

DEVELOPMENT OF DATA SECURITY MANAGEMENT AT DALI UNIVERSITY IN YUNNAN PROVINCE

Shuhui TIAN

Student of Master in Educational Administration, Suan Sunandha Rajabhat University,
Thailand; s67561802147ssru.ac.th

ARTICLE HISTORY

Received: 20 July 2026

Revised: 22 July 2026

Published: 22 July 2026

ABSTRACT

This research explored the present situation of data security management at Dali University in Yunnan Province and put forward development guidelines. A design using mixed methods was utilized. Quantitative data were gathered from 165 administrators, educators, technical employees, and other individuals engaged in educational governance, digital systems, or data handling. Meanwhile, qualitative data were acquired from five key informants. The general degree of data security management was at a medium level (Mean = 3.36, S.D. = 0.64). Educational Administrative Practices (Mean = 3.44, S.D. = 0.61) along with Data Security Governance (Mean = 3.43, Standard Deviation = 0.63) had the highest ranking, while Institutional Decision-Making Processes (Mean = 3.29, S.D. = 0.66) and Data Risk Governance (Mean = 3.25, S.D. = 0.68) constituted the weakest aspects. Significant issues involved inadequate staff training, dispersed responsibilities, restricted inter-departmental cooperation, top-down decision-making model, poorly unified systems, and non-comprehensive continuous risk surveillance. Five sets of guiding principles were put forward: reinforcing educational management operations, bettering governance and responsibility-taking, boosting participatory decision-making processes, incorporating digital infrastructure, and setting up a continuous data risk-handling cycle. The research results offer empirical and practical advice for universities going through digital transformation.

Keywords: Data Security Management, Educational Administration, Data Security Governance, Institutional Decision-Making, Digital Infrastructure Integration

CITATION INFORMATION: Tian, S. (2026). Development of Data Security Management at Dali University in Yunnan Province. *Procedia of Multidisciplinary Research*, 4(7), 59.

INTRODUCTION

Research Background

Digital change has remodeled teaching, research, management, and institutional decision-making in tertiary education. Universities are increasingly dependent on cloud platforms, big-data applications, artificial intelligence, learning-management systems, and interlinked administrative databases. These technological advancements enhance efficiency and the quality of service. However, they also heighten the risk of unauthorized entry, privacy infringements, data spills, system disruptions, and non-adherence to regulations. Data safety has thus turned into an institutional governance matter instead of a duty that can be allocated only to information-technology units.

Global research underlines that efficient data security relies on coordinated governance, well-defined decision rights, responsible leadership, integrated digital infrastructure, and ongoing risk management (Abraham et al., 2021; Sadiq et al., 2021). Digital conversion also necessitates organizational and managerial alteration, as fragmented systems and departmental barriers can undermine both operational effectiveness and security (Mergel et al., 2021; Wessel et al., 2021). Furthermore, the secrecy, wholeness, and usability of institutional data should be safeguarded via systematic controls and risk-centered management (International Organization for Standardization, 2022a, 2022b).

In China, the digitalization of higher education is bolstered by national modernization-oriented policies. Meanwhile, the Data Security Law and the Personal Information Protection Law set more explicit responsibilities for the legal collection, processing, storage, sharing, and safeguarding of data. Dali University has gradually incorporated digital platforms into academic matters, student-oriented services, personnel management, finances, research governance, and institutional administration. However, the growing interconnection has also brought about challenges related to responsibility assignment, system compatibility, access management, staff capabilities, and risk surveillance.

Current research frequently zero in on technological cybersecurity, privacy safeguarding, or overall data management. Fewer research works explore university data security within an educational-administration framework which combines management operations, governance mechanisms, decision-making processes, infrastructure elements, and risk management strategies. This research fills that void by evaluating five aspects of data security management at Dali University and transforming the results into practical development directives.

Research Significance

In theory, the research combines governance theory, information-security principles, risk-management theory, and educational administration into a five-aspect analytical framework: Educational Management Operations, Data Security Governance, Institutional Decision-Making Procedures, Digital Infrastructure Incorporation, and Data Risk Oversight. This conceptual framework views data security as a multi-faceted institutional function instead of a strictly technical problem.

From a practical perspective, the research determines the most robust and the least sturdy parts of the existing system and puts forward suggestions based on evidence for leadership, responsibility-taking, staff growth, making decisions, system unification, and constant risk management. The findings could also provide insights for comparable higher-education establishments in Yunnan Province and other areas going through digital transformation.

Research Questions

What is the present state of data security management at Dali University within the five research aspects?

Which significant issues and limiting factors impact the execution of data security governance?

What guidelines for development can be put forward based on quantitative results, qualitative proof, and relevant theories?

METHODOLOGY

Research Design and Participants

A design that combines multiple methods integrated a quantitative survey using questionnaires with qualitative interviews in-depth. The numerical part measured the general status and differences among dimensions, whereas the qualitative part accounted for practical issues and development requirements. Cross-verification between the two data sources enhanced the interpretation and backed the development of recommendations.

The group was made up of 290 administrators, educators, technical workers, and other individuals engaged in educational governance, digital systems, or data handling at Dali University. Employing the Krejcie and Morgan sampling table, 165 participants were chosen for the survey. Five crucial informants were deliberately chosen: the Head of the Information Technology Center, the Assistant Director of the Academic Affairs Office, an official from the University Data Management Office, the Assistant Director of the Network and Information Center, and an Educational Administration Staff member. Each one held direct duties related to governance, infrastructure, administration, or data safety.

Research Instruments

The survey form included demographic inquiries and 40 items on a five-point Likert scale, having eight items for every one of the five dimensions. Three professionals assessed content validity; Item-Objective Congruence figures varied from 0.67 to 1.00. An initial trial with 30 participants yielded an overall Cronbachs alpha of 0.916, suggesting strong internal consistency.

The somewhat-structured interview framework addressed leadership backing, staff instruction, duty assignment, policy execution, internal review, inter-departmental cooperation, staff involvement, digital-system incorporation, technological enhancement, risk evaluation, supervision, and emergency handling. It underwent review and revision to ensure alignment with the research aims.

Data Collection and Analysis

All 165 disseminated questionnaires were returned fully and validly, resulting in a 100% response rate. Interviews were carried out in person or via the internet after participants were made aware of the study's aim and confidentiality measures. Quantitative data underwent analysis via frequency, percentage, mean, and standard deviation. Qualitative data were transcribed, encoded, classified according to the five dimensions and newly-emerged themes, and combined with the survey results via content analysis.

RESULTS

Respondent Characteristics

Among the 165 individuals who responded, 56.36% were women and 43.64% were men. Administrators made up 36.97%, teachers constituted 35.15%, technical staff accounted for 20.61%, and other personnel accounted for 7.27%. Participants in the 30-39 age bracket made up the biggest age cohort (40.61%), succeeded by individuals below 30 (27.88%), those aged 40-49 (24.85%), and those aged 50 and older (6.67%). Individuals with a bachelors degree made up 59.39%, those with a masters degree 37.58%, and those with a doctoral degree 3.03%. The biggest work-experience cohort was 6 to 10 years (32.12%), succeeded by under five years (26.67%), 11 to 15 years (21.82%), 16 to 20 years (13.33%), and over 20 years (6.06%).

Overall Status and Dimensional Results

The average overall score was 3.36 (Standard Deviation = 0.64), suggesting a medium-level degree. The measurements were ranked in the following order: Educational Management Practices (Mean = 3.44, S.D. = 0.61), Data Security Governance (Mean = 3.43, S.D. = 0.63), Integration of Digital Infrastructure (Mean = 3.38, S.D. = 0.60), Processes of Institutional Decision-Making (Mean = 3.29, S.D. = 0.66), and Data Risk Management (Average = 3.25, S.D. = 0.68). Therefore,

Dali University has set up fundamental managerial, governance, and technological bases, yet decision-making and ongoing risk management are still relatively feeble.

Educational Management Practices

This dimension held the top-position at a medium degree (Mean = 3.44, S.D.= 0.61).Leaderships focus on data security had the highest score (Mean = 3.58, S.D.= 0.60), then came the allocation of responsibilities (Mean = 3.51, S.D.= 0.59).Ordinary staff training had the lowest score (Mean = 3.28, S.D.= 0.70).The results show that the awareness of leadership is more prominent than the institutionalized nature of training, the standardized execution, and the continual administrative enhancement.

Data Security Governance

Data Protection Governance placed second (Mean = 3.43, S.D.= 0.63).Adherence to national data-security regulations obtained the highest score (Mean = 3.62, S.D.= 0.56), whereas routine assessment of the governance framework received the lowest score (Mean = 3.28, S.D.= 0.70).Thus, policies and legal consciousness are relatively well-developed. However, internal auditing, clarification of accountability, consistency in implementation, and closed-loop evaluation need enhancement.

Institutional Decision-Making Processes

This category placed fourth (Average = 3.29, Standard Deviation)= 0.66).Incorporation of data security within strategic planning obtained the highest score (Mean = 3.41, S.D.= 0.64), followed by the involvement of senior-administrators (Mean = 3.36, S.D.= 0.63).Regard for staff input received the lowest score (Mean = 3.13, S.D.= 0.74), and the appropriate allocation of resources was also lacking (Mean = 3.21, S.D.= 0.72).Decision-making process is still characterized by a relatively top-down model, accompanied by restricted participation from front-line staff and inter-departmental consultation.

Digital Infrastructure Integration

Digital Infrastructure Incorporation placed third (Mean = 3.38, S.D.= 0.60).Dependable backup and restoration systems received the highest scores (Mean = 3.48, S.D.= 0.57), whereas routine system updates received the lowest score (Mean = 3.26, S.D.= 0.68).Current systems typically back routine operations. However, out-dated platforms, non-uniform standards, inadequate interoperability, and restricted technical support still bring about risks.

Data Risk Management

Data Risk Management obtained the lowest average (Average = 3.25, S.D.= 0.68).Emergency-preparedness planning received the highest score (Mean = 3.36, S.D.= 0.64), whereas continuous enhancement relying on incidents and assessment outcomes received the lowest score (Mean = 3.14, S.D.= 0.75).The present way is more concentrated on fundamental prevention and reaction rather than on a full-fledged cycle of recognition, appraisal, treatment, surveillance, review, and organizational learning.

Main Problems Identified in Interviews

At the institutional stage, duties stay fragmented. Department-wise standards are non-consistent, and governance assessment and auditing are not well-systematized.At the operational stage, inter-department cooperation is lacking. Systems are built independently. Staff input isnt uniformly integrated, and certain platforms are obsolete.At the staff level, consistent training is not completely institutionalized. Data security is still regarded by certain employees as mainly an IT obligation, and specialized staff and career-advancement opportunities are restricted.

DISCUSSION

Overall Interpretation

The overall moderate level indicates that Dali University is shifting from the initial stage of digital utilization to a more developed phase of institutional data governance.Rules, obligations, backup systems, monitoring processes, and contingency plans are already set up, showing that the

university has formed a basic understanding of data security and has started to build the required administrative and technical bases. However, these components have not been completely incorporated into a unified and constantly enhancing institutional framework. The present pattern can thus be summed up as basic foundations established, but system integration insufficient.

This discovery shows that the primary obstacle is no longer the total lack of data security steps, but instead the fragmentation and non-uniform execution of current measures. Different divisions might possess their own processes, technological platforms, and duty arrangements. However, these may not always function in line with uniform university-wide criteria. Consequently, disparities might appear in data sharing, responsibility, system compatibility, and policy implementation. The comparatively feeble performance of institutional decision-making and data risk management additionally implies that the university's present system is still somewhat responsive. It places more focus on dealing with incidents rather than foreseeing risks, synchronizing decisions, and learning in a systematic manner from prior events.

This outcome backs the governance-centered perspective stating that data security demands coordinated leadership, well-defined accountability, efficient policy execution, technological safeguards, and ongoing risk management (Abraham et al., 2021; Sadiq et al., 2021). It further validates that solely relying on technical safeguards won't guarantee confidentiality, integrity, and availability unless they are incorporated into efficient institutional processes (International Organization for Standardization, 2022a). In actual operation, even well-developed systems might be unable to safeguard institutional data when the responsibilities are indistinct, the staff members have insufficient training, or the departments don't coordinate their work. Therefore, the advancement of data security management at Dali University ought to emphasize not merely on additional technological input, but also on enhancing governance integration, employee involvement, cross-department collaboration, policy assessment, and continuous organizational learning.

Differences among Dimensions

The fairly robust performance of Educational Management Approaches and Data Security Governance shows increasing leadership focus and regulatory coercion. Strategic guidance and coordinated management are key factors promoting digital transformation and institutional robustness (Bryson et al., 2021; Tangi et al., 2021). However, the lower scores in terms of training, auditing, and evaluation indicate a disparity between policy commitment and the operational institutionalization.

Digital Infrastructure Fusion holds an intermediate stance. Backup and restoration mechanisms offer a fundamental level of accessibility, yet fragmented systems and non-uniform standards mirror a wider disparity between adopting technology and attaining true organizational change (Mergel et al., 2021; Wessel et al., 2021). Unified framework, management of the lifecycle, and secure exchange of data are thus crucial.

Institutional decision-making and data risk control are the primary bottlenecks. According to limited staff feedback, there is a hierarchical decision-making framework. In contrast, governance based on evidence and participation can enhance the quality and acceptance of policies (Janssen et al., 2022; Gil-Garcia et al., 2022). The score of low risk management implies a reactive approach instead of an adaptive model. Risk management needs to function continuously via identification, evaluation, handling, surveillance, examination, and enhancement (International Organization for Standardization, 2022b; National Institute of Standards and Technology, 2022).

Theoretical and Practical Implications

The research verifies that the data security of universities is a multi-faceted educational-governance matter which encompasses leadership, power, responsibility, decision-making, infrastructure, and ongoing risk management. The five-dimensional framework broadens research beyond mere technical cybersecurity aspects and presents an integrated foundation for institutional evaluation.

In practice, the improvement process should be carried out in phases. Immediate-term priorities involve staff skill-building, duty delineation, response systems, inspection, and regular surveillance. Medium-range priorities consist of inter-departmental governance, resource distribution, system incorporation, and routine assessment. Sustained development calls for a university-wide framework that combines policy, personnel, technology, decision-making, monitoring, and organizational learning.

DEVELOPMENT GUIDELINES

Strengthen Leadership and Staff Capacity

Universities should integrate data security into their strategic design, yearly administrative focus points, and department-level performance appraisals. High-ranking leaders ought to explicitly convey that data security represents a collective institutional obligation instead of a duty restricted to technical units. They ought to offer adequate financial, technological, and human resources, set up distinct supervisory mechanisms, and routinely assess the execution of data security policies. A training system for specific roles ought to encompass privacy safeguarding, secure management of data, access regulation, phishing avoidance, cloud safety, incident disclosure, and related laws and regulations. The content of training ought to be distinguished according to the duties of administrators, teachers, technical personnel, and system managers. Hands-on exercises, case studies, and regular evaluations ought to be incorporated to enhance staff awareness and operational proficiency. The outcomes of training completion and assessment need to be integrated into staff development initiatives, annual evaluations, and department-level assessments to guarantee continuous involvement and responsibility.

Establish Unified Governance and Accountability

An institution-wide data security governance committee ought to be set up to synchronize academic business, information tech, network management, human resources, finance, research governance, and student support. The panel ought to establish shared institutional criteria, settle cross-departmental disputes, and make sure that data security prerequisites are uniformly executed throughout all units. Ownership of data, authority for decision-making, responsibility for operations, procedures for approval, channels for reporting, and requirements for accountability need to be officially documented and conveyed to relevant staff. Every department ought to have a clear understanding of its function in data gathering, storage, access, sharing, and safeguarding. Furthermore, a closed-loop governance system ought to link policy creation, execution, supervision, inspection, assessment, responsibility assignment, and modification. Periodic assessments need to pinpoint implementation disparities, allocate corrective duties, and guarantee that policies are revised in light of novel technologies, regulations, and emerging hazards.

Improve Participatory Decision-Making

Administrative divisions, teaching entities, technical squads, and system users ought to take part in policy deliberation and significant system-development determinations. Their participation can assist in making sure that policies mirror operational actualities, user requirements, and technical limitations instead of relying solely on top-down administrative determinations. A standardized feedback mechanism ought to encompass issue submission, categorization and assessment, departmental reply, execution tracking, and ultimate outcome feedback. Specific clear deadlines for responses and the responsible entities are to be set to enhance transparency and accountability. Significant decisions ought to be backed up by risk appraisals, technical assessments, cost examinations, legal inspections, and operational proof. Regular advisory meetings, pilot experimentation, and post-implementation appraisals should be put in place so that policies and systems can be constantly adjusted according to practical experience and feedback from stakeholders.

Integrate Digital Infrastructure

The university ought to establish unified technological standards for information systems, databases, digital platforms, identity verification, access management, security supervision, and data sharing. These criteria ought to be implemented throughout departments to minimize replicated systems, non-uniform configurations, and segregated data environments. An architecture across the university should likewise specify how various platforms link, what data is able to be shared, who has the authorization to access it, and how access actions are documented and examined. Integrated identity management, role-centric access control, secure app interfaces, and centralized surveillance can enhance both operational effectiveness and data safeguarding.

Legacy systems ought to be given priority for upgrading in line with their security threats, operational significance, compatibility, and upkeep expenses. Systems which hold sensitive student, staff, financial, or research-related data ought to get specific attention. Prior to replacement or upgrading, the university needs to carry out technical and security evaluations to pinpoint vulnerabilities, integration challenges, and possible impacts on users. New systems ought to adhere to common standards right from the design phase to prevent the formation of extra information silos.

Infrastructure management ought to span the whole systems lifespan, encompassing acquisition, design, construction, testing, roll-out, functioning, upkeep, enhancement, backup, restoration, and decommissioning. Procurement contracts and acceptance procedures ought to incorporate security requirements. Periodic vulnerability assessments, patch upkeep, configuration examinations, backup validations, and recovery drills should be carried out. When systems reach their end-of-life, institutional data must be safely transferred, stored, or disposed of in line with approved protocols. Establish clear channels for technical support to enable users to report issues with the system and obtain prompt assistance.

Establish Continuous Risk Management

A comprehensive risk-management process for systematic risks should include risk recognition, evaluation, ranking, handling, surveillance, reporting, examination, and ongoing enhancement. This loop ought to be incorporated into regular university administration instead of being carried out merely after security occurrences. Regular evaluations ought to encompass key information systems, confidential datasets, cloud-based platforms, third-party providers services, mobile apps, and newly created digital initiatives. Risk evaluations should be carried out prior to the introduction of new technologies or the alteration of significant systems.

A centralized risk log ought to record recognized risks, impacted systems, accountable departments, risk tiers, handling measures, execution deadlines, advancement, and review outcomes. High-jeopardy problems ought to be reported to top-level administrators and monitored until suitable corrective steps are finished. Standardize monitoring indicators and reporting procedures to enable departments to detect abnormal activities and emerging threats in the early phase.

Security events, internal reviews, compliance checks, and emergency drills should be succeeded by formal root-cause examination. The results ought to be applied to modify policies, enhance technical controls, specify responsibilities, better response procedures, and renew staff-training material. Via this unceasing learning procedure, the university is able to shift from reactive incident management to proactive prevention, adaptable management, and long-term institutional robustness.

CONCLUSION

This research discovered that data security administration at Dali University was at a medium level overall. There was better performance in Educational Management Practices and Data Security Governance, while poorer performance in Institutional Decision-making and Data Risk Management. The findings suggest that the university has set up a fundamental policy,

management, and technological basis. However, in terms of responsibilities, involvement, system consolidation, staff competence, and ongoing enhancement, there are still inadequacies.

Five specific guidelines were put forward: enhance leadership and staff capabilities; set up unified governance and responsibility systems; better participatory and evidence-driven decision-making; combine digital infrastructure and lifecycle administration; and carry out continuous data risk control. Collectively, these steps can change data security from a department-centered technical role into a university-wide governance duty and back up confidentiality, integrity, availability, and long-term digital transformation.

The research presents an integrated five-dimension framework and empirical proof from a Chinese higher-education setting. Even though the results are specific to the institution, they might offer a valuable reference for universities that are encountering comparable governance and digital-transformation difficulties.

REFERENCE

- Abraham, R., Schneider, J., & vom Brocke, J. (2021). Data governance: A conceptual framework and research agenda. *International Journal of Information Management*, 60, 102376. <https://doi.org/10.1016/j.ijinfomgt.2021.102376>
- Alenezi, M., Tarhini, A., & Sharma, S. K. (2023). Development of a cybersecurity framework for higher education institutions. *Computers & Security*, 122, 102890. <https://doi.org/10.1016/j.cose.2022.102890>
- Bryson, J. M., Crosby, B. C., & Bloomberg, L. (2021). Public value governance: Moving beyond traditional public administration and the New Public Management. *Public Administration Review*, 81(2), 309–322. <https://doi.org/10.1111/puar.13372>
- Gil-Garcia, J. R., Zhang, J., & Puron-Cid, G. (2022). Smart governance and public sector digital transformation. *Government Information Quarterly*, 39(4), 101742. <https://doi.org/10.1016/j.giq.2022.101742>
- International Organization for Standardization. (2022a). ISO/IEC 27001:2022 information security, cybersecurity and privacy protection—Information security management systems. ISO.
- International Organization for Standardization. (2022b). ISO/IEC 27005:2022 information security risk management. ISO.
- Janssen, M., van der Voort, H., & Wahyudi, A. (2022). Factors influencing big data decision-making quality. *Government Information Quarterly*, 39(2), 101646. <https://doi.org/10.1016/j.giq.2021.101646>
- Mergel, I., Edelmann, N., & Haug, N. (2021). Defining digital transformation: Results from expert interviews. *Government Information Quarterly*, 38(4), 101589. <https://doi.org/10.1016/j.giq.2021.101589>
- National Institute of Standards and Technology. (2022). Risk management framework for information systems and organizations (SP 800-37 Rev. 2). U.S. Department of Commerce.
- Otto, B. (2022). Data governance. *Business & Information Systems Engineering*, 64(4), 507–513. <https://doi.org/10.1007/s12599-022-00778-9>
- Sadiq, S., Indulska, M., & Green, P. (2021). Data governance: A conceptual framework and implications for organizations. *Journal of Strategic Information Systems*, 30(3), 101694. <https://doi.org/10.1016/j.jsis.2021.101694>
- Tangi, L., Janssen, M., Benedetti, M., & Noci, G. (2021). Digital government transformation: A structural equation modelling analysis of driving and hindering factors. *International Journal of Information Management*, 60, 102356. <https://doi.org/10.1016/j.ijinfomgt.2021.102356>
- Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, 13(2), 39. <https://doi.org/10.3390/fi13020039>

- United Nations Educational, Scientific and Cultural Organization. (2023). Digital transformation in education: Policy guidance. UNESCO Publishing.
- Wessel, L., Baiyere, A., Ologeanu-Taddei, R., Cha, J., & Jensen, T. B. (2021). Unpacking the difference between digital transformation and IT-enabled organizational transformation. *Journal of the Association for Information Systems*, 22(1), 102–129. <https://doi.org/10.17705/1JAIS.05831>
- Yusif, S., & Hafeez-Baig, A. (2023). Cybersecurity policy compliance in higher education: A theoretical framework. *Journal of Applied Security Research*, 18(2), 267–288. <https://doi.org/10.1080/19361610.2021.1989271>

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Conflicts of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.



Copyright: © 2026 by the authors. This is a fully open-access article distributed under the terms of the Attribution-NonCommercial-NoDerivatives 4.0 International (CC BY-NC-ND 4.0).