山东科技大学文件

山科大发〔2020〕44号

关于印发《山东科技大学网站管理办法》《山东科技大学网络安全等级保护管理规定》的通知

各校区管委，各部门、各单位:

《山东科技大学网站管理办法》《山东科技大学网络安全等级保护管理规定》已经校长办公会研究通过，现予印发，请遵照执行。

山东科技大学

2020 年 6 月 18 日

山东科技大学网站管理办法

第一章　总　则

第一条　为规范学校网站管理，推进学校信息化建设，根据《互联网信息服务管理办法》等政策法规和学校相关管理制度，结合工作实际，特制定本办法。

第二条　本办法适用于各部门、各单位（以下简称“各单位”）利用学校互联网络域名或互联网 IP 地址设置互联网站的备案和运营管理。

第三条　学校的一级网站域名为：sdust.edu.cn，校内二级网站，原则上使用学校统一的域名机制，二级网站格式为：*.sdust.edu.cn，其中“*”为二级单位汉语拼音首字母组合。

第二章　管理部门与职责

第四条　网络安全与信息化办公室（以下简称“网信办”）的管理职责：

（一）为各单位网站的建设与管理提供技术支持。

（二）对各单位网站进行备案。

（三）提供网站发布和域名服务。

（四）为管理范围内的网站提供物理安全、操作系统安全、防火墙建设和数据备份。

第五条 网站主办单位的管理职责:

（一）负责本单位网站的建设与管理。

（二）明确网站负责人和信息化联络员。

（三）负责本单位网站的安全和管理，网站运行过程中，一旦发生异常，应及时保存异常内容，并迅速向网信办和宣传部报告。

（四）负责联系网站服务厂商提供相应的技术支持、建设与运行维护、数据安全、运维队伍培训等工作。

（五）保证备案信息内容的真实准确，保证网站的互联网络域名或 IP 资质所包括的所有信息内容合法。

（六）配合有关部门的信息安全检查、网站信息内容检查、保密审查工作。

第六条 信息化联络员的职责:

（一）负责本单位信息化建设工作与网信办的联系与沟通。

（二）负责本单位信息系统的运维和信息安全管理。

（三）负责本单位信息系统安全隐患、事件的整改与报告。

第七条 各单位设立网站需经宣传部审查，网站信息内容受宣传部监管。

第三章 网站设立与备案

第八条 各单位网站的建设实行准入制，所有接入校园网的网站，由各单位提出申请，提交宣传部审核、网信办备案后方可

建立。未履行备案手续的，不得设立互联网站。

第九条 各单位党政“一把手”作为本单位网站的第一责任人，负责网站建设和管理工作，并指定至少一名信息化联络员承担具体工作。

第十条 不允许任何单位或个人利用学校互联网络域名或互联网 IP 地址等设立个人网站，任何单位或个人不得利用学校互联网络域名或互联网 IP 地址从事有偿互联网信息服务。

第十一条 学校网站涉及以下服务项目的，须依照法律、行政法规以及国家有关规定，获得国家有关主管部门许可之后，再向学校提交审核备案手续:

（一）从事互联网新闻信息服务。

（二）提供由互联网用户向公众发布信息的服务。

（三）提供互联网信息搜索服务。

（四）从事文化、出版、视听节目、教育等互联网信息服务。

第十二条 在履行备案手续时，应当向网信办提供以下材料:

（一）设立互联网站的目的，信息服务功能说明，服务项目简介。

（二）网站管理人员基本情况，其中网站责任人应为网站主管部门的在编在职教职工。

（三）网站主管部门主要负责人签署的审核意见。

（四）从事本办法第十一条所列举的互联网信息服务项目的，

提供国家有关主管部门的许可文件。

第十三条 网站主办单位在备案有效期内需要变更其备案信息的，应当在相关变更发生之日起 30 日内向网信办履行备案变更手续。

第十四条 网站主办单位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 30 日内向网信办履行备案注销手续。

第十五条 网信办对互联网站备案实行年度审核。网站主办单位应当在每年规定时间向网信办履行年度审核手续。

第十六条 在年度审核时，网站主办单位未在规定时间提交年度审核信息的，网信办有权责令其限期改正；拒不改正的，关闭该网站并注销备案。

第十七条 网站主办单位或个人违反国家有关法律法规或学校有关规章制度，应暂停或终止服务的，网信办应暂时关闭网站，或关闭网站并注销备案。

第四章 网站运营与维护

第十八条 网站管理人员的密码应符合复杂度要求，密码 8 位以上，包含大小写字母、数字及特殊符号，密码至少每三个月更换一次。

第十九条 网站管理人员要妥善保管账号和密码，严禁转借他人使用。如出现账号丢失或密码遗忘等问题，需持相关证件到

网信办更改。

第二十条 在学校网站及各单位网站上设置的其他网站或网页链接，须经网站建设第一责任人审核批准，同时确保链接的有效性和合法性。

第二十一条 校内各网站未经合法授权，不得提供不符合著作权法的在线播放或者下载服务。

第二十二条 各单位应加强对网站系统的配置安全管理，定期检查和补丁升级，确认当前网站访问权限设置符合业务和管理上的要求。

第二十三条 严禁任何未经授权的网站系统维护操作。服务厂商在现场提供技术支持时，须由网站管理人员全程陪同。

第五章 附 则

第二十四条 本办法实施前利用学校互联网络域名或互联网 IP 地址设立互联网站的，应当自本办法施行之日起 60 天内依照本办法的有关规定补办备案手续。

第二十五条 本办法由网络安全与信息化办公室负责解释。

第二十六条 本办法自发布之日起施行。

山东科技大学网络安全等级保护管理规定

第一章　总　则

第一条　为加强学校网络安全管理，确保学校网络信息系统（以下简称“信息系统”）安全，依据《中华人民共和国网络安全法》和《信息安全技术 网络安全等级保护基本要求》（GB/T22239-2019）的相关要求，结合工作实际，制定本规定。

第二条　网络安全管理遵循“确保安全、注重防范、分工负责、规范管理”的原则，以确保网络运行安全和网络信息安全为核心，以抓好安全防范为重点，各部门分工负责、协同配合、责任到人，认真遵守有关网络安全的法律法规和制度规定，共同做好网络安全管理工作。

第三条　按照国家有关网络安全的政策要求，结合实际，制定并完善安全策略、安全管理制度、日常操作规程和记录表单，构建学校网络安全管理制度体系。

第四条　本规定适用于信息系统的安全管理。

第五条　本规定所指信息系统是山东科技大学规划和建设范围内的计算机信息系统，包括所有非涉密信息系统。

第二章　组织机构和职责

第六条　在山东科技大学网络安全和信息化领导小组（以下

简称“领导小组”）领导下，山东科技大学网络安全和信息化领导小组办公室（以下简称“领导小组办公室”）负责信息系统的统一规划、责任分工和资源分配，按照“谁主管谁负责、谁使用谁负责”的原则，由山东科技大学网络安全与信息化办公室（以下简称“网信办”）负责信息系统的建设管理和运行维护。

第七条 网信办是学校信息化工作安全管理和运行维护的部门，负责指定信息系统的系统管理员、安全管理员和安全审计员。系统管理员主要负责系统的日常运行维护，安全管理员主要负责系统的日常安全管理工作，安全审计员主要负责对系统管理员和安全管理员的操作进行审计和评估。安全管理员和安全审计员不得为同一人。

第八条 各部门、各单位负责所属信息系统的建设管理和运行维护工作，负责指定本单位信息化联络员。信息化联络员负责协调本单位在信息系统运维、网络信息安全、信息化建设等方面与网信办的沟通与配合工作。

第九条 各部门、各单位应结合具体情况，制定信息系统安全管理的相关制度，建立健全保障信息安全的工作机制，采取措施落实有关安全要求，确保信息系统与信息的安全。

第三章 规划建设和测评审批

第十条 信息系统按照国家网络安全等级保护要求确定保护等级，进行规划、设计、建设和运行维护管理，并采取相应安

全保护措施。

第十一条 网信办统一负责信息系统的定级工作，并报青岛市公安局备案。

第十二条 信息系统应根据其等保定级、行政级别、地域分布、连接范围等合理划分安全域，安全域之间应采取必要的隔离措施。

第十三条 信息系统安全体系的规划、建设由网信办负责，统一采用防火墙、防病毒系统、入侵防御系统等安全措施。信息安全体系应与信息系统同步规划、同步建设、同步使用。

第十四条 信息系统的设计、建设须选择具有相应信息系统集成资质的单位承担设计、开发、建设和运行维护任务。信息系统建设工程的监理、检测工作应选择具有相应信息系统工程监理、检测资质的单位承担。

第十五条 重要信息系统投入使用前，有关风险评估、安全方案设计、论证、等级保护测评和密码评估等所需经费，应由系统建设使用单位在系统规划时，按照一定比例统一纳入系统建设经费预算。

第十六条 信息系统中使用的安全设备、系统软件、应用软件须采用国家主管部门认定或认可的产品和设备，优先选用国产设备和系统。

第十七条 信息系统设计方案必须通过论证以后方可实施。网信办参与设计方案的论证、审查。设计方案中涉及密码技术产

品的，须报青岛市密码管理局审批。

第十八条 信息系统应要求有完善的鉴别和认证、访问控制、日志审计功能和数据验证功能，杜绝木马和后门，建立源代码控制和软件版本控制机制。

第十九条 重要信息系统建成后，选择网络安全等级保护测评机构开展测评。网络安全等级保护测评机构应根据“中国信息安全等级保护网”提供的《全国等级保护测评机构推荐目录》进行选择。测评前应与测评机构签订工作协议和保密协议，对测评机构和测评人员的测评活动进行严格的监督与管理。信息系统通过测评后方可投入使用。

第二十条 信息系统不再使用时，网信办负责废止管理工作。密码设备退装、销毁等必须符合密码设备管理的有关规定。

第二十一条 网信办负责规范对服务提供商的安全管理工作，代表学校与服务提供商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务，定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。

第四章 使用管理与运行维护

第二十二条 做好统筹联动，加强各类管理人员、各部门、院系之间在网络安全工作方面的合作与沟通，定期召开协调会议，共同协作处理网络安全问题。

第二十三条 建立对外联系机制，拓展与外联单位的沟通与

合作渠道。外联单位包括供应商、业界专家、专业的安全公司、安全组织、上级主管部门、兄弟单位、安全服务机构、电信运营部门、执法机关等。

第二十四条 信息系统应具备文档化的系统安全管理策略，每 6 个月对系统安全管理策略进行审核，如果系统、环境等发生较大变化时，应及时更新安全管理策略。

第二十五条 信息系统应当处于安全可控环境中，其机房建设应符合与网络安全等级相对应的标准要求，具有防火、防水、防雷、防静电、防盗监控和供电、温控保障设施。服务器和交换设备应放置在安全可控的区域，建立相关制度进行环境和设备的运维管理。

第二十六条 信息系统所有计算机应及时升级病毒库，进行病毒查杀；及时安装操作系统、数据库和应用系统补丁程序。

第二十七条 信息系统应当采取身份鉴别、访问控制、安全审计、违规外联监控等技术保护措施。审计日志记录至少保存 1 年。

第二十八条 建立系统备份与恢复策略，对关键系统、关键设备和关键数据至少每 3 个月进行一次全量备份。

第二十九条 基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录。

第三十条 通过信息系统发布信息，按照“谁发布、谁负责”

的原则进行严格审批，建立审批程序，明确责任单位和责任人，做好发布信息的记录工作。

第三十一条 严格限制通过互联网直接向重要信息系统复制信息，确需复制的应采取严格的技术防护措施，防止病毒、木马等的导入传播。

第三十二条 在信息系统中，对用户的授权应按照最小授权原则，只授予其满足开展工作所需的最小访问权限，不得随意扩大用户的访问范围或提高权限等级。安全审计员应做好对授权管理和访问控制策略的监督、审核工作。

第三十三条 提升数据安全防护能力，确保数据完整性、保密性和可用性，加强个人信息保护和剩余信息保护。

第五章 监测预警与应急处置

第三十四条 建立山东科技大学网络安全监测预警和信息通报制度，通报内容包括网络安全态势与风险预警情况、重要漏洞告警及处置措施建议、重大网络安全事件、信息系统高危安全隐患等，按照国家相关规定及省、市有关主管部门的要求，报送网络安全监测预警信息，并及时发现和处理网络攻击和异常行为等。

第三十五条 信息系统安全监测是网络安全检查的重要内容。领导小组办公室结合不同时期的工作需要，组织开展信息系统安全监测预警。对存在安全漏洞隐患的信息系统责任单位通报

监测预警信息，限期整改。

第三十六条 领导小组办公室协调有关部门建立健全网络安全风险评估和应急工作机制。制定网络安全事件应急预案，并定期组织演练。网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第三十七条 网络安全事件发生的风险增大时，领导小组应当按照规定的权限和程序，根据网络安全风险的特点和可能造成的危害，采取下列措施:

（一）要求有关部门和人员及时收集、报告有关信息，加强对网络安全风险的监测。

（二）组织有关部门和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度。

（三）在全校范围发布网络安全风险预警，发布避免、减轻危害的措施。

第三十八条 发生网络安全事件，应当立即启动网络安全事件应急预案。领导小组办公室对网络安全事件进行调查和评估，要求相关部门采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时发布有关的警示信息。

第六章 安全教育与培训

第三十九条 网信办通过多种形式在全校范围内开展网络

安全知识培训和网络安全形势教育，不断增强广大师生网络安全防护意识。网络安全教育注重发挥校园网络的传播媒介作用，充分利用校园网传播网络安全知识和相关法律法规等。

第四十条 各部门、各单位要加强人员在录用、调岗和离岗环节的网络安全教育和管理。

第四十一条 信息系统安全管理人员包括系统管理员、安全管理员及安全审计员，须进行安全培训，经考核合格后方可上岗。

第四十二条 信息系统安全管理人员应定期参加网信办组织的专业培训，了解网络安全形势，学习最新网络安全知识，不断提高安全防护意识，增强做好网络安全工作的能力。

第七章 评价与惩戒

第四十三条 领导小组办公室负责对学校信息系统的等级保护工作进行监督，每年组织一次考核评价，将结果纳入单位的年度绩效考核。

第四十四条 对违反有关规定，造成信息安全隐患的部门，应责令其限期整改；情节严重的，按照有关规定处理。

第八章 附 则

第四十五条 本规定由网络安全和信息化领导小组办公室负责解释。

第四十六条 本规定自发布之日起施行。

山东科技大学办公室 2020年7月20日印发