浙江中医药大学办公室文件

浙中医大办〔2024〕19号

浙江中医药大学办公室关于印发数据安全管理办法的通知

各学院 、部门（单位）：

《浙江中医药大学数据安全管理办法》已经校长办公会议审议通过，现印发给你们，请遵照执行。

浙江中医药大学办公室

2024年3月19日

浙江中医药大学数据安全管理办法

第一章 总　则

第一条　为规范学校信息系统的数据处理活动，加强数据安全管理，保障数据安全，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》、教育部等七部门《关于加强教育系统数据安全工作的通知》、《公共数据安全体系建设指南》等文件要求，制定本办法。

第二条　本办法所指数据与《浙江中医药大学数据管理办法》所指数据范围一致。数据安全管理保障在数据收集、数据存储、数据传输、数据使用、数据销毁等数据全生命周期过程活动中的数据安全。

第三条　数据安全管理的基本原则是：

（一）最小够用原则。所有信息采集和使用必须在最小范围内进行。

（二）分类分级保护原则。按照数据类别和级别采取差异化安全保障措施，高安全级别数据从严保护，低安全级别数据适度保护。

（三）持续优化原则。持续迭代、动态优化，保障数据安全体系满足安全合规和业务发展的实际需要，促进数据的开发利用。

第二章 管理职责

第四条 学校网络与信息安全工作领导小组是学校数据安全管理工作的领导机构，负责学校数据安全管理的重大事项决策。学校信息公开工作领导小组是学校数据公开工作的领导机构，负责数据公开工作的重大事项决策。

第五条 数据安全管理部门设在信息技术中心，负责学校数据安全管理统筹规划与建设工作；负责学校数据安全制度的建设；负责学校数据安全管控平台和数据安全技术支撑能力的建设；负责建立数据全生命周期的安全保障机制和监督检查机制；负责组织、指导和督促各部门进行安全评估、安全培训、应急响应演练等工作。

第六条 各部门党政负责人是本部门数据安全工作第一责任人。各部门指定专人（以下称部门信息安全管理员）负责本部门数据资源全周期安全管理，落实本部门数据安全防护措施、监督数据公开过程、审核数据公开内容、监督数据销毁过程。数据生产部门根据一数一源原则，负责本部门源数据的分类分级和安全管理。数据使用部门负责被授权数据的安全管理。

第三章 数据分类分级管理

第七条 数据安全保障遵循分类分级保护的原则，按照主题、业务、领域等维度确定分类，按照数据重要性、敏感性、影响程度确定1级、2级、3级等三个分级。

1级：经评估后，可向社会公开或可被公众获知、使用的教育系统相关数据。

2级：数据一旦遭到篡改、破坏、泄露或非法获取、非法利

用，可能对社会稳定、公共利益、组织权益和个人权益造成轻微危害。可在学校内部、关联方使用。

3级：数据一旦遭到篡改、破坏、泄露或非法获取、非法利用，可能对组织、个人权益造成严重危害，或对社会稳定和公共利益造成一般或轻微危害，但不危害国家安全、经济运行。由各参与数据处理环节的单位内部人员访问，需满足相关约定条件并获得授权后可使用。

具体分类分级办法和对应保护措施参照《浙江中医药大学数据分类分级指南》。

第八条 数据分类分级结果在数据分类分级平台维护，并与数据资产管理平台联动。

第四章 数据收集的安全管理

第九条 各部门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；收集个人信息的，应有明确告知并征得个人同意。

第十条 新建信息系统应明确数据收集内容和拟定数据等级。数据安全管理部门核实后在数据分类分级平台更新数据定级内容。

第十一条 已建信息系统因升级改造或业务调整新增数据收集项目的，应明确数据收集内容和拟定数据等级，及时向数据安全管理部门报备。数据安全管理部门核实后在数据分类分级平台更新数据定级内容。

第五章 数据存储的安全管理

第十二条 数据原则上须存储在校内，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。

第十三条 密码信息禁止明文存储；2 级以上数据可根据实际需要对表、字段加密存储。

第十四条 信息系统应建立数据归档机制，定期将不活跃的数据转存到专门区域存储；应建立数据容灾备份机制，及时备份数据，并定期进行数据恢复演练。

第六章 数据传输的安全保障

第十五条 信息系统应保证数据传输内容的机密性、完整性和可用性。2 级以上数据须采用加密技术传输，避免被非法访问、窃听或篡改。

第十六条 信息系统应使用安全网络和安全传输协议，保障传输通道安全。特定领域数据须使用专网传输。

第十七条 信息系统应通过身份认证、访问列表、端口限制、黑白名单等措施，保障数据只传输给授权对象。

第七章 数据使用的安全保障

第十八条 各部门使用或共享其他部门数据，须通过规定流程审核。申请的数据只用于业务对接，不得提供给第三方机构或个人。

第十九条 各部门或个人在公开网站上或公开出版物上展示数据，须通过规定流程审核，对拟公开的数据进行脱敏处理，并受部门信息安全管理员监督。

第二十条　各部门提供给合作方的数据应进行脱敏处理；因业务原因确需提供原文的，应通过数据水印等技术手段，确保可数据溯源。

第二十一条　信息系统应综合利用个人生物识别信息（人脸、指纹等），不得使用人脸等生物特征作为身份验证的唯一手段。人脸等生物特征数据建议采用特征值传递，不得在终端保存人脸等生物特征数据，使用完毕时应及时删除。

第二十二条　视频数据只开放给授权部门和个人在线使用。因业务原因确需下载保存或提供给其他部门和个人的，应通过数据水印等技术手段，确保数据可溯源。

第二十三条　数据原则上应在境内保存和使用，因业务原因确需向境外提供的，应当按照国家有关法规进行安全评估，在数据出境前与接收方签订合同或者其他有法律效力的文件，并在合同中明确保障出境数据安全的内容。评估流程参照国家数据出境相关法律法规。

第八章 数据销毁的安全保障

第二十四条　废弃的信息系统或报废的存储设备，确保承载的信息数据被清理后，方可进行注销或报废处理。

第二十五条　存储 2 级以上数据的存储介质不再使用并且离开学校控制范围时，应及时销毁。数据销毁过程应进行日志记录，并受部门信息安全管理员监督。

第九章 数据安全运营管理

第二十六条　各部门应加强数据处理活动的安全风险监控

和告警，推进违规数据处理活动阻断技术措施建设，及时做好风险隐患的溯源排查处置。

第二十七条 各部门应保障与供应链合作过程的数据安全，具体要求参照《浙江中医药大学数据合作方安全管理规范》。

第二十八条 各部门应协同数据安全管理部门定期开展数据安全风险评估，形成风险评估报告。各部门应根据风险评估报告，及时落实数据安全自查和问题修复。

第二十九条 数据安全管理部门负责定期组织校内数据安全处置应急演练，相关部门应积极参与，通过演练提高校内数据安全事件处置能力。

第十章 数据安全管理监督

第三十条 数据安全事件的责任认定，由数据安全管理部门提交网络与信息安全工作领导小组讨论处理。

第三十一条 对违反本办法有关规定，非法收集、泄露、滥用、篡改数据，造成学校经济、名誉损失的，学校将视其情节轻重追究责任。涉及计算机信息犯罪的，依法移交公安机关。

第十一章 附 则

第三十二条 本办法由办公室和信息技术中心负责解释，自发布之日起实施。

抄送：各二级党组织。

浙江中医药大学办公室　　2024 年 3 月 20 日印发