郑州轻工业学院网络信息安全管理规定

第一章 总则

第一条 为了进一步规范各类信息服务行为，切实加强学校校园网信息安全管理工作，维护学校和教职工生的利益，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》、《信息安全等级保护管理办法》以及上级有关文件精神要求，特制定本规定。

第二条 学校网络信息安全管理的对象包括：隶属于学校及校内各级机构的网络、网站、计算机应用软件及其运转过程中的数据和相关的软硬件系统，以下简称网络信息系统。

第三条 网络信息安全管理工作主要包括：网络安全管理、网络信息和网站安全管理、信息系统安全管理、数据安全管理、网络信息安全宣传教育五个方面。

第四条 学校实行“统一领导、分级管理、分工负责”的网络信息安全管理体制，在学校党政的统一领导下，实行两级管理。信息化管理中心和学校党委宣传部为一级管理单位，对学校网络信息安全进行统一管理，信息化管理中心负责统筹技术性工作、学校党委宣传部负责统筹对外信息内容安全工作。校内各行政单位为二级管理单位，对网络信息系统进行二级管理。

第五条 学校网络信息安全领导小组是学校网络信息安全工作的协作、保障平台。

第二章 管理机构及职责

第六条 一级管理单位职责

（一）校党委宣传部的职责

（1）对向校外发布的网络信息进行监督和管理，制定对外网络信息发布工作规范，审核以学校名义对外发布的网络信息内容。

（2）负责学校官方网站、微博、微信等网络信息发布平台的日常管理。

（3）作为主要部门参与网络信息安全应急处置工作。

（4）代表学校落实上级有关网络宣传、意识形态、舆情管理等有关工作要求。

（二）信息化管理中心的职责

（1）对全校网络信息安全工作进行监督和管理，制定学校网络信息安全工作规范、网络信息安全事件应急预案和处置流程。对校内各单位提供网络安全技术指导，组织开展网络安全事件预防、处置工作。

（2）组织开展学校公共网络信息系统的安全管理工作，包括：各校区校园网、学校网络数据中心、学校网站群系统、学校邮件系统、学校数字化校园平台、学校网上办公系统、迎新系统、注册系统、离校系统、学校短信平台等。

（3）代表学校落实上级有关网络信息安全管理的工作要求。

（三）保卫处的职责

协助开展与执法部门的沟通协调和网络安全事件的处置工作。

第七条 二级管理单位职责

（一）负责以本单位名义对外发布的网络信息内容质量管理，确保内容安全、质量合格。

（二）组织开展所管网络信息系统的安全管理工作。

（三）参与所管网络信息系统的安全事件处置工作。

（四）接受一级管理单位的指导、监督和检查。

第三章 校园网络安全

第八条 学校网络及其安全工作由信息化管理中心统一管理，对在学校范围内开展互联网接入服务的运营商进行统一管理，开展与运营商网络有关的网络安全协调处置工作。

第九条 校内各单位对部署于本单位范围内的学校网络设备、线路具有保护义务。未经学校同意，校属各单位和个人：不得更改或破坏学校网络设备和线路；不得擅自铺设线路、开通互联网络；不得向校外单位和个人以代理、VPN 等形式提供接入学校网络的渠道。

第十条 按照国家网络安全法的要求，信息化管理中心在校园网络上开展下列安全保护工作，保障学校网络免受干扰、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、网络入侵等危害网络安全行为的技术措施；

（三）采取记录、跟踪网络运行状态，监测、记录网络安全事件的技术措施，并按照规定留存各种日志；

（四）采取数据分类、重要数据备份和加密等措施；

（五）对校园网用户实行实名制登记；

（六）完成法律、行政法规、上级部门和学校规定的其他网络信息安全工作。

第十一条 任何单位和个人不得在校园网上明文传输具有保密性质的数据。具有保密用途的专用网络应根据保密有关规定采用专用安全设备与校园网进行连接或隔离。

第十二条 在网络建设工程、网络设备、网络运维服务采购过程中，采购部门须组织厂家、集成商、供货商、服务商在质保期、服务期内签订并履行《郑州轻工业学院网络及信息系统安全责任协议（见附件一）》，促使其采取对应措施协助保障学校网络安全。

第四章 网络信息和网站安全

第十三条 各单位党政负责人为各自网络信息发布的第一责任人，需与学校签署《郑州轻工业学院网站安全责任协议（见附件二）》。可根据实际工作需要指定一名班子成员分工负责，同时可确定一名管理员负责本单位的信息搜集、整理、制作和发布。开通或关闭网站、微博、微信平台之前需到宣传部和信息化管理中心履行登记备案手续；如实登记用途，不提供代理和涉嫌侵权的资源服务；一旦开通需做到及时更新、认真管理、注重质量。

第十四条 各单位应严肃开展网络信息发布、转载和链接管理工作，做到“统一规范、先审后上、保证质量”的要求。在学校网站、微博、微信等平台上发布的网络信息由宣传部审核后才可发布；不以学校名义在其他传播平台上擅自发布网络信息；不发布与学校、部门职责无关的信息内容和外部链接。

第十五条 各级网站安全建设、管理要求

（一）校内各部门的网站应使用学校站群系统开发、制作、发布，使用学校域名（zzuli.edu.cn、zzuli.cn）和 IP 地址，并使用学校

服务器资源部署于学校数据中心内，以确保安全。特殊情况下须经宣传部和信息化管理中心技术审核后方可调整方案。

（二）合理设置栏目，公开并及时更新单位概况、职能职责、规章制度、办事指南、工作通知、单位动态等内容；未经批准，不开设聊天室、论坛等开放式交互栏目，一旦批准开设，需安排人员认真审核留言内容，做到如实反映群众意见、过滤不良信息、积极引导网上舆论。

（三）采用安全的网络信息发布技术，避免传播带毒文件；引用、转发外部资讯时做到严格审核，并注明来源。

（四）妥善保管网站管理账户信息，使用不易被猜中的密码，并定期更新；对网站管理人员和用户加强网络安全意识教育和业务培训。

（五）始终关注网站的安全状况，及时联系信息化管理中心处置各种安全问题，配合信息化管理中心网站安全工作。

（六）实行读网制度，各级管理部门要安排值班人员每天登录网站（包括微博、微信等网络传播平台）读网，认真查看页面显示状况，查看各项功能的有效性，查看所发布的信息特别是重要信息是否存在错漏，查看是否存在暗链，发现问题立即纠正。关注校园网上发布的各类信息，加强沟通合作，做到学校网站与部门网站、部门网站与学校网站、部门网站与部门网站之间信息的准确性、一致性与恰当性。定期检查网站到其他网站的链接，防止因其他网站失效、被篡改等原因导致不良社会影响。

（七）严格落实网站维护管理制度。只在校园网内进行运维管理，若需要远程运维或第三方单位（如网站开发单位）协助运维，需要采用

VPN 加密、堡垒机登录等安全方式接入,不得直接远程桌面或直接开放管理端口到互联网。

第五章 网络信息系统安全

第十六条 各网络信息系统的主管单位负责人是系统安全第一责任人,各单位应安排专人负责所管系统的安全管理工作,严格落实《信息安全等级保护管理办法》的要求，准确划分系统安全保护等级，定期开展等级保护测评,按等级对网络信息系统开展网络安全保护工作。

第十七条 学校各类信息系统应统一部署于学校数据中心内,信息化管理中心依托校园网数据中心安全体系为信息系统提供运行安全和数据安全所需的基础环境,系统建设和使用单位负责系统的应用安全，并接受信息化管理中心的测评、扫描，落实信息化管理中心和上级有关部门提出的网络信息安全整改意见。信息化管理中心可根据网络安全事件的性质和威胁程度直接采取封堵、隔离、强制下线等措施。

将系统部署于学校数据中心之外的情况，由建设和使用单位负责提出部署方案，信息化管理中心负责指导并审定相关内容。

第十八条 各业务系统管理单位须根据学校人员和组织机构变动及时调整系统内的信息,确保系统内用户和机构信息与真实情况一致,做到业务操作能审计、追溯。

第十九条 系统建设和使用单位确保须做到不给无关人员授权、授权账号不外泄、加强人员管理、定期开展安全检查，配合信息化管理中心开展网络安全防范和处置工作。

第二十条 定期开展数据备份和系统备份,确保紧急情况下信息系统能够及时恢复。

第二十一条 在信息系统的建设、使用、维护、升级过程中，建设主管单位和使用主管单位须组织参与信息系统建设维护的相关单位和人员签订并履行《郑州轻工业学院网络信息系统安全责任协议（见附件一）》，促使对方落实学校数据保密和网络信息系统安全有关要求。

第六章 数据保密

第二十二条 对具有保密或隐私性质计算机数据，在数据所属业务单位的统一管理下实行使用人员（以下简称责任人）责任制。责任人包括本部门接触保密数据的人员、系统维护厂家及其工作人员、因实际工作需要能接触本单位所管业务数据的其他部门工作人员。

第二十三条 责任人履行如下保密义务

（一）责任人必须严格遵守郑州轻工业学院相关管理规定，合理、规范、安全地使用计算机、网络、数据和信息资源。责任人承诺在工作过程中，视所接触到的资料、数据和项目信息为保密内容，承担保密责任。

（二）来源于郑州轻工业学院的所有资料、数据和项目信息，包括但不限于教职工、学生个人身份信息、郑州轻工业学院组织架构信息、教学、科研、管理、服务等相关业务信息。

（三）责任人未经允许，不得访问、删除、修改、增加、复制、备份、摄录、摘抄、打印数据、资料，绝不擅自传播保密信息。

（四）责任人保存数据、资料的存储介质（云盘、U 盘、终端存储等）不可交由其它人使用，或作其它用途，或必须妥善保管，严防丢失。

（五）责任人未经允许，不得进行影响系统运行的操作，如关闭主机（设备）、关闭关键服务、查询大量数据、修改数据库、修改系统配置等。

（六）责任人对自己管理的账号，必须加强密码管理，要求管理员账号使用字符、数字、符号组合的复杂密码，长度不小于8位，口令30天定期更换。

（七）存有保密信息的介质（硬盘、U盘、磁盘、闪存、光盘等）如需送到单位外维修时，要将涉密资料备份后，对介质进行技术处理（如低级格式化、写零处理等），以防泄密。

（八）责任人在承担项目工作完成以后，不得保留保密信息的副本，一切关于保密信息的资料销毁或返还信息提供部门，保证信息不会外流；责任人承诺若中途不再从事项目有关工作，仍对保密信息承担保密责任。

（九）责任人同意：若违反本承诺书内容，一经发现，学校可视行为严重程度进行行政处分或经济处罚。后果严重者，学校将通过法律途径向责任人索赔，或向司法机关报案处理。

(十)责任人的保密义务至保密信息公开或被公众知悉时终止。

第二十四条 各业务数据的主管部门须与接触到本部门业务数据的内外责任人签订《郑州轻工业学院数据保密协议（见附件三）》，促使对方落实学校数据保密。

第二十五条 涉及国家保密法和其他行政法律法规所规定情形应遵照对应法律法规执行。

第七章 应急处置

第二十六条 网络信息安全事件

网络信息安全事件是指在我校园网和信息系统上发生的服务器病毒感染、安全漏洞、网络攻击、系统侵入、数据篡改、数据泄密等事件。

第二十七条 处置机构及其职责

参与网络信息安全事件应急处置的工作机构包括：学校信息化领导小组、信息化管理中心、信息系统建设使用单位、所涉系统厂商/集成商、用户，以及其他相关部门和工作人员。

（一）信息化管理中心负责网络信息安全事件应急处置的统筹工作；负责按照国家法律、上级有关要求，代表学校履行面向上级的信息安全事件报告与处置的具体工作；

（二）信息系统建设使用单位负责业务应急处置，参与业务信息核实；

（三)所涉系统厂商/集成商负责对所涉及的网络设备、安全设备、信息系统进行安全事件处置技术操作；

（四）用户、其他相关部门根据安全事件的性质和影响，参与到安全事件的处置过程中；

（五）学校信息化领导小组负责检查、评估网络安全事件的处置情况，对重大事项进行决策。

第二十八条 处置过程

（一）信息化管理中心日常做好网络信息安全事件预防和监测工作。其他单位或个人发现或怀疑网络安全事件时，应尽早与信息化管理中心联系。

（二）网络信息安全事件发生时，信息化管理中心组织网络安全厂家将对应服务和系统从学校网络上隔离开，以控制安全事件影响的

进一步扩大。视遭受影响的业务情况通知到建设单位和使用部门，视事件性质和影响程度向学校网络信息安全领导小组和其他部门汇报，必要时直接向公安局报案。

（三）各单位接到通知后，应尽快安排人员参与事件处置，所需安排的人员包括：协助开展业务系统处置的人员、处理业务问题的人员。根据业务遭受影响的程度，妥善进行业务处置，可发布通知停办业务或调整为其他业务受理方式。信息化管理中心负责通知业务系统集成商或厂家参与事件处置，负责业务影响程度评估。

（四）业务系统集成商或厂家与学校信息化管理中心共同开展技术处置，进行安全事件处置。

（五）安全事件处置后信息化管理中心负责组织人员总结评估安全事件的处置过程、结果、损失情况，提出进一步整改和处置措施，报有关部门和领导。

（六）安全事件整改责任部门按要求落实整改工作并制定长效预防机制，形成整改报告报送信息化管理中心。

附件：

附件一：《郑州轻工业学院网络及信息系统安全责任协议》

附件二：《郑州轻工业学院网站安全责任协议》

附件三：《郑州轻工业学院数据保密协议》

附件一：

郑州轻工业学院网络及信息系统安全责任协议

项目名称：_____

甲　　方：_____

乙　　方：_____

第一条　乙方必须严格遵守郑州轻工业学院安全管理规定和管理办法，合理、规范、安全地使用计算机、网络、数据和信息资源。乙方承诺在管理、开发、实施、维护维修项目的过程中，承担安全责任包干如下。

第二条　乙方对系统的硬件、操作系统、网络承担安全责任包干。包括但不限于：（1）保障硬件系统的安全运行状态；（2）对操作系统进行漏洞修补、安全更新；（3）对系统所需的各类网络协议与服务端口进行安全设置；（4）对数据进行备份和加密；（5）对病毒、木马程序及网络上出现的各类攻击手段进行事前防范、应急响应、事后处置等工作。最大限度的保障系统所用软硬件环境的安全。

第三条　乙方对所提供的信息系统及相关辅助软件（如数据库、Web 容器、第三方组件等）承担安全责任包干。包括但不限于：（1）符合学校信息安全技术要求，对学校信息安全环境和其他系统不造成负面影响；（2）对系统进行严格的安全检测、并对安全事件和隐患进行处置；（3）负责落实甲方对系统提出的安全工作指令。

第四条　乙方对乙方工作人员的技术行为承担安全责任包干。包

括但不限于：（1）在对系统进行建设、开发、安装、维护等各类必要的工作过程中，不得在服务器上安装各类与建设维护内容无关的软件（如QQ、支付宝、各类游戏等）；（2）不得在服务器上进行与建设维护内容无关的各类操作（如打游戏、查询股票等）；（3）必须按照甲方提供的登录方式进行工作，不得擅自开启任何后门程序进入；（4）在系统上线之后进行维护操作对系统访问产生影响的，应知会甲方，为甲方提供合理的业务处置时间；（5）做好账号管理工作，防止账号泄露、侵入等事件的发生；（6）履行甲方的安全责任有关要求。

第五条　乙方对安全检测、应急响应和安全事件处置承担包干。包括但不限于：（1）对系统进行经常性的安全检测和监控（每季度不少于一次），并将结果以书面形式报告给甲方；（2）系统被检测出或发生安全问题时，乙方必须在 1 小时内做出响应，24 小时内完成应急处置，有效防止损失的进一步扩大。

第六条　乙方同意：如若乙方无法在规定时间内响应和完成相关安全工作，甲方可自行组织开展相关工作，乙方愿意承担由此产生的费用。

第七条　本协议一式六份，甲方业务部门、乙方、学校信息化管理中心各执二份，经签字确认后生效。乙方若违反本协议愿意承担郑州轻工业学院因此而产生的一切损失。

甲方（盖章）：　　乙方（盖章）：

部门负责人（签字）：　　法人或授权代表（签字）：

签字日期：　　签字日期：

附件二：

郑州轻工业学院网站安全责任协议

为保障学校各类网站的系统安全和内容安全，维护校园稳定和正常教学秩序，根据《中华人民共和国计算机信息安全保护条例》、《中华人民共和国计算机信息网络管理暂行规定》和教育行政主管部门的相关规定，本单位遵守如下规定：

第一条 各单位党政负责人为各自网络信息发布的第一责任人。开通或关闭网站、微博、微信平台之前需到宣传部和信息化管理中心履行登记备案手续；如实登记用途，不提供代理和涉嫌侵权的资源服务；一旦开通需做到及时更新、认真管理、注重质量。

第二条 严肃开展网络信息发布、转载和链接管理工作，做到“统一规范、先审后上、保证质量”的要求。在学校网站、微博、微信等平台上发布的网络信息由宣传部审核后才可发布；不以学校名义在其他传播平台上擅自发布网络信息；不发布与学校、部门职责无关的信息内容和外部链接。

第三条 按照如下要求开展网站安全建设和管理工作

（一）本部门所开设的网站统一使用学校站群系统开发、制作、发布，使用学校域名（zzuli.edu.cn、zzuli.cn）和 IP 地址，并使用学校服务器资源部署于学校数据中心内。特殊情况下须经宣传部和信息化管理中心技术审核后方可调整方案。

（二）合理设置栏目，公开并及时更新单位概况、职能职责、规章制度、办事指南、工作通知、单位动态等内容；未经批准，不开设聊天室、论坛等开放式交互栏目，一旦批准开设，需安排人员认真审核留言内容，做到如实反映群众意见、过滤不良信息、积极引导网上舆论。

（三）采用安全的网络信息发布技术，避免传播带毒文件；引用、转发外部资讯时做到严格审核，并注明来源。

（四）妥善保管网站管理账户信息，使用不易被猜中的密码，并定期更新；对网站管理人员和用户加强网络安全意识教育和业务培训。

（五）始终关注网站的安全状况，及时联系信息化管理中心处置各种安全问题，配合宣传部和信息化管理中心开展网络信息安全工作。

（六）执行读网制度。安排人员每天登录网站读网（包括微博、微信等网络传播平台），认真查看页面显示状况，查看各项功能的有效性，查看所发布的信息特别是重要信息是否存在错漏，查看是否存在暗链，发现问题立即纠正。关注校园网上发布的各类信息，加强沟通合作，做到学校网站与部门网站、部门网站与学校网站、部门网站与部门网站之间信息的准确性、一致性与恰当性。定期检查网站到其他网站的链接，防止因其他网站失效、被篡改等原因导致不良社会影响。

（七）严格落实网站维护管理制度。做到只在校园网内进行运维管理，若需要远程运维或第三方单位（如网站开发单位）协助运维，需要采用 VPN 加密、堡垒机登录等安全方式接入，不得直接远程桌面或直接开放管理端口到互联网。

第四条 校内各单位如违反以上条款，宣传部、信息化管理中心将对违规网站或信息服务进行处理，并上报学校。

宣传部（签字）　　单位（盖章）

日期：

信息化管理中心（签字）　　单位（盖章）

日期：

单位主要负责人（签字）　　单位(盖章)

日期：

附件三：

郑州轻工业学院数据保密协议

第一条　责任人必须严格遵守郑州轻工业学院相关管理规定，合理、规范、安全地使用计算机、网络、数据和信息资源。责任人承诺在管理、开发、实施_____项目的过程中，视所接触到的资料、数据和项目信息为保密内容，承担保密责任。

第二条　来源于郑州轻工业学院的所有资料、数据和项目信息，包括但不限于教职工、学生个人身份信息、郑州轻工业学院组织架构信息、教学、科研、管理、服务等相关业务信息，以及项目建设内部文件、建设规划和建设方案资料。

第三条　责任人未经允许，不得访问、删除、修改、增加、复制、备份、摄录、摘抄、打印数据、资料，绝不擅自传播保密信息。

第四条　责任人保存数据、资料的存储介质（云盘、U 盘、终端存储等）不可交由其它人使用，或作其它用途，或必须妥善保管，严防丢失。

第五条　责任人未经允许，不得进行影响系统运行的操作，如关闭主机（设备）、关闭关键服务、大量数据查询、修改数据库、修改系统配置等。

第六条　责任人对自己管理的账号，必须加强密码管理，要求管理员账号使用字符、数字、符号组合的复杂密码，长度不小于 8 位，口令 30 天定期更换。

第七条　存有保密信息的介质（硬盘、U盘、磁盘、闪存、光盘等）如需送到单位外维修时，要将涉密资料备份后，对介质进行技术处理（如低级格式化、写零处理等），以防泄密。

第八条　责任人在承担项目工作完成以后，不得保留保密信息的副本，一切关于保密信息的资料销毁或返还信息提供部门，保证信息不会外流；责任人承诺若中途不再从事项目有关工作，仍对保密信息承担保密责任。

第九条　责任人同意：若违反本承诺书内容，一经发现，学校可视行为严重程度进行行政处分或经济处罚。后果严重者，学校将通过法律途径向责任人索赔，或向司法机关报案处理。

第十条　责任人的保密义务自本协议盖章之日起开始生效，至保密信息公开或被公众知悉时止。责任人的保密义务并不因双方合作关系的解除而免除。

第十一条　本责任书一式三份，责任部门、责任人、信息化管理中心各执一份，经签字确认后生效。责任人若违反本协议愿意承担郑州轻工业学院因此而产生的一切损失。

责任部门（盖章）：　　责任人（签字）：

责任部门负责人（签字）：　　责任人身份证号：

签字日期：　　签字日期：