

对外经济贸易大学文件

贸大网信发〔2024〕5号

对外经济贸易大学关于印发 《对外经济贸易大学网络安全管理办法(试行)》 的通知

各学院、处（部）级单位：

《对外经济贸易大学网络安全管理办法（试行）》已经2024年3月19日第5次校长办公会审议通过，现印发给你们，请遵照执行。



对外经济贸易大学网络安全管理办法（试行）

第一章 总则

第一条 为规范学校网络安全管理，保障学校网络安全与信息化建设工作顺利开展，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国计算机信息系统安全保护条例》等相关法律法规和上级有关文件精神，结合学校实际制定本办法。

第二条 本办法所称的网络安全管理是指为保障网络与信息化建设基础设施、信息系统（网站）、数据等信息资产的机密性、完整性、可用性而开展的相关管理和技术工作，全校各单位和全体校园网用户须按照本办法认真落实。

第三条 对外经济贸易大学网络安全管理按照“谁主管谁负责、谁建设谁负责、谁使用谁负责、谁运维谁负责”的基本原则，实行统一领导、分级治理、定责到人，强化安全意识，规范处置流程。

第二章 组织机构与职责

第四条 学校网络安全和信息化领导小组是学校网络安全工作的最高领导机构。

第五条 网络安全和信息化领导小组办公室（以下简称“网信办”）设在网络安全和信息化处，是学校网络安全日常管理和

技术支撑部门，负责学校网络安全总体规划、统筹推进及检查考核、协调网络安全事件的处理、对学校信息化基础设施和公共服务平台进行整体防护，组织开展学校网络安全宣传和培训工作。

第六条 学校各二级单位（以下简称“单位”）是本单位网络安全工作的责任主体，负责本单位主机、信息系统（网站）及数据的安全管理工作。

第七条 学校各单位主要负责人是网络安全工作第一责任人，负责领导、落实、监督网络安全工作，与学校网络安全和信息化领导小组签订《对外经济贸易大学网络安全工作责任书》，执行学校的管理规范和技术标准。

第八条 学校各单位应至少选派一人担任网信管理员，负责本单位网络安全和信息化相关工作，包括但不限于维护并更新信息系统（网站）备案信息、定期排查并消除网络安全隐患、参加网络安全培训、按照《对外经济贸易大学网络安全事件应急预案》处置网络安全事件等。离岗、离职前应及时做好工作交接并报网络安全和信息化处收回其管理权限。

第九条 全校教职工和学生均有遵守学校网络安全相关规定的责任和义务。主动学习网络安全相关知识，培养科学健康上网习惯，不得从事危害国家安全、泄露国家秘密、侵犯知识产权、传播不良信息等违法犯罪活动。

第三章 校园网安全

第十条 网络安全和信息化处负责校园网络的安全管理。

第十一条 校园网与互联网实行逻辑隔离，由网络安全和信息化处统一出口、统一管理、统一防护。学校各单位及个人不得擅自建设、拆卸、更改、损毁、挪用校园网设施，不得改变网络结构，不得私自接入其他网络出口。

第十二条 校内师生员工接入校园网，必须进行“实名注册、认证上网”，不得以任何方式私接校园网，不得私自将校园网账号、校园网资源提供给校外人员使用，严禁盗用其他用户账户使用校园网。

第十三条 校园网主要服务于学校教学、科研、管理和服务等各项业务，用户不得将校园网用于其他用途，严禁任何单位和个人利用校园网络及相关基础设施开展未经许可的其他活动。

第十四条 网络安全和信息化处对校园网地址和域名的使用进行统一规划、分配和管理，并定期审查其使用情况，有权禁用涉嫌违法违规的地址和域名。

第十五条 校园网地址未经许可不得对校园网以外提供互联网服务，如教学、科研上确有特殊需求，需要地址对外开放服务，经网络安全和信息化处审批后方可开放，申请单位按照学校规定承担对应的网络安全责任。

第十六条 网络安全和信息化处以保障学校教学、科研的稳定顺畅为首要目标，有权根据运行情况对校园网进行适时调整与优化，对流量过高、挤占带宽资源严重的流量及应用进行限时、限速或封停操作。

第十七条 网络安全和信息化处负责对校园网的安全进行监测管理，对散布病毒、木马等危害校园网安全的情况，有权对相关账号、设备和地址进行封停。

第十八条 校园各类业务专网中的任何设备不得私自接入校园网、互联网，校园网的任何设备也不得私自接入业务专网。

第十九条 学校各单位服务器、自助服务终端、电子显示屏等终端接入校园网，必须进行接入审批和备案。

第四章 信息系统（网站）安全

第二十条 信息系统（网站）包括校内各单位建设的业务系统及网站，网络安全和信息化处负责统筹学校信息系统（网站）安全管理工作，校内各单位承担所建设信息系统（网站）的安全管理责任。

第二十一条 学校信息系统（网站）的建设与运行维护应遵循《对外经济贸易大学信息系统建设与运行维护管理办法》。各信息系统(网站)上线前必须通过网络安全和信息化处安全检测，确保安全隐患清零后方可上线。

第二十二条 各单位定期对本单位信息系统（网站）的系统安全、内容安全、数据安全等进行自查，配合进行网络安全专项检查，并在重大活动、寒暑假、网络安全重要保障期前全面排查网络安全薄弱环节。

第二十三条 各单位应落实信息系统（网站）安全等级保护制度。信息系统（网站）建设单位是信息系统（网站）网络安全

等级保护的责任主体，应全力配合等保定级、备案和测评工作，并按照规定要求进行整改加固。网络安全和信息化处负责统筹学校信息系统（网站）网络安全等级保护工作，组织学校各单位开展信息系统（网站）等保定级、备案和测评。

第二十四条 各单位应落实信息系统（网站）校内备案制度，按照《对外经济贸易大学网站及信息系统校园网备案管理办法》进行备案。

第二十五条 涉密信息系统（网站）、设备按照相关涉密规范进行管理。

第二十六条 各单位应做好供应链安全管理工作，梳理所属信息系统（网站）的供应链清单，与供应商签订安全保密协议，明确保密责任，要求供应商及时提供系统、软件的升级维护等服务，对接触核心系统、数据或拥有管理权限的校外人员进行背景审查和保密审查，从严管理校外运维人员的远程和现场操作。

第二十七条 各单位建设网站应优先选择学校网站群平台，建设及管理按照网站群系统管理规范执行。

第二十八条 网络安全和信息化处为学校各单位和师生员工提供电子邮箱服务，并负责学校电子邮件系统的安全管理。学校各单位和师生员工使用学校电子邮箱应遵守电子邮件管理规范。

第五章 主机安全

第二十九条 主机安全包括服务器、存储及终端设备的安全。

第三十条 网络安全和信息化处负责学校数据中心机房内主

机的物理安全 and 环境安全，对其进行必要的监控，若发现托管单位违反校内网络安全相关制度，或托管服务器出现中毒、被黑客侵入等异常情况，有权终止服务器运行或网络接入。各单位负责自管机房内主机的安全管理。

第三十一条 各单位应指派专人负责本单位托管实体机和虚拟机的安全维护和管理，定期对各类主机进行安全检查、病毒扫描和漏洞修复，及时发现、解决软硬件系统故障。

第三十二条 各单位应落实主机校内备案工作，对于接入校园网的主机，及时向网络安全和信息化处备案。

第三十三条 学校师生员工使用的各类计算机及附属设备，包括且不限于台式电脑、笔记本电脑及其他移动终端，按照“谁使用谁负责”的原则，由使用人负责终端设备的安全管理。

第三十四条 各单位负责本单位的网络打印机、电子显示屏等物联终端及其控制系统的安全防护，落实防范措施，加强安全监管，确保运行安全。

第六章 数据安全

第三十五条 网络安全和信息化处对全校数据安全统筹管理与监督，建立数据资源目录，制定数据分类分级标准，负责学校数据中心平台的安全防护与数据备份恢复管理。学校各单位遵循《对外经济贸易大学数据管理办法》，负责本单位的数据安全管理，应结合实际建立包含收集、存储、使用、加工、传输、公开、销毁等在内的数据全生命周期安全管理机制。

第三十六条 各单位要严格按照“最小够用”原则确定数据收集使用范围，数据原则上应存储于校内，涉及学校基础数据、师生个人信息或敏感信息的信息系统（网站），不得部署在校外。各单位不得在未经许可情况下对外提供学校数据。

第三十七条 各单位要严控所管信息系统（网站）的数据录入、查看、修改和删除等操作权限，实现数据管理、使用和安全审计的权限分离，应详细记录所有数据操作，相关日志保留时间不少于六个月。涉及到由供应商提供外包服务的，要签署保密协议。

第三十八条 各单位要加强本单位数据的安全防护，做好操作系统、数据库、中间件等基础软件的版本迭代和安全配置。数据库服务器要配置内网 IP 地址，并启用防火墙，关闭多余端口和服务。

第三十九条 各单位要建立数据安全响应机制，妥善应对处理数据泄露、篡改、丢失等数据安全事件，并定期开展应急演练。

第七章 个人信息保护

第四十条 学校各单位应注意保护师生个人信息，规范信息发布，发布前进行去标识化处理。各单位每学期对所属信息系统和网站已有公开信息进行清查，如有涉及师生敏感个人信息的内容应及时撤销、删除或去标识化处理。

第四十一条 各单位依法依规收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。处理个人信息应

当注重师生隐私性、敏感性信息的保护，按照“告知-同意”原则，保障其信息处理的知情权和决定权，不得违背收集目的，公开化、商业化开发。

第四十二条 各单位应做好废旧信息处置，对于含有师生个人信息的纸质或电子文件资料，应严格管理、防止泄露。

第四十三条 一旦发现个人信息泄露事件，网络安全和信息化处通知相关责任单位，相关责任单位应及时进行删除或去标识化处理。

第八章 监测预警与应急处置

第四十四条 网络安全和信息化处负责校内网络安全监测工作，定期监测网络设备、主机及网络安全设备的运行状态。在特殊时期，网络安全和信息化处有权关闭信息系统（网站）的外网访问权限。

第四十五条 网络安全和信息化处定期对校内信息系统（网站）进行安全检查，对出现中危及以上安全风险和上级部门通知整改的信息系统（网站），发布校内网络安全整改通知，相关单位及人员应及时自查整改，风险隐患清零后方可上线。对存在中危及以上安全风险不修复、长期无人管理和无固定管理维护人员的信息系统（网站），有权予以清理和关闭。详细规范见附件1《信息系统（网站）漏洞整改管理规范》。

第四十六条 学校各单位需建立信息系统（网站）值守机制，安排专人对所属信息系统（网站）进行巡检，发现网站运行异常

及时处置。定期备份数据，留存日志六个月以上，并采取必要的安全措施，严防黑客入侵、信息泄露、数据篡改等事件发生。

第四十七条 网络安全和信息化处负责学校网络安全应急工作的统筹管理。学校各单位应按照学校网络安全事件报告与处置流程，参照《对外经济贸易大学网络安全事件应急预案》规范，做好各类报告与处置工作。

第四十八条 网络安全和信息化处负责组织校内网络安全事件应急演练，相关部门应全力配合，通过演练提高校内网络安全事件处置能力。

第四十九条 学校各单位和所有师生员工均有义务及时向网络安全和信息化处报告网络安全事件，未经授权不得对外公布或利用所发现的安全漏洞。

第九章 奖励与追责

第五十条 网络安全事件的责任由学校网络安全和信息化领导小组认定。

第五十一条 网络安全工作纳入信息化建设先进集体、个人评选范围，对成绩显著或者做出突出贡献的集体和个人，予以表彰、奖励；发生重大网络安全事件的，取消周期内评优资格。

第五十二条 学校各单位在收到网络安全整改通知书后，应按要求限期整改，整改不力的，给予通报批评并责令改正；对存在网络安全隐患较多且长期未整改或瞒报、漏报网络安全事件的单位或个人，将予以通报，并追究相关人员的责任。

第五十三条 对于违反法律、法规和本办法规定，造成国家、学校、个人损失或网络安全事故的单位或个人，学校将依法依规进行党纪、行政处分，构成犯罪的，配合国家有关机构追究责任。

第十章 附则

第五十四条 本办法由网络安全和信息化处负责解释，自发布之日起施行。原有《对外经济贸易大学信息系统安全管理办法（暂行）》（外经贸学网络字〔2013〕62号）同时废止。

附件

信息系统（网站）漏洞整改管理规范

为落实教育部、公安局等上级管理部门对网络安全漏洞整改的要求，进一步增强快速及时处理漏洞的能力，提高整改效率，消除安全隐患，对于信息系统（网站）漏洞整改的管理规范如下。

一、接到上级管理部门的限时整改通知

信息处接到上级管理部门，包括但不限于教育部科技司、北京市公安局、教育行业漏洞报告平台等的限时整改通知后，向信息系统（网站）负责单位发放《信息系统安全整改通知书》，负责单位在规定的时限内进行漏洞修复和系统整改并反馈至信息处，由信息处统一上报。

对未在规定的时限内完成漏洞修复和系统整改并反馈文件的信息系统（网站），信息处将根据不同情况进行不同程度的处理。

（一）对超过 3 天未完成整改的，将对涉事信息系统（网站）进行关闭校外访问权限；

（二）对关闭校外访问权限后 10 天还未完成整改的，将对涉事信息系统（网站）关闭服务器处理。

二、学校自查发现存在需整改的漏洞

信息处对学校的信息系统（网站）定期进行安全扫描，漏洞扫描结果以邮件的方式发送至信息系统（网站）负责人邮箱。负

责单位应及时进行漏洞修复和系统整改。

（一） 漏洞扫描

根据信息系统（网站）的不同类型和所处的不同时期设置相应的安全扫描频率。

1. 对开通校外访问的信息系统（网站）每月进行安全扫描；
2. 对校内访问的信息系统（网站）每 3 个月进行安全扫描；
3. 重要时期对开通校外访问的信息系统（网站）每周进行安全扫描。

（二） 定期复核

信息处定期对漏洞修复情况进行复核，根据信息系统（网站）的不同类型和所处的不同时期设置相应的复核频率。

1. 对开通校外访问的信息系统（网站）每个月进行漏洞修复情况复核；
2. 对仅限校内访问的信息系统（网站）每 3 个月进行漏洞修复情况复核；
3. 重要时期开始前对开通校外访问的信息系统（网站）进行漏洞修复情况复核。

复核存在中高危漏洞未修复，向其负责单位发放《信息系统安全整改通知书》。

（三） 未整改处理

对未完成漏洞修复和系统整改并反馈文件的信息系统（网站），信息处将根据不同情况进行不同程度的处理。

1. 对开通校外访问的信息系统（网站），收到《信息系统安全整改通知书》后超过 10 天仍未整改的，将关闭其校外访问权限。
2. 对仅限校内访问的信息系统（网站），收到《信息系统安全整改通知书》后超过 10 天仍未整改的，将对其进行关闭服务器处理。