附件2

**山东服装职业学院校园网络安全管理制度**

（试行）

第一章 总 则

**第一条**  为切实加强校园网络安全的管理，进一步规范校园网络信息服务，促进学院信息化建设的健康发展，根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》以及国家和教育行业其他相关法律、法规对网络安全管理的要求，特制定本管理制度。

**第二条**  制度所称的校园网络，是指由学院建设的，提供校园网络应用及服务的软、硬件集成系统，包括由学院相关部门负责维护和管理的校园网络主、辅节点设备，配套的网络线缆设施及网络服务器、网站、各管理信息系统等，以及学院各单位建设的校园网络、网站及应用系统等。

网络安全工作是指为保障学院信息化建设相关的基础设施、信息系统及数据的完整性、可用性及保密性，而采取的安全检测、防护、处置等技术措施，以及相关技术标准规范、管理制度的制定等。校园网络安全中涉及信息内容安全部分、涉密的信息安全等不在本办法管理范畴内，由学院相关部门根据相关规定进行管理。

**第三条** 凡学院范围内按照一定的应用目标和规划对信息进行采集、处理、存贮、传输和检索的校园网络终端均适用本管理办法。

第二章 管理架构

**第四条** 数字化校园建设与信息化领导小组为校园网络安全管理的领导机构，负责学院网络信息技术安全建设的战略决策、实施监督及重大网络信息技术安全事件处理的决策指导。

**第五条** 信息中心为校园网络安全的管理部门，负责学院网络信息技术安全的日常规划及保障、校园网安全建设与管理、网络信息技术安全管理制度的起草与执行以及其他与学院网络信息技术安全相关事务的处理。

**第六条** 各部门主要负责人为本部门网络安全第一责任人，并设置专职或兼职网络安全员，负责本单位内网络安全管理工作。

第三章 管理职责

**第七条** 学院校园网络安全管理工作实行责任制和责任追究制，按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则切实落实各系、各部门网络系统安全责任。

**第八条** 数字化校园建设与信息化领导小组负责对校园网的安全管理工作实行全面的领导、监督和检查。具体职责：

1．提出校园网安全管理工作的原则、任务和要求，制定工作计划，指导宣传教育。

2**．**拟订校园网安全管理工作的规章制度，组织审核校内各单位所制定的网络安全管理措施。

3**．**监督、检查各系、各部门校园网安全管理责任的落实情况。

4**．**组织学院有关职能部门对校园网安全事故的查处，协调校园网安全管理工作中的有关问题。

**第九条** 信息中心负责校园网的日常安全管理工作，落实安全保护技术措施，保障校园网的运行安全和信息安全，对各单位的网络安全工作小组提供网络安全维护方面的技术指导及培训。具体职责：

1**．**负责本单位的网络安全管理工作，制定符合本单位实际情况的实施细则，并建立健全网络安全管理的各项措施，对本单位的上网人员进行安全和保密教育。

2**．**做好本单位的安全及保密教育工作，做好用户信息的管理，保障数据与信息安全。

3**．**及时发布涉及网络及信息安全的通知公告，提供一定的系统安全保障方法及工具，并对各单位的网络安全工作小组的网络信息安全员提供网络安全维护方面的培训及技术指导。

4**．**开展学院各应用管理系统的培训工作，使用户及时掌握正确的使用方法，促进系统的推广实施。

5**．**协助相关部门查处利用校园网进行各种违纪、违法行为。

**第十条** 保卫处校园网安全职责：

1**．**协助相关部门做好校园网安全管理工作。

2**．**查处利用校园网进行的违纪、违法行为。

**第十一条** 各部门的网络安全管理工作接受学院校园网络安全管理小组的领导、监督和检查，应指定专人维护本单位的网络及信息安全。具体职责：

1**．**负责本单位的网络安全管理工作，制定符合本单位实际情况的实施细则，并建立健全网络安全管理的各项措施，对本单位的上网人员进行安全和保密教育。

2**．**负责本单位信息设备的物理安全、系统安全及数据安全，随时监控运行状态等，发现安全隐患和有害信息后，应及时将情况报告信息中心和保卫处。

3**．**负责本单位各类信息设备的管理与维护工作，定期进行系统升级或补丁操作，及时进行漏洞扫描，并在信息中心人员培训指导下做好系统安全及配置管理工作。

4**．**负责本单位各类信息系统、网站的开发、管理与维护工作，定期进行系统升级和信息更新，防止信息泄露和非法攻击。

5**．**负责学院各应用管理系统在本单位的推广与使用，配合学院有关部门开展系统培训，及时掌握系统使用方法及本单位系统维护方式。帮助本单位用户解决网络及计算机方面的日常使用问题。

6**．**协助有关部门查处利用校园网进行各种违法犯罪活动的案件。

第四章 校园网络安全建设与管理

**第十二条** 校园网及相关基础设施由信息中心统一规划、建设、管理，并提供全校统一网络出口，校内各单位及个人不得擅自建设、更改、损毁、挪用校园网设施，不得另外建立外网出口。

**第十三条** 校园网入网实行实名制，校内用户必须通过信息中心实名登记后方可按照入网要求使用校园网，未经登记不得以任何方式私接校园网，严禁盗用其他用户上网信息使用校园网。

**第十四条** 校园网主要服务于学院教学、科研及校务管理等，用户不得将校园网用于其他用途，严禁利用校园网开展各类未经许可的其它活动。

**第十五条** 校园网用户应文明上网，规范网络行为，并做好个人网络信息安全维护。校园网用户的上网行为不得危害到学院整体网络信息安全，严禁利用校园网从事任何无授权的探测、破坏、信息窃取等互联网攻击活动。

**第十六条** 校内各类信息系统原则上应依托于学院数据中心建设，使用学院域名并进行登记备案。未经审批备案的信息系统不属于学院官方行为，不得使用学院资金建设，不得使用校名、校徽等学院标识，一切责任由建设人员承担。

**第十七条** 校内各信息系统的用户认证必须使用学院统一身份认证，不得单独建立用户认证系统，不得单独采集用户个人信息。

**第十八条** 校内各信息系统应遵循学院信息化数据资产相关管理规定，采取必要的安全措施，确保数据安全。

**第十九条** 校园网信息系统的分类。

根据《教育行业信息安全等级保护定级工作指南》，校园网信息系统根据业务对象的不同可分为校务管理类、教学科研类、招生就业类和综合服务类。每一个大类细分为不同的子类。具体如下：

1**．**校务管理类。分为（1）办公与事务处理，（2）公文和信息交换，（3）人事管理，（4）财务管理，（5）资产管理，（6）后勤管理，（7）学生教育工作管理，（8）学生体质健康数据管理，（9）档案管理，（10）党务管理，（11）其他和校务管理相关的信息系统。

2**．**教学科研类。分为（1）教学改革管理，（2）学科与专业管理，（3）教务教学管理，（4）教学资源管理，（5）教学质量评估与保障，（6）科研管理，（7）科研情报，（8）其他与教学科研相关的信息系统。

3**．**招生就业类。分为（1）招生录取管理，（2）学生就业管理，（3）其他与招生就业相关的信息系统。

4**．**综合服务类。分为（1）门户网站，（2）论坛和社区类网站，（3）数字图书馆，（4）电子邮件，（5）视频服务，（6）安防监控，（7）校园一卡通，（8）内网门户与身份认证，（9）公共数据库，（10）运维管理，（11）其他。

**第二十条**  学院信息系统安全等级保护定级、备案及测评工作。

1**．**信息系统安全等级保护定级原则。凡是需提供Internet外网访问服务的学院信息系统，定级为二级及以上安全等级保护（以下简称“等保”）信息系统，必须符合二级及以上信息安全等保要求。仅向校内网络提供访问服务的信息系统，应参照一级或以上等级的信息安全等保要求运行及管理。

2**．**信息系统安全等保备案。按照国家信息系统等级保护制度的相关法律法规、标准规范要求，学院定期向上级主管部门备案学院信息系统安全等级保护定级情况。信息中心作为学院信息系统定级备案归口管理单位，落实上报备案工作，并接受校内二级单位自建自管信息系统的备案。

3**．**信息系统安全等保测评。原有列入校信息化专项建设的信息系统，其安全等保测评由学院统筹安排，并由项目承建单位配合学院落实第三方测评；新建的校信息化专项，应将信息系统的安全等保测评经费列入项目预算。自建自管信息系统的安全等保测评工作由二级单位委托信息中心进行第三方测评，测评发现的问题由本单位落实整改工作，测评和整改费用主要由二级单位承担。

**第二十一条** 服务器及信息系统网络开放范围。服务器或信息系统的网络开放范围将根据安全等保测评的情况而定，完成二级等保测评的信息系统，可以开放被Internet外网访问的权限。未完成二级等保测评的信息系统仅允许开放校内网络访问。学院原则上只有校中心机房内的服务器可开放被Internet外网访问。

**第二十二条** 二级单位自建自管信息系统的安全管理。设有自建自管服务器及信息系统的二级单位，须严格执行信息系统的分级安全保护措施，切实落实责任，建立本单位自建自管信息系统名录，规范建设、运维、使用等各个环节；要严格执行信息发布审核制度，避免保密信息外泄，防止在自管服务器及系统上制作、复制、发布、传播含有法律、法规禁止内容的信息，防止不正当地复制和利用学院具有知识产权的相关数据；要做好相关系统日志不低于60天的留存工作。

**第二十三条** 学院信息化建设项目应采用按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求、服务优良的软、硬件产品或服务厂商通过招标采购，不得由自然人承担信息化项目建设任务。

第五章 网络信息技术安全事件的处理

**第二十四条** 校内网络信息技术安全事件的处理由信息中心负责组织实施，按照学院网络信息技术安全事件处理流程（单独制定）进行分级、分类处理。为避免安全事件不良影响扩大，信息中心有权直接对安全事件相关的网络及信息系统进行断网、停止服务等应急处理。

**第二十五条** 信息中心负责组建校内网络信息技术安全应急响应组织，制定相应的应急响应流程、规范，并按照学院网络信息技术安全事件处理流程处理相关网络信息安全技术事件。

**第二十六条** 校内各单位应根据本单位信息化建设情况制定相应的监控与值守制度，发现网络信息安全问题应及时进行处理，并及时向信息中心报告。

**第二十七条** 网络信息技术安全事件处理后，由信息中心与相关部门共同进行责任认定，报数字化校园建设与信息化领导小组审议，根据安全事件的影响程度提交学院相关部门处理，情节严重的，学院将依法依规追究相关部门及个人的责任。

**第二十八条** 本规定自公布之日起生效，与本制度相关的原有规定同时终止执行，本制度解释权属于山东服装职业学院。