JAIEP

A Novel Integrated Model for Investigation into Employee Compliance with Information Security Policies

Amr R. Kamel[1,2,*], Abdulaziz A. Alqarni[3], Fahad M. Al Subhi[4], Mahmod Othman[5], Abdullahi G. Usman[6], Ahmad Abubakar Suleiman[7], Moataz A. Ahmed[8]

[1]Department of Applied Statistics and Econometrics, Faculty of Graduate Studies for Statistical Research, Cairo University, Giza, 12613, Egypt.
[2]Department of Basic Sciences, El-Gazeera High Institute for Computers and Information Systems, Ministry of Higher Education, El-Mokattam 11571, Egypt.
[3]Department of General Studies, Jeddah College of Technology, Technical and Vocational Training Corporation, Jeddah, Saudi Arabia.
[4]Department of Mathematics, Jamoum University College, Umm Al-Qura University, Makkah, Saudi Arabia.
[5]Department of Information Systems, Universitas Islam Indragiri, Tembilahan 29212, Indonesia.
[6]Department of Analytical Chemistry, Faculty of Pharmacy, Near East University, 99138, Nicosia, Turkish Republic of Northern Cyprus.
[7]Fundamental and Applied Sciences Department, Universiti Teknologi PETRONAS, Seri Iskandar 32610, Malaysia.
[8]Computer science department, faculty of computers and artificial intelligence, Beni-Suef University, Beni-Suef, Egypt.
* Corresponding author: amr_ragab@pg.cu.edu.eg

Abstract

A key component of a company's integrity, both financially and in terms of reputation, is information security. When given the right direction, employees can play a significant role in strengthening information security, despite the fact that they are frequently seen as the weakest link in the chain. Businesses are doing this by implementing information security measures, both in terms of policies and financial stability. Employees are expected to adhere to the organizational and personal goals that executives set through information security rules. Research on employee compliance with information security policies (ISPs) has been done in a number of studies in the literature, but few of these studies have focused on identifying the factors that encourage employees to follow their company's information security policies. This paper is to draw attention to the elements that affect workers' perceptions of adherence to the organization's ISPs. Employees of businesses with ISPs in place were given the questionnaire. A total of 985 companies and organizations from multiple divisions received the questionnaire in Egypt. 303 workers from various industries took part in the poll. The dataset was analyzed using structural equation modeling (SEM) through SmartPLS version 3.3.9. The survey's findings demonstrated that a large number of workers lacked a thorough understanding of the rules outlined in their company's ISPs, demonstrating the necessity of educating and training staff members on security procedures. It's also important to note that only a small portion of the employees who took part in the survey felt that following the company's ISPs would increase their profits. For this reason, it would be advantageous for businesses to provide employees with more incentives to follow the ISPs. Employees do, however, intend to abide by the information security regulations of the companies; thus, any company might benefit from this circumstance with the appropriate tactics. As a result, many businesses do not give information security the consideration it requires. Information security policies should be established, goals should be set, and employees should be trained and made aware of the importance of adhering to information security policies because their role is critical to the integrity of the resources and, consequently, the businesses themselves. Technological solutions alone are insufficient for information security in organizations.

Keywords: Cybersecurity, Information Security Compliance, Information Security Practices, Information Security Risk Management, SmartPLS Software, Structural Equation Modeling.
MSC: 68M25; 91B05

Doi : https://doi.org/10.21608/jaiep.2025.419694.1022
Received: August 30, 2025, Revised: September 24, 2025, Accepted: October 1, 2025

1. Introduction

Since it has a direct impact on how an organization conducts business, information security ought to be its top priority. There are both technical and non-technical aspects to information security. Technical security issues can be resolved by installing a firewall, antivirus software, backing up data, implementing access control measures, encrypting the system, and continuously monitoring it for threats. Measures of employee behavior are considered non-technical measures. Information security-related sociological, psychological, and organizational behavioral theories are included in these procedures to guarantee that employees follow information security policies [1]. A formal system of rules and standards that a business develops to safeguard its information assets by guaranteeing the availability, confidentiality, and integrity of its data is known as an information security policies (ISPs). In addition to providing a framework for security policies, procedures, and duties to protect against threats, satisfy compliance requirements, and preserve operational resilience, it serves as a formal blueprint to advise staff members and users on how to use IT systems and networks. Implementing safeguards and restricting data distribution to only those with authorized access are the goals of an information security policy. ISPs are established by organizations to:

- Create a broad strategy for information security.
- Keep track of user access control guidelines and security procedures.
- Identify and lessen the effects of compromised information assets, including improper usage of computers, networks, mobile devices, data, and apps.
- Preserve the organization's reputation.
- Respect legal and regulatory mandates such as FERPA, GDPR, HIPAA, and NIST.
- Safeguard client information, including credit card numbers.
- Establish efficient procedures for handling grievances and inquiries about actual or suspected cyberthreats, such as ransomware, malware, and phishing.
- Restrict access to important IT resources to those who can legitimately utilize them.

One of the most important steps in preventing security incidents like data breaches and leaks is developing an information security policy that is both effective and compliant with all applicable regulations. ISPs are crucial for both new and existing businesses. Every employee is creating data as a result of increased digitization, and some of that data needs to be shielded from unwanted access. It might even be protected by laws and regulations, depending on your sector. Intellectual property, sensitive data, and personally identifiable information (PII) need to be protected to a higher degree than other types of data. Third-party providers now have access to data due to increased outsourcing. For this reason, an information security strategy must now include a Third-Party Risk Management framework and a Vendor Risk Management program. Third-party risk, fourth-party risk and vendor risk are no joke. The scope of an information security policy is up to you. Social media use, lifecycle management, security training, and IT and/or physical security can

Doi : https://doi.org/10.21608/jaiep.2025.419694.1022
Received: August 30, 2025 Accepted: October 1, 2025

all be covered. A key component of developing and putting into practice efficient security policies is defining security objectives. Figure 1 illustrates a few security policy goals.

Therefore, in today's digital age, information is one of the most valuable assets an organization possesses. It drives decision-making, supports business operations, and underpins relationships with customers, partners, and stakeholders. As reliance on information systems grows, so does the need to protect data from unauthorized access, use, disclosure, disruption, modification, or destruction. This Information Security Policy establishes the framework for safeguarding the confidentiality, integrity, and availability (the "CIA triad") of information assets across the organization. It defines the principles, responsibilities, and procedures necessary to manage and mitigate information security risks in alignment with applicable laws, regulations, and industry best practices. The purpose of this policy is to ensure that all employees, contractors, and third parties understand their roles in protecting sensitive information and maintaining a secure computing environment. By fostering a culture of security awareness and accountability, this policy supports the organization's mission, enhances resilience against cyber threats, and helps maintain trust and compliance in an increasingly interconnected world.

All members of the organization are expected to adhere to the guidelines outlined in this policy. Regular review and continuous improvement of our security practices will ensure that we remain adaptive and responsive to evolving threats and technological advancements.

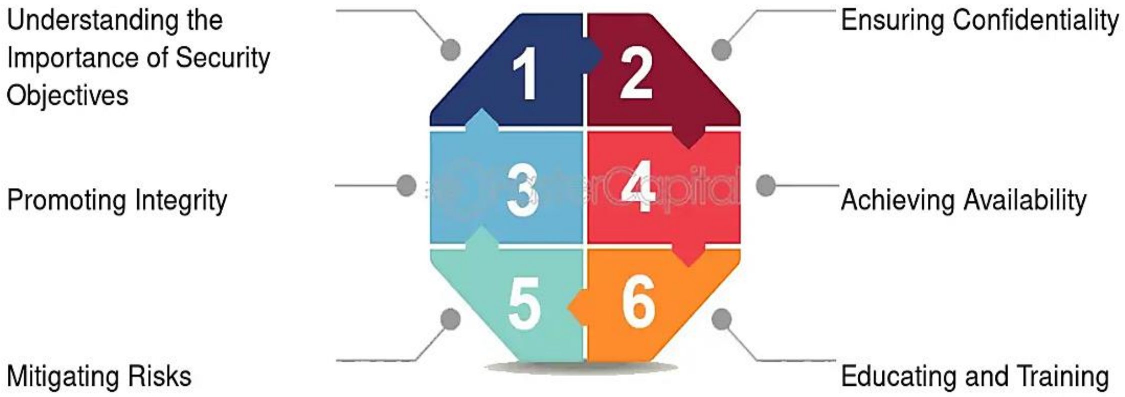

Figure 1: Specifying Security Goals - Security Policy Instruction: How to Develop and Apply Efficient Security Policies

In the digital era, cybersecurity has become a critical component of organizational resilience, operational continuity, and trust. As businesses, governments, and individuals increasingly rely on interconnected systems, cloud services, mobile technologies, and data-driven processes, the threat landscape has expanded in both scale and sophistication. Cyberattacks ranging from phishing and ransomware to advanced persistent threats (APTs) and state-sponsored espionage pose significant risks to the confidentiality, integrity, and availability of information systems and the sensitive data they contain. Cybersecurity (CS) is the practice of protecting computer systems, networks, programs, and data from digital attacks, damage, or unauthorized access. It involves using various technologies, processes, and behaviors to safeguard sensitive information and ensure the confidentiality, integrity, and availability of digital systems and data. Common cyber threats include malware, phishing attacks, and ransomware, making cybersecurity a critical practice for both individuals and organizations.

Cybersecurity is not merely a technical issue; it is a strategic imperative that spans people, processes, and technology. It involves the protection of networks, devices, programs, and data from digital attacks, damage, or unauthorized access. A robust cybersecurity posture requires a comprehensive, multi-layered approach that includes proactive risk assessment, continuous monitoring, incident response planning, employee awareness training, and compliance with regulatory standards such as GDPR, HIPAA, PCI-DSS, and NIST frameworks. This document outlines the organization's commitment to maintaining a secure cyber environment by establishing clear policies, governance structures, and technical controls. It emphasizes the shared responsibility of all stakeholders, executives, IT personnel, employees, contractors, and third-party vendors in identifying vulnerabilities, reporting suspicious activities, and adhering to security best practices. Given the evolving nature of cyber threats driven by emerging technologies like artificial intelligence, the Internet of Things (IoT), and remote work models, cybersecurity must be dynamic, adaptive, and integrated into every level of business operations. Regular audits, threat intelligence integration, penetration testing, and security awareness programs are essential components of a mature cybersecurity strategy.

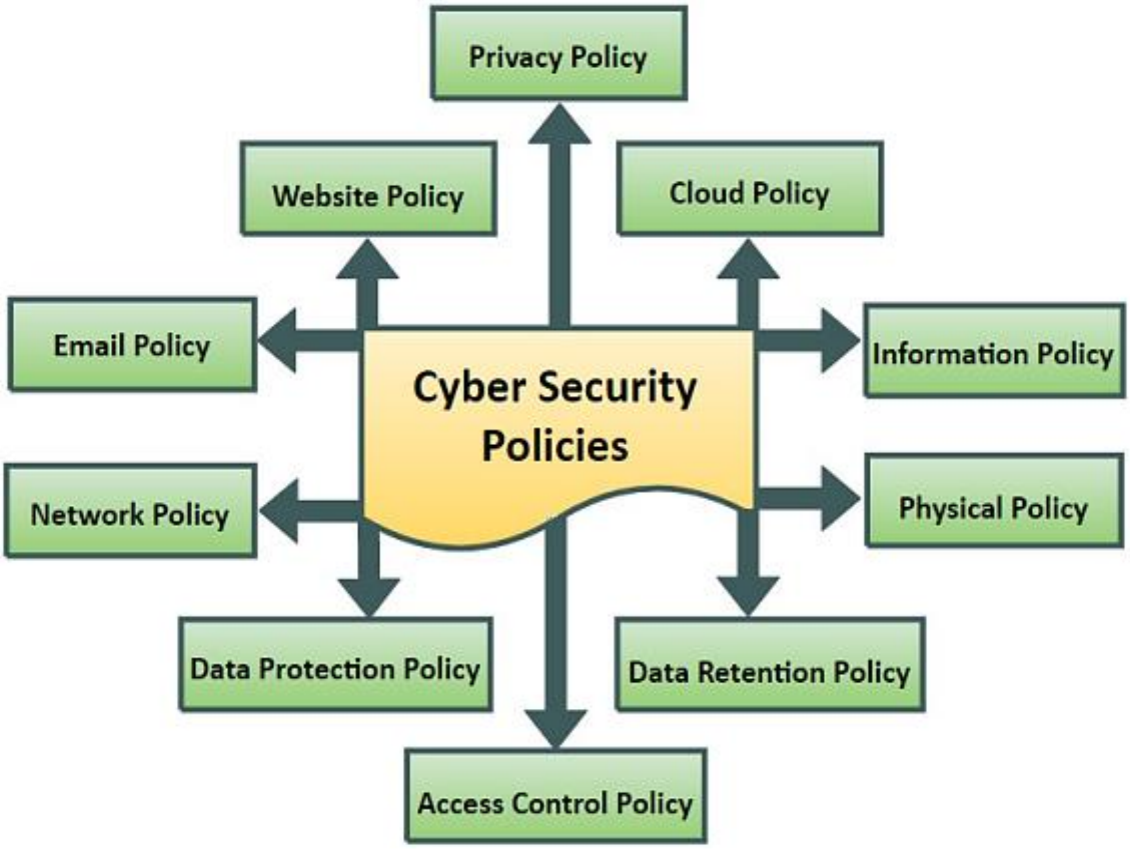

Figure 2: Taxonomy of cybersecurity policies.

The best CS policies for firms are not examined in current CS policy research, and little is known about the common characteristics of CS policies for many kinds. Additionally, a rise in cyberattacks on different companies in recent years has caused corporations to suffer catastrophic losses. Consequently, it has become evident that new techniques are needed to find the best and safest options for this use. The benefits of the new study include addressing more important security rules across a range of companies to give a thorough picture of the safe electronic community in these industries. Ten typical computer science components were found in the literature privacy, website, cloud, email, physical, network, information, access control, data retention, and data protection as illustrated in Figure 2.

Integrity keeps information reliable and guarantees that it is accurate and has remained in its original form throughout. Data that has been stored, shared, or utilized should never be changed without permission from a system or licensed person. Comprehending cybersecurity goals isn't

Doi : https://doi.org/10.21608/jaiep.2025.419694.1022
Received: August 30, 2025 Accepted: October 1, 2025

always simple. However, with a little dedication, structural improvements, and consistent monitoring, the CIA trinity objectives can be accomplished. Speaking of tools, the list is shown in Figure 3.

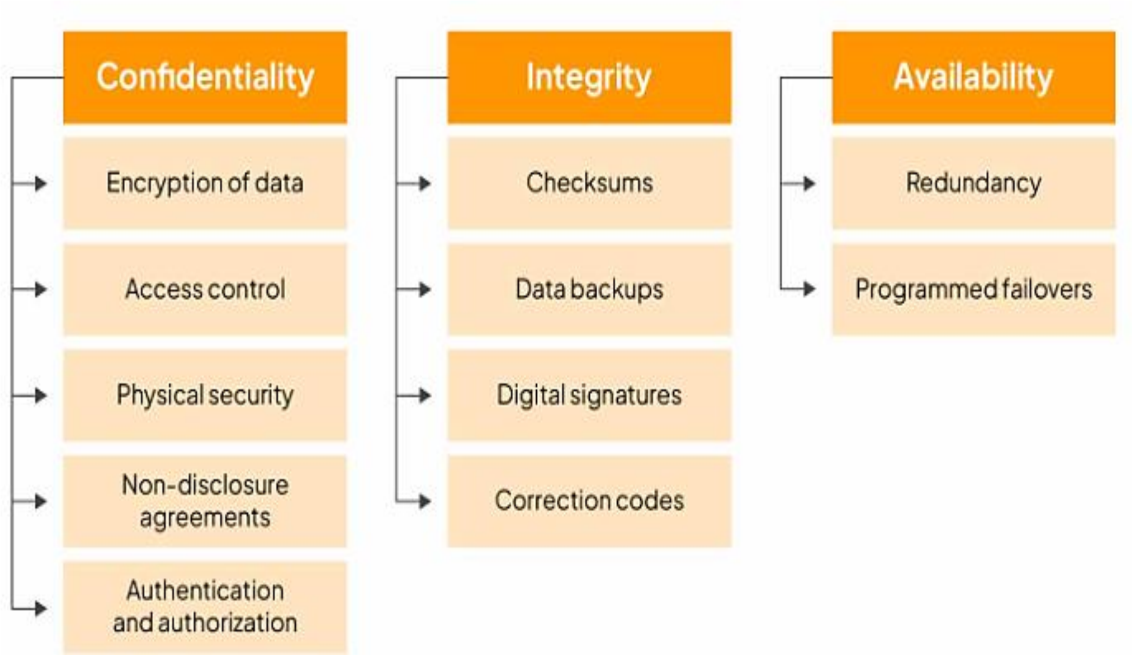

Figure 3: Cyber Security Goals: CIA Triad & Compliance Tools.

The primary risk factor has been identified is employees' disregard for the organization's information security policy [1–3]. Typically, businesses adhere to information security standards, which include guidelines for efficient information security administration. To guarantee the confidentiality, integrity, and availability of information, businesses should establish objectives and make a commitment to abide by the guidelines outlined in the standards. Workers should abide by the information security policies and standards they contain [4]. Additionally, companies should educate and train staff members on information security such that it is a task that will only benefit them [5]. Thus, the goal of this paper is to draw attention to the elements that affect workers' perceptions of adherence to the organization's information security policy.

This paper is structured as follows. In Section 2, we give a brief overview of the theoretical background of ISPs. Section 3 examines the hypotheses development in our study. In Section 4, we introduce the methodology used in our study. Section 5 offers an analysis and results. Finally, Section 6 provides some conclusions and recommendations.

2. Theoretical Background

In the digital age, where employee behavior is frequently seen as the weakest link in maintaining safe information systems, information security has emerged as a crucial organizational goal. Even if businesses use advanced technical security measures like intrusion detection systems, firewalls, and encryption, these measures are ineffective if employees do not comply with ISPs. As a result, theories from information systems, criminology, psychology, and organizational behavior have all been extensively included into studies on employee compliance. ISPs adherence by employees is a complex problem that can be analyzed from behavioral, cultural, motivational, and deterrent perspectives. Theories like PMT and TPB emphasize internal drives and perceptions, whereas deterrence emphasizes external enforcement. Organizational culture highlights the importance of shared ideals, while neutralization theory clarifies the justifications for infractions. When combined, these models show that compliance is influenced by organizational, contextual, and psychological elements and goes beyond simply observing the law. The security climate and corporate culture also have an impact on employees' compliance. Shared beliefs, customs, and procedures that put information security first are highlighted by a strong information security culture. Employees are more likely to internalize security procedures when they believe that management is committed to security and that peers are supporting compliance. From a socio-technical standpoint, compliance is not just a behavioral problem for individuals; rather, it is the result of interactions between people, technology, and organizational procedures. In order to promote voluntary compliance, effective ISPs need to be user-friendly, compatible with employees' work habits, and minimally interfere with productivity.

According to neutralization theory, employees intentionally break ISPs by using excuses to justify their actions, such as "I only did it to finish work faster" or "No harm will result." Managers can create awareness campaigns that refute popular defenses and lower deliberate noncompliance by having a better understanding of these arguments. Furthermore, according to the theory of planned behavior, employees' behavioral intentions, which are influenced by their attitudes toward compliance, subjective norms (the influence of peers and managers), and perceived behavioral control (the capacity to adhere to ISPs) are what determine compliance. By encouraging positive attitudes, creating supportive cultures, and lowering obstacles to policy adherence, organizations can increase compliance. The notion of protection motivation postulates that people follow security regulations when they are driven to defend their companies or themselves against alleged dangers. Assessments of threat (perceived severity and susceptibility) and coping (perceived effectiveness of the response, self-efficacy, and cost of compliance) have an impact on compliance. Employees are more likely to follow ISPs if they think that compliance is both practical and attainable and that threats are credible. According to the deterrence hypothesis, people are less inclined to act in a dangerous or noncompliant manner when they believe there will be harsh repercussions and frequent detection (Straub, 1990). Employees are likely to comply in the setting of ISPs when punishments for infractions are seen as clear, harsh, and immediate.

Comprehensive information security programs, which comprise security policies, security monitoring, security education, and security awareness, are adopted by some organizations. These programs have a major impact on compliance and, consequently, on the building of an organization's security culture [6-7]. Three levels could be distinguished in organizational culture. The organization's security measures are included in the first level, known as the object level. The second is the values level, which encompasses a range of activities like developing security policies, educating employees, and keeping an eye on information security. The organization's security perceptions, which serve as guidelines for employee behavior, make up the last level. According to study findings, merely understanding the security policy does not significantly help to organizational security culture if employees are not trained and made aware of it [7]. Several professional groups' safety cultures were examined by Ramachandran et al. [8]. It was discovered that different professional groups have different safety cultures. Nonetheless, the findings showed that an organization's safety culture is closely related to the team's perceptions of its identity, objectives, compliance, and hazards. Establishing an information security culture within the company requires open communication regarding information security-related matters. To create and implement an information security culture, staff members must be educated and conscious of their duties and obligations in regard to the security requirements of their company [9].

Employee adherence to the company's security policy is crucial to information security success. A security policy is a set of guidelines that an organization must adhere to in order to safeguard its resources. Employees are frequently the weakest link when it comes to information security, it is a truth [10]. An information security policy ought to specify the boundaries of permissible use of the organization's assets, the penalties for breaking the rules, the obligations that employees have to

Doi : https://doi.org/10.21608/jaiep.2025.419694.1022
Received: August 30, 2025 Accepted: October 1, 2025

the company regarding the security policy, and the necessary training. Furthermore, decision-makers' direction is crucial, mostly through affecting workers' emotions to prevent undesired non-compliance behaviors [11]. According to Hu et al. [12], employees' intentions dictate their behavior. Organizational culture has a crucial role in guiding objectives, fostering positive attitudes, and influencing employees' compliance behavior. Additionally, senior management hopes to positively impact employees' intention to adhere to the safety policy through its values and culture.

Safa et al. [13] investigate the elements that affect workers' perceptions of adherence to safety regulations within a company. The findings demonstrate that employee attitudes are positively impacted by information sharing, teamwork, experience, dedication, personal norms, and interventionist variables. Lastly, the study demonstrated that there is a high correlation between attitude and compliance, just as there is between intention and compliance.

People, method, and organization are the three primary categories into which Zammani and Razali [14] separate the success aspects of information security in an organization. Ineffective information security management has a significant financial impact on a company. Success factors in the people category include employees, the audit team, top management, and the information security management team, which needs to be constantly aware of emerging issues and obstacles. Success elements in the organization category include the information security policy, which needs to be understood and in line with the organization's goals and objectives, as well as the procedures for ensuring information security. Through their research, Ernest Chang and Ho [16] contend that the type and scale of the organization, the degree of environmental uncertainty, and the competence of the governing management all affect how well information security works. Organizations must adhere to international information security standards in order to guarantee information security. Employees should receive information security training, security personnel should be present, or this procedure should be contracted out [17].

The structural models that explain the relationships between employees at various organizational levels are known as organizational behavior models. Organizational models show how people and managers behave in general. The organizational model breaks down employee behavior into three tiers. Individual, group, and organizational levels are these three levels. The organizational behavior model takes into account three theoretical approaches: cognitive, behavioral, and social learning frameworks. This research explains how human behaviors impact organizations and how organizations impact people's behavior. The organizational behavior models listed below explain how businesses act to maximize output. It offers information about how workers interact, decide, and shape company culture, all of which have an impact on output and success in the long run. For managers, HR specialists, and leaders looking to enhance workplace dynamics and productivity, this model is essential.

On the other hand, the five main models of organizational behavior describe how managers and employees interact within organizations. The autocratic model is based on authority and control, where employees are expected to follow orders and contribute minimally out of fear or obligation. The custodial model emphasizes security and benefits, making employees dependent on the organization for welfare rather than motivated by performance. The supportive model shifts the focus to leadership and motivation, encouraging employee participation and job satisfaction. In the collegial model, teamwork and a sense of partnership prevail, with employees taking responsibility and contributing collaboratively. Finally, the system model emphasizes trust, shared values, and empowerment, fostering high commitment, self-motivation, and organizational citizenship. Together, these models illustrate the evolution of management practices from control and dependency to collaboration and empowerment [18]. Figure 4 offers the Types of organizational behavior models, various provide frameworks for understanding, analyzing, and predicting human behavior within organizations. These models guide leaders in creating effective management strategies.

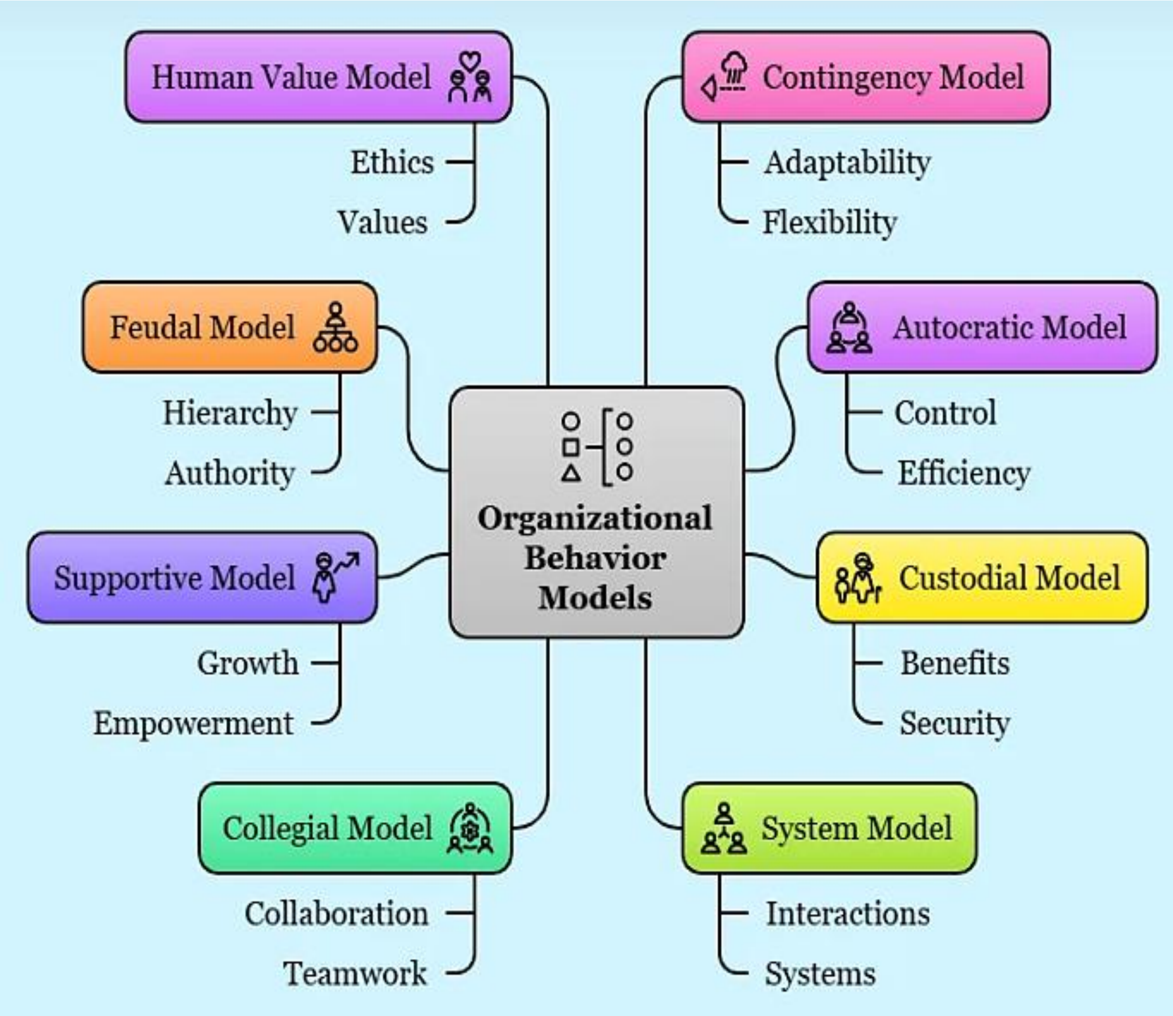

Figure 4: Types of Organizational Behavior Models.

3. Hypotheses Development

Different competitor theories based on different ideas have been provided by behavioral research on ISS. A preliminary study assessed the conceptual and basic similarities between these models and proposed a single combined hypothesis known as the unified model of information security policy compliance (UMISPC). Different data methodologies were used to evaluate the preliminary model. Habit, role values, reaction efficacy, danger, fear, and neutralization were the only six independent variables that had an impact on the reactance construct and/or intention to follow ISPs [19]. The other three punishments, cost/rewards, and enabling conditions showed no discernible impact. As a result, UMISPC (see Figure 5) was used as the foundational theory in this work to evaluate the empirical validity and fill in the ongoing research gaps. Moreover, machine learning models can also be used as in [20].

Doi : https://doi.org/10.21608/jaiep.2025.419694.1022
Received: August 30, 2025 Accepted: October 1, 2025

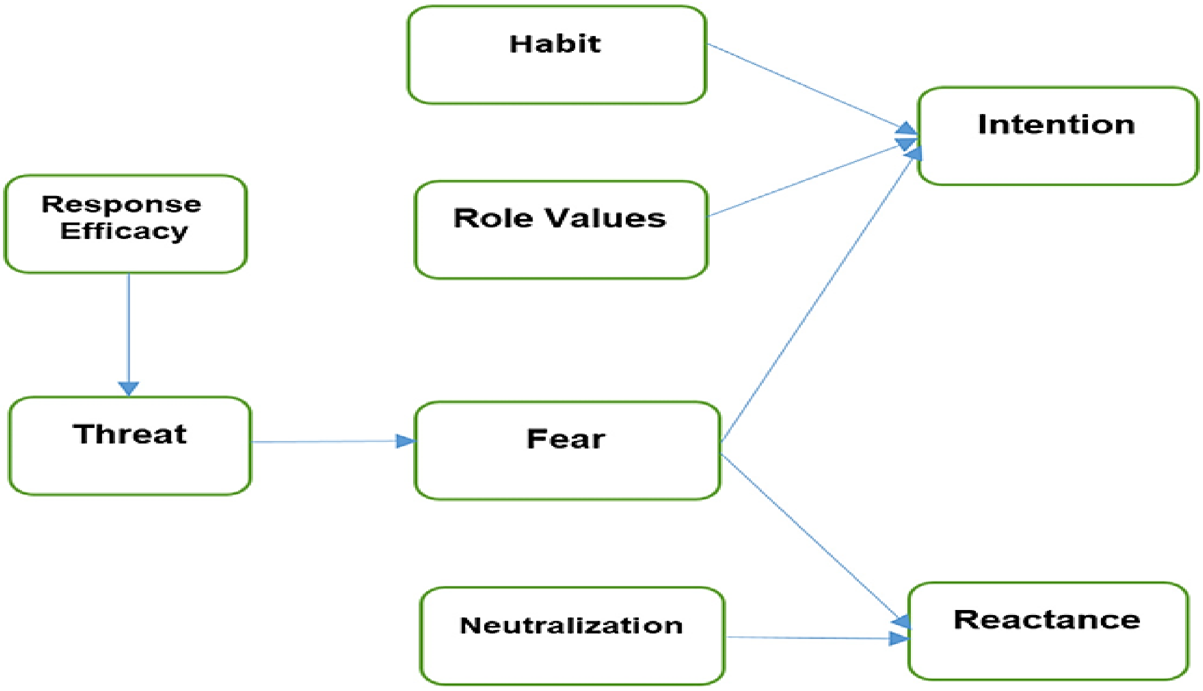

Figure 5: The Unified Model of Information Security Policy Compliance Developed by Gerdin [21].

The following hypotheses are postulated:

H1. The behavior of an employee toward the information security policy is favorably correlated with his or her knowledge of information security

H2. The intention to adhere to the organization's information security policy is positively influenced by an employee's attitude toward doing so.

H3. The identified fear of an employee will be positively impacted by the perceived threat.

H4. The intention of an employee to adhere to the organization's information security policy is positively influenced by their self-efficacy in doing so.

H5. An employee's perceived cost of compliance affects how they feel about adhering to the information security policy criteria.

H6. The intention of an employee to adhere to the information security policy requirements is positively influenced by their opinions regarding compliance with the organization's information security policy.

H7. The identified fear of an employee will be positively impacted by the perceived threat.

4. Methodology

Employees of businesses with information security policies in place were given the questionnaire. A total of 985 companies and organizations from multiple divisions received the questionnaire in Egypt. 303 workers from various industries took part in the poll. The two primary study trends about the intention to adhere to the information security policy requirements are incorporated into the questionnaire, which is based on earlier studies [2, 10, 12, 18]. The five-point Likert scale was employed to operationalize the constructs mentioned above. The data was analyzed using multivariate regression analysis. To determine whether the suggested constructs were reliable indicators of intention or reaction toward adherence to information systems security policy, this was accomplished using structural equation modeling (SEM). Data analysis was conducted using SmartPLS version 3.3.9.

5. Analysis and Results

5.1. Sample characterization

In order to test the measurement model, an appraisal protocol was performed, incorporating the steps outlined below. As shown in Table 1, the demographic profile and sample characterisation guarantee the representativeness of the data and offer a clear knowledge of the participants' backgrounds. The study illustrates the diversity and dispersion of the sample by defining important characteristics, including age, gender, education level, work experience, and employment sector. Since demographic factors frequently affect attitudes, actions, and reactions, this information is crucial for interpreting the results. By demonstrating that the sample is suitable for addressing the study objectives and may provide a trustworthy foundation for extrapolating findings, a well-described demographic profile further enhances the validity of the research. On the other hand, the dataset must also be free of missing values and outliers to ensure reliable and highly efficient results. If the dataset contains missing values or outliers, they must be handled. For more details on methods for handling these problems, see, e.g., [22-31].

Table 1: Sample Characterization

Characterization	Scale	Frequency	Percent
Gender	Male	157	51.815
	Female	146	48.185
Age	Less than 30	59	19.472
	31–40	83	27.393
	41–50	93	30.693
	More than 50	68	22.442
Education	High School	22	7.261
	Diploma	66	21.782
	Bachelor	123	40.594
	Postgraduate	92	30.363
Job Experience	Less than 5 Years	78	25.743
	5–10 Years	132	43.564
	Above10Years	93	30.693
Employment Sector	Private	140	46.205
	Public	163	53.795
Total		303	100%

5.2. Measurement Model

In order to validate the measurement model using SEM, the article relied on SmartPLS as its main software tool. Through factor loading calculations, the SmartPLS framework enables researchers to assess the connections between latent constructs and observable variables. As advised by [32], items with loadings of 0.70 or above were kept because they show a great indication of reliability and validate that each item accurately reflects the underlying concept. High degrees of accuracy, validity, and reliability were shown by the finished measurement model, providing a strong foundation for further structural research. The SEM approach is suitable for evaluating hypotheses in intricate theoretical models because it enables researchers to examine reflective and formative constructs. The output of the SEM method indicates that the majority of the items had factor loadings greater than 0.70. According to the standard SEM recommendations, items with low loadings serve as poor markers of the corresponding latent constructs, which might hurt the measurement model's validity and reliability. The removal of these components became important to better model fit and retain unidimensional measurement for each construct.

Doi : https://doi.org/10.21608/jaiep.2025.419694.1022
Received: August 30, 2025 Accepted: October 1, 2025

A few descriptive and inferential statistics are shown in Table 2. Furthermore, a popular coefficient of internal consistency that assesses how well a collection of test or scale items consistently evaluates the same underlying construct is Cronbach's alpha. Cronbach's alpha came out to be 0.8649. This high number suggests that the items are closely connected and produce similar scores, as well as more internal consistency.

Table 2: Descriptive Statistics for All Variables.

Variables	Mean	Std. Deviation
Attitude	4.5208	0.60481
Intention	4.5679	0.53392
Fear	4.2716	0.67464
Self-efficacy	3.6204	1.14064
Beliefs	4.4105	0.60563
Perceived cost	4.8148	0.43791
Response Efficacy	4.0221	0.9873

Table 3 displays the results of the discriminant validity assessment using the Fornell-Larcker criterion. On the diagonal (bold) are the square roots of the Average Variance Extracted (AVE) for each construct, all of which are higher than the off-diagonal correlations with other constructs. As a result, all of the study's variables have sufficient discriminant validity, as each construct has more variance with its own items than with those of other constructs.

Table 3: Evaluation of Discriminant Validity Using the Fornell-Larcker Criterion.

Variables	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Attitude	**0.8435**						
Intention	0.1427	**0.8172**					
Fear	0.2783	0.0956	**0.9173**				
Self-efficacy	0.0189	0.1973	0.2134	**0.8873**			
Beliefs	0.0637	0.0983	0.0142	0.0603	**0.8693**		
Perceived cost	0.5638	0.0641	0.0468	0.0948	0.2126	**0.8329**	
Reactance	0.4832	0.0284	0.0732	0.7583	0.3981	0.5829	
Response Efficacy	0.3621	0.0525	0.0334	0.2831	0.1946	0.6082	**0.9038**

The Hetero-trait/Monotrait (HTMT) ratio is used in Table 4 to evaluate discriminant validity. Each construct retains its uniqueness from the others, as evidenced by the HTMT values in Table 4 being less than 0.85.

Table 4: Heterotrait/Monotrait Ratio-Based Discriminant Validity Evaluation.

Variables	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Attitude	---						
Intention	0.2541	---					
Fear	0.4821	0.0745	---				
Self-efficacy	0.0379	0.2893	0.1927	---			
Beliefs	0.0584	0.0736	0.0154	0.0378	---		
Perceived cost	0.7832	0.0593	0.0487	0.0429	0.1873	---	
Reactance	0.3762	0.0732	0.0693	0.6532	0.1732	0.6831	
Response Efficacy	0.4283	0.0863	0.0893	0.3923	0.3876	0.9835	---

Figure 6 displays the path coefficients (β) from the construct relationships in the SEM model. The structural model results lead to the model seeming to have a significant predictive ability. The hypothesis test findings for the proposed structural model are shown in Table 6, emphasizing the extent and importance of the correlations between the variables. T-statistics, p-values, path coefficients, and the ultimate determination of each hypothesis's level of support are important metrics. The results indicate that several predictors have a statistically significant effect, since all the study hypotheses were accepted except for the second hypothesis, which was not statistically significant. The current study's findings indicate that employees' desire to adhere to the ISPs is correlated with their attitude, normative views, and self-efficacy.

Table 5: Results of Hypotheses Testing.

Hypothesis	Path	***β*** coefficients	***T***-Statistics	***p***-values	Decision
H1	Intention → Attitude	0.582	14.165	0.000	Supported
H2	Fear → Attitude	0.049	0.893	0.373	Not Supported
H3	Self-efficacy → Attitude	0.131	1.98	0.048	Supported
H4	Self-efficacy → Perceived cost	0.266	5.017	0.000	Supported
H5	Beliefs → Perceived cost	0.267	5.056	0.000	Supported
H6	Reactance → Self-efficacy	0.486	9.347	0.000	Supported
H7	Reactance → Response Efficacy	0.511	11.138	0.000	Supported

Doi : https://doi.org/10.21608/jaiep.2025.419694.1022
Received: August 30, 2025 Accepted: October 1, 2025

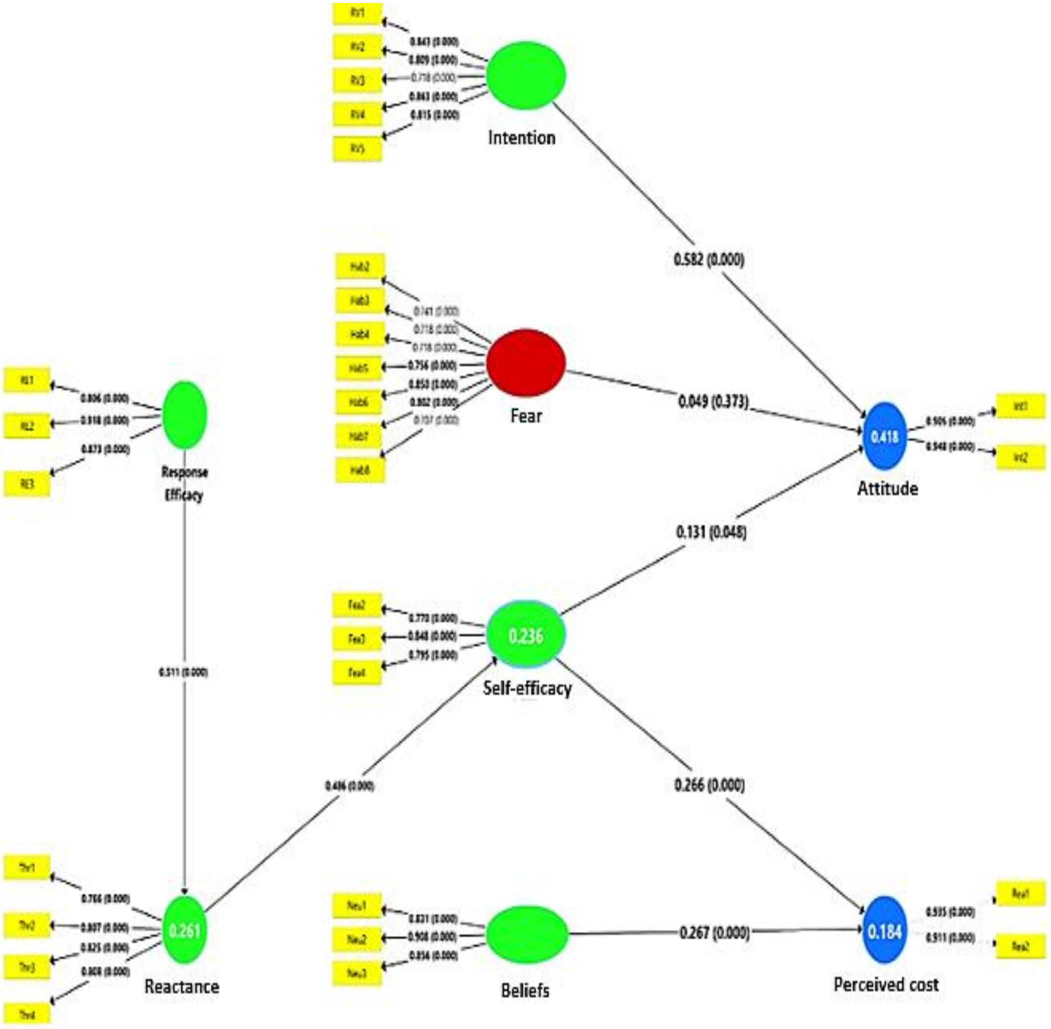

Figure 6: Coefficients for Structural Model Paths**.**

6. Conclusion

The survey's findings demonstrated that a large number of workers lacked a thorough understanding of the rules outlined in their company's information security policy, demonstrating the necessity of educating and training staff members on security procedures. It's also important to note that only a small portion of survey respondents said that following the company's information security policies would increase their profits. For this reason, it would be advantageous for businesses to provide employees with more incentives to follow the information security policy. Employees do, however, intend to abide by the information security regulations of the companies; thus, any company might benefit from this circumstance with the appropriate tactics. As a result, many businesses do not give information security the consideration it requires. Information security policies should be established, goals should be set, and employees should be trained and made aware of the importance of adhering to information security policies because their role is critical to the integrity of the resources and, consequently, the businesses themselves. Technological solutions alone are insufficient for information security in organizations.

The main emphasis of this study was on how employees perceived problems pertaining to their adherence to the information security policies of the organizations they work for. It is suggested that a thorough investigation of the variables and incentives influencing employees' adherence to information security policy be conducted. In order to achieve effective employee compliance, the results may serve as recommendations for execution by the company's managers. According to the aforementioned concept, research might focus on managers' behavior and actions that encourage staff members to adhere to information security standards, in addition to employee behavior and intention. The most successful information security rules could also be researched. Lastly, examining workplace and employee characteristics in connection to their adherence to information security standards is a recommendation for additional research. Workplace, educational, and personal qualities may all have an impact on ISPs compliance.

Conflict of interest: The authors declare that they have no conflict of interest.

Data Availability: The data is available in this article.

References

1. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.
   Koohang, A., Anderson, J., Nord, J. H., & Paliszkiewicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*, *120*(1), 231-247.
2. Williams, A. S., Maharaj, M. S., & Ojo, A. I. (2019). Employee behavioural factors and information security standard compliance in Nigeria banks. *Int. J. Comput. Digit. Syst*, *8*(4).
3. Li, Y., Pan, T., & Zhang, N. (2020). From hindrance to challenge: How employees understand and respond to information security policies. *Journal of enterprise information management*, *33*(1), 191-213.
4. AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in human behavior*, *49*, 567-575.
5. Chen, Y. A. N., Ramamurthy, K., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11-19.
6. Ramachandran, S., Rao, C., Goles, T., & Dhillon, G. (2013). Variations in information security cultures across professions: A qualitative study. *Communications of the Association for Information Systems*, *33*(1), 11.
7. Solomon, G., & Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management*, *34*(4), 1203-1228.
8. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548.
9. Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, *22*(1), 42-75.
10. Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.
11. Zammani, M., & Razali, R. (2016). Information security management success factors. *Advanced Science Letters*, *22*(8), 1924-1929.
12. Ernest Chang, S., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345-361.

Doi : https://doi.org/10.21608/jaiep.2025.419694.1022
Received: August 30, 2025 Accepted: October 1, 2025

13. Yildirim, E. Y., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, *31*(4), 360-365.
14. Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems*.
15. Kamarova, S., Gagné, M., Holtrop, D., & Dunlop, P. D. (2025). Integrating behavior and organizational change literatures to uncover crucial psychological mechanisms underlying the adoption and maintenance of organizational change. *Journal of Organizational Behavior*, 46(2), 263-287.
16. Kamel, A. R., & Alqarni, A. A. (2022). A New Approach for Model Selection with Two Qualitative Regressors. *Computational Journal of Mathematical and Statistical Sciences*, *1*(1), 63-79.
17. Almetwally, E. M., Elbatal, I., Elgarhy, M., & Kamel, A. R. (2025). Implications of machine learning techniques for prediction of motor health disorders in Saudi Arabia. *Alexandria Engineering Journal*, *127*, 1193-1208.
18. Gerdin, M. (2025). Validating and extending the unified model of information security policy compliance. *Information & Computer Security*, *33*(1), 25-48.
19. Kamel, A. R. (2021). *Handling outliers in seemingly unrelated regression equations model*, MSc thesis, Faculty of graduate studies for statistical research (FGSSR), Cairo University, Egypt.
20. Youssef, A. H., Abonazel, M. R., & Kamel, A. R. (2022). Efficiency comparisons of robust and non-robust estimators for seemingly unrelated regressions model. *WSEAS Transactions on Mathematics*, *21*, 218-244.
21. Youssef, A. H., Kamel, A. R., & Abonazel, M. R. (2021). Robust SURE estimates of profitability in the Egyptian insurance market. *Statistical journal of the IAOS*, *37*(4), 1275-1287.
22. Abonazel, M., & Rabie, A. (2019). The impact of using robust estimations in regression models: An application on the Egyptian economy. *Journal of Advanced Research in Applied Mathematics and Statistics*, *4*(2), 8-16.
23. Alharbi, Y. S., & Kamel, A. R. (2022). Fuzzy System reliability analysis for Kumaraswamy distribution: bayesian and non-bayesian estimation with simulation and an application on cancer data set. *WSEAS Transactions on Biology and Biomedicine*, *19*, 118-139.
24. Alghamdi, F. M., Kamel, A. R., Mustafa, M. S., Bahloul, M. M., Alsolmi, M. M., & Abonazel, M. R. (2024). A statistical study for the impact of REMS and nuclear energy on carbon dioxide emissions reductions in G20 countries. *Journal of Radiation Research and Applied Sciences*, *17*(3), 100993.
25. Alharbi, A. A., Kamel, A. R., & Atia, S. A. (2022). A New Robust Molding of Heat and Mass Transfer Process in MHD Based on Adaptive-Network-Based Fuzzy Inference System. *WSEAS Transactions on Heat and Mass Transfer*, *17*, 80-96.
26. Kamel, A. R., Alqarni, A. A., & Ahmed, M. A. (2022). On the Performance Robustness of Artificial Neural Network Approaches and Gumbel Extreme Value Distribution for Prediction of Wind Speed. *Int. J. Sci. Res. in Mathematical and Statistical Sciences Vol*, *9*(4).
27. Kamel, A. R., & Abonazel, M. R. (2023). A simple introduction to regression modeling using R. *Computational Journal of Mathematical and Statistical Sciences*, *2*(1), 52-79.
28. Abonazel, M. R. (2020). Handling outliers and missing data in regression models using R: Simulation examples. *Academic Journal of Applied Mathematical Sciences*, *6*(8), 187-203.
29. Kline, R. B. (2023). *Principles and practice of structural equation modeling*. Guilford publications.