西安开放大学文件

西开大发〔2024〕80号

西安开放大学
关于印发《西安开放大学网络安全与信息化工作管理办法》的通知

各处室、各直属办学单位:

为进一步加强和规范学校网络安全和信息化建设工作，确保网络安全和信息化建设项目科学、规范、合理有序实施，全面提高网络安全和信息化建设质量，保证网络安全和信息化建设可持续发展，对西开大发〔2022〕28号《西安开放大学网络安全与信息化工作管理办法》进行了修订。经学校党委会研究通过，现将

修订后的管理办法予以印发，请遵照执行。

西安开放大学

2024年12月12日

西安开放大学
网络安全与信息化工作管理办法

第一章　总　则

为加强西安开放大学（以下简称学校）网络安全与信息化管理，提高学校网络信息安全防护能力，提升信息化建设与管理水平，为全校师生和社会公众提供安全、可靠、稳定的网络服务和信息服务，保障学校各项事业健康有序发展，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》《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》《西安市教育系统网络与信息安全管理办法(暂行)》及《财政部网络安全和信息化建设管理办法》等国家有关法律、法规对网络与信息技术安全管理的要求，结合学校实际，制定本办法。

第一条 网络安全和信息化建设与管理中必须坚持党的统一领导，按照归口管理、一体化推进的要求，遵循以下原则：统筹规划、统一标准；突出重点，分步实施；整合共享、讲求效益；加强管理，确保安全。实行学校、业务主管部门、使用部门分级管理制度，明确职责范围与责任。

第二条 本办法所称网络安全和信息化建设是指根据学校各处室提出的建设需求，应用技术手段而进行的学校网络安全和信息化建设，内容包括：学校网络安全和信息化规划设计、应用系统建设与运行维护，安全、网络、机房、系统软硬件等基础设

施建设与运行维护，学校信息、数据资源开发利用，学校网络安全和信息化标准规范制定，学校网络安全和信息化管理等。

第三条 学校校园网络是指由西安开放大学投资建设，为学校教学、科研、管理及办学服务的计算机网络，包含校园有线网络、无线网络。

第四条 网络与信息安全是指保护校园网络硬件设施、各类信息系统（含网站）及其承载的信息内容，不因偶然或恶意的原因导致信息数据被攻击、泄露、更改、破坏、未经授权访问和使用，保障网络服务不中断，信息系统（含网站）连续、可靠、正常地运行，确保信息内容的机密性、完整性、可用性、可控性和不可否认性。

第五条 信息安全等级保护制度是国家提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设健康发展的一项基本制度。学校按照“同步规划、同步建设、同步运行”的原则，规划、设计、建设、运行、管理网络与信息安全设施，建立健全网络与信息安全防护体系，全面实施信息系统安全（含网站）等级保护制度。

第二章　组织机构及职责

第六条 按照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中“分级管理、逐级负责”的指导原则，建立西安开放大学网络安全与信息化工作领导小组（以下简称“学校网信领导小组”），学校党委书记和校长任组长，其他校领导任副组长，

现代教育技术处、办公室、财务处、纪检监察室、后勤保卫处负责人为成员。主要职责有:

（一）研究部署国家、省、市网络安全和信息化发展战略、方针政策在学校的贯彻落实;

（二）审定学校网络安全和信息化工作规章制度、发展规划、年度计划;

（三）决策学校网络安全和信息化重大事项;

（四）组织领导学校网络安全和信息化重大事件的应急处置;

（五）审议学校网络安全和信息化工作领导小组办公室的工作报告;

（六）对网络安全和信息化建设工作进行检查评估与考核。

第七条 学校网络安全和信息化工作领导小组办公室（以下简称“学校网信办”）设在现代教育技术处，是学校网络安全和信息化建设的管理和执行机构。现代教育技术处负责人任主任，网络中心相关工作人员为成员。学校网信办主要职责有:

（一）在学校网信领导小组的领导下，负责学校网络安全和信息化建设工作的统一管理、统一协调;

（二）编制学校网络安全和信息化建设规划，拟订学校网络安全和信息化规章制度、标准规范及重大突发事件应急预案，并监督落实;

（三）整理报告学校网络安全和信息化年度工作情况;

（四）研究分析学校网络安全和信息化建设需求，审定学校

网络安全和信息化建设的项目立项和鉴定，并监督、指导项目建设、实施、验收、运维等；

（五）健全信息技术安全防护体系，组织开展学校网络与信息安全不稳定隐患的排查，登记汇总、梳理归档。

第八条 学校网络安全和信息化工作实行归口管理、分级负责，网络安全和信息化工作应列入各部门年度工作计划。各部门主要负责人是本部门网络安全和信息化工作第一责任人，负责本部门网络安全和信息化工作的推进和落实；各部门设置网络安全和信息化管理员（简称网信管理员），并报备学校网信办，网信管理员负责本部门网站及信息系统的日常管理、相关业务系统数据的更新和维护等具体工作。

第三章 信息基础设施建设与管理

第九条 学校网络安全和信息化基础设施是指为学校师生提供网络、信息服务的物质工程设施，包括：数据中心机房（含精密空调、UPS 等设备设施）、校园网络（含有线和无线）、信息化设备(含网络设备、安全设备、存储设备、服务器、终端设备等)、校园范围内建设的各类通讯管线、通讯电缆和光缆、弱电设备间、楼内弱电布线等。

第十条 学校信息化基础设施建设由现代教育技术处牵头组织实施和管理，各部门配合；各部门专用实验实训室的建设由各部门牵头组织实施、管理。

第十一条 学校基建工程应将工程范围内的信息化基础设

施（如楼宇网络等）建设纳入工程预算及实施验收范畴，并提前告知现代教育技术处参与前期规划、设计等。学校信息基础设施管理权属于现代教育技术处，校园信息基础设施的新建、扩建、改造、使用、变更等，由现代教育技术处负责组织实施。

第四章　网络安全威胁监测和预警

第十二条 网络安全监测预警和信息通报工作应遵循及时发现、科学认定、有效处置的原则，通过建立监测预警和信息通报机制，对风险进行预警，做到“早发现、早报告、早处置”，减少和防止不良信息的传播，确保信息网络的畅通和安全。

第十三条 借助网络监测设备、安全设备等技术手段，现代教育技术处负责对全校网络环境、信息系统和网站进行安全监测及防护，监测内容包含通信线路状态、网络设备运行状况、网络流量、网络基础服务、恶意 IP 地址、恶意电子邮件、恶意程序、应用服务器高危漏洞和弱密码等各类网络安全隐患，对监测中发现的安全问题及时通报相关部门处置。

第十四条 网络安全预警信息来源以教育部、省教育厅、网信部门等上级或主管机关以及国内外安全组织发布的网络安全威胁信息为主。在收到上级单位的安全信息通报时，学校网信领导小组及学校网信办应立即对所收到的通报进行分析判断、汇总归纳整理，并根据所收到的内容进行有针对性的归口整改通报。

第十五条 网络安全通报处置程序如下：

（一）现代教育技术处接收到网络安全通报后，第一时间向

学校网信领导小组汇报;

（二）同时将通报内容转发给责任部门负责人，并抄送给分管校领导;

（三）责任部门根据通报内容在规定时间内实施信息系统整改并撰写整改报告，加盖公章后将纸质整改报告反馈给学校网信办;

（四）学校网信办将整改报告上报主管单位。

第十六条 现代教育技术处负责对各类突发网络安全事件和可能引发突发事件的有关信息进行收集、分析、判断和持续监测，出现异常情况时，及时发布最新网络安全威胁信息和解决方案。

第十七条 网络安全预警信息报送的内容应包括:

（一）信息基本情况描述;

（二）可能产生的危害及程度;

（三）可能影响的用户及范围;

（四）截至信息报送时已知晓该信息单位/人员范围;

（五）建议应采取的应对措施及建议。

第五章　信息标准和信息编码

第十八条 学校网信办参照教育部、省、市、国家开放大学等相关标准制定并发布本校的信息标准、数据共享和交换规范，对信息标准实施统一管理，协调解决信息标准编制中的冲突，有权责令编制冲突相关部门进行整改。

第十九条 各部门新开发的信息系统必须使用统一的信息编

码，保持学校信息编码的唯一性，严格执行统一的信息编码，不得随意增加、删除编码。如需修订，须报学校网信办审核后统一修订。

第二十条 已上线运行的信息系统，若信息编码规则与学校信息标准不一致，应使用学校信息标准进行替换，存在替换困难的，可暂时通过代码转换接入使用，待系统升级时更正。

第六章　网络与信息安全管理

第二十一条 学校网络与信息安全工作由网络安全、系统安全和信息内容安全三部分组成。网络安全是指校园网基础设施的安全，设施包括：光纤通信线路、弱电设备间、弱电布线和路由器、交换机等；系统安全是指承载信息系统的服务器、软件运行环境以及系统数据的安全；内容安全是指通过网络发布的各种信息中具体内容的安全。

第二十二条 学校网络与信息安全工作按照“谁主管、谁负责，谁运营、谁负责，谁使用、谁负责”的原则进行。各部门负责人为本部门的网络信息安全责任人，网信管理员和普通用户也承担相应的网络信息安全责任。

第二十三条 现代教育技术处牵头负责网络安全和系统安全，包括：校园网基础设施、门户网站、校园网互联网接入、统一身份认证、数据中心机房、学校综合业务应用服务管理信息系统等；各部门负责其主管的信息系统安全和内容安全，做好必要的数据备份和归档工作；办公室牵头负责门户网站新闻栏目的信

息内容安全工作。

第二十四条 现代教育技术处定期组织开展对学校及各部门负责的信息系统和网站进行恶意代码、安全漏洞等技术检测，对存在高安全风险的信息系统和网站下达限期整改通知书，责令有关部门限期完成安全整改，并在整改完成后进行安全复查。各部门应积极配合实施安全检查，及时修补系统漏洞和处置异常访问等操作，现代教育技术处提供指导和必要的协助。

第二十五条 校园网用户应遵守《中华人民共和国网络安全法》《网络安全审查办法》等国家法律法规，不得利用校园网从事违反国家法律法规和学校规章制度的活动，不得利用信息系统或校园网站，制作、复制、查阅、传播涉密信息和《互联网信息服务管理办法》所禁止的内容。校园网用户应妥善保管自己的校内个人系统账号，因个人账号管理不善对信息安全造成严重危害的，应追究当事人责任。

第二十六条 在紧急情况下，现代教育技术处可以采取特别技术措施以维护校园网的网络信息安全。

第二十七条 任何部门或个人，不得利用网络及计算机信息系统从事危害国家安全、学校安全和师生合法权益的活动，不得危害校园网络及信息系统的安全。

第七章 网络安全和信息化项目的建设与管理

第二十八条 学校网络安全和信息化建设项目包括智慧校园应用平台、系统、移动应用程序（APP、小程序等）的开发和

集成、各类教学、教务、科研、管理及服务工作的信息系统及相关产品、校园网络安全建设、校园网络基础设施建设和网络基础应用等。

第二十九条 学校网信办组织各部门上报本部门网络安全和信息化建设需求及规划（填写《西安开放大学网络安全和信息化项目需求申报表》（附件1）；初审通过后，提交学校网信领导小组审批，审批通过后由学校网信办组织行业专家进行立项项目论证，形成专家组论证意见，申报部门根据专家意见修改完善申报书；项目立项完成后由现代教育技术处提出项目预算申请，报学校预算管理部门审核报批。未经学校网信办批准的项目，不得自行筹集经费组织建设。

第三十条 网络安全和信息化项目实施管理应建立健全责任制，由现代教育技术处统筹、业务需求部门协同负责，严格执行政府采购、合同管理、内部控制、验收评价等制度，遵循国家有关网络安全和信息化建设与实施的标准规范，验收通过后方可投入使用。

第三十一条 平台、系统及移动应用程序必须按照《计算机信息系统安全保护等级划分规则》《信息系统安全等级保护管理办法》等相关规定，开展安全等级定级、评估、安全测评，不符合等级保护要求的系统不得投入正式运行。

第三十二条 所有平台、系统及移动应用程序均须办理登记备案，各归属部门须向现代教育技术处提交《西安开放大学平台、

系统及移动应用程序备案表》（附件 2），并配合完成有关备案的协调工作，备案通过后方可上线使用。登记备案的信息包括但不限于信息系统名称、主办（主管）部门、责任人、技术管理员、服务器放置地、数据库类型、开发商、域名、IP 地址、开放端口、运行有效期等。

第三十三条 由上级组织明确发文要求推广的有关移动应用程序，可不作准入审查，直接登记备案后推广。未按照要求完成备案和审核的，不得上线推广使用。

第三十四条 各部门部署在校内的信息系统原则上须使用学校互联网 IP 地址和学校互联网络域名后缀（xaou. sn. cn），不得私自建立以西安开放大学命名的网站。

第三十五条 各归属部门负责本部门平台、系统及移动应用程序的使用和管理，负责对其进行安全加固、数据维护和备份，并签署网络安全和信息化安全承诺书（附件 3）。

第三十六条 各部门网信管理员（或系统管理员）应积极参加学校组织的应用系统培训活动，熟练掌握各应用系统的操作方法，及时做好本部门人员培训工作和应用系统的推广使用。

第八章 安全保障与处置

第三十七条 现代教育技术处定期对学校各信息系统和互联网站安全状况、安全保护制度及措施的落实情况进行自查，并配合有关部门的信息安全检查、信息内容检查、保密检查与审批等工作。对于已经废弃使用的信息系统、互联网站和移动应用程

序，协同建设管理部门及时关停，并更新备案信息。

第三十八条 现代教育技术处应建立网站应急值守制度，规范应急处置流程，由专人对学校门户网站进行监测，发现网站运行异常及时处置。对于使用频率不大、阶段性使用的网站，可采取非工作时间或寒暑假、节假日关闭的方式运行。各部门网信管理员应对本部门管理的网站平台等进行监测，发现运行异常及时处置并上报学校网信办。

第三十九条 学校内网站与信息系统在委托第三方进行开发时，注重对运维和安全修复方面条款的要求，在服务合同中明确网络与信息安全保密责任，不得将学校数据提交给境外机构，确保使用中出现网络安全相关问题时，能积极响应并迅速解决。

第四十条 加强信息系统的账号管理和权限管理。严格规范系统管理员账号和特权账号的密码设定规则，避免使用过于简单的密码，并做到定期更换。管理员账号和特权账号不得交予他人登录系统。信息系统账号授权应采取最小化授权原则，不得授予超出工作内容范围的信息系统管理与操作权限。

第四十一条 学校加强对系统维护和系统账户管理，严格管理系统账户密码及账户授权。因岗位或职责发生变更时，及时更改系统管理账户密码和相关账户授权，避免授权不当的风险。因密码或数据泄露造成损失和不良后果的，追究相关人员责任。

第四十二条 任何部门和个人出现或发现网络安全与信息安全事故时，应按照《西安开放大学网络安全与信息安全应急预

案》（附件 4）所规定的流程，第一时间报告现代教育技术处，根据安全事件的级别进行相应处置；同时，根据网络与信息安全事故类型，向学校后勤保卫处报告网络违法犯罪行为，向学校办公室报告有害信息发布行为，做好事发紧急报告与处置、事中情况报告与处置、事后整改报告与处置工作。未按要求及时报告的，学校将给予通报批评，依纪依法追究相关人员的责任。

第四十三条 重要或特殊时期，根据上级部署和学校要求，学校对校园网络、信息服务和信息系统采取加强性应急保护措施，对校园网络通信及信息系统进行不间断监控。

第四十四条 学校制定网络安全和信息化培训规划，组织开展形式多样、针对性强的网络安全宣传教育和技能提升活动，不定期举办各类培训讲座，提高全校师生的网络安全防范意识与信息化能力水平。

第九章 附则

第四十五条 对于涉及国家秘密的信息系统，按照国家保密工作部门的相关规定和标准进行保护，接受学校党委保密委员会及上级部门监督指导。

第四十六条 本办法将根据国家相关法律法规、学校的相关要求变化做出相应调整。

第四十七条 本办法自发布之日起执行，原西开大发〔2022〕28 号文件即行废止。

第四十八条 本办法最终解释权归现代教育技术处所有。

附件：1.西安开放大学网络安全和信息化项目需求申报表

2.西安开放大学平台、系统及移动应用程序备案表

3.西安开放大学网络安全和信息化安全承诺书

4.西安开放大学网络安全与信息安全应急预案

附件 1

西安开放大学
网络安全和信息化项目需求申报表

项目名称				
项目类型				
项目建设部门				
项目负责人	姓名		联系电话	
项目联系人	姓名		联系电话	
项目拟实施周期				
项目简介				
建设的必要性				
建设部门负责人审核意见				
学校网信办审核意见				

附件 2

西安开放大学
平台、系统及移动应用程序备案表

责任部门信息			
部门名称(盖章)		部门负责人	(签字)
应用联系人		联系电话	
平台、系统及移动应用程序信息（一个应用填一张表）			
应用名称			
开发/运营单位			
开发/运营联系人		联系电话	
等级保护备案号		ICP 备案号	
应用提供方式	□自主开发 □外购 □上级要求使用		
后台服务器部署方式	□校内部署 □云部署 □其他机房----------		
应用后台开发语言		使用数据库	
应用前端平台	□在线平台/系统 □PC 端程序 □APP □微信小程序		
应用功能类型	□教育学习类 □管理服务类 □社会服务类		
服务对象	□学生 □教师 □培训学员 □社会大众		
是否具有以下功能	□论坛 □收费 □直播 □其他，----------		
主要功能及服务内容			
收集了用户那些信息	□姓名 □学号 □手机号 □身份证 □照片 □住址 □----------		
用户登录认证措施	□实名 □绑定手机号码		

附件 3

西安开放大学
网络安全和信息化安全承诺书

本部门郑重承诺，遵守本责任书各项承诺，对所列事项负责，如有违反，由本部门承担由此带来的相应责任。

一、本部门承诺遵守《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》及其他国家信息技术安全的有关法律、法规和行政规章制度。

二、本部门已知悉并承诺执行《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》《西安开放大学网络安全和信息化工作管理办法》中的相关规定。

三、本部门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、本部门承诺完善部门内部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。

五、本部门承诺加强信息系统安全，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。

六、本部门承诺加强终端计算机安全，落实软件正版化，推

进具有自主知识产权的软硬件应用，规范工作人员的使用行为。

七、本部门承诺规范本单位数据采集和使用，不采集超越职能范围的数据，保障数据安全。

八、本部门承诺对负责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。

九、本部门承诺当信息系统或网站发生信息技术安全事件时，迅报告与处置，将损害和影响降到最小范围，并按照要求及时进行整改。

十、若违反国家相关法律法规和本承诺书有关条款的，本部门愿承担责任。

十一、本承诺书自签署之日起生效。

主要负责人（签字）:

盖　　章

年　月　日

附件 4

西安开放大学网络安全与信息安全应急预案

第一章　总则

第一条 为有效预防并科学应对网络安全与信息安全突发事件，确保校园网络与信息系统正常运行，根据《信息安全事件分类分级指南》《教育系统网络与信息安全类突发公共事件应急预案》《信息技术安全事件报告与处理流程》等国家和教育行业有关法律法规，结合学校实际，制定本预案。

第二条 网络安全与信息安全事件是指校园信息化基础设施、应用系统、网站、系统数据等因各种因素遭到破坏，对学校各项工作造成负面影响的事件。

第三条 本预案的适用范围：由西安开放大学负责建设与管理的网站、平台及网络安全事件的应急处理。

第二章　网络与信息安全事件等级

第四条 网络安全与信息安全事件依据发生过程、性质和特征不同，可分为以下四类：

（一）网络攻击事件：由于遭受有害程序感染、非法入侵或其他技术手段攻击，造成校园网络和信息系统运行异常或存在潜在危险，或造成信息被篡改、假冒、泄漏、窃取等而导致的信息安全事件。

（二）设备故障事件：由于信息系统或外围软硬件设施故障、人为误操作等，造成信息系统破坏、业务中断、系统宕机、网络瘫痪等导致的信息安全事件。

（三）灾害性事件：因洪水、火灾、雷击、地震、台风、非正常停电等外力因素造成网络与信息系统损毁，导致业务中断、系统宕机、网络瘫痪等安全事件。

（四）信息内容安全事件：利用校园网络在校内外传播法律法规禁止的信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

第五条 根据网络信息安全突发事件的可控性、严重程度和影响范围，将网络信息安全突发事件分为四级：

（一）I 级（特别重大）：造成学校网络与信息系统发生大规模瘫痪，事态的发展超出区一级相关主管部门的控制能力，对国家安全、社会秩序、公共利益或教育形象造成特别严重损害的突发事件。

（二）II 级（重大）：造成学校或其它上一级部门重要网络与信息系统瘫痪，对国家安全、社会秩序、公共利益或教育形象造成严重损害，需要上级政府或公安部门协助，乃至需跨地区协同处置的突发事件。

（三）III 级（较大）：造成学校网络与信息系统瘫痪，对国家安全、社会秩序、公共利益或教育形象造成一定损害，但只需在本区政府或区信息中心协同处置的突发事件。

（四）IV 级（一般）：造成学校校园网络重要网络与信息系统受到一定程度的损坏，对师生、家长或其他人员和单位的权益有一定影响，但不危害国家安全、社会秩序和公共利益，可由区教育主管部门或学校处置的突发事件。

第三章　组织机构及职责

第六条 学校网络安全与信息工作领导小组为网络安全与信息安全事件应急处理领导机构，学校网络安全与信息工作领导小组办公室负责具体处置工作。其职责包括：

（一）负责网络安全与信息安全工作的组织、协调和监督，制定相关制度和应急预案；

（二）根据网络安全与信息安全事件程度提出相应级别预案的启动，组织协调成员单位落实应急预案，共同做好处置工作；

（三）负责及时收集、通报和上报网络安全与信息安全事件处置的有关情况；

（四）对全校各单位贯彻执行预案以及在事件处置工作中履行职责情况进行检查督办。

第四章　工作原则

第七条 积极防御、综合防范。立足安全防护，加强预警，重点保护重要信息网络和关系社会稳定的重要信息系统；从预防、监控、应急处理、应急保障和打击不法行为等环节，在管理、技术、宣传等方面，采取多种措施，充分发挥各方面的作用，构筑学校网络与信息安全保障体系。

第八条 明确责任、分级负责。按照“谁主管、谁负责”的原则，加强网络安全管理，认真落实各项安全管理制度和措施。加强计算机信息网络安全的宣传和教育，进一步提高师生的信息安全意识。

第九条 落实措施、确保安全。对机房、网络设备、服务器等设施定期开展安全检查，对发现安全漏洞和隐患的进行及时整改；实行网站的巡检制度，密切关注互联网信息动态，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。

第五章　处置程序

第十条 启动预案：发生网络与信息安全事件后，现代教育技术处和涉事部门，应第一时间采取断网等有效措施，将损害和影响降低到最小范围，保留现场，并报告学校网信办主任和学校分管领导。

第十一条 事件定级：现代教育技术处组织有关单位，尽最大可能收集事件相关信息，鉴别事件性质，确定事件来源，弄清事件范围，评估事件带来的影响和损害，确认事件的类别和等级。

第十二条 应急响应：根据事件等级采取相应的响应方式

（一）IV 级：现代教育技术处组织相关单位及时、自主进行应急处置，做好处置记录。

（二）III 至 II 级：现代教育技术处应立即上报学校网信领导小组组长，由领导小组指挥、协调成员单位进行应急处置。

涉及人为主观破坏事件时由学校后勤保卫处报告当地公安部门。

（三）I 级：现代教育技术处立即上报学校网信领导小组组长，由学校报告教育部和当地公安部门，公安部门指挥协调有关单位和学校协同进行应急处置。

第十三条 应急处理方式：根据网络与信息安全事件分类采取不同应急处置方式。

（一）网络攻击事件：判断攻击的来源与性质，关闭影响安全的网络设备和服务器设备，断开信息系统与攻击来源的网络物理连接，跟踪并锁定攻击来源的 IP 地址或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照事件发生的性质采取以下方案：

病毒传播：及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围；为避免产生更大的损失，保护健康的计算机，必要时可关闭相应的端口，甚至相应楼层的网络，及时请有关技术人员协助进行杀毒处理。

外部入侵：判断入侵的来源，区分外网与内网，评价入侵可能或已经造成的危害。对入侵未遂、未造成损害的，且评价威胁很小的外网入侵，定位入侵的 IP 地址，及时关闭入侵的端口，限制入侵的 IP 地址的访问。对于已经造成危害的，应立即采用断开网络连接的方法，避免造成更大损失和影响。

内部入侵：查清入侵来源，如 IP 地址、所在办公室等信息，同时断开对应的交换机端口，针对入侵方法调整或更新入侵检测

设备。对于无法制止的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

（二）设备故障事件：判断故障发生点和故障原因，迅速联系设备厂家或 IT 运维公司尽快抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。

（三）灾害性事件：根据实际情况，在保障人身安全的前提下，保障数据安全和设备安全。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。

（四）信息内容安全事件：接到校内网站出现不良信息的报案后，应迅速屏蔽该网站的网络端口或拔掉网络连接线，阻止有害信息传播，查找信息发布人并做好善后处理。对公安机关要求学校协查的外网不良信息事件，根据校园网上网相关记录查找信息发布人。

（五）其它不确定安全事件：可根据总的安全原则，结合具体情况，做出相应处理，不能处理的及时咨询国家信息安全机构。

第十四条 事后处理

（一）安全事件最初应急处置后，应及时采取措施，抑制其影响进一步扩大，限制潜在的损失与破坏，同时要确保应急处置措施对涉及的相关业务影响最小。

（二）安全事件被抑制后，通过对有关事件或行为的分析结果，找出问题根源，明确相应补救措施并彻底清除。

（三）安全事件解决后，要及时清理系统，恢复数据、程序、

服务，恢复工作应避免出现误操作导致的数据丢失。

第十五条 总结上报

（一）系统恢复运行后，现代教育技术处对事件造成的损失、事件处理流程等进行分析评估，总结经验教训，撰写事件处理报告，报学校网信领导小组。

（二）发生III至Ⅰ级事件，在报告学校的同时，应按照教育部办公厅《信息技术安全事件报告与处置流程（试行）》报告上级主管部门，属于重大事件或存在非法犯罪行为的，还须第一时间向公安机关报案。

第六章 附 则

第十六条 本办法由现代教育技术处负责解释，自发布之日起施行。

西安开放大学办公室 2024年12月12日印发