J-MS
JOURNAL MOBILE TECHNOLOGIES

Received: 1 Aug 2025 | Revised: 10 Aug 2025 | Accepted: 1 Sep 2025 | Published: 10 Sep 2025 E-ISSN: 2986-478X, P-ISSN: 2986-1535

DOI: 10.59431/jms.v3i2.633

RESEARCH ARTICLE

Cloud Storage Ethics in Industrial Engineering: A Comparative Analysis of Microsoft OneDrive and SharePoint

Riki Afrianto [1*] | Sari Nusivera [2] | Hikam Haikal [3]

[1*,2,3] Department of Information Technology, Swiss German University, Tangerang 15143, Indonesia.

Correspondence

[1*] Department of Information Technology, Swiss German University, Tangerang 15143, Indonesia.
Email: Afrianto.riki@gmail.com.

Funding information
Swiss German University.

Abstract
This study investigates the technical, ethical, and organizational implications of adopting Microsoft OneDrive and SharePoint within industrial engineering. Both platforms operate under Microsoft's enterprise cloud infrastructure but differ significantly in governance design and ethical alignment. SharePoint's hierarchical structure enables effective compliance, accountability, and workflow automation, making it suitable for regulated industrial environments. In contrast, OneDrive prioritizes user flexibility and mobility, which, while enhancing convenience, increases risks related to data misuse, shadow IT, and inconsistent policy adherence. Through a qualitative descriptive approach involving practitioners and academic users, the study identifies that organizational ethics, privacy management, and governance transparency are decisive factors in maintaining digital integrity. The findings indicate that technical safeguards such as encryption and access control must be reinforced by ethical responsibility and user education. Furthermore, sustainable cloud governance requires continuous monitoring, multi-factor authentication, and transparent data policies that respect user privacy and organizational accountability. The study concludes that OneDrive and SharePoint should function as complementary systems—balancing autonomy with oversight—to promote ethical, secure, and efficient collaboration in industrial digital ecosystems.

Keywords
Cloud Governance; Ethics; Industrial Engineering; Data Privacy; OneDrive–SharePoint.

1 | INTRODUCTION

Cloud storage and online collaboration technologies have become integral to modern industrial engineering operations, supporting the exchange of design data, production reports, and project documentation across geographically dispersed teams. Among the most prevalent tools, Microsoft OneDrive and SharePoint enable flexible yet structured digital collaboration within industrial ecosystems. OneDrive for Business provides users with extensive personal storage and device synchronization, while SharePoint offers centralized document governance, version control, and workflow automation. These systems now host critical corporate assets—including intellectual property and client data—with a 2020 Cloud Security Alliance survey revealing that nearly 70% of organizations store their most sensitive information on Microsoft's cloud platforms (Cloud Security Alliance, 2020). However, as cloud adoption expands, ethical and governance

challenges become increasingly pronounced. Concerns regarding privacy, data protection, access control, and user accountability remain central to debates surrounding digital responsibility. Scholars contend that both service providers and end-users share moral duties in ensuring transparency, fairness, and accountability within cloud ecosystems (de Bruin & Floridi, 2017; Dhirani *et al*., 2023). Technical safeguards—such as encryption, multi-factor authentication, and automated compliance controls—represent key defenses but are insufficient without ethical alignment and regulatory consistency (Dawood *et al*., 2023; Issaoui *et al*., 2023). Microsoft integrates such mechanisms across OneDrive and SharePoint; however, their contrasting structures—user-centric versus organization-centric—create distinct ethical dynamics. OneDrive prioritizes individual flexibility, heightening the risk of inconsistent governance, while SharePoint's centralized framework strengthens compliance but may reduce user autonomy (Freitas *et al*., 2025; Al-Ruithe *et al*., 2019). In engineering environments, this dichotomy reflects broader Industry 4.0 trends, where digital platforms must balance scalability and governance to sustain operational integrity (Gharibvand *et al*., 2024; Li *et al*., 2024). This study therefore examines the technical and ethical distinctions between OneDrive and SharePoint, and investigates how organizational practices, regulatory frameworks, and user behavior influence the ethical use of cloud storage in industrial engineering. It further hypothesizes that SharePoint's embedded governance tools—such as hierarchical permissions and automated workflows—are better aligned with ethical data management principles, whereas OneDrive's flexibility demands stronger individual discipline and oversight to prevent misuse (Bednar *et al*., 2020; Yang *et al*., 2025; Mettler, 2024).

2 | BACKGROUND THEORY

The transformation of industrial engineering has been profoundly shaped by the framework of Industry 4.0, which integrates cyber-physical systems, Internet of Things (IoT), and cloud computing to redefine the structure and operation of production systems. Within this paradigm, Cloud-Based Manufacturing (CMfg) emerges as a key innovation that allows manufacturing resources and capabilities to be virtualized, shared, and managed across organizational boundaries. Gharibvand *et al*. (2024) provide a comprehensive examination of CMfg and demonstrate how cloud integration supports scalability, cost efficiency, and operational responsiveness. Their findings show that CMfg systems leverage technologies such as artificial intelligence, RFID, 3D printing, and big data analytics to enable real-time decision-making and production agility. Nevertheless, these benefits are accompanied by complex integration challenges, as manufacturing environments often depend on heterogeneous infrastructures and legacy systems. The core challenge, therefore, lies not only in harmonizing these diverse technologies but also in ensuring that cloud-based systems remain secure, reliable, and ethically governed. This challenge is analogous to the operational dynamics of Microsoft OneDrive and SharePoint in industrial contexts, where balancing user flexibility with centralized governance becomes essential to maintaining both productivity and ethical integrity. While efficiency remains a central driver of cloud adoption, ethical dilemmas and privacy challenges continue to dominate academic discourse. Dhirani *et al*. (2023) argue that cloud services, as a form of emerging technology, create deep ethical ambiguities, particularly concerning data ownership and governance. They identify three principal risks: first, ambiguous service agreements that obscure how user data is collected, stored, and processed; second, weak governance policies that are inconsistently implemented across organizations; and third, a lack of transparency that diminishes user trust and impedes informed consent. These issues are particularly relevant to industrial engineering, where cloud platforms often host sensitive assets such as intellectual property, client databases, and confidential design files. Failure to address these risks can lead to ethical breaches, financial loss, and reputational damage. Consequently, Dhirani *et al*. emphasize that ethical responsibility cannot be confined to compliance with existing regulations. Instead, organizations must embed principles of fairness, accountability, and transparency into their cloud governance frameworks to sustain user trust and organizational accountability.

Building on the ethical perspective, Dhinakaran *et al*. (2024) expand the discussion by introducing technical mechanisms for privacy preservation in IoT-enabled cloud systems. Their survey identifies several strategies applicable to industrial practice, including the implementation of encryption techniques (such as homomorphic encryption and lightweight ciphers) to secure sensitive industrial data, anonymization frameworks to prevent re-identification in shared datasets, and AI-driven access control systems capable of dynamically detecting and limiting unauthorized access. While these mechanisms enhance data protection, they must be carefully adapted to the unique scale and complexity of industrial environments, which involve high data volume, velocity, and variety. In this sense, platforms such as OneDrive and SharePoint can strengthen their ethical and technical reliability by incorporating these privacy-preserving solutions directly into their architectures, rather than relying solely on administrative or policy-based controls. Parallel to these discussions, Li *et al*. (2024) emphasize the importance of cloud service composition and optimization in intelligent manufacturing. Their review argues that successful adoption of cloud technology requires not merely deploying individual tools but integrating them into coherent frameworks that optimize interoperability, performance, and governance. The study outlines key optimization indicators—quality of service, cost efficiency, latency reduction, and compliance with security standards—as essential metrics for

evaluating industrial cloud systems. By treating cloud platforms such as OneDrive and SharePoint as interconnected components of a larger industrial ecosystem, organizations can align operational performance with ethical and compliance objectives, ensuring that technological advancement supports both efficiency and responsibility. Taken together, these studies reveal the multifaceted character of cloud adoption in industrial engineering. The literature suggests four interconnected dimensions that must be addressed holistically: (1) the technological promise of scalability and cost efficiency offered by CMfg (Gharibvand *et al*., 2024); (2) ethical uncertainty stemming from weak governance and opaque data policies (Dhirani *et al*., 2023); (3) the necessity of privacy-preserving mechanisms to safeguard data integrity (Dhinakaran *et al*., 2024); and (4) the optimization frameworks needed to ensure cloud systems operate ethically and effectively within industrial ecosystems (Li *et al*., 2024). This synthesis highlights that cloud technology in industrial engineering cannot be assessed solely through its technical merits. Instead, a balanced approach that integrates technological, ethical, and organizational perspectives is vital to achieving secure and sustainable digital transformation.

Table 1. Summary of Key Studies Reviewed in the Background Theory

Author(s)	Year	Focus Area	Key Findings / Contributions
Gharibvand *et al*.	2024	Cloud-Based Manufacturing (CMfg)	Demonstrates that CMfg enhances scalability and cost efficiency but faces challenges in integration and ethical governance.
Dhirani *et al*.	2023	Ethics & Privacy in Emerging Tech	Identifies ethical risks in cloud systems, including ambiguous service agreements and limited transparency.
Dhinakaran *et al*.	2024	Privacy in IoT-Cloud Systems	Reviews encryption, anonymization, and AI-based access control to enhance privacy and data security.
Li, Liu, & Shi	2024	Cloud Service Composition	Defines optimization indicators for cloud service orchestration, focusing on efficiency, compliance, and security.

In summary, the reviewed literature indicates that industrial adoption of cloud technologies requires a dual emphasis on technical optimization and ethical accountability. While previous studies have explored various aspects of cloud integration, few have conducted direct comparisons between enterprise platforms such as OneDrive and SharePoint. Given their extensive adoption in industrial engineering, a comparative study is essential to evaluate how these platforms address both technical dimensions—such as scalability, interoperability, and system optimization—and ethical imperatives including privacy, transparency, and governance. This research, therefore, seeks to bridge that gap by analyzing how OneDrive and SharePoint align with the broader technological and moral responsibilities embedded in Industry 4.0-driven industrial environments.

3 | METHOD

This study adopted a qualitative descriptive design combined with comparative analysis to examine the technical and ethical dimensions of using Microsoft OneDrive and SharePoint in industrial engineering contexts. The qualitative approach was deemed appropriate because the aim of this research was to obtain an in-depth understanding of how these platforms differ not only in their technical features but also in the ethical implications that arise from their adoption in real-world professional settings. Unlike quantitative assessments that emphasize numerical measurement, this approach focuses on the interpretation of user experiences, behavioral patterns, and governance practices. The study population included industrial engineering practitioners, university lecturers, and postgraduate students who regularly utilize cloud storage applications in their professional and academic activities. A purposive sampling technique was applied to select 20 respondents who had at least six months of experience with either OneDrive or SharePoint, ensuring that participants possessed sufficient familiarity to provide informed insights into their technical performance and ethical management practices. Data were obtained through three primary instruments: semi-structured questionnaires, in-depth interviews, and literature documentation. The questionnaire focused on indicators such as data security, ease of collaboration, transparency, ethical responsibility, and compliance with regulatory standards. In-depth interviews were conducted online, each lasting approximately 30–45 minutes, to capture participants' perceptions of ethical challenges—particularly regarding privacy, governance, and accountability in data handling. The literature review complemented empirical findings by drawing on scholarly sources and technical reports to contextualize results within broader industrial and technological discussions. References included studies on data governance (Al-Ruithe *et al*., 2019), privacy engineering (Bednar *et al*., 2020), and ethical frameworks for cloud adoption (de Bruin & Floridi, 2017; Dhirani *et al*., 2023), alongside analyses of cloud service integration (Gharibvand *et al*., 2024; Li *et al*., 2024) and industrial data management

(Freitas *et al*., 2025).

Data analysis followed a thematic procedure that involved transcription, coding, and categorization to identify recurrent themes and relationships among variables. Responses were grouped under core categories including security management, data governance, ethical behavior, and compliance mechanisms. Descriptive statistics were used to summarize quantitative data from questionnaires, while qualitative interview data were analyzed inductively to interpret user narratives and identify patterns of ethical awareness and technological application. The process of comparative analysis between OneDrive and SharePoint emphasized differences in user autonomy, access control, and organizational oversight. These findings were further aligned with the theoretical frameworks of vendor dependency and cybersecurity risk, as discussed by Opara-Martins *et al*. (2016) and Dawood *et al*. (2023), to explore how dependency on a single cloud provider and increasing cyber vulnerabilities can influence ethical decision-making in industrial contexts. Opara-Martins *et al*. (2016) warn that vendor lock-in may limit an organization's ability to migrate data or enforce independent governance policies, potentially compromising ethical accountability. Similarly, Dawood *et al*. (2023) emphasize that technical safeguards such as encryption and authentication are necessary but insufficient without continuous organizational oversight and ethical responsibility in data stewardship. Ethical considerations were integral to this study. All participants provided informed consent prior to involvement, and their identities were anonymized to ensure confidentiality. Participation was voluntary, and respondents could withdraw at any point without consequence. These measures align with international research ethics standards emphasizing respect, transparency, and autonomy. Nevertheless, the study recognizes certain limitations, including the relatively small sample size and the predominance of participants from academic environments, which may restrict the generalizability of findings to broader industrial settings. Despite these constraints, the methodological rigor—supported by triangulation of data sources, literature integration, and thematic depth—provides a robust foundation for analyzing the ethical and technical implications of cloud storage systems in industrial engineering.

4 | RESULTS AND DISCUSSION

4.1 Results

The study identified several dimensions of difference between Microsoft OneDrive and SharePoint in industrial engineering contexts, namely: technical risk, organizational impact, technical infrastructure, ethical implications, governance and compliance, and organizational usage. The results demonstrate that while both platforms operate within the same Microsoft 365 ecosystem, they represent distinct paradigms of cloud utilization. OneDrive emphasizes personal autonomy, flexibility, and user control, whereas SharePoint prioritizes centralized management, collaboration, and compliance assurance. In terms of technical risk, both platforms employ encryption at rest and in transit, yet their security performance is contingent upon user and organizational implementation. As observed by Dawood *et al*. (2023), weaknesses in encryption key management and identity and access management (IAM) remain primary sources of vulnerability in cloud environments. Human error—such as key misplacement or improper configuration—poses as great a risk as external attacks. OneDrive, due to its user-centric nature, is more exposed to individual mismanagement, while SharePoint's centralized governance structure provides greater administrative oversight. The findings further reveal notable social and organizational impacts. Opara-Martins *et al*. (2016) found that vendor lock-in constitutes a major challenge in cloud adoption due to proprietary formats and limited interoperability. Industrial firms dependent on Microsoft ecosystems often face restricted data portability, constraining strategic flexibility. Conversely, as Yang *et al*. (2025) highlight, cloud integration enhances collaboration and accelerates supply chain responsiveness. Yet, this openness requires robust governance to prevent overexposure of proprietary data. In addition, Mettler (2024) points out that enhanced monitoring features in cloud systems blur the boundary between transparency and surveillance, raising concerns about privacy and trust in the "connected workplace."

The comparative technical infrastructure of both platforms aligns with their functional intentions. OneDrive serves as a personal workspace focused on synchronization and device mobility, whereas SharePoint offers enterprise-level document management with metadata control, hierarchical permissions, and workflow automation (Freitas *et al*., 2025). Both platforms share Microsoft's global cloud backbone, ensuring high availability and redundancy, though their differing governance structures influence organizational deployment strategies. From an ethical standpoint, the study finds that privacy and jurisdictional concerns persist across both systems. OneDrive's decentralized control leaves users dependent on Microsoft's transparency regarding data handling, echoing Dhirani *et al*. (2023), who note that users often lack clarity over where and how their data is stored. SharePoint's centralized model improves accountability but shifts ethical responsibility toward the organization itself. Cross-border data storage adds further complexity; Issaoui *et al*. (2023) demonstrate that conflicting international regulations—such as GDPR versus the U.S. CLOUD Act—create legal ambiguity in determining data

access rights. Regarding governance and compliance, both systems provide extensive security and auditing tools but differ in oversight models. SharePoint aligns more naturally with compliance frameworks like ISO/IEC 27001 and GDPR, offering built-in audit trails, permission hierarchies, and workflow automation (Issaoui *et al*., 2023; Dhirani *et al*., 2023). OneDrive, while compliant at the technical level, relies heavily on user discipline and supplementary policy enforcement. Organizations that fail to formalize governance processes, as noted by Al-Ruithe *et al*. (2019), risk fragmented data management and reduced accountability. Finally, organizational usage results indicate that OneDrive and SharePoint function best as complementary systems rather than substitutes. OneDrive supports individual productivity and draft work, while SharePoint ensures document traceability and organizational coherence. When integrated through proper governance, the two platforms form a balanced cloud ecosystem that supports both flexibility and regulatory compliance (Freitas *et al*., 2025; Al-Ruithe *et al*., 2019).

Table 2. Comparative Analysis of Microsoft OneDrive and SharePoint in Industrial Engineering

Dimension	Microsoft OneDrive	Microsoft SharePoint
Primary Use Case	Personal cloud storage and file sharing	Enterprise collaboration and document governance
Access Control	File/folder level; user-managed	Role-based, hierarchical; centrally administered
Governance Tools	Limited to admin settings and retention policies	Integrated workflows, metadata, audit logs
Privacy Risk	Higher—perceived personal space may lead to misuse	Lower—transparent structure enables accountability
Adoption Barriers	Low—high usability, minimal training required	High—requires structured training and planning
Compliance Suitability	Moderate—dependent on external policy enforcement	High—built-in ISO/GDPR-aligned compliance features
Ethical Alignment	Weaker—relies on user responsibility and vendor transparency	Stronger—emphasizes centralized governance and oversight

4.2 Discussion

The findings affirm that technological and ethical considerations in cloud storage are inseparable from governance and organizational culture. OneDrive's flexibility supports decentralized innovation but amplifies risks tied to personal mismanagement and limited oversight. SharePoint, by contrast, embeds accountability into its architecture, aligning with the principles of ethical engineering governance identified by de Bruin and Floridi (2017). This distinction underscores the trade-off between autonomy and control in digital infrastructures. Technical risks identified by Dawood *et al*. (2023) illustrate that even advanced systems remain vulnerable when human oversight falters. Effective mitigation requires adopting layered security mechanisms, such as MFA, conditional access, and secure key management, supported by continuous staff training. These findings resonate with Bednar *et al*. (2020), who argue that ethical engineering must incorporate "privacy-by-design" principles at both technical and behavioral levels. From a socio-organizational perspective, the results suggest that cloud adoption reshapes power structures and accountability lines. Vendor lock-in (Opara-Martins *et al*., 2016) and over-centralized ecosystems can restrict autonomy, while insufficient governance frameworks foster ethical ambiguity. However, properly structured cloud ecosystems, as seen in SharePoint deployments, can reinforce transparency, coordination, and compliance. This aligns with Yang *et al*. (2025), who highlight the role of digital integration in enhancing supply chain resilience and operational efficiency.

Ethically, both platforms demand critical awareness of privacy, data jurisdiction, and lifecycle management. Dhirani *et al*. (2023) and Issaoui *et al*. (2023) highlight that unclear cross-border policies exacerbate risks of misuse and surveillance. As such, industrial firms must adopt dual-layered ethics frameworks—combining legal compliance with internal principles of fairness and accountability—to ensure that cloud use aligns with stakeholder rights. Governance emerges as the linchpin connecting technical and ethical integrity. Al-Ruithe *et al*. (2019) and Freitas *et al*. (2025) both demonstrate that structured data governance—supported by automation, access hierarchies, and audit systems—is essential to realizing the full potential of industrial cloud tools. Without coherent governance, even the most advanced platforms reproduce traditional inefficiencies under digital facades. In essence, OneDrive and SharePoint represent two ends of a governance spectrum: individual autonomy versus organizational structure. The optimal strategy for industrial engineering lies in their integration—a hybrid system in which OneDrive supports personal productivity and SharePoint enforces collective accountability. This balance ensures that cloud storage serves both human flexibility and institutional responsibility, advancing the ethical and operational sustainability of digital industry practices.

5 | CONCLUSIONS

This study underscores the intertwined ethical, technical, and organizational dimensions of cloud storage adoption within industrial engineering. Both Microsoft OneDrive and SharePoint provide robust enterprise-level security infrastructures; however, their contrasting governance architectures determine their suitability for different operational contexts. SharePoint's hierarchical control, audit mechanisms, and compliance integrations make it more appropriate for industries requiring strict regulatory adherence and ethical accountability. In contrast, OneDrive's design emphasizes user autonomy and flexibility, offering convenience and accessibility but exposing organizations to greater risks of misuse, shadow IT practices, and inconsistent alignment with corporate data governance standards. From an ethical standpoint, the findings highlight the necessity for organizations to balance efficiency with accountability. Productivity gains must not compromise privacy, data protection, or informed consent. Effective governance requires clear internal policies delineating which data types are suitable for each platform, along with mandatory safeguards such as encryption, least-privilege access, and role-based authorization. Sensitive or confidential engineering data should be confined to secure SharePoint environments, while OneDrive use must be restricted to non-confidential drafts or individual work files. Continuous employee education is essential to ensure awareness of ethical responsibilities, proper data handling, and compliance with institutional standards.

Moreover, the study emphasizes that technical safeguards alone are insufficient without strong organizational enforcement. Multi-factor authentication, periodic access audits, and restrictions on external sharing must be institutionalized through transparent governance frameworks. Ethical data practices should extend to employee privacy: personal files must not be accessed without explicit consent, and any monitoring activity must be conducted proportionally, with clear communication regarding its scope and purpose. Only through this balance of security, ethics, and transparency can organizations maintain trust and integrity in cloud-enabled environments. Future research should build upon these findings through empirical investigation of industrial organizations actively utilizing OneDrive and SharePoint. Subsequent studies could examine how user behavior, governance maturity, and ethical training programs influence compliance outcomes and risk mitigation. Longitudinal analyses would also be valuable in assessing the long-term effectiveness of organizational interventions and policy frameworks designed to align cloud storage technologies with ethical engineering principles and sustainable digital governance.

REFERENCES

Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2019). A systematic literature review of data governance and cloud data governance. *Personal and Ubiquitous Computing, 23*(5–6), 839–859. https://doi.org/10.1007/s00779-017-1104-3

Bednar, K., Spiekermann, S., Langheinrich, M., & Korunovska, J. (2020). Engineering privacy by design: Are engineers ready to live up to the challenge? *The Information Society, 36*(4), 256–277. https://doi.org/10.1080/01972243.2020.1769741

Cloud Security Alliance. (2020). *Cloud Security Alliance's CASB survey finds nearly 70% house their most sensitive data in Microsoft SharePoint Online / OneDrive*. https://cloudsecurityalliance.org

Dawood, M., *et al*. (2023). Cyberattacks and security of cloud computing: A complete guideline. *Symmetry, 15*(11), 1981. https://doi.org/10.3390/sym15111981

de Bruin, B., & Floridi, L. (2017). The ethics of cloud computing. *Science and Engineering Ethics, 23*(1), 21–39. https://doi.org/10.1007/s11948-016-9759-0

Dhinakaran, D., Udhaya Sankar, S. M., Selvaraj, D., & Edwin Raja, S. (2024). Privacy-preserving data in IoT-based cloud systems: A comprehensive survey with AI integration. *arXiv Preprint*. https://arxiv.org/abs/2401.00794

Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. *Sensors, 23*(3), 1151. https://doi.org/10.3390/s23031151

Freitas, N., Rocha, A. D., & Barata, J. (2025). Data management in industry: Concepts, systematic review and future directions. *Journal of Intelligent Manufacturing.* Advance online publication. https://doi.org/10.1007/s10845-025-02570-z

Gharibvand, V., *et al*. (2024). Cloud-based manufacturing: A review of recent developments in architectures, technologies, infrastructures, platforms and associated challenges. *The International Journal of Advanced Manufacturing Technology, 131*(1), 93–123. https://doi.org/10.1007/s00170-024-12989-y

Issaoui, A., Örtensjö, J., & Islam, M. S. (2023). Exploring the General Data Protection Regulation (GDPR) compliance in cloud services: Insights from Swedish public organizations on privacy compliance. *Future Business Journal, 9*(1), 107. https://doi.org/10.1186/s43093-023-00285-2

Li, C., Liu, L., & Shi, L. (2024). Review of cloud service composition for intelligent manufacturing. *arXiv Preprint*. https://arxiv.org/abs/2408.01795

Mettler, T. (2024). The connected workplace: Characteristics and social consequences of work surveillance in the age of datification, sensorization, and artificial intelligence. *Journal of Information Technology, 39*(3), 547–567. https://doi.org/10.1177/02683962231202535

Opara-Martins, J., Sahandi, R., & Tian, F. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. *Journal of Cloud Computing, 5*(1), 4. https://doi.org/10.1186/s13677-016-0054-z

Yang, D., Li, R., & Liu, S. (2025). Exploring the influence of cloud computing on supply chain performance: The mediating role of supply chain governance. *Journal of Theoretical and Applied Electronic Commerce Research, 20*(2), 70. https://doi.org/10.3390/jtaer20020070

How to cite this article: Afrianto, R., Nusivera, S., & Haikal, H. (2025). Cloud Storage Ethics in Industrial Engineering: A Comparative Analysis of Microsoft OneDrive and SharePoint. *Journal Mobile Technologies (JMS)*, *3*(2). https://doi.org/10.59431/jms.v3i2.633.