广 东 工 贸 职 业 技 术 学 院

关于印发《广东工贸职业技术学院网络与信息安全管理办法》的通知

各部门、各二级学院:

经校长办公会批准通过《广东工贸职业技术学院网络与信息安全管理办法》（制度编号：GDGM-WI-IT-03-03），现印发给你们，请认真贯彻执行。

广东工贸职业技术学院

2025 年 3 月 25 日

密级	主动公开	制度编号	GDGM-WI-IT-03-03
管理模块	信息系统管理	制度级别	三级

广东工贸职业技术学院
网络与信息安全管理办法

修　订　记　录

日期	版本	修订内容概要	拟订	审核	通过形式	批准
2025 年 2 月	V1.0	新增	苏安伦	卢志海 詹东霖	经 2025 年第 2 次校长办公会审定	何汉武

广东工贸职业技术学院
网络与信息安全管理办法

第一章　总　则

第一条【目的和依据】根据《中华人民共和国网络安全法》（主席令第53号）的要求，进一步加强校园网络信息安全的管理，规范学校各级网络信息平台建设，保证网络信息安全，结合我校实际情况，特制定本管理办法。

第二条【适用范围】本办法适用于广东工贸职业技术学院拟建、在建以及运行的信息系统。

第三条【定义】本办法所指信息系统指广东工贸职业技术学院门户系统及其他相关业务系统。本办法中的网络信息是指广东工贸职业技术学院在校园网内由学校各部门、各二级学院和个人建立的服务器、网络、业务系统、网站、新媒体（论坛、博客、微博、公众账号、即时通信工具、网络直播等）等网络信息平台中的所有信息。

第四条【原则】本办法的原则为“涉密不上网，上网不涉密”；本办法的编制参照了以下国家、教育行业的标准和文件：

《信息安全技术 信息系统安全管理要求》（GB/T 20269—2006）

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）

《信息系统等级保护 安全建设技术方案设计要求》（报批稿）

第二章 组织与职责

第五条【党委会】承担以下职责:

（一）审批信息安全管理目标及管理规划;

（二）审批重大安全事故（遭到攻击致使校园网络、重要信息系统瘫痪或者受到上级安全管理部门通报批评的事故）的处理方案及报告;

（三）其他信息安全相关重大事项（预算金额达到500万元及以上）审批工作。

第六条【校长办公会】承担以下职责:

（一）审议信息安全管理目标及管理规划;

（二）审议重大安全事故的处理方案及报告;

（三）其他信息安全相关重大事项（预算金额达到50万元及以上，500万元以下）审议工作。

第七条【安全管理委员会】承担以下职责:

（一）审议信息安全管理目标及管理规划;

（二）指导信息安全管理工作;

（三）审议重大安全事故的处理方案及报告;

（四）其他信息安全相关重大事项审议工作。

第八条【组织宣传统战部】组织宣传统战部是校园信息舆情管理部门，负责校园信息舆情的审查、监督、监察、监管，对媒体加强集中管理，严格规范审批与备案程序。

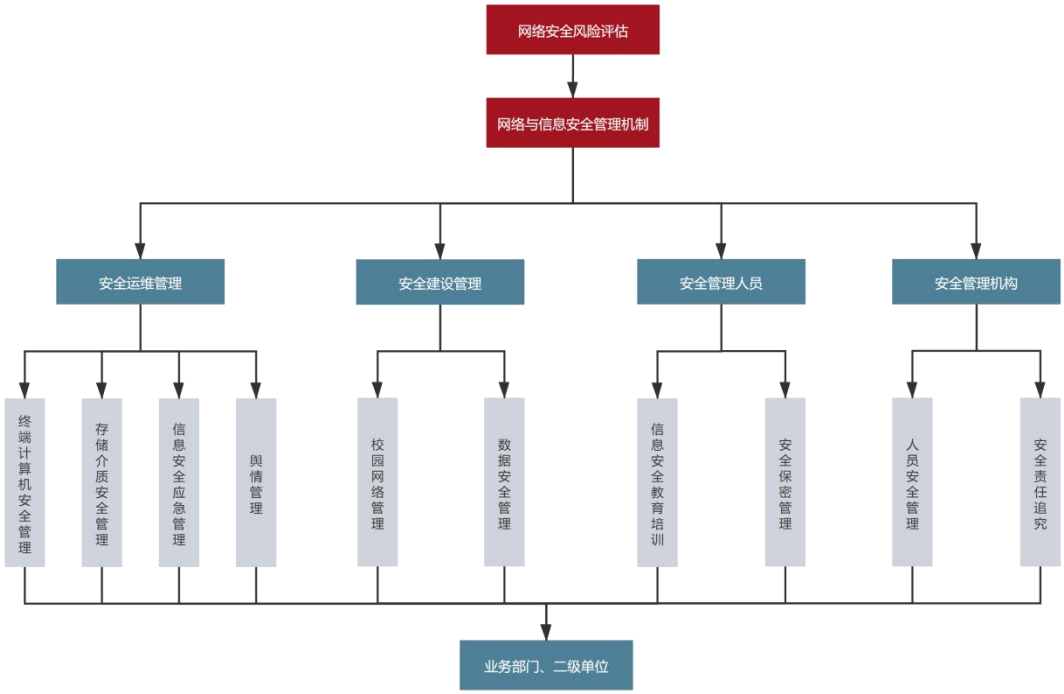
第九条【保卫部（武装部）】负责校园网络信息安全事故的上报，协助信息中心完成网络安全事故的处理。

第十条【信息中心】负责校园网络信息安全的技术防护与保障，通过技术手段，对服务器、网络、业务系统、网站加强集中管理，严格规范审批与备案程序。

第十一条【其他部门】本部门信息系统管理岗兼任信息安全员，负责本部门相应信息系统的安全管理。需将信息安全员及其联系电话报党委宣传部审核和信息中心备案；如人员发生变更，需在调整发生之日起两个工作日内通知党委宣传部和信息中心。各部门、各二级学院对各自主管的网络信息平台信息负有审查、监察、监管的责任，各部门、各二级学院所需应用系统的建设由信息中心统一策划并组织实施，原则上各部门、各二级学院的互联网站应建立在学校网站群中、网络课程应建立在学校网络课程平台中。

第三章　管理机制

第十二条【管理机制】结合我校实际情况及信息系统的安全需求，加强对于信息系统的网络安全风险评估，我校建立配套的网络与信息安全管理机制，并为落实相关的工作，将工作细分为安全建设管理、安全管理人员、安全管理机构以及安全运维管理，具体的内容如下所示：



第四章　信息安全教育培训

第十三条【组织培训】信息中心负责组织学校信息安全宣传和教育培训工作，建立健全相关制度。

第十四条【提高意识】信息中心定期组织开展针对师生员工的信息安全教育，提高师生员工的安全和防范意识。

第十五条【技能培训】信息中心定期开展针对信息安全管理人员和技术人员的专业技能培训，提高信息安全工作能力和水平。

第五章　校园网络管理

第十六条【校园网络管理】所有网络服务的开设需由信息中心审批，落实安全责任，完善配套管理办法，做好网络服务备案和信息安全等级保护工作，并按公安部门要求保存用户日志 180 天以上，以备追查。

各部门、各二级学院应建立完善的网络信息发布与审核制度，确定负责内容编辑、内容审核、内容发布的人员名单，明确审核与发布程序，保存相关操作记录。原则上各部门、各二级学院和个人不允许开设 BBS、电子论坛、留言板、聊天室等交互式服务，因特殊原因需开设，要严格办理登记手续，并附有关的管理办法和用户实名注册技术措施，并有专人监控和管理，对不良信息要及时发现和处理。

严格遵守学校校园计算机网络、电子邮件、网站建设及信息系统建设等管理办法中安全方面的规定。校园网内所有终端设备必须实名登记注册才能上网，所有信息系统必须通过安全检测、登记备案后才能上线。

第六章　数据安全管理

第十七条【录入】数据的采集和录入要遵循源头、真实、准确、完整、及时的原则。重要数据的录入及修改应指定专人来完成。

第十八条【权限】根据数据的保密规定和用途，确定使用人员的存取权限和方式，防止越权操作，禁止私自泄露、外借和转移内部数据与信息。

第十九条【管理】根据学校的职能域将数据进行分类管理。外单位或外部信息系统需要利用或共享数据时，需要书面申请，通过审批后，由学校数据来源部门提供。任何单位和个人不得擅自对外提供学校内部数据。

第二十条【备份】建立数据备份、容灾和恢复机制，加强数据存储和归档管理，确保重要数据有备份、可恢复。

第七章　安全保密管理

第二十一条【安全保密】遵守国家有关法律、法规，严格执行安全保密制度，不得利用计算机网络进行搜集、整理、窃取、发布或谈论涉及国家及学校机密信息。不得利用电子邮件传递、转发或抄送此类信息。

未经审批，学校内部文件、试卷、教案等学校内部信息，以及师生的身份证号、家庭住址和电话等个人隐私信息严禁挂网。

发现国家及学校机密泄露的情况，应立即向学校保卫处报告。保卫处按要求上报省教育厅、省公安厅等有关部门，并配合有关部门查处。

第八章　舆情管理

第二十二条【舆论引导】各部门、各二级学院应加强主流舆论的引导，营造出学习先进、弘扬正气的舆论氛围，促成健康、积极的主流舆论的形成。

第二十三条【舆情汇集】组织宣传统战部建立网络舆情汇集机制，紧紧围绕师生关注的热点、焦点问题及学校管理决策、师生权益等方面，通过BBS、百度贴吧、QQ、微信、微博、博客等渠道，进行舆情信息收集，及时掌握苗头性、预警性信息。网络舆情汇集结果协同给保卫部（武装部）和信息中心。

第二十四条【分析研判】组织宣传统战部建立网络舆情分析研判机制，增强舆情危机的预见性。定期组织开展网上信息调研，对采集的舆情信息进行整理分析，准确把握舆情态势，并提出引导舆情或解决问题的对策建议。

第二十五条【舆情干预】组织宣传统战部建立网络舆情干预机制，增强网络舆情可控性。对发现的不良信息，学校第一时间进入应对状态，避免事态扩大。同时，坚持网上网下联动，对师生在网上反映的问题及时落实解决，寓舆情管理于服务之中。

第九章　终端计算机安全管理

第二十六条【责任】按照“谁使用，谁负责”的原则，终端计算机使用人负有保管和安全使用的责任。

第二十七条【正版软件】终端计算机设备上安装、运行的软件须为正版软件。使用盗版软件带来的安全和法律责任由终端计算机使用人承担。

第二十八条【备份】终端计算机使用人应做好数据日常管理和保护，定期进行数据备份。非涉密计算机不得存储和处理涉密信息。

第二十九条【安全防范】终端计算机使用人应做好终端计算机的安全防范，如发现终端计算机出现可能由病毒或攻击导致的异常系统行为或其他安全问题，应立即断网后进行处理。

第十章　存储介质安全管理

第三十条【采购】原则上，存储阵列、磁带库等大容量介质应由信息中心统一采购和管理，存放在学校数据中心机房。信息中心应采取必要技术措施防范数据泄漏风险，确保存储数据安全。

第三十一条【管理】学校各部门、各二级学院应建立移动介质管理办法，记录介质类型、重要程度、存放地点、领用、交回、维修、报废、销毁等情况。介质使用人按照“谁使用，谁负责”的原则，对其移动介质负有保管和安全使用的责任。

第三十二条【脱敏】非涉密移动存储介质不得用于存储涉密信息，不得在涉密计算机上使用。介质使用人应注意存储介质的内容管理，对送出维修或销毁的介质应事先清除敏感信息。

第三十三条【保密】涉密介质应当按照秘密载体安全保密要求进行管理。各部门、各二级学院对涉密介质应实行集中管理，责任到人。

第十一章　人员安全管理

第三十四条【责任】学校各部门、各二级学院应建立健全本单位的岗位信息安全责任制度，落实信息安全责任。关键岗位的计算机使用和管理人员应签订《信息安全保密承诺书》，明确信息安全与保密要求和责任。

第三十五条【考核】学校各部门、各二级学院应对信息技术安全岗位的人员进行安全知识和技能的考核，并对考核结果进行记录和保存。

第三十六条【回收】学校各部门、各二级学院应加强人员离岗、离职管理，及时终止相关人员所有系统访问权限，收回各种身份证件、钥匙、徽章以及学校提供的软硬件设备。

第十二章　信息安全检查

第三十七条【检查】学校各部门、各二级学院定期对本单位

信息系统的安全状况、安全保护制度及措施的落实情况进行自查，并配合信息中心的信息安全检查、保密检查等工作。

第三十八条【整改】信息中心对学校各部门、各二级学院的信息技术安全工作落实情况进行检查，对发现的问题下达限期整改通知书，责成相关单位制订整改方案并落实到位。

第三十九条【总结】信息中心对年度安全检查情况进行全面总结，按照要求完成检查报告并报上级信息安全主管部门。

第十三章　信息安全应急管理

第四十条【预案】信息中心负责学校信息安全应急工作的统筹管理，负责制定安全事件应急预案，规范网络与信息安全事件报告与处置流程。

第四十一条【处置】学校各部门、各二级学院应按照学校信息安全事件报告与处置流程，做好事发、事中情况报告与处置和事后整改报告与处置工作，做到安全事件早发现、早报告、早控制、早解决。

第四十二条【报告】学校各部门、各二级学院或师生员工均有义务及时向信息中心报告网络信息安全事件，不得在未授权情况下对外公布、尝试或利用所发现的安全漏洞或安全问题。

第十四章　安全责任追究

第四十三条【责任人】网络信息安全管理按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则切实落实信息安全责任。明确责任、加强引导、突出重点、保障安全。学校各部门、各二级学院是本部门、本二级学院的网络信息安全责任主体，部门中层正职是本部门网络信息安全的第一责任人，二级学院党委书记与院长是本二级学院网络信息安全的第一责任人，信息安全员是主要责任人，系统管理员是直接责任人。

第四十四条【通报追责】对所开设网络服务监管不力造成有害信息传播或秘密信息泄露的单位，给予通报批评和相应的行政纪律处分，追究信息安全员责任，情节特别严重的追究单位负责人的领导责任。

第四十五条【处分处理】各部门、各二级学院或个人收到网络信息安全限期整改通知书后，整改不力或导致严重安全后果的，将根据学校有关规定予以处分。触犯刑律的，移交司法机关处理。

第十五章　附　则

第四十六条【制度管理者】本制度管理者为信息中心负责人，由其负责本文件的拟订与优化、使用培训与解释，以及牵头落地执行。

第四十七条【生效日期及解释权主体】本办法由校长办公会批准生效，自发布之日起施行。本办法由校长办公会授权信息中心负责解释。