中共天津科技大学委员会文件

津科大党发〔2023〕64号

关于印发《天津科技大学数据安全与个人信息保护管理办法（试行）》的通知

各基层党委（党总支）、各单位、机关各部门:

《天津科技大学数据安全与个人信息保护管理办法(试行)》已经2023年10月12日学校党委常委会第32次会议研究通过，现予印发，请遵照执行。

附件:天津科技大学数据安全与个人信息保护管理办法(试行)

中国共产党天津科技大学委员会

2023年10月22日

附件：

天津科技大学数据安全与个人信息保护管理办法（试行）

第一章 总则

第一条 为加强学校网络与信息安全，规范数据管理，保护学校重要数据和个人信息，切实维护广大师生的合法权益，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》等相关法律法规和政策规定，结合学校网络与信息安全工作实际，制定本办法。

第二条 本办法所指数据为学校产生的各类教育数据，包括学校、教职工、学生基础数据以及教育、教学、科研、管理产生的数据和常态数据。开展教育数据处理活动涉及保密以及涉及公共数据的政府信息公开的，依照《中华人民共和国保守国家秘密法》《中华人民共和国政府信息公开条例》等法律、法规的规定执行。本办法所指各单位包括学校各机关部、处、室，学院、直属单位、附属单位以及有关科研机构。

第三条 本办法遵循统筹审核、分级分类、最少够用、授权共享、安全管理的原则，从管理和技术两个维度，全面提高学校数据安全保障能力，并按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，建立健全数据安全责任体系。

第二章 管理机构与职责

第四条 网络安全和信息化领导小组（以下简称“领导小组”）是数据安全与个人信息保护工作的领导机构。主要职责是贯彻落实上级有关部门关于数据安全与个人信息保护工作的发展战略、宏观规划、重大政策和工作部署，统一领导、统一谋划、统一部署学校的数据安全与个人信息保护工作，统筹协调和决策学校数据安全与个人信息保护工作中的重大问题等。

第五条 网络安全和信息化办公室（简称“网信办”）是网络安全和信息化领导小组常设办事机构，主要负责组织落实领导小组的各项决议与工作部署，研究制定数据安全与个人信息保护工作发展规划、工作计划、规章制度和标准规范，建立覆盖数据采集、存储传输、处理使用、开放共享等全生命周期的数据安全保障和监督检查机制。组织开展数据资产梳理、分级分类、合规性评估、权限管理、安全审计、应急响应、教育培训等工作，统筹协调和落实数据安全管理相关工作。

第六条 各机关部、处、室，学院、直属单位、附属单位以及有关科研机构党政负责人是本单位数据安全与个人信息保护工作第一责任人，同时按照“谁收集，谁负责”、“谁使用，谁负责”、“谁发布、谁负责”的原则责任到人，落实本单位数据安全防护措施，保障数据安全。

第三章 数据分类分级

第七条 数据根据内容属性分为机构数据、人员数据和业务数据等三类。具体可细分为学生数据、教职工数据、教学数据、资产数据、科研数据、管理数据等。学校的数据安全保障遵循分级保护的原则。基于数据重要性、敏感性确定数据级别，根据数据级别明确保障措施。

第八条 根据数据泄露、滥用、篡改、破坏或者非法获取、非法利用、非法共享可能对国家安全、经济运行、社会稳定和公共利益、学校及个人利益造成的影响程度，将数据划分为四级，其中 1 级和 2 级数据对应一般数据，3 级数据对应重要数据，4 级数据对应核心数据。具体分级方法详见《天津科技大学数据分类分级管理办法（试行）》。

第九条 信息系统的使用单位根据《天津科技大学数据分类分级管理办法（试行）》对现有的数据进行分类分级。

第四章 数据采集

第十条 未经学校领导小组批准，校内任何单位和个人不得以任何理由，私自收集学校范围内的师生、聘用人员等个人信息；各单位未经单位负责人批准，任何人不得以任何理由，私自收集本单位师生、聘用人员等个人信息。

第十一条 数据采集应遵循最小够用原则，明确采集依据、范围、场景和用途，原则上不得超越各单位的工作职能采集数据。

第十二条 新建信息系统应在建设方案中明确数据采集内容和数据等级。由网信办和相关专家进行建设方案评审，对数据采集的必要性和数据分级的合理性进行审核。

第十三条 各单位对已建信息系统的数据采集项目建立信息资源目录，并报网信办备案，由网信办和相关专家进行审核，如有新增数据采集项目应及时更新报备信息。

第十四条 各单位按照“一数一源”的原则，优先由学校数据共享平台匹配需求，原则上数据共享平台中已有数据应通过共享的方式获取数据。

第十五条 各单位原则上不得采集学生、家长、教师的个人生物识别信息。采集敏感数据或采集五百以上个人数据需报网信办审核批准。

第五章 数据的存储与传输

第十六条 学校的敏感数据应保存在学校数据中心，禁止保存在校外数据中心（含云服务平台）；所有数据禁止保存在设置在境外的数据中心。

第十七条 各单位使用的信息系统应根据数据安全级别采用数据加密、访问控制、数据防泄漏等安全措施。个人信息数据应采用符合国家要求的密码算法进行加密存储。

第十八条 各单位使用的信息系统应制定数据备份恢复策略和操作规范。

第十九条 在线的敏感数据传输应采用加密传输信道或专

线，以保证数据传输的机密性和完整性；离线的敏感数据应加密后传输，且不得使用社会电子邮件系统、聊天平台等方式传递。

第二十条 根据国家有关数据出入境相关规定，核心数据和重要数据禁止出境；严格遵守“涉密信息不上网，上网信息不涉密”。

第六章 数据应用

第二十一条 学校鼓励在保障数据安全的前提下，充分发掘数据潜在价值。对数据开展统计分析、科学研究、决策分析时，需经业务职能部门同意，且确保不泄露敏感信息。敏感数据使用前应采用适当的脱敏技术进行脱敏处理。

第二十二条 信息系统使用单位应记录对业务数据的查询、修改、增加、删除、导出等操作日志，保留时间不少于六个月。

第七章 数据访问与共享

第二十三条 信息系统使用单位应实现数据管理、数据使用和数据审计的权限分离；数据管理人员负责分配数据使用权限、按最小化原则授予各级各类人员的相关权限；数据使用人员根据业务和权限需要使用数据；数据审计人员负责对各类人员的数据操作进行审计记录和分析。

第二十四条 根据数据分级分类和相关法规确定数据访问与共享权限。敏感数据的共享权限统一由网信办统筹负责分配。非敏感数据的共享权限由信息系统使用单位负责，自行决定是否共享。

第二十五条 数据信息不得用于商业用途。未经学校同意，

禁止与第三方共享。

第二十六条 信息发布或共享使用前必须先经过脱敏处理，所有涉及人员身份、联系方式、学生学籍、人事、金融、资产、招生、科研、档案等中含有敏感数据的应采用屏蔽、变形、替换等多种手段来满足不同的隐私数据匿名化的数据合规性。

第二十七条 根据“谁主管谁负责、谁批准谁负责、谁使用谁负责”的原则，信息系统的使用单位应明确本单位所采集数据的安全防护要求。数据共享审核单位负责与被共享单位通过协议等方式确定数据共享范围、用途和安全责任，并将安全防护要求告知被共享单位。被共享单位负责落实数据防护安全，保障数据不被窃取、滥用和篡改。

第二十八条 共享个人信息原则上通过接口方式实现，确需通过拷贝进行共享的，应报本单位领导同意，并由被共享方签订安全承诺书报网信办备案。

第八章 数据开放

第二十九条 学校应当依照政务数据开放目录，通过开放平台主动向社会开放政务数据，提供无偿服务。数据开放应当以企业、群众需求为导向，依法、安全、有序向公民、法人和其他组织开放。

第三十条 学校数据信息公开按照《中华人民共和国政府信息公开条例》有关规定执行，不得擅自向社会发布和公开所获取的教育数据。

第三十一条 学校信息披露前，应当依照《中华人民共和国保守国家秘密法》以及其他法律、法规和国家有关规定对拟公开的信息进行审查。按照信息披露三级审核流程操作，严格落实信息发布审核制度。

第九章 数据安全管理

第三十二条 数据的安全管理是指从管理和技术层面确保数据始终可用，保障数据安全的行为。

第三十三条 以“分类管理、分级应用"为基本思路，结合数据的共享开放价值和数据涉及公民及法人隐私程度等因素制定分类分级标准。学校参照标准，采用数据分类分级管理、备份、加密、防护等措施，加强对个人信息和核心数据保护，保护个人信息和重要数据免受泄露、窃取、篡改、毁损、非法使用等。

第三十四条 数据库是数据的存储系统，对数据库的攻击是获取数据最为直接的方式，数据库安全风险主要包括拖库、刷库、撞库等，各单位应根据信息系统安全等级和数据级别采用必要的数据库安全防护措施以保障数据库安全。

第三十五条 数据库系统原则上不应使用公网 IP 地址部署，如确需使用，应将具体情况说明上报网信办审核，采用公网部署的数据库系统必须采用高强度的安全防护措施以保障数据库安全。

第三十六条 各类系统平台应采用身份认证、访问控制等技术措施，防止未经授权的数据活动。各单位应指定专人负责数据库的安全管理，制定严格的数据库访问控制权限，采用高强度的

系统密码策略，检测数据库系统存在的安全问题，对数据库的安全状况进行持续化监控，保持数据库的安全健康状态。

第三十七条 数据库系统负责人应对数据库系统存在的安全漏洞进行及时修补，以降低数据库攻击风险；同时须定期对数据库访问行为进行审计，对出现的异常访问行为要及时排查和处置。

第十章 检查与监督

第三十八条 按照“谁发动采集、谁负责排查”、“谁共享数据、谁负责排查”的原则，各单位定期开展敏感数据和个人信息收集与对外共享情况排查工作，做到数据底数清、去向明。数据采集与对外共享过程中，需签署数据安全保密协议，对数据共享和使用范围做出严格界定。

第三十九条 各单位对于自查中发现的问题需要及时整改，认真做好整改落实工作，坚持做到事故原因不查清不放过、整改措施未落实不放过、责任人员未受到教育或处理不放过，尽力杜绝类似事件再次发生。

第四十条 各单位应向网信办提交本单位采集、使用数据的情况报告，切实承担起数据安全和个人信息保护的责任与义务，落实本单位数据安全保障措施，提升个人信息保护水平。

第四十一条 网信办负责学校数据安全和个人信息保护工作落实情况的监督检查，建立健全数据安全监督检查机制，联合相关单位定期组织开展学校数据安全风险评估检查工作，及时发现问题并督促相关部门进行整改。

第四十二条 网信办负责对数据安全检查情况进行全面总结，并报领导小组。

第十一章 保密管理

第四十三条 涉及国家秘密、国家安全、社会公共利益和个人隐私的教育数据，不得对外开放共享；确需对外开放的，要对利用目的、用户资质、保密条件等进行审查，并严格控制知悉范围。

第四十四条 涉及保密的教育数据的采集生产、加工整理、管理和使用，按照国家有关保密规定执行。

第十二章 责任追究

第四十五条 对违反本办法规定的行为，《中华人民共和国数据安全法》等法律、法规已经规定法律责任的，适用其规定。

第四十六条 违反本办法规定，有下列行为之一的，按照上级教育行政主管部门的要求限期改正；情节严重的，将线索转至纪检监察机关对直接负责的主管人员和其他直接责任人员依法给予处理：

（一）未按照规定做好教育数据的收集获取、目录编制、共享开放、更新维护和安全保障等工作；

（二）未按照规定进行数据汇聚、共享、开放；

（三）未依法履行教育数据安全管理相关职责；

（四）泄露、出售或者非法向他人提供履行职责过程中知悉的隐私、个人信息、商业秘密或者其他应当保密的数据；

（五）对发现的数据安全风险，拒不进行整改、核实、更正；

（六）未按照网络安全事件应急预案处置流程，进行应急响应，或出现瞒报、缓报、处置和整改不力等情况的；

（七）违反本办法规定的其他行为。

第十三章 附则

第四十二条 本办法自发布之日起施行，由网信办负责解释和修订。

天津科技大学办公室　　2023年10月22日印制