温州医科大学文件

温医大〔2021〕90号

温州医科大学关于印发
数据安全管理办法的通知

各部门、单位:

现将《温州医科大学数据安全管理办法》印发给你们，请遵照执行。

温州医科大学

2021年10月11日

温州医科大学数据安全管理办法

第一章 总 则

第一条 为规范学校通过信息化手段开展的数据活动，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《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术个人信息安全规范》（GB/T35273-2020）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，制定本办法。

第二条 本办法所指的数据包括学校各部门、单位在履行职能时，通过信息化手段获取的业务数据和统计数据，覆盖数据采集、存储传输、处理使用、共享开放等数据全生命周期活动。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。

第三条 本办法遵循一数一源、最小够用、分级保护、安全合规的原则，从管理和技术两个维度，重点保障个人信息安全和重要数据安全，全面提高校园数据安全保障能力。

第二章 工作职责

第四条 由信息技术中心负责统筹数据安全管理工作，制定数据安全管理制度，建立数据全生命周期的安全保障机制和监督检查机制。信息技术中心是数据安全的技术支撑单位，负责组织

开展数据安全评估，保障学校公共数据平台（以下简称数据中心）的运维安全。

第五条 信息技术中心会同学校办公室、发展规划处做好数据规划与管理工作，规范数据收集管理，统筹学校事业发展数据的安全保障工作。

第六条 各部门、单位对本部门、单位信息系统的数据安全负直接责任，要编制信息系统资源目录，提出数据分级建议，明确不同等级数据防护措施，保障数据安全。

第三章 数据分类分级

第七条 数据安全保障遵循分类分级保护的原则，基于数据重要性、敏感性确定数据等级，根据数据等级明确保护措施。

（一） 第一级数据：即公开数据，是指国家、教育行业、学校公开的数据标准、代码信息，以及学校主动公开和依申请公开的行政数据和业务数据。

（二） 第二级数据：即内部数据，是指不予公开，但可在一定范围内共享的数据，包括各部门、学院、附属医院和特定对象间共享的数据。按照职能收集并为公共服务、管理决策提供支撑的数据。

（三） 第三级数据：即敏感数据，是指一旦遭篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成严重损害的数据。

第八条 业务部门须根据分级要求确定数据等级，并报信息技术中心备案。确定为第三级数据的，经信息技术中心审核后，报网络技术安全和信息化工作领导小组(以下简称网信领导小组)审定。

第四章 数据收集的安全保障

第九条 各部门、单位须按照“一数一源”的原则，优先通过共享方式从学校数据中心获取数据。原则上不得重复收集数据。

第十条 各部门、单位利用信息系统收集数据应遵循最小化原则，并明确收集依据、范围、数量和用途。

第十一条 新建信息系统应在建设方案中明确数据收集内容和拟定数据等级，提供数据资源目录与表结构。信息技术中心对数据收集的必要性和数据等级的合理性进行审核。

第十二条 已建系统因升级改造或业务调整新增数据收集项目的，应及时更新数据资源目录与表结构，并反馈至信息技术中心。

第十三条 计划收集 100 万条以上个人信息的信息系统，报网信领导小组审核同意后方可实施。

第五章 数据存储传输的安全保障

第十四条 各部门、单位须明确数据存储和传输的安全策略，确保数据安全和系统稳定运行。

第十五条 数据原则上须存储在校内，第三级数据应保存在信息技术中心或学校指定的数据中心。所有数据不得保存至境外服务器。因业务原因确需保存至公有云端储存的，应事先开展安全评估并在通过国家云计算服务安全评估的公有云平台进行储存。

第十六条 在提供服务过程中，应综合利用师生个人生物识别信息（人脸、指纹等），不得使用人脸识别作为身份验证的唯一手段。

第六章 数据中心建设与安全保障

第十七条 数据中心主要包括支撑各类应用系统运行的中心数据库、代码标准、数据标准与质量管理、数据交换服务等。

第十八条 信息技术中心负责学校数据中心建设与安全管理、各信息系统业务数据库与数据中心的数据交换，以及业务数据的质量核检。

第十九条 各部门、单位应基于学校数据中心实施本部门信息化建设。在提交数据资源申请前，须签订《温州医科大学数据安全管理责任书》，申请的数据原则上只能用于业务系统对接使用，不得随意导出数据文件，确需查询导出的，须经部门领导同意并做好防毒防盗及保密工作，未经授权不得向第三方机构或个人提供所申请的数据。

第二十条 数据共享遵循“谁主管谁负责、谁审核谁负责、谁使用谁负责”的原则。

第二十一条 业务部门因开发对接需要，把数据接口密钥信息交给第三方时,必须与第三方签订学校提供的《数据保密协议》。

第二十二条 各部门、单位的网管员应认真履行职责，发现数据下发异常的情况，应及时与信息技术中心联系处理。

第二十三条 数据使用部门负责下发数据的管理，落实使用完毕的数据清理和销毁工作，对数据的安全、保密负责。

第二十四条 校内师生为其个人信息所有者，在学校信息化建设中，师生有权查询、更正、补充本人的个人信息，有权对信息化建设中违规处置个人信息的行为向数据源头部门进行反馈或向信息技术中心报告。

第二十五条 校内师生作为个人信息的所有者，应当及时更新信息化建设中使用到的个人信息,保证信息的准确性和完整性,并在信息化应用过程中妥善保管。由于师生个人原因造成个人信息泄露、损坏或丢失的，由本人承担相应责任；如对他人个人信息造成不良影响的，应追究相关责任人的责任。

第二十六条 业务主管部门原则上必须通过业务系统采集数据，不允许线下采集。业务主管部门应对采集的个人信息进行审核和及时更新，确保个人信息的准确性和完整性。师生个人信息如发生变更或采集的数据有误,可向业务主管部门提出更新申请,业务主管部门应及时更新个人信息。

第二十七条 业务主管部门采集到的个人信息，除存储在相关的业务系统数据库中，还应通过学校相关数据交换途径，交换到学校数据中心。

第二十八条 依照本办法获取的个人信息，经过匿名化、脱敏处理后无法识别特定个人且不能复原的，经过数据源部门审批后，可应用于学校的科学研究，研究成果归学校所有。

第二十九条 对于非学校信息化工作中的个人信息查询，原则上只接受公安部门和上级主管部门依法依规的查询请求。查询请求受理部门为数据源头部门,其他业务部门不得接受查询请求，也不得进行个人信息查询和提供个人信息数据。

第三十条 只有相关法律法规和学校制度有明确规定需要公开的个人信息，方可进行公开。公开个人信息遵循最小化原则，严禁超范围公开其他相关信息。个人敏感信息进行脱敏处理后方可公开。

第三十一条 注销的信息化项目或报废的存储设备，确保承载的信息数据被清理后，方可进行注销或报废处理。

第三十二条 各部门、单位因违反信息安全保密管理等规定，导致敏感信息泄露的,信息技术中心有权关闭相关数据接口权限。涉嫌违法犯罪的，移交司法机关处理。

第七章 数据安全监督管理

第三十三条 各部门、单位应积极配合网信领导小组、审计部门进行检查、审计，落实数据安全责任制度，规范数据管理，加强安全防范。

第三十四条 网信领导小组对发生重大数据安全事件报告处置不及时、不到位的部门、单位进行问责。构成违法和犯罪的，移交司法机关处理。

第八章 附 则

第三十五条 本办法自发文之日起施行，由信息技术中心负责解释。

温州医科大学办公室　　2021 年 10 月 11 日印发