The Effect of Information Security on the Trust of Users of Information Systems in the Tourism Sector

Jamil Saleh Issa[1], **Ali Moneer Albahloul**[2]

[1]Lattakia University, Department of Business Administration, Syria
ORCID: https://orcid.org/0009-0005-8042-6793

[2]Lattakia University, Department of Business Administration, Syria
ORCID: https://orcid.org/0009-0007-7418-2635

Abstract: The study aimed to explore the impact of information security on the confidence of information system users in the Syrian tourism sector. In this study, the quantitative descriptive approach was adopted to describe the studied phenomenon related to the studied variables. The analysis was conducted on 396 data obtained by simple random sample**.**

The study results showed varying significant effects of information security dimensions on user trust, security regulation and security policies having the greatest impact, while individual security had an inverse effect, information maintenance had a weak effect, and asset control had no significant effect. The results confirmed that information security policies are a fundamental pillar of building trust, whether through access and authorization policies, two-factor authentication, encryption, ongoing employee training, or data backup.

The outputs of the current study offer several recommendations for decision-makers in the tourism sector, highlighting the potential for leveraging information security as a competitive advantage to enhance the position of Syrian tourism in regional and international markets.

Keywords: information security, user trust, information systems.

JEL Classification: M15, D83, O33

1 Introduction

In today's business environment, organizations need accurate, up-to-date and reliable information to reach effective decisions at all levels. With the rapid development of information technology, information networks, wired and wireless networks have emerged, expanding their scope of use to simplify and accelerate human activity in all fields. This has led to a tremendous growth in data and information, making it necessary to find a means through which data and information can be collected, stored, retrieved and used when needed (Lis et al., 2020).

All this has prompted organizations to develop an information system that provides technical support for the basic administrative functions of planning, organizing, directing, controlling in business organizations, and achieves quality in administrative decision-making, in addition to providing satisfaction and confidence among users about its basic outputs (Quyet et al., 2023).

On the other hand, information security and its systems in the digital environment represent the protection of information in terms of its availability, trust and integrity. An information security program usually includes two basic elements: Risk analysis and Risk management.

The risk analysis journey takes into account the compatibility of the data and information repository with all available system in the organization, while risk management includes control methods and security measures that reduce the organization's exposure to various risks. Therefore, information security is one of the infrastructure's elements that must be available for information system, through which particular policies for the individuals and information security is determined, as well as the roles and responsibilities of users, security personnel and members of the information systems management committee are defined (Anday et al., 2012).

The domestic tourism industry continues to grow and develop by the travel management system through online which ensures a provision of diverse, safe, accurate and comprehensive services to meet users' preferences. As tourism computerization is a vital factor in the sustainable development of the tourism sector, especially in light of using modern information and internet technology that has contributed to introducing new changes in management and important updates to the quality of tourism services. (Nan & Kanato, 2021).

The value that information and communication technology has created to develop the global tourism infrastructure is interesting. When a tourist can view tourism information in a country via the World Wide Web and obtain appropriate audio-visual and tourism information, he will be interested and sense his needs through it. Therefore, the need for a secure information system has become an imperative necessity so users could receive relevant information and services(Aghdaie & Katebi, 2016).

Tourism organizations use several methods and standards to conduct security audits and determine whether information systems are secure to assess risks and protect the organization's assets, as they need an effective information security framework by following clear standards for IT governance in a tourism field (Panjaitan et al., 2022).

In tourism organizations, successful implementation of information security policies plays a crucial role in protecting data and mitigating potential breaches. One critical aspect is user awareness and training programs that are provided. Several key elements contribute to the effectiveness of an information security policy, such as clear guidelines and procedures to define expected behaviors regarding handling information, defining roles and responsibilities clearly so users are aware of their duties in maintaining security protocols (Rostami et al., 2023).

On the other hand, the fact that there is no effective information security system means that there is a lack of some elements of trust in all information systems. Users have to be sure that their privileges will not be offended by supervisors who in turn have to trust that users will behave well and not expose the system to danger. Also, the developer of the information system must have confidence that they will provide a good and secure system with minimal errors and will fulfill their obligations that related to the information security policy (Hakkala et al., 2018).

Information security policy builds trust and improves decision-making. Therefore, information security systems must include both, explanatory power and transparency as key elements in their design to enhance users' trust and compliance with information security and protection policy (Zywiolek, 2024).

This research highlights the impact of information security policy on the trust of users in information systems in Syrian tourism environment. Especially in light of the difficulties and challenges faced by tourism organizations in Syria which related to information security and protection policy. The importance of the relationship between information security and users' trust in the tourism field is reflected in the link between information security and the protection of all resources that are used to process information. This includes protecting each of organization, individuals, computers and information media which contains organization's data through procedures and means of protection that include integrity, confidentiality, validity of information security. Users' trust in the efficiency of information system is about a continuous improvement system of security, human and technical operations to minimize and contain expected risks.

The second section of the paper format includes a literature review related to information security and users' trust in the information system, while the third section includes comprehensive details of the used data in the study and hypothesis testing with the final results.

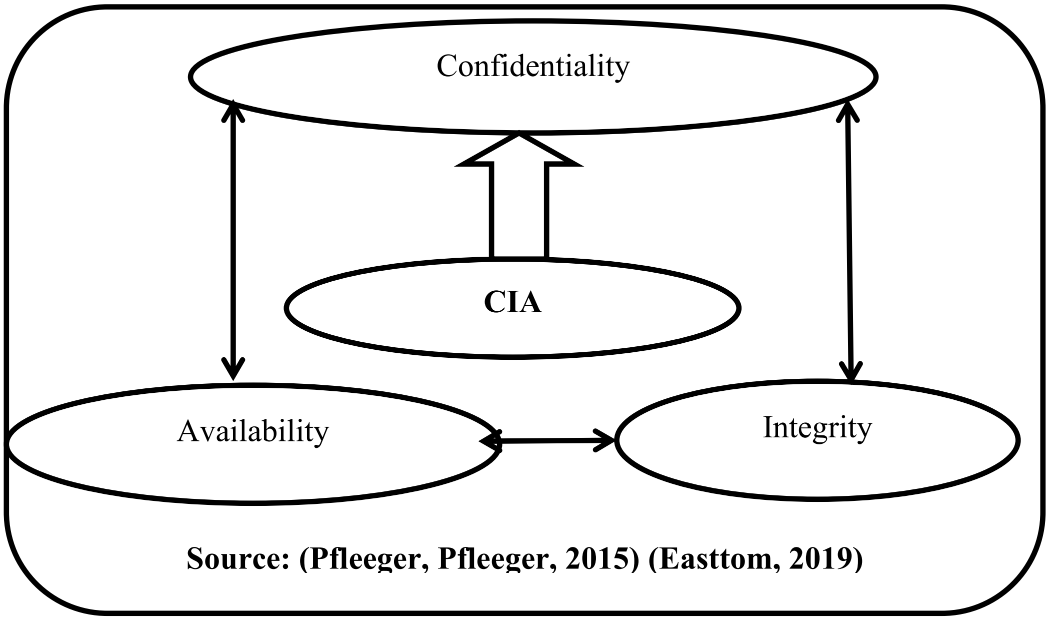
2 Literature Review

2.1 The concept of Information security

Information security represents one of the elements of the basic infrastructure that must be available for the information system, which requires the existence of a general framework for security policies in the organization that includes natural security, personnel security and information security. Information security refers to the protection of information and its important elements, including systems and devices that use, store and send this information (Whitman & Mattord, 2005). Technical and non-technical solutions are expressed in the technical field of information security which aim to use technology as a means to eliminate any security breach of systems (Victoria, 2010). (Campbell, 2016) confirms that information security refers to the set of processes or standards and mechanisms which protect information against an unauthorized access, misuse or destruction with the aim of ensuring the integrity of information, this applies to any form of information, whether traditional or digital. We emphasize that the concept of information security in tourism organizations includes all procedures are used to protect information and everything related to such as, processing, transfer, preservation, and storage tools from any harm or misuse, this needs the existence of an information security system which ensures that the information has confidentiality, integration, content integrity and continued availability.

Information security depends on three basic elements that must be available in the information that requires protection, these elements are confidentiality, integrity, and information availability, which are known as the CIA Triangle. They are considered the main elements of any information system according to the standards of information security and management policies, as shown in figure(1) (Pfleeger, Pfleeger, 2015) (Easttom, 2019):

Figure 1
Information security elements



Source: (Pfleeger, Pfleeger, 2015) (Easttom, 2019)

Implementing and operating an information security system is a way of life that depends on four major components that must be dealt with as integrated manner ,as follows (Andress, 2014) (Kaaria, 2023):

- Operations: Operations are an essential and indispensable component for any information security system, they are major and have a continuous nature.
- Human Resources: include employees, consultants, contractors, and technicians who perform all operations and services.
- Technology: Technology is ready, available and its products have a relatively short life cycle. Also, technology market has a competitive in nature.
- Culture: It is related to the interpretation of business environment and organization's ethics towards society.

Information security risks can be classified into three different categories as follows: physical risks, electronic information risks, and internal risks, which can be explained as follows:

- Physical risks: they are a result of physical access to the components of information security system or a damage in the available resources for information security.
- Electronic risks: often come outside the information security system by people who are not related to or do not have access rights. It is about hacking information, breaching regulatory and security controls of the system to obtaining confidential information.
- Internal risks: There are several risks that originate from within the information security system, whether from a human factor, a deficiency in the system, or a penetration of its structure represented by its physical components of hardware and software.

2.2 Trust building in the information system

With technological progress and increasing development in the field of information security, creating and maintaining trust among users of the information system is one of the pivotal elements of the organization's success by its application of the large-scale information system in order to improve the quality of provided services in all fields (Maqableh et al., 2021).

Users of information systems and its applications must trust the organization's digital environment by running as scheduled without any malfunctions, problems or errors. Therefore, access to secure networks and a preparation of controlling security standards comes as a result of user requirements, the loss of confidence in the information system and the application that based on it, stems from misuse, failure to meet expectations, and uncertainty about the final outputs. Therefore, digital information systems need to build acceptable procedures and rules to all parties dealing with it in order to provide environment that increase trust and credibility in these systems (Wang, 2023).

On the other hand, judgment on the reliability of information systems and ensuring their credibility is determined by five basic principles which the information system must meet in order to be relied upon, namely: Information Security, Information Confidentiality, Information Privacy, Information Safety and Readiness. Trust System identifies four requirements for implement the five principles successfully: Development policies, Communicate policies effectively to all its users, Design appropriate control procedures to implement policies and Monitor the system to take appropriate actions to maintain compliance with policies through the support of senior management(Romey & Steinbart, 2018).

2.3 Research hypothesis

Based on the above literature, the main research hypothesis is that information security, which can be measured by security policy, security organization, personnel security, information maintenance, and asset control, is positively related to the trust of information system users in the tourism sector.

3 Methodology and Tools

3.1 Data and variables

The quantitative descriptive approach was adopted to describe the studied phenomenon related to the studied variables in detail in the Syrian tourism environment. The questionnaire was used as a study tool based on the five-point Likert scale according to five degrees (1: strongly disagree, 2: disagree, 3: neutral, 4: agree, 5: strongly agree). The quantitative data was collected and analyzed statistically using the Amos-V23 program.

A questionnaire was developed to measure the independent variable (information security) based on the studies of (Shahrani, 2019) (Azzoug & Chelouache, 2023) (Shaddood, 2023) (Quyet et al., 2023), and the dependent variable (user confidence) based on the studies of (Bejjar & Boujelbene, 2013) (Maqableh et al., 2021) (Rabbani et al., 2023) (Zywiolek, 2024).

The research population was represented by managers, department heads, administrators, and technicians in Syrian tourism organizations. Considering that the research population numbered more than 6,000 individuals, we relied on a simple random sample from the studied population using the following probability law (Krejcie & Morgan, 1970):

$$n = \frac{\chi 2\ \mathrm{NP}(1-\mathrm{P})}{d^2(N-1) + \chi 2\ \mathrm{P}(1-\mathrm{P})} = \frac{3.841 * 6500 * 0.5(1-0.5)}{0.05^2(6500-1) + 3.841 * 0.5(1-0.5)} = 363$$

512 questionnaires were distributed, 448 of which were returned, 52 questionnaires were excluded due to their invalidity, and 396 questionnaires were valid for analysis.

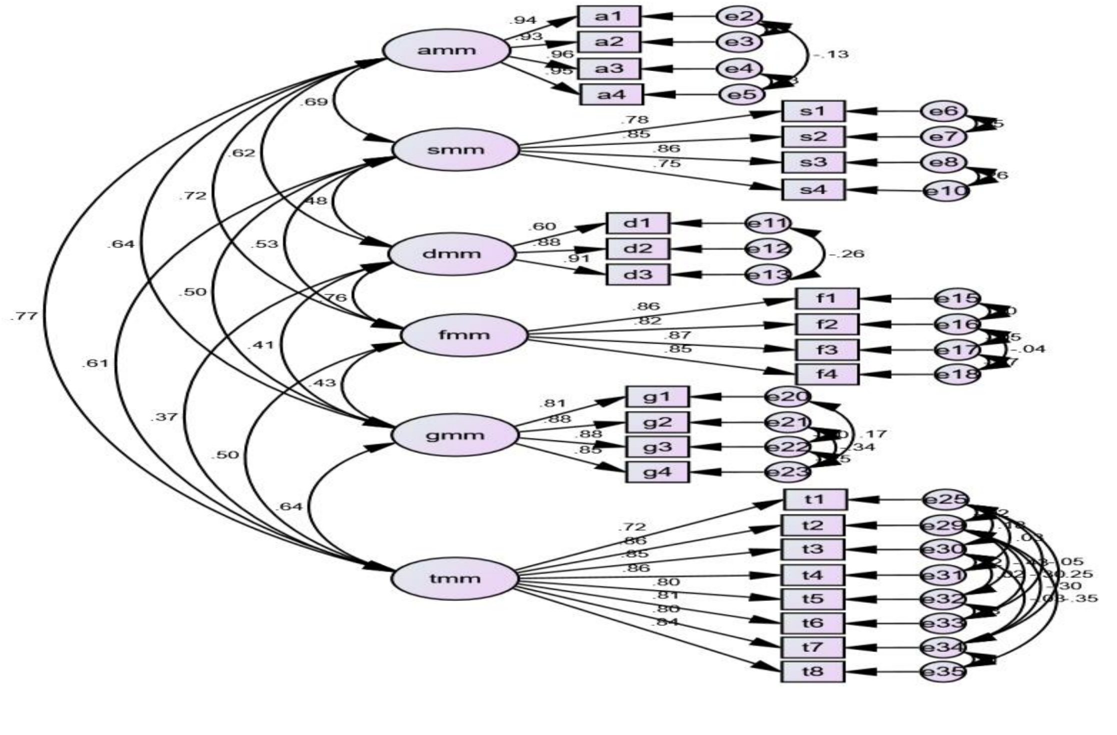
3.2 Validity and Reliability of the Scale

3.2.1 Convergent Validity of the Scale

The researchers verified the validity of the data by verifying the validity and reliability of the scale. Convergent validity was confirmed by relying on confirmatory factor analysis. The model, which consists of 6 main variables, was built and designed based on AMOS 23 by entering 5 independent variables and the dependent variable according to the figure(2):

Figure 2

Confirmatory analysis model for the study dimensions



Source: Prepared by the researchers based on AMOS 23 outputs

Through the results of the confirmatory factor analysis of the model, the value of the chi-square coefficient was equal to 548.0 and the degrees of freedom df was equal to 281. The value of the χ2/df index was equal to 548/281 = 1.950, which is less than 3, indicating a good degree of fit for the hypothetical model for the studied data (Carmines & McIver, 1981). The value of the comparative fit index (CFI) was equal to 0.973, which indicates a high degree of fit for the proposed hypothetical model (Hu & Bentler, 1999). The value of the TLI (Tucker-Lewis coefficient) was equal to 0.966, which indicates a high degree of fit for the hypothetical model studied (Kyriazos, 2018), since the model's fit increases as it approaches one, the value of the root mean square of the residuals (RMR) was equal to 0.04, which is less than 0.05, is a value close to zero, indicating a high degree of model fit, the GFI coefficient value is equal to 0.905, and all of them are greater than 0.9, indicating a high degree of model fit (Bentler, 1990) The RMSEA value was 0.049, which is less than 0.05, indicating the model's fit (Kenny, 2006).

3.2.2 Content Validity

In order to ensure the validity of the content, the degree of saturation of each of the model elements was relied upon. The degree of saturation for each of the used statements in measuring the six questionnaire axes ranged between 0.600 and 0.962, which is greater than 0.5, the value of the average variance extracted index (AVE) ranged between 0.653 and 0.894, and all of which are greater than 0.5, which means that each axis is able to explain more than half of the variance of its indicators, which means that the condition of content validity for the scale was met (Urbach & Ahlemann, 2010).

3.2.3 Discriminant Validity

Table 1

Discriminant validity of the model

	CR	AVE	MSV
gmm	0.917	0.734	0.410
amm	0.971	0.894	0.591
smm	0.885	0.658	0.482
dmm	0.846	0.653	0.582
fmm	0.914	0.728	0.582
tmm	0.942	0.669	0.591

Source: Prepared by the researchers based on AMOS 23 outputs

From Table (1), the values of the maximum common variance index (MSV) for all the questionnaire axes were smaller than the corresponding average variance extracted values (AVE), which were all greater than 0.5.

Table 2

values of the square root of the average variance extracted

	MaxR (H)	gmm	amm	smm	dmm	Fmm	tmm
Gmm	0.920	0.857					
Amm	0.973	0.636	0.946				
Smm	0.891	0.502	0.694	0.811			
Dmm	0.898	0.406	0.620	0.484	0.808		
Fmm	0.916	0.429	0.723	0.530	0.763	0.853	
Tmm	0.945	0.640	0.769	0.614	0.371	0.498	0.818

Source: Prepared by the researchers based on AMOS 23 outputs

From Table (2), the values of the square root of the average variance extracted (shown diagonally in bold black) were greater than the values of their correlation coefficient with the other dimensions. Through the above, the condition of discriminant validity for the used study tool was met (Almen et al, 2018).

3.2.4 Scale Reliability

Table 3

Scale Reliability

	code	N of Items	Cronbach's Alpha	CR
Security Policy	gmm	4	0.903	0.917
Security regulation	amm	4	0.972	0.971
Information maintenance	smm	4	0.893	0.885
Individual security	dmm	3	0.819	0.846
Asset control	fmm	4	0.912	0.914
User trust	tmm	8	0.941	0.942

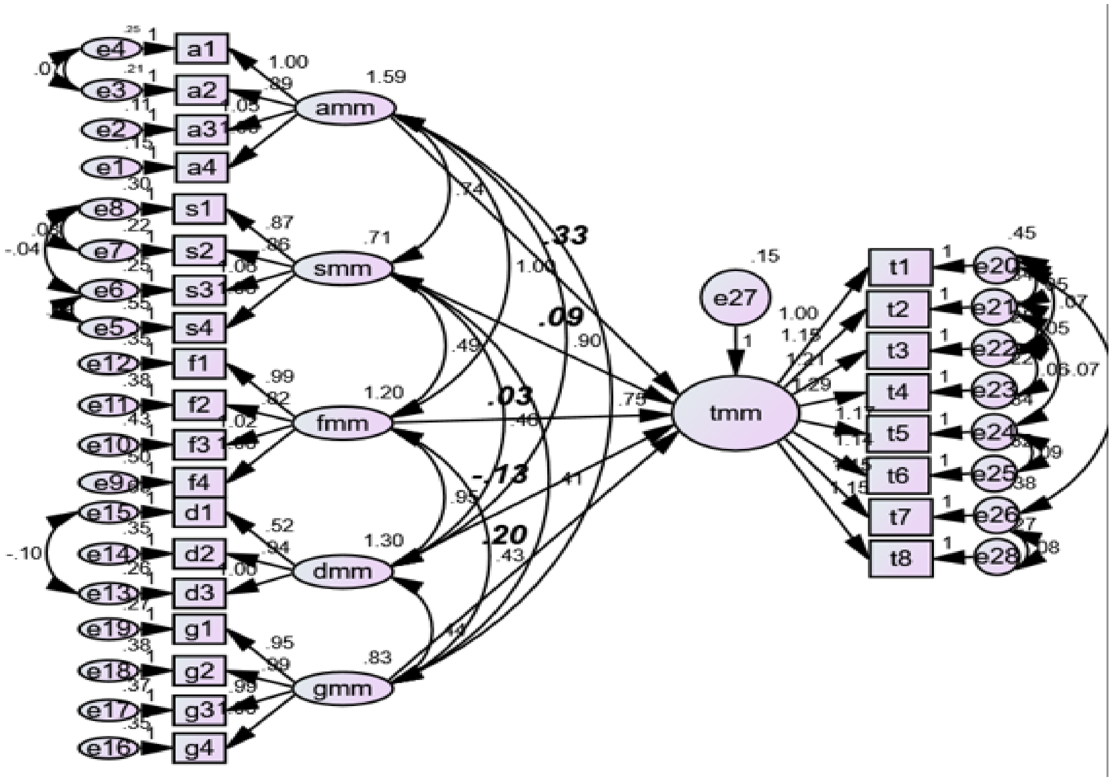
Source: Prepared by the researchers based on AMOS 23 outputs

From Table (3), Cronbach's alpha coefficient values ranged between 0.819 and 0.972, the composite reliability coefficient ranged between 0.846 and 0.942, and all of which were greater than 0.7, indicating the reliability of the scale (Almen et al., 2018) (Tavakol, Dennick, 2011). There was no need to modify or change any of the instrument's phrases.

4 Hypothesis Testing

Figure 3

Hypothesis testing using structural equations SEM



Source: Prepared by the researchers based on AMOS 23 outputs

After ensuring the validity of the data for analysis by verifying the validity and reliability conditions of the used measurement tool, the structural equations SEM were relied upon to test hypothesis, where the value of CMIN/DF = 1.976, which is less than 3, the values of CFI = 0.971, TLI = 0.966, GFI = 0.900, and all of which are greater than 0.9, RMSEA = 0.05, which is less than 0.08, which means that the model's fit conditions were met.

Table 4

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P
tmm	<---	amm	.327	.041	8.009	***
tmm	<---	smm	.094	.043	2.181	.029
tmm	<---	fmm	.032	.043	.730	.465
tmm	<---	dmm	-.130	.037	-3.523	***
tmm	<---	gmm	.195	.038	5.104	***

Source: Prepared by the researchers based on AMOS 23 outputs

From the table(4), the P value was all less than 0.05, which means that there is a significant effect on the confidence of information systems users, except for (the third dimension), which was greater than 0.05, which means that there is no significant effect. The greatest effect was for the first dimension, as the proverbs were equal to 0.327, while the least significant effect was for the second dimension. Only the fourth dimension had a negative effect, as the proverbs had a negative sign.

The value of the coefficient of determination R2 was 0.663, which means that the dimensions of information security explain 66.3% of the changes in users' confidence in information systems according to the hypothesized multiple regression model.

5 Results And Discussion

This study aims to investigate the relationship between information security and its impact on the trust of information systems users. The tourism sector in Syria was selected as a practical application environment, through analyzing data collected from a random sample of managers working in the sector. Structural equation modeling was employed to study multiple regression between the dimensions of the independent variable (information security) and trust in information systems.

The results revealed a significant impact of information security dimensions on the trust of information system users in the tourism sector. A strong influence of security organization on trust was found, especially with the sector's significant shift towards electronic payment, online booking, and the use of social media and communication technologies in travel planning. Organizing information has become a fundamental necessity to gain users' trust and enhance their loyalty. This finding aligns with previous studies such as (Benitez, 2025) (Benitez, 2024), which emphasized the importance of strengthening and organizing information security, particularly against cyberattacks to protect customer data and build trust.

Accordingly, the study concludes that effective organization of information security will positively reflect on customer trust, whether by developing the legislative framework, complying with international data protection regulations, obtaining global quality certifications such as ISO/IEC 27001, or implementing internal and external periodic audits to ensure data protection measures. Furthermore, the study recommends strengthening cooperation between tourism sector organizations, both governmental and private, to develop data protection protocols that can be applied regionally and internationally.

Regarding security policies, the study found a moderate positive impact on users' trust. Information security policies have consistently contributed to enhancing user confidence in digital technologies, particularly information systems, especially with the ongoing digital transformation in the tourism sector. These findings are consistent with several studies such as (Choi et al., 2023) (Moreno & Nair, 2024) (Tiwari et al., 2023), which confirmed that enhancing security policies-especially those related to privacy and security-boosts trust in information systems. Further support comes from (Al-Sharafi et al., 2018) (Choudhuri et al., 2024), emphasizing that increasing security threats and policy weaknesses lead to a decline in users' trust.

Security policies are thus considered a fundamental pillar in building customer trust, through practices such as access and permission policies, two-factor authentication, encryption, continuous employee training, data backup, and emphasizing privacy protection compliance with national and international regulations. Transparency with customers regarding security policies is also crucial.

On the other hand, the study found a negative impact of individual security on users' trust in information systems, contrary to many previous studies such as (Olasumbo et al., 2021), which indicated a positive relationship. The current study suggests that heightened awareness of information privacy could increase users' anxiety and concerns, negatively affecting their trust. Moreover, excessive security measures could lead to discomfort and decreased confidence in technology overall.

As for information maintenance, the study recorded a weak impact on user trust, despite findings from other research (e.g., Wang, 2024) emphasizing the role of information maintenance in improving cybersecurity, employing big data analytics, and enhancing information quality. The current study attributes this weak effect to the limited number and homogeneity of platforms in the Syrian environment, in addition to political and security challenges. In a stable environment, regular data updates and error correction would substantially boost user trust.

Regarding asset control, the study found no significant impact on user trust in information systems, contrary to many prior studies (e.g., Wei et al., 2024) (Elshaer et al., 2024), which highlighted asset control as crucial for transparency, reliability, data confidentiality, and compliance with international standards. The absence of a significant relationship in this study may be due to limited diversity in the systems used by the sample, or due to other indirect factors like perceived usefulness or user satisfaction. Furthermore, the level of competitive information security practices in Syria may not be sufficiently mature to demonstrate such effects.

6 Conclusion

This study examined the impact of information security dimensions on the trust of information systems users within the Syrian tourism sector, based on field data and structural equation modeling analysis. The results showed varying degrees of influence for the security dimensions, with security organization and security policies having the strongest impacts. A negative impact was observed for individual security, and a weak impact for information maintenance, while no significant impact was found for asset control.

The findings emphasize the need to focus on developing and organizing information security practices in the tourism sector, enhancing security policies, and promoting transparency in handling user data. Moreover, it is essential to manage the balance between raising user awareness about security measures and maintaining high levels of trust.

6 Future Implications

Future research is recommended to integrate intermediary variables such as customer satisfaction or the nature of the organization when studying the relationship between information security and user trust. It is also advised to expand the research scope to explore external environmental factors, particularly the political and economic conditions of the tourism sector. Lastly, investigating the potential of leveraging information security as a competitive advantage to strengthen Syria's tourism position in regional and international markets is highly encouraged.

References

-Atkinson, G., & Nevill, A. (1998). Statistical Methods for Assessing Measurement Error(Reliability) in Variables Relevant to Sports Medicine. *Sports Med, 26(4),* 217-238.

-Anday, A., Francese, E., Huurdeman, H., Yilmaz, M., & Zengenene, D. (2012). Information Security Issues in a Digital Library Environment: A Literature Review. *Bilgi Dunyasi, 13 (1),* 117-137.

-Andress, J. (2014). The Basics of Information Security. Syngress.

-Aghdaie, S., & Katebi, M. (2016). Analyzing the Role of Information Technology (IT) and Security in Tourism Industry. *International Review of Management and Business Research, 5(3),* 1241-1255.

-Al-Sharafi, A., Arshah, R., Herzallah, A., & Abu-Shanab, E. (2018). The impact of customer trust and perception of security and privacy on the acceptance of online banking services: Structural equation modeling approach*. International Journal of Industrial Management (IJIM), 4,* 1-15.

-Arenas, A., Ray, G., Hidalgo, A., & Uruena, A. (2023). How to keep your information secure? Toward a better understanding of users security behavior. *Technological Forecasting & Social Change, 198,* 1-13.

-Azzoug, Y., & Chelouache, K. (2023). Information security strategies in university libraries in light of the digital environment. Conference paper, 1-22.

-Bejjar, A., & Boujelbene, Y. (2013). The Impact of Information Systems on user Performance: An Exploratory Study. *Journal of Knowledge Management, Economics and Information Technology, 2*, 1-28.

-Berisha, A. (2014). Management Information System and Decision-Making. Academic *Journal of Interdisciplinary Studies, 3(2),* 19-23.

-Basholli, F., Mezini, R., & Basholli, A. (2023). Security in the components of information systems. *Advanced Engineering Days, 7,* 185-187.

-Campbell, T. (2016). Practical Information Security Management. Berlin, Springer.

-Choi, K., Wang, Y., Sparks, B., & Choi, S. (2023). Privacy or security: does it matter for continued use intention of travel applications? *Cornell Hospitality Quarterly, 64(2),* 267-282.

-Choudhuri, D., Singh, A., Ravi, R., & Badhusha, M. (2024). An analysis of factors influencing consumer trust in online banking security measures. *Educational Administration: Theory And Practice, 30(2)*, 660-666.

-Easttom, C. (2019). Computer Security Fundamentals. USA: Pearson.

-Edo, O., Ang, D., Billakota, P., & Ho, J. (2023). A zero-trust architecture for health information systems. Health and Technology, International Union for Physical and Engineering Sciences in Medicine.

-Elshaer, I., Alyahya, M., Azazz, A., Ali, M., Fathy, E., Fouad, A., & Fayyad, S. (2024). Building digital trust and rapport in the tourism industry: a bibliometric analysis and detailed overview. *Information, 15(10),* 598.

-Florido-Benitez, L. (2024). The cybersecurity applied by online travel agencies and hotels to protect users' private data in smart cities. *Smart Cities, 7(1),* 475-495.

-Florido-Benitez, L. (2025). The role of cybersecurity as a preventive measure in digital tourism and travel: a systematic literature review. *Discover Computing, 28(1),* 28.

-Golden, M. (2017). The Handbook of Information Security for Advanced- Neuroprosthetics. Second Edition Publisher: Synthypnion Academic.

-Hina, S., & Dominic, D. (2016). Information security policies: Investigation of compliance in universities. Paper presented at the 2016 3rd International Conference on Computer and Information Sciences.

-Hakkala, A., Heimo, O., Hyrynsalmi, S., & Kimppa, K. (2018). Security, Privacy'); DROP TABLE Users; and Forced Trust in the Information Age? *ACM SIGCAS Computers and Society, 47(4),* 68-80.

-John, M., & Thomas, H. (2019). Protecting Information with Cybersecurity. Berlin: Springer International Publishing AG.

-Krejcie, R., & Morgan, D. (1970). Determining sample size for research activities. *Educational and Psychological Measurement, 30*, 607-610.

-Kaaria, A. (2023). Human Resource Information Systems Information Security and Organizational Performance of Commercial State Corporations in Kenya. *East African Journal of Information Technology, 6(1),* 256-278.

-Lis, T., Bajdor, P., Grondys, K., & Ptak, A. (2020). The Role of Information Relations in Network Organizations. *European Research Studies Journal, XXIII, 1*, 516-529.

-Maqableh, M., Hmoud, H., Jaradat, M., & Masa'deh, R. (2021). Integrating an Information Systems Success Model with Perceived Privacy, Perceived Security, and Trust: The Moderating Role of Facebook Addiction. Journal Pre-proof, HELIYON.

-Moreno, C., & Nair, P. (2024). Consumer Trust in Digital Environments: Examining the Impact of Privacy and Security Measures on Brand Perception. *Business, Marketing, and Finance Open,* 1(6).

-Nan, X., & Kanato, K. (2021). Role of information security-based tourism management system in the intelligent recommendation of tourism resources. *Mathematical Biosciences and Engineering, 18(6),* 7955-7964.

-Olasumbo, O., Ozturen, A., & Ilkan, M. (2021). Effects of privacy concern, risk, and information control in a smart tourism destination. *Economic research-Ekonomska istrazivanja, 34(1),* 3119-3138.

-Pfleeger, C., Pfleeger, S. (2015). Security in Computing. 5th ed, Pearson.

-Panjaitan, F., Purnamasari, S., & Melisa, W. (2022). Tourism Application Information System Security Audit Using Cobit 5 Framework on Palembang City. *Journal of Information Systems and Informatics, 4(1),* 156-166.

-Quyet, N., Tien, N., & Phung, T. (2023). Comparative analysis of information security policies at Big 4 Vietnamese logistics companies. *International Journal of Multidisciplinary Research and Growth Evaluation, 4(6),* 683-690.

-Romney, M., & Steinbart, P. (2018). Accounting Information Systems. 14th edition, Pearson.

-Rostami, E., Karlsson, F., & Gao, S. (2023). Policy components– a conceptual model for modularizing and tailoring of information security policies. *Information and Computer Security, 31(12),* 331–352.

-Rabbani, M., Wijaya, J., Kusuma, R., Purba, W., & Tajib, R. (2023). Digital Payments in Indonesia: Understanding the Effect of Application Security on User Trust. *Indonesian Journal of Computer Science, 12(5),* 2475-2486.

-Shahrani, M. (2019). Information Security and its Impact on Intellectual and Security Protection in Saudi Press Institutions. The 10th International Scientific Conference, Global Proceedings Repository, American Research Foundation, 2460-2492.

-Shadood, W. (2023). Enhancement the Security by creating ontology-based Trust Management using Semantic Web tools. *Alkadhum Journal of Science, 1(2),* 11-16.

Tiwari, V., Mishra, A., & Tiwari, S. (2024). Role of data safety and perceived privacy for acceptance of IoT-enabled technologies at smart tourism destinations. *Current Issues in Tourism, 27(19),* 3079-3094.

-Victoria, M. (2010). Information Security Awareness: System Administrators and End-User Perspectives at Florida State University. degree doctor of philosophy, Florida State University, USA.

-Whitman, M., & Mattord, H. (2005). Principles of Information Security. Course Technology, Cengage Learning, 4th edition.

-Wang, J., Wang, Z., Song, J., & Cheng, H. (2023). Attribute and User Trust Score-Based Zero Trust Access Control Model in IoV. *Electronics, 12*, 1-20.

-Wang, L. (2024). Enhancing tourism management through big data: Design and implementation of an integrated information system. *Heliyon, 10(20).*

-Wei, Y., Fan, D., Zhang, B., Li, T., & Feng, Y. (2024). How to improve tourists' trust in official tourism destination websites in China-an empirical research based on CV and PASP. *Humanities and Social Sciences Communications, 11(1),* 1-15.

-Zywiolek, J. (2024). Empirical examination of ai-powered decision support systems: ensuring trust and transparency in information and knowledge security. *Scientific papers of silesian university of technology organization and management, 197,* 680-695.