西安邮电大学网络与信息安全管理办法

（试行）

第一章 总则

第一条 为提高网络与信息安全防护能力和水平，保证学校网络与信息安全工作顺利进行，保障学校各项事业健康有序发展，结合我校实际，制定本办法。

第二条 学校网络与信息安全，包括校园计算机网络（以下简称校园网络）与信息系统（含网站，下同）的运行安全和信息内容的安全。

第三条 学校按照国家有关网络安全和信息化建设的法律、法规、规章，制定网络与信息安全总体规划，加强安全管理与技术研究，建立健全相关规章制度，并在实际工作中予以落实。

第二章 管理体制和职责

第四条 学校网络安全和信息化工作领导小组负责协调全校网络与信息安全保障体系建设。各部门、各单位（以下统称各单位）应在本单位内部相应成立网络与信息安全工作小组，其主要负责人为第一责任人，并指定专人担任信息安全管理员，负责本单位及下属单位的网络与信息安全工作。

第五条 学校网络安全和信息化工作领导小组办公室负责对网络

和信息系统进行调查、取证、处理，根据相关证据及事态影响或破坏程度，对违规者按照有关规定进行处理。

第六条 信息中心负责学校基础网络的日常管理和维护，保障网络与信息系统的正常运行；保存网络运行日志，配合调查取证；负责入网单位和个人办理入网登记手续，签署相应的安全责任书。

第七条 学校涉稳网络舆情的日常监测、分析研判、信息报送和应急处置工作按照《西安邮电大学涉稳网络舆情管理与处置实施办法》（西邮党发〔2018〕9 号）执行。

第八条 坚持“谁主管谁负责，谁主办谁负责，谁使用谁负责”原则。网络与信息系统的主办单位承担安全监管责任，包括内容安全监管、技术安全保障和监督检查等职责；网络与信息系统的使用单位和个人对系统操作与信息内容的安全监管承担直接责任。网络与信息系统通过外包服务方式进行维护的，主办单位负责督促外包服务单位做好安全运维工作，网络与信息系统的安全监管责任主体仍为主办单位。

第三章 安全秩序

第九条 校园网络和信息系统接入互联网必须采取防火墙、身份认证、MAC 地址绑定、安全审计、病毒防护及入侵检测等安全技术手段。校内互联网接入由信息中心统一管理，包括 IP 地址、域名及网络帐号等。

第十条 学校域名为 xupt.edu.cn、xiyou.edu.cn，各主办单位按

信息系统名称的拼音或英文缩写简写设置域名并提出申请，经信息中心批准后使用。任何单位和个人均须落实实名登记网络帐号信息，并对网络帐号安全使用负责。

第十一条 任何单位和个人不得私自与校外单位联网，不得私自发展校外用户。

第十二条 校园网络实行信息系统报批备案制。需要在校园网上开办信息系统的单位，应到信息中心办理登记注册手续，其中 BBS、论坛、聊天室、博客、微博等公众信息服务系统，以及在微信、QQ 等互联网社交平台上开办公众服务号，应到党委宣传部报备批准。未经许可，任何入网单位或个人不得以冠有“西安邮电大学”或“西邮”中外文字样的任何名义开通信息发布、BBS、论坛、聊天室、博客、微博、微信等公众信息服务系统。

第十三条 各单位原则上应依托校园网开展信息系统建设。涉及学校基础数据、师生员工个人信息或敏感信息的信息系统，不得部署在校外。需要在校外开办信息系统的单位，应到信息中心办理备案手续。部署在校外的网络和信息系统，安全监管责任主体仍为主办单位。

第十四条 经批准建立的公众信息服务系统应明确专门的管理员和制订相应管理制度，包括安全保护技术措施、信息发布审核登记制度、信息监视保存清除备份制度、不良信息报告和协助查处制度、管理人员岗位责任制。

第十五条 各单位应建立健全信息发布、信息审查、应急处置机制，指定人员负责审查上网信息和信息系统保密管理，负责涉及学校

或本单位舆情的处置引导，以及监管本单位师生开设的博客、微博、微信等自媒体平台。

第十六条 在校园网络上严禁制作、查阅、复制或传播下列信息：

（一） 煽动抗拒、破坏宪法和国家法律、行政法规实施；

（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；

（三） 损害国家荣誉和利益；

（四） 煽动民族仇恨、民族歧视，破坏民族团结，或者侵害民族风俗习惯；

（五） 宣扬恐怖主义、邪教、封建迷信，违反国家宗教政策；

（六） 捏造或者歪曲事实，散布谣言，扰乱社会秩序，破坏社会稳定；

（七） 侮辱他人或者捏造事实诽谤他人；

（八） 含有淫秽、色情、赌博、暴力、欺诈等内容；

（九） 含有法律、法规禁止的其他内容。

第十七条 在校园网络上严禁下列行为：

（一） 破坏、盗用、篡改计算机网络中的信息资源；

（二） 故意泄露、窃取、篡改个人电子信息，擅自利用网络收集、使用个人电子信息，出售或者非法向他人提供个人电子信息；

（三） 违背他人意愿、冒用他人名义发布信息；

（四） 攻击、入侵、破坏计算机网络、信息系统及设备设施；

（五） 故意阻塞、中断校园网络，恶意占用网络资源；

（六） 故意制作、传播、使用计算机病毒、木马、恶意软件等破坏性程序；

（七） 故意大量发送垃圾电子邮件、垃圾短信等，干扰正常网络秩序；

（八） 盗用他人帐号、盗用他人 IP 地址；

（九） 私自转借、转让用户帐号造成危害；

（十） 私自开设二级代理和路由接纳网络用户；

（十一） 上网信息审查不严，造成严重后果；

（十二） 以端口扫描和私搭 DHCP 服务器等方式，破坏网络正常运行；

（十三） 私自将外网串接到校园网络。

（十四） 其它违反法律法规或危害网络与信息安全的行为。

第四章 安全防护

第十八条 各单位作为安全等级保护的责任主体，应当按照国家信息安全等级保护的管理规范、技术标准确定信息系统的安全保护等级，并报学校有关部门审核。学校按相关规定选择具有相关技术资质和安全资质的测评单位，对二级及以上的信息系统进行等级测评。经测评，信息安全状况未达到安全保护等级要求的，信息系统的主办单位应制定整改方案并落实到位。

第十九条 各单位对于新建、改建、扩建的信息系统，应当在规划、设计阶段同步建设网络信息安全保障措施。新开发的信息系统必

须经过第三方安全检测机构出具检测报告、签订《西安邮电大学网络与信息安全责任书》后方可上线运行。

第二十条 各单位对于主办的信息系统，应当采取必要的安全措施，严防入侵、篡改、泄露等事件发生。信息系统的主办方和运维方要各司其职，各负其责。

第二十一条 各单位应建立检查巡查机制，定期或不定期组织开展信息系统安全演练，查找安全漏洞和隐患；对机房、网络设备、服务器等设施定期开展安全检查；更新和升级必要的服务器软件，及时安装补丁，包括操作系统、web 服务器、应用中间件、数据库等，加强服务器应用的安全性。对上述检查中发现安全漏洞和隐患的，检查单位应及时填发《隐患告知书》，逾期未采取措施和提交处理报告的，检查单位应及时填发《隐患整改通知书》。对于一时难以修复或整改落实的，应当立即采取措施进行隔离，直至修复完成。

第二十二条 各单位应建立本单位信息安全值守制度， 做到安全事件早发现、早报告、早控制、早解决。

第二十三条 各单位对于主办的信息系统，每季度至少进行 1 次安全检查。检查内容包括：

（一） 查杀病毒，清除木马、后门等恶意程序，升级系统补丁；

（二） 检查网页和重要数据的备份情况；

（三） 检查网页内容，及时清除无关网页和暗链；

（四） 定期更改口令，清理不必要的管理帐号；杜绝空口令、

弱口令和默认口令；

（五） 检查 SQL 注入和跨站脚本等安全漏洞；

（六） 检查服务器安全策略，关闭不必要的端口和服务；

（七） 检查系统日志留存情况，留存相关日志不少于六个月。

第二十四条 各单位对于主办的重点信息系统， 应当采取措施重点防护，保障系统和重要数据的安全。每月至少进行 1 次安全检查。重点信息系统包括：

（一） 学校 WWW 门户网站；

（二） 学校重要办公网站和办公信息系统；

（三） 统一身份认证、校园卡等校级重要公共服务平台；

（四） 教学、科研、人事、财务、设备、房产等学校重要业务信息系统及相关重要数据库。

第二十五条 建立网络安全监测预警和信息通报制度。信息中心负责信息收集、分析和通报工作，按照规定向全校统一发布网络安全监测预警信息。各单位应做好网络与信息安全事件的风险评估和隐患排查工作，制订完善相关应急预案，及时采取有效措施，避免和减少网络与信息安全事件的发生及其危害。

第二十六条 建立健全学校网络与信息安全类突发公共事件应急工作机制，提高应对网络与信息安全类突发公共事件的能力，预防和减少由此造成的损失和危害，维护学校的安全和稳定。

第五章 责任追究

第二十七条 对存在网络安全隐患和安全漏洞的网络信息系统，由网络安全和信息化工作领导小组办公室核定，信息中心执行对其进行关停，并责令其限期整改。

第二十八条 对于违反本管理办法的单位和个人，网络安全和信息化工作领导小组办公室将协同学校有关部门共同查处，并由相关部门根据国家和学校相关规定做出处罚决定。

第六章 附则

第二十九条 本办法由网络安全和信息化工作领导小组办公室负责解释。

第三十条 本办法自发布之日起施行。