# FACTORS AFFECTING INFORMATION SECURITY CULTURE AND ITS INFLUENCE ON INFORMATION SECURITY AWARENESS (ISA) AT STELLA MARIS HOSPITAL MAKASSAR

**Jayanti Novitasari[1*], Irwandy [2] , Noer Bahry Noor [3], Fridawaty Rivai [4], Andi Indahwaty Sidin [5]**

[1] *Student of Master of Hospital Administration Study Program, Faculty of Public Health, Hasanuddin University*
[2,3,4,5]*Hospital Administration Study Program, Faculty of Public Health, Hasanuddin University*

**Abstract:**
Background: Information security awareness (ISA) is crucial for hospitals to protect patient data from cyber threats. Objective: This study examines the influence of intrinsic and extrinsic factors on information security culture (ISC) and its impact on ISA at Stella Maris Hospital Makassar. Methods: A quantitative study with a cross-sectional design was conducted, involving 220 respondents selected through stratified purposive sampling. Data were collected using a Likert-scale questionnaire and analyzed using linear regression. Results: The results indicate that intrinsic factors, such as knowledge and compliance, have a greater influence on ISC (B = 0.493, p = 0.001) than extrinsic factors (B = 0.230, p = 0.001). ISC also has a weak but positive relationship with ISA (B = 0.140, p = 0.036). Conclusion: Enhancing ISA in hospitals can be achieved by strengthening ISC through strategies that improve intrinsic and extrinsic factors. Continuous security training and management support are key steps in increasing healthcare workers' awareness and compliance with information security.

Keywords: *Information Security Awareness, Information Security Culture, Intrinsic Factors, Extrinsic Factors, Hospital*

## INTRODUCTION

Information security awareness is crucial in hospitals, where patient data is a sensitive asset that must be protected. Low awareness of information security can increase the risk of incidents that harm, such as data theft or disruption of medical services (Dafid & Dorie, 2020). Managing patient data through the Hospital Management Information System (SIMRS) must be done carefully as information technology evolves (Putu et al., 2024).

Hospitals must have clear policies to protect patient data and build a strong information security culture. Research shows that proper training and supportive leadership can enhance information security awareness among staff (Akhsan & Pendrian, 2024; Nurillah & Trihandoyo, 2024). Additionally, intrinsic factors such as motivation and extrinsic factors like policies and training significantly influence security culture (Triono et al., 2021).

At Stella Maris Hospital Makassar, information security awareness remains low, with most employees never attending training or seminars related to security (80% never attended training, 93.3% unaware of how to report threats). This creates vulnerabilities for cyber threats that could jeopardize the integrity of patient data and hospital systems. Successful information security management requires clear policies, active leadership, and continuous training to establish a strong security culture and improve awareness among staff.

## METHODS

This research uses a quantitative approach. Quantitative research is used to test theories by investigating the relationships between variables. These variables are measured using research

instruments, allowing for numerical data that can be analyzed using statistical procedures (Yusuf, 2014). This is an analytical observational study, where the researcher seeks to examine the relationships between variables and analyze the collected data. The approach used is a cross-sectional study design, which involves measuring or observing variables at a single point in time (point time approach) (Raihan, 2017). The research was conducted at Stella Maris Hospital in Makassar in January 2025.

**Population and Sample**

The population of this study consists of employees at Stella Maris Hospital, Makassar, totaling 555 people, namely doctors, nurses, midwives, pharmacists, laboratory assistants, radiographers, nutritionists, medical recorders, and management staff. The sample size was calculated using the Slovin formula with a margin of error of 5%, resulting in 220 employees. The number of samples selected was in accordance with the minimum number needed for quantitative research. The sampling technique used is stratified purposive sampling, where the sample is selected proportionally from different strata based on the type of profession, ensuring that each group with different roles in the use of the Hospital Management Information System (SIMRS) is represented. The sample is selected randomly within each group, according to the inclusion and exclusion criteria.

**Data Collection Procedure**

In this study, a Likert-scale questionnaire was used to measure the intrinsic and extrinsic factors influencing Information Security Culture (ISC) and their impact on Information Security Awareness (ISA) among hospital staff. The questionnaire was structured into different sections, each addressing key dimensions related to security culture and awareness.

The intrinsic factors section assessed employees' knowledge of information security, their compliance with security policies, their security behavior, and their general awareness of security threats in the workplace. These factors were measured through statements regarding the importance of protecting sensitive data, understanding security risks, following security protocols, and responding to potential cyber threats.

The extrinsic factors section examined aspects such as training and awareness programs, operational management, organizational culture, top management support, and workplace capabilities. This section aimed to evaluate the hospital’s role in fostering a security-conscious environment through leadership commitment, policy enforcement, regular system audits, and risk management strategies.

The questionnaire also included a specific section on Information Security Culture (ISC), which measured employees' perceptions of the organization's security policies, monitoring systems, and overall commitment to information security. Additionally, Information Security Awareness (ISA) was assessed through dimensions of knowledge, attitude, and behavior to determine how well employees recognize and respond to cybersecurity threats in their daily tasks.

The questionnaire was distributed to selected respondents based on the inclusion criteria. Responses were collected electronically and manually to ensure maximum participation. Once completed, the data was reviewed for completeness and accuracy before proceeding with statistical analysis.

**Statistical Analysis**

The collected data will be processed using SPSS software. Univariate analysis was conducted using descriptive statistics to examine variable distributions. Bivariate analysis with simple linear regression assessed the relationship between intirinsic and extrinsic factors with information security culture (ISC) and its correlation with information security awareness (ISA), while multivariate analysis with multiple linear regression evaluated the combined influence of multiple factors on ISC. Reliability testing was performed using Cronbach’s alpha ($\geq 0.6$), and validity testing ensured the questionnaire accurately measured research variables. The findings help identify key factors influencing ISC and

ISA at Stella Maris Hospital.

**Research Ethics**

This study was conducted in accordance with the principles of research ethics. Prior to data collection, ethical approval was obtained from the Ethics Committee of the Faculty of Public Health, Hasanuddin University. All respondents were given informed consent and explained that participation was voluntary and anonymous. The data collected were used only for research purposes and kept confidential

**RESULTS**

The characteristics of the respondents studied included age, gender, last education, length of service at the hospital and employment status.

**Table 1Distribution of Respondents Based on Respondent Characteristics at Stella Maris Hospital Makassar in 2024**

| Respondent Characteristic | | Amount | |
|---|---|---|---|
| | | n | % |
| **Age** | < 35 Years | 156 | 70.9 |
| | ≥ 35 Years | 64 | 29.1 |
| **Total** | | **220** | **100** |
| **Gender** | Male | 30 | 13.6 |
| | Female | 190 | 86.4 |
| **Total** | | **220** | **100** |
| **Education** | High School | 9 | 4.1 |
| | Diploma | 49 | 22.3 |
| | Bachelor's Degree | 142 | 64.5 |
| | Postgraduate/Specialist | 20 | 9.1 |
| **Total** | | **220** | **100** |
| **Employment Status** | Doctor | 31 | 14.1 |
| | Nurse | 107 | 48.6 |
| | Midwife | 7 | 3.2 |
| | Pharmacist | 22 | 10 |
| | Laboratory Assistant | 9 | 4.1 |
| | Physiotherapist | 3 | 1.4 |
| | Radiographer | 7 | 3.2 |
| | Nutrinionist | 1 | 0.5 |
| | Medical Record | 18 | 8.2 |
| | Managemet | 15 | 6.8 |
| **Total** | | **220** | **100** |
| **Length of Work** | < 5 Years | 116 | 52.7 |
| | ≥ 5 Years | 104 | 47.3 |
| **Total** | | **220** | **100** |

*Source: Primary Data*

Table 1 presents the distribution of respondents based on their characteristics at Stella Maris Hospital in 2024. In terms of age, the majority of respondents (70.9%) are under 35 years old, while 29.1% are 35 years or older. Regarding gender, most respondents are female (86.4%), with 13.6% being male. In terms of education, the majority of respondents hold a Bachelor's degree (64.5%),

followed by those with a Diploma (22.3%). Regarding employment status, most respondents are nurses (48.6%), followed by doctors (14.1%). For length of work, more than half of the respondents (52.7%) have less than 5 years of work experience, while 47.3% have worked for more than 5 years. The total number of respondents in this study is 220.

**Table 2. Distribution of Respondents Based on Intrinsic Factor Dimensions**

| **Dimensions** | | **n** | **%** |
|---|---|---|---|
| Knowledge | Good | 149 | 67.7 |
| | Not Good | 71 | 32.3 |
| **Total** | | **220** | **100** |
| Security Compliance | Good | 127 | 57.7 |
| | Not Good | 93 | 42.3 |
| **Total** | | **220** | **100** |
| Security Behaviour | Good | 124 | 56.4 |
| | Not Good | 96 | 43.6 |
| **Total** | | **220** | **100** |
| Soft Issues - Workplace Independent | Good | 117 | 53.2 |
| | Not Good | 103 | 46.8 |
| **Total** | | **220** | **100** |

*Source: Primary Data*

Table 2 presents data on four dimensions related to Information Security Culture among 220 respondents at Stella Maris Hospital in 2024. In terms of **Knowledge**, 149 respondents (67.7%) rated their understanding as "Good," while 71 respondents (32.3%) rated it as "Not Good." Regarding **Security Compliance**, 127 respondents (57.7%) reported "Good" compliance with security policies, while 93 respondents (42.3%) rated their compliance as "Not Good." For **Security Behavior**, 124 respondents (56.4%) rated their behavior as "Good," with 96 respondents (43.6%) rating it as "Not Good." Finally, in the dimension of **Soft Issues - Workplace Independent**, 117 respondents (53.2%) rated their awareness of workplace-related security issues as "Good," while 103 respondents (46.8%) rated it as "Not Good." These findings indicate varying levels of understanding, compliance, behavior, and awareness of information security practices among the respondents, with the majority indicating a "Good" rating in each dimension, highlighting the overall positive but diverse security culture within the hospital.

**Table 3. Distribution of Respondents Based on Extrinsic Factor Dimensions**

| **Dimensions** | | **n** | **%** |
|---|---|---|---|
| Training and Awareness | Good | 151 | 68.6 |
| | Not Good | 69 | 31.4 |
| **Total** | | **220** | **100** |
| Operational Management) | Good | 103 | 46.8 |
| | Not Good | 117 | 53.2 |
| **Total** | | **220** | **100** |
| Organizational Culture | Good | 166 | 75.5 |
| | Not Good | 54 | 24.5 |
| **Total** | | **220** | **100** |
| Top Management Support | Good | 103 | 46.8 |
| | Not Good | 117 | 53.2 |

| | | | |
|---|---|---|---|
| **Total** | | **220** | **100** |
| Workplace Capabilities | Good | 167 | 75.9 |
| | Not Good | 53 | 24.1 |
| **Total** | | **220** | **100** |
| Risk and Response Factors | Good | 92 | 41.8 |
| | Not Good | 128 | 58.2 |
| **Total** | | **220** | **100** |
| Change Management | Good | 84 | 38.2 |
| | Not Good | 136 | 61.8 |
| **Total** | | **220** | **100** |
| Information Security Policies | Good | 74 | 33.6 |
| | Not Good | 146 | 66.4 |
| **Total** | | **220** | **100** |

*Source: Primary Data*

Based on the distribution of respondents according to extrinsic factors, the majority rated several dimensions as inadequate. In **Training and Awareness**, 68.6% felt it was good, while 31.4% did not. For **Operational Management**, 46.8% considered it good, but 53.2% did not. In **Organizational Culture**, 75.5% rated it good. **Top Management Support** was rated good by 46.8%, while 53.2% found it lacking. **Workplace Capabilities** were good for 75.9%, but 24.1% disagreed. In **Risk and Response Factors**, 41.8% rated it good, while 58.2% did not. **Change Management** and **Information Security Policies** were rated good by only 38.2% and 33.6%, respectively, with the rest finding them inadequate. Overall, most respondents rated extrinsic factors such as operational management, top management support, and information security policies as lacking.

**Table 4. Results of Simple Linear Regression Analysis**

| **Variabel Independen** | **Information Security Culture (Y)** | | | | | |
|---|---|---|---|---|---|---|
| | **R** | **Anova** | | **Koefisien Regresi** | | |
| | | **F** | **Sig** | **B** | **t** | **Sig** |
| **(constant)** | | | | 0.791 | 8.561 | 0.000 |
| **Intrinsic Factors ($X_1$)** | 0.243 | 69.938 | 0.000 | 0.493 | 8.363 | 0.000 |
| **(constant)** | | | | 1.183 | 11.541 | 0.000 |
| **Extrinsic Factors ($X_2$)** | 0.053 | 12.214 | 0.001 | 0.230 | 3.495 | 0.001 |
| **Variabel Independen** | **Information Security Awareness (Z)** | | | | | |
| | **R** | **Anova** | | **Koefisien Regresi** | | |
| | | **F** | **Sig** | **B** | **t** | **Sig** |
| **(constant)** | | | | 1.345 | 12.596 | 0.000 |
| **Information Security Culture (Y)** | 0.020 | 4.436 | 0.036 | 0.140 | 2.106 | 0.036 |

*Source: Primary Data*

The results of the Simple Linear Regression analysis between Intrinsic Factors and Information Security Culture (ISC) at Stella Maris Hospital Makassar show a significant positive relationship. The regression equation **$Y = 0.791 + 0.493 (X_1)$** indicates that for each one-unit increase in Intrinsic Factors, ISC increases by 0.493 units. However, the model explains only 24.3% of the variation in ISC,

suggesting other factors also contribute. The ANOVA test shows a significant F-statistic (69.938, p = 0.000), confirming the model's validity.

In the analysis of Extrinsic Factors, the regression equation **Y = 1.183 + 0.230(X2)** indicates that each one-unit increase in Extrinsic Factors leads to a 0.230 unit increase in ISC. Despite its significance, the model explains only 5.3% of ISC variation, highlighting the influence of other factors. The ANOVA test shows an F-statistic of 12.214 (p = 0.001), reinforcing the role of Extrinsic Factors.

For ISC's impact on Information Security Awareness (ISA), the regression equation **Z = 1.183 + 0.141(Y)** shows a weak effect, with each unit increase in ISC raising ISA by only 0.141 units. The model explains just 2% of ISA variation, suggesting other factors influence awareness. The ANOVA test (F = 4.436, p = 0.036) confirms the model's statistical significance, indicating that ISC still plays a role in shaping ISA, albeit weakly.

**Table 5. Results of Multiple Linear Regression Analysis**

| Variabel Independen | Information Security Culture (ISC) | | | | | |
|---|---|---|---|---|---|---|
| | R | Anova | | Koefisien Regresi | | |
| | | F | Sig | B | t | Sig |
| (constant) | 0.243 | 34.902 | 0.000 | 0.770 | 7.159 | 0.000 |
| Intrinsic Factors | | | | 0.482 | 7.388 | 0.000 |
| Extrinsic Factors | | | | 0.025 | 0.376 | 0.707 |

*Source: Primary Data*

The multiple linear regression analysis shows a significant relationship between intrinsic and extrinsic factors and Information Security Culture (ISC) at Stella Maris Hospital Makassar. The regression equation is:

**$Y = 0.770 + 0.482(X_1) + 0.025(X_2)$**

Intrinsic factors (X1) have a greater impact on ISC, with a coefficient of 0.482, meaning each unit increase in intrinsic factors raises ISC by 0.482 units. The p-value of 0.000 indicates a significant effect. In contrast, extrinsic factors (X2) have a smaller impact, with a coefficient of 0.025, and a p-value of 0.707, indicating no significant effect on ISC.

The model explains 24.3% of ISC variation ($R^2 = 0.243$), suggesting other factors also influence ISC. The ANOVA test shows the model is significant (F = 34.902, p = 0.000), but the impact of extrinsic factors is minimal compared to intrinsic factors.

## DISCUSSION

### 1. The Influence of Intrinsic Factors on ISC

The results of simple linear regression analysis indicate that intrinsic factors significantly influence Information Security Culture (ISC) at Stella Maris Hospital. This is evidenced by the correlation coefficient (R = 0.243), F-value (69.938, p = 0.000), and regression coefficient (B = 0.493, t = 8.363, p = 0.000). These findings suggest that intrinsic factors positively contribute to the development of ISC. Specifically, as an individual's intrinsic factors increase, the stronger the information security culture within the hospital.

ISC is a critical aspect of safeguarding data, particularly in hospitals dealing with sensitive information such as patient medical records (Collier et al., 2023; Jylhä et al., 2017). This study demonstrates that intrinsic factors, including knowledge, security compliance, security behavior, and soft issues, significantly impact ISC. A higher level of intrinsic factors within individuals correlates with a stronger ISC.

One key dimension of intrinsic factors is knowledge. The study shows that 67.7% of respondents possess good knowledge, while 32.3% do not. High knowledge levels indicate that most hospital employees are aware of information security risks, such as data leaks and cyber threats, and understand

preventive measures. A strong understanding of security improves awareness and adherence to policies, contributing to a robust ISC (Kamarulzaman et al., 2022). However, employees with low knowledge present a challenge, as this ignorance increases the risk of security breaches.

Security compliance is another crucial factor. Results show that 57.7% of respondents comply well with security policies, while 42.3% do not. High compliance reflects individuals' adherence to established security procedures, such as using strong passwords and following protocols for handling sensitive information. The lack of compliance in some employees poses a security risk, which may stem from insufficient monitoring or weak enforcement of policies. High compliance is essential for sustaining an effective ISC (Ejigu et al., 2024). Therefore, hospital management must ensure security policies are not only enforced but internalized by all staff as part of the organizational culture.

Security behavior is also a significant factor influencing ISC. The study finds that 56.4% of respondents exhibit good security behavior, while 43.6% do not. Positive security behavior includes actions such as locking screens when leaving workstations and avoiding sharing patient data through insecure channels. However, the proportion of employees displaying poor security behavior suggests that, despite adequate knowledge, daily practices may still fall short. According to the Theory of Planned Behavior (Ajzen, 1991), individuals' actions are influenced by attitudes, social norms, and perceived behavioral control. Therefore, creating an environment that encourages consistent security behavior is crucial, for instance, by offering reminders, conducting security drills, and rewarding compliance.

Lastly, soft issues related to workplace awareness play a vital role in shaping ISC. The study shows that 53.2% of respondents have good awareness, while 46.8% have low awareness. Information security awareness goes beyond understanding policies—it involves proactive actions to protect data and a collective responsibility across the organization. In organizations with strong ISC cultures, individuals feel responsible for maintaining data security and will remind each other about policy violations (Prasetyo et al., 2023). Low awareness, however, may lead employees to view security as solely the responsibility of IT or management. To address this, organizations should enhance security awareness through internal campaigns, interactive training, and clear communication about the risks and consequences of neglecting data security.

**2. The Influence of Extrinsic Factors on ISC**

Extrinsic factors play a significant role in shaping the Information Security Culture (ISC) at Stella Maris Hospital. Simple linear regression analysis shows a significant impact of extrinsic factors on ISC, with an R-value of 0.053, F-value of 12.214, and a regression coefficient of B = 0.230 (p = 0.001). Although the correlation is lower than that of intrinsic factors, extrinsic factors still contribute to the development of ISC through organizational policies, management support, and workplace capabilities in implementing information security effectively.

One key extrinsic factor is training and awareness. The study reveals that 68.6% of respondents have good training and awareness, while 31.4% do not. Training is crucial for helping employees understand the importance of information security and how to implement security practices in daily work. Organizations with structured training programs tend to develop stronger ISC cultures (Aldulaimi et al., 2024). If training is inconsistent, employees may overlook security risks, which weakens the overall security posture. Thus, the hospital should improve the frequency and quality of training to ensure that all employees understand security risks and the actions required to safeguard information.

Another influential dimension is operational management, which reflects the effectiveness of leadership in managing information security. The study shows that only 46.8% of respondents rate operational management as good, while 53.2% rate it poorly. This low rating indicates a lack of coordination and supervision in implementing information security policies. Inadequate management can lead to inconsistent application of security policies, increasing the risk of breaches (Ait El Hadj et al., 2019). To strengthen ISC, hospital management must ensure that security policies are not only

formally established but are also effectively implemented through rigorous monitoring and evaluation systems.

Organizational culture is another crucial factor in ISC. The study finds that 75.5% of respondents rate the organizational culture positively, while 24.5% rate it poorly. A positive organizational culture encourages employees to be more disciplined and aware of the importance of information security. When the organizational culture supports security practices, employees are more likely to proactively follow security policies. Conversely, if the culture does not prioritize security, employees may neglect the importance of adhering to security policies (Ejigu et al., 2024; Mikuletič et al., 2024). Therefore, the hospital needs to foster a culture that emphasizes information security as a shared responsibility.

Top management support also plays a pivotal role in ISC. Only 46.8% of respondents rate top management support as good, while 53.2% rate it poorly. Effective support from top management is critical to ensuring that information security policies are properly implemented throughout the organization. If leadership does not prioritize information security, the policies are unlikely to be effective. Top management must demonstrate commitment by allocating sufficient resources, providing clear policies, and being actively involved in security programs (Darmasaputra Leksono et al., 2020; Munir et al., 2015)

Workplace capabilities also contribute to building ISC. The study indicates that 75.9% of respondents rate workplace capabilities in supporting information security positively, while 24.1% rate them poorly. Workplace capabilities include facilities, infrastructure, and the availability of technology to support security measures. Organizations with strong security systems find it easier to implement ISC effectively (Đukić & Vuletić, 2022). However, inadequate infrastructure or tools can hinder employees' ability to implement security policies effectively.

The risk and response factors dimension received a lower perception score than other dimensions. The study shows that only 41.8% of respondents rate risk and response factors positively, while 58.2% rate them poorly. This suggests that many employees feel the organization's incident response system is not optimal. An organization must have clear procedures for handling security incidents, including effective reporting systems and teams prepared to respond to emerging threats.

Another significant factor is change management, which was rated positively by only 38.2% of respondents, while 61.8% rated it poorly. Change management ensures that information security policies and systems can adapt to technological advancements and regulatory changes. Without an effective change management strategy, security policies may become outdated and ineffective against new threats (Burton, 2024). Therefore, the hospital must develop a dynamic change management strategy, involving employees in all security-related changes.

Lastly, the information security policies dimension received the lowest perception score. Only 33.4% of respondents rated security policies positively, while 66.6% rated them poorly. This reflects a widespread sense that the hospital’s security policies are unclear or difficult to implement. Poorly implemented policies lead to uncertainty in day-to-day security practices (Chaisiri & Ko, 2016). The hospital must ensure that security policies are not only formally established but also communicated clearly to all employees, with robust monitoring mechanisms in place.

**3. The Influence of ISC on ISA**

The results from simple linear regression analysis, as shown in Table 17, reveal that Information Security Culture (ISC) has a significant impact on Information Security Awareness (ISA), with a regression coefficient (B) of 0.140, t-value of 2.106, and a significance level of 0.036. This suggests that improvements in ISC at the hospital contribute to a heightened awareness of information security among employees.

Further support for this finding comes from Table 16, which shows the relationship between ISC and ISA through cross-tabulation. The data indicates that 62.6% of respondents with good ISC also have good ISA, while only 37.4% of respondents with good ISC exhibit poor ISA. Conversely, among those with poor ISC, the majority (51.4%) also have poor ISA. This highlights that a strong information

security culture in the workplace is likely to enhance individual awareness of information security risks and importance.

A good ISC creates a work environment where security policies, norms, and habits are integrated into daily activities (Da Veiga, 2021; Ejigu et al., 2024). When an organization establishes a strong ISC, employees' awareness of information security threats and risks tends to improve. In contrast, a weak ISC often results in employees being less aware of the risks associated with mishandling information (Pankajakshan & Maheshwari Bangur, 2024).

This study's findings align with previous research, which emphasizes the positive effect of culturally sensitive information security frameworks (ISC) on enhancing ISA among system users. A study in Saudi Arabia showed that adapting security frameworks to the local culture significantly improved ISA levels, which were previously low, by fostering greater participation and understanding of the security risks in the workplace. Implementing ISC tailored to the local cultural context effectively changes users' behaviors and perceptions, thereby strengthening the overall information security system (Alkahtani, 2019).

**4. The Most Influential Factors on ISC**

The results of multiple linear regression analysis indicate that intrinsic factors have a more dominant influence on Information Security Culture (ISC) compared to extrinsic factors. The regression coefficient for intrinsic factors is 0.482, with a significance level of 0.000, indicating a highly significant impact on ISC. In contrast, extrinsic factors have a regression coefficient of 0.025 with a significance level of 0.707, suggesting that their influence on ISC at Stella Maris Hospital is not significant.

These findings suggest that knowledge, compliance with security policies, security behavior, and awareness of information security issues play a more crucial role in the success of ISC than management support, security policies, or other external environmental factors. In other words, the culture of information security is more shaped by how individuals understand, internalize, and apply information security principles in their daily work activities, rather than by structural factors like policies and regulations.

One key reason intrinsic factors have a greater impact is that an individual's understanding and compliance with information security policies directly affect the implementation of security culture in the workplace (Da Veiga, 2021; Prasetyo et al., 2023). An employee who is well-informed about information security risks and disciplined in following rules will be more vigilant in protecting patient data, using strong passwords, and adhering to security procedures. On the other hand, even if the hospital has stringent security policies and strong management support, if individuals lack awareness and compliance, these policies are difficult to enforce effectively.

This highlights that while extrinsic factors such as policies and supporting infrastructure play a role in shaping ISC, their success is largely dependent on the readiness and awareness of individuals to implement those policies. Relying solely on regulations and organizational support without sufficient understanding and discipline from employees will hinder the optimal development of an information security culture. Therefore, more effort is needed to strengthen intrinsic factors through strategies such as enhancing training and education programs on information security, increasing employee awareness through internal campaigns, and implementing reward and punishment systems to ensure compliance with information security policies (Ejigu et al., 2024; Heyasat et al., 2023).

## CONCLUSION

Based on the research conducted at Stella Maris Hospital in 2024 regarding the influence of intrinsic and extrinsic factors on ISC, as well as the impact of ISC on ISA, it can be concluded that intrinsic factors significantly influence the information security culture at Stella Maris Hospital Makassar, with a regression coefficient of 0.493, highlighting the importance of individual awareness, compliance, and motivation. Extrinsic factors also affect the culture, though their impact is smaller (regression coefficient 0.230), with management support, policies, training, and infrastructure playing

key roles. Additionally, a stronger information security culture positively impacts information security awareness (regression coefficient 0.140). In the multiple linear regression analysis, intrinsic factors were found to be the dominant influence (coefficient 0.482, sig = 0.000), while extrinsic factors had a minimal, non-significant effect (coefficient 0.025, sig = 0.707).

## CONFLICT OF INTEREST STATEMENT

The author declares that there is no conflict of interest in the implementation and reporting of this research. This research was conducted independently without any influence or intervention from any party that could affect the objectivity of the research results.

The authors have no financial, professional, or personal relationships that could influence or be perceived to influence the objectivity of this research. All data collected and analyzed in this study were treated confidentially and anonymously, in accordance with approved research ethics protocols.

The authors are committed to maintaining scientific integrity and transparency throughout the research process and reporting of results. Any potential conflicts of interest that may have arisen during the research process have been openly disclosed and handled in accordance with applicable research ethics standards.

## REFERENCES

Ait El Hadj, M., Khoumsi, A., Benkaouz, Y., & Erradi, M. (2019). Efficient security policy management using suspicious rules through access log analysis. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11704 LNCS*(September), 250–266. https://doi.org/10.1007/978-3-030-31277-0_16

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Akhsan, L., & Pendrian, O. (2024). Pengaruh Budaya Organisasi dan Motivasi Kerja Terhadap Kinerja Karyawan di Era Industri 4.0. *Journal of Economics and Business UBS*, *13*(1). https://doi.org/10.61994/equivalent.v2i2.627

Aldulaimi, S. H., Abdeldayem, M., Abu-Alsondos, I. A., Almazaydeh, L., Alnajjar, I. A., & Mushtaha, A. S. (2024). Robust Information Security for Strengthening HR in Organizations. *2nd International Conference on Cyber Resilience, ICCR 2024*, *February*, 1–5. https://doi.org/10.1109/ICCR61006.2024.10533019

Alkahtani, H. (2019). *Raising the information security awareness level in Saudi Arabian organizations through an effective , culturally aware information security framework Raising the Information Security Awareness Level in Saudi Arabian Organizations Through an Effective Cul*. Loughborough University.

Burton, S. L. (2024). Securing Tomorrow: Synergizing Change Management and Cybersecurity in the Digital Era. *HOLISTICA – Journal of Business and Public Administration*, *15*(1), 1–20. https://doi.org/10.2478/hjbpa-2024-0001

Chaisiri, S., & Ko, R. K. L. (2016). From reactionary to proactive security: Context-aware security policy management and optimization under uncertainty. *Proceedings - 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 10th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Symposium on Parallel and Distributed Proce*, 535–543. https://doi.org/10.1109/TrustCom.2016.0107

Collier, H., Morton, C., Alharthi, D., & Kleiner, J. (2023). Cultural Influences on Information Security. *European Conference on Information Warfare and Security, ECCWS*, *2023-June*(2018), 143–150. https://doi.org/10.34190/eccws.22.1.1127

Da Veiga, A. (2021). Achieving a Security Culture. *Research Anthology on Business Aspects of Cybersecurity*, 233–261. https://doi.org/10.4018/978-1-6684-3698-1.ch011

Dafid, & Dorie. (2020). Metode MCDA Untuk Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *7*(1), 11–20. https://doi.org/10.35957/jatisi.v7i1.296

Darmasaputra Leksono, F., Siagian, H., & Josowanto Oei, S. (2020). The Effects of Top Management Commitment on Operational Performance Through the Use of Information Technology and Supply Chain Management Practices. *SHS Web of Conferences*, *76*, 01009. https://doi.org/10.1051/shsconf/20207601009

Đukić, A., & Vuletić, D. (2022). Basics of information security culture in the organization. *Bezbednost, Beograd*, *64*(3), 140–154. https://doi.org/10.5937/bezbednost2203140d

Ejigu, K., Siponen, M., & Muluneh, T. (2024). Impact of Organizational Culture on Information Security Policy Compliance. *SINET: Ethiopian Journal of Science*, *47*(1), 17–32. https://doi.org/10.4314/sinet.v47i1.2

Heyasat, H., Mubarak, S., & Evans, N. (2023). *Security Culture and Security Education, Training and Awareness (SETA) Influencing Information Security Management BT - Proceedings of the Second International Conference on Innovations in Computing Research (ICR'23)* (K. Daimi & A. Al Sadoon (eds.); pp. 332–343). Springer Nature Switzerland.

Jylhä, V., Mikkonen, S., Saranto, K., & Bates, D. W. (2017). The impact of information culture on patient safety outcomes: Development of a structural equation model. *Methods of Information in Medicine*, *56*(MethodsOpen), e30–e38. https://doi.org/10.3414/ME16-01-0075

Kamarulzaman, M. S., Shuhidan, S. M., & Wahid, K. A. (2022). *The Moderating Role of Information Security Behaviour (ISB) on the Relationship between Digital Literacy (DL) and Information Security Culture (ISC): A Proposed Research Framework*. *Dl*, 35. https://doi.org/10.3390/proceedings2022082035

Mikuletič, S., Vrhovec, S., Skela-Savič, B., & Žvanut, B. (2024). Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees. *Computers and Security*, *136*(April 2023). https://doi.org/10.1016/j.cose.2023.103489

Munir, R. A., Talib, S., Nuha, N., Molok, A., Ridzuan Ahmad, M., & Furnell, S. (2015). *Factors Influencing Top Management Engagement in Information Security*. https://ssrn.com/abstract=4648851

Nurillah, R. A., & Trihandoyo, A. (2024). Analisis Faktor-Faktor Keamanan Informasi Perusahaan Dalam Penerapan Bring Your Own Device (BYOD). *IKRA-ITH Informatika : Jurnal Komputer Dan Informatika*, *8*(2), 136–145. https://doi.org/10.37817/ikraith-informatika.v8i2.2973

Pankajakshan, J., & Maheshwari Bangur, R. (2024). Employee Awareness and Attitudes Towards Cybersecurity Technologies. *Journal of Advances and Scholarly Researches in Allied Education*, *21*(5), 113–120. www.ignited.in

Prasetyo, N. A., Wahid, A., & Azim, F. (2023). Assessing Information Security Culture from an Individual's Viewpoint: A Quantitative Measurement Approach. *INSIDE-Jurnal Sistem Informatika Cerdas*, *1*(1), 1–8.

Putu, I., Subagya Putra, A., Komang, I., & Hendrawan, R. (2024). Analisis Manajemen Risiko SIMRS pada Rumah Sakit Ganesha Menggunakan ISO 31000 Risk Management Analysis of SIMRS at Ganesha Hospital using ISO 31000. *Jurnal Teknologi Dan Informasi*, *14*(1), 1. https://doi.org/10.34010/jati.v14i1

Raihan. (2017). Metodologi Penelitian. In *Metodologi Penelitian* (p. 85). Universitas Islam Jakarta.

Triono, T., Agustang, A., Muhammad Idkhan, A., & Rifdan, R. (2021). Motivasi Kerja Pegawai Dalam Pelayanan Publik. *JISIP (Jurnal Ilmu Sosial Dan Pendidikan)*, *5*(4), 1627–1631. https://doi.org/10.58258/jisip.v5i4.2583

Yusuf, A. M. (2014). *Metode Penelitian Kuantitatif, Kualitatif dan Penelitian Gabungan* (Pertama). Kencana.

.