福建生物工程职业技术学院文件

闽生工院〔2024〕99号

福建生物工程职业技术学院关于印发数据安全管理办法（试行）的通知

各单位、各部门:

《福建生物工程职业技术学院数据安全管理办法（试行）》已经校长办公会研究通过，现印发给你们，请遵照执行。

福建生物工程职业技术学院

2024年11月22日

福建生物工程职业技术学院数据安全管理办法（试行）

第一章　总　则

第一条　为规范学校数据安全管理工作，保障个人信息和重要数据安全，维护广大师生和学校的合法权益，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》等相关法律法规和教育部等七部门《关于加强教育系统数据安全工作的通知》（教科信函〔2021〕20号）等文件要求，并结合学校实际，制定本办法。

第二条　本办法所指的数据是指学校各类信息系统所涉及的相关数据，包括各类信息系统中的业务数据、系统数据、教学资源、档案资料等相关数据。

第三条　本办法中的数据安全管理是指对上述第二条所涵盖的数据的采集、存储、共享、公开、使用过程以及安全保障等的全过程管理。涉及国家秘密信息的数据安全管理，按照国家相关法律和规定执行。

第四条　数据安全管理原则

（一）统筹管理，各负其责。学校数据的采集、存储、共享、公开、使用过程以及安全保障等工作要在学校统筹管理、统一标准的基础上，由各单位分头管理、各负其责。数据提供单位应确保数据真实性、准确性、完整性和及时性，数据使用单位应确保

数据使用合规，控制范围，保障安全。

（二）统一标准，一数一源。数据的格式及管理应符合国家、教育部、学校制定的相关标准和制度，保证在系统数据具备统一的数据标准；明确数据的权威来源，遵照“一数一源，一次采集，重复使用”原则。

（三）数据公有，授权共享。数据是学校公共资源，归学校公有。各单位在履行职责过程中各负其责，共同管理，在确保数据安全的前提下，实行以充分共享为原则，不共享为例外的授权共享机制。

（四）规范程序，保障安全。明确数据各环节的管理程序，建立全过程管控体系，做到学校数据管理全过程有规可依。依托国家信息安全保障体系，完善数据共享机制，保护个人隐私信息，保障数据资源安全。

第二章　管理职责与分工

第五条　学校网络安全和信息化领导小组负责数据安全管理工作的领导、组织、协调和重大问题的决策，研究制定学校数据安全管理工作发展规划，指导相关管理制度的制定。

第六条　网络安全与信息化中心负责信息化数据安全策略与规范的制定与执行；负责数据存储平台、数据交换平台、数据信息门户等公共基础平台（简称“数据中心”）的建设、运维和技术支持工作；牵头组织开展数据安全评估，全面保障学校的数

据安全。

第七条 学校各单位（部门）本着“谁产生数据，谁负责管理”的原则，负责各自分管领域数据的产生、维护、存储、归档和备份的全周期管理，并对使用其他部门的数据负相应安全职责。各单位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 学校各单位（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管理，保证其数据的真实性、完整性和有效性。

（一）真实性：各单位（部门）的数据必须真实可靠，必须经过本单位数据管理第一责任人审核。

（二）完整性：各单位（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：各单位（部门）在规定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 数据生产单位（部门）须遵循“一数一源”原则，严格按照应用系统的使用规范实施数据的采集和录入。

第十条 数据生产单位（部门）应明确数据录入人员的责任要求，按照“谁录入、谁负责”的原则，保证责任到人。

第十一条 学校各单位（部门）在变更其应用系统数据结构时，须提前向网络安全与信息化中心提交《应用系统数据结构变更备案表》（附件1），避免数据混乱及服务异常。

第四章 数据运维

第十二条 数据运维是指学校各单位（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。

第十三条 学校各单位（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；未经本单位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

第十四条 学校各单位（部门）负责其应用系统数据的本地存储、备份和归档，并按要求留存操作日志、访问日志等运行数据。

第十五条 网络安全与信息化中心负责数据中心上公共平台数据的存储、备份、容灾和恢复等管理工作，保障数据的完整性和安全性。

第六章 数据共享与使用

第十六条 本办法所称数据共享，是指学校各单位（部门）

间数据的共享，分为无条件共享、有条件共享和不予共享等三种类型。

（一）无条件共享：无条件共享数据是指在学校范围内，无需数据提供单位（部门）授权，可直接从数据共享交换平台提供给所有单位（部门）共享使用的数据资源。

（二）有条件共享：有条件共享数据是指在学校范围内，经数据提供单位（部门）授权或协议提供给数据使用单位（部门）共享使用的数据资源。

（三）不予共享：数据提供单位（部门）确定的不提供共享使用的数据资源。凡列入不予共享类的数据资源，须有学校文件或上级政策法规等依据。

第十七条 共享数据的产生单位（部门）应按照“谁主管、谁提供、谁负责”的原则，及时提供、维护和更新共享数据，保障数据的完整性、准确性，确保所提供的共享数据与本单位（部门）的数据一致。

第十八条 数据使用单位（部门）共享其他单位（部门）数据时，需办理数据使用申请，说明共享需求和用途，经数据提供单位（部门）审批后方可使用。

第十九条 数据使用单位（部门）使用共享数据应严格遵守数据保密规范，并保证数据用途与申请用途一致。数据使用单位（部门）对获取的共享数据有疑义或发现有明显错误的，应及时

反馈给数据生产单位（部门）予以校核。

第七章　数据安全

第二十条　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。

第二十一条　网络安全与信息化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，每季度组织专业网络安全公司实施系统安全检查。

第二十二条　各单位(部门)应遵循数据安全管理相关制度、规范，加强对数据采集、使用等相关工作人员的数据安全教育和培训，提高本单位（部门）人员数据安全意识和法制意识，切实落实安全管理责任。

第二十三条　为保障数据安全，各单位（部门）的应用系统向网络安全与信息化中心技术报备后方可上线运行。

第二十四条　各单位（部门）应加强服务器、存储等硬件设施的管理维护，结合实际，定期对本单位（部门）负责管理的数据资源、系统运行状况、备份数据进行检查，做好检查记录，防止因意外事件发生造成数据丢失、破坏。

第二十五条　各单位（部门）发生信息泄露、毁损、丢失等数据安全事件，或者发生数据安全事件风险明显加大时，应当立即采取补救措施，并按要求向网络安全与信息化中心报告。

第二十六条 应用系统管理单位(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。如果因业务开发对接需要,把数据接口密钥信息交给第三方时,必须与第三方签订数据安全保密协议。

第八章 附 则

第二十七条 对于违反本办法有关规定,擅自泄露或篡改应用系统中的数据,且将数据信息用于申请用途以外的活动,并造成损失的单位或个人,学校将视情节轻重给予相应处理。

第二十八条 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。

第二十九条 本办法由网络安全与信息化中心负责解释,自发布之日起试行。

附件

应用系统数据结构变更备案表

申请单位（部门）		系统管理员	
应用系统名称		系统版本	
变更描述 （变更缘由、目标等）			
数据表	字段	变更说明 （表/字段增、删、改、关联变更）	
经办人	签名: 日期:		
申请单位（部门）负责人意见	签名: 日期:		
网络安全与信息化中心审批意见	签名: 日期:		

福建生物工程职业技术学院党政办公室 2024 年 11 月 22 日印发