中共泰山科技学院委员会
泰山科技学院文件

泰科党字〔2026〕2号

关于印发《泰山科技学院网络安全管理制度（试行）》的通知

各部门、各单位:

现将《泰山科技学院网络安全管理制度（试行）》印发，请各部门、各单位高度重视，认真贯彻执行。

特此通知

中共泰山科技学院委员会　　泰山科技学院

2026年1月19日

泰山科技学院
网络安全管理制度（试行）

第一章 总则

第一条 为保障校园网络基础设施、信息系统及数据的安全稳定运行，维护公共秩序和学校稳定，防范网络安全风险，落实网络安全责任，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》等法律法规文件的规定，结合学校实际，制定本制度。

第二条 本制度适用于学校所有单位和个人，适用于学校信息化设施设备和系统（包括线缆）的建设、运行、维护和网络使用。

第三条 学校倡导诚实守信、健康文明的网络行为，严禁一切利用互联网从事危害师生身心健康的活动，学校将致力于构建健全的网络舆论导向和安全健康的网络环境。学校鼓励全校师生合理合法地利用互联网，任何个人和组织在使用网络时，必须遵守宪法和法律，维护公共秩序，尊重社会公德，严禁危害网络安全，严禁利用网络从事危害国家安全、荣誉和利益的活动，包括但不限于煽动颠覆国家政权、推翻社会主义制度、煽动分裂国家、破坏国家统一、宣扬恐怖主义与极端主义、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行为。

第四条 各单位信息系统应遵循“谁建设，谁主管，谁负责”及网络安全“三同步”的基本原则，在设计和建设阶段必须严格按照学校网络安全标准执行，并在运行过程中持续强化网络安全管理。

第二章 组织机构与工作职责

第五条 学校网络安全和信息化领导小组是学校网络与信息安全工作的领导机构（后简称领导小组）。领导小组由书记和校长任组长，学校其他领导任副组长，校内各二级职能部门、学院、教学部负责人任成员，统筹协调、指导推进学校网络与信息安全工作。

领导小组的主要职责：

（一）贯彻落实国家、教育部以及上级主管部门网络安全工作的方针、政策；

（二）审定学校网络与信息安全建设的总体规划及经费预算；

（三）审议学校网络与信息安全工作的规章制度；

（四）明确网络与信息安全工作中各部门的责任分工、资源分配；

（五）对网络与信息安全建设中的重大项目、重大问题进行讨论决策。

第六条 领导小组下设办公室，具体负责学校网络与信息安全工作的管理和落实，定期向领导小组汇报网络与信息安全工作

并提出建议，办公室设在网络与信息管理中心（后简称网信中心），由分管信息化的责任领导任办公室主任，网信中心和品牌营销与新闻中心负责人任副主任。

网络安全和信息化办公室主要职责：

（一）贯彻执行学校网络安全与信息化领导小组的各项决策决议；

（二）拟定学校网络安全与信息化发展的总体规划、政策法规、标准规范以及经费预算；

（三）负责进一步完善网络安全和信息化工作管理体系；

（四）负责保障学校网络信息安全和基础网络安全，建立健全信息网络安全防范机制，制定安全事件应急预案，推动开展网络舆情收集、分析以及网络舆论引导工作；

（五）负责学校网络信息平台的建设以及各单位、各部门网络信息平台的审核，规范各种网络信息平台（含移动端）的审批流程，加大监管力度，加强公共信息平台应用的推广和培训工作；

（六）负责分期实施学校信息化规划，对信息化项目进行组织协调与实施，对各单位申报的信息化新建和改造项目进行审核，对各业务系统信息资源进行整合集成，为各单位信息化提供技术支持；

（七）负责建设、管理和维护学校基础网络设施，合理分配信息网络资源；

（八）负责统一组织和协调校企合作网络信息化项目，涵盖

项目的审核、合同签订、组织实施及验收等各个环节。

（九）定期召开网络与信息安全专项工作会议，有针对性地进行研究和论证，协商决议网络与信息安全重点建设项目、规章制度制定及突发事件应急处置等事宜，为领导和学校提供决策依据。

第七条 学校各单位作为本单位网络与信息安全工作的责任主体，其单位负责人承担第一责任人的职责，分管信息化工作的负责人负责本单位的网络与信息安全工作，信息化联络员具体负责管理和协调本单位的网络与信息安全事务。

第八条 学校积极倡导多措并举提升网络安全人员的专业技能，将通过多种途径加大对网络安全人才的培养和培训力度，持续推动教学与技术的深度融合与交流。

第三章 网络安全

第九条 学校依据国家法律法规的规定，履行网络与信息安全保护职责。通过实施上网实名制、网络资源使用备案制、网络资产分级分区保护策略等措施，确保校园网络免受干扰、破坏或未经授权的访问，保障网络系统的稳定运行，防止数据泄露、被窃取或篡改。

第十条 任何单位和个人严禁从事入侵他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的行为，包括故意制作、传播计算机病毒等破坏性程序，不得提供用于入侵网络、干扰网络正常功能、窃取网络数据等危害网络安全活动的信息、

工具及制作方法，不得为他人实施危害网络安全的活动提供技术支持、广告推广、支付结算等协助。

第十一条 任何单位和个人应对其网络使用行为负责，不得建立用于实施诈骗、传授犯罪方法、制作或销售违禁物品、管制物品等违法犯罪活动的网站或通讯群组，不得利用网络发布涉及上述违法犯罪活动的信息。

第十二条 任何单位和个人通过网络发送的电子邮件、电子信息及提供的应用软件等，不得含有恶意程序，不得包含法律法规禁止发布或传输的信息。

第十三条 校园网与互联网及其他公共网络按需实行物理或逻辑隔离，由学校统一出口、统一管理和统一防护，校园网络管理部门在校园网络出口部署用户行为管理、网络安全检测防护、网络安全日志记录管理等设备，保障用户合法上网行为。

第十四条 校园网络内部采取分级分区保护策略，将网络划分为系统核心区域、学生宿舍区域、教学实训区域和公共网络区域，针对不同区域实施相应的网络安全防御策略，确保网络的便利性与安全性。系统核心区域细分为一般系统区域、重要系统区域和核心系统区域，并分别部署相应的网络安全设备和防护措施。

第十五条 校园网络实行实名认证上网制度，师生使用学校网络需通过实名制认证后方可上网。学校在任何网络接入点均需进行实名认证，杜绝非本校人员非法接入。各单位及个人未经批

准，不得擅自改变校园网络结构，不得通过其他渠道接入互联网及其他公共网络。对危害校园网络安全的用户，网络安全和信息化办公室有权采取断网处理并追究其责任。

第十六条 校园网络账号由网信中心统一集中管理。教师和学校工作人员账号由网信中心统一分配，学生账号由学校委托合作运营商营业厅实名办理。各部门公共账号由网信中心确定实名管理人后按需分配。

第十七条 对学校网络资源的使用和托管实行审批备案制度。凡需使用服务器托管、公网 IP 及域名、校园内网固定 IP 地址等网络资源，须通过 OA 流程进行审批，审批通过后由网信中心协助开通使用。

第十八条 运营商入校建设基站、机房、室分天线、光纤线缆及有线无线网络设备等，须按要求向网信中心提交完整的建设资料，包括建设方案、设备清单、建设图纸和建设承诺书等，经网信中心、资产处、基建后勤处审批后方可施工建设。

第十九条 学校定期组织网络安全培训与教育活动，增强师生网络安全意识与防护技能，确保师生能够正确识别网络风险，合理使用网络资源，避免因人为疏忽导致的网络安全事件。

第二十条 建立网络安全应急响应机制，网信中心负责制定网络安全应急预案，明确应急处置流程与责任分工。一旦发生网络安全事件，应立即启动应急预案，迅速采取措施控制事态发展，减少损失，并及时向上级主管部门报告。

第二十一条 网信中心应定期对校园网络进行安全检查与风险评估，及时发现并修复安全漏洞，消除安全隐患。同时，建立网络安全日志记录与分析系统，对网络活动进行全程监控，为网络安全事件的追溯与处理提供依据。

第二十二条 对于违反本制度的单位和个人，学校将视情节轻重给予相应的纪律处分；构成犯罪的，将依法追究其刑事责任。同时，学校鼓励师生积极举报网络安全违法行为，对举报有功人员给予表彰与奖励。

第四章 信息系统安全

第二十三条 信息系统的建设实行审批备案制度，并严格按照《泰山科技学院信息化工作管理办法》的相关要求进行备案、建设与管理，未经审批备案的信息系统不得在校园网内部署或接入。

第二十四条 学校网站及二级网站的建设、内容发布实行审批备案制度，并严格按照《泰山科技学院校园媒体平台管理办法》的具体要求进行备案和管理，网站主办单位对所发布内容的真实性、合法性负责，定期开展内容自查，杜绝违法违规信息。

第二十五条 学校微信、微博、抖音等新媒体平台的建设实行实名审批备案制度，并严格按照《泰山科技学院校园媒体平台管理办法》进行备案和管理。平台运营单位需指定专人负责内容审核与安全管理，建立信息发布审核台账，严禁发布危害国家安全、破坏社会稳定或侵犯他人权益的信息。

第二十六条 信息系统的建设与管理应满足基本的安全要求，落实以下防护措施：

（一）机房安全防护：信息系统所在机房应具备电源防护、防雷接地、UPS不间断电源、防火、防静电、防震等基础安全设施，建立机房出入登记制度，非授权人员不得进入。

（二）网络安全防护：部署防火墙、入侵检测/防御系统（IDS/IPS）、网络隔离设备，严格控制端口开放范围，启用访问审计、态势感知及日志审计功能，对终端设备安装杀毒软件和终端安全管理工具。

（三）人员与权限管理：信息系统管理人员实行审批备案制度，各级管理权限经学校审批后报网信中心备案。管理人员需履行安全管理责任，规范权限分配与访问控制，记录权限分配明细，严禁非法授权、越权访问或私自篡改数据。

（四）日志留存要求：信息系统应留存网络日志、操作系统日志和应用系统日志，保存期限不少于6个月，确保可追溯网络攻击、异常访问等安全事件。

第二十七条 所有重要信息系统（使用公网IP的信息系统）必须根据《信息安全等级保护管理办法》实施定级备案，具体要求如下：

（一）在校运行的各平台、业务系统均须根据网信办下发的“定级指南”进行定级，定级工作由网信中心组织开展，系统管理部门配合实施。

（二）等级保护测评不合格的系统，须立即下线整改，由系统管理部门牵头、网信中心配合，整改期不得超过3个月，整改完成后，系统负责部门需提交整改报告至网络安全与信息化办公室，经分析研判合格后方可恢复运行。

第二十八条 各单位建设、使用和维护的信息系统，应当严格落实网络与信息安全主体责任，按照网络安全等级保护制度要求，履行下列安全保护义务:

（一）制定内部网络安全制度、安全巡检制度及应急预案，明确网络安全负责人，落实安全责任。

（二）采取防范计算机病毒、网络攻击、网络侵入等危害网络安全行为的技术措施。

（三）部署监测、记录系统状态和网络安全事件的技术措施，确保事件可追溯。

（四）对数据进行分类管理，对重要数据实施容灾备份和加密保护。

（五）规范数据使用流程，涉及学生个人信息、成绩信息等重要数据，仅限系统管理员下载使用；非管理人员需使用时，须经单位领导批准，使用后在管理员监督下立即删除或销毁，并做好使用记录。

（六）履行法律法规规定的其他安全保护义务。

第五章 数据安全

第二十九条 学校核心数据是指涉及学校战略及发展的重大

核心数据，包括财务数据、学校重大发展规划、战略举措、学校领导重要讲话、重要非对外管理制度章程、学校上报的各类统计数据，以及一旦泄露会对学校产生重大舆情或重大事故的数据。核心数据管理应符合以下要求：

（一）实行隔离保存，由部门专门购置非联网计算机存储此类数据；

（二）严格限制数据操作权限，对使用隔离计算机的人员进行权限分配与管控；

（三）规范存储介质管理，对U盘、光盘等介质进行登记和专人保管；

（四）隔离计算机需设置开机密码，密码由部门领导或指定人员保管；

（五）数据拷贝或计算机使用需进行严格登记，记录操作人、时间、用途等信息；

（六）定期对隔离计算机进行杀毒处理，防止恶意程序感染。

第三十条 学校重要数据是指除核心数据外需重点保护的数据，包括涉及教师及学生隐私的各类业务系统数据、管理信息数据、合同图纸、一卡通消费数据、教职工通讯联系方式等。重要数据管理应符合以下要求：

（一）仅限校园内部使用，确需对外流转或公布的，须经上级领导授权；

（二）可在办公电脑中处理，但禁止拷贝至私人电脑；

（三）严格限定师生隐私信息的掌握范围，制定数据使用流程，使用后及时销毁；

（四）涉及重要数据的办公电脑需设置开机密码、安装杀毒软件，启用终端安全管理工具。

第三十一条 任何单位及个人不得将学校核心数据、重要数据上传至各类文库或对外买卖。一经发现，将根据后果严重性予以处分；涉嫌违法的，移交公安机关处理。

第三十二条 学校对核心数据、重要数据实施分层分类重点保护，采取防破坏、防篡改和异地灾备等技术措施，确保数据完整性和可用性。

第三十三条 学校根据信息系统规模购置备份系统，按数据重要程度分级备份，填写《备份登记表》并标注备份内容。备份介质需定期存放在安全地点并编号管理。

第三十四条 数据异常破坏需恢复时，数据管理员应立即上报并申请恢复，优先使用最近备份数据，最大限度降低损失。恢复操作需记录备案，包括故障原因、恢复过程、数据完整性校验结果等。

第三十五条 对于涉及学校核心数据和重要数据的操作，必须进行双人复核机制，确保每一步操作都经过至少两人的确认，防止数据误操作或恶意篡改。

第三十六条 学校应定期组织数据安全培训，增强全体教职工的数据安全意识，确保每位员工都能了解并遵守数据保护的相

关规定和流程。

第三十七条 在数据传输过程中，必须采用加密技术，确保数据在传输过程中的安全性，防止数据在传输过程中被截获或篡改。

第三十八条 学校应建立数据泄露应急响应机制，一旦发生数据泄露事件，能够迅速启动应急响应流程，及时通知相关人员，采取有效措施防止损失扩大，并按照规定上报相关部门。

第六章 个人信息安全

第三十九条 个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括但不限于姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码、电子邮箱、行踪信息等。学校对个人信息实行全生命周期安全管理，遵循合法、正当、必要原则，保障师生个人信息权益。

第四十条 个人信息收集与处理

（一）各单位在开展教学、科研、管理等活动时，如需收集师生个人信息，应明确告知收集目的、方式、范围及使用规则，取得本人同意后方可收集，禁止强制或变相强制收集无关信息。

（二）收集个人敏感信息（如身份证号、银行卡号、病历资料等）时，须对信息收集过程进行记录备案。

（三）禁止通过欺骗、误导、胁迫等方式获取个人信息，禁止从非法渠道购买、收受他人个人信息。

第四十一条 个人信息使用与传输

（一）使用个人信息时不得超出收集时声明的范围，如需用于其他目的，应再次取得本人同意；禁止篡改、伪造、泄露或非法向他人提供个人信息。

（二）个人信息在内部传输时，须通过学校加密邮件系统或专用传输平台，禁止使用微信、QQ 等非加密工具传输；向外部单位传输时，须签订数据共享安全协议，明确双方安全责任及数据使用限制。

（三）利用个人信息开展数据分析、模型训练等活动时，应对数据进行脱敏处理（如去标识化、匿名化），确保无法识别特定个人，且脱敏后数据不得反向还原。

第四十二条 个人信息共享与公开

（一）因工作需要共享个人信息的，须经学校网络安全与信息化办公室审批，共享对象仅限具备相应安全保障能力的单位或机构，并对共享数据用途、期限进行严格限定。

（二）公开个人信息（如公示获奖名单、学术成果等）前，应进行必要性审查，对涉及隐私的内容（如联系方式、家庭住址）进行删除或脱敏处理；未经本人同意，不得公开其个人敏感信息。

第四十三条 个人信息安全事件处置

（一）发生个人信息泄露、丢失、篡改等安全事件时，相关单位应立即启动应急预案，采取补救措施（如封锁漏洞、撤回信息、通知受影响人员），并在 24 小时内向网络安全与信息化办公

室报告事件详情及处置进展。

（二）网络安全与信息化办公室接到报告后，应组织评估事件影响范围及危害程度，必要时协调公安、网信等部门介入调查，并按照规定向教育主管部门报备。

第四十四条 个人信息主体权利保障

师生有权查询、复制、更正本人个人信息，有权要求删除与收集目的无关或已过保存期限的个人信息。相关单位应在收到申请后15个工作日内予以答复或处理，对合理诉求不得拒绝或拖延。

第四十五条 任何单位和个人违反本章规定，造成个人信息泄露或滥用的，学校将依据本办法第九章“责任追究”相关条款处理；情节严重构成犯罪的，移交司法机关依法追究刑事责任。

第七章 安全产品与服务采购安全

第四十六条 学校安全产品与服务采购应遵循安全优先、合规可控、质量保障原则，严格执行国家网络安全法律法规及学校采购管理制度，确保采购的产品和服务符合网络安全等级保护及数据安全要求。

第四十七条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或

者当事人约定的期限内，不得终止提供安全维护。

第四十八条 网络安全设备的采购，原则上由网信中心负责牵头组织，如二级单位有采购计划的，必须与网信中心协商，并共同拟定初始安全策略。

第四十九条 任何单位不得采购或使用未经安全认证、来源不明的网络安全产品，不得委托无资质机构提供安全服务。

第八章 监测预警与应急处置

第五十条 监测机制与责任分工

学校建立“日常监测+专项巡查+技术防护”三位一体的网络安全监测体系，实现对校园网络、信息系统及数据的全时段、全覆盖监控。

（一）网络安全与信息化办公室牵头负责全校网络安全监测工作，通过部署安全态势感知平台、入侵检测系统（IDS）、日志审计系统等技术工具，实时监测网络攻击、异常访问、数据泄露等安全事件，定期形成《安全态势分析报告》报送领导小组。

（二）各二级单位指定信息化联络员为监测第一责任人，每日巡查本单位业务系统、网站及数据存储设备运行状态，发现问题立即处置并在2小时内上报网络安全与信息化办公室。

（三）品牌营销与新闻中心负责网络舆情监测，对校园论坛、社交媒体、新闻网站等平台涉及学校的敏感信息进行7×24小时巡查，建立舆情分级预警机制（一般、较大、重大），按《网络舆情突发事件处置预案》流程上报处置。

第五十一条 预警流程与响应机制

（一）预警分级

根据安全事件的危害程度和影响范围，分为四级预警：

一级预警（特别重大）：核心系统瘫痪、大规模数据泄露（如全校师生个人信息泄露）、重大网络攻击导致校园网中断超24小时；

二级预警（重大）：重要系统故障、敏感数据泄露（如财务数据、考试信息）、网络攻击影响多个部门业务；

三级预警（较大）：单一系统漏洞、局部网络异常、小规模舆情扩散；

四级预警（一般）：终端病毒感染、账号盗用等个体性安全事件。

（二）预警发布与处置

一级、二级预警由领导小组组长签发《预警通知书》，立即启动校级应急预案，协调网信中心、保卫处、品牌营销与新闻中心等部门联合处置；

三级、四级预警由网络安全与信息化办公室主任签发，通知相关单位在4小时内完成处置，并反馈结果。

第五十二条 应急响应与处置流程

（一）事件报告

发生网络安全事件后，事发单位须立即通过电话、OA系统双渠道向网络安全与信息化办公室报告，报告内容包括：事件类

型、发生时间、影响范围、已采取措施及联系人。网络安全与信息化办公室在1小时内研判事件等级，按预警分级流程上报。

（二）应急处置

技术处置：网信中心牵头对受影响系统进行隔离，阻断攻击源，留存日志证据（如IP地址、攻击路径、操作记录），同时启动备用系统恢复业务连续性；

舆情管控：品牌营销与新闻中心对事件相关舆情进行实时跟踪，通过官方渠道发布权威信息，防止谣言扩散；

人员调度：领导小组根据事件需要，调动应急技术组、公关组、后勤保障组等专项工作组，明确职责分工和时间节点。

（三）事件终止

当满足以下条件时，可终止应急响应：

1.攻击行为已彻底阻断，系统漏洞修复完成；

2.受影响数据已恢复，未造成进一步扩散；

3.舆情态势平稳，相关负面信息得到有效管控。

第五十三条 事后恢复与总结改进

（一）系统恢复

应急处置结束后，由网络安全与信息化办公室组织技术团队对系统进行安全加固（如补丁更新、权限重置、数据加密），通过渗透测试、漏洞扫描确认无残留风险后，方可恢复系统运行，恢复过程需留存《系统恢复确认书》。

（二）事件复盘

网络安全与信息化办公室在事件结束后5个工作日内组织召开复盘会议，分析事件原因、处置过程及责任认定，形成《网络安全事件调查报告》，报送领导小组审议。对因管理失职、处置不当导致事件扩大的单位或个人，按第九章“责任追究”条款处理。

第五十四条 各单位须将网络安全监测预警与应急处置纳入年度工作考核，对在事件处置中表现突出的个人给予表彰奖励，对迟报、漏报、瞒报或处置不力的单位及责任人予以通报批评。

第九章 责任追究

第五十五条 凡网络与信息安全相关工作涉密人员（包括但不限于各类网络关键基础设施、信息系统、重要数据的管理及运维人员）均应按照学校要求签订保密承诺书，履行保密责任。

第五十六条 发现有违反保密协议的个人，或违反网络与信息安全管理制度、网络与信息安全工作存在不足和隐患且逾期不改的单位，网络安全与信息化办公室将上报学校给予通报。

第五十七条 任何个人和组织有权向学校网络安全与信息化办公室举报危害学校网络与信息安全的行为，收到举报后，网络安全与信息化办公室应当及时牵头开展调查，并依纪依规进行处置。调查、处置过程中应当对举报人的相关信息予以保密，保护举报人的合法权益。

第五十八条 网络安全事件的责任认定，由网络安全与信息化办公室提交领导小组研究处理。对拒不执行网络与信息安全管

理相关制度、漠视网络安全工作以致造成重大事故和案件的单位，学校将追究该单位主要负责人和直接责任者的责任。对损坏校园网络或信息系统设备设施、泄露危害数据安全及个人信息安全的个人，学校将视其情节轻重追究责任。如触犯法律，将移交公安司法机关处理。

第十章 附则

第五十九条 本制度与国家法律法规和规范性文件不一致的，以国家法律法规和规范性文件为准。

第六十条 本办法由网络安全与信息化办公室负责解释，自公布之日起施行，以前学校有关规定与本办法相抵触的，以本办法为准。

第六十一条 本办法在执行过程中，若因实际情况需要修订或补充，网络安全与信息化办公室应及时组织相关人员进行研讨，提出修订或补充建议，并按照学校规定的程序进行审批和发布。

第六十二条 学校各单位应积极配合网络安全与信息化办公室开展网络安全管理工作，提供必要的支持和协助，共同维护学校网络与信息安全。

中共泰山科技学院委员会办公室　　2026年1月19日印发