Hans Journal of Data Mining 数据挖掘, 2026, 16(2), 48-59
Published Online April 2026 in Hans. https://www.hanspub.org/journal/hjdm
https://doi.org/10.12677/hjdm.2026.162005

Hans汉斯

信息化背景下高校合规性数据安全防护体系建设

冯李春，陈泽生，孙　涛，周　敏*，李炳南，陈伟杰，陈勇标

广州美术学院信息技术中心，广东 广州

收稿日期：2026年3月7日；录用日期：2026年3月30日；发布日期：2026年4月9日

摘　要

面对高校信息化推进中数据多源化、高敏感化挑战及合规政策要求，为解决高校制度碎片化、技术与合规脱节、责任机制松散等问题，文章采用文献研究法、案例分析法，梳理合规核心要求，剖析痛点，构建“一个合规核心 + 四大子体系 + N个支撑模块”的防护框架。以合规为统领，整合全生命周期制度子体系、业务部门数据安全实施路径子体系、跨部门协同与责任管控子体系、学校高层支持与领导推动子体系，辅以政策跟踪、经费保障等模块。通过浙江财经大学制度文本验证表明，该框架可有效应对数据合规风险，兼具包容、适配与补全能力，为高校数据安全合规建设提供实践方案，也为教育领域数据安全治理提供参考。

关键词

高校信息化，数据安全，防护体系，数据生命周期

Building a Regulatory-Compliant Data Security Protection System for Higher Education in the Informatization Context

Lichun Feng, Zesheng Chen, Tao Sun, Min Zhou*, Bingnan Li, Weijie Chen, Yongbiao Chen

Information and Technology Center, Guangzhou Academy of Fine Arts, Guangzhou Guangdong

Received: March 7, 2026; accepted: March 30, 2026; published: April 9, 2026

Abstract

In response to the challenges of data diversification and high sensitivity, as well as compliance policy

*通讯作者。

文章引用: 冯李春, 陈泽生, 孙涛, 周敏, 李炳南, 陈伟杰, 陈勇标. 信息化背景下高校合规性数据安全防护体系建设[J]. 数据挖掘, 2026, 16(2): 48-59. DOI: 10.12677/hjdm.2026.162005

requirements in the advancement of university informatization, and to address issues such as fragmented institutional frameworks, disconnect between technology and compliance, and loose accountability mechanisms, this study adopts the methods of literature research and case analysis. It systematically sorts out core compliance requirements, analyzes key pain points, and establishes a protection framework of "one compliance core + four major subsystems + N supporting modules". With compliance as the guidance, the framework integrates four major subsystems, including the institutional subsystem for the full data lifecycle, the subsystem for data security implementation paths in business departments, the subsystem for cross-departmental collaboration and responsibility management, and the subsystem for university leadership support and promotion. It is supplemented by modules such as policy tracking and funding support. Verification through the institutional texts of Zhejiang University of Finance and Economics shows that this framework can effectively address data compliance risks and possesses the capabilities of inclusiveness, adaptability, and supplementation. It not only provides a practical solution for the development of data security and compliance in colleges and universities but also offers a reference for data security governance in the education sector.

Keywords

Higher Education Informatization, Data Security, Protection System, Data Lifecycle

1. 引言

在国家教育数字化战略行动的大力推动下，人工智能等前沿技术于高校教学、科研及管理场景中加速落地应用[1]。《教育强国建设规划纲要(2024~2035 年)》《关于加快推进教育数字化的意见》等政策陆续出台，高校通过数字化转型赋能已进入纵深发展新阶段，随之而来的数据安全问题也日益凸显。例如，心理咨询预约平台存在越权访问漏洞，导致恶意用户可以获取其他用户数据，存在隐私和安全问题；科研管理平台因存在弱密码安全漏洞，导致管理员账号存在被非法利用的风险，攻击者可借此获取全校科研人员的身份信息，同时造成全校科研项目数据与论文相关信息发生泄露；进校参观预约系统因地址遍历漏洞，导致报备入校人员身份信息批量泄露；云存储平台因配置不当，导致教职工薪酬等敏感管理数据被非法访问。与此同时，《数据安全法》《个人信息保护法》及教育部等主管部门发布的网络和数据安全相关政策，对高校数据分类分级、全生命周期管理提出刚性要求，但多数高校仍面临制度碎片化、技术防护与合规需求脱节、跨部门责任边界模糊的现实矛盾，如何构建适配当前信息化高速发展情境下的合规性数据安全防护体系，成为高校信息化建设亟待突破的关键议题。

国内学者围绕高校数据安全已开展系列研究，但主要集中在数据治理、区块链、数据共享、隐私保护等领域。例如，巫莉莉等人[2]通过数据安全治理能力、数据安全过程和业务场景三个维度构建了一套高校数据安全治理模型。王英人等[3]从数据要素视角，深入剖析公共数据安全的保障与开放利用的若干问题。叶可可等人[4]以区块链为底层架构，提出了一种去中心化机制的数据共享方案，解决数据共享过程中的数据隐私问题。王焕杰等人[5]结合区块链、知识图谱、加密技术，提出一种“存储分节点、访问需授权、行为可追溯”的数据共享方案，在一定程度上实现了安全便捷的数据共享服务。梳理现有研究发现，聚焦高校数据安全防护体系合规性的成果数量偏少，且在高校以数字化转型为导向、推进信息化建设的场景下，数据安全防护体系合规性研究更显滞后。

本研究提出“一个合规核心 + 四大子体系 + N 个支撑模块”的防护框架，其中合规核心锚定法律法规要求，四大子体系包括数据全生命周期、业务部门数据安全实施路径、跨部门协同与责任管控、学校高层支持与领导推动，N 个支撑模块包括但不限于政策跟踪、技术工具、经费保障等模块。最终通过浙江财经大学案例验证体系可行性，并证明该防护框架具备包容、适配与补全能力，为高校信息化部门提供了数据安全防护体系的构建框架及实施建议，助力高校整体提升数据安全治理水平。

2. 数据安全合规相关理论与政策基础

2.1. 核心概念

2.1.1. 高校数据

教育部在《高等学校数字校园建设规范(试行)》中明确指出学校数据的具体体现是信息资源[6]。信息资源包括以结构化数据为主的基础数据和业务数据，以及非结构化数据为主的数字化教学资源、科研资源、文化资源等，还包括信息系统和设备运维过程中产生的半结构化数据等，这些都归类为信息资源[7]。

2.1.2. 数据安全合规

高校数据安全合规是指在教育数字化转型背景下，高校通过制度化建设、技术适配与流程优化等协同机制，对教学、科研、管理等核心业务数据的全生命周期实施系统性风险管控，以满足法律规范、行业标准与办学需求的动态管理过程。数据安全合规在高校中的实践既要将数据利用与数据相关的刚性法律要求转化为校本化的操作规则，又需平衡数据安全防护与数据开放共享的内在需求，其本质是实现数据风险可控前提下的教育价值最大化。

2.2. 理论支撑

2.2.1. 数据分级分类理论

数据分级分类理论是高校数据安全合规的基础性理论支撑。该理论以《数据安全法》确立的分类分级保护制度为法律依据，通过识别数据的业务属性、敏感程度及危害影响范围，建立层级体系。在高校场景中，假设数据分为核心数据、重要数据和一般数据，那么师生的个人敏感信息可定为核心数据；项目经费、账务等普通的财务数据可定为重要数据；学校的基本信息等公开数据可定位一般数据。这种分级方式不仅为差异化防护提供静态基础依据，更能通过动态调整机制，在实时响应合规要求与业务变化的同时，进一步破解高校数据类型复杂、敏感度随场景动态变化的管理难题。

2.2.2. 纵深防御理论

纵深防御是来自于军事理论，在网络和数据安全领域中也得到应用，旨在通过多重的安全措施构建多道防线，提高信息系统的安全性和可靠性[8]。李海蓉[9]在其构建的智慧校园信息安全纵深防御体系中，将智慧校园信息安全的层次分为应用安全层、网络安全层、系统安全层和物理安全层。早明华等人[10]在工业控制系统中也将纵深防御体系划分为物理层、主机层、网络层、应用层和数据层。从二者的体系划分可见，纵深防御在不同领域的应用虽因场景需求存在层级侧重差异，但均遵循分层防护、协同联动的核心逻辑。其中，早明华等人明确纳入数据层，更凸显了纵深防御从传统网络防护向数据防护的延伸。此外，随着数字场景的拓展，纵深防御体系的层级划分还会动态适配新风险，这种灵活适配的特性，进一步强化了其应对多元安全威胁的能力。

2.2.3. 数据生命周期理论

数据生命周期理论将数据管理划分为数据采集、存储、处理、传输、共享和销毁共 6 个阶段[11]，规范了数据全流程合规管控的实施逻辑。在高校场景中，采集阶段遵循最小必要原则，如智慧考勤系统仅

收集必要的学生身份信息；传输阶段对涉密数据采用加密传输协议；存储阶段实施分级存储策略；处理阶段通过权限动态调整实现按需授权；销毁阶段对废弃服务器中的数据执行不可逆删除。这种全流程管控既响应了《个人信息保护法》对数据处理全环节合规的要求，又针对性解决了高校数据管理痛点，确保合规要求贯穿数据从产生到消亡的完整生命周期。

2.2.4. 协同治理理论

协同治理是指不同领域、不同层级的多元主体基于共同目标，通过明确权责分工、建立沟通协作机制、整合资源等，共同参与事务管理与问题解决，以实现单一主体难以达成的治理效能的治理模式。在高校数据安全领域，协同治理则是围绕高校数据的安全保护目标，由高校内部的信息和网络安全领导小组、信息技术中心、人事处等各职能部门，联合师生群体，并结合校外的网络安全监管部门、技术服务提供商、数据合规咨询机构等外部主体，构建的多维度协同防护体系。其中，信息和网络安全领导小组牵头统筹数据安全整体规划、责任划分与跨部门协调，避免单一部门治理的碎片化；信息技术中心提供技术支撑，负责校园数据系统的漏洞检测、应急响应技术保障；人事处聚焦教职工个人信息的采集规范、权限管控与隐私保护，其他各职能部门侧重数据管理与泄露风险的管控；师生群体通过参与数据安全培训提升风险意识，减少因操作失误导致的数据安全问题；校外主体则从外部赋能，例如网络安全监管部门提供政策指导与合规监督，技术服务提供商助力安全技术升级和数据合规咨询等要求。各主体通过协同合作，为高校数字化教学、科研创新与校园管理筑牢安全屏障。

2.3. 政策基础

2.3.1. 国家层面政策，确立合规底线

国家层面以《网络安全法》《数据安全法》《个人信息保护法》为基础框架，确立数据分类分级、敏感信息保护等基础性要求。《网络数据安全管理条例》进一步给出了在处理个人信息收集方式、征询同意模式等内容的个人信息保护指导，以及网络数据跨境的管理条例。

2.3.2. 教育行业层面政策，细化实践要求

教育行业层面以教育部等七部门联合发布的《关于加强教育系统数据安全工作的通知》为核心依据和行动指南，目标为建立数据安全责任和数据分类分级制度，要求规范数据生命周期管理，健全数据安全保障体系[12]。2022 年，教育部在《教育系统核心数据和重要数据识别认定工作指南(试行)》中给出对各级教育部门梳理数据资产，识别并上报核心数据与重要数据清单，为差异化安全防护提供依据的指导[13]。2025 年 7 月，教育部职业院校信息化教学指导委员会[14]发布的《职业院校智慧校园规范(试行)》中描述了各类数据赋能的应用场景，并在数据治理的要求中强调学校的数据标准应充分借鉴和引用国家、行业和地方的标准，以及学校的数据服务应以国家条例规则为依据等多项条例。这些都是教育行业层面对高校数据安全合规性提出的具体要求。

3. 信息化背景下高校数据安全合规现状与痛点

3.1. 整体现状

目前，高校数据安全合规体系建设整体仍处于初步探索与局部推进阶段，尚未形成系统化、常态化的治理格局。多数高校虽依据相关法律法规制定了基本管理制度，并部署了防火墙、访问控制等基础安全措施，但在实际落地与持续运行方面存在显著短板。数据治理层面，普遍存在数据资产底数不清、分类分级模糊、权责归属不明等问题，大量历史与非结构化数据尚未纳入有效管控，导致合规要求难以精准贯彻。此外，各部门独立建设业务系统，而学校又缺乏数据中台或数据共享平台，导致了数据孤岛，

阻碍了统一安全策略的实施与跨域风险管控，且制度执行与技术防护之间尚未实现有效协同。整体而言，高校数据安全合规工作尚未完全实现从被动响应到主动治理的转变，体系建设在顶层设计、跨部门协同和持续运营能力方面仍有待加强。

3.2. 高校数据安全痛点

在高校信息化建设进程中，数据安全合规痛点集中体现为“业务需求优先、安全责任错位”的矛盾。一方面，各业务部门在推进信息化系统建设时，普遍以业务效率提升为核心目标，将数据安全需求置于次要位置，甚至完全不清楚数据安全需求。例如，教务部门搭建在线选课系统时，优先满足选课流程顺畅、数据实时更新的业务诉求，未同步设计学生学籍信息的访问权限分级机制，导致非授权人员可查询批量学生的隐私数据；科研部门上线科研项目管理系统时，聚焦项目申报进度跟踪、成果统计便捷性，未对涉密实验数据设置加密存储与传输防护，存在数据外泄风险；财务部门推进缴费信息化时，侧重支付流程简化、到账信息同步，未落实交易数据的合规留存与脱敏处理，不符合《个人信息保护法》对敏感信息的管控要求。

此外，业务部门普遍将数据安全责任归属于信息部门，忽视自身作为数据产生与使用主体的安全义务。《党委(党组)网络安全工作责任制实施办法》提出了“谁主管谁负责”的原则[15]。各高校在近年也纷纷发布校级层面的网络安全和数据安全等管理办法，以“谁主管谁负责、谁使用谁负责、谁运维谁负责”的原则，将网络安全和数据安全的责任分解至二级学院及行政部门。表 1 列举了部分高校网络安全管理责任归属条例。

Table 1. Reflection of cybersecurity management responsibility attribution principles in some universities
表 1. 部分高校网络安全管理责任归属原则体现

高校	制度名称	年份	具体条例
中国科学技术大学	网络与信息安全工作管理办法[16]	2021	学校网络与信息安全工作遵循“谁主管谁负责、谁使用谁负责、谁运维谁负责”的原则，按照校院两级管理体制，实行安全等级保护制度，全面加强对各类网站及信息系统安全的管理。
华东师范大学	网络安全管理办法[17]	2022	按照“谁主管谁负责，谁运维谁负责，谁使用谁负责”和“属地管理，逐级负责”的原则，学校党委负责指导和监管全校网络安全工作，各相关机构、各部处在职能范围内负责网络安全监督管理工作，各二级单位党组织对本单位网络安全工作负主体责任。
中国美术学院	网络安全管理办法[18]	2025	各单位应按照“谁主管谁负责、谁主办谁负责、谁运行谁负责、谁使用谁负责”的原则，负责本单位主管、运维、 使用的主机、信息系统及数据的安全管理工作，建立本单位的网络安全管理制度和应急处置预案。
桂林电子科技大学	网络安全管理办法[19]	2022	各单位各部门应根据本部门信息化建设情况，建立本部门内部的网络安全管理制度，组织和实施本部门的网络安全工作，遵循学校的管理规范和技术标准，负责本部门建设、运维使用的信息系统及内部网络的安全工作。

续表

复旦大学	校园网系统安全管理规定[20]	2021	各部门、各单位网络安全工作小组负责本单位的网络安全管理工作，接受学校校园网络安全管理小组的领导、监督和检查，维护本单位的网络及信息安全。
大连理工大学	网络安全管理办法[21]	2024	校内各单位按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，分别负责本单位主管、运维、使用的各信息系统及内部网络的安全工作。校内各单位应根据本单位信息化建设情况，建立本单位的网络安全管理制度和应急处置预案。

由表 1 可知，各业务部门需对其主管领域的网络安全负直接责任。然而，高校业务系统建设部门既未充分认识到自身需承担的网络安全责任，也缺乏相应的网络安全管理能力。

《教育部关于加强教育行业网络与信息安全工作的指导意见》中也强调“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，并明确指出网络与信息系统的运行维护部门承担系统的技术安全保障责任，网络与信息系统的使用单位和个人承担系统操作与信息内容的直接安全责任。但实践中，各部门以系统为信息技术中心搭建为由，未能明确自身的责任主体定位。

信息技术中心在高校数据安全中承担的是技术支撑与统筹协调的角色，其核心职责是搭建全校统一的数据安全技术框架、提供安全技术培训与咨询、协助各业务部门解决技术层面的安全问题，而非包揽所有安全责任，这种责任错位和过度依赖的现状，使得高校信息化建设中的数据安全合规始终处于被动应对的状态。

4. 高校合规性数据安全防护体系构建

针对高校在数据安全合规性方面存在的实际问题，提出构建“一个合规核心 + 四大子体系 + N 个支撑模块”的数据安全防护框架，如图 1 所示。该框架以合规性为核心，整合全生命周期制度、业务部门数据安全实施路径、跨部门协同与责任管控、学校高层支持与领导推动四大子体系，并辅以政策跟踪、经费保障等支撑模块，旨在提升高校数据安全的合规性和防护能力。

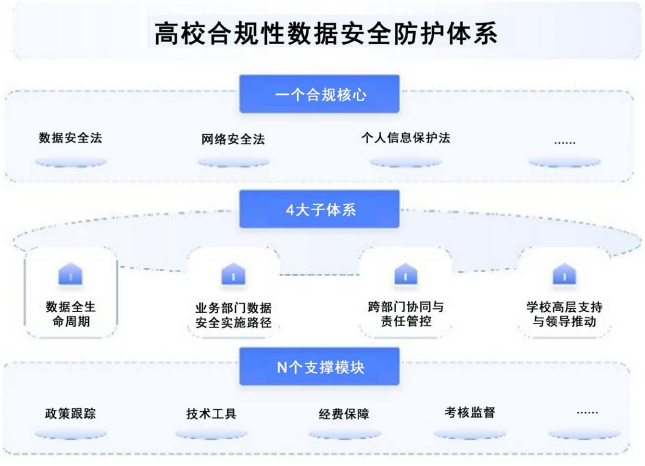

Figure 1. Architecture of regulatory-compliant data security protection system for higher education
图 1. 高校合规性数据安全防护体系架构

4.1. 一个合规核心

在高校数据安全防护体系的建设中，合规性是体系的核心。不仅确保高校的数据处理活动符合国家法律法规的要求，而且通过与高校具体信息化业务的深度结合，避免合规措施与实际操作之间的脱节。

在法规适配方面，高校需要全面梳理并遵循国家及行业的相关法律法规，制定符合学校实际情况的数据安全合规策略。关键内容包括数据的分类分级、责任划分以及数据处理的基本规范。高校应根据《数据安全法》及《个人信息保护法》等相关法律，将数据划分为不同的类别，如核心数据、重要数据和一般数据，并根据不同等级制定相应的防护措施。

在业务贴合方面，合规性不仅要符合法律要求，还应与高校的信息化业务深度结合，确保合规要求能够适配实际工作。例如，在科研协作场景中，涉及跨境国际合作的数据应提交出境安全评估申请，在智慧教学场景中，学情数据需要进行脱敏后才能用于教学分析。通过制定这些具体的操作规范，确保合规要求能够切实融入到数据安全工作中。

合规核心还需要促进高校内部的全员合规文化，不能仅仅依赖于法务或技术部门，而应成为全体师生的共同责任。例如，可以通过定期的网络安全及数据安全，提升每一位师生的合规意识。在这种合规文化的驱动下，高校有更大可能建立起一套持续、动态的合规性管理机制，从而确保数据安全防护体系的长期有效性。

4.2. 四大子体系

4.2.1. 数据全生命周期制度子体系

全生命周期管控是高校数据安全防护体系中的核心子体系之一，它贯穿数据从采集、存储、处理、传输、共享和销毁的各个环节，确保数据在整个生命周期中始终处于受控和安全的状态[2]。

在数据采集阶段，高校需严格落实“告知与同意”原则，采集前应向数据主体明确说明采集目的、范围、使用方式及可能影响，并取得明确授权，确保采集过程符合个人信息保护法等法律法规要求。在数据存储阶段，高校需根据数据敏感级别实施分级存储和权限管理。核心数据应置于高安全等级环境，普通数据可存储于一般环境。同时，对存储过程进行严格的访问控制和加密保护，防止未经授权的访问和泄露。在数据处理阶段，应实行最小权限原则，仅授权人员可在特定业务场景中处理相应数据，并记录操作日志以便追溯。同时，对敏感数据进行脱敏、去标识化等合规处理，并定期开展合规审计，确保数据使用安全合法。在数据传输阶段，应采用加密协议和安全通道，保障传输中的机密性和完整性，防止非法拦截或篡改。在数据共享阶段，应依托共享平台，按照预设规则和权限实现数据有序流转并全程保留流转痕迹。在数据销毁阶段，应对过期或不再需要的数据实施不可逆销毁，如物理销毁或安全删除。

4.2.2. 业务部门数据安全实施路径子体系

在高校的数据安全合规体系中，业务部门作为数据的产生、使用与管理主体，需具体落实其数据安全责任。首先，应在信息化系统建设的初期，明确数据安全需求。这一阶段，需从自身的业务特性出发，评估和识别数据安全需求，并确保这些需求在系统设计阶段得到充分考虑。其次，根据业务系统已规划的需求，落实日常数据安全管理，通过严格执行校级制度和标准操作流程，确保各项数据安全措施不落空。然后，应强化数据安全意识与技术能力。应定期组织数据安全教育培训，提高对数据安全风险的识别能力和应对措施的理解。增强技术支持能力，配置具备理工科背景的数据安全管理员，能执行基本的业务系统和服务器运维，理解数据加密、访问控制等基本的数据安全逻辑，确保数据安全不完全依赖信息技术中心的单一支持，能真正实现“谁建设谁负责、谁运维谁负责”的技术保障。此外，还应建立自查机制，定期评估和检查现有的安全措施，并进行整改。设定定期自查机制，评估数据安全措施的执行效

果，尤其是在数据存储、访问、共享等环节，确保无漏洞可乘。自查过程中发现的任何问题，都需要及时采取整改措施，优化数据安全管理流程或技术手段，防止问题再次发生。

4.2.3. 跨部门协同与责任管控子体系

在高校数据安全合规体系的建设过程中，各业务部门之间的协同至关重要。数据安全管理不仅仅是某一个部门的责任，而是需要多部门协作、共同执行的任务。特别是在数据处理和共享过程中，如何确保各部门的责任分工明确、协同高效，成为数据安全防护体系中必须解决的核心问题。

跨部门协同与责任管控体系的目标，是通过构建有效的协作机制和责任管控框架，确保各部门按照既定的政策要求共同推进数据安全工作，避免各部门独立行动，导致资源浪费、信息割裂、责任错位等问题。

4.2.4. 学校高层支持与领导推动子体系

为了确保数据的安全性和合规性，必须从校级层面明确各部门在数据安全管理中的职责。校级层面应发布统一的《数据安全管理办法》，明确每个部门在数据安全中的责任和任务，避免责任不清、互相推诿的现象。设立数据安全协调小组，负责推动全校范围内的数据安全工作。协调各部门之间的需求和资源，确保数据安全措施的有效实施；解决跨部门合作中的问题和障碍，确保信息流通无阻；监控各部门在数据安全实施过程中的进展，确保任务按时完成。各部门应定期召开数据安全协作会议，分享工作进展、讨论存在的问题和挑战。会议的重点应集中在业务部门的数据安全需求、信息技术中心提供的技术支持和资源协调等方面，确保各方在同一目标下协作。

4.3. N 个支撑模块

为了确保高校数据安全合规防护体系的有效运行，除了合规核心和四大子体系的建设外，还需要一系列支撑模块来为体系提供技术、政策、经费、考核与监控等方面的保障。这些支撑模块帮助高校从多维度保障数据安全，确保在信息化建设过程中能够有效落实数据保护措施，规避潜在风险。表 2 列出了部分支撑模块及其概述。

Table 2. Names and brief descriptions of N supporting modules
表 2. N 个支撑模块名称及其概述

模块名称	模块概述
政策跟踪与合规适配模块	建立机制及时跟踪各项新出台的法律法规，并将其转化为校内制度。
技术工具模块	为数据安全防护提供专业技术工具，提升数据安全的技术保障能力。
经费保障模块	为高校数据安全工作提供资金保障，确保数据安全项目顺利实施。
考核监督模块	制定考核规则，与绩效、评优挂钩，强化业务部门数据安全自主监督意识。
数据安全自查模块	业务部门定期开展数据安全自查，及时处置异常情况。
人员队伍建设模块	组建专业的数据安全队伍，提升专职人员的数据安全管理能力与业务素养。
数据分类分级管理模块	建立科学的数据分类分级标准与操作规范，开展数据分类分级工作。
...	...

5. 高校数据安全合规框架的实践验证

国家标准《GB/T 22080-2025》采用了 ISO、IEC 等国际国外组织的标准，设置了“领导、规划、支持、运行、绩效评价和改进”的信息安全管理体系，其中领导和规划与所提出的“一个核心”理念相似，

但是“支持、运行、绩效评价和改进”对教学科研等高校特殊业务场景适配性不足。美国国家标准与技术研究院发布的“The NIST Cybersecurity Framework (CSF) 2.0”将网络安全的框架核心定义为“功能–类别–子类别”三层体系，功能上划分为“治理、识别、保护、侦测、回应和复原”，其框架更多的是从技术角度分析网络安全。与上述国内外两项框架相比，本文所提出的框架对高校的适应场景更具针对性。

为验证本文所提出的框架的有效性，以浙江财经大学的七项公开制度作为分析依据，如表 3 所示。研究核心并非对该校制度进行单纯归纳，而是聚焦本文所提出的“一个合规核心 + 四大子体系 + N 个支撑模块”高校数据安全合规框架，从包容能力、适配能力、补全能力三个维度展开验证，旨在证明该框架并非专属化模型，而是具备跨高校迁移价值的通用管理工具，为不同类型高校数据安全合规实践提供可参考的适配路径。

Table 3. Partial public regulations of Zhejiang University of Finance and Economics
表 3. 浙江财经大学部分公开制度

序号	制度名称
1	浙江财经大学个人信息保护管理办法
2	浙江财经大学数据安全管理办法
3	浙江财经大学数据分类分级指南
4	浙江财经大学网络安全与数据安全应急预案
5	浙江财经大学校园网络管理办法
6	浙江财经大学信息化管理办法
7	浙江财经大学信息化项目管理办法

5.1. 一个合规核心的包容能力验证

一个合规核心的核心要义为“以数据安全法律法规为底线，适配高校差异化业务场景”，这一逻辑在浙江财经大学制度体系中得到充分体现，且框架对该校作为财经类高校的特色需求具备显著包容度。

从法规底线契合性来看，该校 7 项制度均以《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》等为根本依据。浙江财经大学 1 号管理办法直接援引“最小必要”、“知情同意”等法定原则，区分普通与敏感个人信息的保护标准，确保制度文本与国家法规无偏差。浙江财经大学 2 号管理办法明确遵循国家数据安全法律法规，落实数据安全管理责任，将数据全生命周期安全要求转化为校内操作规范。这种法规到制度的深度衔接，与框架“一个合规核心”的内涵完全一致，证明框架对高校合规性需求的基础包容。

5.2. 四个子体系的适配能力验证

5.2.1. 数据全生命周期制度子体系的适配

该子体系要求覆盖数据全生命周期，形成闭环管控。浙江财经大学通过 1、2、3 号制度，构建了与框架高度契合的全生命周期管控流程。在采集环节，遵循一数一源原则，规定数据中台已有数据需通过共享获取，禁止重复采集。采集敏感数据或超 500 条个人数据需经学校数字化办公室审批备案。在传输与存储环节，明确 L3 级数据需加密传输。学校内部数据及敏感数据原则上应保存在学校数据中心，禁止校外或境外存储。在共享环节，要求 L2 级及以上数据共享需经数据源单位与数字化办公室双重审核。该校的全生命周期管控流程未脱离框架逻辑，而是将框架要求转化为符合财经类高校实际的操作规范，证

明框架子体系可与高校现有数据管理流程无缝对接，无需高校打破原有管理惯性。

5.2.2. 业务部门数据安全实施路径子体系的适配

该子体系明确业务部门在数据安全管理中的角色与操作路径，避免责任虚化。浙江财经大学在 2 号和 6 号制度中，明确学校各单位主要负责人为本单位数据安全第一责任人，将责任落实到具体岗位。同时，针对不同业务部门的职能，在 3 号制度中提供差异化实施指引，例如要求教务部门重点核查学籍数据(L3 级)，财务部门核验工资数据(L3 级)。这种“责任绑定 + 场景化指引”的实施路径，证明框架可适配高校已有的部门权责划分，只需将框架要求转化为业务部门可执行的具体任务即可。

5.2.3. 跨部门协同与责任管控子体系的适配

该子体系要求“明确跨部门协同主体、流程与责任，解决部门推诿问题”。浙江财经大学在数据共享、项目验收等关键场景的制度设计，与框架逻辑完全一致：在数据共享场景中，根据数据分级确认数据共享策略，具体包括数据来源单位的审批和数字化办公室的评估，以及数据共享前的脱敏等策略。该校的跨部门机制未突破框架设定的协同与责任逻辑，而是通过制度明确协同节点与责任边界，证明框架可适配高校现有的跨部门管理模式，为协同流程提供更清晰的逻辑支撑。

5.2.4. 学校高层支持与领导推动子体系的适配

该子体系要求高层统筹决策、保障资源投入，确保数据安全工作战略落地。浙江财经大学的制度设计充分体现这一要求：在决策层面，6 号制度明确由校长任组长的网络安全与信息化领导小组，审议学校信息化发展的中长期规划和信息化建设与管理中的重大问题。在考核层面，2 号制度要求数据处理过程中的关键岗位人员需要对其进行数据安全专业能力考核。该校的高层推动机制与本文所提出的框架要求高度契合，这一实践证明框架可适配高校现有的顶层决策体系，能够通过整合高层决策和考核层面的关键动作，进一步强化数据安全工作的战略地位。

5.3. N 个支撑模块的补全能力验证

5.3.1. 政策跟踪与合规适配模块的补全作用

浙江财经大学 7 项制度均发布于 2023~2024 年，文本中未提及政策动态调整机制，即未明确国家或地方性法规修订后，校内制度如何同步优化，存在制度滞后风险。框架政策跟踪与合规适配模块可针对性补全这一空白。该模块建议组建政策和业务适配工作组，定期梳理国家与地方层面的数据安全新政，同时建立法规政策和学校制度的映射台账，将新规条款拆解为校内制度修订任务。通过动态调整机制提升制度时效性，体现框架对高校管理空白的补全价值。

5.3.2. 技术工具模块的补全作用

浙江财经大学 2 号制度仅概括性地描述需要采用数据加密、访问控制、日志审计等技术措施，未明确技术工具如何贴合财经类业务场景，存在技术与业务脱节的风险，而技术工具模块可补全这一细节。该模块建议针对财经类数据的非结构化特征，通过财经数据专用安全工具，例如开发支持 Excel、PDF 格式的加密工具，确保财经数据在存储与传输过程中保持格式兼容性，同时建议在财务系统或科研经费管理系统中内置操作日志定向审计工具，重点监测大额经费数据查询、修改、导出等敏感操作，自动识别非授权访问行为并触发告警。该模块通过技术工具的业务化适配，将该校原则性的技术要求转化为可落地的具体方案，填补技术工具与业务场景脱节的空白。

5.3.3. 师生数据权益保障模块的补全作用

浙江财经大学 1 号制度仅提及师生可向数据源部门申请更新个人信息，但未明确数据查询、更正、

删除等权益的响应流程与时限，师生权益诉求缺乏闭环机制，而师生数据权益保障模块则可补全这一缺口。该模块建议该校在校园服务 APP 或一站式服务平台增设数据权益申请入口，师生可在线提交个人学籍数据查询、个人信息数据更正、非必要数据删除等申请；同时，明确业务部门响应时限，建立权益争议复核机制，确保权益诉求得到公正处理。该模块通过权益响应流程，填补该校师生权益保障的空白，提升数据安全管理的人文性与合规性。

6. 结论

本研究针对高校信息化推进过程中数据多源化、高敏感化的趋势，以及法律法规的政策要求，围绕高校制度碎片化、技术与合规脱节、责任机制松散等现实问题，构建了“一个合规核心 + 四大子体系 + N 个支撑模块”的防护框架，并以浙江财经大学的 7 项制度为样本验证。研究表明，该框架具备包容、适配和补全能力，可提供通用逻辑与特色调整相结合的迁移方案，解决单一技术或孤立制度的局限。鉴于本研究案例验证聚焦财经类高校，未来可进一步拓展至理工科、艺术类等多类型高校验证适配性，并细化高层资源投入、技术工具选型等实操指标，推动框架从理论模型向可落地的行业实践指引转化。

基金项目

中国高校产学研创新基金(2024MU039)；广州美术学院体制机制改革项目(20231125-029)。

参考文献

[1] 吴砥. 国家数字化战略行动三年成效与未来展望[N/OL]. 中国教育报, 2025-04-24(02). http://paper.jyb.cn/zgjyb/html/2025-04/24/content_144741_18467339.htm, 2025-10-16.

[2] 巫莉莉, 黄志宏, 何斌斌. 高校数据安全治理的模型研究[J]. 网络安全与数据治理, 2025, 44(7): 43-49.

[3] 王英, 马海群. 数据要素视角下公共数据安全保障的若干问题研究[J]. 现代情报, 2024, 44(8): 4-12.

[4] 叶可可, 高宏民, 张雨荷, 等. 基于去中心化验证的多方数据安全共享方案[J]. 信息安全研究, 2025, 11(6): 578-584.

[5] 王焕杰, 魏铨, 刘祺, 等. 海洋装备数据安全共享方案[J]. 舰船科学技术, 2024, 46(22): 170-173.

[6] 高等学校数字校园建设规范(试行) [EB/OL]. http://www.moe.gov.cn/srcsite/A16/s3342/202103/t20210322_521675.html, 2025-09-04.

[7] 陶昀翔, 王钧, 李全香. 大模型技术在高校非结构化数据领域的应用研究[J]. 科技资讯, 2025, 23(16): 215-218.

[8] 高晓虎. 集团司库系统网络安全纵深防御研究[J]. 网络安全技术与应用, 2025(7): 128-131.

[9] 李海蓉. 智慧校园环境下的校园信息安全纵深防御体系的应用研究[J]. 信息记录材料, 2023, 24(8): 229-231.

[10] 早明华, 柳晓静, 官雄明, 等. 工业控制系统网络安全纵深防御体系构建[J]. 中国科技信息, 2025(17): 115-118.

[11] 张昊星, 赵景欣, 岳星辉, 等. 全生命周期数据安全管理和人工智能技术的融合研究[J]. 信息安全研究, 2023, 9(6): 543-550.

[12] 虞萍, 周南. 高校科学开展数据分类分级策略[J]. 中国教育网络, 2024(5): 70-73.

[13] 王孝亮. 基于数据安全的高校数据分类分级方法探究[J]. 信息技术与标准化, 2025(8): 36-39.

[14] 教育部职业院校信息化教学指导委员会. 《职业院校智慧校园规范(试行)》[EB/OL]. 2025-08-02. https://www.tech.net.cn/news/show-106396.html, 2025-09-04.

[15] 贯彻落实《党委(党组)网络安全工作责任制实施办法》的实施意见[N]. 黑龙江日报, 2022-07-11(004).

[16] 中国科学技术大学网络与信息安全工作管理办法(试行) [EB/OL]. https://wxb.ustc.edu.cn/2022/0412/c30555a551735/page.htm, 2025-09-25.

[17] 《华东师范大学网络安全管理办法》[EB/OL]. https://labcomm.ecnu.edu.cn/47/11/c41105a608017/page.htm, 2025-09-25.

[18] 关于印发《中国美术学院网络安全管理办法》的通知[EB/OL]. https://itc.caa.edu.cn/info/1022/1090.htm, 2026-03-16.

[19] 关于印发《桂林电子科技大学网络安全管理办法》的通知[EB/OL]. https://www.guet.edu.cn/xjzx/2024/0715/c1586a126354/page.htm, 2025-09-25.

[20] 复旦大学校园网络系统安全管理规定[EB/OL]. https://xxb.fudan.edu.cn/42/4a/c33381a410186/page.psp, 2025-09-25.

[21] 关于印发《大连理工大学网络安全管理办法(修订)》的通知[EB/OL]. https://its.dlut.edu.cn/#3, 2026-03-16.