据的采集关，确保信息系统数据真实、准确、完整、及时。

（三）定期考评原则。相关业务部门对所管理的数据具有责任，对其权限范围内所负责的数据管理工作要进行定期的管理考评。

第六条 信息系统数据管理应达到如下目标：

（一）统一数据语言：要求数据管理有标准，即具备完善的数据标准管理规范，保证在系统建设过程中应用统一的数据标准。

（二）保障数据准确：在数据整个生命周期的各个环节建立完善的数据质量核查机制，制定完善的数据质量管理规范，确保数据的准确性。

（三）防止非法篡改和伪造：明确数据的所有权及更改权限，制定完善的数据所有权管理规范，确保对数据的所有更改均有据可查，对于不可更改的数据，应提供相应的安全技术防篡改和伪造。

（四）建立数据备份、容灾和恢复机制：建立数据的备份、容灾和恢复机制，加强数据存储和归档管理，制定完善的数据安全管理规范，确保所有数据有备份、可恢复。

（五）预防信息泄漏：根据国家和学校的要求，做好数据的保密工作，确保数据安全。

（六）提供数据服务：制定完善的数据服务管理规范，保证数据易获取、易应用，以充分发挥数据作为学校资产的价值。

第七条 数据分类和涉及部门，根据学校的职能域将数据划分为九大类：

（一）人力资源域：教职工基本信息管理、教职工招聘、入校离校、职称评审、职务聘任、考核管理、薪资管理、党团工作、出国管理、离退休管理等。涉及部门有人事处、外事办、党委办公室、各院(系)等。

（二）教学资源与管理域：教学计划管理、开课计划管理、排课管理、选课管理、成绩管理、学位管理等。涉及部门有：教务处、各院(系)等。

（三）学生管理域：招生管理、迎新管理、学生基本信息、学籍基本信息、学生奖惩管理、党团管理、毕业管理等。涉及部门有：招生就业处、学生处、教务处、校团委、党委办公室、图书馆等。

（四）科研管理域：项目管理、合同管理、成果管理、科研机构管理、科研经费管理等。涉及部门：教务处、财务处、各院(系)等。

（五）财务域：财务管理、经费管理等。涉及部门：财务处等。

（六）资产域：固定资产管理、实验室管理、设备管理、招投标管理、房产管理等。涉及部门：后勤处、财务处等。

（七）档案域：人事档案管理、学生档案管理、文件档案管理、科研档案管理等。涉及部门：人事处、教务处、学校办公室、各院(系)等。

（八）公共服务域：电子邮件服务、电子图书服务、校园一卡通服务等。涉及部门：网络中心、图书馆、财务处等。

（九）系统数据域：实现操作系统功能所涉及数据的管理、实现数据库管理系统功能所涉及数据的管理、实现应用软件系统功能所涉及数据的管理等。涉及部门：网络中心等。

第二章　数据管理角色及职责

第八条 学校数据管理部门包括网络中心、各行政处室、各分院（系部）与数据管理相关的有关部门或科室。学校数据管理部门根据数据管理的目标设置数据管理具体角色，包括总体规划、数据标准和规范的制定与执行、数据实施和运维、数据应用。

第九条 各类角色的职责是：

（一）总体规划的制定与执行：制定数据管理的战略规划和总体目标，由学校网络安全和信息化领导小组审批。承担部门：领导小组办公室。

（二）数据标准和规范的制定与执行：制定学校数据指标体系；制定学校的数据模型；制定和执行学校信息系统数据标准；制定和执行数据所有权管理规范；制定和执行数据安全规范；制定和执行数据服务管理规范；制定和执行数据质量核查机制。承担部门：网络中心。

（三）数据实施和运维的范围与执行：进行数据整合、数据分析、数据的采集与运维管理、存储、归档等。承担部门：各行政处室、各分院（系部）与数据管理相关的有关部门或科室。

（四）数据应用范围与执行：数据的日常应用和提供共享、利用服务等；承担部门：网络中心、各行政处室、各分院（系部）与数据管理相关的有关部门或科室。

第三章　数据采集、录入与审核

第十条 数据采集应遵循真实、完整、规范、及时的原则。

（一）真实：操作人员应准确录入相关数据，不得随意修改、增减。数据还必须得到权威部门的审核。

（二）完整：要按照各类应用子系统的有关要求进行数据采

集，保证数据齐全，避免数据的缺失。

（三）规范：数据采集应按照相关标准进行。

（四）及时：数据要在规定的时间内采集，确保数据与实际业务同步。

第十一条 学校数据管理部门应统一制定数据采集、录入、审核规范，并在进行数据采集、录入、审核时要求各业务职能部门严格按照规范操作，如果各业务职能部门在执行过程中遇到规范未涉及的问题，应及时向学校数据管理部门上报。

第十二条 在各类信息系统中，要严格按照规定进行岗位设置和授权，严格按照岗位权限进行操作。严禁在未按规定授权的情况下委托他人以本人的账户和密码进行有关的数据录入和修改。各系统用户应当定期更改自己的口令，确保数据安全。

第四章　数据运维管理

第十三条 数据运维管理是指学校各行政处室、各分院（系部）在业务操作过程中对系统中数据进行修正、补充、更新、删除等的管理。

第十四条 学校各行政处室、各分院（系部）应指定数据运维的负责人和接口人，在学校数据管理部门的指导和协助下，开展数据运维工作。

第十五条 学校各行政处室、各分院（系部）应在学校数据

管理部门的指导和协助下，结合本部门实际情况，制定数据运维规范，明确数据维护的权限和职责，制定数据维护的规程。凡是进入信息系统中的数据，应严格按照规程进行操作。

第十六条 学校数据管理部门应建立运维知识库，建立技术支持支撑平台。数据管理相关部门应及时研究数据运维过程中的问题，定期对系统中发现的各类问题进行分析，将经常出现的问题和解决方法分类汇总后予以发布，及时反馈给学校各行政处室、各分院（系部）的数据运维接口人员。

第十七条 学校数据管理部门建立数据监控中心，实时统计数据分析结果。以业务需求为驱动，建立技术与业务结合互动的数据分析和利用的长效工作机制，提供方便、快捷的分析、统计工具，加强数据监控，不断提高数据质量。

第十八条 学校数据管理部门建立数据运行平台，提高运行维护工作的实效。数据在系统运行中不可避免地遇见一些实际问题，需要建立统一的运行维护平台，及时、有效地进行信息的反馈和核查，确保信息系统数据运行和维护工作的有效性。

第十九条 学校数据管理部门制定数据在修正、补充、更新、删除时需要记录的审计日志规范，并将其作为信息系统的必须实现的功能。信息系统在记录审计日志的同时，应提供方便简捷的方式实现查询审计日志记录功能。审计记录的访问只能是被授权

的只读访问，任何人不得修改。

第五章　数据存储和归档

第二十条 学校数据管理部门负责保管信息系统产生的数据。

第二十一条 学校数据管理部门应当配备数据存储、管理、服务和安全等必要的软硬件设施，构建统一的数据管理系统，确保数据的完整性和安全。

第二十二条 学校数据管理部门应当按照相关规定建立数据备份制度，制定数据备份恢复方案的容灾系统，对重要数据实行异地备份。

第二十三条 学校数据管理部门应针对重大突发事件的特殊需求，建立数据加工、处理的技术储备与保障，为应急工作提供数据和技术支持。

第二十四条 学校数据管理部门应当配备专业技术人员，设定岗位，履行相关职责。

第二十五条 网络中心作为电子数据归档部门，应根据《电子文件归档与管理规范》（中华人民共和国国家标准GB/T18894-2002)、《电子公文归档管理暂行办法》（国家档案局第 6 号令)，建立数据归档以及归档后的数据查询、交换、复制和维护的管理制度，对电子数据实现有效归档和利用。

第六章　数据利用和服务

第二十六条 学校数据管理部门应建立相应的数据决策支持系统和分布式信息服务系统，提高数据的集成与应用水平，为学校领导提供决策支持服务，以及为社会提供相应的信息服务。

第二十七条 学校数据管理部门应制定数据服务管理和安全规范，明确定义数据服务的用户和提供服务的方式以及相关的安全管理规定。

第二十八条 外单位或外部信息系统需要利用或共享信息系统的数据时，需要出具书面申请文件和需求文档，并按照规定经过审批后，由学校数据管理部门提供。

第二十九条 未经批准，任何单位和个人不得擅自提供信息系统的内部数据。对于不能披露数据的利用和服务，数据管理部门应进一步制定相应办法予以明确。对于违反规定、非法披露、提供数据的单位和个人，应依照相关规定予以处罚。

第七章　数据安全管理

第三十条 信息系统数据保护是数据安全管理的中心内容，主要指对信息系统用户数据（包括业务数据和系统数据）及安全功能数据的机密性、安全性和可用性的保护。

第三十一条 学校对信息系统数据实施统一安全管理策略，具体包括行政管理和技术管理等两方面。行政管理主要包括安全

管理机构、制度、人员、责任和监督机制等内容。技术管理贯串信息系统建设、运行和维护的各环节，如开发、试用、验收和推广各阶段上的安全管理，设备网络特别是保密设备和密钥的安全管理等。

第三十二条 学校数据管理部门应根据信息安全等级保护要求对数据建立相关的流程和制定相应的管理制度，信息系统应严格在流程管理和制度管理的约束下实施。

第三十三条 学校数据管理部门应制定介质管理制度，对存储一般数据介质（特别是移动介质）应加强存放管理，对存储关键数据或敏感数据介质应实施全生命周期管理(包括存放、使用、传输、销毁等)。

第八章　奖惩

第三十四条 学校制定相应的奖励制度，对学校改进信息系统安全作出显著贡献的个人或集体进行表彰或奖励。

第三十五条 对于违反本办法造成损失的单位或个人，视情节轻重予以相应行政处分。

第三十六条 对于有危害公共安全、国家安全、泄露国家秘密以及其他违反法律、法规和规章规定行为的，由公安、国家安全、保密以及其他监督管理部门依法处理；构成犯罪的，依法追究刑事责任。

第九章　附则

第三十七条 本办法解释权归学校网络安全和信息化领导小组办公室所有。

第三十八条 本办法自发布之日起施行。

网络中心

2017 年 9 月 28 日

安阳学院数据信息保密制度

随着网络不断进步与发展，数据信息中心机房的重要数据安全保密已成为高校信息化建设的重要工作。因此为保障我校网络中心数据保密及安全管理，特制本制度：

1、明确网络中心工作职能，落实工作责任。进出中心机房执行严格记录，中心机房管理人员对中心机房综合环境每日监测。并对中心机房中应用系统使用、产生的介质或数据按其重要性进行分类，对存放有重要数据的介质，应备份必要份数，并分别存放在不同的安全地方，做好防火、防高温、防震、防磁、防静电及防盗工作，建立严格的安全保密保管制度。

2、做好机房内重要数据(介质)的安全保密工作。保留在机房内的重要数据(介质)，应为系统有效运行所必需的最少数量，除此之外不应保留在机房内。对入网（公网、专网）PC 机（网卡、IP、硬盘）必须进行登记、定期升级杀毒软件，使用前先进行病毒和恶意软件扫描再进行操作的流程。

3、根据数据的保密规定和用途，确定使用人员的存取权限、存取方式和审批手续。

4、重要数据(介质)库，应设专人负责登记保管，未经批准，不得随意挪用重要数据(介质)。

5、在使用重要数据(介质)期间，应严格按国家保密规定控制转借或复制，需要使用或复制的须经批准。

6、对所有重要数据(介质)应定期检查，要考虑介质的安全保存期限，及时更新复制。损坏、废弃或过时的重要数据(介质)应由专人负责消磁处理,秘密级以上的重要数据(介质)在过保密期或废弃不用时，要及时销毁。

7、机密数据处理作业结束时，应及时清除存储器、联机磁带、磁盘及其它介质上有关作业的程序和数据。

8、机密级及以上秘密信息存储设备不得并入互联网。重要数据不得外泄，重要数据的输入及修改应由专人来完成。重要数据的打印输出及外存介质应存放在安全的地方,打印出的废纸应及时销毁。

9、门户网站公开信息必须执行分级审核录入、安全运行的管理制度。

10、在实际工作中不断完善制度，以有效的对局域网进行监测，以防止保密数据流入公网，造成不必要的损失。保障网络的畅通,所录入的数据合法有效,防止数据非法篡改,病毒攻击等。确保我校中心数据库平稳运行。

安阳学院信息系统账号管理规定

第一章 总则

第一条 为加强我校信息系统用户账号和权限的规范化管理，确保各信息系统安全、有序、稳定运行，防范应用风险，特制定本制度。

第二条 本制度适用于我校各类信息系统，以及以用户密码方式登录的服务器、网络设备、网站系统等。

第三条 信息系统用户、角色、权限的划分和制定，以各部门的部门职能定位和各部门内部分工为依据。

第四条 信息系统用户和权限管理的基本原则是：

（一）用户、权限和密码设置由网络中心系统管理员全面负责。

（二）用户、权限和密码管理必须作为我校系统账号管理的强制性要求。

（三）用户、权限和密码管理采用实名制管理模式。

（四）严禁杜绝一人多账号登记注册。

第二章 管理职责

第五条 系统管理员职责

系统管理员由网络中心指派专人担任，主要负责本级用户管

理以及对下一级系统管理员管理。包括创建各类申请用户、用户有效性管理、为用户分配经授权批准使用的业务系统、为业务管理员提供用户授权管理的操作培训和技术指导。

第六条 业务管理员职责

业务管理员以各部门内部分工为依据指派专人担任部门业务管理员，负责本级本业务系统角色制定、本级用户授权及下一级本业务系统业务管理员管理。负责将上级创建的角色或自身创建的角色授予相应的本级用户和下一级业务管理员，为本业务系统用户提供操作培训和技术指导，使其有权限实施相应业务信息管理活动。

第七条 用户职责

用户必须严格管理自己用户名和密码，遵守保密性原则，除获得授权或另有规定外，不能将收集的个人信息向任何第三方泄露或公开。系统内所有用户信息必须采用真实信息，实名制登记。

第三章 用户管理

第八条 用户申请和创建

（一）申请人在《安阳学院各级管理员变更申请表》上填写基本情况，提交本部门负责人。

（二）部门负责人确认申请业务用户的身份权限，并在《安阳学院各级管理员变更申请表》上签字确认。

（三）网络中心主任进行审批后，由系统管理员和业务管理员创建用户或者变更权限。

（四）系统管理员和业务管理员将创建的用户名、密码告知申请人本人，并要求申请人及时变更密码；

（五）系统管理员和业务管理员将《安阳学院各级管理员变更申请表》存档管理，系统管理员保留原件，业务管理员保留复印件。

第九条 用户变更和停用

（一）部门主管确认此业务用户角色权限或变更原因，并在《安阳学院各级管理员变更申请表》上签字确认。

（二）网络中心主任进行审批后，由系统管理员和业务管理员执行用户变更和停用操作。

（三）系统管理员变更，应及时向上级系统管理员报告，并核对其账户信息、密码以及当时系统中的各类用户信息及文档，核查无误后方可进行工作交接。新旧管理员填写《安阳学院各级管理员变更申请表》完成领导审批程序后，新任系统管理员应及时变更账户信息及密码。

（四）业务管理员变更，应及时向本级系统管理员及上级业务管理员报告，新旧业务管理员填写《安阳学院各级管理员变更申请表》完成领导审批程序后，上级业务管理员和系统管理员及

时变更业务管理员信息。

（五）用户注销，用户因工作岗位变动，调动、离职等原因导致使用权限发生变化或需要注销其分配账号时，应填写《安阳学院各级管理员变更申请表》，按照用户账号停用的相关流程办理，有系统管理员和业务管理员对其权限进行注销。

第四章 安全管理

第十条 使用各信息系统应严格执行国家有关法律、法规，遵守学校的各项规章制度。

第十一条 密码管理

（一）系统管理员创建用户时，应为其分配独立的初始密码，并单独告知申请人。

（二）用户在初次使用系统时，应立即更改初始密码。

（三）用户要严格按照《安阳学院密码管理制度》执行密码管理工作。

（四）用户不得将账户、密码泄露给他人。

第十二条 账号审计

账号审计工作有网络中心系统管理员进行审计，并应定期向其领导进行汇报，由网络中心领导定期和不定期检查。

第十三条 应急管理

（一）用户及业务管理员账户信息泄露遗失

用户及业务管理员账户信息泄露遗失时，应在 24 小时内通知本级系统管理员。本级系统管理员在查明情况前，应暂停该用户的使用权限，并同时对该账户所报数据进行核查，待确认没有造成对相关数据的破坏后，通过修改密码，恢复该账户的报告权限，同时保留书面情况记录。

（二）系统管理员账户信息泄露遗失

系统管理员账户信息泄露遗失时，应立即向上级系统管理员报告，暂停其系统管理员账户权限，同时对系统账户管理及数据安全进行核查，采取必要的补救措施，在最终确认系统安全后，方可恢复其系统管理员账户功能。

第五章 附则

第十四条 本制度由网络中心负责制定、修改和解释。

第十五条 本办法自发布之日起施行。

网络中心

2017 年 9 月 28 日

安阳学院密码管理制度

为加强对学校密码安全工作的管理，完善学校密码管理体系，提高学校服务器、信息系统的安全性，根据国家相关法律法规及学校关于密码安全管理工作的相关规定，特制定本管理制度。

一、各单位保管的信息系统账号和密码要专人专管不得转借他人使用。为了避免账号被盗，要求密码长度不少于6位，密码规则采用字符、数字与符号密码组合使用，密码每三个月更换一次，并详细填写《安阳学院密码更新记录表》。

二、如果用户密码忘记，需用户本人亲自向网络中心提出恢复密码的申请，网络中心负责做好相关密码恢复记录。

三、服务器和服务器数据库超级用户必须设置密码，系统管理员严格保管数据库和服务器的登录密码。

四、服务器和数据库的超级用户密码设置位数必须大于 10 位。服务器密码由网络中心服务器管理员定期更换，服务器超级用户密码大于 10 位两个月更换一次，数据库超级用户密码大于 10 位设置好后不做更换，系统管理员密码大于 6 位三个月更换一次，并详细填写《安阳学院密码更新记录表》。

五、各单位密码管理人员要严格执行密码管理规定，要定期做好密码更新工作并做好详细记录，任何密码不得外泄，如有因密码外泄造成的各种损失，由当事人负全部责任。

六、网络中心有监督检查的责任，会不定期进行抽查，每学期不少于二次，并做好详细记录。

七、本规定自发布之日起实施。

安阳学院密码管理规定

为确保网络安全运行，保护拥护权益不受侵害，特制订此规定。

一、密码的设置：

1、服务器的密码，由网络管理中心负责人和系统管理员商议确定，必须两人同时在场设定。

2、服务器的密码须网络管理中心负责人在场时要由系统管理员记录封存。

3、密码内容设置规则：必须由数字、字符和特殊字符组成；密码长度不能少于 8 个字符；机密级计算机设置的密码长度不得少于 10 个字符；设置密码时应尽量避开有规律、易破译的数字或字符组合作为自己的密码。

4、密码要定期更换:一般服务器密码更换周期不得多于 30 天；重要服务器密码更换周期不得超过 7 天.

5、重要服务器需要分别设置 BIOS、操作系统开机登录和屏幕保护三个密码。

二、密码和口令的保存

1、中心服务器设置的用户密码由系统管理员自行保存，严禁将自用密码转告他人；若工作需要必须转告，应请示上级领导批示；非系统管理员使用密码完成工作后，系统管理员应该及时更改密码，保证密码安全。

2、中心服务器所有设置的用户密码须登记造册，由系统管理员管理保存，并将备案记录交于网络管理中心负责人封存。

3、密码更换后系统管理员需将新密码或口令记录登记封存。

4、如发现密码有泄密迹象或黑客入侵，系统管理员要立刻报告网络管理中心负责人，网络管理中心负责人应及时与系统管理员商定修改密码，并严查泄密源头修补系统漏洞，将详细情况以书面形式上报上一级领导。

安阳学院信息化人员保密协议书

甲方（主管单位）：安阳学院

乙方（信息管理员）：

根据《根据中华人民共和国保密法》、《中华人民共和国网络安全法》以及其它相关法律法规规定，甲方因为工作关系向乙方提供电脑和网络系统，乙方在保守信息系统秘密的基础上，不得利用甲方提供的计算机和网络等信息技术、设备进行违反网络安全的活动，并接受甲方监管，据此双方签订本协议。

第一条 保密内容约定

一、学院信息系统涉及到的保密信息包括（但不限于）以下内容：用户信息、平台技术信息、网络拓扑信息、通讯协议信息、登陆用户名与密码等其它的相关联的系统信息；

二、上述保密信息可以以数据、文字及记录在上述内容的文档、光盘、软件、图书等有形介质体现，也可通过口头等视听方式传递。

第二条 甲方责任及义务

一、提供工作需要的计算机、网络、信息系统等其它现代信息技术设施设备与工作环境；

二、慎重听取来自相关各级部门关于网络安全与信息化的有益建议和提出的问题并认真研讨，做出工作指示；

三、行使主管单位工作范围内的其它一切管理权力。

四、不定期巡查监管全校系统管理员的工作行为与工作状态，发现问题及时纠正；

五、及时发送国家各级网络安全与信息化相关安全要求与注意事项；

六、定期对信息系统管理员进行网络安全与信息化相关培训；

七、定期向学校汇报网络安全与信息化工作情况。

第三条 网络安全与信息系统保密责任及义务

一、乙方应当时刻提高保密意识，做好保密工作，具体内容包括：

（一）保证该保密信息仅用于与学校有关的用途，不得将涉及学校保密的信息用于学校项目以外的任何用途，除为执行学校项目目的外，不得对保密信息进行复制，对外泄漏，未经学校同意也不得利用保密信息进行新的研究；

（二）保证对保密信息予以妥善保管，不得与单位业务无关的任何人通过任何渠道谈论和传播保密信息，并对保密信息在工作期间发生的非技术原因失密事故承担相关责任；

（三）未经学校授权，不得将该承诺书所涉及的各项安全信息保存在非学校所属（如外部云存储网络空间）的个人网络存储空间之中；

（四）因退休、离职、转岗等原因离开系统管理员岗位时，

应及时将承载保密信息的介质原件及复印件全部返还学校，最迟不得超过学校规定日期；

（五）离岗后不得将各种涉及学校信息系统的安全信息对外泄漏，否则，学校保留追究泄密损失的权利。

二、乙方承诺不利用甲方提供的信息系统，网络和技术设备制作、复制、发布、转载、传播含有下列内容的信息与行为：

（一）违反宪法基本原则的；

（二）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；

（三）损害国家荣誉和利益的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）破坏国家宗教政策，宣扬邪教和封建迷信活动的；

（六）散布谣言，扰乱社会秩序，破坏社会稳定的；

（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或教唆犯罪的；

（八）侮辱或者诽谤他人，侵害他人权益的；

（九）造谣滋事、煽动偏激情绪、制造恐慌气氛，扰乱正常工作秩序的；

（十）包含法律法规禁止的其它内容；

（十一）发送垃圾邮件，攻击其它网络和计算机系统，传播计算机病毒，以及其它危害互联网安全的行为。

第四条　违约责任

乙方违反本协议中的任何规定，甲方有权行使以下权利：

一、责令乙方停止违反协议约定行为；

二、视情节处以扣罚奖金或者其它纪律处分、行政处分直至开除；

三、要求乙方赔偿其违反协议约定行为而导致的一切经济损失及其可能的寻求法律途径过程中产生的一切费用；

四、触犯法律的，请有关部门追究其法律责任。

甲方（盖章）：　　乙方（签名）：

年　月　日　　年　月　日

安阳学院校园计算机网络管理规定

一、为了加强安阳学院校园计算机网络(以下简称校园网络)的运行和管理，确保网络安全、可靠、稳定地运行，促进校园网络的健康发展，依照《中华人民共和国计算机信息网络国际联网管理暂行规定》和国家教育部的有关规定，特制定本管理暂行规定。

二、校园网络是为全校教学、科研和行政管理建立的计算机信息网络，其目的是利用先进实用的计算机技术和网络通信技术，实现校内计算机互联、计算机局域网互联，提供院内公共信息交换平台，并通过中国教育和科研计算机网(CERNET)与国际互联网络(Internet)互联，实现信息的快捷沟通和资源共享。其服务对象主要是全校各学院、部、处、室、实验室和广大师生。

三、网络中心负责校园网络（包含运营商合作共建）全面规划、建设、运行、管理和发展并负责学院网站的建设、管理和维护任务。

四、校园网络的所有设备，包括光缆、布线设施及其附属配件、路由器和交换机等由网络中心进行统一规划管理，各入网单位和个人应加以爱护，发现问题应及时报告网络中心。网络中心负责网络的运行管理、设备管理和规划建设，保证网络的畅通。

五、各入网单位用户及个人用户负责在网络中心的统一规划和指导下，按有关要求和规定进行本单位联网设备的建设、运行

和管理。网络中心有责任协助、指导和监督各单位的网络建设并使其接入主干网运行。各单位的服务器等主要信息点经网络中心配置、调试后，方可入网运行。对于不符合要求的，网络中心有权拒绝其加入主干网。

六、上网单位和个人应当遵守国家有关法律、行政法规，严格执行安全保密制度。对在网上公开发布的信息要进行保密审查，对重要部门和信息应制定周全的保密措施，严格控制访问人员的范围和权限，定期更换密钥。禁止以普通信息形式在网上发送涉密文件和数据。确有必要发送这类信息时，需作加密处理。违规者按本院教师和职员考核办法论处。

七、需要入网的单位和个人应向网络中心提交入网申请，经批准之后方可接入主干网；未经批准，入网单位和个人不得私自扩充下级子网或与校外单位联网，不得私自发展校外用户，严禁利用校园网络从事危害国家安全、泄露国家机密等违法犯罪活动。不得制作、查阅、复制和传播妨碍社会治安的信息和淫秽色情等信息，不得利用校园网络开展商业性活动，此类事情一经发现，立即解聘，并向有关部门报告追究其法律责任。

八、严格控制和防范计算机病毒对校园网络的侵袭。上网单位和个人应定期对计算机进行病毒检查，所有拟在上网计算机上使用的U盘等存储介质都必须经过病毒检查。禁止下载来路不明的网上免费软件，以防止计算机病毒传入。如发现计算机病毒应及时将染毒计算机与校园网络断开并向网络中心报告，违者按申

诫论处。

九、IP 地址是宝贵的网络资源，全校网络 IP 地址由网络中心负责统一管理和分配。入网单位和个人应向网络中心申请分配或增加 IP 地址。入网单位和个人应严格使用由网络中心所分配的 IP 地址，不得盗用他人 IP 地址或私自乱设 IP 地址。网络中心有权切断非法的 IP 地址入网，以保证校园网络的正常运行。

十、用户计算机要求入网和个人要求办理其他信息系统帐户，应先提出申请，经有关部门主管批准后，由网络中心对入网计算机和用户进行登记，分配 IP 地址，在有关系统上开户并备案，办理有关手续。网络中心负责审查和监督，符合要求的计算机和用户方可入网运行、对外通信。

十一、除网络中心外，其他单位和个人未经批准不得在校园网络上设立任何公开的信息站点。确需设立公共文件服务器或 Web 服务器等信息服务站点的单位，应事先向网络中心提出申请，指定专人负责，经审查批准后方可设立运行，并接受网络中心的监督。所提供的信息只能限于学术交流范畴，不得涉及政治或违反知识产权的内容，违者按申诫论处。

十二、任何单位和个人都不得在校园网络上设立游戏站点或纯娱乐性的、与校园网络宗旨相悖的站点。一经发现，网络中心有权将其从校园网络上隔离出去，违者按申诫论处。

十三、网络中心和各入网单位要定期对相应的网络用户进行有关的信息安全和网络安全教育，并根据国家有关规定对上网信

息进行检查。发现问题应及时上报，并采取处理措施。

十四、网络中心、入网单位和个人必须接受并配合国家和学院有关部门依法进行的监督检查。

十五、对于任何破坏网络设备，盗用 IP 地址，盗用他人口令、入侵和破坏网络及计算机系统的行为，给予记过处分。

十六、本规定由网络中心负责解释。

十七、本规定自公布之日起实施，修正时亦同。

安阳学院互联网教室上网管理规则

一、为便于上网登记管理，上网的学生必须携带学生证、校园卡。

二、进入机房后要对号入座，不得私自同他人调换座位，有问题举手提问，不得随便走动，必须保持机房的安静整洁，不准喧哗、嬉戏及乱扔纸屑，严禁吸烟。严禁把所带物品放到电脑旁边。否则按有关规定做相应处理。

三、爱护设备及公物，上机前应检查该座位设备有无损坏或丢失，有问题及时上报管理员。上机期间须轻敲键盘、鼠标。未经许可严禁私自移动机房内的任何设备及物品，不得私自改变系统设定、硬件配置及终端设备。若造成损坏的按物品的市场价格进行赔偿。

四、严禁携带易燃易爆和强磁物品及其它与机房工作无关的物品进入机房。

五、不准携带移动存储硬盘、光盘进入机房。

六、授课教师或管理员应维持上机秩序，学生严禁做玩游戏、聊 QQ 等与上机无关的事情。

七、不准乱下载文件，以防机器感染病毒。

八、不准私设开机和屏幕保护密码。不准更改 WINDOWS 的桌面和系统设置。

九、不准删除系统文件或应用程序。

十、不准私自拆开机箱，更不准插拔电脑各个部件及拆开电源。发现鼠标、键盘不好用报告管理员处理，不得私自调换。

十一、上网学生不得有以下行为，如有违反规定，一经发现，将严肃处理：

（一）煽动抗拒、破坏国家宪法和法律实施；

（二）煽动民族、种族歧视或仇视、破坏民族团结；

（三）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪和有害青少年身心健康等；

（四）造谣惑众、诽谤或侮辱他人；

（五）损害各级政府机构的公众信誉；

（六）故意传播计算机病毒等破坏性程序；

（七）窃取、泄露政治、军事、经济、科技等国家秘密；

（八）进行其它损害国家利益、危害社会安全、影响社会稳定的行为；

（九）禁止利用电子公告板（BBS）或通过电子函件（Email）传播含有反动、色情内容的有害信息，禁止传播涉及有害信息的网址；

（十）损害学院声誉、影响学院安全稳定。

十二、本规则自公布之日起实施，修正时亦同。

安阳学院办公用计算机管理办法

为了加强学院各部门办公用计算机的分配和管理，提高电脑的使用效率，有效地发挥其在管理、教学、科研方面的功能，利于学院的办公自动化建设，同时也为了更好地维护学院的固定资产，根据我院的实际情况，特制定本办法。

一、办公计算机的使用规定

（一）计算机为学院固定资产，在各部门使用时应由专人负责管理。

（二）办公用计算机（如辅导员、教研室共用的计算机）应放置在独立的办公区域，方便各办公人员使用，不能私自挪为己用。

（三）办公计算机为工作之所用，任何人在工作时间不得用它来做与工作无关的事，（如：浏览不健康网站、安装与工作无关的软件、聊天、玩游戏、看电影）。

（四）办公计算机应正确使用，请勿使用来路不明的磁盘片（如移动硬盘、优盘、软盘、光盘等）；自行携带的磁盘片应在使用前先杀毒再使用。各计算机使用人员应该定期升级杀毒软件。

（五）严禁私自拆卸计算机，调换配件，违者将按照学院考核制度执行，若造成损坏，按照《实验室仪器设备器材损坏丢失

赔偿处理办法》赔偿。计算机使用过程中如出现故障需要维修时，请与网络中心人员联系。

（六）保持计算机的清洁，并做好防尘、防水、防雷电等其他维护保养工作。

（七）及时做好重要文件的备份，重要资料不要存在C盘（系统盘）内，以免计算机系统故障而造成数据的丢失。

（八）下班时要正确关闭计算机及显示器电源。并做好防盗工作，下班时及办公室无人值守时应将锁好门窗.如发现失窃，应保护好现场，应及时通知保卫处。

（九）办公用计算机使用时应遵守我院《安阳学院校园计算机网络管理规定》、《安阳学院信息系统安全管理规定》。

二、各系部办公用计算机配备原则

（一）分院主任、副书记、教学秘书各配计算机一台；

（二）各分院辅导员按学生处规定配发计算机；

（三）各分院每教研室配一台；

（四）研究生及副教授以上教师的办公用计算机配备按人事处有关文件执行；新聘人员如人事处规定配发计算机的按人事处规定执行；

三、各行政单位办公用计算机配备原则

各院级领导、行政一级主管、科级人员按每人一台计算机配备；其他人员原则上按每两人一台配备，特殊情况的可根据工作需要另行申请配备。

四、办公用计算机的管理

（一）除外教、研究生所配的专用计算机外，各行政及教学部门所配的办公用计算机应指派专人负责管理，包括办理领用、报修及报废手续等，计算机实际的使用人可到管理人处登记。计算机不得带出办公室等公共场所使用。

（二）研究生及一些副教授以上人员所配发的专用计算机属学院一次性配发，计算机仍为学院公有资产，使用人拥有在职期间的使用权。使用期间如因各人原因导致计算机故障应由使用人负责，其他非人为原因的计算机问题应及时与网络中心联系解决。使用人离职时应交回原计算机，交回的计算机应能正常使用。

（三）外教所配发的专用计算机由外事办负责统一领用，并指派专人管理。

（四）计算机日常的维护由使用人负责。

（五）办公用计算机在领用时管理人应保存好随机资料和保修卡，在交还时或转帐时应将随机资料和保修卡一起交还。

五、办公用计算机的维修

（一）办公用计算机如果在使用时出现故障，直接与网络中心维修人员联系。

（二）网络中心维修方式：

1、上门维修，或送到网络中心维修。约定好地点和时间，方便及时有效的排除故障；

2、对于网络中心解决不了的故障，及时跟网络中心负责人

联系申请维修。

六、办公用计算机的报废

（一）对符合以下标准的办公用计算机可申请报废。

1、使用年限已超过六年的；

2、无法维修或多次维修仍然不能正常使用，且没有维修价值的。（二）办公用计算机的报废按学院物品管理办法中甲类物品的报废办法执行，在报废时，需经网络中心和保管室鉴定，部门主管领导同意，院领导批准后方可生效。报废的计算机应统一交回保管室处理。

七、本规定自批准之日起执行

安阳学院办公计算机上网管理规定

为了保证校园网的安全和运行通畅，加强对办公计算机上网的管理，根据教育厅有关文件精神，特制订本规定。

一、办公计算机上网人员必须遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中国教育和科研计算机网络管理办法》和国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。

二、办公机使用者不得利用计算机网络从事危害国家安全、破坏社会安定的违法犯罪活动，不得查阅、发布各种有害信息。

三、办公机使用者有义务配合国家安全部门依法对网络使用情况等进行监督检查。

四、任何办公机使用者未经许可不得在网上进行商业和其他任何盈利性活动。

五、办公机使用者不得进行任何干扰其他网络用户，破坏网络设施的活动。这些活动包括(但并不限于)商业公告、散布计算机病毒、进入未经授权的计算机系统、盗用非法的 IP 地址入网等等。

六、办公机使用者有义务向网络管理员报告任何违反办公机使用者上网规定的行为，并对自己在网络使用中的行为负责。

七、对被动收到的不良信息，应及时予以删除，严禁扩散，同时应及时报告网络管理员和学院有关管理部门，并协助删除。

八、入网用户要认真填写《校园网新增信息点审批表》。

九、严禁私拉网线，严禁私用交换机及所有影响网络正常运行的设备。

十、严禁私自更改网络中心分配的 IP 地址及网关等，如出现冲突情况或网络出现其他问题请及时将信息反馈给网络中心，以便及时解决问题。

十一、入网的机器必须安装杀毒软件和防火墙，并及时升级。如有技术问题可与网络中心联系协助解决。

十二、不得在互联网上发表反动、不健康的言论，不得上不健康的网站，做到安全、文明、健康、守法上网。

十三、上班时间不得利用网络做与工作无关的事情，不准在计算机上聊天、玩游戏等。

十四、不得用软件进行网络扫描，不得利用黑客软件攻击其它电脑。

十五、上网用户对上网行为负责。如有违反，网络管理员有权停止对其的服务，情节严重者移交学院或公安机关处理。

校园网新增信息点审批表

填表日期　　年　　月　　日

申请单位		联系电话	
使用地点		IP 地址	
申请人签字		单位负责人签字	
申请单位公章	单位主管领导意见 年 月 日	分管副院长意见 年 月 日	网络中心审核意见 年 月 日
注：1. 表格由申请人亲自填写，领导签字后方可来网络中心办理。 2. 需要交换机、网线等其它设备，必须另写申请。			

安阳学院校园网安全管理制度

一、总则

（一）为了保护校园网的安全、促进我院计算机网络的应用和发展、保证校园网的正常运行和网络用户的使用权益，根据有关网络安全的法律和规定，特制定本安全管理制度。

（二）本管理制度所称的校园网系统，是指由学院出资购买、由网络中心负责维护和管理的校园网络主、辅节点设备、配套的网络线缆设施及网络服务器、工作站所构成的、为校园网络应用及服务的硬件、软件的集成系统。

（三）校园网系统的安全运行和系统设备管理维护工作由网络中心负责，网络中心可以委托相关单位指定人员代为管理子节点设备。任何单位和个人，未经同意、不得擅自安装、拆卸或改变网络设备。

（四）任何单位和个人、不得利用联网计算机从事危害校园网及本地局域网服务器、工作站的活动，不得危害或侵入未授权的（包括其它互联网在内的）服务器、工作站。

二、网络安全

（一）校园网主要设备和系统由网络中心负责维护管理，分散在各部门的网络设备由各部门网络管理员（兼职）协同网络中心管理。

（二）需增加接入或变更接入我校校园网的任何服务器或工作站需向网络中心提出申请，领取网线并按网络中心指定的网络地址连接入网。

（三）各用户局域网 IP 地址，未经网络中心同意不得擅自变更。

（四）校园网各类服务器开设的帐号和口令为个人用户所拥有，网络中心对用户口令保密，不得向任何单位和个人提供这些信息。

（五）网络用户不得利用各种网络设备或软件技术从事用户帐号及口令的侦听、盗用活动。

（六）校园内从事施工、建设，不得危害计算机网络系统的安全，确需移动线缆者，应先征得网络中心同意。施工后要及时恢复。

（七）除网络中心，其他单位或个人不得以任何方式试图登陆进入校园网主、辅节点、服务器等设备进行修改、设置、删除等操作；任何单位和个人不得以任何借口盗窃、破坏网络设施。

（八）校园网主、辅节点设备及服务器等发生案件、以及遭到黑客攻击后，网络中心必须在二十四小时内向保卫处及公安机关报告。

（九）严禁在校园网上使用来历不明、引发病毒传染的软件；对于来历不明的可能引起计算机病毒的软件应使用杀毒软件检查、杀毒。

（十）校园网中对外发布信息的 WWW 服务器中的内容必须经各单位领导审核，学院主页上公共信息及新闻由学院院办负责收集、整理、审核和制作上传。

（十一）如发现有以下行为的，将保留有关原始记录，在二十四小时内向当地公安机关报告：

1、煽动抗拒、破坏宪法和法律、行政法规实施。

2、煽动颠覆国家政权，推翻社会主义制度。

3、煽动分裂国家、破坏国家统一。

4、煽动民族仇恨、民族歧视、破坏民族团结。

5、捏造或者歪曲事实、散布谣言，扰乱社会秩序。

6、宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪。

7、公然侮辱他人或者捏造事实诽谤他人。

8、损害国家机关信誉。

9、其他违反宪法和法律、行政法规。

10、有损学院声誉的信息。

（十二）对所有联网计算机及上网人员要及时、准确登记备案。多人共用计算机上网的各级行政单位、教学业务单位上网计算机的使用要严格管理，部门负责人为网络安全负责人。学院公

共机房不准对社会开放，上网人员必须出示学生证、教师证，机房工作人员记录上网人员身份和上下网时间、机号。公共机房使用网络的记录要保留一年。

（十三)网络中心必须落实各项管理制度和技术规范,监控、封堵、清除网上有害信息。为了有效地防范网上非法活动，校园网要统一出口管理、统一用户管理，进出校园网访问信息的所有用户必须使用网络中心设立的代理服务器、Email 服务器等。未经网络中心同意及校领导批准，各单位一律不得开设代理服务器、Email 服务器。

（十四）因扩展信息点而在有关部门安装的网络设备，如交换机、集线器、服务器光纤转换器等，应由安装点所在部门指定兼职管理人员，协助网络中心对该设备进行监控和管理，发现问题及时通报网络中心解决。

（十五)所有用户有义务向学院有关部门报告违法犯罪行为和有害信息。

（十六）本管理制度自公布之日起实施，修正时亦同。

安阳学院网络安全事故通报制度

为及时了解和妥善处理好网络安全事故，特制定本制度。

一、本制度所称网络安全事故是指

（一）网站页面被篡改。

（二）涉密信息失窃。

（三）黑客攻击而导致网络服务中断。

（四）黑客或病毒导致重要数据丢失或损坏。

（五）校内或校外在一些贴吧、BBS、论坛上发表不正当言论者，如以下言论：

1、煽动抗拒、破坏宪法和法律、行政法规实施的；

2、损害国家机关声誉的；

3、煽动分裂国家、破环国家统一的；

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、教唆犯罪的；

7、公然侮辱他人或捏造事实诽谤、恶意攻击他人的；

8、损害学院声誉，影响学院安全稳定的；

9、其他违反宪法和法律行政法规的。

二、如出现以上事故时，除要在1个工作日内向学院有关部门报告外，应同时以电话或其他有效方式直接向网络中心报告。

三、网络安全事件报告与处置。网络安全事件发生并得到确认后，有关人员应立即将情况报告有关领导，由领导指挥处理网络安全事件。应及时向当地公安机关报案。阻断网络连接，进行现场保护，协助调查取证和系统恢复等工作，有关违法事件移交公安机关处理。

四、为加强网络安全信息共享和统一协调行动，按照“统一领导、归口负责”的原则，由网络中心负责网络安全事件通报工作的组织、指导和协调。

五、安全事件通报可采取例行通报、紧急通报两种方式进行。例行通报为定期方式，适用于对网络安全信息的汇总分析。紧急通报为不定期方式，适用于对突发的网络安全事件或重大网络安全预警信息的发布，对具有紧急和有重要指导作用的网络安全事件应在当天内完成通报。

六、网络安全事件发生通报内容包括事件的性质、类型、影响范围、影响程度、发生时间、持续时间、事件定级，以及目前已经采取的响应措施和实际效果。

七、网络安全事件预警通报内容包括可能发生的事件的性质、类型、影响效果、影响程度、可能爆发的时间，以及可采用的措施等。

八、在收到网络安全事件通报或重大网络安全事件报告时，应立即对所收到的通报或报告的安全事件进行分析判断、汇总归纳整理，并根据所收到的内容对本级网络安全系统进行有针对性的整改通报。

九、对一些涉及到保密内容的网络安全事件通报，应严格按照有关保密管理规定执行。

十、对发生重大信息网络安全事件或网络安全预警事件没有及时进行通报的，特别是故意瞒报、缓报、谎报的应追究相关部门、相关责任人的相应行政责任，可处以批评、警告、严重警告、记过等处分。

安阳学院网站登记、备案制度

为规范校园网络信息服务备案及备案管理，促进校园网的健康发展，根据国务院颁布的《互联网信息服务管理办法》（国务院令第292号）、信息产业部颁布的《非经营性互联网信息服务备案管理办法》（信息产业部令第33号）、我院颁布的《安阳学院网站建设管理规定》等规定，特制定本制度。

一、安阳学院校园内建设的各类网站均须办理登记备案手续。

二、校园内开设网站应先到网络中心填写《安阳学院网站登记备案申请表》，根据备案要求认真填报申请表并确保信息的真实可靠。由网站所属部门主管领导在申请表上签字，加盖所属部门公章，并经学院网站建设领导小组组长审核签字后再加盖学院公章最后到网络中心申请。全部审核通过方可填写备案登记表，开设网站。

三、网站登记备案有效期为五年，网站登记备案五年后，须在两个星期内，按照本制度第一、二条规定重新申请登记备案。超过两个星期尚未申请登记备案的网站，网络中心将视为自愿放弃网站服务，并关闭该网站，停止相关服务。

四、网络中心负责对符合相关要求的单位网站提供虚拟主机、分配学院域名及其他符合规定并经过审批的服务。

五、对不按期履行备案手续的网站，网络中心将发布公告，并根据有关规定予以处理。

六、网站在备案有效期内需要变更其《安阳学院网站登记备案申请表》中填报信息的，应当先到网络中心网站领取《安阳学院网站登记备案申请表》，根据备案要求认真填报申请表并确保信息的真实可靠。由网站所属部门主管领导在申请表上签字，加盖所属部门公章后到网络中心履行备案变更手续。

七、网站在备案有效期内需要终止提供服务的，应当在服务终止之日起两个星期内到网络中心履行备案注销手续。

八、对违反有关法律或校园网络管理规定的网站，网络中心将关闭其网站，并追究相关人员的责任。

安阳学院计算机应用信息系统安全管理规定

一、为了保证本院计算机应用信息系统的正常运行，完成系统各项应有功能，保证各系统数据、资料的安全性、有效性、完整性，特制定本安全管理规定。

二、学院任何单机版应用信息系统的使用、维护及系统数据的安全保护由本部门负责承担；学院其它网络版应用信息系统的使用、维护及系统数据安全保护由网络中心负责承担。相应部门必须有专人负责应用信息系统的使用、维护及安全保护。

三、为了各系统数据的安全性，运行应用信息系统的计算机原则上不得与因特网直接进行联接。特别需要提供远程网上查询的系统与因特网进行联接时应该有完善的安全防范办法，同时不得将原始数据直接与因特网联接。

四、计算机应用信息系统的使用实行严格的权限分散管理制度。严禁任何非授权人员管理、操纵运行信息应用系统的计算机。计算机应用信息系统的使用人员分为系统管理人员和应用人员，明确系统管理人员、应用人员的权限和操作范围。各应用信息系统的系统管理人员视本系统大小确定一个人或一个管理小组，人员名单由负责部门的主管推荐，并报经院长批准。应用人员名单

及对相应系统的使用权限由使用该系统的部门主管确定，并报网络中心备案。

五、计算机应用信息系统管理人员负责为应用人员分配系统的使用权限；并定期及时进行系统数据备份（本地备份和异地备份）；当发生数据错误时，应该及时恢复；应该定期对所管理之应用信息系统的安全状况进行检查，发现问题及时处理。

六、计算机应用信息系统管理人员应该熟悉本部门所使系统的各项功能，熟练完成系统提供的各项功能，并能够及时排除软、硬件故障。计算机应用信息系统应用人员应该熟悉本系统的各项功能，能够严格按照系统提供的功能正确进行操作，完成相关工作。

七、不得在运行应用信息系统的计算机上使用、浏览任何与系统无关的程序、游戏、文档等资料；不得使用任何不明来历的磁带、光盘、软盘等外部存储设备；不得制造、复制、传播任何色情、暴力、迷信等有害资料及计算机病毒。

八、计算机应用信息系统的管理和应用人员须做好各自系统软、硬件的防火、防水、防盗等安全工作。

九、计算机应用信息系统的使用人员应对系统的各类数据、资料严格保密。如有违反规定泄漏学院机密者，按绩效考核制度从严惩处。

十、计算机应用信息系统核心部分开发的技术人员调离时，必须移交全部技术手册、文档、资料；计算机应用信息系统管理

人员调离时，必须确认系统数据的有效性、完整性，并由接管人更换计算机的有关口令和密钥。计算机应用信息系统应用人员调离时，应移交有关的技术手册、文档、资料和相关业务。

十一、本规定适用于学院内的所有计算机应用信息系统。

十二、本规定自发布之日起执行，修正时亦同。

安阳学院用户上网实名注册制度

为加强对我院校园网信息安全的管理，规范校园网用户上网行为，维护我院的安全和稳定，根据国务院信息办、公安部、国家安全部、教育部等部门颁布相关网络管理条例和文件精神，特制定本制度。

一、申请入网的院内用户应认真阅读《校园网安全管理制度》、《安阳学院校园宿舍网用户守则》，持有效证件（教职工持本人身份证、校园卡；学生持本人身份证、学生证、校园卡）到学院网络中心领取《校园网新增信息点审批表》（只对办公网用户），学院宿舍网要认真填写《校园网用户入网备案表》，填写后交网络中心，办理开户手续。届时用户在登记表上签字，网络中心给与分配 IP 地址，开通网络。

二、用户若需停止校园网的使用，本人应到网络中心办理注销手续。退网时间从注销登记之日算起。退网手续应本人亲自办理不得他人代办。

三、注意事项

（一）校园网用户必须遵守执行国家有关互联网法律法规，严格执行安全保密制度，积极配合实施实名注册制度，提供准确有效的注册资料。

（二）校园网用户有义务向公安机关举报网络上的违法行为和违法信息。

（三）网络中心为校园网用户提供网络通讯服务，负责用户信息端口的正常运行。用户端的设备（如个人 PC、网卡等）由用户自己负责，若出现故障由用户自行解决。

（四）网络中心为用户分配的 IP 地址已与用户的网卡地址绑定，用户不要随意改动 IP 地址。若用户改动 IP 地址引起的网络故障，追究相关用户责任。

（五）用户更换网卡，须向网络中心提出申请，报告新的 MAC 地址，网络中心负责重新捆绑。

（六）校园网用户必须遵守以上所有规定，违反规定的用户网络中心有权停止其使用，终止其接入校园网络，情节严重的报学院有关部门给予处分。

四、本制度自公布之日起执行

安阳学院校园网用户入网备案表

<table>
<tr><td colspan="4">申请人填写</td><td rowspan="3"></td><td colspan="2">网络中心填写</td></tr>
<tr><td>姓名*</td><td></td><td>性别</td><td></td><td>批准日期</td><td>年 月 日</td></tr>
<tr><td>身份证*</td><td colspan="3"></td><td>用户 IP 地址</td><td></td></tr>
</table>

专业班级*			用户子网掩码	
宿舍号*			用户网关	
联系电话*			用户 DNS	
帐户名*			第二 DNS	
帐户密码*				

填写说明	此表一式两份，用户领取入网备案表，认真填写并签字。网络中心审定批准后，一份在网络中心备案，一份用户留存。 填写前请仔细阅读《安阳学院校园网安全管理规定》及国家制定的互联网有关规定。 校园网入网中心地址：网络中心办公室 校园网咨询电话：5998165
申请人承诺	申请人人必须承诺： 守互联网相关法规，不通过网络传播任何法律法规禁止的有害信息。对本单位的行为和发布的信息而引起的任何政治责任、法律责任及造成的经济损失承担全部责任。
	申请人签字：

注：“*”为必填项。帐户名为学号，帐户密码为宿舍楼号加宿舍号。

安阳学院网络中心制表

安阳学院网站管理规定

为了加强学院网站建设，实施科学化、规范化管理，弘扬学院文化，树立良好社会形象，经研究，特制定本制度。

一、学院网站管理工作由学院办公室统一协调，规范管理。

二、学院网络中心负责学院整体网站的技术支持及安全管理工作，并对学院主网站进行全面维护、更新。

三、各部门网站管理负责人分管本部门网站的日常管理、维护工作，以及本部门上传信息审核、网站内容监控工作。

四、各学院、各处室开展活动的新闻、报道稿件须在活动结束两天内（包括活动当天）审核上传，且内容不得包含错别字、病句以及常识性错误。

五、学院官网上传新闻、报道等信息时必须严格按照以下程序执行，严禁任何未经审核的信息发布在相关栏目内：

拟稿→主管审核→主管院领导签发→交网络中心上传→部门网站管理负责人在线复查。

六、关于各部门上传新闻有关格式的规定（关于格式问题可在 WORD 中先按以下格式排版好，然后再复制到网站管理后台即

可）：

（一）标题：黑体，不加粗，小三，居中，单倍行距，可分一行或多行居中排布。回行时，要做到词意完整，排列对称，不能把完整的词拆开。

（二）副标题：双破折号用宋体（以显示无中间裂隙），文字用仿宋体，不加粗，四号，居中，单倍行距，段前段后各 0.5 行。

（三）正文：宋体，小四，首行缩进 2 字符，1.5 倍行距。

（四）图片：所有上传照片必须经过图像软件加工后才能使用，每条新闻图片尽量不要超过 10 张。图片如有文字说明，则一律将文字说明排在图片下方，用宋体，五号，居中排列。

（五）出处：标题下要注明文章来源部门。正文后要注明文章和图片作者，采用正文后加括号，作者信息填写在括号内，字体为小四，楷体。样式：（文/张三 图/李四）

（六）以上要求仅限新闻排版格式，字体颜色可根据部门特色和需求自行设置，但要总体美观，大方。

七、各部门网站管理负责人是本部门网站管理、维护及上传信息审核的第一责任人，要切实做好该项工作。

八、学院办公室要做好网站管理的督查工作，每月汇总上报，并对各部门网站管理情况及时做出通报。

九、本规定自发布之日起施行。修正时亦同。

安阳学院上网信息审核登记制度

一、坚持"谁上网谁负责"的原则，确保涉密信息不上网，上网信息不涉密，遵守上网信息宣传纪律（见《安阳学院上网信息宣传纪律与规定》）。

二、校园网的所有工作人员和上网单位及个人必须保守国家机密的各项法律和规定，严格执行网络信息安全保密制度。

三、严禁发布不真实的信息，严禁传送具有威胁性、不友好、有损国格和人格、有损学院声誉的信息。

四、各部门主管负责该部门上网内容的审查，对本单位所提供的信息负责，并负责相应的网络安全和信息安全工作。

五、各部门网络信息员对其在本部门网站上发布的所有信息都要经过相关部门审核批准，其上网信息的具体审核分类如下：

（一）涉及到本部门的业务信息须报请本部门主管审核批准。

（二）涉及到学院整体宣传方面的信息经本部门主管审阅后须交学院办公室审核批准。

（三)涉及到本部门人事方面的信息(如专兼职教师人数等）经本部门主管审阅后须交人事处审核批准；

（四）涉及到政治宣传方面的信息（如党团活动等）经本部门主管审阅后须报院办公室审核批准。

六、因各部门对上网信息审查不严，出现严重问题，造成不良影响的,追究部门领导和网络信息员的责任。若违反有关规定，严肃处理。

七、各部门应当对所发布的信息记录备案，规范对本部门上网信息的管理，以方便上级部门的检查。

安阳学院校园宿舍网用户守则

一、总则

（一）为加强学院校园宿舍网的管理，维护学院的正常教学、工作及生活秩序，规范校园网络服务，保障学院校园网络的正常运行和发展，同时也为了维护学院及用户的正当权益，更好地为广大校园宿舍网络用户（以下简称用户）服务，根据国家关于计算机网络的法律法规和学院的相关管理规定，制定本守则。

（二）校园宿舍网的服务对象为：学院的专任教职员工、在校学生和经批准临时接入校园宿舍网的用户。凡接入学院校园宿舍网的网络用户都必须遵守本守则。

（三）校园宿舍网由学院学生宿舍区、教职工生活区的计算机网络组成，是学院教学和科研的重要基础设施之一。

（四）学院和网络中心针对学院校园计算机网络及其用户所制定的所有规章制度同时适用于本网及本网的用户。

（五）任何人不得利用校园网络危害国家安全、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。

（六）学院校园宿舍网络由网络中心负责规划、建设、管理、运行和维护；并负责办理上网帐号管理、缴费充值、故障受理等相关业务。

（七）校园宿舍网的运行与维护由网络中心负责。所有楼内信息插座及网络线路、布线槽、网络设备、机柜内跳线等，统一由学院负责安装、维护、连接、设置。未经许可，任何人不得占用、更换、损毁；不得改变其物理的位置、形态、性能；不得改变其连接关系、运行状态、系统配置；不得登录网络设备。电信运营商在进行电话安装等服务时必须按照我院的要求进行规范安装；室内网络布线需向网络中心、后勤处提出符合规范、安全、美观要求的申请后，经相关部门批准后方可操作。当网络管理员进行网络维护时、本楼楼管员应积极配合。

（八）校园宿舍网用户的计算机操作系统、杀毒软件、个人防火墙及其它软件的安装由用户个人负责,计算机内的网络配置及到信息插座的网络连接也由用户个人负责。

二、安装使用资格及接入要求

（一）凡符合本守则第二条规定的人员个人宿舍网填写《安阳学院校园网用户入网备案表》，办公网用户填写《校园网新增信息点审批表》，向网络中心提出开通申请。

（二）符合申请资格的个人必须提供个人真实信息，严格按照《用户上网实名注册制度》进行实名注册。

（三）所有校园宿舍网用户，其帐号仅限于在其本人使用的计算机及其所登记的宿舍楼中接入校园网。

（四）对于帐户余额不足，且连续四个月未缴费的校园网帐号，网络中心将予以注销（寒暑假包括在内）。已注销的用户如想重新使用校园网，必须重新办理开户手续。用户如变更接入信息（IP 地址、Mac 地址等）需用户本人持有效证件到网络中心校园网用户办理处办理变更手续。

（五）用户在离校或搬迁时必须到网络中心办理注销或信息变更手续；学生毕业离校办理离校手续时，原校园宿舍网用户应向网络中心申请注销其校园网账号，若在学院规定离校日期 3 日内没有办理校园网帐户注销手续的，视为自动同意注销其校园网帐户；同时网络信息点也为学院宿舍内的固定财产，楼管员在学生毕业离校时要检查网络信息点的完整性。

三、安全管理及运行

（一）个人的通信自由和通信秘密受法律保护。任何人不得违反法律规定，利用网络侵犯用户的通信自由和通信秘密。校园网网络用户必须遵守国家关于互联网络的相关管理规定和学院关于宿舍网络的相关管理办法。

（二）网络中心为用户分配的 IP 地址已与用户的网卡地址（MAC 地址）绑定。用户在网络中应使用自己注册的 IP 地址、

账号，不得私自给与他人使用，一经发现，将撤销该用户的入网资格；因用户改动网络配置及网卡物理地址引起的网络故障，由用户自己负责。盗用他人 IP 地址、帐号的，一经发现则给予处分。

（三）学生宿舍内每个床铺下各有一个信息点，用户上网时必须使用一个交换机设备（只允许使用 HUB 或普通二层交换设备），用户端的设备（如个人 PC、网卡）由用户自己负责，若出现故障由用户自行解决。用户上网指南及疑难问题解答参见学院网络中心网站。

（四）遵照有关法律规定，严禁通过使用宽带路由器、私设代理服务器等方式进行多用户使用同一帐号上网，一经发现，网络中心有权对违规用户进行一周至一个月的断网，并报学院给予处分。

（五）网络中心有权对宿舍内计算机进行定期或不定期检查，用户应积极配合，并接受检查人员所提出的整改要求。

（六）校园宿舍网用户在按规定联网后，有权了解校园网使用性能、用户端的配置参数与方法、系统当前的运行状态等情况；网络中心对校园宿舍网用户在使用宿舍网过程中所遇到的问题提供技术支持。

（七）用户有权要求通过校园宿舍网侵害其正当权益行为的人立即停止其侵害行为；有权要求相关服务提供人或网络信息管

理部门追查或协助追查通过校园网侵害其自身正当权益的行为及其行为人。

（八）校园宿舍网用户发现违反有关法律、法规和规章制度的人或事应该予以制止或向网络中心反映、举报。同时应该协助有关部门或管理人员对上述人或事进行调查、取证、处理，向调查人员如实提供所需证据。

（九）校园宿舍网用户和网络管理人员在所有与校园网相关的活动中必须接受国家安全机关、公安机关和学院相关部门依照有关法律、法规和管理规定进行的管理和监督。

（十）校园宿舍网用户有权拒绝身份不明的人员行使网管员的职权；有权对校园宿舍网及其运行、管理工作提出意见和建议；在对校园宿舍网的现状或网管员的服务不满意时，有权向学院网络中心投诉。

（十一）校园宿舍网用户必须按照有关规定缴纳相关费用。

（十二）网络中心可根据实际情况和需要采用新技术，调整网络结构和系统功能、变更系统参数和使用方法、排除系统隐患等，无须征得用户同意。但如果上述工作影响到用户的使用性能和使用方法，网络中心应预先通知用户。

（十三）对于校园宿舍网络在使用过程中出现的故障，网络中心接到故障报告严格按照《安阳学院校园网维修服务承诺书》进行维修。如因人为原因造成的网络故障，网络中心将根据情节

的轻重按规定对责任人进行处理，并向全院通报，若造成网络设备损坏的，应根据相关规定进行赔偿。

四、本规定自发布之日起实施，修订时亦同

安阳学院校园网安全保密管理规定

为进一步加强我院校园网安全、保密工作，更好地为全院师生员工提供一个先进、可靠、安全的计算机网络环境，充分发挥校园网的作用，全面支持学院的教学、科研管理工作，保护校园网的安全运行，特制定本条例。

一、网络中心全面负责学院网络安全保密工作。各系、部、处室设网络信息安全管理员，具体负责本部门网络安全和信息保密工作，并定期对网络用户进行信息保密和网络安全教育。

二、学院校园网实行统一管理，分层负责的管理制度。网络中心对全院的资源进行统一管理，各系、部、处室负责本部门的资源管理。网络中心和各部门的网络安全保密管理员有权对相应部门的网络安全和信息保密情况进行定期和不定期的检查及监控，并有责任向院领导报告有关情况。

三、各类业务局域网（如财务系统等）必须实现与校园网的物理隔离。严禁将涉及党、国家和学院秘密的信息和属于国家重点或保密科研项目的信息上网或存放在入网计算机中。

四、严禁任何部门和个人擅自联入校园网。所有网络用户和个人使用校园网，要首先办理入网登记手续，到网络中心进行用户和计算机的相关信息登记，自觉遵守校园计算机网络管理规定。网络中心只对符合设置域名条件的系、部、处室配置域名，并定期检查所开设用户的状况。

五、校园网的工作人员和所有入网用户必须严格遵守国家的法律、法令和法规及《安阳学院校园计算机网络管理规定》，接受并配合学院有关部门依法进行的监控和检查，不得利用计算机网络从事危害国家安全、泄露国家和学院秘密等活动，不得制作、查阅、复制和传播妨碍社会治安和伤风败俗的淫秽色情信息。

六、校园网上不允许进行任何干扰网络用户，破坏网络服务和破坏网络设备的活动，不允许在网络上发布不真实的信息、散布计算机病毒、用未经授权使用的计算机进入网络、以不真实身份使用网络资源、随意拷贝或使用未经安全检查的系统软件和应用软件等。一经发现，网络中心将采取必要措施保证校园网的正常运转。

七、不得利用网络对他人进行诽谤、诬陷、欺诈、教唆等；不得侵犯他人的名誉权、姓名权等人身权利；不得侵犯他人的商誉、商标、版权、专利、专有技术和商业秘密等各种知识产权。

不准利用网络私自投稿，对外投稿的论文、稿件要严格按照学院保密审查的程序逐级审查后，才可发出。

八、网络管理员有权制止不法行为，并有权向有关部门报告违法犯罪行为和有害信息情况。

九、对违反本管理规定者，学院将按照国家和学院的相关规定给予严肃查处。对构成犯罪者，将依法追究其刑事责任。

十、本规定自发布之日起施行。修正时亦同。

安阳学院上网信息宣传纪律与规定

一、网站宣传要坚持党的宣传方针和政策，遵守宣传纪律，以正面宣传为主，弘扬正气，兴利除弊。

二、校园网的所有工作人员和上网单位及个人必须保守国家机密的各项法律和规定，严格执行网络信息安全保密制度。

三、任何单位和个人不得利用计算机网络从事危害国家安全、泄露国家秘密的活动；不得发布任何危害国家安全的言论及封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖和教唆犯罪的内容；严禁链接有关政治、宗教等方面的违法信息；不得查阅、复制、传播各种有碍社会稳定、校园秩序和伤风败俗的种种信息。

四、严禁发布不真实的信息，严禁传送具有威胁性、不友好、有损国格和人格、有损学院声誉的信息。

五、各上网单位主管负责该单位上网内容的审查，网络信息宣传要遵守有关纪律法规和信息发布的审批制度，对所提供的信息负责，并负责相应的网络安全和信息安全工作。

六、一经发现网上有内容反动、不健康、不真实以及涉密信息等情况，要及时报告院党委办公室和网络中心，网络中心的网络管理人员有监管、备份和删除的权力。

七、因各单位对上网信息审查不严，出现严重问题，造成不良影响的，追究单位领导和网络信息员的责任。若违反有关规定，严肃处理。

八、信息发布单位应当对所发布的信息记录备案，规范对本单位上网信息的管理，以方便上级部门的检查。

九、信息审核单位应当做好信息请求、处理、转发的备案工作。

安阳学院网络中心值班管理规定

为进一步加强对值班工作的管理，进一步规范值班人员行为，确保值班工作的有效进行，特制定本规定。

一、值班人员的主要职责

（一）负责接听电话，解决校园网络用户报修问题；

（二）负责开放机房的正常值班；

（三）负责其他临时交办的工作。

二、值班人员应提前做好值班准备工作，不得迟到，早退；当日不能值班者经值班负责人批准可提前自行调换，并由值班负责人填写值班记录。

三、值班人员要认真受理和解答校园网用户来电，及时解决反映的问题并做好记录。

四、值班人员必须严格遵守各项规章制度，不得擅离职守，不得占用值班电话拨打私人电话，不得做与值班工作无关的事项。

五、值班人员要保持值班室环境整洁，物品摆放整齐。

六、值班负责人负责组织值班人员做好值班工作，值班过程中保证值班人员全部到岗，并负责检查本班次人员的到岗情况。

七、直接责任人和值班负责人值班脱岗一次，按缺勤一个工作日。

八、值班时间：

周一至周五 18：30——20：30

安阳学院网络中心消防安全制度

为了加强消防安全管理工作，杜绝火灾、保证网络中心设备及师生的人身安全，中心的消防安全工作在主任的直接领导下，实行分级责任制，使消防安全工作层层有人抓，处处有人管。并把消防安全工作纳入中心的日常管理工作之中，现特制定以下消防安全制度。

一、网络中心以中心主任为消防安全责任人，下设安全员一名。

二、成立消防安全卫生管理小组。由中心主任以及相关人员组成，负责对中心的消防安全卫生等工作进行检查、落实。

三、加强员工的安全消防教育、培训。员工都应达到“三懂”、“三会”。三懂：1、一懂本岗位产生火灾的危险性；2、二懂本岗位预防火灾的措施；3、三懂本岗位扑救火灾的方法。 三会：1、一会报警，做到人人都知道火警报警电话119；2、二会使用本岗位灭火器材；3、三会扑救初起火。

四、制定监督检查制度，定期检查，发现问题及时整改。

五、加强用电安全检查，管理人员要定期邀请电工对实验室的线路、稳压电源等进行检查，如发现存在安全隐患，要及时进行整改、维护、确保安全。

六、员工在工作中一律讲安全，遵守操作规程，不得违章操作，否则通报批评，造成经济损失的追究其经济责任。

七、建立消防器材管理制度。消防器材、设施的保管、检查一律落实到人，明确职责、责任到人，定期检查，发现问题及时向院保卫处报告，由院保卫处统一进行处理。

八、根据谁主管谁负责的原则划分安全管理责任区，明确职责，责任到人，谁的责任区出安全事故谁负责。

九、本制度自公布之日开始执行。

安阳学院网络中心消防安全操作规程

为保证网络中心消防操作的安全、正确性，确保本辖区的安全，特制定本规程。

一、每位管理人员必须对辖区内的电气线路和电气设备的种类及性能熟悉，对电气设备性能未充分了解时，禁止冒险作业。

二、管理人员应定期检查辖区内电线、稳压电源等设备情况，检查中发现问题，必须及时处理或及时报修。

三、除临时施工用电或临时采取的措施外，不允许架临时电线，不允许乱挂灯、仪表工具等，应用安全的开关和插座，原电气线路不得擅自更改。

四、管理人员应注意灭火器等消防器材的质保期，确保消防器材安全有效。

五、要熟练运用各种消防器具。

六、对于已经老化的设备要及时报废更新，确保安全。

安阳学院网络中心中心机房安全管理制度

中心机房是支持信息系统正常运行的重要场所。为保证机房设备与信息的安全，保障机房有良好的运行环境和工作秩序，特制定本制度。

一、校园网中心机房由网络中心负责管理。根据工作需要，中心机房需配备系统管理员一名，负责系统数据和系统日志备份、系统安全检查、系统相关参数的配置与软件安装；负责对机房内各类设备进行安全维护和管理。

二、系统管理人员必须加强对网络中心设备的运行监控，认真处理网络数据，数据损坏后须及时检查，如出现错误应立即

改正；发现网络故障等问题要及时报告并采取相应的措施。有关情况和操作及时记入维护日志。

三、网络中心机房内工作人员应严格遵守操作规程，对各类设备、设施实行规范操作,并做好日常维护和保养。定时做好中心服务器的日志和存档工作,任何人不得删除运行记录的文档，否则追究责任。

四、网络管理、维护和开发人员要确保数据信息的安全，数据资料和软件必须由专人负责保管，未经允许、不得私自拷贝、下载和外借，严禁任何人使用未经检测允许的介质(软盘、光盘、U 盘等)。严禁未经许可私自在服务器上安装软件。未经许可任何人不得挪用和外借机房内的各类设备、资料及物品。

五、系统管理员须制定 IP 地址分配表、中心内部线路的布局图，给每个交换机端口编上号码，以便操作和维护。系统管理员须经常注意机房内温度、湿度、电压等参数，并做好记录，发现异常及时采取相应措施。

六、机房内服务器、网络设备、UPS 电源、空调等重要设施由专人严格按照规定操作，严禁随意开关。系统管理员的操作须严格按照操作规程进行，任何人不得擅自更改系统设置。

七、网络中心机房的核心服务器要做好安全设定,包括端口、漏洞、补丁等，做好防范措施，要设置自动杀毒程序更新及系统补丁更新，重要数据要定期做好本地备份和异地备份。

八、网络中心机房的核心交换设备，路由器、交换机的配置

要有规划和记录，每次配置列表要备份并进行详细记录，以便故障出现时及时恢复。

九、机房的网络线路包括光纤跳线、电缆及光缆等要做好标记，方便查找。

十、管理员必须在上、下班时间检查机房设备和系统运行情况，并做好运行记录。设备（UPS 电池）寿命到期，要提前提出更换方案。

十一、保持机房整洁、卫生。所有设备摆放整齐有序，不得将任何废弃物品留在机房内；不存放与工作无关的物品。机房内物品不允许私自带出。管理人员离开机房时，必须锁好门窗，如暂时离开，须随手关门。

十二、严格加强机房安全管理，采取防火防盗、防潮防雷措施。管理人员能熟练操作消防器材，每周检查一次消防器材。发现问题及时处理。

十三、做好信息数据的安全保密工作，一旦发现中心服务器有被侵入及恶意攻击记录，应及时采取措施制止并向主管领导报告；若发现网上有色情及政治敏感内容，及时报告有关部门处理。

十四、做好电源及 UPS 管理。

（一）机房内的电源开关、电源插座要明确标出控制的设备。

（二）不得随便更改线路和变动开关。

（三）熟悉 UPS 的工作原理和操作规程。

（四）对 UPS 的工作异常情况要做好记录，并及时联系有关单位进行处理。

（五）UPS 应妥善保养，每 3 个月放电一次。

十五、做好空调管理。

（一）网络中心机房为保证设备良好的工作环境，应保持合适的机房温度和湿度，机房温度应保持在 23℃--26℃，机房湿度应低于 70%。

（二）定期进行日常巡视，确保空调系统的正常运行。

（三）定期进行一次室外机的清理，防止因散热不良造成空调的工作异常。

（四）每年进行一次全面检修。

十六、机房钥匙有专人保管，禁止外借，主任处留一份备用存档。

十七、严格执行机房人员进入登记制度。外来人员一律要进行登记，不得邀请无关人员进入网络中心机房参观，外单位系统、线路维护人员如要进入机房需提前与网络中心人员联系，批准后方可由管理人员陪同进入，并做好登记。

十八、如机房发现意外和紧急情况要及时报告单位主管，对重大事故要注意保护现场，并采取果断措施制止事态发展，同时向院领导汇报。

十九、如管理人员对上述规定执行不力或违反规定，按照学院考核办法处理。

二十、本规定自公布之日起实施，修正时亦同。

安阳学院网络与信息安全责任书

为切实做好学校网络的安全工作，根据“谁使用，谁负责”的原则，现需签订网络与信息安全责任书。

一、自觉遵守法律、行政法规和其他有关规定，不侵犯国家的、社会的、集体的利益和公民的合法权益，不从事犯罪活动。

二、不利用互联网制作、复制、查阅和传播下列信息：

（一）煽动抗拒、破坏宪法和法律、行政法规实施的；

（二）煽动颠覆国家政权，推翻社会主义制度的；

（三）煽动分裂国家、破坏国家统一的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）捏造或者歪曲事实，散布谣言，扰乱社会秩序的；

（六）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖、教唆犯罪的；

（七）公然侮辱他人或者捏造事实诽谤他人的；

（八）损害国家机关信誉的；

（九）其他违反宪法和法律、行政法规的。

三、不从事下列危害计算机信息网络安全的活动

（一）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；

（二）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；

（三）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；

（四）故意制作、传播计算机病毒等破坏性程序的；

（五）其他危害计算机信息网络安全的。

四、建立安全保护管理制度、落实各项安全保护技术措施，保障本单位网络运行安全和信息安全。

五、严格遵守国家有关法律法规，做好本单位信息网络安全管理工作，设立信息安全责任人和信息安全审查员，对发布的信息进行实时审核，发现有以上二、三点所列情形之一的，应当保留有关原始记录并在二十四小时内向公安机关、网络安全部门报告。

单位名称：

负责人签字：

年　月　日

安阳学院信息安全事件
报告和处置管理制度

一、目的

为提高网络与信息安全突发事件的处置能力，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，维护正常的政治、经济和社会秩序。

二、适用范围

本制度适用于安阳学院内发生的网络与信息安全突发事件和可能导致网络与信息安全突发事件的应对工作。

三、职责

本制度由网络与教育技术中心制订，结合信息网络快速发展和我校发展状况，结合相关法律法规的制定、修改和完善，适时修订本制度，本制度自印发之日起实施。

四、要求

（一）工作原则

1、预防为主：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、应急保障和打击犯罪等环节，在法律、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。

2、快速反应：在网络与信息安全突发公共事件发生时，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。

3、以人为本：把保障公共利益以及公民、法人和其他组织的合法权益的安全作为首要任务，及时采取措施，最大限度地避免公民财产遭受损失。

4、分级负责：按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”以及“条块结合，以条为主”的原则，建立和完善安全责任制及联动工作机制。根据各部门职能，各司其职，加强部门间、科室间的协调与配合，形成合力，共同履行应急处置工作的管理职责。

5、常备不懈：加强技术储备，规范应急处置措施与操作流程，定期进行预案演练，确保应急预案切实有效，实现网络与信息安全突发公共事件应急处置的科学化、程序化与规范化。

（二）组织指挥机构与职责

发生网络与信息安全突发事件后，应成立网络与信息安全应急协调小组(以下简称协调小组)，为我校网络与信息安全应急处

置的组织协调机构，负责领导、协调我校内网络与信息安全突发公共事件的应急处置工作。网络与信息安全协调小组下设办公室(以下简称协调小组办公室)，负责日常工作和综合协调，并与公安网监处进行联系。

（三）先期处置

1、当发生网络与信息安全突发公共事件时，事发部门应做好先期应急处置工作，立即采取措施控制事态，同时向相关主管部门通报。

2、网络与信息安全事件分为四级：特别重大(Ⅰ级) 、重大(Ⅱ
级) 、较大(Ⅲ级) 、一般(Ⅳ级) 。

3、主管部门在接到我校网络与信息安全突发公共事件发生或可能发生的信息后，应加强与有关方面的联系，掌握最新发展态势。对Ⅲ级或Ⅳ级的网络与信息安全突发事件，由该主管部门自行负责应急处置工作。对有可能演变为Ⅱ级或Ⅰ级的网络与信息安全突发事件， 要为协调小组处置工作提出建议方案，并做好启动本预案的各项准备工作。主管部门要根据网络与信息安全突发事件发展态势，视情况决定赶赴现场指导、组织派遣应急支援力量，支持事发部门做好应急处置工作。

（四）应急处置

1、应急指挥

应急预案启动后，根据协调小组会议的部署，担任总指挥的领导和参与指挥的领导迅速赶赴相应的指挥平台，进入指挥岗位，启动指挥系统。相关联动部门按照本制度确定的有关职责立即开展工作。需要成立现场指挥部的，事发部门立即在现场开设指挥部，并提供现场指挥运作的相关保障。现场指挥部要根据事件性质迅速组建各类应急工作组，开展应急处置工作。现场指挥部在校内协调小组的领导下全权负责现场的应急援救工作。主管部门负责对发生网络与信息安全突发公共事件的网络与信息系统的现场应急处置工作。

2、应急支援

应急预案启动后， 协调小组的应急响应先遣小组，赶赴事发地，督促、指导和协调处置工作。协调小组办公室根据事态的发展和处置工作需要，及时增派专家小组和应急支援单位，调动必需的物资、设备，支援应急工作。参加现场处置工作的各有关部门要在现场指挥部统一指挥下，协助开展处置行动。

3、信息处理

（1）现场信息收集、分析和上报。事发部门应对事件进行动态监测、评估、及时将事件的性质、危害程度和损失情况及处

置工作等情况，及时报协调小组办公室，不得隐瞒、缓报、谎报。

（2）信息处理。协调小组办公室要明确信息采集、编辑、分析、审核、签发的责任人，做好信息分析、报告和发布工作。

（3）信息发布和咨询。当网络与信息安全突发公共事件发生时，协调小组办公室要及时做好信息发布工作，通过校内信息发布平台发布网络与信息安全突发公共事件预警及应急处置的相关信息，通知各部门做好应急准备及预防措施。

（4）应急结束。网络与信息安全突发公共事件经应急处置后，得到有效控制，经各监测统计数据上报协调小组办公室，由协调小组办公室向协调小组提出应急结束的建议，经批准后实施。

五、后期处置

（一）善后处置

在应急处置工作结束后，事发单位要迅速采取措施，抓紧组织抢修受损的基础设施，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，迅速组织实施。有关主管部门要提供必要的人员和技术、物资和装备以及资金等的支持，并将善后处置的有关情况报备协调小组办公室。

（二）调查和评估

在应急处置工作结束后，主管部门应立即组织有关人员和专家组成事件调查组，对事件发生及其处置过程进行全面的调查，查清事件发生的原因及财产损失状况和总结经验教训，并根据问责制的有关规定，对有关责任人员做出处理。

六、相关资源

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》制定本预案。

安阳学院网络与信息安全应急预案

为了切实做好安阳学院网络与信息安全突发事件的防范和应急处理工作，进一步提高学校预防和控制网络与信息安全突发事件的能力和水平，减轻或消除突发事件的危害和影响，确保网络与信息安全运行，结合学校工作实际，制定本预案。

第一章　总则

第一条 本预案所称突发性事件，是指自然因素或者人为活动引发的危害安阳学院网络设施及信息安全等有关的灾害。

第二条 本预案的依据文件是《安阳学院信息安全工作总体方针和安全策略》。

第三条 本预案适用于发生在安阳学院计算机与网络上的突发性事件应急处置工作。

第四条 应急处置工作原则：统一领导、协同合作、快速反应，积极预防、综合防范，明确责任、分级负责，依靠科学、发挥优势、保障安全。

第二章　职责任务

第五条 网络与教育技术中心成立网络与信息安全应急处置

小组。小组的主要职责与任务是统一负责全校信息网络的灾害应急工作，全面负责学校信息网络可能出现的各种突发事件的处置工作，协调解决灾害处置工作中的重大问题等。

第三章　事件分类和分级

第六条 事件分类

根据网络与信息安全突发事件的发生过程、性质和特征，网络与信息安全突发事件可划分为网络安全突发事件和信息安全突发事件。

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安全系统的损坏；信息安全突发事件是指利用信息网络进行有组织的大规模的反动宣传、煽动和渗透等破坏活动。

自然灾害是指地震、台风、雷电、火灾、洪水等；

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；

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、恐怖袭击等事件。

第七条 事件分级

根据网络与信息安全突发公共事件的可控性、严重程度和影响范围，将网络与信息安全突发公共事件分为四级：

I 级(特别重大)：网络与信息安全系统发生全局性大规模瘫痪，事态发展超出自己的控制能力，对国家安全、社会秩序、经济建设和公共利益造成特别严重损害的突发公共事件。

II 级(重大)：网络与信息安全系统造成全局性瘫痪，对国家安全、社会秩序、经济建设和公共利益造成严重损害需要跨部门协同处置的突发公共事件。

III 级(较大)：某一部分的网络与信息安全系统瘫痪，对国家安全、社会秩序、经济建设和公共利益造成一定损害，但不需要跨部门、跨地区协同处置的突发公共事件。

IV 级(一般)：网络与信息安全系统受到一定程度的损坏，对公民、法人和其他组织的权益有一定影响，但不危害国家安全、社会秩序、经济建设和公共利益的突发公共事件。

第四章　处置措施

第八条 处置措施

处置的基本措施分灾害发生前与灾害发生后两种情况。

（一）灾害发生前。学校网络与教育技术中心要预先对灾害预警预报体系进行建设，开展灾害调查，编制灾害防治规划，建设专业监测网络，并规划建设灾害信息管理系统，及时处理灾害讯情信息。加强灾害险情巡查，进行定期和不定期的检查，加强

对灾害重点部位的监测和防范，发现有不良险情时，要及时处理并向领导报告。建立健全灾情速报制度，保障突发性灾害紧急信息报送渠道畅通。

（二）灾害发生后。立即启动应急预案，采取应急处置程序，判定灾害级别，并立即将灾情向相关负责人报告，在处置过程中，应及时报告处置工作进展情况，直至处置工作结束。

第五章　处置程序

第九条 处置程序

（一）发现情况

学校网络与教育技术中心要严格执行信息安全制度，做好信息系统安全的日常巡查及其日志保存工作，以保障最先发现灾害并及时处置此突发性事件。

（二）预案启动

一旦灾害发生，立即启动应急预案，进入应急预案的处置程序。

（三）应急处置方法

在灾害发生时，首先应区分灾害发生是自然灾害还是人为破坏两种情况，根据这两种情况把应急处置方法分为两个流程。

1、流程一：当发生的灾害为自然灾害时，应根据当时的实

际情况，在保障人身安全的前提下，首先保障数据的安全，然后是设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

2、流程二：当人为或病毒破坏的灾害发生时，具体按以下顺序进行：判断破坏的来源与性质，断开影响安全与稳定的信息网络设备，

断开与破坏来源的网络物理连接，跟踪并锁定破坏来源的 IP 或其它

网络用户信息，修复被破坏的信息，恢复信息系统。

按照灾害发生的性质分别采用以下方案：

1、网络中断：首选进行故障排除。网络中断后，技术人员要迅速判断故障节点，查明故障原因。路由器，交换机等网络设备故障，网络与教育技术中心应立即检修并调试畅通；需更换设备应报上级领导，经批准后马上更换故障设备，尽快恢复系统正常运行；服务器属于租赁其他厂商的服务器，需要迅速与运营商取得联系，敦促尽快恢复线路故障；无法修理的应立即通知相关供应商及维护人员，在最短时间内安排修理。

2、大规模病毒传播：针对这种现象，要及时断开传播源，判断病毒的性质、采用的端口，然后关闭相应的端口，在网上公布病毒攻击信息以及防御方法。

3、网络入侵：对于网络入侵，首先要判断入侵的来源，区分外网与内网。入侵来自外网的，定位入侵的 IP 地址，及时关闭入侵的端口，限制入侵地 IP 地址的访问，在无法制止的情况下可以采用断开网络连接的方法。入侵来自内网的，查清入侵来源，IP 地址、上网帐号等信息，同时断开对应的交换机端口。然后针对入侵方法建设或更新入侵检测设备。

4、信息被篡改：这种情况，要求一经发现马上断开相应的信息上网链接，并尽快恢复。

5、应用程序故障：应用程序平时必须存有备份，应用程序发生故障后，安全员应立即向上级进行汇报，经确认后停止该系统，并切换至备份系统保证业务正常进行。安全员检查日志等资料，确定故障原因，处理完毕后将处理过程及结果备案存档。

6、数据库系统故障：数据库系统必须备份，数据库发生故障后，应立即向上级汇报，经同意后采用重启或者其他手段尽快恢复数据库运行，保证业务不中断。网络与教育技术中心应及时的做好数据库系统的切换和有关数据的恢复工作、检查日志等资料，确定故障原因，解决后，将处理过程及结果备案存档。

7、其它没有列出的不确定因素造成的灾害，可根据总的安全原则，结合具体的情况，做出相应的处理。不能处理的可以请示相关的专业人员。

（四）情况报告

灾害发生时，一方面按照应急处置方法进行处置，同时需要判定灾害的级别，首先向学校网络与信息安全应急处置工作小组汇报，并及时报告处置工作进展情况，直至处置工作结束。

情况报告内容包括：灾害发生的时间、地点，灾害的级别，灾害造成的后果，应急处置的过程、结果，灾害结束的时间，以后如何防范类似灾害发生的建议与方案等。

（五）发布预警

灾害发生时，可根据灾害的危害程度适当地发布预警，特别是一些在其它地方已经出现，或在安全相关网站发布了预警而学校信息网络还没有出现相应的灾害，除了在技术上进行防范以外，还应当向网络信息用户发布预警，直至灾害警报解除。

（六）预案终止

经鉴定，灾害险情或灾情已消除，或者得到有效控制后，由学校的网络与信息安全应急处置工作小组宣布险情或灾情应急期结束，并予以公告，同时预案终止。

第四章　保障措施

灾害应急防治是一项长期的、持续的、跟踪式的、深层次的和各阶段相互联系的工作，是有组织的科学与社会行为，而不是

随每次灾害的发生而开始和结束的活动。因此，必须做好应急保障工作。

第十条 人员保障

重视人员的建设与保障，确保在灾害发生前的人员值班，灾害处置过程和灾后重建中的人员在岗。

第十一条 技术保障

重视网络信息技术的建设和升级换代，在灾害发生前确保网络信息系统的稳定与安全，灾害处置过程中和灾后重建中的相关技术支撑。

第十二条 物资保障

学校要根据近三年全国网络信息系统安全防治工作所需经费情况，购买相应的应急设施。建立应急物资储备制度，保证应急抢险救灾队伍技术装备的及时更新，以确保灾害应急工作的顺利进行。

第十三条 训练和演练

加强学校网络信息用户的防灾、减灾知识的宣传普及，增强用户的防灾意识和自救互救能力。有针对性地开展应急抢险救灾演练，确保灾后应急救助手段及时、到位和有效。

第五章　附则

第十四条 本预案自发布之日起施行。

电信运营商及第三方合作运营商归口管理制度

网络基础的建设和通信网络的建设是高校信息化基础建设的重要环节，借助电信运营商及第三方合作运营商的资源和力量来支持学校的建设，为了让学校师生从中获益，在相互合作的基础上实现各自利益诉求，提升高校与运营商的合作效果，特制定本归口管理制度。

第一章 总则

为了规范电信运营商及第三方合作运营商在我校开展电信业务经营行为，保护用户合法权益，促进电信行业在我校健康发展，极大方便师生使用电信服务。

第二章 基本原则

我校与电信运营商及第三方合作运营商归口管理的基本原则：以我为主、以我所用，各负其责、各司其职。

第三章 制度内容

（一）明确管理部门

1、学校管理部门

为了便于梳理我校通信相关业务、提供整体服务，由我校网络中心进行管理，统一负责通信运营商在我校的通信设施和通信增值管理工作，包括网络、基站、室分、固话管理等，以推进整体规划和框架性合作，最大程度上保护校内用户权益。若运营商所开展的业务涉及校内多个部门，也由网络中心审核通过后再协调校内其他部门配合运营商开展工作。

2、电信运营商及第三方合作运营商管理部门

为了准确定位对接人，保证任务的快速执行，在合作过程中，电信运营商必须指定一位校园经理与我校对接，由该校园经理负责其内部协调、沟通事宜。

（二）明确管理职责

1、按责任划分管好，不缺位

网络中心主要负责规范校内通信工程建设，保证校方和运营商双方利益，要对运营商在校内通信工程建设进行有组织、规范化的建设，充分借助电信运营商力量做好学校运营基站、室内分布系统等业务的管控。

电信运营商及第三方合作运营商主要负责基站建设、管理和维护。首先，全面梳理校内基站情况，做好其负责的校内各类业务统计和规划。其次，制定基站规划方案，综合考虑校内用户分

布情况、用户通信需求、各运营商基站信号覆盖范围，根据需要建设新基站。定期对校内基站的运行状况进行排查，保持基站的良性运转。

2、不该管的不乱插手、乱干预，不错位

对于非职能范围内的事情不乱插手、乱干预，由电信运营商按规定和要求自主完成。

3、超出责任权限范围的，不乱审批、不越位

对于超出责任权限的材料，网络中心不能越权审批，必须按照严格的审批流程进行审核，避免越位现象的发生。

（三）构建多网融合环境

多家电信运营商通过多网融合，减少资金、资源浪费，由学生自由选择网络接入，避免电信运营商垄断我校营销市场，构建和谐的校园通信环境。

第四章 附则

本管理制度自发布之日起开始执行。

安阳学院信息系统登记备案管理办法

第一章 总则

为加强对我校各单位信息系统的管理，同时也是为了落实公安部、工信部、教育部相关文件的规定及要求，特制定本办法。

校内各单位所拥有的已建或在建的信息系统，无论是否对校外用户开放访问服务，均适用本办法。

第二章 登记备案管理

各信息系统拥有单位应指定一名本校教职工负责本单位信息系统的建设、维护和管理工作。

各信息系统拥有单位应填写《安阳学院信息系统申请备案表》。

网络中心受理信息系统备案申请后，应当对信息系统的备案情况进行审核，对审核无误的，应当在收到备案申请之日起的3个工作日内填写申请备案表副联；发现不符合的，应当在收到备案材料之日起的 3 个工作日内通知备案单位予以纠正并重新备案。信息系统拥有者应当保证所提供的信息内容合法。

第三章 备案材料的变更管理

各单位在本单位所拥有的已备案的信息系统发生某些变动或更改，且这些变动或更改涉及到本办法所规定的各项备案材料时，系统负责人应在变动发生后的5个工作日内重新填写《安阳学院信息系统申请备案表》。网络中心在接到申请的3个工作日内，进行备案材料变更处理，并向原备案单位通报变更结果。

第四章 各备案信息系统状况的监控

网络中心应采取适当的技术或非技术手段，对校内所有的信息系统进行监控。

（一）如发现已备案的信息系统存在问题时，应及时向系统的备案单位通报。

（二）如发现有未备案的信息系统上线运行时，网络中心应当及时向系统拥有单位通报，并限期做相应的补充或改正。逾期不做相应的补充或改正，或所做的补充或改正不合格时，网络中心有权断开其网络连接。

（三）已上线的信息系统连续或累计一周未能正常提供相应服务，网络中心有权撤销其备案信息并断开网络连接。

本条款所指的未备案的信息系统包括：从未按本办法的规定

进行备案的系统；虽已备案，但系统发生变动或更改，且按本办法第三章的规定需要进行重新备案却未备案的系统。

第五章 附则

本办法自发布之日起实行。

本办法的解释权归网络中心。