Indonesian Journal of Electrical Engineering and Computer Science
Vol. 22, No. 1, April 2021, pp. 469~475
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v22.i1.pp469-475

Measuring information security policy compliance: content validity of questionnaire

Angraini[1], Rose Alinda Alias[2], Okfalisa[3]
[1]School of Computing, Faculty Engineering, Universiti Teknologi Malaysia, Johor, Malaysia
[2]Department of Information System, Azman Hashim International Business School, Universiti Teknologi Malaysia, Johor, Malaysia
[3]Department of Informatics Engineering, Faculty Science and Technology, Universitas Islam Negeri Sultan Syarif Kasim, Riau, Indonesia
[1]Department of Information System, Faculty Science and Technology, Universitas Islam Negeri Sultan Syarif Kasim, Riau, Indonesia

Article Info

Article history:

Received Mar 15, 2020
Revised Dec 5, 2020
Accepted Jan 11, 2021

Keywords:

Compliance
Content validity
Information security policy
Instruments
Questionnaire

ABSTRACT

Instruments used to measure compliance with information security policies have been developed by many researchers before, but only a few have conducted validity tests per item, especially for variables selected based on qualitative research. This study aims to validate the questionnaire will be used to measure user compliance with policies of information security. This study began by designing a questionnaire and conducting content validation using content ratio validation (CVR) and content index validation (CVI). As many as eight experts from the university assessed the items given. The results of 72 items submitted a questionnaire, as many as 22 items eliminated, and only 50 items that have CVR and CVI values above 0.75. Also, Kappa statistical calculations show that items have excellent reliability among assessors at the item level. This study revealed that this instrument had obtained an appropriate level of validity to measure compliance with information security policies.

Corresponding Author:

Angraini
Department of Information System
Faculty Science and Technology
Universitas Islam Negeri Sultan Syarif Kasim
Pekanbaru, Riau, Indonesia
Email: angraini@uin-suska.ac.id.com

1. INTRODUCTION

Compliance is one of the critical aspects of information security policy in an organization. Since 2010, employees' compliance with information security has been attracting much interest due to the increase in organizational threats [1]. Therefore, technical and IS security policies are needed to overcome these problems [2]. Besides, employees are often the weakest connection in an organization, and they are also a source of high strength in developing effective and efficient defences. Information technology is proficient and cannot guarantee the safety of the environment or assets. Therefore, it requires human resources [3]. Organizations attempt to encourage employees to comply with information security policies to avoid damages resulting from policy violations.

Further research is needed to determine the influencing social and behavioural factors as an effort to build a substantial theoretical foundation [4]. Organizations create policies to ensure the security of their information; therefore, their employees need to comply with these policies [5]. Data were obtained from tertiary institutions to ascertain their compliance with information security policies that are poorly checked and without validation. The result showed that universities need to focus on developing a comprehensive information security policy as an effort to securing students' data [6].

Compliance with these security policies in higher educational institutions is relatively under-examined with less validated evidence [6]. Moody [7] conducted research using 32 theories to determine the factors responsible for users' ability to comply with information security policies. However, the questionnaire's data showed that previous studies failed to analyze the content validation they utilized. This study, therefore, aims to validate the variables previously used, while modifying the items used by the universities. This research consists of several sections, namely, introduction, literature review, research methodology, findings, discussion, and conclusions. It starts by explaining the background of the research and then proceeds to review some of the previous studies. The process associated with its conduction is explained in the methodology followed by research findings, discussions and conclusions.

2. LITERATURE REVIEW

2.1. Information security policy compliance

Information security policies are used to create IT security related-rules for organizations to solve specific problems and address individual systems [8]. It includes policies on the distribution of information, maintenance, and granting access to rights, as well as the accurate ways to operate a computer system. Therefore, a policy is defined as a guide, standard, or procedure used to shape IT users' security behavior [9-10]. Individual and organizational factors need to evaluated compliance with information security policies [11]. Metalidou [12] classified five human factors, namely, motivation, awareness, belief, behaviour, incapable of using technology. Some researchers have carried out studies to determine the factors that influence users' ability to comply with information security policy. Pahnila [13], proposed a model to identify the factors responsible for employees' inability to comply with information security policies. The results from the empirical study showed that employees' attitudes, normative beliefs, and habits have a significant impact on the user's intention to comply with the IS security policy. Other factors, such as subjective norms, self-efficacy, and perceived severity of sanctions, were also found by Sommestad [14]. These variables were developed as an extended theory of planned behaviour used to explain compliance with information security policies [14]. Moody [7] carried out comprehensive research used to develop a unified model of information security using the eleven theory.

2.2. Content validity

Studies on users' involvement in information security policies need to be validated to ascertain the wrongly measured items. Although the items used are duplicates from previous studies, the research context's differences can affect its validation [15]. Content validation, based on a demonstration, shows that the test is representative of all items in the domain of interest. Fitzgerald [16] described six different views on content validity, including four that focus on test items, namely the clarity of the content domain, the relevance of the test, sampling the adequacy of the test content, and the technical quality of the items. The techniques used by experts to obtain quantitative results are content validity ratio (CVR) and content validity index (CVI) [17]. CVR is a statistical technique used to determine the validity of each instrument item, as assessed by a panel of content experts. CVI provides numerical values for the overall average CVR of all items included in the instrument. Both techniques are used to provide a quantitative measurement of the simulation evaluation instruments for researchers and consumers [18]. The items selected based on CVR values are considered acceptable, assuming the value is 0.78 or higher [19]. When an item fails to reach the threshold, it is eliminated from the final instrument. CVR is an item statistic used to reject or store individual items, and it is internationally recognized as a method for building content validity [20]. CVI is the mean CVR for all items included in the final instrument [19]. Therefore, the level of agreement between appraisers is determined by calculating the kappa value, which is also used to measure the level of intraexaminer and interexaminer agreement. Furthermore, several experts have developed guidelines to determine the level of practical, substantive, or clinical importance [21, 22]. The Guidelines developed by Cicchetti and Sparrow [21] are similar to Fleiss's [22] model and also represents a simplified version of Landis and Koch (1977). The guidelines stated that, when the reliability coefficient is below 0.40, between 0.40 and 0.59, 0.60 and 0.74, and between 0.75 and 1.00, the levels of significance is bad, fair, good and perfect, respectively [23].

3. RESEARCH METHOD

Content validity is one of the stages used to validate well-prepared questionnaire items before it is distributed to respondents. This stage starts with defining the questionnaire items, selecting experts, and calculating the i-CVI values needed to eliminate the invalid ones. This process, adapted from Almanasreh [24] is used to validate the questionnaire item. The detailed process of content validity is shown in Figure 1.

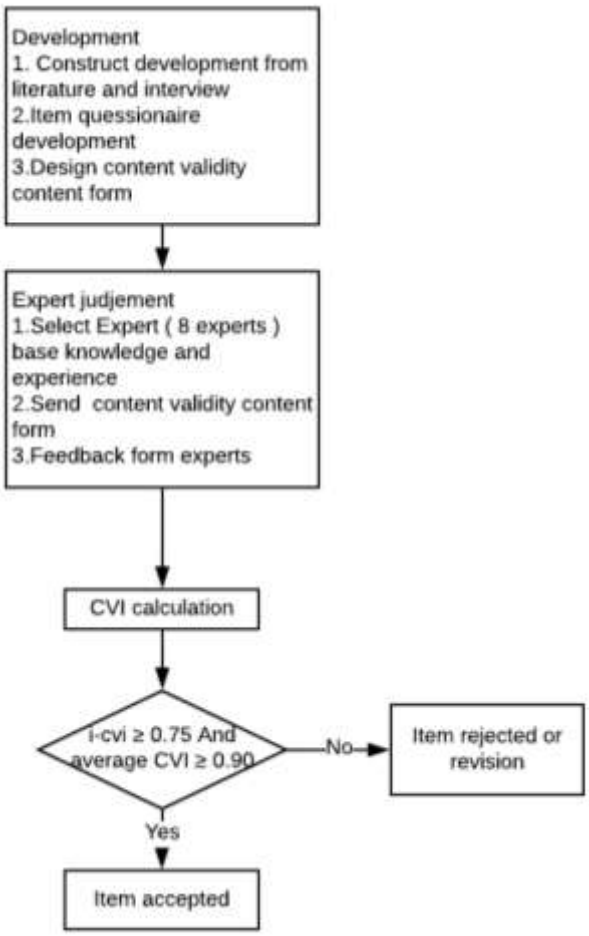

Figure 1. Content validity process

Questionnaire items were obtained from preliminary studies in the form of interviews and literature reviews, with in-depth interviews conducted with the head of IT at the university. This study comprises of eight variables, with a total of 72 items used to validate the questionnaire by an expert. Validation is usually carried out by seven or more experts to determine the item that reflects the attributes of the variable studied [18]. As many as eight experts participated in this study, with the majority from universities. Table 1 shows the details of the participants.

Table 1. Details of expert

Expert	Organization	Designation	Expertise
1	Public University	IT chairman	IT management
2	Public University	IT chairman	Computer networking
3	Public University	Professor	IT security
4	Private University	IT chairman	IS management
5	Private University	Lecture	Management security IT
6	Private University	Senior Employee	IT security
7	Government	Government Employee	Computer networking
8	Private Institute	Senior Lecture	Management security IT

The experts involved in this research are stakeholders representing policymakers and academics in the field of data security and IT management. The data collection process is carried out by directly providing form content validation and via email. This stage was carried out to determine the assessment provided by experts to strengthen the validity of parameters and indicators in the questionnaire. The experts assessed the form with the following scale items, namely not needed, need to be revised, relevant, and very relevant. Furthermore, this research uses the calculation of CVR and CVI from Lawshe. CVR was calculated based on the "important" rating of each expert, as shown in (1).

CVR Calculation [17]:

$$CVR = \frac{N_{e-N/2}}{N/2} \quad (1)$$

Ne = number of experts indicating "important" ranking per item
N = total number of experts.

Based on the calculation results, when the CVR value is above 0.75 for eight experts, then the items are acceptable and can be used in the instrument. However, when the value is less than 0.75, the items from the questionnaire are deleted (Lawshe). CVI is the average of the items and represents the content validity of all instruments. There are two types of CVI, namely iCVI (item level) and sCVI (scale-level). In (2) shows the formula used to calculate i-CVI.

iCVI formula [17]:

$$iCVI = n_a/N \quad (2)$$

iCVI is the Item-Content Validity Index, and n_a is the number of experts with values of 3 (relevant) and 4 (very relevant). Reliability assessment of the questionnaire items were statistically measured to determine the agreements between several raters using Kappa Fleiss. The results are interpreted according to those used by Landis and Koch (1977), as shown in Table 2. This interpretation table used to determine the items to be used based on kappa values. Items used if the kappa value is at least 0.5 or with a moderate agreement

Table 2. The interpretation kappa value

kappa	Interpretation
< 0	Poor agreement
0.01 – 0.20	Slight agreement
0.21 – 0.40	Fair agreement
0.41 – 0.60	Moderate agreement
0.61 – 0.80	Substantial agreement
0.81 – 1.00	Almost perfect agreement

4. RESULTS AND ANALYSIS

This study validated 72 questionnaire items in eight variables, with each consisting of a different number of question items. During the calculation process, most of the items submitted had invalid values and were eliminated. The result left 50 items with an i-CVI and CVR value greater than 0.75 and a kappa value above 0.5. Twenty-three items were removed because they had values below the specified standard. Table 3 shows the details of the calculation of i-CVI, CVR, and kappa values.

Table 3 shows the number of fixed items used while eliminating the 20 items not mentioned in Table 2. In the first variable, related to Information Security Policy Compliance (ISPC), there are six items. However, only four met the standards, and an item has perfect agreement from eight experts. Out of the 12 organizational commitment variable (OC) submitted, only five were approved. Organizational culture (OL) and reward (RW) variables are the overall items with CVR value above 0.75. Five experts approved only two items on the OL variable. The leadership variable (LD) removed five items, and two had a CVR value of 0.75. However, an item had a kappa value of 0.53due to its significance, which is above 0.5. All items of user awareness (AW), moral belief (MB), and intention variables were used because the i-CVI and CVR values meet the standard. Finally, the habit variable eliminated four items, and six items were used. From 50 selected items, 46% had a perfect agreement presentation, 48% were substantial, and 6% moderate. However, the minimum agreement used in this study is moderate.

Table 3. Calculation of content validity

Construct	Item Code	NA	CVR	i-CVI	Kappa value	
Information security policy compliance (ISPC)	ISPC 1	8	1	1	1	Perfect Agreement
	ISPC 2	8	1	1	0.75	Substantial Agreement
	ISPC 3	8	1	1	0.75	Substantial Agreement
	ISPC 4	8	1	1	0.75	Substantial Agreement
Organization Commitment	OC 2	8	1	1	0.75	Substantial Agreement
	OC 3	8	1	1	1	Perfect Agreement
	OC 5	7	0.75	0.875	0.75	Substantial Agreement
	OC 6	8	1	1	0.75	Substantial Agreement
	OC 12	7	0.75	0.875	0.75	Substantial Agreement
Organization culture	OL 1	8	1	1	1	Perfect Agreement
	OL 2	8	1	1	0.57	Moderate Agreement
	OL 3	8	1	1	0.57	Moderate Agreement
	OL 4	8	1	1	0.75	Substantial Agreement
	OL 5	8	1	1	1	Perfect Agreement
Reward	RW 1	8	1	1	1	Perfect Agreement
	RW 2	8	1	1	0.75	Substantial Agreement
	RW 3	7	1	1	0.75	Substantial Agreement
	RW 4	7	0.75	0.875	0.75	Substantial Agreement
	RW 5	8	1	1	0.75	Substantial Agreement
	RW 6	7	0.75	0.875	0.75	Substantial Agreement
Leadership	LD 1	7	0.75	0.875	0.53	Moderate Agreement
	LD 2	8	1	1	0.75	Substantial Agreement
	LD 3	8	1	1	1	Perfect Agreement
	LD 8	8	1	1	1	Perfect Agreement
	LD 10	7	0.75	0.875	0.75	Substantial Agreement
	LD 11	8	1	1	1	Perfect Agreement
User Awareness	AW 1	8	1	1	1	Perfect Agreement
	AW 2	8	1	1	1	Perfect Agreement
	AW 3	8	1	1	1	Perfect Agreement
	AW 4	8	1	1	0.75	Substantial Agreement
	AW 5	8	1	1	0.75	Substantial Agreement
	AW 6	8	1	1	1	Perfect Agreement
Moral Belief	MB 1	8	1	1	1	Perfect Agreement
	MB 2	8	1	1	0.75	Substantial Agreement
	MB 3	8	1	1	0.75	Substantial Agreement
	MB 4	8	1	1	1	Perfect Agreement
	MB 5	8	1	1	1	Perfect Agreement
	MB 6	7	0.75	0.875	0.75	Substantial Agreement
Intention	IN 1	8	1	1	1	Perfect Agreement
	IN 2	7	0.75	0.875	0.75	Substantial Agreement
	IN 3	8	1	1	1	Perfect Agreement
	IN 4	8	1	1	0.75	Substantial Agreement
	IN 5	8	1	1	1	Perfect Agreement
	IN 6	8	1	1	1	Perfect Agreement
Habit	HA 1	8	1	1	1	Perfect Agreement
	HA 2	8	1	1	0.75	Substantial Agreement
	HA 4	8	1	1	1	Perfect Agreement
	HA 7	8	1	1	1	Perfect Agreement
	HA 9	8	1	1	1	Perfect Agreement
	HA 10	8	1	1	0.75	Substantial Agreement

5. DISCUSSION

The questionnaire developed in this study consisted of nine constructs. However, after calculating content validity, some items were eliminated with organizational commitment the highest. The items used in the organizational commitment were previously used by Safa [3], Ifinedo [25], Gerber [26], and Hewart [27] with the modified organizational commitment theory developed by Mowday [28]. Almost half of the items proposed were considered unnecessary by the expert due to the varying organizations. Previous studies were not specific to any university, and it was possible to obtain different results. The next variable is the

organizational culture which was chosen based on the results of an interview with one of the university leaders, and because it was also used by [29-33].

The organization culture is considered one of the factors that influence compliance due to cultural differences in each region. This variable was followed by leadership, which is rarely used to determine compliance with information security policies. The items used in this questionnaire was adapted from a study carried out by Ogbonna [34]. This variable was also chosen by Manga [35] to determine the factors that influence an employee's decline in information security policies. Reward, user awareness, moral belief, and behaviour intention variables widely used with high validation.

The last variable used in this study is a Habit. This variable was used by Moody [7], to develop a sophisticated model of compliance with information security policies. Question items adopted from psychological theories developed by Verplankan [36]. The statements items on average habits were less than others. Therefore, as many as six items eliminated

6. CONCLUSION

This research presents a process for developing and validating items used to measure user compliance with university information security policies. Questionnaires were developed based on literature reviews and interviews. In general, the stages in this study started with a comprehensive literature review, item creation, and expert assessment of the item. This was followed by validating all instruments and items evaluated by eight experts by calculating the CVR and CVI. Out of 72 items, the content validity process identified nine parameters, namely Information security policy compliance, organizational commitment, culture, reward, leadership, user awareness, moral beliefs, intention, and Habit. From the expert judgment, 50 items were elected to have good content validity with an iCVI value higher than 0.75. Furthermore, a total of 22 items had ICVI that are smaller than 0.75. Therefore, they were rejected. The overall SCVI of the instrument is equal to 0.9 (SCVI/Ave). Besides, Kappa statistical calculations showed that the appraisal tool has excellent interrater with a reliability above 0.74. This research was conducted with a separate expert. Therefore, there was no in-depth discussion of validated items. The selection of more experts and discussion groups tend to produce a correct item, with expert judgment capable of influencing the number of variables and questions. This study discloses that this instrument obtained an appropriate level of content validity and can be used to measure compliance with information security policies at universities.

REFERENCES

[1] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Policy As Antecedents of Employees' Security Engagement iQuality and Fairness of an Information Security Pn the Workplace: An Empirical Investigation," *Syst. Sci. (HICSS), 2010 43rd Hawaii Int. Conf.*, pp. 1-7, 2010.

[2] M. Siponen, M. Adam Mahmood, and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study," *Inf. Manag.*, vol. 51, no. 2, pp. 217-224, 2014, doi: 10.1016/j.im.2013.08.006.

[3] N. S. Safa and R. Von Solms, "An information security knowledge sharing model in organizations," *Comput. Human Behav.*, vol. 57, pp. 442-451, 2016, doi: 10.1016/j.chb.2015.12.037.

[4] J. Y. Han, Y. J. Kim, and H. Kim, "An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective," *Comput. Secur.*, vol. 66, no. 2017, pp. 52-65, 2017, doi: 10.1016/j.cose.2016.12.016.

[5] M. Nohlberg, "Why Humans are the Weakest Link," in *Social and Human Elements of Information Security : Emerging Trends*, p. 22, 2009, doi: 10.4018/978-1-60566-036-3.ch002.

[6] R. Ayyagari and J. Tyks, "Disaster at a University: A Case Study in Information Security," *J. Inf. Technol. Educ. Innov. Pract.*, vol. 11, pp. 85-96, 2012, doi: 10.28945/1569.

[7] G. D. Moody, M. Siponen, and S. Pahnila, "Toward a Unified Model of Information Security Policy Compliance," *MIS Q.*, vol. 42, no. 1, pp. 285-311, 2018, doi: 10.25300/MISQ%2F2018%2F13853.

[8] NIST, "Glossary of Key Information Security Terms [NISTIR 7298 Rev 2]," 2013, doi: 10.6028/NIST.IR.7298r3.

[9] W. A. Al-Hamdani and W. D. Dixie, "Information security policy in small education organization," in *2009 Information Security Curriculum Development Conference on-InfoSecCD '09*, p. 72, 2009, doi: 10.1145/1940976.1940991.

[10] M. Chan, I. Woon, and A. Kankanhalli, "Perceptions of Information Security at the Workplace : Linking Information Security Climate to Compliant Behavior Mark Chan National University of Singapore Irene Woon School of Computing, National University of Singapore Atreyi Kankanhalli School of Com," *J. Inf. Priv. Secur.*, vol. 1, no. 3, pp. 18-41, 2005, doi: 10.1080/15536548.2005.10855772.

[11] A. J. T. Chang, C. Y. Wu, and H. W. Liu, "The effects of job satisfaction and organization commitment on information security policy adoption and compliance," in *2012 IEEE 6th International Conference on Management of Innovation and Technology, ICMIT 2012*, pp. 442-446, 2012, doi: 10.1109/ICMIT.2012.6225846.

[12] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, and G. Giannakopoulos, "The Human Factor of Information Security: Unintentional Damage Perspective," *Procedia-Soc. Behav. Sci.*, vol. 147, pp. 424-428, 2014,

doi: 10.1016/j.sbspro.2014.07.133.
[13] S. Pahnila, M. Siponen, and A. Mahmood, "Employees' behavior towards IS security policy compliance," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 1-10, 2007, doi: 10.1109/HICSS.2007.206.
[14] T. Sommestad, J. Hallberg, K. Lundholm, and J. Bengtsson, "Variables influencing information security policy compliance: A systematic review of quantitative studies," *Inf. Manag. Comput. Secur.*, vol. 22, no. 1, pp. 42-75, 2014, doi: 10.1108/IMCS-08-2012-0045.
[15] D. W. Straub, "Validating Instruments in MIS Linking MiS Research," *MIS Q.*, no. June 1986, pp. 103-118, 1989.
[16] G. Fitzgerald and R. Hirschheim, "Information Systems Research Methodology : an Introduction To the Debate," https://www.researchgate.net/publication/240048857, pp. 1-7, 1985.
[17] C. H. Lawshe, "A Quantitative Approach To Content Validity," *Pers. Psychol.*, vol. 28, no. 4, pp. 563-575, 1975, doi: 10.1111/j.1744-6570.1975.tb01393.x.
[18] G. E. Gilbert and S. Prion, "Making Sense of Methods and Measurement : Lawshe ' s Content Validity Index," *Clin. Simul. Nurs.*, vol. 12, no. 12, pp. 530-531, 2016, doi: 10.1016/j.ecns.2016.08.002.
[19] D. F. Polit, T. Beck, and S. V Owen, "Focus on Research Methods Is the CVI an Acceptable Indicator of Content Validity ? Appraisal and Recommendations," Volume 30 , Number 4; pp. 459-467, 2007.
[20] F. R. Wilson, W. Pan, and D. A. Schumsky, "Recalculation of the critical values for Lawshe's content validity ratio," *Meas. Eval. Couns. Dev.*, vol. 45, no. 3, pp. 197-210, 2012, doi: 10.1177%2F0748175612440286.
[21] D. V. Cicchetti, D. Shoinralter, and P. J. Tyrer, "The Effect of Number of Rating Scale Categories on Levels of Interrater Reliability: A Monte Carlo Investigation," *Appl. Psychol. Meas.*, vol. 9, no. 1, pp. 31-36, 1985.
[22] J. L. Fleiss, B. Levin, and M. C. Paik, "The Measurement of Interrater Agreement," *Stat. Methods Rates Proportions*, pp. 598-626, 2004, doi: 10.1177%2F014662168500900103.
[23] D. V Cicchetti, "Guidelines, Criteria, and Rules of Thumb for Evaluating Normed and standardized assessment instruments in psychology.," *Psychol. Assess.*, vol. 6, no. 4, pp. 284-290, 1994, https://psycnet.apa.org/, doi: 10.1037/1040-3590.6.4.284.
[24] E. Almanasreh, R. Moles, and T. F. Chen, "Evaluation of methods used for estimating content validity," *Research in Social and Administrative Pharmacy*, vol. 15, no. 2, pp. 214-221, 2019, doi: 10.1016/j.sapharm.2018.03.066.
[25] P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," *Inf. Manag.*, vol. 51, no. 1, pp. 69-79, 2014, doi: 10.1016/j.im.2013.10.001.
[26] N. Gerber, R. McDermott, M. Volkamer, and J. Vogt, "Understanding information security compliance - Why goal setting and rewards might be a bad idea," *Int. Symp. Hum. Asp. Inf. Secur. Assur. (HAISA 2016)*, vol. 10., no. Haisa, pp. 145-155, 2016, doi: 10.5445/IR%2F1000081976.
[27] H. Stewart and J. Jürjens, "Information security management and the human aspect in organizations," *Inf. Comput. Secur.*, vol. 25, no. 5, pp. 494-534, 2017, doi: 10.1108/ICS-07-2016-0054.
[28] R. T. Mowday, R. M. Steers, and L. W. Porter, "The Masurement of Organizational Commitment : A Progress Report," *J. Vocat. Behav.*, vol. 14, no. 2, pp. 224–247, 1979, doi: 10.1016/0001-8791(79)90072-1.
[29] T. Arage, F. Belanger, and T. Beshah, "Influence of National Culture on Employees' Compliance with Information Systems Security (ISS) Policies: Towards ISS Culture in Ethiopian Companies," in *AMCIS 2015 Proceedings*, no. 2010, pp. 1-7, 2015.
[30] T. Sommestad, "Social Groupings and Information Security Obedience Within Organizations," *Int. Fed. Inf. Process.*, pp. 325-338, 2015, doi: 10.1007/978-3-319-18467-8_22.
[31] K. A. Alshare, P. L. Lane, and M. R. Lane, "Information security policy compliance: a higher education case study," *Inf. Comput. Secur.*, vol. 26, no. 1, pp. 91-108, 2018, doi: 10.1108/ICS-09-2016-0073.
[32] A. Al Hogail, "Cultivating and assessing an organizational information security culture; an empirical study," *Int. J. Secur. its Appl.*, vol. 9, no. 7, pp. 163-178, 2015, doi: 10.14257/IJSIA.2015.9.7.15.
[33] A. Martins and J. Eloff, "Information Security Culture," pp. 191-201, 2002, doi: 10.1007/978-0-387-35586-3_16.
[34] E. Ogbonna and L. C. Harris, "Leadership style, organizational culture and performance: Empirical evidence from UK companies," *Int. J. Hum. Resour. Manag.*, vol. 11, no. 4, pp. 766-788, 2000, doi: 10.1080/09585190050075114.
[35] J. Manga and E. Ayaburi, "Think and Act Positively : A Motivational Organizational Citizenship Behavior Approach Towards Information Security Policy Compliance," pp. 1-5, 2019.
[36] B. Verplanken and S. Orbell, "Reflections on Past Behavior: A Self-Report Index of Habit Strength," *J. Appl. Soc. Psychol.*, vol. 33, no. 6, pp. 1313-1330, 2003, https://psycnet.apa.org/, doi: 10.1111/j.1559-1816.2003.tb01951.x.