北京市工业技师学院

信息化建设与管理制度

**第一章 总则**

第一条　目的

为加快北京市工业技师学院信息化建设，规划软件应用系统、网络建设与使用、计算机及相关设备管理和信息系统安全管理的工作，规范建立和完善学院的各项信息系统，最大程度满足北京市工业技师学院信息化的需求，促进北京市工业技师学院信息化有序规范地发展，特制定本制度。

第二条　适用范围

本制度适用于北京市工业技师学院各部门和专业系（组）。

1. **信息化建设与管理的原则及职责**

第一条　我院信息化建设与管理遵循以下基本原则：

（一）发展导向原则：信息化管理应纳入到学院本身的发展战略中，要与学院未来的目标管理发展充分结合，信息化规划要适合学院的发展规模和发展阶段的需要。

（二）统一规划原则：学院信息化需要以发展的眼光，站在学院的高度，组织各部门，做好学院信息化的中长期发展规划。

（三）分步实施原则：学院的信息化建设工作由学院信息中心进行整体统一规划，具体实施将采取按计划、分阶段、逐步实施的过程。

第二条　学院信息中心在学院信息化建设与管理方面的主要工作职责包括：

（一）拟订和调整学院信息化建设整体规划方案。

（二）组织实施学院信息化建设的整体规划方案。

（三）主导学院各类信息系统、数字化资源、软硬件和网络的建设、日常管理和维护。

（四）协助学院其它部门进行与学院信息化建设相关的项目的申报、招标、采购，并有根据自身专业出发对相关产品进行合理化建议和推荐的义务。

（五）组织处理学院各类信息系统故障。

（六）配合其它部门对学院的信息资产进行统一管理。

（七）根据国家相关法律法规，加强学院信息安全管理。

第三条 各部门和专业系须配备相对稳定的信息员，要求信息员熟悉计算机和网络操作。信息中心定期组织信息员进行技能培训、竞赛以及考核。

**第三章 信息设备的相关管理**

第一条　信息中心负责学院各职能部门计算机及相关信息系统设备的配置技术标准等管理。

第二条　信息中心负责收集计算机及网络设备的最新市场行情信息，向学院其它部门提供建议，并参加对采购的设备进行技术性验收。

第三条　在未通知信息中心的情况下，各部门信息系统使用人员不得调换、拆卸计算机内的零部件及网络设备，如有发生，信息中心按相关规章进行相应处理。

第四条　计算机或网络设备出现故障，知情人员必须及时告知信息中心，由信息中心安排相关人员进行现场技术处理并给予修复，对不能进行修复的设备，由信息中心相关人员明确故障原因，出具鉴定结果，送相关外部机构进行维修处理。

第五条　对需要送修的计算机或网络设备，应由设备的使用责任人或保管责任人提出申请，由信息中心审核后，报后勤部门送相关外部机构维修。

**第四章 软件系统管理**

第一条　学院各部门根据工作需要，向信息中心提出新增或修改相关软件系统，由各部门提出相关需求后，由信息中心进行主导进行。信息中心根据各部门需求情况进行汇总、论证、审核，出具明确的可行性意见，供学院领导决策。

第二条　本院软件系统由信息中心负责相关操作的技术支持和协助。所有信息系统软件帐号由劳资部门向信息中心管理人员提出分配需求，由信息中心管理人员进行帐号和相关权限的分配。

第三条　各类应用软件系统的使用人员均应按系统要求的规范进行操作。

第四条　信息中心负责各类应用软件系统的升级、维护和管理。

**第五章 信息化建设与信息资源管理**

第一条　学院信息化建设，信息中心根据各部门的需求，统一规划，制定相应方案报相关领导负责人审批后组织实施。

第二条 在信息化建设中，各部门的信息化建设应遵循以下原则：

　　1．各部门提出书面申请理由和详细的业务需求报学院信息中心。

　　2．由信息中心进行论证审核，适当时侯，组织专家进行可行性评估论证，报学院领导审批该项目是否向市财政局申请专项经费。

　　3．凡需申请专项经费的信息化项目，由信息中心整理汇总学院当年各信息化建设项目，制定详细的技术指标和要求，列明设备清单，于当年九月份上报经信委和市财政局，拟建项目的金额达到政府采购要求的，应按财务制度相关规定进行政府采购。

　　4．协助相关部门选择项目的合格承建方，确认合同技术条款。

5．项目建设完毕，及时会同各相关部门进行验收，报资产部门及时登记入账。

第三条　学院计算机网络线路、设备、服务器均由信息中心统一组织安装、管理、维护，其他人员不得擅自更换线路和设备，不得擅自拆卸设备、改变计算机和网络配置。

第四条 严禁师生员工利用学院网络资源进入非法网站、下载浏览非法信息，发布非法言论；严禁在学院电脑上保存非法资料和利用黑客等手段下载保存学院信息系统内的机密信息。对于造成违法结果的，信息中心有权配合公安部门对相关日志、记录等信息进行提取和备案，并将追究其责任。

第五条 由于学院网络带宽资源的有限性，网络资源本着满足最紧要事项的原则，信息中心有权对网络资源进行带宽限制和合理分配。上班期间严禁利用办公网络资源进行与工作无关的聊天、游戏、下载、听音乐、看电影等，信息中心将对此进行定期检查工作。如有发现上述情况第一次给予口头警告，每二次直接截断其网络连接，待使用人向其部门负责人及信息中心负责人说明情况后再恢复网络连接。

第六条　信息中心应按合同要求组织信息化项目建设的施工，对工程施工过程进行有效的监督，并在施工完成后，召集相关部门负责人和后勤部门一起共同组织项目验收。

第七条　信息中心应遵守学院保密制度，对学院的信息安全负责，定期对网络线路和全院信息化设备的运行情况进行检查。

第八条　本院任何人不得向其他任何人员泄漏本院网络结构、网络布局、布线系统及软件结构、代码、软件注册码或序列号等有关方面的任何信息。

第九条　各专业系的数字化资源的开发由信息中心制定技术标准规范，信息中心参与验收工作，信息中心对各系的数字化资源的使用进行监督。

**第六章 网络使用与网站管理**

　第一条 各部门人员都有义务维护学院计算机网络的正常运行，并严格遵照有关的规定入网。

　第二条 在工作用网络上只允许进行与业务工作有关的操作，不得进行非法操作。一经发现，将依照有关规定进行处理。

　第三条 不得在工作用网络上传播计算机病毒，造成损失的，将依照国家法律，移交有关部门处理。

　第四条 不得通过工作用网络系统进行营利性的商业行为及散发任何的垃圾邮件。

　第五条 要严格遵守国家关于网络管理的相应法律，不得在网上传播和散布反动、淫秽信息，也不得散布攻击他人的言论。

　第六条 任何人不得对学院网络系统软件设施和信息文件有意破坏和攻击，对于采取破坏手段，无论是否造成不良后果的，追究其个人责任。

　第七条 涉密网络与互联网要完全物理隔离，严禁把工作用涉密网络以任何方式连接到互联网上。

　第八条 个人的入网口令应注意保密，防止其他用户侵入网络设备，保证数据资料安全。办公使用的计算机操作系统应设置口令，并开启屏保口令功能，与其他应用系统的口令都应注意保密，防止被盗用。

第九条 学院网站由信息中心负责管理，各部门信息员负责收集本部门需要及时更新的栏目内容，由本部门负责人审核后，交由院办审核，院办将审核后需上传的栏目文档交与信息中心，信息中心设置专人对网站信息进行操作，其它任何人员无权对网站信息进行更新和删除等操作。

**第七章 信息安全管理**

第一条　学院的信息安全由信息中心统一进行监控管理。

第二条　信息中心负责人为学院信息安全责任人，对学院信息安全负责，信息中心配备信息安全专岗，岗位人员具备信息安全岗位能力要求，原则上要求信息中心负责人具备国家注册信息安全工程师资质。

第三条 使用网络及设备的工作人员应自觉遵守相关法律法规和制度规定。对违反规定使信息化网络及设备不能正常工作和造成重大事故者，追究其相应责任，后果严重的，依法追究法律责任。

第四条 严禁在信息化设备上安装与工作无关的、未经广泛验证为安全的软件程序。严禁带电拔插计算机内部配件。移动非便携式信息网络设备应断电后进行。离开工作场所前，须关闭计算机，切断电源。

第五条 非指定的技术人员不得擅自打开信息化网络设备，进行任何配置和检测。不得擅自将信息网络设备（包括报废设备）的配件私自拆卸，移植到其它设备。

第六条 未经分管领导批准，任何人不得随意更换信息化网络设备，不得随意外借、处置信息网络设备。外部人员如需使用本单位的信息网络设备，需经分管领导同意，并在现场监督的情况下进行。

第七条 对计算机进行硬盘格式化和删除操作系统文件，须事先做好数据备份工作，并由信息中心技术人员进行操作。

第八条 各部门和专业系的信息化网络设备的使用人、保管人、责任人等情况的变更，应及时报信息中心登记备案。

第九条 为防止计算机病毒造成严重后果，对外来移动存储介质（光盘、U盘、移动硬盘等）要严格管理，原则上不允许外来移动存储介质在我院内部专网计算机上使用，确因工作需要使用的，事先必须进行防（杀）毒处理，经信息中心技术人员证实无病毒感染后，方可使用。

第十条 信息中心管理人员应定期对学院信息化网络设备进行系统维护及必要的数据备份，并安装指定的杀毒软件，进行定期杀毒、系统漏洞修补、杀毒软件升级。

第十一条 信息化网络设备报废或调拨时，须进行必要的清理工作，防止资料泄密。

第十二条 为保障信息化网络设备安全、稳定、持续运行，发挥最优性能，设备必须按照技术人员制定的方案和要求进行统一配置，设备的使用者不得拒绝，并不得随意更改设备已配置好的参数。

第十三条　信息中心负责组织信息系统的备份工作，学院信息平台系统及各业务子系统等必须定期、定时进行数据库的备份转存，保证系统故障后能及时恢复。信息系统使用人员应对本人使用的系统帐号和口令保密，由于帐号、口令泄露造成不良后果的，由帐号拥有人负全部责任。

第十四条　信息中心负责学院整体计算机病毒防范工作，负责收集病毒木马信息并进行及时报告，追踪最新病毒动向，制定相应的防范措施，中心机房要求安装有效的杀毒软件或及时下载最新杀毒软件指导计算机使用人员进行病毒防范。

第十五条 信息中心负责对各部门计算机信息系统安全和保密工作进行指导和督促检查。要求各部门密切配合，共同做好计算机信息系统安全和保密工作。

第十六条 加强保密意识教育，提高工作人员保密观念，增强防范意识，自觉执行保密规定。

第十七条 与重点岗位的计算机使用人员签订安全保密责任书，明确安全和保密要求与责任。

第十八条 计算机使用人员离岗离职，信息中心应当即时取消其计算机信息系统访问授权，收回计算机、移动存储设备等相关物品。

第十九条 各部门加强内部计算机信息系统安全和保密管理情况的监督，定期开展自我检查、自我评估，发现问题及时纠正。

第二十条 涉密计算机系统进行维护检修时，须保证所存储的涉密信息不被泄露，对涉密信息应采取涉密信息转存、删除、异地转移存储媒介等安全保密措施。无法采取上述措施时，信息中心技术人员须在维修现场监督，并对维修人员、维修对象、维修内容、维修前后情况做好详细记录。

第二十一条 存有涉密信息的存储介质不得接入或安装在非涉密计算机或低密级的计算机上，不得转借他人，不得带出工作区，下班后存放在本单位指定的保密柜中。因工作需要必须携带出工作区的，须由科室主要负责人填写《涉密存储介质外出携带登记表》，经主管领导批准，返回后要经主管领导审查注销。

第二十二条 严禁维修人员擅自读取和拷贝数字复印机、多功能一体机等涉密设备存储的涉密信息。涉密电子设备出现故障送外维修前，必须将涉密存储部件拆除并妥善保管；涉密存储部件出现故障，如不能保证安全保密，必须按照涉密载体销毁要求予以销毁。

第二十三条 用户密码使用规定：

　　（1）密码必须由数字、字符和特殊字符组成；

　　（2）秘密级计算机设置的密码长度不能少于8个字符，密码更换周期不得多于30天；

　　（3）机密级计算机设置的密码长度不得少于10个字符，密码更换周期不得超过7天；

（4）涉密计算机需要分别设置BIOS、操作系统开机登录和屏幕保护三个密码。

第二十四条 各级用户不得自行对未经核实和签发的信息加载和更新。网站页面（含主页、子页）不得加载涉密资料、信息，有关涉密的统计调查资料。

第二十五条 各部门应及时对本部门涉密文件进行密级标识，要定期做好备份，备份介质必须标明备份日期、备份内容以及相应密级，严格控制知悉此备份的人数，做好登记后进保密柜保存。涉密文件和资料的备份应严加控制。未经许可严禁私自复制、转储和借阅。对存储涉密信息的磁介质应当根据有关规定确定密级及保密期限，并视同纸制文件，分密级管理，严格借阅、使用、保管及销毁制度。

第二十六条 严禁将接入互联网络的计算机设定为网络共享，严禁将机内文件设定为网络共享文件。严禁使用含有无线网卡、无线鼠标、无线键盘等具有无线互联功能的设备处理涉密信息。

第七章 突发情况处理

第一条　网络系统核心设备或主干网络线路发生故障，或因服务器软硬件故障、黑客、病毒攻击，学院主要的应用系统停止服务或系统瘫痪等情况时，信息中心应及时组织力量解决突发事故，恢复信息系统正常运行。

第二条　突发事故发生后，信息中心需及时通知相关领导和其他负责人。

第三条　突发事故处理完后，信息中心需组织查明事故发生原因，对事故进行估，并提交分析评估报告给相关领导。

第四条　接到学院临时停电预报，信息中心应及时通知各部门作好备份和应急准备。

第五条　各部门应配合信息中心部做好计算机的登记、检查和维护工作。

第八章 附 则

第一条　本制度由信息中心进行起草和修订，并做好执行监督。

第二条 本制度自发布之日起生效，未尽事宜由信息中心核准并做相应调整。

第三条 本制度中所指信息安全涉及到的国家相关法律法规是指

《北京市微博客发展管理若干规定》（2011年12月16日公布并施行）

《北京市公共服务网络与信息系统安全管理规定》

《北京市党政机关计算机网络与信息安全管理办法》

《保守国家秘密法（1989）（2010年修订） 》

《计算机信息系统安全保护条例（1994） 》

《全国人民代表大会常务委员会关于维护互联网安全的决定（2000）》

《中华人民共和国治安管理处罚法》

《中华人民共和国电子签名法》

《中华人民共和国侵权责任法》

《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27号）

《中华人民共和国刑法修正案(九)》2015年11月1日起执行。

第四条 本制度由学院信息中心负责解释。

北京市工业技师学院

2015年12月31日