Jurnal Minfo Polgan
Volume 12, Nomor 2, September 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.13018 p-ISSN : 2089-9424

Terbit : 01 September 2023

Ethics-Based Leadership in Managing Information Security and Data Privacy

[1]Zuhri Halim, [2]Ngurah Pandji Mertha Agung Durya, [3]Kraugusteeliana Kraugusteeliana, [4]Suherlan, [5]Ayu Latifah Alfisyahrin
[1]Prodi Teknik Informatika, Universitas Muhammadiyah Prof. Dr. HAMKA, Indonesia
[2]Prodi Akuntansi, Universitas Dian Nuswantoro Semarang, Indonesia
[3]Prodi Sistem Informasi, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia
[4]Prodi Administrasi Publik, Universitas Subang, Indonesia
[5]Prodi Ekonomi Pembangunan dan Perbankan, Universitas Bosowa, Indonesia

[1]zuhri@uhamka.ac.id, [2]ngurahdurya@dsn.dinus.ac.id, [3]kraugusteeliana@upnvj.ac.id, [4]suherlanfia@gmail.com, [5]ayulatifah@universitasbosowa.ac.id

ABSTRACT

In the advancing digital age, technological transformation has created endless opportunities for efficiency, innovation and connectivity. However, behind these advancements lie significant challenges related to information security and data privacy. Adverse data breaches and cyber-attacks have reminded us of the vulnerabilities inherent in today's digital environment. Therefore, protecting information security and data privacy has become a top priority for organisations around the world. This research aims to explore how ethical leaders can influence decision-making and practices related to information security and data privacy. This research is a literature review that adopts a qualitative method approach, which means it will analyse and interpret data by relying on information and text from various sources. The study results arrive at a statement that ethical leaders ensure that technical aspects and ethical values go hand in hand in making decisions related to information security and data privacy. Through ethics-based leadership, organisations are able to build a culture that cares about data privacy, create a secure and transparent environment for customers and users, and comply with increasingly stringent regulations. The trust of customers and business partners built through ethical practices in information and data management will be a competitive advantage for organisations in the ever-changing digital age.

Keywords: Leadership, Ethics, Information Security, Data Privacy

INTRODUCTION

In the era of rapid digital advancements, the proliferation of technology has given rise to a multitude of possibilities in terms of enhanced productivity, novel ideas, and interconnectedness (Wahyoedi et al., 2023). Nevertheless, the progress made in these areas is accompanied with notable obstacles pertaining to the domains of information security and data privacy. The occurrence of detrimental data breaches and cyber-attacks has served as a reminder of the inherent vulnerabilities present in the contemporary digital landscape (Gadzali et al., 2023). Consequently, safeguarding information security and preserving data privacy has emerged as a crucial concern for enterprises everywhere (Fabrègue & Bogoni, 2023).

Given the prevailing difficulties, it is evident that ethics-based leadership is increasingly being recognised as a robust framework for effectively managing information security and data privacy. Leaders who use ethics as a guiding principle in their decision-making process demonstrate a comprehensive approach that encompasses not only technical and business considerations, but

Jurnal Minfo Polgan
Volume 12, Nomor 2, September 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.13018 p-ISSN : 2089-9424

also takes into account the broader social and moral implications of their actions (Scholl et al., 2016). Effective leadership not only upholds the integrity of the company, but also guarantees the incorporation of ethical ideals throughout a wide range of operations pertaining to information security (Basir et al., 2023).

The significance of leadership rooted in ethical principles in the management of information security and data privacy is evident across multiple dimensions. To begin with, there is a growing interconnection between technical issues and moral and ethical principles. The ethical ramifications of actions such as data gathering, processing, and storage extend beyond their technological dimensions (Touriano et al., 2023). Ethical leaders are responsible for not only ensuring the reliability of technology, but also for implementing norms that take into account the privacy rights of individuals (Guo, 2022).

Additionally, it is crucial to emphasise the need of establishing trust within corporate and community ties. Organisations that can demonstrate their dedication to information security and data privacy will earn the confidence of consumers, workers, and business associates (Martin et al., 2017). The role of ethics-based leadership is crucial in building the positive image and credibility of a company.

Furthermore, the implementation of more rigorous legislation pertaining to the protection of data privacy underscores the significance of adhering to compliance standards and upholding ethical obligations in the realm of data management. Leaders who prioritise ethics will perceive regulation as a valuable tool for establishing optimal strategies in the realm of information security and data privacy management (Dwivedi et al., 2022).

The significance of conducting research on Ethics-Based Leadership in Managing Information Security and Data Privacy is heightened within this particular setting. The primary objective of this study is to investigate the impact of ethical leadership on decision-making and operational procedures pertaining to information security and data privacy. This project aims to offer comprehensive insights into the significance of ethics-based leadership in addressing information security and data privacy concerns in a complex digital world. It will achieve this by including case studies, literature analysis, and interviews with organisational leaders.

By gaining a deeper comprehension of the significance of ethics-driven leadership in the realm of information security and data privacy, it is anticipated that organisations can enhance their approaches to preserving data integrity, fostering trust, and satisfying progressively rigorous ethical and regulatory requirements.

LITERATURE REVIEW

Leadership

Leadership is the ability of a person or group of individuals to direct, influence, and inspire others or groups to achieve specific goals (Cahyono et al., 2023). It involves a number of skills, attitudes and behaviours designed to move a team or organisation in a desired direction. Leadership is not just about a position or title, but more about how one leads and influences others effectively (Zen et al., 2023). There are several approaches to understanding leadership:

1. Trait Approach: This approach focuses on certain personal characteristics and traits that make someone an effective leader. For example, traits such as confidence, courage, emotional intelligence, and communication skills are often identified as leadership traits.
2. Behavioural Approach: This approach assesses the behaviours and actions performed by the leader rather than his or her personal characteristics. It identifies leadership styles such as transactional (using incentives and rewards), transformational (inspiring and motivating), and democratic (encouraging group participation in decision-making).
3. Situational Approach: This approach recognises that effective leadership styles may vary depending on the particular situation or context. Leaders should be able to adapt their approach to the situation at hand.
4. Relationship Approach: This approach emphasises the importance of building good relationships between leaders and team members. Leaders who care and listen to team members tend to be more effective in motivating and inspiring.

Jurnal Minfo Polgan
Volume 12, Nomor 2, September 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.13018 p-ISSN : 2089-9424

5. Values-Based Approach: This approach emphasises the importance of leadership rooted in ethical and moral values. Leaders who lead based on ethical principles tend to make better decisions and pay more attention to social and moral impact.

Leadership can occur in a variety of contexts, including organisations, community groups, politics and more. Leaders are often responsible for articulating a vision, motivating teams, overcoming obstacles and achieving shared goals. The importance of leadership in directing a group or organisation makes it a central concept in the study of management, psychology and other related fields.

Ethics

Ethics is the science or study of moral principles and values that govern human behaviour in various situations and interactions (Iaccarino, 2001). It involves judgements about what is considered right or wrong, good or bad, and how individuals or groups should act based on existing moral norms. Ethics addresses questions of justice, human rights, responsibility, and views on what constitutes good behaviour (Varkey, 2021). The importance of ethics lies in its role in guiding individuals and society in making meaningful decisions and building good relationships with others (Torelli, 2021). Some important aspects of ethics include:

1. Moral Values: Moral values are principles that guide individuals in distinguishing good and bad actions. These can include values such as honesty, integrity, compassion, justice, and respect for human rights.
2. Moral Norms: Moral norms are rules or guidelines that individuals or societies follow in making ethical decisions. These norms can differ between cultures, religions, and specific social contexts.
3. Consequentialism: This concept focuses on the outcomes or consequences of actions. The consequentialism approach judges actions as good or bad based on their impact. For example, utilitarianism judges actions based on how much happiness they produce.
4. Deontology: This approach emphasises moral obligations or universal principles in making ethical decisions. It focuses more on whether the action conforms to established moral norms.
5. Cooperation Ethics: Cooperation ethics or relationship ethics emphasises the importance of building good relationships with others. This includes mutual respect, caring, and the ability to empathise with the views and needs of others.
6. Professional Ethics: Professional ethics focuses on the moral norms that govern behaviour in the context of a particular job or profession. This includes responsibilities to clients, obligations to society, and integrity in the performance of professional duties.

Ethics has a broad impact on all aspects of human life, including in the business environment, politics, social relations, and so on. In the context of leadership, an ethics-based approach is important to shape leaders who not only have managerial skills, but also have a strong moral foundation in their decision-making and interactions with others.

Information Security

Information security refers to protecting information so that it remains confidential, intact, and available only to those with access rights (Celikel Cankaya, 2020). It involves the use of strategies, practices, and technologies to prevent unauthorised access, unauthorised changes, or loss of critical data. The primary goal of information security is to maintain the confidentiality, integrity, and availability of information (Qadir & Quadri, 2016). There are three main components in information security:

1. Confidentiality: Confidentiality involves ensuring that information can only be accessed by those with access rights. This includes the use of encryption and authentication to prevent unauthorised access.
2. Integrity: Integrity is concerned with ensuring that information remains unchanged or distorted without authorisation. This includes the use of digital signatures, version control, and change detection systems to protect the integrity of information.

Jurnal Minfo Polgan
Volume 12, Nomor 2, September 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.13018 p-ISSN : 2089-9424

3. Availability: Availability involves ensuring that information can be accessed by those authorised when needed. This involves the use of data backup, redundancy, and disaster recovery plans to maintain information availability.
4. The importance of information security cuts across many sectors, including business, government and non-profit organisations. Threats to information security can come from a variety of sources, including cyberattacks, data theft, computer viruses and even human error. Information loss or security breaches can have a serious impact on reputation, customer trust and overall business operations.

In an increasingly connected and technology-dependent world, information and data protection has become a major challenge. Therefore, effective information security practices involve a holistic strategy, including technology, policy, training, and an understanding of the ethical impact of information management. Information security is also closely related to data privacy, where organisations must ensure that customers' and users' personal data is managed securely and in compliance with applicable regulations.

Data Privacy

Data privacy refers to the right of individuals to maintain confidentiality and control over their personal information (Rath & Kumar, 2021). It involves the protection of data that can identify an individual, such as name, address, phone number, financial information, medical history, and so on (Sukenti, 2023); (Salamah, 2023) and (Hermansyah, 2023). Data privacy includes control over how personal data is collected, used, stored and shared by organisations or other entities (Quach et al., 2022). The importance of data privacy includes several aspects:

1. Personal Security: Data privacy protects individuals from potential misuse of their personal information. It prevents identity theft, fraud, and misuse of data by unauthorised parties.
2. Information Control: Data privacy gives individuals control over how their personal information is collected and used. Individuals have the right to know the purposes for which data is being collected and to consent or object to the use of such data.
3. Freedom and Autonomy: Through data privacy, individuals can maintain their freedom and autonomy in keeping personal information private. This allows individuals to safeguard their personal lives from unwanted scrutiny.
4. Legal Arrangements: Data privacy also includes a legal framework that governs how organisations should manage and protect personal information. Regulations such as GDPR in the European Union and data privacy laws in other countries set standards that organisations must adhere to.

In today's digital age, data privacy protection is increasingly complex as a wide range of personal data is collected by companies, governments and other organisations for various purposes. In the business context, data privacy is of paramount importance as customers and users expect that their personal information will be properly safeguarded and used ethically (Azzaakiyyah et al., 2023) and (Bélanger & Crossler, 2011). Organisations must comply with applicable data privacy regulations and adopt appropriate practices to manage and protect personal data. This involves the use of clear privacy policies, encryption practices, strong cybersecurity and an understanding of ethics in data management. By respecting data privacy, organisations can build trust with customers and users and ensure that sensitive data is properly safeguarded in an increasingly complex digital environment.

RESEARCH METHOD

This research is a literature review that adopts a qualitative approach, which means it will analyse and interpret data by relying on information and texts from various sources. The main focus of a qualitative literature review is to collate, evaluate and integrate existing knowledge on the topic under study, namely ethics-based leadership in managing information security and data privacy. In this research, data will be collected from various sources relevant to the topic under study, such as scientific journals, books, research reports, and other articles. The data period covers the time from 2000 to 2023, which allows the researcher to see developments, trends, and changes that have

Jurnal Minfo Polgan
Volume 12, Nomor 2, September 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.13018 p-ISSN : 2089-9424

occurred during this period.

The qualitative approach in the literature review allows researchers to describe and characterise complex and multidimensional issues in greater depth (Elo et al., 2014). In addition, this method makes it possible to involve multiple sources of information and cover a range of different viewpoints, thus enriching the analysis and strengthening the validity of the findings. The data collection process will involve meticulous text analysis, searching for information, and categorising relevant data for the research topic. Subsequently, the author will collate this information in a structured format, compare and synthesise findings from multiple sources, and identify patterns, themes and trends that emerge from the collected data.

One of the advantages of a qualitative literature review is its flexibility in understanding and explaining complex phenomena, as it is not limited by numerical or statistical constraints (Rahman, 2016). This method also allows researchers to gain deep insights into how the topic under study has evolved over time, as well as how concepts and understandings of the topic have changed over the years. In this research, it is important to scrutinise the reliability and credibility of the sources used, as well as critically analyse the information collected. With a qualitative approach, the researcher must be able to present findings objectively and reflectively, provide clear and accurate interpretations, and recognise the limitations of the methods and data used (Bradshaw et al., 2017). The conclusion of this research will hopefully provide a comprehensive picture of the development of the topic under study over the 2000 to 2023 time period, and may also provide recommendations for further research that can broaden the understanding of issues related to the topic.

RESULTS AND DISCUSSION

In the context of a progressively intricate and interconnected digital epoch, the issues surrounding information security and data privacy are assuming greater prominence. Instances such as large-scale data breaches, cyber-attacks, and the unauthorised exploitation of personal information serve as poignant reminders of the pressing need to prioritise data protection and safeguard individual privacy rights. Amidst the dynamic nature of the current environment, there is a noticeable shift occurring in the leadership paradigm (Ramakrishnan, 2021). The significance of ethics-based leadership is increasingly recognised as a fundamental element in the effective management of information security and data privacy.

Ethics-based leadership entails a more comprehensive and profound methodology for making decisions. Ethics-driven leaders demonstrate a comprehensive approach to decision-making by taking into account not only the technical and business ramifications of their actions, but also the broader consequences on individuals, communities, and society at large. An ethical leader possesses the capability to establish a connection between technology and human values, hence prioritising information security and data privacy as fundamental aspects of their policies and practises (Knijnenburg et al., 2022).

The implementation of ethics-based leadership in the management of information security yields significant and wide-ranging positive effects. First and foremost, ethical considerations play a crucial role in guiding executives as they develop and execute a comprehensive information security plan. Ethical leaders possess the ability to construct security systems that are more resilient, mitigate the occurrence of data breaches, and minimise dangers to individuals' privacy rights by taking into account moral ideals and assessing the social consequences of each choice (Culnan & Williams, 2009). In addition, ethical leaders play a pivotal role in shaping corporate cultures that prioritise and uphold the principles of data privacy. Leadership that exhibits a steadfast dedication to ethical practises in the management of information and data serves as a model for fellow employees (Grego-Planer, 2022). This cultivates a conducive atmosphere wherein team members are encouraged to confidentially disclose security breaches, engage in deliberations regarding ethical dilemmas, and actively contribute to data-driven decision-making processes.

Ethics-driven leadership acknowledges the significance of adhering to progressively rigorous standards concerning data privacy. Leaders who prioritise ethics not only adhere to legal

Jurnal Minfo Polgan
Volume 12, Nomor 2, September 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.13018 p-ISSN : 2089-9424

requirements, but also internalise the ethical principles that form the basis of these regulations (Nicolaides & Tornam Duho, 2019). Consequently, the implementation of optimal strategies in information security management is facilitated, enabling businesses to carry out their activities with a strong commitment to ethical behaviour and accountability. Nevertheless, the practical difficulties associated with incorporating ethics-driven leadership into the realm of information security management should not be overlooked. Leadership necessitates the resolution of intricate ethical predicaments, such as striking a harmonious equilibrium between ensuring security and facilitating information accessibility, or effectively and transparently governing data management. This necessitates a comprehensive comprehension of the ramifications of technology and legislation, coupled with the capacity to decipher the multifarious perspectives that may emerge.

Therefore, doing thorough research on the topic of Ethics-Based Leadership in Managing Information Security and Data Privacy holds immense significance. This research aims to enhance our comprehension of the integration of ethical values in the management of information security and data privacy. The findings of this study have the potential to offer practical recommendations for firms in the development of robust security measures, fostering ethical organisational cultures, and cultivating deeper ties with consumers and society in the intricate digital era. Therefore, the implementation of ethics-based leadership will serve as a significant milestone in upholding integrity and fostering trust within our progressively interconnected society.

The implementation of ethics-driven leadership in the management of information security and data privacy has a substantial influence on the image and reputation of a business. An entity that is recognised for its role in safeguarding sensitive information and upholding data privacy will establish credibility and engender trust among customers, business associates, and the broader community. The portrayal of a corporation that demonstrates a steadfast dedication to ethical principles in the realm of information management might yield a competitive edge amongst the intensifying landscape of business rivalry (Azmi, 2006).

In practical application, the implementation of ethics-driven leadership in the management of information security and data privacy encompasses a series of fundamental measures. Leaders must prioritise the cultivation of a comprehensive comprehension regarding the norms and regulations pertaining to data privacy that are applicable within their operational jurisdiction. This practise guarantees that the organisation functions in compliance with relevant legal regulations and mitigates the potential financial liabilities associated with lawsuits. Additionally, it is imperative for leaders to actively support the implementation of unambiguous and all-encompassing rules and practises pertaining to data privacy. This include the development of protocols for the acquisition, utilisation, retention, and dissemination of personal data that align with ethical principles and relevant regulatory frameworks. Furthermore, it is imperative for ethical leaders to give precedence to the provision of education and training opportunities for their team members and employees, with a specific focus on enhancing their understanding of the significance of information security and data privacy. The recognition of the potential hazards and consequences associated with data breaches can serve as a catalyst for proactive measures and a prudent approach towards the management of information (Raghupathi et al., 2023). In the realm of managing information security, the practise of ethics-based leadership emphasises the significance of fostering transparent and open communication with customers and users. The provision of comprehensive details regarding the collection, utilisation, and safeguarding of data not only fosters trust but also upholds the privacy rights of individuals. In conclusion, it is imperative for ethical leaders to embrace a flexible and proactive approach towards technological advancements and the evolving landscape of data privacy. The advent of novel technical advancements has the capacity to unlock untapped potential in the realm of information security management (Kant & Anjali, 2020). However, it is important to acknowledge that these advancements also introduce a fresh set of obstacles. Hence, it is imperative for leaders to guarantee the regular updating and effective implementation of best practises.

In the context of the dynamic digital landscape, it is imperative to establish a solid framework of ethics-driven leadership for effectively addressing the complexities and potentialities associated with information security and data privacy. Organisations have the potential to establish

Jurnal Minfo Polgan
Volume 12, Nomor 2, September 2023 e-ISSN : 2797-3298
DOI : https://doi.org/10.33395/jmp.v12i2.13018 p-ISSN : 2089-9424

a secure, ethical, and reliable environment for all stakeholders by integrating technology, regulatory measures, and ethical principles (Zhao & Gómez Fariñas, 2023). In addition to safeguarding data and privacy rights, it is imperative to focus on constructing a more promising future for an ever more interconnected global community.

In practical application, the effective implementation of ethics-based leadership in the management of information security and data privacy necessitates a comprehensive and cooperative approach. It is imperative for leaders to effectively incorporate ethical principles throughout all tiers of the company, encompassing both the executive and operational levels. The establishment of efficient and consistent strategies for safeguarding information security and data privacy necessitates collaboration among several departments, including IT, legal, compliance, and marketing. Furthermore, it is imperative for leaders to cultivate an organisational culture that fosters principles of integrity and accountability. This entails the implementation of incentive mechanisms that facilitate the adoption of sound information security and data privacy practises. Leaders should exemplify the role of a model in demonstrating respect for data privacy and supporting ethical principles, thereby fostering inspiration among team members and other employees to emulate such behaviour.

It is imperative to proactively address the problems associated with the implementation of ethics-based leadership within the realm of information security and data privacy. This may encompass continuous training programmes designed to enhance leaders' ability to identify and comprehend circumstances and decisions that entail intricate ethical consequences. Leaders may encounter situations when they are confronted with tensions between the preservation of information security and data privacy on one hand, and the pursuit of economic profits or urgent public demands on the other. Hence, the capacity to engage in meticulous moral evaluations and deliberate on several perspectives is crucial in the context of ethics-driven leadership. Furthermore, it is imperative for executives to consistently monitor regulatory advancements and the ever-changing landscape of data privacy trends. The landscape of data privacy regulation is undergoing significant transformations, necessitating that leaders prioritise the continuous compliance of firms with these regulations and effectively incorporate any modifications into their daily operational procedures.

Ethics-based leadership in the management of information security and data privacy is not only a necessity but also presents a potential advantage. Organisations that adopt ethical principles in the handling of information and data will experience enduring advantages, such as enhanced trust, a favourable reputation, and improved risk management capabilities. In a contemporary society characterised by heightened interconnectivity and technological advancements, the adoption of ethics-based leadership emerges as a fundamental cornerstone that will steer enterprises towards a future characterised by security, ethical conduct, and trustworthiness.

CONCLUSION

In the contemporary era characterised by heightened complexity and interconnectivity in the digital realm, the preservation of integrity and trust necessitates the utmost importance of information security, data privacy protection, and leadership guided by ethical principles. The effective management of information security and data privacy demands more than the mere formulation of technological solutions; it also entails a profound understanding and acknowledgment of the moral and ethical principles that underpin each decision and course of action. Ethical leaders prioritise the harmonious integration of technological considerations and ethical principles when making decisions pertaining to information security and data privacy. By adopting an ethics-driven approach to leadership, firms may establish a corporate culture that prioritises data protection, fosters a secure and transparent environment for customers and users, and ensures compliance with progressively severe regulatory frameworks. Organisations operating in the dynamic digital world can gain a competitive edge by cultivating trust among their customers and business partners through the use of ethical practises in information and data management. Therefore, in view of all the above, this study arrives at the following suggestions:

a) Implement Training and Education: Organisations should prioritise ongoing training and education for team members and employees on the importance of information security and data privacy. This will increase awareness and understanding of the risks involved and the precautions to be taken.
b) Establish Clear Policies: Organisations need to develop clear and comprehensive policies regarding information security and data privacy. This policy should include procedures for data collection, use, storage and sharing of personal information in accordance with ethical values and applicable regulations.
c) Create an Ethical Organisational Culture: Leaders should create an organisational culture that promotes integrity, responsibility and respect for data privacy. This involves implementing incentive systems that support good information security and data privacy practices.
d) Conduct Regular Evaluations: Organisations should regularly evaluate their information security and data privacy practices to ensure that they remain in line with technological developments and regulatory changes.
e) Focus on Regulatory Compliance: Leaders should prioritise understanding and complying with applicable data privacy regulations in their area of operation. This will help prevent potential legal risks that may arise.
f) Adopt a Collaborative Approach: Ethics-based leadership in managing information security and data privacy requires co-operation across departments, including IT, legal, compliance and marketing. This collaboration will ensure that strategies and practices are consistent and coherent.
g) Integrate Ethical Values in Decision Making: Leaders should always remind themselves to integrate ethical values in every decision relating to information security and data privacy. Careful moral analysis and considering diverse viewpoints should be part of this leadership approach.

By implementing these suggestions, organisations can build a solid foundation in managing information security and data privacy, and lead with integrity and ethics in a digital age full of challenges and opportunities. In doing so, they will be able to maintain customer trust, minimise the risk of data breaches, and contribute to positive developments in an increasingly connected society.

REFERENCES

Azmi, R. A. (2006). Business Ethics as Competitive Advantage for Companies in the Globalization Era. *SSRN Electronic Journal*, 1–8. https://doi.org/10.2139/ssrn.1010073

Azzaakiyyah, H. K., Wanof, M. I., Suherlan, S., & Fitri, W. S. (2023). Business Philosophy Education and Improving Critical Thinking Skills of Business Students. *Journal of Contemporary Administration and Management (ADMAN)*, *1*(1), 1–4. https://doi.org/10.61100/adman.v1i1.1

Basir, A., Puspitasari, E. D., Aristarini, C. C., Sulastri, P. D., & Ausat, A. M. A. (2023). Ethical Use of ChatGPT in the Context of Leadership and Strategic Decisions. *Jurnal Minfo Polgan*, *12*(1), 1239–1246. https://doi.org/https://doi.org/10.33395/jmp.v12i1.12693

Bélanger, & Crossler. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017. https://doi.org/10.2307/41409971

Bradshaw, C., Atkinson, S., & Doody, O. (2017). Employing a Qualitative Description Approach in Health Care Research. *Global Qualitative Nursing Research*, *4*, 1–8. https://doi.org/10.1177/2333393617742282

Cahyono, A. S., Tuhuteru, L., Julina, S., Suherlan, S., & Ausat, A. M. A. (2023). Building a Generation of Qualified Leaders: Leadership Education Strategies in Schools. *Journal on Education*, *5*(4), 12974–12979. https://jonedu.org/index.php/joe/article/view/2289

Celikel Cankaya, E. (2020). Security and Privacy in Three States of Information. In *Security and Privacy From a Legal, Ethical, and Technical Perspective*. IntechOpen. https://doi.org/10.5772/intechopen.91610

Culnan, & Williams. (2009). How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches. *MIS Quarterly*, *33*(4), 673. https://doi.org/10.2307/20650322

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., … Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative Content Analysis. *SAGE Open*, *4*(1), 1–10. https://doi.org/10.1177/2158244014522633

Fabrègue, B. F. G., & Bogoni, A. (2023). Privacy and Security Concerns in the Smart City. *Smart Cities*, *6*(1), 586–613. https://doi.org/10.3390/smartcities6010027

Gadzali, S. S., Gazalin, J., Sutrisno, S., Prasetya, Y. B., & Ausat, A. M. A. (2023). Human Resource Management Strategy in Organisational Digital Transformation. *Jurnal Minfo Polgan*, *12*(2), 760–770. https://doi.org/https://doi.org/10.33395/jmp.v12i2.12508

Grego-Planer, D. (2022). The relationship between benevolent leadership and affective commitment from an employee perspective. *PLOS ONE*, *17*(3), 1–27. https://doi.org/10.1371/journal.pone.0264142

Guo, K. (2022). The Relationship Between Ethical Leadership and Employee Job Satisfaction: The Mediating Role of Media Richness and Perceived Organizational Transparency. *Frontiers in Psychology*, *13*, 1–13. https://doi.org/10.3389/fpsyg.2022.885515

Hermansyah, A. M. S. (2023). The Effect of Dividend Policy on Corporate Financial Performance. *Journal of Contemporary Administration and Management (ADMAN)*, *1*(1), 5–8. https://doi.org/10.61100/adman.v1i1.2

Iaccarino, M. (2001). Science and ethics. *EMBO Reports*, *2*(9), 747–750. https://doi.org/10.1093/embo-reports/kve191

Kant, N., & Anjali, K. (2020). Can blockchain be a strategic resource for ODL?: a study. *Asian Association of Open Universities Journal*, *15*(3), 395–410. https://doi.org/10.1108/AAOUJ-09-2020-0061

Knijnenburg, B. P., Page, X., Wisniewski, P., Lipford, H. R., Proferes, N., & Romano, J. (2022). *Modern Socio-Technical Perspectives on Privacy* (B. P. Knijnenburg, X. Page, P. Wisniewski, H. R. Lipford, N. Proferes, & J. Romano, Eds.). Springer International Publishing. https://doi.org/10.1007/978-3-030-82786-1

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, *81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Nicolaides, A., & Tornam Duho, K. C. (2019). Effective Leadership in Organizations: African Ethics and Corruption. *Modern Economy*, *10*(07), 1713–1743. https://doi.org/10.4236/me.2019.107111

Qadir, S., & Quadri, S. M. K. (2016). Information Availability: An Insight into the Most Important Attribute of Information Security. *Journal of Information Security*, *07*(03), 185–194. https://doi.org/10.4236/jis.2016.73014

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. *Journal of the Academy of Marketing Science*, *50*(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y

Raghupathi, W., Raghupathi, V., & Saharia, A. (2023). Analyzing Health Data Breaches: A Visual Analytics Approach. *AppliedMath*, *3*(1), 175–199. https://doi.org/10.3390/appliedmath3010011

Rahman, M. S. (2016). The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language “Testing and Assessment” Research: A Literature Review. *Journal of Education and Learning*, *6*(1), 102–112. https://doi.org/10.5539/jel.v6n1p102

Ramakrishnan, R. (2021). Leading in a VUCA World. *Ushus Journal of Business Management*, *20*(1), 89–111. https://doi.org/10.12725/ujbm.54.5

Rath, D. K., & Kumar, A. (2021). Information privacy concern at individual, group, organization and societal level - a literature review. *Vilakshan - XIMB Journal of Management*, *18*(2), 171–186. https://doi.org/10.1108/XJM-08-2020-0096

Salamah, S. N. (2023). Financial Management Strategies to Improve Business Performance. *Journal of Contemporary Administration and Management (ADMAN)*, *1*(1), 9–12. https://doi.org/10.61100/adman.v1i1.3

Scholl, J. A., Mederer, H. J., & Scholl, R. W. (2016). Leadership, Ethics, and Decision-Making. In *Global Encyclopedia of Public Administration, Public Policy, and Governance* (pp. 1–11). Springer International Publishing. https://doi.org/10.1007/978-3-319-31816-5_2407-1

Sukenti, S. (2023). Financial Management Concepts: A Review. *Journal of Contemporary Administration and Management (ADMAN)*, *1*(1), 13–16. https://doi.org/10.61100/adman.v1i1.4

Torelli, R. (2021). Sustainability, responsibility and ethics: different concepts for a single path. *Social Responsibility Journal*, *17*(5), 719–739. https://doi.org/10.1108/SRJ-03-2020-0081

Touriano, D., Sutrisno, S., Kuraesin, A. D., Santosa, S., & Ausat, A. M. A. (2023). The Role of Information Technology in Improving the Efficiency and Effectiveness of Talent Management Processes. *Jurnal Minfo Polgan*, *12*(2), 539–548. https://doi.org/https://doi.org/10.33395/jmp.v12i2.12454

Varkey, B. (2021). Principles of Clinical Ethics and Their Application to Practice. *Medical Principles and Practice*, *30*(1), 17–28. https://doi.org/10.1159/000509119

Wahyoedi, S., Suherlan, S., Rijal, S., Azzaakiyyah, H. K., & Ausat, A. M. A. (2023). Implementation of Information Technology in Human Resource Management. *Al-Buhuts*, *19*(1), 300–318. https://doi.org/https://doi.org/10.30603/ab.v19i1.3407

Zen, A., Siminto, S., Harahap, M. A. K., Prasetya, Y. B., & Ausat, A. M. A. (2023). Effective Leadership: A Literature Review of Concepts, Characteristics, and Best Practices. *Innovative: Journal Of Social Science Research*, *3*(2), 2209–2219. https://doi.org/https://doi.org/10.31004/innovative.v3i2.430

Zhao, J., & Gómez Fariñas, B. (2023). Artificial Intelligence and Sustainable Decisions. *European Business Organization Law Review*, *24*(1), 1–39. https://doi.org/10.1007/s40804-022-00262-2