 DOI: https://doi.org/10.12349/iser.v7i4.10045

Research on the Construction and Practice of Network Data Security Governance System in Universities

Yang Qi

Hubei Institute of Engineering, Xiaogan, Hubei, 432000, China

Abstract

With the rapid development of information technology and digital education, the security of network data in universities is facing increasingly complex threats and challenges. This article takes the governance of network data security in universities as the research object, and systematically explores the construction methods of the network data security governance system from four dimensions: institutional construction, technical protection, organizational management, and education and training. By analyzing the existing security management practices in universities, this study proposes a comprehensive strategy for network data classification and grading management, risk assessment, monitoring and early warning, emergency response, and education and training. Practice has shown that building a sound network data security governance system can enhance the information system protection capabilities of universities, standardize data management behavior, enhance the network security awareness of teachers and students, and provide guarantees for the digital transformation and smart campus construction of universities.

Keywords

universities; network data security; governance system; risk management; information security

高校网络数据安全治理体系构建与实践研究

祁洋

湖北工程学院，中国 · 湖北 孝感 432000

摘　要

随着信息技术和数字化教育的快速发展，高校网络数据安全面临日益复杂的威胁和挑战。本文以高校网络数据安全治理为研究对象，从制度建设、技术防护、组织管理和教育培训四个维度，系统探讨网络数据安全治理体系的构建方法。研究通过分析高校现有安全管理实践，提出网络数据分类分级管理、风险评估、监测预警、应急响应及教育培训的综合策略。实践表明，构建完善的网络数据安全治理体系能够提升高校信息系统防护能力、规范数据管理行为、增强师生网络安全意识，为高校数字化转型和智慧校园建设提供保障。

关键词

高校；网络数据安全；治理体系；风险管理；信息安全

1 引言

高校信息化建设快速推进，大量教学、科研和管理数据集中存储与传输，使网络数据安全成为重要议题。网络攻击、数据泄露及内部管理不规范等问题对高校教育科研活动及信息资产保护构成威胁，影响学校正常运转和声誉。现有安全管理多依赖单一技术防护，缺乏系统性治理机制和制度保障，难以应对复杂多变的网络安全风险。本文基于高校信息化现状，探讨网络数据安全治理体系构建的方法，包括制度建设、技术手段、组织管理和教育培训，提出可实施的策略与实践路径，为高校信息安全管理提供理论依据与操作指南。

【作者简介】祁洋（1998–），男，中国湖北随州人，硕士，从事计算机应用技术、人工智能研究。

2 高校网络数据安全现状分析

2.1 数据类型及管理特点

高校网络数据涵盖教学资源、科研数据、行政管理信息以及师生个人信息等多种类型，呈现出数据种类复杂、敏感程度差异明显以及分布范围广泛等特点。教学与科研数据通常包含学术成果、实验数据和研究资料，涉及知识产权保护和科研成果安全；行政管理数据则涉及学生学籍、财务信息及校园管理运行情况，具有较高的敏感性；个人信息数据则直接关系到师生隐私与合法权益。不同类型数据在使用方式、访问权限和安全等级方面存在差异，这对数据管理提出了更高要求。因此，高校在数据安全治理中需要根据数据的重要程度和敏感等级实施分类分级管理，通过明确数据存储规范、访问控制方式以及传输安全机制，使不同类别数据在生命周期各阶段均能够得到相应的安全保护。

2.2 现有管理制度分析

目前，多数高校已经建立了基本的信息安全管理制度，对网络系统运行和数据使用进行了初步规范。然而，在实际执行过程中仍存在一定不足。一方面，部分制度在数据管理环节中的覆盖范围不够全面，对数据访问权限、存储加密以及网络访问控制等关键环节缺乏统一标准。另一方面，一些制度在执行过程中缺乏监督和评估机制，导致制度落实程度不高。此外，高校内部不同部门之间的信息管理体系相对独立，跨部门协同不足，使数据管理缺乏整体协调性。在技术防护方面，部分高校的安全技术措施与管理制度之间未能形成有效衔接，从而导致管理与技术之间存在脱节现象。这些问题在一定程度上削弱了网络数据安全治理的整体效果。

2.3 安全威胁与风险特征

高校网络环境面临的安全威胁具有多源性和复杂性。外部网络攻击、恶意软件传播以及网络钓鱼等行为可能对校园信息系统造成破坏，而内部误操作或权限管理不当也可能导致数据泄露或系统故障。此外，由于高校科研活动频繁，大量科研数据在网络环境中进行存储和传输，一旦受到攻击或篡改，可能对学术研究和知识产权产生严重影响。同时，师生个人信息和行政管理数据一旦泄露，也可能造成社会影响和法律风险。高校网络安全风险通常具有突发性和隐蔽性，问题往往在短时间内迅速扩散，并可能带来较大的损失。因此，高校网络数据安全治理需要具备风险预防、实时监测、应急处置以及持续改进等多方面能力，以提高整体安全防护水平。

3 高校网络数据安全治理体系构建

3.1 制度与规范建设

在高校网络数据安全治理体系中，制度与规范建设是实现有效管理的重要基础。高校应构建系统化的数据安全管理制度，涵盖数据分类分级管理、访问权限控制、信息安全审计以及应急响应机制等内容，从制度层面明确各部门在数据管理中的职责分工和操作流程。制度体系需要覆盖数据生成、存储、传输、使用以及销毁等全过程，使数据在不同阶段均能够受到规范化管理。同时，随着信息技术的发展和网络安全威胁形式的不断变化，相关制度也应保持动态更新，通过定期评估和修订，使制度内容与技术环境保持一致。通过制度化和标准化管理，可以增强数据安全管理的可操作性与可执行性，为高校网络数据安全治理提供稳定的制度保障。

3.2 技术防护与安全措施

技术防护是保障网络数据安全的重要支撑。在高校信息系统运行过程中，应通过构建多层次安全防护体系来保护数据资源的安全。常见技术措施包括部署防火墙系统、入侵检测系统以及身份认证机制，以实现对网络边界和内部访问行为的有效控制。同时，通过采用数据加密技术，可以对敏感信息进行保护，防止在传输和存储过程中被非法获取。此外，建立数据备份与恢复机制能够在系统出现故障或遭受攻击时快速恢复数据，减少损失。结合日志监控与数据分析技术，还可以对系统运行情况进行持续监测，一旦发现异常行为即可及时发出预警。通过技术防护与管理制度相结合，可以形成更加完善的网络数据安全防护体系。

3.3 风险评估与动态管理

在高校网络数据安全治理过程中，风险评估是实现科学管理的重要环节。高校应建立基于风险的管理机制，对网络系统、数据资产以及关键应用平台进行定期评估。评估过程通常通过分析潜在威胁来源、发生概率以及可能产生的影响程度，对不同风险进行量化分类，从而确定风险等级并制定相应的处置策略。在此基础上，通过持续监测网络运行状态和数据使用情况，可以及时发现新的安全隐患并进行调整。动态管理机制强调持续改进和循环优化，使安全治理体系能够适应不断变化的技术环境和安全挑战。通过将风险评估结果应用于管理决策，可以提高高校网络数据安全治理的前瞻性与灵活性。

4 高校网络数据安全组织与实践

4.1 安全组织架构设计

在高校网络数据安全治理体系建设中，完善的组织架构是保障管理措施有效实施的重要基础。高校应建立统一的网络数据安全管理机构，以校级信息中心为核心统筹安全管理工作，同时明确各学院、科研单位及相关职能部门在数据安全管理中的职责分工。通过构建校院两级管理体系，可以实现政策制定、技术管理与监督审计之间的有效衔接。校级层面主要负责安全策略制定、重大安全事件处置和资源协调，各二级单位则承担日常网络安全管理和数据使用监管任务。此外，组织架构设计还应兼顾技术支持与行政管理职能，使安全决策能够迅速落实，并推动跨部门之间的协同合作。通过明确责任主体和管理流程，可以实现安全管理责任的可追溯性，从而形成系统化、规范化的网络数据安全治理机制。

4.2 教育培训与安全文化建设

在高校网络安全治理体系中，技术防护措施与制度管理需要与安全教育相结合，才能形成长期稳定的安全环境。高校应通过开展网络安全培训、专题讲座及应急演练等方式，提高师生对网络安全风险的认识，使其掌握基本的数据保护和信息安全技能。培训内容应涵盖数据保密意识、密码安全管理、移动终端使用规范以及网络诈骗防范等方面，使师生能够在日常学习和科研活动中主动采取安全措施。同时，通过校园宣传活动和安全教育课程，可以逐步营造良好的网络安全文化氛围，使安全意识成为校园行为规范的一部分。通过构建“技术防护、制度管理与安全教育”相结合的治理模式，可以增强全体师生的安全责任意识，从而在整体层面提升高校网络数据安全管理水平。

4.3 应急响应与事件管理

在网络安全管理体系中，应急响应机制是应对突发安全事件的重要保障。高校应建立完善的网络安全事件处理流程，包括事件识别、风险评估、应急处置以及系统恢复等环节，使安全事件能够得到及时控制和有效处理。通过建设统一的安全监测平台，可以实现对网络运行状态和异常行为的实时监控，当系统检测到潜在安全风险时能够及时发出预警。与此同时，高校应定期组织网络安全应急演练，通过模拟攻击或系统故障情景，提高管理人员和技术人员的应急处理能力。在事件处理完成后，还应对相关过程进行记录与分析，总结经验并完善安全制度和技术措施。通过持续改进事件管理机制，可以不断提升高校网络安全治理体系的风险防控能力与管理水平。

5 BIM 与数据分析技术在安全治理中的应用

5.1 BIM 技术与校园网络资源可视化

在高校网络数据安全管理体系建设中，引入 BIM 技术能够为信息资源管理提供新的技术路径。通过建立数字化模型，可将校园网络结构、服务器设备、数据中心以及信息系统节点进行三维可视化呈现，使复杂的网络架构更加直观清晰。管理人员可以通过可视化平台实时查看网络拓扑结构、设备运行状态以及数据传输路径，从而更准确地掌握网络运行情况。与此同时，可视化系统还能够标识关键安全节点和重要数据资源位置，使安全管理人员在发生异常时迅速定位问题来源并采取应对措施。此外，通过将网络设备、机房环境以及信息系统运行状态纳入统一模型，可以实现信息资源的动态监控与管理，提高管理效率。BIM 技术在校园网络资源管理中的应用，使原本抽象的数据系统具备直观展示能力，为高校网络安全治理提供更加清晰和高效的管理工具。

5.2 数据分析与风险预测

在高校网络安全治理过程中，数据分析技术对于提升风险识别能力具有重要作用。通过对网络日志、访问行为记录以及历史安全事件数据进行系统收集与整理，可以建立多维度数据分析模型，从而识别潜在安全风险。利用大数据分析技术，可以对用户访问模式、数据传输频率以及系统异常行为进行统计分析，及时发现异常访问或潜在攻击行为。同时，通过机器学习和统计模型对历史数据进行建模，可以预测未来网络安全风险的发展趋势，为安全管理提供预警机制。数据驱动的风险预测不仅能够提高网络安全防护的前瞻性，还能够帮助管理部门合理配置安全资源。例如，在风险较高的系统节点增加安全监控措施，在重点数据区域加强访问控制，从而形成更加科学和精准的网络安全管理模式。

5.3 信息集成与智能化管理

在高校网络安全治理体系中，信息集成平台是实现智能化管理的重要基础。通过构建统一的信息管理平台，可以将制度规范、技术防护措施、监测数据以及安全培训信息进行整合，形成完整的数据管理体系。该平台能够实现多系统之间的数据互通，使网络安全管理由分散式管理转向集中化管理。通过平台系统，可以实现网络安全事件的自动识别与预警，并结合权限管理机制对用户访问行为进行控制。同时，平台还具备审计追踪功能，对系统操作记录进行保存与分析，为安全事件调查提供依据。在突发安全事件发生时，平台可启动应急联动机制，实现快速响应和协同处置。通过信息集成与智能化管理，高校网络安全治理体系能够实现数据监测、风险预警、应急处理和持续改进的闭环管理，从而提升整体安全管理水平。

6 结语

高校网络数据安全治理体系的构建需要制度建设、技术防护、组织管理与安全教育协同推进。通过实施数据分类分级管理、完善访问控制机制、加强技术防护措施以及开展风险动态评估，可实现对数据生成、存储、传输与使用全过程的安全管理。同时，借助信息集成平台与智能化监测技术，可以提升网络运行监控能力和风险预警水平，使安全治理更加科学与高效。实践表明，系统化的治理体系不仅能够提升网络安全防护能力，还能规范数据管理流程并增强师生的安全意识，为智慧校园建设提供稳定支撑。未来，高校应持续完善制度规范、强化技术应用能力并加强安全教育与应急管理机制，推动网络数据安全治理向系统化、智能化和可持续方向发展，从而为教育教学与科研活动提供可靠的信息安全保障。

参考文献

[1] 欧阳飞.高校网络信息安全治理体系构建[J].网络安全和信息化,2025,(10):26-28.

[2] 张杨.高校数据中心网络安全加固体系构建研究[J].电脑编程技巧与维护,2025,(08):168-171.

[3] 钱小龙,葛黄雅,黄蓓蓓.基于云平台的高校数据安全治理体系构建与应用研究[J].科技管理研究,2024,44(17):122-128.

[4] 张建娇.高校数据中心网络安全入侵防护体系构建[J].网络安全和信息化,2024,(08):126-128.

[5] 魏楚元,任彦龙,李欣.高校网络安全治理体系构建研究[J].网络安全技术与应用,2021,(01):96-98.