西安理工大学文件

西安理工网信〔2019〕1 号

关于印发《西安理工大学网络与信息安全管理办法》的通知

校属各单位：：

《西安理工大学网络与信息安全管理办法》已经 2019 年第 1 次校务会审议通过，现予以印发，请遵照执行。

西安理工大学

2019 年 5 月 28 日

（此页无内容）

校长办公室　　2019年6月4日印发

西安理工大学网络与信息安全管理办法

第一章　总 则

第一条　为建立健全学校网络与信息安全保障体系，加大网络与信息安全应急处置的监管力度，增强信息系统防护能力，保障信息系统稳定运行和网络数据安全，推动学校教育信息化建设顺利发展，依据《中华人民共和国网络安全法》《教育部关于加强教育行业网络与信息安全工作的指导意见》（教技〔2014〕4号）等国家有关法律、规定对网络与信息安全的管理要求，结合学校工作实际，制定本办法。

第二条　学校网络与信息安全工作实行领导责任制和责任追究制。按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，实行“统一领导、分级管理、分工负责、责任到人”，确保学校网络与信息安全工作的系统性和完整性。

第三条　未经学校网络信息管理中心备案批准，任何单位和个人均不得以“西安理工大学××”等与学校名义相关的方式在互联网注册域名和建立信息系统。

第四条　西安理工大学信息系统实行审批备案管理制度，严格执行问题信息系统退出机制。凡使用信息系统的单位和个人，应主动接受和配合上级主管部门、公安部门和网络信息管理中心开展的安全检查、漏洞整改等工作。

第二章　定义和范围

第五条　本办法中的信息系统主要是指:

（一）校属各单位主管、主办或承办的所有业务系统及各级门户网站，包括应用系统、Web 网站、FTP 等文件传输服务、移动 APP、微博、微信相关应用等;

（二）校属各单位及个人申请固定 IP 用于各类公网应用服务的信息系统;

（三）校属各单位内网应用系统、网站提供互联网业务服务的信息系统;

（四）学校师生以西安理工大学名义创建的各类系统及网站，包括使用运营商提供的互联网连接的网站、使用非教育网域名的网站和在本校校园网内开设的外单位网站等。

第六条　本办法涉及的数据包括学校数据交换与共享平台公共数据、各应用系统、数字教学资源库、网站、专用数据库等信息系统产生和保存的数据，以及没有信息系统支撑但已进行电子化维护和保存的各类信息，包括结构化和非结构化数据。

第七条　本办法适用于在学校范围内建设、运营、维护和使用的信息系统；在互联网上以西安理工大学名义建设、运营、维护和使用的信息系统。

第八条　本办法所指的校属各单位包括各学院、二级部门、附属单位等。适用于校属各单位及全体师生员工。

第三章　组织机构和工作职责

第九条　西安理工大学网络安全与信息化领导小组(以下简

称“领导小组”）是学校网络安全与信息化工作的领导机构，其主要职能是：贯彻落实上级的网络安全与信息化战略部署，统筹制定学校网络安全与信息化发展规划和重大政策，研究解决网络安全与信息化重要问题。各成员单位应配合做好学校网络安全与信息化工作，并负责本单位网络安全与信息化日常工作。

第十条 领导小组办公室设在网络信息管理中心，是领导小组的日常办事机构。办公室主任由网络信息管理中心主要负责人兼任；设秘书一名，具体负责领导小组办公室日常工作。

第十一条 网络信息管理中心是学校网络安全与信息化工作的归口管理与技术支撑单位，负责统筹学校网络安全、信息化以及数据管理与数据安全工作，具体包括：

（一）负责制定与实施学校教育信息化发展规划，学校信息化建设的总协调与项目建设推进工作，对信息化项目进行评估和管理；负责学校信息化建设项目的规划、立项、经费管理与使用，为各部门教育信息化建设提供技术支持；

（二）负责学校数据交换与共享平台建设与管理，对数据资源进行统一规划，制定数据标准、编码标准、技术规范和管理规范，监管各信息系统数据资源的采集、治理与合理使用；

（三）负责建立健全学校信息技术安全防护与应急处置体系；统筹网络信息基础设施的运维与安全管理工作；负责网络安全监督检查、网络舆情监控工作；负责信息系统的申请、备案、审核及停用等管理工作；对校属各单位、个人建立的信息系统开展常态化监测，发现存在信息安全事件的信息系统，及时通报、

限时修复、跟踪核查整改结果;

（四）对教育部、省教育厅、省委网信办、省公安厅等上级部门通报的信息系统安全事件，协助相关部门做好整改工作;

（五）面向网络信息员和全校师生，组织开展网络安全宣传教育与技术培训，切实提高网络安全意识和信息素养，提升网络安全保障能力。

第十二条 校属各单位党政主要负责人为本单位的网络安全与信息化管理领导责任人; 各单位应设立网络信息员，负责网络安全保护措施及相关规章制度的落实，并做好网络安全管理工作; 学生团体自建信息系统的网络安全责任由团体负责人及其管理部门共同承担; 师生以个人名义在校园网内自建的信息系统，其网络安全责任由本人及其所在部门承担。

第十三条 校属各单位应针对所建的信息系统设立相应的管理员，负责信息系统的日常管理、维护、监测及信息安全事件的处理工作。

第四章 信息系统的备案与变更

第十四条 校属各单位申请新建信息系统或在校内其他已备案网站上建立链接的信息系统时，应明确网络安全与信息化管理领导责任人和信息系统管理员，提交《西安理工大学信息系统备案登记及域名申请表》(附件 1); 如需开放公网访问权限，还须提交《西安理工大学公网访问权限安全承诺书》(附件 2)。

第十五条 校属各单位、用户通过校园网之外的运营商接入互联网并开设信息服务的信息系统，应参照第四章第十四条如实

向网络信息管理中心履行备案手续，并根据国家相关法律规定完成备案工作。

第十六条 信息系统的域名、人员等备案信息发生变动时，管理员应主动向所属单位网络信息员报备，并于15个自然日内上报网络信息管理中心更新备案信息。逾期未履行上述手续的视为无效备案信息，按照第六章第三十四条规定处理。

第十七条 校属各单位应做好信息系统备案工作，并督促在本单位信息系统上建立链接的其他校内信息系统进行备案。对未按规定向网络信息管理中心进行备案的，应取消在本网站上的链接。

第五章 信息系统安全管理

第一节 上线审核

第十八条 校属各单位的网站应统一纳入网站群系统进行建设和管理，降低网站安全漏洞风险，提升网站安全防护能力；对于各类短期使用的信息系统，到达使用期限后将关闭其互联网服务。

第十九条 网络信息管理中心对申请上线的信息系统进行安全扫描并出具评估报告，符合相关规定的方可予以上线；对于存在安全风险的信息系统，由申请单位完成整改后，经网络信息管理中心重新进行核查，确认无安全隐患后方可上线。

第二节 运行规定

第二十条 校属各单位应建立健全本单位信息系统安全管理制度，采取有效措施加强安全管理。信息系统的开办单位及用户有义务对自己维护的重要系统和数据作周期性异机备份及安

全维护，以防数据丢失和发生信息安全事件。

网络信息管理中心定期在知行网发布《网络安全威胁通告》，包括漏洞影响范围、解决方案等，校属各单位应按照通告要求，核查本单位信息系统，做好漏洞修补工作。

第二十一条 校属各单位的信息系统数据只能通过数据交换与共享平台与校内业务系统进行业务基础数据交换，数据的采集、存储和使用应经网络信息管理中心与相关职能部门审批，严禁私自采集、存储和使用业务数据或与校外第三方系统进行数据交换。实施细则详见《西安理工大学信息系统数据管理办法》。

第二十二条 信息系统的信息安全，坚持“谁发布谁负责、谁管理谁负责”的原则，遵循《计算机信息网络国际联网安全保护管理办法》(公安部令第33号)、《互联网信息服务管理办法》，规范网络行为和信息发布；校属各单位应对本部门网站发布信息内容的准确性和合法性负责，建立完善的网站信息发布与审核制度，明确审核与发布人员名单，保存相关操作记录。

第二十三条 校属各单位应加强信息系统的监控，发现法律、行政法规禁止发布或者传输的信息，应立即停止传输，采取消除等处置措施，防止信息扩散，保存有关记录，并向网络信息管理中心报告。

第二十四条 信息系统上线后，应由本单位管理员进行管理和维护，定期检查信息系统运行状况和内容的合规性、合法性，并及时做好补丁更新，消除安全隐患；对于宣传类、门户类的网站需保证及时更新。

涉及招生、考试、学籍、资助、教师管理等核心业务的重要信息系统，必须建立独立的数据库实例，针对各信息系统数据库实例设置最小权限的管理账户，并严格控制数据库管理员帐户的操作行为。

第二十五条 信息系统的账号和密码应指派专人负责管理。应使用不小于8位、至少三种字符组合的复杂口令，禁止多个账户使用同一口令，并对口令登录尝试次数进行限制，有条件的单位可以采用双因素认证等其它安全模式进行高强度用户认证；应加强对信息系统非授权访问行为的安全审计，并根据业务需求制定数据离线保存策略，做好数据离线保存及数据转移工作。

第二十六条 校属各单位通过信息系统向用户提供服务的，应当采取技术和其他必要措施，维护网络数据的完整性、保密性和可用性。数据安全的技术性要求主要包括：

（一）对数据访问日志进行审计，且日志留存时间不低于180日；

（二）对数据进行分类，将敏感数据与普通数据区别化处理；

（三）对重要数据进行加密、备份、容灾；

（四）对个人信息进行脱敏。

第二十七条 信息系统在委托第三方进行开发时，应注重对运维和安全修复方面条款的要求，在规定或者本部门约定的期限内，应要求第三方不得终止提供安全维护，以确保使用中发生信息安全事件时能快速响应。

第二十八条 任何个人和单位提供的应用软件，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；不得利用黑客软件等手段侵入或干扰信息系统的正常运行；不得利用信息系统漏洞做出有可能危害系统安全或干扰系统正常运行的行为。

第二十九条 任何个人和单位使用网络应当遵守国家法律，遵守公共秩序，尊重社会公德，不得利用网络、信息系统泄露国家秘密及敏感信息；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。

第三节 监测预警与处置

第三十条 网络信息管理中心建立网络安全监测预警和信息通报制度，细则详见《西安理工大学网络安全事件应急管理工作指南》（附件 3）。在发生网络安全事件时，应立即发布应急响应方案，校属各单位应按照方案要求，及时处置系统漏洞、计算机病毒等安全风险，采取相应的补救措施，并按照规定向网络信息管理中心报告。

第三十一条 网络信息管理中心定期对校内信息系统进行安全扫描和风险评估，并将评估报告反馈给各单位网络信息员，由网络信息员协调组织涉及问题的信息系统管理员处理安全隐患。对于存在高风险安全隐患的信息系统，将停止其互联网访问，

并责令在5个工作日内修复，逾期未修复的将被关闭，待整改审核后，重新上线；对于发生信息安全事件的信息系统，无法联系到网络信息员和管理员时，视为无人管理维护，进行关停处理，并对域名或IP进行回收。

第三十二条 网络信息管理中心负责学校网络安全监控预警工作，对于发生信息安全事件的信息系统，即被教育部、省教育厅、省委网信办、省公安厅等上级部门通报的，将按照《西安理工大学网络安全事件应急管理工作指南》（附件3）规定，停止其互联网访问，并通知涉事单位3个工作日内完成修复与整改。整改完成后，涉事单位须提交书面整改报告至网络信息管理中心，经整理、核查后，上报有关单位。

第六章 考核规则

第三十三条 校属各单位的网络安全工作实施考核评价制度，并将各单位履行网络安全工作责任制及日常相关工作情况纳入学校年度考核及评优工作。

第三十四条 网络信息管理中心对无人运维或运维缺乏基本保障、未进行备案以及发生安全问题的信息系统有权采取关停措施，并对域名或IP进行回收。

第三十五条 对管理不当或用户账号和口令过于简单，造成信息系统数据丢失、不良信息被发布、弱口令等，责令整改，并追究相关人员的责任；情节较重的，将追究部门负责人的领导责任。

第三十六条 对所开办信息系统因监管不力，发生重大安全

事件，产生不良影响或严重后果的，由网络安全与信息化领导小组办公室进行调查后上报网络安全与信息化领导小组，结合学校有关规定对相关责任人进行追责。

第三十七条 违反本管理办法第五章第二十六条，未按要求采取技术措施的，责令责任人十五日内进行整改。逾期未整改或整改不力的，上报网络安全与信息化领导小组，按照学校有关规定处理。

第三十八条 违反本管理办法第五章第二十八条、第二十九条的，由网络安全与信息化领导小组办公室联合相关部门进行调查后，进行网络安全事件定级认定，填写网络安全事件级别认定表（附件 4），并上报网络安全与信息化领导小组，按照学校有关规定处理；拒不改正或者导致危害网络信息安全等严重后果的，根据学校有关规定给予以纪律处分。触犯法律的，移交司法机关处理。

第三十九条 对于其它违反本管理办法的行为，由西安理工大学网络安全与信息化领导小组按学校相关管理办法进行处罚。

第七章 附 则

第四十条 本办法自发布之日起实施，由网络信息管理中心负责解释。

附件 1

西安理工大学信息系统备案登记及域名申请表

年　　月　　日

<table>
<tr><td>单 位 名 称</td><td colspan="5"></td></tr>
<tr><td rowspan="2">单位负责人</td><td>姓　名</td><td></td><td>联系电话</td><td colspan="2"></td></tr>
<tr><td>E-mail</td><td colspan="4"></td></tr>
<tr><td rowspan="2">技术负责人</td><td>姓　名</td><td></td><td>联系电话</td><td colspan="2"></td></tr>
<tr><td>E-mail</td><td colspan="4"></td></tr>
<tr><td>名称</td><td colspan="5"></td></tr>
<tr><td>信息系统类别</td><td colspan="5">□网站　　□ 管理信息系统　　□ 其他: _____</td></tr>
<tr><td>信息系统功能</td><td colspan="5"></td></tr>
<tr><td>开通时间</td><td colspan="5" rowspan="2">短期信息系统需填写这项内容</td></tr>
<tr><td>到期时间</td></tr>
<tr><td>拟 申 请 的 域 名</td><td colspan="5">.xaut.edu.cn</td></tr>
<tr><td>服 务 器 IP地 址</td><td colspan="5"></td></tr>
<tr><td>信息系统开发语言</td><td colspan="2"></td><td>数据库版本</td><td colspan="2"></td></tr>
<tr><td>网络信息员签名</td><td colspan="5"></td></tr>
<tr><td>申请单位签字
（盖章）</td><td colspan="5">负责人签字（盖章）:
日期:</td></tr>
<tr><td>党委宣传部签字
（盖章）</td><td colspan="5">负责人签字（盖章）:
日期:</td></tr>
<tr><td>网络信息管理中心
（盖章）</td><td colspan="5">负责人签字（盖章）:
日期:</td></tr>
</table>

填表说明

1、使用学校域名或 IP 地址设立信息系统，应填写本表，在网络信息管理中心备案；校属各单位、用户通过校园网之外接入互联网并开设信息服务的信息系统，应如实向网络信息管理中心填报相关信息，进行备案；申请注册学校校园网域名，也适用本表。

2、本表所列备案信息有变动时，网站主办者应在相关变更发生之日起 30 日内向网络信息管理中心履行备案变更手续。

3、申请注册学校互联网络域名，应符合学校互联网络域名体系。域名的名称应使用组织机构名称、信息系统业务名称、活动（会议）主题的英文、英文缩写、汉语拼音或汉语拼音缩写。原则上，不得使用个人姓名及缩写作为域名的名称。

4、填写本表，应先阅读《西安理工大学网站管理办法》和《西安理工大学互联网域名管理办法》及《西安理工大学网络与信息安全管理办法》

5、对于短期使用的信息系统，申请上线时，需填写信息系统的开通、到期时间。

6、网络信息管理中心联系电话：82312079，电子邮箱：nic@xaut.edu.cn，地址：教 6 楼 10 层 1011 室（信息管理部）。

附件 2

西安理工大学公网访问安全承诺书

本单位因 **<填写项目名称>** 需开放公网访问权限，郑重承诺遵守本承诺书的所列事项，对所列事项负责，如有违反，由本单位承担由此带来的相应责任。

一、本单位承诺遵守《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》、《计算机信息网络国际互联安全保护管理办法》和《信息安全等级保护管理办法》等国家网络与信息安全的有关法律、法规和行政规章制度。

二、本单位已知悉并承诺执行《西安理工大学计算机网络管理办法》、《西安理工大学网络与信息安全管理办法》、《网站建设管理办法》、《信息系统建设管理办法》等西安理工大学网络安全有关工作的文件规定。

三、本单位保证不利用网络危害国家安全、泄露国家秘密，不侵犯国家的、社会的、集体的利益和第三方的合法权益，不从事违法犯罪活动。

四、本单位承诺完善本单位的信息技术安全管理，建立健全信息技术安全责任制和相关规章制度、操作规程；加强信息系统安全，落实信息系统安全等级保护制度，提高信息系统安全防护能力。

五、本单位承诺提升应急响应能力，制定本单位应急预案，

对本单位的信息系统进行安全监测，并对监测发现和通报的安全问题进行限时整改；当信息系统发生信息技术安全事件，迅速进行报告与处置，将损害和影响降到最小范围，并按照要求及时进行整改。

六、本承诺书自签署之日起生效，一式两份，网络信息管理中心、申请单位各执一份。

信息系统主要负责人（签字）:

单位主要负责人（签字）:　　单位盖章

年　　月　　日

附件 3

西安理工大学网络安全事件应急管理工作指南

1 总则

1.1 编制目的

为建立健全我校网络安全事件应急工作机制，提高网络安全事件应急防范能力，预防和减少网络安全事件造成的损失和危害，保障校园基础信息网络和信息系统正常运行，保护校园网用户权益，结合我校工作实际，制定本指南。

1.2 编制依据

《中华人民共和国网络安全法》、《中华人民共和国突发事件应对法》、《国家网络安全事件应急预案》、《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007）、《教育部教育系统网络与信息安全类突发公共事件应急预案》、《教育部信息技术安全事件报告与处置流程（试行）》（教技厅函〔2014〕75 号）等相关规定。

1.3 适用范围

本指南所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对学校网络和信息系统或者其中的数据造成危害，对我校工作、学习、生活秩序及学校在社会上的形象造成负面影响的事件。

本指南所称的网络是指校园网络基础设施，信息系统请参照《西安理工大学网络与信息安全管理办法（试行）》中第五条；重要网络是指校园网核心设备；重要信息系统是指学校门户网站、各单位主要对外服务网站及涉及核心业务（招生、考试、学籍、资助、教师管理等）的信息系统。

1.4 事件分类与定级

网络安全事件依据发生过程、性质和特征不同，可分为以下几类：

（1）有害程序事件：蓄意制造、传播有害程序，危害学校系统中数据、应用程序或操作系统的保密性、完整性或可用性，而导致校园网络和信息系统运行异常的信息安全事件；

（2）网络攻击事件：通过网络或其他技术手段，利用学校网络和信息系统的配置缺陷、协议缺陷、程序缺陷或使用暴力实施攻击，并造成学校网络和信息系统异常的信息安全事件；

（3）信息破坏事件：通过网络或其他技术手段，造成学校信息系统中的信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件；

（4）信息内容安全事件：利用互联网、校园网发布、传播危害国家安全、社会稳定和公共利益的内容的安全事件；

（5）设备设施故障：由于学校网络与信息系统自身故障或外围保障设施故障而导致的业务中断、系统宕机、网络瘫痪等情况，以及人为的使用非技术手段有意或无意的造成网络与信息系

统破坏而导致的信息安全事件;

（6）灾害性事件：由于不可抗力（包括水灾、台风、地震、火灾、恐怖袭击等）对学校网络与信息系统造成物理破坏而导致的信息安全事件。

网络安全事件按照可控性、严重程度和影响范围不同，可划分为四级：

（1）I 级（特别重大网络安全事件）：学校重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力，或学校重要敏感信息和关键数据被窃取、篡改，或利用互联网及校园网发布非法信息引发学校大规模群体性事件，对学校教学、工作造成特别严重损害，造成特别严重的社会影响，事态发展超出学校控制能力;

（2）II 级（重大网络安全事件）：学校重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响，或学校重要系统数据被窃取、篡改，或利用互联网及校园网发布非法信息引发局部群体性事件，对学校教学、正常工作造成严重损害，造成一定社会影响，事态发展超出技术部门控制能力，需要相关单位协同处置;

（3）III级（较大网络安全事件）：学校局部重要网络和信息系统遭受较大的系统损失，造成系统中断、故障，业务处理能力受到影响，或利用互联网及校园网发布敏感信息、谣言等引起不良影响，对学校教学、工作造成一定危害，但未造成社会影响，

事态发展相关负责单位可控;

（4）IV级（一般网络安全事件）：学院或单位重要网络和信息系统受到一定程度损害，学院或单位的正常教学、工作受到一定影响，但不危害学校整体工作。

除上述情形外，对学校教学、工作和校园网用户利益构成一定威胁、造成一定影响的网络安全事件，亦为一般网络安全事件。

1.5 工作原则

坚持统一领导、分级管理、分工负责、责任到人；坚持预防为主，快速反应、科学处置；坚持“谁主管谁负责、谁运营谁负责、谁使用谁负责”，充分发挥校属各单位力量共同做好网络安全事件的预防和处置工作。

2 组织机构和工作职责

2.1 西安理工大学网络安全与信息化领导小组，是学校网络安全的领导机构，负责统筹规划我校网络安全事件应对工作，建立健全跨部门联动处置机制，对学校网络安全中的重大问题和政策性问题进行决策，负责特别重大网络安全事件、重大网络安全事件处置的组织指挥和协调。

2.2 网络信息管理中心负责学校网络安全事件的具体处置工作，其职责包括：

（1）负责学校网络安全应急工作的组织、协调、预防、监测、监督，制定学校相关安全制度和应急预案；根据网络安全事件程度提出相应级别应急预案的启动，负责网络安全应急跨部门

协调工作和事务性工作;

（2）负责校园基础网络系统安全，对学校发生网络安全事件的单位,在处置工作中履行职责情况进行检查督办;及时收集、通报和上报网络安全事件处置的有关情况;

（3）牵头组织重大敏感时期、重要活动、重要会议期间网络安全的保障工作和网络安全事件应急处置工作,并对校园网络整体进行 7*24 小时监控。

2.3 校属各单位负责本单位网络和信息系统网络安全事件的应急处置工作，应对照本指南，建立网络安全应急处置机制。

3 监测与预警

3.1 预警监测

（1）网络信息管理中心建立网络安全监测预警和信息通报制度，健全技术防护体系，规范信息系统安全应急处置流程，确保信息安全应急处置工作落到实处;

（2）网络信息管理中心组织对校属各单位信息系统进行安全监测，定期进行安全扫描和风险评估，并出具评估报告反馈至相关单位;

（3）校属各单位按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，加强信息系统的监管力度，组织对本单位建设运行的网络和信息系统开展网络安全监测工作,进一步完善管理制度和技术保障措施，确保信息系统安全运行。

3.2　预警研判和发布

网络信息管理中心对互联网安全预警信息及校园网运行监测信息进行研判，认为需要立即采取防范措施的，及时发布预警通知，研究制定防范措施，做好校园整体安全防护；同时组织学校各单位做好保护措施，对可能发生重大及以上网络安全事件的信息及时向西安理工大学网络安全与信息化领导小组报告。

预警信息包括事件的类别、级别、起始时间、可能影响范围、警示事项、应采取的措施和时限等要求。

4　应急处置

4.1　事件报告

网络安全事件发生后，网络信息管理中心第一时间采取限制互联网访问措施，根据事件级别启动应急预案，事发单位应按照本单位应急处置机制，控制事态发展，实施处置并及时报送信息至网络信息管理中心。对于初判为特别重大、重大网络安全事件的，网络信息管理中心应立即报告西安理工大学网络安全与信息化领导小组。

4.2　应急响应

网络安全事件应急响应分为四级，分别对应特别重大（Ⅰ级）、重大（Ⅱ级）、较大（Ⅲ级）和一般网络安全事件（Ⅳ级）。

4.2.1　Ⅰ级响应

属特别重大网络安全事件的，网络信息管理中心及时启动Ⅰ级响应，确认事件的来源与类别，评估事件带来的影响和损害，

上报西安理工大学网络安全与信息化领导小组，由领导小组组织协调成员单位实施处置，结合各自实际有针对性地加强防范，防止造成更大范围的影响和损失，控制事态发展。在报告学校的同时，应及时报告陕西省教育厅；对于存在违法犯罪行为的，还应第一时间向公安机关报案。网络信息管理中心实行 24 小时值班。

4.2.2　II 级响应

属重大网络安全事件的，网络信息管理中心及时启动 II 级响应，确认事件的来源与类别，评估事件带来的影响和损害，上报西安理工大学网络安全与信息化领导小组，由网络信息管理中心组织协调事发单位及有关单位实施处置，防止造成更大范围的影响和损失，控制事态发展。在报告学校的同时，应及时报告陕西省教育厅，存在违法犯罪行为的，还应第一时间向公安机关报案。

4.2.3　III 级、IV 级响应

根据事件级别，网络信息管理中心及时启动相应预案，确认事件的来源与类别，由网络信息管理中心组织协调事发单位实施处置，防止造成更大范围的影响和损失。

4.2.4　信息系统网络安全事件发生后，还应按照陕西省教育厅《关于进一步加强我省教育信息系统安全应急处置工作的通知》（陕教保办〔2017〕15 号）文件要求，责令涉事单位 3 个工作日内修复整改，并填写《陕西省教育信息安全事件处置反馈表》，由网络信息管理中心进行核查后，上报省教育厅。

4.3 应急结束

特别重大网络安全事件由西安理工大学网络安全与信息化领导小组组织有关单位进行调查处理和总结评估，由网络信息管理中心汇总后，按程序上报。重大及以下网络安全事件由事件发生单位自行组织调查处理和总结评估，其中重大网络安全事件相关总结调查报告应上报网络信息管理中心。总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施，找出问题根源，以绝后患。

5 保障措施

5.1 机构和人员

校属各单位要落实网络安全应急工作责任制，把责任落实到具体部门、具体岗位和个人，并建立健全应急工作机制。

5.2 技术支撑队伍

加强网络安全应急技术支撑队伍建设。网络信息管理中心建立学校网络信息安全员队伍，建立顺畅高效的网络安全事件应急处理与协调机制。校属各单位应落实本单位网络信息员，负责本单位网络安全的统筹管理工作，并针对所属信息系统设立相应的管理员，负责信息系统的监测及安全事件的处理工作。

5.3 安全培训和演练

网络信息管理中心定期对各单位网络信息安全员和管理员进行网络安全知识培训，增强预防意识和应急处置能力，有针对性地开展应急演练，确保相关措施有效落实。

5.4 经费保障

学校为网络安全事件应急处置提供必要的资金保障。网络信息管理中心利用现有政策和资金渠道，支持网络安全应急技术支撑队伍建设、专家队伍建设、基础平台建设、技术研发、预案演练、物资保障等工作开展。

6 附则

6.1 本指南每年应根据网络技术的发展进行修订和补充完善。

6.2 本指南由网络信息管理中心制定并负责解释。

6.3 本指南自发布之日起实施。

附件 4

网络安全事件级别认定表

部门名称：　　报告时间：____年___月___日

<table>
<tr><td rowspan="2">联系人</td><td rowspan="2"></td><td>手机</td><td colspan="2"></td></tr>
<tr><td>电子邮箱</td><td colspan="2"></td></tr>
<tr><td>责任人</td><td></td><td>网络信息员</td><td colspan="2"></td></tr>
<tr><td>部门负责人</td><td colspan="4"></td></tr>
<tr><td>安全事件名称</td><td colspan="4"></td></tr>
<tr><td>安全事件类别</td><td colspan="4">□安全漏洞　□暗链　□网页篡改　□弱口令
□信息泄露□系统后门　□网页挂马
□其它_____</td></tr>
<tr><td>安全事件级别</td><td colspan="4">□　Ⅰ级特别重大网络安全事件
□　Ⅱ级重大网络安全事件
□　Ⅲ级较大网络安全事件
□　Ⅳ级一般网络安全事件
□　一年内被漏洞平台通报三次及以上
□　其他</td></tr>
<tr><td>信息系统
基本情况</td><td colspan="4">1.系统名称:
2.系统网址和 IP 地址:
3.系统主管单位/部门:
4.系统运维单位/部门:
5.系统使用单位/部门:
6.系统主要用途:
7.是否定级　□是　　□否，所定级别:
8.是否备案　□是　　□否，备案号:</td></tr>
</table>

存在安全事件 主要原因	
处理过程 及结果	
网络安全与信息化领导小组办公室认定处理意见	公章：_____ 负责人签名：
人事处 审核意见 （签字）	公章：_____ 负责人签名：
网络安全与信息化领导小组审定意见 （签字）	