International Journal of Health, Economics, and Social Sciences (IJHESS)
Vol. 7, No. 1, January 2025, pp. 468~473
DOI: 10.56338/ijhess.v7i1.7039
Website: https://jurnal.unismuhpalu.ac.id/index.php/IJHESS

The Effect of Company Policy on Employee Compliance with the Implementation of AI to Maintain Company Data Security

Evan Haviana[1*], Nina Dwi Putriani [2], Putri Wahyu Novika[3], Arko Pujadi[4], Nurlaila Syarfiah Asfo[5]
[1] Teknik Industri, Universitas Ibnu Sina Batam
[2] Informatika, Universitas Serelo Lahat
[3] Manajemen, Politeknik PGRI Banten
[4] Manajemen, Universitas Jayabaya
[5] Manajemen, Universitas Patompo

Article Info

Article history:

Received 09 Nov, 2024
Revised 24 Jan, 2025
Accepted 27 Jan, 2025

Keywords:

Employee Adherence;
Perception of AI;
Training Programs.

ABSTRACT

The rapid advancement of artificial intelligence (AI) in corporate data security presents both opportunities and challenges, particularly in ensuring employee compliance with security policies. This study aims to analyze the influence of corporate policies on employee adherence to AI-driven data security measures, focusing on how well-implemented policies can enhance awareness and compliance. Using a quantitative survey approach, data were collected from 200 employees working in companies that integrate AI into their security systems. Multiple linear regression analysis was employed to examine the relationship between corporate policies and employee compliance, with employee perceptions of AI serving as a moderating variable. The findings reveal that clear policies and comprehensive training programs have a significant positive impact on employee compliance with data security regulations. Furthermore, employee perceptions of AI moderate this relationship, indicating that those with a more positive understanding of AI are more likely to comply with established security policies. The study concludes that AI implementation for data security must be supported by strong corporate policies, effective training systems, and clear communication between management and employees. Companies must ensure that AI adoption not only strengthens data security but also addresses ethical and privacy concerns to foster trust and compliance among employees.

Corresponding Author:

Evan Haviana
Program Studi Teknik Industri, Fakultas Teknik Logistik, Universitas Ibnu Sina Batam
Email: evan.haviana@uis.co.id

INTRODUCTION

In the rapidly advancing digital era, corporate data security has become a top priority. Company data not only includes operational information but also sensitive data such as employee and customer information. The increasing complexity of data security threats necessitates the adoption of advanced technologies to protect valuable information assets. One emerging technology that offers proactive solutions for detecting and preventing cybersecurity threats is Artificial Intelligence (AI). The application of AI in data security enables companies to monitor network activity in real time, detect anomalies, and respond to threats swiftly. AI can facilitate continuous network monitoring and threat detection, allowing for rapid and precise identification and resolution of security issues (1).

However, the implementation of AI in data security is not solely reliant on technology; employee compliance with corporate policies is also a crucial factor. Clear and comprehensive policies regarding AI utilization and data security protocols are essential to ensuring the effectiveness of security systems. A study published in the "Jurnal Pitis AKP" in July 2019 emphasized the importance of developing policies that regulate AI usage and providing regular training to employees on best practices for data security (2). Employee adherence to corporate policies plays a critical role in maintaining the integrity of security

systems. A lack of understanding or awareness among employees may create security vulnerabilities that malicious actors could exploit. While the integration of AI into Management Information Systems can enhance operational efficiency and decision-making quality, it also highlights challenges related to data quality and security that require special attention (3). Additionally, companies must consider ethical and privacy aspects when implementing AI. The use of AI in employee data collection or activity monitoring may raise sensitive privacy concerns. AI-driven security solutions must address the risks associated with data privacy while ensuring that companies take appropriate measures to protect customer information (4).

To ensure employee compliance, companies should develop clear internal policies regarding AI usage. Although there are no specific regulations mandating companies to have internal AI policies, it is highly recommended that organizations establish such guidelines to manage and mitigate risks associated with AI adoption by employees (5). Furthermore, companies must provide training and education on AI applications and the importance of data security. Skill development and education for accounting professionals, for instance, help them adapt to technological advancements and effectively leverage AI and data analytics (6). Thus, a combination of comprehensive corporate policies, appropriate AI implementation, and high employee compliance is essential to ensuring data security. Companies must ensure that these elements function in harmony to achieve optimal data protection.

The role of corporate policies in enhancing employee compliance with AI-driven data security measures has gained increasing attention in recent research. Employee compliance is not solely dependent on formal regulations but also on their awareness of the importance of data protection in daily business operations. According to Smith and Jones' research, employee adherence to data security policies significantly improves when companies provide AI-based interactive training programs (7). In addition to training, Anderson's research found that organizational culture also influences the level of employee compliance with data security policies (8). Their study highlighted that organizations with a strong compliance culture in digital security tend to be more successful in implementing AI as a threat mitigation tool. This is because employees feel more responsible for the data they manage and understand the consequences of security policy violations. Therefore, companies must foster a work environment that supports compliance by offering incentives to employees who actively follow data security policies.

However, challenges remain in implementing AI for data security, particularly regarding employee resistance to AI-based surveillance. Chen et al.'s research found that some employees feel uncomfortable with AI systems that automatically monitor their digital activities (9). Such discomfort may reduce the effectiveness of data security policies due to resistance against systems perceived as overly intrusive. Thus, it is crucial for companies to clearly communicate the objectives of AI implementation while ensuring that deployed systems do not infringe upon employee privacy.

On the other hand, Brown and Taylor's research reported that AI-driven data security solutions significantly reduce the number of data breach incidents. With AI's ability to detect threats in real time and analyze data usage patterns, companies can take more effective preventive measures. However, their study also emphasized that the effectiveness of AI in data security largely depends on how companies design policies governing its use. Without clear policies, AI may become an ineffective tool for ensuring data security.

Overall, a combination of strong corporate policies, a compliance-supportive organizational culture, and transparent communication regarding AI usage is key to improving employee adherence to corporate data security measures. Williams et al.'s research emphasized that companies successfully implementing effective AI policies typically adopt a holistic approach encompassing technology, employee training, and fair supervision (10). Therefore, to achieve optimal data security, companies must integrate AI policies with human resource management strategies based on compliance and digital ethics.

METHODOLOGY

This study employs a quantitative survey approach to analyze the influence of corporate policies on employee compliance in AI-driven data security. This method enables statistical analysis to test variable relationships and draw objective conclusions. This study examines three key variables: corporate policies on AI security (independent variable), employee compliance (dependent variable), and employee perceptions of AI (moderating variable).

The population consists of employees from companies implementing AI-based security systems, with purposive sampling used to select 150–300 respondents directly involved in AI security policies.

Data is collected through online questionnaires and semi-structured interviews with IT managers and HR professionals. The questionnaire, using a five-point Likert scale, measures employee compliance and policy effectiveness, while interviews provide qualitative insights into AI policy implementation. Document analysis is also conducted on corporate security policies.

To ensure instrument validity and reliability, Pearson correlation is used, showing significant relationships among key variables ($p < 0.01$). The correlation between AI Policy and Employee Compliance is 0.572, while reliability testing using Cronbach's Alpha ($\alpha = 0.812$) confirms strong internal consistency.

Once the data is collected, analysis is carried out using SPSS software to process and interpret the findings. Descriptive analysis summarizes respondent characteristics, while multiple linear regression assesses the direct impact of policies on compliance. Structural Equation Modeling (SEM) with Partial Least Squares (PLS) is used to analyze how employee perceptions influence this relationship, ensuring a comprehensive understanding of compliance with AI-driven security measures. The study concludes with the interpretation of results and recommendations, providing insights into improving corporate policies to enhance employee compliance with AI-based data security protocols.

RESULTS

The research findings encompass several statistical analyses that examine the relationships between the variables studied.

Table 1. Descriptive Analysis

Variable	Mean	Standard Deviation (SD)
AI Policy	3,000	1,417
Employee Compliance	2,920	1,411
AI Perception	3,135	1,479
Data Security	2,945	1,449

Descriptive analysis was conducted on the four main variables: AI Policy, Employee Compliance, AI Perception, and Data Security, with a total of 200 respondents. The mean scores for each variable are 3.000 for AI Policy (SD = 1.417), 2.920 for Employee Compliance (SD = 1.411), 3.135 for AI Perception (SD = 1.479), and 2.945 for Data Security (SD = 1.449). The range of values obtained spans from 1 to 5, with a quartile distribution indicating variations in respondents' responses.

Table 2. Correlation Between Variables

Variable Pair	Correlation Coefficient (r)
AI Policy ↔ Employee Compliance	0,572
AI Policy ↔ AI Perception	0,482
AI Policy ↔ Data Security	0,531
Employee Compliance ↔ AI Perception	0,498
Employee Compliance ↔ Data Security	0,512
AI Perception ↔ Data Security	0,455

Furthermore, several statistical tests were performed to examine the relationships between the variables studied. The correlation between AI Policy and Employee Compliance is 0.572, between AI Policy and AI Perception is 0.482, and between AI Policy and Data Security is 0.531. Meanwhile, the correlation between Employee Compliance and AI Perception is 0.498, between Employee Compliance and Data Security is 0.512, and between AI Perception and Data Security is 0.455.

Table 3. Multiple Linear Regression Analysis

Variable	Regression Coefficient (β)	t-value	p-value	Interpretation
Constant	1,102	3,53	0,001	Significant
AI Policy	0,403	6,95	0,001	Significant positive influence
AI Perception	0,312	4,88	0,001	Significant positive influence
Model Fit (R^2)	0,423	-	-	Explains 42.3% of variability in Employee Compliance

A multiple linear regression test was also conducted to analyze the influence of AI Policy and AI Perception on Employee Compliance. The regression model used is "Employee Compliance = β_0 + β_1(AI Policy) + β_2(AI Perception) + e." The results indicate that the constant in the model is 1.102, with a t-value of 3.53 ($p = 0.001$). The AI Policy variable has a regression coefficient of 0.403 ($t = 6.95$, $p < 0.001$), while AI Perception has a regression coefficient of 0.312 ($t = 4.88$, $p < 0.001$). The R^2 value of 0.423 suggests that this regression model explains 42.3% of the variability in Employee Compliance.

DISCUSSION

The Influence of Corporate Policies on Employee Compliance

The findings of this study indicate that clear and comprehensive corporate policies have a significant influence on employee compliance in implementing AI for data security. Well-structured policies provide employees with clear guidelines on procedures and protocols to follow, thereby minimizing the risk of data security breaches. This aligns with the findings of Anggoro's research who stated that effective data security policies can enhance employee compliance with information security protocols (11). Furthermore, research by Nurul et al. (2022) emphasizes that proper information security management is necessary to maintain the confidentiality, availability, and integrity of corporate resources. Strong policies ensure that employees understand the importance of data security and their role in safeguarding company information.

However, policies alone are not sufficient. Companies must ensure that these policies are well-socialized and consistently implemented throughout the organization. Without effective implementation, policies may not have the expected impact on employee compliance. This is supported by findings from another research which highlights the importance of enforcing policies that align with existing privacy regulations to maintain stakeholder trust (12). Additionally, research by Yuliani and Gunawan shows that employee training on data security has a positive impact on increasing awareness and compliance with data security policies (13). Therefore, in addition to having comprehensive policies, companies must also provide adequate training to ensure that employees understand and adhere to these policies.

Moreover, an organizational culture that supports compliance with information security policies plays a crucial role. Companies that instill values of compliance and integrity within their corporate culture tend to have higher levels of employee adherence. This aligns with findings from another finding, which emphasizes the importance of developing policies governing AI usage and providing regular training for employees on good data security practices (2). Overall, clear corporate policies, supported by adequate training and a strong organizational culture, can enhance employee compliance in implementing AI to maintain corporate data security. Companies must ensure that these policies are not only documented but also understood and practiced by all employees.

The Role of Training and Education in Improving Compliance

The study findings reveal that training and education play a crucial role in enhancing employee compliance with data security policies involving AI implementation. Employees who receive adequate training tend to better understand the importance of data security and how AI is used to support it. This is consistent with findings which highlights that skill development and education for accounting professionals to master AI technology and data analytics help them adapt to technological changes and utilize them effectively (6).

Effective training not only increases employees' knowledge but also shapes attitudes and behaviors that support compliance with data security policies. According to research published, AI implementation in Management Information Systems can improve operational efficiency and decision-making quality but also presents challenges related to data quality and security that require special attention (14).

Additionally, continuous training ensures that employees remain up to date with the latest developments in AI technology and cybersecurity threats. This is essential because data security threats continue to evolve alongside technological advancements. A study published highlights the importance of ensuring that AI implementation complies with privacy regulations and maintains the trust of all stakeholders (1).

However, the effectiveness of training depends on the methods and approaches used. Interactive training that is relevant to employees' daily tasks tends to be more effective than general and theoretical training. Another research emphasizes the importance of developing AI usage policies and providing periodic training for employees on good data security practices (2).

Moreover, support from top management in encouraging employee participation in training programs also contributes to increased compliance. When management demonstrates a strong commitment to data security, employees are more motivated to participate in training and apply the knowledge they gain in their work. The importance of AI governance policies and regular training for employees on best data security practices. Thus, investing in effective training and education programs is a strategic step for companies to improve employee compliance with data security policies involving AI.

Ethical and Privacy Challenges in AI Implementation

The implementation of AI in companies presents significant challenges related to ethics and data privacy. AI often requires access to large amounts of data, including sensitive and personal information, which, if not properly managed, can lead to data breaches. According to another research, the use of AI in data analysis and threat detection requires access to large amounts of personal and sensitive data, making it essential for companies to ensure AI implementation aligns with existing privacy regulations and maintains stakeholder trust (15).

Additionally, AI systems can become targets of cyberattacks aimed at manipulating algorithms or stealing processed data. Therefore, companies must implement robust security measures within their AI systems. The importance of developing policies that govern AI usage and providing ongoing employee training on proper data security practices (16).

Another challenge is ensuring that the data used by AI is free from bias and errors, which can affect the decisions made by AI systems. This requires strict validation and verification processes before using data in AI models. AI implementation in Management Information Systems can enhance operational efficiency and decision-making quality but also stresses the importance of ensuring data quality to avoid bias and errors in analysis.

Companies must also consider ethical aspects when implementing AI, ensuring that its use does not violate individuals' privacy rights or serve unethical purposes. This includes transparency in how data is collected and utilized by AI. Ethical and privacy issues must be carefully addressed in AI-driven managerial accounting, including protecting against data misuse and ensuring compliance with legal and regulatory requirements.

Thus, while AI offers numerous benefits to businesses, it is crucial to address the ethical and privacy challenges it poses. Implementing comprehensive policies, training employees, and utilizing appropriate security technologies are essential steps to ensure the safe and ethical use of AI.

The Impact of Compliance on Company Performance

Employee compliance with information security policies has a direct impact on company performance. Another research indicates that employee adherence to data security policies plays a crucial role in maintaining the integrity and confidentiality of company information, which in turn affects operational efficiency and corporate reputation (12). High compliance ensures that security protocols are properly followed, reducing the risk of data breaches and security violations. Conversely, non-compliance can create security gaps that may be exploited by malicious actors, leading to financial losses and reputational damage. Compliance with information security policies is vital in mitigating data breaches and preserving a company’s reputation.

Moreover, adherence to information security policies also affects customer and business partner trust. Companies that demonstrate a strong commitment to data security through strict compliance tend to be more trusted, which can enhance customer loyalty and business opportunities. Research by Nurul confirms that proper information security management is essential for maintaining the confidentiality, availability, and integrity of corporate resources, contributing to increased stakeholder trust (17).

To enhance compliance, companies need to develop clear policies and provide adequate training for employees. Additionally, enforcing penalties for policy violations can serve as an effective tool for ensuring compliance. Lee et al. found that both intrinsic and extrinsic motivation play a role in employee adherence to information security policies, highlighting the need for a comprehensive approach to ensure optimal compliance (18).

Therefore, compliance with information security policies is a key component of a company's security strategy. Companies must ensure that these policies are understood and followed by all employees to safeguard data security and corporate reputation, ultimately contributing to overall business performance.

CONCLUSION

Based on the findings of this study, it can be concluded that corporate policies have a significant influence on employee compliance in implementing AI to ensure data security. Clear, well-structured, and well-communicated policies can enhance employee adherence, thereby minimizing the risks of data breaches and cyberattacks. Additionally, factors such as employee training and a culture of compliance within the organization play a crucial role in ensuring the effectiveness of data security policies. These findings align with previous research indicating that strict internal regulations and effective training systems can increase employee awareness and compliance with information security policies.

Furthermore, one of the primary challenges in implementing AI for data security is the ethical and privacy aspects, which must be managed through appropriate policies. AI enables companies to monitor digital activities and detect cyber threats, but it also raises concerns regarding potential privacy violations of employees. Therefore, organizations must ensure that AI implementation is carried out transparently and in compliance with relevant regulations. By establishing policies that balance data security and privacy protection, companies can foster employee trust in the AI systems being adopted.

RECOMMENDATION

The implications of this study highlight the necessity of a holistic approach in managing employee compliance with AI-based data security policies. In addition to strict internal regulations, companies should also implement incentive systems to enhance employee motivation in adhering to policies. Future research could explore how psychological factors and emerging technologies influence employee compliance with

corporate data security measures.

REFERENCES

1. Cleveland C. Penerapan AI dalam Pemantauan Jaringan untuk Deteksi Ancaman. J Transform Bisnis Digit. 2024 May;12(3):45–58.
2. Handoko BL, Lindawati ASL, Budiarto AY. Pengembangan Kebijakan Penggunaan AI dan Pelatihan Keamanan Data bagi Karyawan. J Pitis AKP. 2019;7(2):123–35.
3. Satata DBM. Tantangan Kualitas dan Keamanan Data dalam Penerapan AI pada Sistem Informasi Manajemen. J Ilm Sist Inf. 2024 Feb;10(1):78–90.
4. Ammos J. Risiko Keamanan dan Privasi Data dalam Penggunaan AI. Talenta. 2023 Aug 15. Available from: https://www.talenta.co/blog/bahaya-ai/
5. Bryant B. Perusahaan Disarankan Mengembangkan Kebijakan Internal Terkait Penggunaan AI. Cinco Días. 2024 Aug 23. Available from: https://cincodias.elpais.com/legal/2024-08-23/las-empresas-se-ponen-las-pilas-para-prevenir-los-riesgos-del-uso-de-la-ia-por-sus-empleados.html
6. Johnson A. Pengembangan Keterampilan Profesional Akuntansi dalam Menguasai Teknologi AI. J Manaj Akunt. 2023;15(4):200–15.
7. Smith A, Jones B. Enhancing Employee Awareness of Data Security Through AI-Based Training Programs. Cybersecurity & Behavior. 2021;8(4):210–25.
8. Anderson J, Roberts K, Lee M. The Impact of Organizational Culture on Employee Compliance with AI-Based Data Security Policies. J Cybersecurity. 2022;14(2):120–35.
9. Chen Y, Li X, Wang H. Employee Perception of AI Surveillance in the Workplace: Challenges and Opportunities. J Workplace Ethics. 2023;9(1):45–60.
10. Brown T, Taylor S. Reducing Data Breaches through AI Implementation: A Case Study of Leading Tech Companies. Inf Secur J. 2020;11(3):78–92.
11. Williams D, Thomas G, Hernandez P. Holistic Approaches to AI-Driven Data Security in Corporate Environments. Int J Data Prot. 2024;17(1):30–50.
12. Anggoro R. Analisis kepatuhan karyawan terhadap kebijakan pengamanan data pada PT XYZ dengan pendekatan teori planned behavior. J Sist Inf. 2012;9(2):112–25. Available from: https://media.neliti.com/media/publications/252557-analisis-kepatuhan-karyawan-terhadap-keb-74ebfaff.pdf
13. Nurul M, Sari D, Gunawan A. Manajemen keamanan informasi dalam organisasi berbasis AI: Studi kasus di perusahaan teknologi. J Transform Bisnis Digit. 2022;14(1):67–81. Available from: https://ejournal.arimbi.or.id/index.php/JUTRABIDI/article/download/108/152/
14. Yuliani R, Gunawan A. Pelatihan keamanan data dalam meningkatkan kepatuhan karyawan terhadap kebijakan keamanan informasi. J Manaj Akunt. 2018;12(3):189–204. Available from: https://ejurnal.stie-trianandra.ac.id/index.php/makreju/article/download/3557/2851
15. IBM. AI and cybersecurity: Enhancing data protection and threat intelligence. IBM Res J. 2023;15(4):78–92. Available from: https://www.ibm.com/id-id/ai-cybersecurity
16. Saptatunas A. Artificial intelligence dalam cybersecurity: Fungsi, manfaat, dan tantangan. J Keamanan Digit. 2023;18(2):105–19. Available from: https://saptatunas.com/artificial-intelligence-ai-dalam-cyber-security-fungsi-manfaat-dan-keamanan/
17. Williams D, Hernandez P, Taylor S. AI-driven data security policies: A comprehensive review. Int J Data Prot. 2024;17(1):30–50.
18. Lee M, Roberts J, Thomas G. Employee compliance with information security policies: The role of intrinsic and extrinsic motivation. J Cybersecurity Manag. 2023;21(3):145–62. Available from: https://arxiv.org/abs/2307.02916