IAIC International Conference Series
Vol. 4, No. 1, 2023, pp. 153 ~ 164
E-ISSN: 2774-5899 | P-ISSN: 2774-5880
DOI: https://doi.org/10.34306/conferenceseries.v4i1.647

Analysis of Information Security Culture at FMIPA Halu Oleo University Using Partial Least Squares-Structural Equation Modeling Method

[1]Elsa Julfiana, [2*]Natalis Ransi, [3]Gusti Arviana Rahman
[1,2,3]Department of Computer Science, Haluoleo University, Indonesia
E-mail: [2*]natalis.ransi@uho.ac.id, [3]arviana.rahman@uho.ac.id
***Corresponding author**

(Received November 8, 2023 Revised November 17, 2023 Accepted November 25, 2023, Available online December 19, 2023)

Abstract

This research aims to analyze the information security culture at FMIPA Halu Oleo University. The results of the analysis show that exogenous latent variables, such as information security awareness, the role of faculty leaders, and information security policies, have a significant positive impact on information security culture. The research results show that the security awareness variable has a positive effect (0.221) on the Information Security Culture variable. Apart from that, the top management variable also has a positive effect (0.185) on the Information Security Culture variable. Likewise, the security policy variable has a significant positive influence (0.233) on the Information Security Culture variable. These findings provide an in-depth understanding of the factors that influence the culture of information security in the FMIPA Halu Oleo University environment, which can be the basis for recommending improvements in increasing information system security at the faculty.

***Keywords**: FMIPA, Information Security Culture, Security Awareness, Top Management, Security Policy*

1. Introduction

Security Culture is a set of practices and traditions adopted by an organization or community to reduce information security risks. This is important to improve data protection in an organization or community [1]. Establishing a security culture is usually based on strict industry certifications, policies, laws and regulations such as GDPR, ISO 27000 and SOC. However, effective security practices must be tailored to the organization's culture [2]. For this reason, organizations must understand employee perceptions, attitudes and behavior in managing information to form a conducive security culture [3].

Companies, organizations, schools and governments need information technology for data management and security [4]. Therefore, implementing a good information system is very important to improve performance and provide better services. Information technology governance is included in the governance of companies, organizations, schools and governments which aims to manage information systems and technology well, as well as reduce risks related to information [5].

Based on Law Number 19 of 2016 concerning Electronic Information and Transactions, Article 1 paragraph 1 explains that Electronic Information is one or a collection of electronic data, including but not limited to writing, sound, images, maps, plans, photos, electronic data interchange (EDI), letters. electronic (electronic mail), telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols or perforations that have been processed which have meaning or can be understood by people who are able to understand them. An information security culture must be implemented in information technology governance in order to overcome information security risks [6].

Faculty of Mathematics and Sciences (FMIPA), Halu Oleo University (UHO) was officially established on September 21 1998 based on the Decree of the Minister of Education and Culture Number 233/O/1998 [7]. The UHO Faculty of Mathematics and Natural Sciences has various information systems such as SIAKAD, E-Learning, and department and study program websites that require good management and risk management to prevent the risk of data leaks [8]. Information security culture analysis is needed to understand the implementation of information security policies, training and awareness at FMIPA UHO. It is hoped that this analysis can provide an in-depth understanding of the information security culture in the faculty and recommendations for improvements to increase information system security [9].

Partial Least Squares Structural Equation Modeling (PLS-SEM) is often used to analyze information system security [10]. This method has the advantage of overcoming the unique characteristics of information system security culture data, such as the ability to handle complex data, the ability to handle small samples, and the ability to examine cause-and-effect relationships between latent variables and qualitative indicators in the analysis model.

This research tries to find related factors that influence information security culture at FMIPA Halu Oleo University using the PLS-SEM method so that later it can become a reference in improving security culture.

Information security culture in Bandung City Pratama clinics using the sampling method and PLS-SEM data analysis techniques [11]. [12] examined the factors that influence the culture of information security in Bandung City health centers using the PLS-SEM method and WarpPLS 6.0 software. [13], this research uses the Webqual 4.0 method to measure the quality of Google Classroom and PLS-SEM to model the relationship between the quality of Google Classroom and the level of student satisfaction. [14] evaluated information security policies and their use in organizations using quantitative descriptive research methods [15]. [16] conducted research using a survey method on 101 SIMSDM users in the public sector.

Data

Data are facts that describe actual events at a certain time. Data is obtained from events that actually occur, for example from sales transactions, purchases, and so on. Data is identical to evidence of transactions that occur in a company such as receipts, invoices, forms and so on. The data that has been processed can then produce information in the form of reports, such as financial reports, sales reports, and so on [17]. Some examples of data include:

1. Formatted data is data that has a format, for example data that displays time or displays a collection of numeric values.
2. Text is a series of numbers, letters or certain symbols, for example a tabloid or magazine.
3. Image is data in the form of an image, for example photos, graphs and so on.
4. Audio is data in the form of sounds or sounds, for example music, people talking, etc.
5. Video is a series of images that are processed so that when combined they can display fast moving images and are usually equipped with audio, video is often used to record an activity.

1.1. Information

Information or in English is information, comes from the French word informacion. The word is taken from Latin, namely "informationem" which means "concept, idea, outline". Information is data that has been processed or processed so that it becomes a form that has meaning for the recipient of the information and has useful value. Information is something that results from data processing. Existing data is packaged and processed in such a way that it becomes useful information [18].

Information Security

Information security is used to describe the protection of information assets, including computer and noncomputer equipment, facilities, and data to ensure the confidentiality, integrity, and availability of information through application, education and technology policies. The goal of information security is to ensure business continuity, minimize business losses, and maximize return on investment. Therefore, organizational management is not only expected to maintain secure information resources, but is also expected to maintain the organization so that it can continue to function after a disaster security system [2].

1.2. Security Culture

Security Culture can be interpreted as an attitude and behavior in managing and protecting assets related to information and communication technology (ICT) safely and effectively. A document from ENISA, (2017) entitled "Cyber Security Culture in Organizations" explains that Security Culture is a concept that includes safety culture, risk management and security in an organization [19].

By adopting a strong Security Culture, organizations can strengthen their defenses against cyberattacks and reduce security risks that could threaten their operations.

1.3. Information Security Standards

The ISO/IEC 27001 standard for information security management systems, the main objective is to maintain the confidentiality, integrity and availability of information by implementing an effective risk management process and convincing interested parties that risks have been managed properly. The information security management system is integrated into the organization's processes and management structure as a whole.

1.4. Partial Least Square

Partial Least Square (PLS) is a method that can be used as an alternative in modeling structural equations, with the aim of testing the relationship between latent constructs (unobserved variables) and many indicators (observed variables). PLS is often referred to as "soft modeling" because it does not follow classic assumptions such as data must have a multivariate normal distribution, measurements must be carried out on a certain scale, or the sample size must be large. Thus, PLS provides flexibility in its use without having to fulfill strict assumptions [20].

1.5. Structural Equation Modeling

Structural Equation Modeling (SEM) is a multivariate analysis method used to describe the linear relationship between observed variables (indicators) and latent variables that cannot be measured directly. Latent variables can be variables that cannot be observed (unobserved) or cannot be measured (unmeasured) directly, but must be measured through several indicators. In SEM, there are two types of latent variables, namely endogenous variables and exogenous variables.

1.6. Partial Least Square - Structural Equation Modeling

Partial Least Square Structural Equation Modeling (PLS-SEM) is used because the data does not have to meet classical assumptions and is suitable for variables that have complex relationships. PLS-SEM is used if:

1. Small sample size
2. Have a little theory
3. Predictive accuracy in the model is paramount
4. Correct model specifications cannot be confirmed.

PLS-SEM is appropriate if the model formed is predictive, has a weak theoretical basis and ignores classical assumptions.

1.7. Slovin Sample Size Formula

The sample formula presented by Slovin is known as "the Slovin's (1960) formula" or also known as the "Slovin Formula". The sample size formula based on the Slovin formula is known to be very easy to understand and easy to do. The formula is as follows.

$$n=N1+Ne2 \qquad (1)$$

Information:
n = large sample
N = large population
e = the desired error limit (the desired margin of error) or the error that is tolerated (error of tolerance).

The amount of margin of error really depends on the researcher, or is known as the discretion of the researcher, but usually the generally accepted margin of error (acceptable margin) is 5% or 0.05.

2. Research Methods

This research as a whole was carried out using the Plan, Do, Check, Act research procedure or abbreviated as PDCA which can be seen in Figure 1.

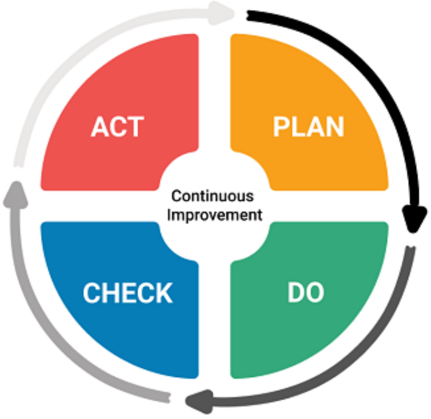

Figure 1. MethodPlan, Do, Check, Act (PDCA)

The following is a brief explanation of each stage of the PDCA model in the context of research:

1. Plan (planning), at this stage research planning is carried out by identifying research objectives and formulating research questions.
2. Do (carry out), at this stage the research is carried out in accordance with the plan that has been made.
3. Check, at this stage, the data that has been collected is checked to ensure accuracy, completeness and validity.
4. Act (act), at this stage action is taken based on the results of the analysis and findings that have been found.

2.1. Method of collecting data

Sample and Population

In this research, the population that is the focus is all active students of the Faculty of Mathematics and Natural Sciences (FMIPA) at Halu Oleo University (UHO). To determine the research sample, researchers will use the Slovin Sample Size Equation which allows selecting a representative sample from all FMIPA UHO students.

Data Collection Techniques

Data collection in this research will be carried out quantitatively by distributing questionnaires to the research sample. The questionnaire used in this research was adapted from the journal [8] which uses the Partial Least Squares-Structural Equation Modeling (PLS-SEM) method to study the relationship between student satisfaction levels and the quality of Google Classroom based on the Webqual 4.0 method. The questionnaire has been modified and adapted to suit the aims of this research.

2.2. Data Analysis Method

The data analysis method used in this research is Partial Least Squares Structural Equation Modeling (PLS-SEM), a multivariate data analysis technique used to model the relationship between various variables.

Outer Model

The Outer Model is the first stage in PLS-SEM analysis and involves specifying the relationship between latent variables and their indicators. The outer model is often referred to as a measurement model because it explains the characteristics of latent variables with indicators or manifest variables. This stage includes testing the validity and reliability of the indicators that form the latent construct. This test includes convergent validity, discriminant validity, average variance extracted (AVE), and composite reliability tests.

Inner Model

After the outer model has been prepared, the next step is to build the inner model, which is a specification of the relationship between latent variables (structural model). This inner model explains the relationship between latent variables based on the substantive theory of the research. In the context of this research, the inner model will help in understanding how the factors that influence information security culture are interconnected.

Model Illustration

The PLS-SEM model used in this research will be presented in the form of images or visualizations. The modeling image will illustrate the relationship between the variables being studied. The PLS-SEM model can be seen in Figure 2.

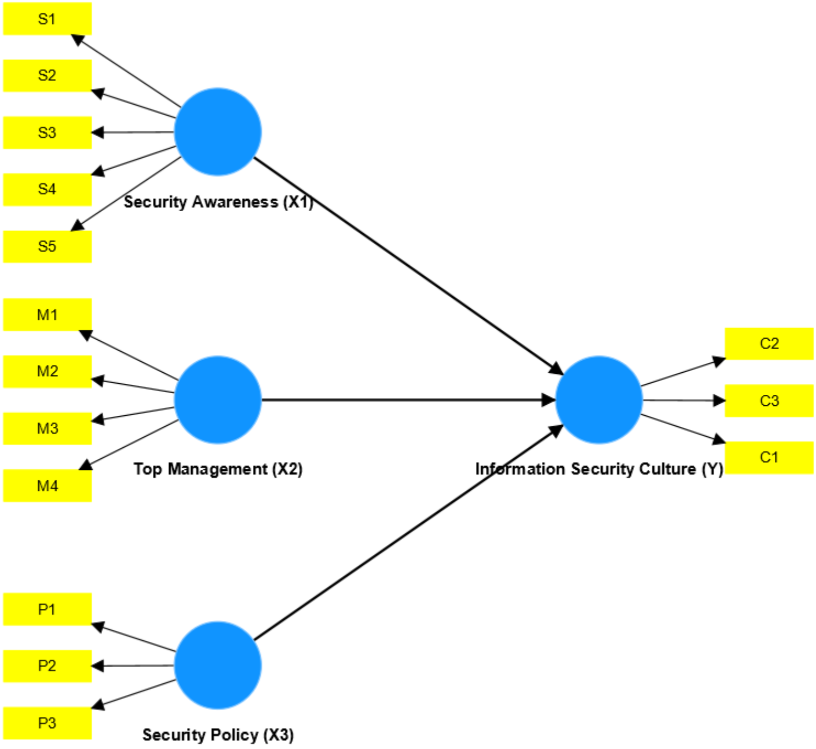

Figure 2. PLS-SEM model (Source: Author's preparation)

Model Test

At this stage, the model that has been built will be tested to measure the extent to which the model fits the data obtained. Model testing involves testing both the outer model (measurement model) and the inner model (structural model).

Outer Model: Validity and reliability tests of indicators will be carried out. Validity will be measured by testing convergent validity, discriminant validity, average variance extracted (AVE), and composite reliability. With this test, we can ensure that the indicators used in measuring latent variables are valid and reliable.

Inner Model: At this stage, the structural model will be tested to check the extent to which the relationships between latent variables are in accordance with existing theory. This test will ensure whether the model that has been built is in accordance with the data obtained and whether the research hypotheses can be accepted or not.

Using the PLS-SEM method, this research will analyze the factors that influence the information security culture at FMIPA UHO and provide an in-depth understanding of the relationship between the variables being studied.

3. Results and Discussion

The data taken in this research was obtained based on a questionnaire that was distributed to all FMIPA UHO students in the form of an online Google Form questionnaire. The sampling method used was random sampling with Slovin.

3.1. Description of the Research Object

The number of study programs in the FMIPA faculty is 11 study programs. The population in this study were 3507 undergraduate students from the Faculty of Mathematics and Natural Sciences and the sample size was determined using the Slovin formula with a confidence level of 5%.

$n = N1 + Ne2$
$n = 35071 + 35070.052$
$n = 35079.7675$
$n = 359,0478628103404$
$n = 359$

with

n = sample size
N = population size
e = margin of error (percentage of allowance for sampling error accuracy that can still be tolerated)

The sample size from a population of 3507 with a margin of error of 5% is 359.

3.2. Respondent Characteristics

By Gender

The data obtained has a gender distribution from sample data of 359 people, it is known that there are 57% women or around 203 people and 43% men or around 156 people.

Based on Study Program

The data obtained has a distribution for each sample, the Mathematics study program obtained sample data of 10% or 33 people, Physics as much as 9% or 33 people, Chemistry as much as 9% or 33 people, Biology as much as 9% or 33 people, Statistics as much as 9% or 33 people. people, Computer Science as many as 9% or 33 people, Biotechnology as many as 9% or 33 people, Mining Engineering as many as 9% or 32 people, Geological Engineering as many as 9% or 32 people, Geophysical Engineering as many as 9% or 32 people, and Geography as many as 9 % or 32 people.

Based on Class

The data obtained has a distribution of sample data based on college class, namely 0.002% or 1 person from the Class of 2018, 14% or 47 people from the Class of 2019, 17% or 59 people from the Class of 2020, 19% or 67 people from the Class of 2021, and 50 % or 173 people from the Class of 2022.

3.3. Analysis PLS-SEM

In this research, there are four latent variables, namely Security Culture, Security Awareness, Top Management, and Security Policy. Each latent variable is measured by several indicators. For PLS-SEM analysis the author uses smartPLS software.

Evaluate the Measurement Model or Outer Model

At this stage, a measurement model analysis (outer model) is carried out, there are three points which are test indicators, namely Convergent Validity (Loading Factor, Cross Loading), Discriminant Validity (Average Variance Extracted/AVE), Reliability (Cronbach's Alpha, Composite Reliability). The following are the results of running the PLS-SEM algorithm which explains the measurement model (outer model).

Convergent Validity (Convergent Validity)

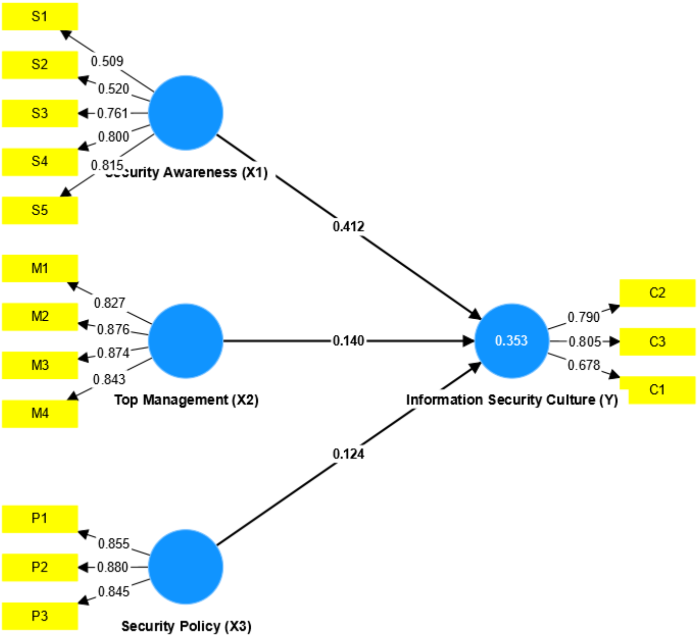

Figure 3. Convergent Validity

The results of the convergent validity test can be seen in Figure 3. Based on the picture, it can be seen that several indicators X1, and Y < 0.70, this indicates that these indicators are unable to explain the latent variable so it can be said that these indicators are invalid. Based on the results of the Convergent Validity Test above, convergent validity was obtained via outer loading which can be seen in the following table.

Table 1.Outer Loading

	Information Security Culture (Y)	***Security Awareness (X1)***	***Security Policy (X3)***	***Top Management (X2)***
C2	0.79	-	-	-
C3	0.805	-	-	-
M1	-	-	-	0.827
M2	-	-	-	0.876
M3	-	-	-	0.874
M4	-	-	-	0.843
P1	-	-	0.855	-
P2	-	-	0.88	-
P3	-	-	0.845	-
S1	-	0.509	-	-
S2	-	0.52	-	-
S3	-	0.761	-	-
S4	-	0.8	-	-
S5	-	0.815	-	-

Based on the results from Table 1, it can be seen that several indicators do not meet the value > 0.70, so what can be done is to delete these indicators and repeat the PLS-SEM analysis calculation process. After deleting and repeating the PLS-SEM process, a new outer loading model was obtained which can be seen in Figure 4.

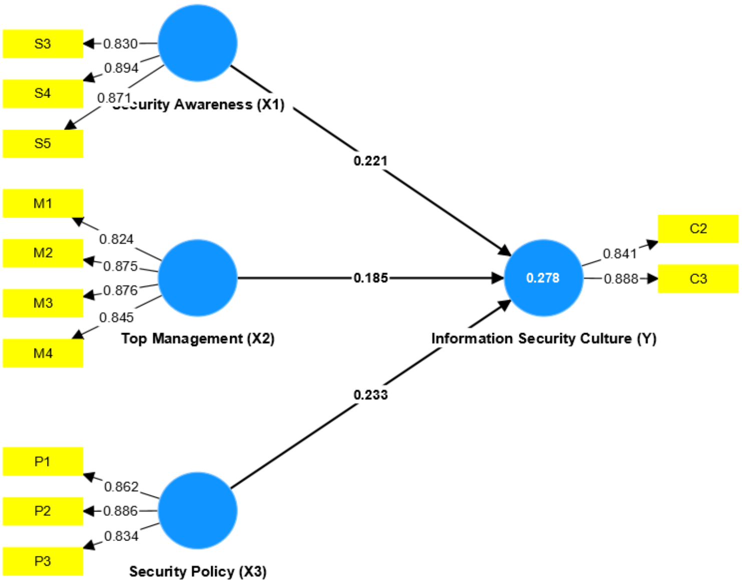

Figure 4. Outer Loading (valid)

The convergent validity table can be seen in Table. The table shows that all indicator values have met the value > 0.70.

Table 2. Outer Loading (valid)

	Information Security Culture (Y)	*Security Awareness* (X1)	*Security Policy* (X3)	*Top Management* (X2)
C2	0.841	-	-	-
C3	0.888	-	-	-
M1	-	-	-	0.824
M2	-	-	-	0.875
M3	-	-	-	0.876
M4	-	-	-	0.845
P1	-	-	0.862	-
P2	-	-	0.886	-
P3	-	-	0.834	-
S3	-	0.83	-	-
S4	-	0.894	-	-
S5	-	0.871	-	-

Discriminant Validity (Discriminant Validity)

In this research, the convergent validity value is also seen from the Average Variance Extracted (AVE). Based on the results obtained, it can be seen that the AVE values for all indicators of each latent variable are different from the indicators for other variables. The assessment criteria is an AVE value ≥ 0.5, this is proven by an AVE value of more than 0.5 in each latent variable which can be seen in Table 3

Tabel 3. Average Variance Extracted

	Average variance extracted (AVE)
Information Security Culture (Y)	0.749
Security Awareness (X1)	0.749
Security Policy (X3)	0.741
Top Management (X2)	0.732

Reliability

The variable reliability test is measured by Cronbach's Alpha and composite reliability, with Cronbach's Alpha and composite reliability values greater than or equal to 0.7. The following composite reliability test results can be seen in Table 4 for Cronbach's Alpha and Table 5 for Composite Reliability values.

Tabel 4. Cronbach's Alpha

	Cronbach's alpha
Information Security Culture (Y)	0.666
Security Awareness (X1)	0.837
Security Policy (X3)	0.826
Top Management (X2)	0.878

Based on data from Cronbach's Alpha, one value was obtained below 0.7 for variable Y, and the values for variables X1,

Tabel 5. Composite Reliability

	Composite reliability (rho_a)	***Composite reliability (rho_c)***
Information Security Culture (Y)	0.678	0.856
Security Awareness (X1)	0.885	0.899
Security Policy (X3)	0.833	0.896
TopCronbach's Alpha Management (X2)	0.881	0.916

Based on data from Composite Reliability, one value was obtained below 0.7 for variable Y in the Composite Reliability assessment (rho a), and the values for variables X1, With this, each variable has a level of reliability above the criteria, so it is declared reliable.

Evaluation of the Structural Model or Inner Model

Hypothesis Testing and Regression Coefficients

The results of hypothesis testing on endogenous variables can be seen in Table 6 which describes the correlation of each variable. It can be seen from the three hypotheses that two of them show a positive influence. This can be seen from the original sample value which is > 0 (positive). Meanwhile, the influence that occurs is also significant, seen from the P value, which is smaller than 0.05, which indicates that the influence is significant.

Table 6. Hypothesis Testing from ResultsBootstrap

	***Original sample* (O)**	***P values***
Security Awareness (X1) -> *Information Security Culture* (Y)	0.221	0
Security Policy (X3) -> *Information Security Culture* (Y)	0.233	0.01
Top Management (X2) -> *Information Security Culture* (Y)	0.185	0.046

Based on the table, hypothesis testing is carried out as follows:

1. The first hypothesis tests the influence of the security awareness variable (X1) on Information Security Culture (Y1). There are significant results in hypothesis testing which reveal the influence of security awareness on the information security culture variable in this research
   H1: The security awareness variable has a significant effect on Information Security Culture
   Basis for Decision Making:
   P value ≥ 0.05, then H1 is rejected.
   P value < 0.05, then H1 is accepted.
   Results:
   P value = 0.00 < 0.05, then H1 is accepted.
   Conclusion: The security awareness variable has a significant effect on Information Security Culture.
2. The second hypothesis tests the influence of top management variables (X2) on Information Security Culture (Y1). There are significant results in hypothesis testing which reveal the influence of top management on the information security culture variable in this research..
   H2: Top management variables have a significant effect on Information Security Culture
   Basis for Decision Making:
   P value ≥ 0.05, then H2 is rejected.
   P value <0.05, then H2 is accepted.
   Results:
   P value = 0.04 < 0.05, then H2 is accepted.
   Conclusion: Top management variables have a significant effect on Information Security Culture.
3. The third hypothesis tests the influence of the security policy variable (X3) on Information Security Culture (Y1). There are significant results in hypothesis testing which reveal the influence of security policy on the information security culture variable in this research.
   H3: The security policy variable has a significant effect on Information Security Culture.
   Basis for Decision Making:
   P value ≥ 0.05, then H3 is rejected.
   P value <0.05, then H3 is accepted.
   Results:
   P value = 0.01 < 0.05, then H3 is accepted.
   Conclusion: The security policy variable has a significant effect on Information Security Culture.

Tabel 7. Model Fit Indeks

	Saturated model	*Estimated model*	
SRMR	0.076	0.076	*SRMR*
d_ULS	0.452	0.452	*d_ULS*
d_G	0.234	0.234	*d_G*
NFI	0.79	0.79	*NFI*

Based on Table 4.8, the output results can explain that:

1. SRMR (Standardized Root Mean Square Residual): SRMR values range from 0 to 1. Lower values indicate a better fit to the data. Values above 0.08 can be considered questionable, while values below 0.08 are often considered good.
2. d_ULS (Dunn's ULS) and d_G (Dunn's G): These two metrics measure the fit of the model to the data. Lower values indicate better fit. However, there is no common threshold value for these two metrics. The assessment should be done by comparing the estimated model with the reference model.
3. NFI (Normed Fit Index): NFI values range from 0 to 1. Higher values indicate a better fit to the data. Values above 0.90 are often considered good.

3.4. Discussion

Analysis of information security culture in the FMIPA Halu Oleo University environment will include the influence of exogenous latent variables (security awareness, top management and security policy) on endogenous latent variables (information security culture). The results of the analysis indicate that awareness of information security, the role of faculty leaders, and information security policies have a significant impact on the information security culture within the FMIPA Halu Oleo University environment.

The influence of security awareness on the information security culture variable

Exogenous latent variables can be said to have a positive effect on endogenous latent variables if the original sample value is more than 0 (> 0). Based on the research results, it is known that the security awareness variable (X1) has a positive effect on the Information Security Culture variable (Y1). This can be seen from the original sample value of the security awareness variable (X1) on the Information Security Culture variable (Y1), namely 0.221.

The influence of top management on information security culture variables

Exogenous latent variables can be said to have a positive effect on endogenous latent variables if the original sample value is more than 0 (> 0). Based on the research results, it is known that the top management variable (X2) has a positive effect on the Information Security Culture variable (Y1). This can be seen from the original sample value of the top management variable (X2) on the Information Security Culture variable (Y1), namely 0.185.

The influence of security policy on the information security culture variable

Exogenous latent variables can be said to have a positive effect on endogenous latent variables if the original sample value is more than 0 (> 0). Based on the research results, it is known that the security policy variable (X3) has a positive effect on the Information Security Culture variable (Y1), this can be seen from the original sample value of the security policy variable (X3) on the Information Security Culture variable (Y1), namely 0.233.

4. Conclusion

Based on the research results, the factors that influence information security culture are Security Awareness, Top Management, and Security Policy. These factors contribute positively to the formation of an information security culture (Security Culture) within the MIPA Faculty of Halu Oleo University which is in accordance with the ISO 27000 standard.

From the results of the analysis that has been carried out, all existing variables were found to have an influence on security culture at the Faculty of Mathematics and Natural Sciences, Halu Oleo University, namely Security Awareness, Top Management, and Security Policy. Therefore, the suggestions from this research are as follows:

1. Based on the research findings, it is recommended that the faculty and university management consider increasing information security awareness among members of the FMIPA community.
2. University management also needs to pay attention to the importance of support from leadership in implementing information security policies.
3. Dissemination and implementation of information security policies must be improved to ensure better understanding and compliance with these policies.

References

[1] Allibang, S. Research Methods: Simple, Short, and Straightforward Way of Learning Methods of Research. Sherwyn Allibang. 2020.

[2] Y. Y. R. Rachmawati, Y. P. A. Sanjaya, and S. Edilia, “Web-based temperature, oxygen saturation, and heart rate monitoring system,” *IAIC Trans. Sustain. Digit. Innov.*, vol. 4, no. 1, pp. 38–45, 2022.

[3] Dalleh, J., Akrim, A., & Baharuddin, B. Pengantar Teknologi Informasi (T. E. RGP (ed.)). PT RajaGrafindo Persada. 2020.

[4] R. Faza, R. A. Darmawan, and D. T. Setiamanah, “Evaluation of Rebar Waste Rate Calculation Model Utilizing BIM Function: High Rise Building Case Study,” *Aptisi Trans. Technopreneursh.*, vol. 5, no. 2, pp. 128–135, 2023.

[5] ENISA. Cyber Security Culture in Organisations. 2017.

[6] Fachriandi, B., Dirgahayu, T. Kepedulian Keamanan Informasi di Pemerintahan: Praktik Manajemen dan Dampaknya. Jurnal Manajemen Informatika (JAMIKA). 2021; 11(1): 72–87.

[7] B. P. K. Bintoro, N. Lutfiani, and D. Julianingsih, “Analysis of the Effect of Service Quality on Company Reputation on Purchase Decisions for Professional Recruitment Services,” *APTISI Trans. Manag.*, vol. 7, no. 1, pp. 35–41, 2023.

[8] Marliana, R. R. Partial Least Squares-Structural Equation Modeling Pada Hubungan Antara Tingkat Kepuasan Mahasiswa Dan Kualitas Google Classroom Berdasarkan Metode Webqual 4.0. Jurnal Matematika, Statistika, & Komputasi. 2020; 16(2): 174–186.

[9] N. Wiwin, P. A. Sunarya, N. Azizah, and D. A. Saka, "A Model for Determine Upgrades for MSMEs using Analitical Hyrarcy Process," *ADI J. Recent Innov.*, vol. 5, no. 1Sp, pp. 20–32, 2023.

[10] Putri, R. A. Buku Ajar Basis Data (R. R. Rerung (ed.); Edisi Kedu). Media Sains Indonesia. 2022.

[11] A. Williams and C. S. Bangun, "Artificial Intelligence System Framework in Improving The Competence of Indonesian Human Resources," *Int. J. Cyber IT Serv. Manag.*, vol. 2, no. 1, pp. 82–87, 2022.

[12] Syauqina, S., Sari, P. K., Prasetio, A., Candiwan. Analisis Budaya Keamanan Informasi di Puskesmas Kota Bandung. Jurnal Kesehatan Vokasional. 2019; 4(2): 70–79.

[13] S. Purnama and C. Sriliasta, "Independent Learning and Blended Learning Information System Student," *Int. Trans. Educ. Technol.*, vol. 1, no. 2, pp. 144–150, 2023.

[14] Astuti, E. F., Sari, P. K. Analisis Budaya Keamanan Informasi di Klinik Pratama Kota Bandung. *Jurnal Mitra Manajemen (JMM Online).* 2019; 3(3): 314–325.

[15] R. Widayanti, M. H. R. Chakim, C. Lukita, U. Rahardja, and N. Lutfiani, "Improving Recommender Systems using Hybrid Techniques of Collaborative Filtering and Content-Based Filtering," *J. Appl. Data Sci.*, vol. 4, no. 3, pp. 289–302, 2023.

[16] Leguina, A. A primer on partial least squares structural equation modeling (PLS-SEM). In International Journal of Research & Method in Education. 2015; 38(2).

[17] Octariza, N. F. Analisis Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO/IEC 27001 Dan ISO/IEC 27002 Pada Kantor Pusat PT Jasa Marga. 2019.

[18] Rusdiana, Irfan, M. Sistem Informasi Manajemen. In Sistem Informasi Manajemen. Pustaka Setia. 2014.

[19] Veiga, A. da, Martins, N. Information Security Culture: A Comparative Analysis of Four Assessments. 2014; 8: 49–57.

[20] Desy Ria, M., Budiman, A. Perancangan Sistem Informasi Tata Kelola Teknologi Informasi Perpustakaan. Jurnal Informatika Dan Rekayasa Perangkat Lunak (JATIKA). 2021; 2(1): 122–133.