福州软件职业技术学院数据安全管理办法

为加强学校信息化数据的统一规划管理，建立有效的数据共建、共享、共工作机制，保证数据的完整性、规范性和一致性，为学校教学、科研、管理、服务以及持续发展提供准确、权威、及时、安全的数据与信息服务，根据《中华人民共和国计算机信息系统安全保护条例》、《信息安全等级保护管理办法》、《教育管理信息化建设与应用指南》等国家法律、法规，结合学校实际，特制定本办法。

第一章 总则

第一条 本办法中的数据是指学校各类信息系统所涉及的相关数据，包括各类应用系统中的业务数据、系统数据、教学资源、档案资料及用户服务支持系统中的相关数据。

第二条 本办法中的数据安全管理是指学校各项业务过程中与数据处理相关联的工作，包括与数据相关的标准规范、规章制度、工作流程的制定完善以及与数据采集、录入、运维、存储、应用等活动相关的其他事项。

第三条 数据安全管理原则

(一)统一标准原则。数据的格式及管理应符合国家、教育部、学校等制定的相关标准和规范。

(二)全程管控原则。建立数据从产生、处理、维护、应用的全面管控体系，重点加强数据质量、安全和使用等方面的管理。

(三)安全共享原则。在保证数据安全的前提下，实现数据与信息的共享、应用以及衍生服务，为学校发展提供决策支持。

第四条 数据安全管理目标

(一)保障数据完整准确：实行数据质量核查机制，保障数据在各个环节的规范性、完整性和准确性。

(二)保证数据安全可靠：建立数据的分级管理与备份、容灾机制;明确数据的所有权和管理权限，保证数据更改的可追溯;根据国家、教育部和学校的相关要求，做好数据保密工作。

(三)提升数据服务质量：全面提高数据质量和提升管理服务水平，充分发挥数据在学校发展中的重要战略作用。

第五条 根据学校业务划分，数据分类及数据所涉及部门如下：

(一)人力资源类：包括教职工基本信息、人员招聘、入职离校、职称评审、职务任免、考核管理、培训管理、薪资管理、党团工作、出国事务管理以及离退休等相关数据。主要涉及部门包括党委办公室、党委宣传部、学校办公室、教务科研处、人力资源部、财务处、后勤与资产管理处、图书馆、教学质量监控与评价中心、现代教育技术中心等。

(二)学生管理类：包括专科生、成教师资等所有与学生相关的基本信息，以及招生、迎新、学籍、奖惩、党团、毕业、就业和生活等相关数据。主要涉及部门包括各学院(系、

部)、党委宣传部、教务科研处、学生工作处（团委）、财务处、后勤与资产管理处、校友会、招生就业处、图书馆等。

(三)教学资源与管理类：包括专科生学籍、课程安排等教学管理，研究生学籍、培养计划制定等教学管理，教育教学资源等相关数据。主要涉及部门包括各学院(系、部)、教务科研处、图书馆等。

(四)科研管理类：包括科研项目管理、合同管理、成果管理、科研机构管理、科研经费管理等相关数据。主要涉及部门包括教务科研处、财务处、图书馆等。

(五)财务资产类：包括财务管理、经费管理、招投标管理、固定资产管理、实验室管理、设备管理、房产管理、土地管理等相关数据。主要涉及部门包括财务处、后勤与资产管理处等。

(六)数字档案类：包括人事档案管理、学生档案管理、文件档案管理、科研档案管理、教职工电子健康档案等相关数据。主要涉及部门包括党委办公室、学校办公室、图书馆等。

(七)公共服务类：包括新闻服务、电子邮件服务、校园网公共服务、电子图书服务、校园卡服务、医疗健康服务、校园安全治理等相关数据。主要涉及部门包括党委宣传部、财务处、安全保卫部、图书馆、现代教育技术中心等。

(八)系统数据类：主要指云数据中心相关技术参数，包括：网络出口参数、路由交换参数、数据库配置参数、安全

策略参数、应用系统安全配置数据等实现网络连接、操作系统管理、数据库管理、应用系统功能等相关数据。主要涉及部门包括现代教育技术中心等。

第二章 管理机构

第六条 现代教育技术中心负责信息化数据安全策略与规范的制定与执行，以及数据存储平台、数据交换平台、数据信息门户等公共基础平台的建设、运维和技术支持工作。

第七条 学校其他部门，本着“谁产生数据，谁负责管理”的原则，负责本部门数据的产生、维护、存储、归档和备份的全周期管理。各部门主要负责人为数据安全管理第一责任人。

第三章 数据产生

第八条 学校各部门作为数据产生单位，应遵照本办法，按照特定目标和业务过程产生数据，并统一纳入应用系统的管理。各部门应保证其数据的真实性、完整性和有效性。

(一)真实性：各部门的数据必须真实可靠，必须经过本部门数据管理第一责任人审核。

(二)完整性：各部门在进行系统操作时，必须按照规范要求录入全部数据项目，确保数据齐全，避免数据缺失，保证数据操作过程可追溯。

(三)时效性：各部门在规定的时间内按照数据规范进行采集，确保数据与实际业务同步，防止无效数据产生。

第九条 学校各部门须严格按照应用系统的使用规范实施数据的采集和录入。

第四章 数据运维

第十条 数据运维是指学校各部门在实际业务活动中，对其信息化数据所实施的日常补充、修正、更新和删除等操作。

第十一 条学校各部门须依照其业务数据运维的权限和职责，明确数据的修正、补充、更新、删除等操作流程的规定;未经本部门数据管理第一责任人授权不得越过应用系统直接对数据实施修正、补充、更新、删除等操作;须保存数据运维过程中所有相关的电子记录。

第五章 数据存储与归档

第十二条 学校各部门负责其应用系统业务数据的本地备份和归档，以及云数据中心数据的存储、备份、容灾和恢复等管理工作，保障数据的完整性和安全性。

第十三条 现代教育技术中心作为电子数据归档部门，负责数据归档及归档数据的查询、交换、复制和维护等管理工作，确保电子数据的有效归档和利用。

第六章 数据使用与服务

第十四条 学校各部门或个人在公开网站上或公开出版物上所展示的数据不得涉及学校内部信息或个人隐私信息，凡涉及学校内部信息的内容必须通过相关部门审核发布。

第十五条 学校各部门(或应用系统承建公司)在通过数据接口使用或共享其他部门数据时，需经相关部门审批后方可使用。

第十六条 各部门应避免使用无明确来源的数据。数据使用部门对于来源于校外或校内其他部门的数据，应在明确其来源的前提下进行引用和衍生，必要时可采取适当措施以保证其与原始数据的一致性。

第七章 数据安全

第十七条 数据安全是指数据处理系统的硬件、软件及数据本身受到保护，不受偶然的或恶意的原因而遭到破坏、更改和泄露。

第十八条 学校非涉密数据要求统一存放在学校的云数据中心存储介质上，数据维护由各部门自行负责。

第十九条 为保障数据安全，各部门的应用系统必须经现代教育技术中心技术检测合格后方可上线运行。

第二十条 现代教育技术中心负责根据应用系统等级保护评定的等级设置不同的安全防御策略。

第二十一条 各部门的信息系统管理员需要定期对数据安全进行检查，并做好检查记录。现代教育技术中心定期

组织专业网络安全公司实施系统安全检查，不符合相关安全防范要求的部门必须及时对其应用系统进行整改。

第二十二条 应用系统管理部门不但对产生的数据负有安全管理责任，而且对参与应用系统开发建设的企业负有安全管理和约束的责任。

第八章 奖惩

第二十三条 对于违反本办法有关规定，擅自泄露或篡改信息系统中的数据，且将数据信息用于申请用途以外的活动，并造成损失的部门或个人，视情节轻重给予相应处理。

第二十四条 对于有危害公共安全、国家安全、泄露国家秘密以及其他违反法律、法规和规章规定行为的，由公安、国家安全、保密以及其他监督管理等国家相关部门依法处理；涉嫌犯罪的，移送司法机关，依法追究刑事责任。