高校数据安全治理框架研究*

牛永亮[1]，朱江琳[2]
（1. 山西财经大学　网络与信息教育技术中心，山西　太原　030006；
2. 山西财经大学　文化旅游与新闻艺术学院，山西　太原　030006）

摘　要：高校数据安全治理对保障数据安全、促进数据有序流通与价值释放，进而支撑教育数智化转型具有重要意义。通过分析高校数据安全现状，对比数据安全治理与网络安全、数据治理的差异，结合教育行业特点及相关法规政策要求，提出以合法合规、统筹协调、共享共治和规范集约为基本原则，构建涵盖管理、技术与运维三个维度的数据安全治理框架；进一步从组织、制度、人才等管理体系建设，以及数据分类分级、全生命周期安全及典型应用场景等技术体系保障两个方面，提出具体可行的实施方案。最后，建议树立“数据与人并重”的安全发展理念，持续建设合规管理环境，逐步完善技术保障体系。

关键词：高校数据安全；治理框架；目标原则；分类分级
中图分类号：TP309. 2；G647　　**文献标志码：**A　　DOI：10. 19358/j. issn. 2097-1788. 2026. 06. 009

中文引用格式：牛永亮，朱江琳. 高校数据安全治理框架研究[J]. 网络安全与数据治理，2026，45(6)：66-74.
英文引用格式：Niu Yongliang，Zhu Jianglin. Research on university data security governance framework[J]. Cyber Security and Data Governance，2026，45(6)：66-74.

Research on university data security governance framework

Niu Yongliang[1]，Zhu Jianglin[2]
（1. Center of Network and Information Education Technology，Shanxi University of Finance and Economics，Taiyuan 030006，China；
2. School of Culture Tourism and Journalism Arts，Shanxi University of Finance and Economics，Taiyuan 030006，China）

Abstract：The governance of data security in higher education institutions is of great significance for ensuring data security，promoting orderly data circulation，and supporting the transformation of education digital intelligence. On the basis of analyzing the current situation of data security，comparing data security governance with network security，data governance，and combining the characteristics of the education industry and the requirements of relevant laws and policies，this paper proposes to build a data security governance framework covering three dimensions of management，technology and operation and maintenance based on the basic principles of legality and compliance，overall coordination，sharing and common governance，and standardization and intensification. Further，it is suggested to establish a management system from aspects such as organization，system，and talent，and build a technical guarantee system from aspects such as data classification and grading，full life cycle security，and typical application scenarios，to form a specific and feasible implementation plan. Finally，it is recommended to establish a security development concept that attaches equal importance to data and people，continuously build a compliant management environment，and gradually improve the technical guarantee system.

Key words：university data security；governance framework；goals and principles；classification and grading

0　引言

数据作为一种新型生产要素，正成为推动全域数字化转型和国家治理现代化的关键驱动力。然而，随着勒索病毒升级演进、数据泄露事件频发，数据安全问题已演变为关系国家、社会以及个人隐私安全的核心问题。当前，高校面临着数据安全意识薄弱，全生命周期安全管控缺失，数据分类分级标准模糊，数据共享与安全权责不明等严峻挑战。2023 年，江西某高校由于数据安全管理制度和技术保障措施不够完善，导致存储 3 000 余万条信息的数据库被入侵，其中 3 万

* 基金项目：山西财经大学 2025 年校级教学改革创新项目（2025331）

余条师生敏感数据在境外互联网被非法兜售[1]。2025年8月，河南某高校网站公示的新闻、通知及附件中存在未脱敏处理的身份证号等敏感信息，被公安部门及教育主管部门通报[2]。因此，开展高校数据安全治理研究，不仅能够完善教育行业数据安全治理理论体系，有效平衡数据安全与利用的双重需求，而且可以为教育行业数字化向数智化的高阶转型提供内生动力，对实现“安全可控、开放共享”的智慧教育生态具有重要实践意义。

近年来，我国数据安全治理体系建设已进入深化发展阶段。2021年，《中华人民共和国数据安全法》（以下简称《数据安全法》）《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）的相继实施，奠定了数据安全治理的法治基石。2024年，《网络数据安全管理条例》《GB/T 43697—2024 数据安全技术 数据分类分级规则》等政策、标准的出台，进一步细化了技术规范与操作指南，为构建科学化、精准化的数据安全治理体系提供了关键制度支撑。2025年，教育部等九部门联合印发《关于加快推进教育数字化的意见》再次强调全面落实教育数据全生命周期安全防护，强化核心和重要数据防篡改、防泄露、防滥用能力。这一系列政策演进既彰显了数据要素市场化配置与安全治理的制度创新，也反映了教育行业在数字化转型过程中对数据治理安全合规的迫切需求。

1 研究背景及高校数据安全现状

1.1 数据安全研究成果

目前，数据安全治理相关理论框架、治理实践、内容要素等研究工作已相继展开，并取得了丰富的研究成果，主要集中在以下方面。

一是数据安全治理相关概念、理念及实践指南研究。在国外，2010年微软提出隐私、保密和合规性的数据治理计划，2015年Gartner提出数据安全治理理念[3]。两者均基于方法论视角从宏观层面描述了数据安全治理的基本思路和框架。在国内，中关村网信联盟、中国信息通信研究院分别持续发布《数据安全治理白皮书》（1.0~6.0）[4]、《数据安全治理实践指南》（1.0~4.0）[5]，两者通过研究数据安全形势、制度与政策标准，提出相应的实践路线。这些研究为理解数据安全治理概念、理论及行业实践提供了重要参考。

二是多重视角下的数据安全治理框架研究。黄科满[6]等从数据社会化视角，提出“技术-产业-标准-政策-实践”五位一体的数据流通安全治理框架。王健[7]等提出基于规则的数据安全治理框架，旨在平衡数据治理过程中“保护”和“利用”的失衡现象。李晓东[8]等在总体国家安全观视域下为数据安全治理进行价值定位并探索治理路径。马海群[9]、张涛[10]、梅傲[11]等分别从国际视野研究了美、英、日的数据安全治理体系。

三是不同行业视角下的数据安全治理研究。饶圆[12]等讨论了档案数据安全治理模型及优化路径；陈立吾[13]针对金融行业提出数据安全治理策略；梅振荣[14]等从法理思想维度对智慧图书馆的数据开放和安全治理平衡进行了研究。

四是对数据安全治理内容要素的研究。胡新瑞[15]对数据分类分级保护制度进行了研究；韩钢[16]等从全生命周期视角对数据安全治理进行研究和探讨；郭德香[17]对出境场景下数据面临的安全困境进行分析，提出相应治理对策。

综上，现有理论框架、不同视角的审视以及多层次要素研究，为深刻理解数据安全治理提供了重要基础。然而，针对高校开展数据安全治理的理论研究和实践探讨相对较少。鉴于此，本文深入探讨高校数据安全治理面临的问题，厘清其与网络安全、数据治理的差异，从管理、技术、运维角度尝试构建高校数据安全治理框架，以期为教育行业数据安全治理和数智化转型提供有益的理论参考和实践借鉴。

1.2 高校数据安全现状

随着教育信息化2.0的推进，高校在教学、科研和管理等多场景中积累了海量数据，这些数据不仅是数字化转型的核心动能，也是推动教育数智化高质量发展的关键要素。近年来，高校通过数据治理逐步建立了标准化体系，提升了数据质量、共享效率和整体管理效能。然而，相较于数据治理的快速进展，数据安全体系建设仍显滞后，依赖传统的“区域隔离、边界防护和入侵阻断”网络安全逻辑，难以有效应对数据高汇聚性、动态流动性及应用场景复杂性等带来的新安全挑战。

（1）数据汇聚风险。大规模数据集中存储在提升利用价值的同时，也显著增加了安全风险。一方面，整合各业务系统数据资源并构建“数据资源湖”，虽有助于推进数据标准化与按需共享，但也使其易成为高价值攻击目标。另一方面，原本价值密度较低、敏感性较弱的离散数据，经过关联分析可能生成新的高价值资产。例如，汇聚教学行为、科研活动、消费记

录与健康数据等多源信息并进行关联分析，可形成“师生全景画像”。此类高价值敏感数据若未能实施有效的分类分级管理与精准管控，其利用过程不仅涉及隐私泄露问题，还可能引发关乎教育公平的伦理风险。

（2）数据流动性风险。与传统资产不同，数据资产的核心特征在于其流动性。数据在组织内部的高效流动与共享利用，虽能实现价值倍增与效率提升，但也突破了传统安全防护边界。其多节点、多路径的流动特性，使得诸如篡改、泄露和滥用等安全风险在采集、传输、存储等全生命周期持续扩散，致使基于静态防护逻辑的传统网络安全体系难以有效应对。如师生个人数据在流动过程中，从收集时需获“明示同意”，到敏感身份数据的加密传输与存储，再到校内跨平台多终端的可视化展示及校外第三方公司运维，其风险囊括了终端物理安全、网络传输安全以及数据本身的泄漏、篡改与勒索威胁。

（3）应用场景的复杂性带来数据“共享”与“安全”相悖困境。基于“一数一源、一源多用”构建的网状数据拓扑结构，有效支撑了校园多场景应用，但随之也衍生出安全治理困境。一方面，管理授权面临“开放—管控”两难，过度限制将抑制数据要素流动效率，而权限泛化则可能诱发滥用风险。另一方面，在数据共享使用环节，由于安全意识薄弱、数据标识体系缺失、流动数据的多副本特性和传播路径复杂性，使得数据安全事件溯源困难。如师生人脸识别数据应用于门禁、支付等多个场景，若使用审批不严、角色权限划分粗放，将导致数据安全责任主体难以落实，安全问题发生时更无法有效溯源。

数据安全治理如若失效，将会形成“数据流通阻滞—价值转化受阻—共享意愿衰减”的负反馈循环，最终制约数据要素的价值释放。因此，在安全合规前提下，高校应构建多部门协调参与、安全权责清晰、数据保护分类分级明确、覆盖全生命周期、适用校园场景的数据安全治理体系，形成共建、共治、共享的数据安全治理格局。

2 高校数据安全治理概念及框架设计

2.1 相关概念辨析

2.1.1 网络安全与数据安全治理

近年来，数据安全事件层出不穷，调查表明除黑客攻击因素外，70%以上的数据泄露安全事件是由组织内部（离职）人员的失误或故意造成的[18]。显然，数据安全治理与传统网络安全在实现目标、保护对象及防护理念等方面存在较为明显的差异（见表1）。

表1 传统网络安全与数据安全治理差异（部分）

	传统网络安全	数据安全治理
实现目标	保护内部对象不受黑客的入侵、破坏	数据的安全使用
主要保护对象	组织内的终端设备、信息系统、数据等	组织内不易公开的重要、核心、敏感数据
主要防范对象	黑客、恶意程序等	内部（离职）人员及其对数据的相关操作
防护理念	划分安全区域、建立边界防护	建立数据分类分级体系，确保数据全生命周期安全
技术与管理的密切程度	相对分离	深度整合

虽然两者之间存在差异，但数据的采集、传输、存储、共享等环节仍需要网络载体来实现自身价值。因此，数据安全治理应在网络安全的基础上，通过管理与技术的弥补和深度整合，实现数据的安全管控。

2.1.2 数据治理与数据安全治理

在《信息技术 大数据 数据治理实施指南》中，数据治理定义为对数据资源管理行使权力和控制的活动集合[19]。作为其核心子集，数据安全治理的核心在于通过系统性、多维度的安全防护措施，最终实现数据的安全利用。两者之间的最终目标相同，但在主导部门、核心对象及产出结果上存在差异（见表2）。

表2 数据治理与数据安全治理异同（部分）

	数据治理	数据安全治理
主导部门	IT技术部门	安全管理部门
核心对象	“数据”	“人”和“数据”
目标	提升数据质量，发挥资产价值	数据使用更安全
最终产出	通过数据资产梳理、清洗，建立数据规范，形成组织内部的元数据和“数据湖”	摸清重要、核心、敏感数据的状况，建立数据的分类分级目录，并制定相应安全策略

2.2 高校数据安全治理的定义

数据安全治理概念由Gartner于2015年提出并逐步完善，其不仅仅是一套产品级解决方案，更是贯穿组织决策层至技术层、涵盖管理制度与支撑工具的完整体系[20]。《数据安全治理白皮书5.0》进一步指出数据安全须具备动态性和持续性，而“治理”不仅为

一整套规则条例，更是一系列协调活动的集合[21]。综上，数据安全治理是一套目标明确、持续动态且须多方协调的系统化治理过程。

相应地，高校数据安全治理是在学校顶层安全战略的指引下，以国家法规和教育行业标准为遵循，以自身发展的内生需求为出发点，通过系统构建管理制度、技术工具与运维规范，所形成的“全局管控、标准统一、动态更新”的一体化治理体系，确保数据安全合规使用，从而为高校数字化转型与智慧校园建设提供核心支撑。

2.3 高校数据安全治理框架

2.3.1 基本原则

（1）合法合规原则。高校数据安全治理应遵循《网络安全法》《数据安全法》《个人信息保护法》等国家法律法规、相关标准及教育行业要求（见表3）。在合法合规基础上，应完善顶层设计，构建包含数据分类分级、全生命周期安全防护、重要数据备份与加密等在内的制度体系。

（2）统筹协调原则。高校应坚持开发利用与安全保护并重，在释放数据价值的同时强化安全管控，通过加强组织领导，破除部门间壁垒，建立以界定数据权属、规范流通共享、落实安全责任为核心的协调机制，并以此为基础推进数据安全治理。

（3）共享共治原则。为高效释放数据价值，高校应在健全分类分级标准的基础上推动共享共治。参照《数据安全技术 数据分类分级规则》，高校数据大多属于“一般数据”，其安全风险相对可控。因而可以建立较为灵活的安全共享机制，在保障安全的前提下最大化数据利用效能。

（4）规范集约原则。针对经费有限的现实约束，高校应强调集约化建设。通过复用现有数据治理与安全防护基础、统筹调配设备资源、调优数据安全策略，畅通数据共享渠道，避免重复投入，从而构建经济、可靠、高效的数据安全体系。

表3 我国法律法规、标准及行业要求中关于“数据安全”相关内容

实施时间	名称	颁发机构	数据安全相关内容
2017-6-1	《网络安全法》	第十二届全国人民代表大会常务委员会第二十四次会议	首次提出“数据分类”“重要数据”相关概念，要求采取数据分类、重要数据备份加密等措施，防止网络数据泄露或篡改
2021-4-6	《教育部等七部门关于加强教育系统数据安全工作的通知》	教育部、中央网信办、最高人民法院、最高人民检察院、工业和信息化部、公安部、市场监管总局	按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，健全数据安全责任体系；建立教育系统数据分类分级制度，健全全生命周期的数据安全保障制度，重点保障个人信息安全
2021-9-1	《数据安全法》	第十三届全国人民代表大会常务委员会第二十九次会议	要求建立健全数据安全治理体系，提高数据安全保障能力；提出国家建立数据分类分级保护制度；确定重要数据具体目录，并进行重点保护
2021-11-1	《个人信息保护法》	第十三届全国人民代表大会常务委员会第三十次会议	确认个人信息知情权、决定权、查阅权、复制权、更正权、补充权、删除权；加强生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息的保护，处理此类信息应当取得个人的单独同意
2024-10-1	《数据安全技术 数据分类分级规则》	国家市场监督管理总局、国家标准化管理委员会	按照科学实用、边界清晰、就高从严、点面结合、动态更新的原则实现数据分类分级，并给出数据分类、分级规则以及参考流程
2025-5-1	《个人信息保护合规审计管理办法》	国家互联网信息办公室第18号令	处理100万人以上个人信息的处理者应当指定保护负责人，负责个人信息保护合规审计工作；处理超过1 000万人个人信息的个人信息处理者，应当每两年至少开展一次个人信息保护合规审计
2025-6-1	《人脸识别技术应用安全管理办法》	国家互联网信息办公室、中华人民共和国公安部	明确应用人脸识别技术处理人脸信息的基本要求及处理规则；个人信息处理者应当履行告知、影响评估等义务；应当取得个人在充分知情的前提下自愿、明确作出的单独同意，个人有权撤回同意；人脸信息存储数量达到10万人之日起30个工作日内应向所在地省级以上网信部门备案

2. 3. 2 框架设计

高校数据安全治理的框架设计应综合考虑校情实际，遵循合法合规、统筹协调、共享共治、规范集约原则，以“数据”和“人”为治理核心，通过构建管理、技术、运营三维安全体系，实现数据安全、有序、高效使用。其中数据安全管理是开展治理工作的基础和先导；数据安全技术是保障全生命周期数据安全的重要工具支撑；数据安全运营是实现数据要素持续安全高效、进行价值转化的重要保障。框架设计如图 1 所示。

3 高校数据安全管理体系建设

3. 1 组织管理

高校数据安全组织架构应基于现有体系，以保障“数据安全使用”为目标，面向具体业务场景，协调相关部门成立统筹全局的数据安全治理机构。该机构通常由高校领导班子主要负责人担任第一责任人，首席网络与数据安全官作为直接责任人，下设决策、管理、监督与执行机构（见表 4）。在此基础上，进一步合理定岗、定责、定员，构建权责清晰的工作体系，确保治理要求有效落地。

图 1 高校数据安全治理的框架设计

表 4 高校数据安全组织架构

功能划分	人员组成	相关职责
决策层	由分管网络和数据安全的校长、相关部门负责人组成数据安全治理委员会	制定数据安全战略、规划和评价考核政策，统筹各类资源调配
管理层	由主抓安全和数据管理的部门负责人及技术团队成立相应的办公室	制定数据安全制度；设立数据管理员、审计员和安全员等岗位；开展人员培训、安全风险评估、应急演练及事件处置
监督层	数据资产、安全、人事等相关部门成员	对数据安全落实情况开展督查与审计，发现影响数据共享与安全的不合理因素，完善安全监测、预警、通报和综合评价体系
执行层	部门数据管理员以及运维团队	承担本级数据安全与保密责任，建立本级数据分类目录，落实数据安全规章制度，确保业务范畴内的数据全生命周期安全管理

3.2 管理制度及标准

结合学校数据安全风险现状和重要、敏感数据防护需求，高校应准确定义数据安全管理内容和技术规范，明确数据安全工作职责，健全数据安全制度和标准，使数据安全工作有章可依，责任落实到人，为可持续化的数据安全治理能力提供支撑，见表5。

表5 高校数据安全管理制度、标准示例

类别		名称
制度流程	管理政策	《数据安全治理办法》
	管理规范	《数据资产管理办法》
		《数据分类分级管理办法》
		《数据全生命周期安全管理办法》
		《数据安全评估管理办法》
		《数据安全事件应急响应与处置预案》
		《供应链管理办法》
	操作规程、手册	《数据分类分级操作规程》
		《敏感数据操作规程》
		《数据存储介质管理规程》
	申请表单、审批报告	《数据分类分级清单》
		《数据资产使用审批表》
		《数据共享与使用保密协议》
标准	数据安全技术标准	《数据分类分级标准》
		《数据共享接口标准》
		《数据脱敏技术标准》

3.3 人员培训

数据安全组织建立后，需要定岗定员。依据数据安全要素进行专业化分工，赋予完成岗位职责的最小权限，并对重要岗位人员开展背景审查。

加强人才的培养及培训是数据安全治理的重要举措。学校应结合业务场景、安全操作规范以及现实案例，针对不同岗位角色开展周期性数据安全培训及考核，稳步提升员工安全意识和操作技能。

4 高校数据安全技术体系建设

4.1 数据分类分级

高校数据分类分级应结合校情，参考《数据安全技术 数据分类分级规则》，遵循边界清晰、就高从严、动态扩展、稳定可执行与易于维护等原则，采用工具发现自动化与人工审核的方式，对数据资产进行梳理、识别、标注，最终形成统一的数据分类分级目录。通过明确数据分类分级标准，不仅能对不同类型的数据进行差异化保护，也可为后续开展数据安全风险评估、制定安全策略、实施权限管控提供重要依据。

4.1.1 数据分类

应结合教育行业属性、高校业务特点以及数据使用与管理的实际需求对高校数据细化分类。高校不仅承担社会服务职能，更聚焦于教学、科研、管理等核心业务发展，并密切关注师生群体的切身利益。鉴于个人信息受《个人信息保护法》《信息安全技术 人脸识别数据安全要求》等法律法规与标准的专门保护，本文将此类数据单独列为一类。据此，高校数据可分为机构数据、业务数据、人员数据与其他数据四类。其中机构数据是指高校在经营管理过程中收集或产生的，用于向社会提供公共服务的数据；业务数据是指校内教学、科研等业务部门在履行职能或开展业务活动中收集、产生的数据；人员数据是指高校所收集、产生的能够表征或描述自然人特征及活动情况的数据；其他数据是指不属于以上类别的数据。

4.1.2 数据分级

高校数据分级应综合考量数据对社会经济发展的重要程度、遭破坏后可能产生的危害后果以及数据量级等因素进行细化。在多数情况下，高校数据若发生泄露、篡改、毁损或非法使用，通常不会对国家安全或公共利益构成严重危害，但可能对个人或学校权益造成较大影响，或对社会秩序、公共利益带来一般性乃至轻微危害；且所处理的个人信息数量一般低于100万条。依据《数据安全技术 数据分类分级规则》与《个人信息保护合规审计管理办法》[22]，高校数据整体上可归类为“一般数据”。在此基础上，根据数据重要程度与影响范围由低至高，进一步划分为公开级、内部级和敏感级三个级别（见表6）。

随着高校业务活动的拓展，数据分类分级展现出动态变化的特征。在明确分类分级标准后，校内各业务部门应依据权属关系，建立并完善本单位及学校整体的数据分类分级目录（见表7）。若发现原有分级无法满足实际安全管理需求，应及时重新定级。

数据分类分级目录的建立，有助于摸清数据资产安全底数，为后续开展风险评估、制定安全策略和实施差异化保护提供基础。具体而言，可对重要敏感数据探测与定位；根据数据访问情况，评估账号权限设置是否合理；对数据存储环境进行评估，排查是否存在漏洞、数据备份与恢复机制是否完备等。基于风险评估结果，可灵活制定数据安全策略，避免“一刀切”的保护方式，从而降低合规成本，提升数据价值开发利用的效率。

表 6　高校数据分级定义示例

安全等级	定义	保护措施
公开级	数据遭破坏后，仅对个人权益、组织权益造成一般危害或无危害，如教育行业公开的学校代码信息、学校网站主动公开的新闻和业务数据	完全公开共享
内部级	数据遭破坏后，对个人权益、组织权益造成严重危害，如教学、科研、管理等业务处理过程中收集、产生的数据	不予公开，校内有条件共享
敏感级	数据遭破坏后，对个人权益、组织权益造成特别严重危害或者对经济运行、社会秩序、公共利益造成一般危害，如个人敏感数据	不予公开、共享，获得授权后可使用

表 7　高校数据分类分级示例

一级分类	二级分类	三级分类	示例	分级建议
机构数据	基础数据	学校概况	学校标识码、学校名称、地址、社会信用代码等	公开级
		机构设置	部门名称、部门职责、内设机构、办事流程等	公开级
		办学条件	占地面积、藏书数量等	公开级
	学科数据	学科基本数据	学科门类数据、硕士/博士点数据等	公开级
	招生就业数据	招生就业基本数据	招生专业目录、招生/就业政策等	公开级
业务数据	教学数据	教学基础数据	教室数据、教材数据、专业培养数据等	内部级
		教学活动数据	教学计划数据、排课数据、实训管理数据等	内部级
		教学质量与评价数据	课程名称、任课教师、课程质量评价等	内部级
		教学成果数据	教学成果、教改项目、完成人及角色等	内部级
	科研数据	科研项目数据	项目编号、项目名称、经费来源等	内部级
		科研机构数据	科研机构名称、重点实验室、机构人员等	内部级
		科研成果数据	成果类型、成果名称、项目来源、奖励等级等	内部级
	管理支撑数据	综合办公数据	公文数据、会议数据等	内部级
		财务资产数据	预算/决算数据、财务管理数据、资产数据、审计数据	内部级
		组织人事数据	干部管理数据、人员培训数据等	内部级
		档案管理数据	档案基本数据、档案查阅数据等	敏感级
		信息化建设数据	信息系统建设数据、系统运维管理数据等	内部级
人员数据	教职工	基本信息	姓名、工号、性别、学历、工作部门等	公开级
		个人成长数据	担任职务、任课信息、科研信息等	内部级
		敏感数据	奖惩信息、工资数据、健康数据、身份识别数据等	敏感级
	学生	基本信息	姓名、学号、性别等	公开级
		个人成长数据	院系、实践活动数据等	内部级
		敏感数据	奖惩、资助、成绩、家庭成员、健康、身份识别等数据	敏感级
其他数据	其他数据	其他数据	其他数据	依情分级

4.2　数据全生命周期安全保障

数据全生命周期安全保障是在数据采集、传输、存储、处理、共享及销毁等环节中，系统实施风险评估，识别存在的脆弱性与外部威胁，并制定相应的防护措施与应急策略。通过持续迭代，最终构建数据安全闭环，推动安全策略的不断优化，见图 2。

（1）数据采集。数据采集是指业务系统新产生或通过教育行业系统接收到新的数据。该阶段应坚持“合法、正当、必要”原则，明确采集目的、处理方式、采集范围和相应规则。对于敏感数据还应明确告知采集对象并获得授权同意，及时进行分类分级标记，做好个人隐私保护。

（2）数据传输。数据传输指数据在校内业务系统之间或业务系统到应用终端之间传输的过程。该阶段应采取必要的通道加密、内容加密、传输终端身份鉴别、传输链路冗余等方式，确保数据安全传输。

（3）数据存储。数据存储指数据以数字格式进行存储。该阶段应对敏感数据进行加密存储，对于数据存储介质的访问行为应进行身份认证并进行审计，同时做好数据备份与恢复策略。

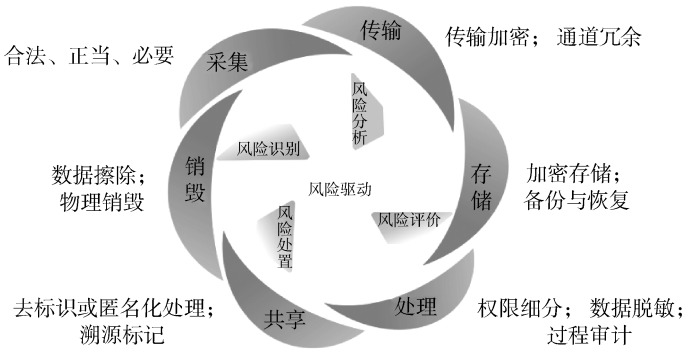

图 2　数据全生命周期安全风险驱动示意图

（4）数据处理。对数据进行整合、分析、可视化等操作的阶段。该阶段应采用数据脱敏、算法模型审核、操作过程审计等技术手段细化角色权限、完善身份鉴别。针对个人信息的必要公开展示，敏感数据应脱敏处理；对于业务处理衍生数据、汇聚数据应进行分类分级标记，若安全级别发生变化应及时动态调整。

（5）数据共享。数据共享是校内信息系统之间或与第三方进行数据交换、共享的阶段。该阶段应对交换接口进行安全检查，设置访问策略，对敏感数据进行去标识和匿名化处理，并进行溯源标记。

（6）数据销毁。数据销毁是指对超时限数据、存储介质进行彻底销毁且无法恢复的阶段。高校应根据国家和行业规定，对超时限数据进行删除或匿名化处理；对敏感数据及其存储介质进行数据擦除或物理销毁，并验证销毁效果。

高校应定期通过运用技术手段、问卷调研、人员谈话、运维日志审计等方式对数据安全现状进行评估，重点识别账号口令、角色权限、安全策略、加密字段、系统漏洞等方面存在的脆弱性与外部威胁（详见表 8）。

4.3　基于应用场景的数据安全

随着数据要素价值的凸显与业务需求的拓展，高校数据应用场景呈现出多样化发展趋势，“一刀切”的数据防护模式已难以适应不同应用场景下的差异化安全需求。为此应系统梳理数据业务，识别关键应用场景，并制定针对性的安全策略。常见应用场景有：

（1）数据云端部署。由于成本与运维压力，高校常将部分数据部署于云端以提供公共查询服务，如招生就业、迎新预报到等面向公众的智能应答业务。然而，云环境中更易面临攻击威胁。因此，云端部署的数据应限定为公开数据或经匿名化处理的数据，并加强数据传输链路、身份鉴别与数据水印技术等方面的防护，以防范数据盗取、个人隐私泄露及恶意数据投毒等风险。

（2）数据第三方共享。高校在与第三方机构共享数据时，虽会签订安全协议，但仅凭书面合同难以全面约束、监测第三方的数据处理行为。在此类场景中，应强化数据共享的审批流程，积极采用数据水印与溯源技术，以便在数据泄露时能够及时追溯并落实责任。

（3）数据库运维。数据安全治理不仅需要防范外部攻击，也应重视组织内部使用安全，特别是数据库运维过程中的潜在风险。据统计，由内部人员引发的数据安全事件往往代价更高且更难察觉。因此，运维操作应事前实施严格的身份鉴别与细粒度的权限控制；事中规范内部人员的数据访问与操作行为，对敏感数据采取加密与权限管控措施；事后应建立有效的追溯

表 8　数据生命周期常见脆弱点和外部威胁（部分）

阶段名称	脆弱点	外部威胁	应对措施	
采集	过度采集；未获用户明示同意；终端设备未进行安全设置	钓鱼攻击、勒索攻击	加强采集终端安全防护	加强制度约束和督查；周期性技能、管理能力培训；建立数据安全应急预案，定期进行演练
传输	敏感数据明文传输；传输链路冗余不足	网络监听	传输链路冗余，加密传输	
存储	未进行存储介质管控；缺乏备份恢复机制；敏感数据未加密存储	数据拖库；内部人员恶意下载、泄露数据	账号权限跟踪；敏感数据加密与隔离；禁用弱口令；修复数据库漏洞	
处理	敏感数据公开未脱敏；角色权限未细分	数据库敏感操作频繁；数据恶意爬取	异常行为发现与禁止；建立权限基线；操作合规审计；业务层动态脱敏	
共享	接口未进行安全检测；敏感数据未脱敏；共享数据未加水印	敏感数据非法交易；数据接收方未采取数据防护措施	数据分发审核；数据溯源跟踪	
销毁	销毁的数据可以恢复；师生个人敏感数据未按规定删除	数据恶意恢复	物理销毁、监督和审查	

与审计机制，以保障全程可监督、可回溯。

5 高校数据安全治理的建议

数据要素已成为推动高校信息化建设的关键驱动力，其安全治理已愈发迫切。为此，高校应建设以“数据+人”为中心的安全治理体系，不断完善数据管理机制建设，构建数据全生命周期安全技术体系和运营规范，赋能高校数字化治理和高质量发展。

（1）建立“数据+人”为中心的安全发展理念。传统依赖边界防护的安全模式，难以管控数据流通风险，也制约了数据在不完全可信环境下的有效利用。因此，高校必须建立新的治理体系，自上而下统一数据安全思维与行动，形成治理合力。

（2）依法构建数据安全管理环境。为落实国家教育现代化战略，高校需立足实际，系统完善数据安全管理制度，强化专业人才培养，夯实治理根基，形成权责清晰、多方协同、监督有力的良性环境，从而释放数据价值，提升共享流通效率。

（3）稳步构建数据安全技术保障体系。数据安全技术是保障数据安全利用、价值提升的重要保障。高校应围绕数据全生命周期，构建集自动化监测、智能预警、协同处置与溯源于一体的数据安全技术保障体系，以支撑校园数智化建设的稳步推进。

6 结束语

高校数据安全治理涵盖管理、技术与运营等核心要素，需随业务发展与安全需求的变化，对相关制度、流程、标准进行持续评估与周期性优化。然而，因其投入产出难以量化，且教育本身具有非营利属性，高校在专业队伍、持续资金及制度落地等方面常面临保障不足的困境。因此，必须依靠管理层的顶层设计与高度重视，通过优化资源配置与全面布局，为数据安全治理提供坚实保障。

参考文献

[1] 南昌网警. 罚款 80 万！南昌某高校发生数据泄露案件[EB/OL]. (2023-08-17)[2025-09-18]. https://weibo. com/ttarticle/p/show? id=2309404935767939219655.

[2] 凤凰网. 河南一高校泄露身份证号等个人敏感信息被通报，正紧急排查[EB/OL]. (2025-08-16)[2025-09-18]. https://i. ifeng. com/c/8lrXbH0LcND.

[3] 姜海舟,王学进,王少华,等. 数字政府网络安全合规性建设指南 密码应用与数据安全[M]. 北京:机械工业出版社, 2024:147-151.

[4] 中国日报. 重磅!《数据安全治理白皮书 6.0》正式发布[EB/OL]. (2024-05-21)[2025-09-18]. https://caijing. chinadaily. com. cn/a/202405/21/WS664c3c55a3109f7860 ddec0e. html.

[5] 澎湃新闻.《数据安全治理实践指南 4.0》亮点提前看[EB/OL]. (2024-11-26)[2025-09-18]. https://www. thepaper. cn/newsDetail_forward_29464452.

[6] 黄科满,许多,杜小勇. 数据社会化视角下的数据流通安全治理:五位一体框架[J]. 大数据,2024,10(6):5-15.

[7] 王健,周国民,廖方宇,等. 基于规则的科学数据安全治理框架:理解数据“保护-利用”失衡及挑战的新工具[J]. 农业大数据学报,2024,6(3):295-306.

[8] 李晓东,董少平,吴菁. 总体国家安全观视域下数据安全治理的路径选择[J]. 中国科技论坛,2024(2):147-157,167.

[9] 马海群,蔡庆平,崔文波,等. 美国数据与算法安全治理:进路、特征与启示[J]. 信息资源管理学报,2023,13(1):52-64.

[10] 张涛,崔文波,刘硕,等. 英国国家数据安全治理:制度、机构及启示[J]. 信息资源管理学报,2022,12(6):44-57.

[11] 梅傲,李坤佳. 日本数据安全治理制度述评及其启示[J]. 情报理论与实践,2023,46(7):195-200.

[12] 饶圆,夏子涵. 档案数据安全治理模型构建研究[J]. 山西档案,2025(3):17-24.

[13] 陈立吾. 金融数据安全治理工作的思考[J]. 中国金融,2023(18):38-40.

[14] 梅振荣,王海伶,许慧,等. 智慧图书馆数据开放共享及安全治理平衡研究[J]. 图书馆,2024 (9):96-101.

[15] 胡新瑞. 数字化转型中教育数据分类分级的治理制度研究[J]. 北京理工大学学报(社会科学版),2025,27(2):215-222.

[16] 韩钢,刘琨,孙树鹏. 数据全生命周期的合规安全治理研究[J]. 通信管理与技术,2024(5):51-54,58.

[17] 郭德香. 我国数据出境安全治理的多重困境与路径革新[J]. 法学评论,2024,42(3):170-181.

[18] 蔡东赟. 零信任安全 技术详解与应用实践[M]. 北京:机械工业出版社,2024:1-7.

[19] GB/T 44109—2024 信息技术 大数据 数据治理实施指南[S]. 2024.

[20] 刘隽良,王月兵,覃锦端,等. 数据安全实践指南[M]. 北京:机械工业出版社, 2022:28.

[21] 搜狐.《数据安全治理白皮书 5.0》发布(全文)[EB/OL]. (2023-05-20)[2025-09-10]. https://www. sohu. com/a/677476807_121123713.

[22] 国家互联网信息办公室. 个人信息保护合规审计管理办法[EB/OL]. (2025-02-14)[2025-09-18]. https://www. cac. gov. cn/2025-02/14/c_1741233507681519. htm.

（收稿日期：2025-11-17）

作者简介：

牛永亮（1984-），男，硕士，实验师，主要研究方向：网络安全、数据安全、校园信息化管理。

朱江琳（1985-），女，博士，讲师，主要研究方向：国家安全、文化安全。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部