**Journal of Emerging Information Systems and Business Intelligence**
**ISSN: 2774-3993**
Journal homepage: https://ejournal.unesa.ac.id/index.php/JEISBI/

# ANALYSIS OF INFORMATION SECURITY CULTURE AMONG STUDENTS

**Achmad Raafi'ud Cholsa[1], Rahadian Bisma[2]**

[1,2] *Information Systems, Faculty of Engineering, Surabaya State University*

achmad.20092@mhs.unesa.ac.id, rahadianbisma@unesa.ac.id

## ABSTRACT

This research aims to analyze the information security culture among university students, which is becoming increasingly important in today's digital era. In the context of increasing threats to personal data and sensitive information, understanding the culture of information security among the younger generation is crucial. The method used in this research is a quantitative survey involving 400 student respondents from various universities in Surabaya, the data is analyzed using descriptive statistical techniques to describe students' understanding, attitudes, and behavior towards information security. The results showed that students have low awareness of information security, even though they actively use digital technology. Many respondents have experienced data breaches but did not take sufficient preventive measures. The research recommends increased education and socialization about information security on campus, as well as the development of structured training programs to improve security awareness and practices among students.

**Keyword:** Information security culture, Student data security, University in Surabaya.

**Article Info:**
*Article history:*
*Received December 26, 2024*
*Revised March 01, 2025*
*Accepted August 26, 2025*

**Corresponding Author**
Achmad Raafi'ud Cholsa
Surabaya State University, Surabaya, Indonesia
achmad.20092@mhs.unesa.ac.id

## 1. INTRODUCTION

Technology and information are getting faster. evolving, changing rapidly over time without ever revealing its true nature. The advancement of information technology is undoubtedly beneficial to its users, as it makes it easier to access the necessary information wherever and whenever we are. It has permeated every aspect of human life, with education being the most prominent area, especially among students. Students have many activities, especially those related to information technology. This includes general activities and activities related to the field of education. The amount of information technology that enters the daily lives of students will not be a problem.

It is beneficial if we only use it for personal use because every technology will be very helpful if we can use it optimally and minimize the negative impact on ourselves and the surrounding community. However, there are always drawbacks to the use of information technology. *We Are Social*, an English media company, released a report titled "Digital 2021: Latest Insights into the Core of the Digital State" on February 11, 2021.

Widespread use of smartphones in Indonesia, which is also the country with the highest internet usage rate in the world. The study presents preliminary findings on social media and internet usage in many countries, including Indonesia. Of Indonesia's overall population of 274.9 million, active social media users number around 170 million. The number of social media users in Indonesia is equivalent to 61.8% of the total Indonesian population as of January 2021. In addition, this number increased by 10 million, or about 6.3 percent, when compared to the previous year (Rizal, 2021). The above-mentioned numbers obscure many houses connected to privacy and user information. The more rapid the development of social media, the more important the attention to information security and privacy. the use of social media as a source of leaking confidential information has become common today. Social media can be a channel for crime or leakage of company information. Therefore, the problem that arises is awareness of information security and privacy in the use of social media. This research focuses on university students with the aim of exploring their views, as part of the millennial generation, towards information security and privacy in the use of social media.

The purpose of this research is to develop a model that assesses and evaluates current perceptions of information security culture and fosters positive information security in public higher education. The importance of understanding information security to maintain privacy data and minimize crimes that are now rampant such as *Cyber Crime* or cybercrime and other information security problems. One of the most negative aspects is security. There are many cases related to this information security. One of the factors that trigger information security and privacy breaches is because digital media users have insufficient awareness in using smartphones safely, some of them have sufficient knowledge in the use of digital media but they do not apply it properly. This can result in data loss or damage to sensitive information. Based on statistics from the *International Telecommunication Union* (ITU 2017) *Global Cyber Security Index* Indonesia is ranked 70th out of 165 countries in this ranking.

Information security among today's college students is becoming increasingly important given the extensive use of digital technologies in academic and social activities. Students often use personal devices, internet access, and various online applications to study, communicate, and manage personal data. This makes them vulnerable to security threats such as phishing, malware, identity theft and privacy breaches. Many universities provide education and training programs on information security for students. These include seminars, workshops, and online courses that address cyber threats and best practices for protecting personal data. Universities usually have security policies that govern the use of campus networks, devices, and data. These policies are designed to protect systems and information from internal and external threats. Universities develop incident reporting systems that allow students to report security concerns or suspicious activity without fear of retribution. This helps in the early detection and handling of security incidents.

The findings of previous research indicate that the level of information security awareness among university students must be monitored to ensure that the data and privacy owned by students are safe. This research uses the Structural Equation Modeling (SEM) method, which is a statistical analysis technique used to build and test statistical models based on causal relationships. SEM integrates regression analysis, factor analysis, and path analysis to simultaneously calculate the relationship between latent variables, evaluate the loading value of indicators on latent variables, and map the path model between these latent variables. In general, SEM is a multivariate method that allows visualization of a series of causal relationships in the form of path diagrams.

The subject of this research is active students in higher education, but only focuses on the data security platform owned by students, where the results show that the level of anxiety of students is relatively high in terms of data security and privacy owned by students in the college

environment. This study develops previous research using the SEM method, which based on the results of the study is expected to increase the awareness of students in maintaining the security and privacy of their data. In general and related organizations in order to identify the steps needed to improve and maintain data security and privacy. improve the maintenance standards of existing IT services in higher education.

## 2. METHODS

This type of research is a type of quantitative descriptive research using the *Structural Equation Modeling* method. Quantitative research aims to test the relationships between variables that exist in a system of sampling from a population and using structured questionnaires as a tool for data collection.

The research location chosen by the author is located at Surabaya State University. The choice of location for data collection is based on several considerations of the author so that the location is chosen. Data collection is spread across all student circles. This research was carried out from March to completion.

The focus of this research is the assessment of the human aspects of an information security program and organizational security culture. The measurement of security culture is based on students' perceptions of the information security program and culture at their higher education institutions. Therefore, this research answers the following questions:

1) What are the human aspects that influence and foster an information security culture?
2) How do organizational security policies and sanctions influence information security culture?
3) What is the effect of student commitment to information security on information security culture?
4) How management organization influence information security culture?
5) How awareness security awareness affect information security culture?

The variables in the model are measured by indicators (questions) in the instrument survey. Each indicator was validated from previous research in the literature with modifications to meet the specific research focus. Analysis of the variables and their relationships was conducted using Structural Equations Modeling (SEM). Following hypotheses were proposed to test the relationship between variables in the model.

The questionnaire was prepared with the aim of obtaining the data required for the research. The statements are made based on two categories, namely information security and privacy and respondents can choose "Agree, Strongly Agree, Moderately Agree, Disagree, Strongly Disagree".

This research uses the SEM-PLS method in data analysis, which involves two main stages: measurement model and structural model analysis**.** The measurement model or outer model stage aims to test the validity and reliability of the data. Tests conducted at this stage include *convergent validity***,** *discriminant validity*, and *composite reliability***.** Meanwhile, the structural model stage is used to evaluate hypothesis validity or deciding the acceptance and rejection of the research hypothesis. At this stage, testing includes *coefficient of determination* **(**$R^2$**)**, effect size **(**$f^2$).

## 3. RESULTS AND DISCUSSION

Table 1. Outlier Evaluation

| | Original Sample (O) | Sample Average (M) | Standard Deviation (STDEV) | T Statistic (\|O/STDEV\|) |
|---|---|---|---|---|
| KKI.H.1.1 <- KKI_ | 0.798 | 0.793 | 0.029 | 27.643 |
| KKI.H.2.1 <- KKI_ | 0.794 | 0.793 | 0.026 | 30.793 |
| KKI.H.3.1 <- KKI_ | 0.820 | 0.818 | 0.023 | 35.269 |
| KM.H.1.1 <- K.M | 0.850 | 0.847 | 0.040 | 21.474 |
| KM.H.2.1 <- K.M | 0.795 | 0.791 | 0.045 | 17.875 |
| KO.H.1.1 <- K.O | 0.824 | 0.823 | 0.026 | 32.100 |
| KO.H.2.1 <- K.O | 0.825 | 0.820 | 0.030 | 27.323 |
| KO.H.3.1 <- K.O | 0.719 | 0.721 | 0.046 | 15.702 |
| ODM.H.1.1 <- ODM | 0.718 | 0.713 | 0.043 | 16.684 |
| ODM.H.2.1 <- ODM | 0.815 | 0.814 | 0.020 | 41.203 |
| ODM.H.3.1 <- ODM | 0.812 | 0.810 | 0.025 | 32.509 |
| ODM.H.4.1 <- ODM | 0.787 | 0.787 | 0.024 | 32.217 |
| PKM.H.1.1 <- PKM | 0.845 | 0.843 | 0.028 | 30.075 |
| PKM.H.2.1 <- PKM | 0.866 | 0.866 | 0.024 | 35.571 |
| VAT.H.1.1 <- VAT_ | 0.786 | 0.783 | 0.026 | 30.006 |
| VAT.H.2.1 <- VAT_ | 0.789 | 0.788 | 0.026 | 30.728 |
| VAT.H.3.1 <- VAT_ | 0.764 | 0.762 | 0.031 | 24.384 |
| VAT.H.4.1 <- VAT_ | 0.728 | 0.727 | 0.033 | 22.310 |

From the table above, indicator validity is evaluated by looking at the factor loading value between the variable and the indicator. Validity is considered adequate if the factor loading value is more than 0.5 or the T- statistic value exceeds 1.96 (based on the Z value at $\alpha = 0.05$). Factor loading represents the correlation between indicators and variables. If the value is more than 0.5, then validity is met, and if the T-statistic value is greater than 1.96, then significance is achieved.

Based on the outer loading table above, all reflective indicators on the variables of information security culture, prevention of negative behavior, organizational policies, student commitment to security, student training and awareness, and organizational management support show factor loading values (original sample) above 0.50 and are significant (the T-statistic value is greater than the Z value at $\alpha = 0.05$ or 5%, which is 1.96). Therefore, the estimation results show that all indicators have met convergent validity, so their validity is considered good.

Table 2. Cross Loading

| | KKI_ | KM_ | KO_ | ODM_ | PKM_ | VAT_ |
|---|---|---|---|---|---|---|
| KKI.H.1.1 | 0.798 | 0.302 | 0.431 | 0.361 | 0.347 | 0.484 |
| KKI.H.2.1 | 0.794 | 0.323 | 0.427 | 0.409 | 0.399 | 0.432 |
| KKI.H.3.1 | 0.820 | 0.379 | 0.430 | 0.422 | 0.458 | 0.516 |
| KM.H.1.1 | 0.367 | 0.850 | 0.411 | 0.471 | 0.350 | 0.398 |
| KM.H.2.1 | 0.319 | 0.795 | 0.399 | 0.408 | 0.422 | 0.367 |
| KO.H.1.1 | 0.458 | 0.332 | 0.824 | 0.431 | 0.528 | 0.568 |
| KO.H.2.1 | 0.460 | 0.467 | 0.825 | 0.446 | 0.411 | 0.524 |
| KO.H.3.1 | 0.332 | 0.370 | 0.719 | 0.441 | 0.369 | 0.447 |
| ODM.H.1.1 | 0.361 | 0.494 | 0.453 | 0.718 | 0.404 | 0.429 |
| ODM.H.2.1 | 0.410 | 0.386 | 0.444 | 0.815 | 0.437 | 0.478 |
| ODM.H.3.1 | 0.389 | 0.417 | 0.400 | 0.812 | 0.461 | 0.484 |
| ODM.H.4.1 | 0.391 | 0.392 | 0.433 | 0.787 | 0.404 | 0.509 |
| PKM.H.1.1 | 0.414 | 0.351 | 0.496 | 0.479 | 0.845 | 0.520 |
| PKM.H.2.1 | 0.444 | 0.443 | 0.457 | 0.453 | 0.866 | 0.446 |
| VAT.H.1.1 | 0.475 | 0.310 | 0.506 | 0.464 | 0.407 | 0.786 |
| VAT.H.2.1 | 0.452 | 0.314 | 0.471 | 0.422 | 0.379 | 0.789 |
| VAT.H.3.1 | 0.434 | 0.365 | 0.523 | 0.498 | 0.487 | 0.764 |
| VAT.H.4.1 | 0.462 | 0.437 | 0.501 | 0.478 | 0.454 | 0.728 |

From the cross-loading data, it is obtained that all load factor values (shaded) on each indicator both on the Information Security Culture variable (KKI), Negative Peril Prevention (PPN), Organizational Policy (KO), Student Commitment to Security (KM), Student Training and Awareness (PKM), Management Support Organization (ODM) show a loading factor value above 0.5 so that it can be said that all indicators in this study have fulfilled their validity or good validity.

AVE, or "Average Variance Extracted," is a measure in factor analysis and structural research that indicates how much of the variance of the indicators can be explained by the construct in question. AVE is used to assess the convergent validity of a construct; higher AVE values (generally above 0.5) indicate that the construct is able to explain more than half of the variance of the measured items.

Table 3. Average Variance Extracted (Ave)

| | Average Extract ed Variance (AVE) |
|---|---|
| K.M | 0.677 |
| K.O. | 0.626 |
| KKI_ | 0.647 |
| ODM | 0.615 |
| PKM | 0.732 |
| VAT_ | 0.588 |

The AVE measurement model is a value that shows the amount of indicator variance contained by the latent variable. Convergent AVE values greater than 0.5 indicate the

adequacy of validity as a latent variable.

The AVE test results for the Information Security Culture variable or (KKI) are 0.647, the Commitment variable is 0.647. Student (KM) of 0.677, Organizational Policy (KO) of 0.626, Management Support Organization (ODM) of 0.615, Student Training and Awareness (PKM) variable of 0.732, and Prevention of Negative Behavior (PPN) of .558. Based on this table, it can be seen that the AVE value of Information Security Culture or KKI,

Analysis of Results PLS

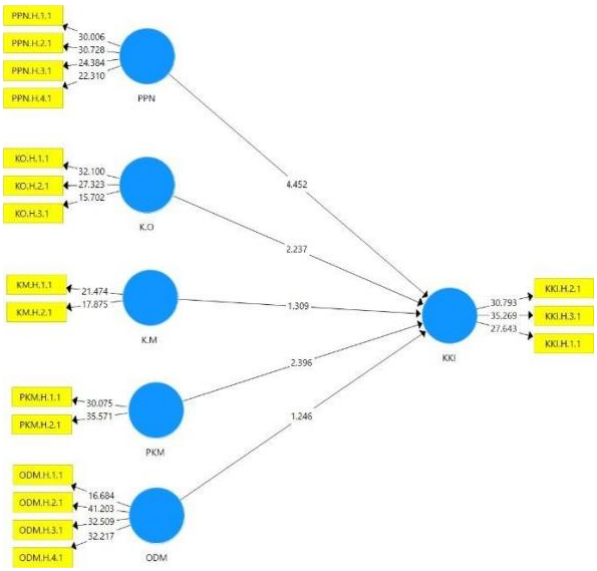


Figure 1. Outer Model with Factor Loading, Path Coefficient and R-Square Source: data processing, SmartPLS output

Student Commitment (KM), Organizational Policy (KO), Management Support Organization, Student Training and Awareness, and Prevention of Negative Behavior variables are more than 0.5. So, these variables have met the requirements of conferent validity.

Table 4. Composite Reliability

| | Composite Reliability |
|---|---|
| K.M | 0.808 |
| K.O. | 0.833 |
| KKI_ | 0.846 |
| ODM | 0.864 |
| PKM | 0.845 |
| VAT_ | 0.851 |

Construct reliability is measured by the composite reliability value, the construct is reliable if the composite reliability value is above 0.70, so the indicator is called consistent in measuring the latent variable.

The results of Composite Reliability testing show that the variable Student Commitment to Information (KM) variable is 0.808, the Organizational Policy (KO) variable is 0.833, the Information Security Culture (KKI) variable is 0.846, Management Support Organization (ODM) is 0.864, Student Training and Awareness (PKM) is 0.845 and Prevention of Negative Behavior (PPN) is 0.851. The six variables show a Composite Reliability value above 0.70 so that it can be said that all variables in this study are reliable.

Table 5. Latent Variable Correlation

| | K.O_ | KKI | KM_ | ODM | PKM | VAT_ |
|---|---|---|---|---|---|---|
| **K.O_** | 1,000 | | | | | |
| **KKI** | 0,577 | 1,000 | | | | |
| **KM_** | 0,603 | 0,490 | 1,000 | | | |
| **ODM** | 0,645 | 0,605 | 0,611 | 1,000 | | |
| **PKM** | 0,630 | 0,581 | 0,463 | 0,665 | 1,000 | |
| **VAT_** | 0,725 | 0,685 | 0,561 | 0,737 | 0,691 | 1,000 |

In PLS, the relationship between variables or constructs can be correlated, both between exogenous and endogenous variables and between exogenous variables, as seen in the *latent variable correlations* table above. The correlation between variables has a maximum value of 1, where the closer the value is to 1, the stronger the correlation relationship is considered.

Based on the *latent variable correlations* table, the average correlation value between variables shows a fairly high and diverse level of correlation. The highest correlation was found between the variables of Management Support Organization (ODM) and Prevention of Student Negative Behavior (PPN) with a value of 0.737. This shows that, among the variables in the research model, the relationship between ODM and VAT is stronger than the relationship between other variables.

From the PLS output image above, you can see the factor loading value for each indicator, which is located above the arrow connecting the variable and its indicator. In addition, the *path coefficients* can be found above the arrow line connecting the exogenous variables with the endogenous variables. The R-Square value can also be seen inside the circle representing the endogenous variable (in this case, the Information Security Culture variable).

Inner Model (Structural Model Testing) Structural model testing is done by analyzing the R-Square value, which is used as an indicator of *goodness-of-fit* model. Inner model testing can be seen through the R-Square value in the relationship between latent variables. The $R^2$ value illustrates the extent to which the exogenous (independent / free) variables in the model are able to explain the endogenous (dependent / dependent) variables.0

R-squared ($R^2$) is a statistical measure used in regression analysis to assess how well the regression model explains the variance of the dependent variable. More specifically, $R^2$ indicates the percentage of variation in the data that can be explained by the independent variables in the model.

$R^2$ measures the variance explained in each endogenous construct, therefore it is a measure of the explanatory power of the model.

$R^2$= 0.75, 0.50 and 0.25 (substantial, moderate and weak).Multicollinearity

"Acceptable $R^2$ values are based on the context and in some disciplines an $R^2$ value as low as 0.10 is considered satisfactory, for example, when predicting stock returns".

R-squared:

1. Value Range: $R^2$ ranges from 0 to 1.
   - $R^2$= 0: The model does not explain the variance at all.
   - $R^2$= 1: The model explains all the variance in the data.
2. Interpretation: Higher $R^2$ values

indicates that the model is better at explaining the data. For example, $R^2$ = 0.8 means 80% of the variation in the dependent variable can be explained by the independent variables.

3. Limitations: $R^2$ does not indicate

causal relationship and cannot be used to compare models with different numbers of variables. In addition, a high value does not necessarily mean that the model is good, as

overfitting can occur.

4. Applications: $R^2$ is widely used in various fields, including economics, social sciences, and health sciences, to assess prediction models.

Table 6. R Square

| | R Square | Adjusted R Square |
|---|---|---|
| KKI | 0,425 | 0,418 |

The value of $R^2$ = 0.425. It can be interpreted that the model is able to explain the phenomenon of Information Security Culture which is influenced by independent variables including Prevention of Negative Behavior, Organizational Policy, Student Commitment to Security, Training and Student Awareness and Management Support Organization with a variance of 42.5%. While the remaining 57.5% is explained by other variables outside this study (other than Prevention of Negative Behavior, Organizational Policy, Student Commitment to Security, Training and Student Awareness and Management Support Organization). In addition to the $R^2$ value, the *Goodness of Fit of the* research model can also be measured using $Q^2$ (*Q-Square predictive relevance*), which is used to evaluate the extent to which the structural model and its parameter estimates are able to predict observed values well. If the $Q^2$ value> 0, the model is considered to have *predictive relevance*, while if $Q^2 \leq 0$, the model is considered to have less *predictive relevance*. The $Q^2$ value is calculated using the following formula:

$Q^2$ is a means of assessing the predictive relevance of the model (Hair et al., 2014).

In particular, a $Q^2$ value > 0 for a given endogenous construct indicates that the observed values have been well reconstructed so that the model has predictive relevance (Hair et al., 2014).

As a rule of thumb (Hair et al., 2019), the value of $Q^2$ describes the value of predictive relevance; >0 (small), >0.25 (medium) and >0.50 (large).

Q2=1–(1–R12)(1–R22)...(1–Rp2)

where R12,R22,...,R2$R_1^2$, $R_2^2$,...,$R_p^2$R12,R22,...,R2$^2$ is the R-square value of the endogenous variables in the model. The $Q^2$ value is in the range $0 < Q^2 < 1$, and the closer to 1, the better the model is considered. This $Q^2$ value is equivalent to the total coefficient of determination in *path* analysis.

In this study, the $Q^2$ value was calculated as follows:

Q2=1-(1-0.425)=0.425.$Q^2$= 1 - (1 - 0.425=

0,425.Q2=1–(1–0,425)=0,425.

Based on the calculation results which show a $Q^2$ value of 0.425, it can be concluded that the research model has *predictive relevance*.

*Hypothesis Testing.*

Furthermore, hypothesis testing can be seen from the coefficient results and the T-statistic value of the inner model in the following table

Table 7. Path Coefficients (Mean, Stdev, T- Values)

| | Original Sample (O) | Sample Average (M) | Standard Deviation (STDEV) | T Statistics (\|O/STDEV\|) | P Values |
|---|---|---|---|---|---|
| K.O_ -> KKI | 0.072 | 0.071 | 0.055 | 1.309 | 0.191 |
| KM_ -> KKI | 0.154 | 0.149 | 0.069 | 2.237 | 0.026 |
| ODM -> KKI | 0.096 | 0.100 | 0.077 | 1.246 | 0.213 |
| PKM -> KKI | 0.151 | 0.149 | 0.063 | 2.396 | 0.017 |
| VAT_ -> KKI | 0.318 | 0.322 | 0.071 | 4.452 | 0.000 |

Source: data processing, *SmartPLS* output

From the table above it can be concluded that the hypothesis that states:

H1: Organizational Policy (KO) has a negative effect on Information Security Culture (KKI) can be accepted, with path coefficients of 0.072, and a T-statistic value of 1.309 < 1.96 (T-table value of Zα = 0.05), then it **is not significant (negative).**

H2: Student Commitment (KM) has a positive effect on Information Security Culture (KKI) can be accepted, with path coefficients of 0.154, and a T-statistic value of 2.237 < 1.96 (T-table value of Zα = 0.05), then **Significant (positive).**

H3: Management Support Organization (ODM) has a negative effect on Information Security Culture (ISC) can be accepted, with path coefficients 0.096, and a T-statistic value of 1.246< 1.96 (T-table value of Zα = 0.05), then it is not **significant (negative).**

H4: Student Training and Awareness (PKM) has a positive effect on Information Security Culture (KKI) can be accepted, with path coefficients of 0.151, and a T-statistic value of 2.396 < 1.96 (T-table value of Zα = 0.05), then **Significant (positive).**

H5: Prevention of Negative Behavior (PPN) has a positive effect on Information Security Culture (ISC) can be accepted, with path coefficients 0.318, and a T-statistic value of 4.452 < 1.96 (T-table value of Zα = 0.05), then **Significant (positive).**

*Discussion of Research Results*

*A. Effect of Negative Behavior Prevention on Information Security Culture*

Based on the results of the research that has been conducted, the results show that Prevention of Negative Behavior (PPN) makes a real contribution in improving Information Security Culture (ISC). The higher the Prevention of Negative Behavior, the better the Information Security Culture among Surabaya students in maintaining information security in Higher Education. In the analysis of this study, it is stated that the Information Security Culture of students can be influenced by the Prevention of Negative Behavior. The existence of written and unwritten guidelines and regulations shows that it can be a tool for students to maintain the information security culture that exists in their respective universities. Punishment and reward levels have a significant effect on compliance intentions carried out by students. This is reinforced when there is a high level of certainty that rewards or punishments will be enforced. Also the impact of punishment on the intention to comply is greater when the reward is low. This identifies that Prevention of Negative Behavior among Surabaya students can prevent information leakage and information security needs to provide the right information to the right people so that it will not

fall into the wrong hands or be misused.

The results of this study are in accordance with research conducted by Henry (2018) which states that behavioral prevention has a significant influence on information security culture.

*B. Effect of Organizational Policy on Information Security Culture*

Based on the results of the research that has been conducted, the results show that Organizational Policy (KO) does not make a real contribution to improving Information Security Culture (ISC). The higher the Organizational Policy, the still no effect on Information Security Culture.

In this research analysis, it states that there is an information security policy at universities in Surabaya. There is a possibility that Surabaya students are not aware of the policy. Therefore, the policy is not effective if it is not known to exist and cannot be accessed as a reference. The results of this study in accordance with research conducted by Henry (2018) which states that Organizational Policy has no or insignificant effect on Culture Security Information impact.

negative and insignificant.

*C. The Effect of Student Commitment to Security on Information Security Culture*

Based on the results of the research that has been conducted, the results show that Student Commitment (KM) does not make a real contribution to improving Information Security Culture (ISC). The higher the Student Commitment, the no effect on the Information Security Culture of Surabaya students in the analysis of this study states Student Commitment has not referred to the attitude of Surabaya students. Surabaya overall towards. the organization's information security program and their involvement in protecting its assets.

The results of this study are in accordance with research conducted by Henry (2018) which states that Student Commitment to Information Security Culture has a negative and insignificant impact.

*D. The Effect of Training and Student Awareness on Information Security Culture*

Based on the results of the research that has been done, the results show that Training and Student Awareness (PKM) make a real contribution in improving Information Security Culture (KKI). The higher the Student Awareness Training, the no effect on Information Security Culture.

In the analysis of this research states that students need knowledge to use the system correctly, compliance with policies, and handling of data. Information security in Higher Education should implement training and awareness programs that focus on policies, roles, and responsibilities. Students' lack of awareness and proper training can make organizations face security risks.

The results of this study are inversely proportional to research conducted by Henry (2018) which states that Training and Student Awareness have a negative or insignificant effect on Information Security Culture.

*E. Effect of Management Support Organization on Information Security Culture*

Based on the results of the research that has been carried out, the results show that the Management Organization (ODM) does not make a real contribution to improving Information Security Culture (ISC). The higher the contribution of the Management Support Organization, the no effect on Information Security Culture.

In the analysis of this study states that Organizational Management support is an important factor in fostering information security culture. The more visible the organizational support, the healthier and more positive the information security culture in Higher Education. From the results of the study, it shows that many respondents believe that organizational support has not had an impact on information security culture. Such support includes budget, technology and human resources. Support and leadership from management are key contributors to the success of information security implementation efforts.

The results of this study compare with research conducted by Henry (2018) which states that the Management Support Organization on Information Security Culture has a positive effect while the results of research conducted by the author are not significant Information Security Culture.

## CONCLUSION

Based on results testing with using PLS-SEM analysis method to test the knowledge information security culture among higher education students, the following conclusions can be drawn

1. Organizational Policy (KO) has a **negative** and insignificant influence on Information Security Culture (ISC) with a **path cooefficient** of 0.072 and a T- statistic value of 1.309< 1.96 (T-table value of Zα = 0.05). This indicates that policies that are too strict can reduce efficiency without having a positive impact on information security.
2. Student Commitment to Security (KM) has a **positive** and significant influence on Information Security Culture (ISC) with a **path coefficient** of 0.154 and a T- statistic value of 2.237 < 1.96 (T-table value of Zα = 0.05). This emphasizes that students' active participation in maintaining information security contributes greatly to the overall security culture.
3. Management Support Organization (ODM) has a **negative** and insignificant effect on Information Security Culture (ISC) with a **path coefficient** of 0.096 and a T-statistic value of 1.246 < 1.96 (T-table value of Zα = 0.05). This indicates that supportive management can increase compliance and awareness of students.
4. Student Training and Awareness (PKM) has a **positive** and significant influence on Information Security Culture (KKI) with a **path coefficient** of 0.151 and a T- statistic value of 2.396 < 1.96 (T-table value of Zα = 0.05). This indicates that the better the prevention of negative behavior, the more the information security culture of students will increase.
5. Prevention of Negative Behavior (PPN) has a **positive** and significant influence on Information Security Culture (ISC) with a **path coefficient** of 0.138 and a T- statistic value of 4.452 < 1.96 (T-table value of Zα = 0.05). This indicates that the better the prevention of negative behavior, the more students' information security culture will increase.

This model can be implemented through a combination of effective training, relevant policies, management support, student commitment, and incentives that encourage positive behavior. The main focus is on raising students' awareness to involve them in efforts to keep their data and privacy safe in the university environment in Surabaya. In this way, privacy and student data security in higher education can be optimally maintained. This approach can also be applied to other universities with adjustments to the needs of each institution.

## ACKNOWLEDGEMENTS

The author's gratitude goes to Allah SWT. who has given his gifts and grace to the author so that he can complete this scientific journal well. The author is also grateful to those who have guided, motivated, and provided assistance, namely by parents, supervisors, siblings, friends, and friends in arms. May their kindness and sincerity be rewarded by Allah with more blessings.

## REFERENCES

[1] Ando, Remi, Shigeyoshi Shima, and Toshihiko Takemura. 2016. "Analysis of Privacy and Security Affecting the Intention of Use in Personal Data Collection in an IoT Environment." *IEICE TRANSACTIONS on Information and Systems* 99 (8): 1974-81.

[2] Arpaci, Ibrahim, Kerem Kilicer, and Salih Bardakci. 2015. "Effects of Security and Privacy Concerns on Educational Use of Cloud Services." *Computers in Human Behavior* 45: 93-98
[3] Enaizan, Odai, Bilal Eneizan, Mohammad Almaaitah, Ahmad Tawfig Al-Radaideh, and Ashraf Mousa Saleh. 2020. "Effects of Privacy and Security on the Acceptance and Usage of EMR: The Mediating Role of Trust on the Basis of Multiple Perspectives." *Informatics in Medicine Unlocked* 21: 100450
[4] Farida, Lina Suli. 2010. "Multiple Linear Regression Analysis with Heteroscedasticity through Weight Least Square Approach: Study of Apbn Data Year 1976-2007."
[5] Glaspie, Henry, "Assessment of Information Security Culture in Higher Education" (2018). *Electronic Theses and Dissertations.* 6009.
[6] Ghozali, Imam. 2013. "Application of Multivariate Analysis with the IBM SPSS 21 Update PLS Regression Program. Semarang: Diponegoro University Publishing House."
*Information Technology* 2 (2).
[7] Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS- SEM: Indeed a silver bullet. Journal of Marketing Theory and Practice, 19(2), 139-152. https://doi.org/10.2753/MTP1069-6679190202.
[8] Haeussinger, Felix J., and Johann J. Kranz. 2013. "Information Security Awareness: Its Antecedents and Mediating Effects on Security Compliant Behavior." International Conference on Information Systems (ICIS 2013): Reshaping Society Through Information Systems Design 3 (December 2013): 2222-37.
[9] Hox, J. J., & Bechger, T. M. (1998). An introduction to structural equation modeling. Family science review, 11, 354-373.
[10] ITU. 2017. Global Cybersecurity Index (GCI) 2017. ITU-D Global. https://www.itu.int/dms_pub/itu- d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.
[11] Jaeger, Lennart. 2018. "Information Security Awareness: Literature Review and Integrative Framework." Proceedings of the Annual Hawaii International Conference on System Sciences 2018-Janua (3): 4703- 12. https://doi.org/10.24251/hicss.2018.593.
[12] Kurniawan, Deny. 2008. "Linear Regression." Statistics.
[13] Narimawati, U., & Sarwono, J. (2007). Structural equation modeling (SEM) in economic research: using lisrel. Gaya Medias.
[14] Nurjanah, Devi, and Senie Destya. 2022. "Measuring the Level of Student Information Security Awareness in Online Learning." Journal of Information Systems and Technology (JustIN) 10 (1): 81. https://doi.org/10.26418/justin.v10i1.44362.
[15] Riyandhika, Raja Rizky. 2020. "Analysis of Cybersecurity Awareness among Students in Indonesia." AUTOMATA 1 (2).
[16] Whitman, Michael E, and Herbert J Mattord. 2011. "Principles of Information Security Fourth Edition." Learning, 269, 289