# A Model of Information Security Policy Compliance for Public Universities: A Conceptual Model

Angraini[1,4(✉)], Rose Alinda Alias[2], and Okfalisa[3]

[1] School of Computing, Faculty Engineering, Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia
Angraini@uin-suska.ac.id
[2] Department of Information System, Azman Hashim International Business School, Universiti Teknologi Malaysia, 81310 Skudai, Johor, Malaysia
[3] Department of Informatics Engineering, Faculty Science and Technology, Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru, Riau, Indonesia
[4] Department of Information Engineering, Faculty Science and Technology, Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru, Riau, Indonesia

**Abstract.** The university is an organization that manages much public information, and therefore, information security policies are developed to ensure data security. However, during implementation still founded disobey behavior user and has an impact on data security. The previous research has been conducted to find influencing factor user comply with information security, although some model and theories still limited to implementation. There is a lack of researchers combine behavioral theory and organizational theory to develop models and previous model inadequate to universities that have unique characteristics. This study aims to explore and identify factors that influence information security compliance and continue to develop conceptual models for assessing information security policies. This conceptual model creates based on a systematic literature review and preliminary study. The results in the conceptual model found several variables, namely habits, attitudes, moral beliefs, self-efficacy from behavioral theories and human culture, commitment, rewards, costs can be used to evaluate user compliance with information security policies. Conceptual will be tested further to contribute to help universities to ensure and assess users to comply with information security policies.

**Keywords:** Information security · Security policy · Compliance · User behavior

## 1 Introduction

This study addresses the issue of compliance with information security policies such as individual frequently trespass policies [1]. Employees unrealized non-compliance with information security lead to related safety [2], generate security threat [3, 4], increase security risk [5]. A significant increase in incidents in recent years has reminded that to overcome the increasing threat, in addition to technical solutions, necessary to provide


F. Saeed et al. (Eds.): IRICT 2019, AISC 1073, pp. 810–818, 2020.
https://doi.org/10.1007/978-3-030-33582-3_76

an information security policy [4]. However, during implementation user tend to ignore that policy because they are unaware and realize importance comply with information security policy. This opinion is in line with the research conducted by Abed to find out how the intention to comply with the policy or intention to refuse [6]. Conceptual attempt to encourage employees to comply with information security policies when organizational damage resulting from information violations becomes serious. Therefore, necessary to develop a substantial theoretical foundation that concerns about a social issue and human behavior [2]. Management as policymaker needs to encourage user confidence in the ISP to employees in the organization to ensure and achieve information security objectives, although the organization is conscious of the obstacles in information security related to unskilled employees of security technology because of a lack of security knowledge [7]. Many empirical studies have been conducted to find out and explain the human factors that influence compliance with information security policies [1–8].

However, the discussion about the importance of the value of information has less discussed explicitly human factors like the source of unpredictable and uncontrolled vulnerability in information security because of changes in human behavior. Research on information security behavior has the opportunity to combine people, technology, and organizations. Understanding individual behavior will enhance positive behavior while reducing harmful behavior. Understanding human behavior will be able to improve adherence to policies by knowing the motivation, modification, and prevention [21]. Therefore, necessary to understand how to change people in organizations becoming allied security, instead of just being a security risk. The policy of information significance can influence the level of awareness and behavior of users towards information security [8].

Level of awareness and security behavior problem occurs because it is often encountered Information security conflicts with the efficiency of information systems such as active sharing of critical information resources, standardizing business processes, and downloading applications or components to complete specific tasks. Consequently, challenging for the user to comply with information security policies. Employees prefer to complete their work and follow their colleagues to not complying with their policies [9]. There are some compliance regulatory from industrial and government such as the Federal Information Security Management Act (FISMA), U.S. Intelligence Community (IC), DoD Information Assurance Certification and Accreditation Process (DIACAP), Homeland Security/Presidential Directives and National Institute of Standards Technology (NIST) 800-XX series [10]. Unfortunately, this standard not always applicable to the university. Difference requirement and limited resources make the university can adopt an international standard to its security policy [9–11]. Universities have amount information technology resources, and access is given to the public and increase the risk for universities [12]. An academic institution with weak policies in information security creates threats for university data [13]. Universities with ineffective systems in information security create risks for university data.

The university is an organization with various activities and type of users. It becomes a challenge for universities to ensure organizational information, which saved, processed, and disseminated with information technology. Security incidents caused

density, high dependence on the accuracy, integrity, and availability of technology-based information resources [27]. A well-known problem with information security is that it does not take into account user behavior and organization condition. The organization was more concerned about technical issues than the requirements of the organization or user habits that can have an impact on information security. Moreover, information security policy inefficiency because during implementation, not well-monitoring. Therefore, their need model to measure and evaluate the level of user comply with information security policy.

## 2 Literature Review

Information security policy is a document to ensure information security based on top management's vision related to key strategic business objectives within the scope of management goals and contains basic requirements. Information security policies contain rule, guidelines, and control to secure information asset [14]. Information security policies aim to provide management goals and support for information security [15]. Information security policy contained with Program Policy used to create an organization's IT security program, Issue-Specific Policies, and System-Specific Policies to address individual systems [16]. Security policies must continuously be reviewed and updated regularly by considering changes in circumstances, environment, changing needs in the business context, and identified risks [17]. Compliance with policies aims to ensure the application of organizational security standards [18]. Ross from the NIST lab conducted a study by performing a series of procedures to assess security controls and privacy controls used in federal information systems and organizations. Assessment procedures, carried out at various phases of the system development life cycle, are consistent with security and privacy controls using the NIST 800-53 standard [19]. Exactly the measuring instruments used can only be applied to organizations that have used these standards in the process of developing information security policies.

Sommestad added security awareness to developed a model of information security policy compliance. The results find other factors such as explanatory power and anticipated regret that have a significant effect While habit variables have a significant result to strengthen the model [20]. A different result was found by Moody [30] who combined eleven theories with building a unified model of information security policies compliance. His research found that habits can influence behavioral intentions to comply with information security policies. Information security behavior builds a relationship with people, technology, and organizations. Necessary for understanding individual behavior will enhance positive behavior while reducing harmful behavior. Understanding human behavior will be able to improve adherence to policies by knowing the motivation, modification, and prevention [21].

Vroom evaluated human behavior in safeguard organizational information and other valuable assets with audits and found that this method is not sufficient for testing human behavior on information security [22]. This interpretation contrasts with that of Kankanhalli who argue that Human factors, organizational factors can influence compliance with information security policies [23]. The significant impact of

organizational factors on the effectiveness of information security management implementation [24]. Research on this subject has been mostly restricted to limited comparisons of theory about human behavior.

Lowry [21] develops a model for compliance with information security policies using organizational control theory. The results of empirical studies conducted by scenarios for professional workers show that there are reactions that arise when an organization applies threats and controls. Responses that appear related to anger and hatred towards the organization but are fully compliant [25]. Feasible regulation from organization mismatched with national culture and organization culture. Because according to Alshare [26], organizational culture is a significant predictor for determining crime against information security policies [26]. Likewise, the research conducted by Arage [37], states that national culture has an impact on information security compliance. Another factor within the organization is user involvement and leadership, this potential was seen by Amankwa [38] in his research on Establishing information security policy compliance culture in organizations using the theory of organizational behavior and organization culture. However, differences in results found by Sommestad [36] investigated the relationship between individual intentions in social groups rather than the workplace and the effects of this group by using the theory of planned behavior and information security culture.

The results found that culture does not have a significant impact on behavioral intention because the culture of information security is a concept that is used and interpreted in many different ways. [36]. The similarly discovered by Gerber [32] Management involvement is more needed to ensure user compliance. Participation from top management will influence user behavior intentions towards information security policies compared to organizational culture (2016).

## 3 Conceptual Framework

This research aims to construct a conceptual model presenting perspective or a way to understand practical phenomena. Therefore, a model was developed that showed the relationship between factors that influence compliance with information security policies. This model is the initial model used to prepare more complex models. The development of this model expected will support research problem, identifying relevant factors, and then providing a relationship to map the problem frame. Figure 1 will describe a conceptual model of information security compliance.

This conceptual model consists of ten variables composed of independent, dependent, and mediating variables. The dependent variable is information security policy compliance. Independent variables include organizational commitment, organization culture, reward, perceived cost, self-efficacy, attitude, moral belief, and habit. Moreover, behavioral intention as a mediating variable. This variable choosing based on literature review, conceptual survey, and interview.

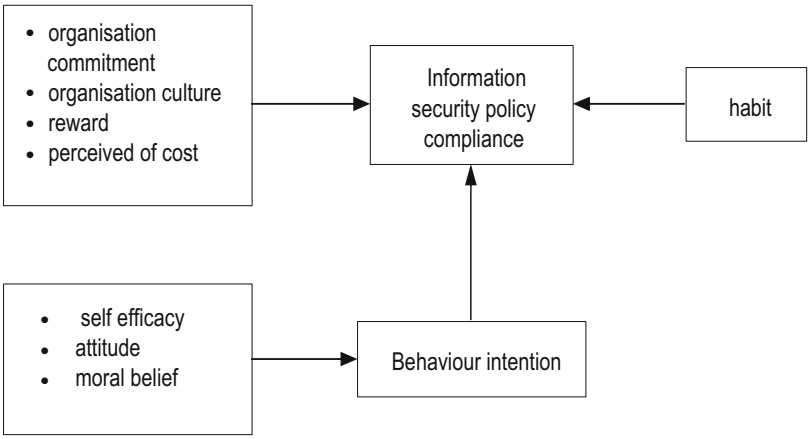


**Fig. 1.** Conceptual model of information security policy

The hypothesis for this study is as follows:

hypothesis 1. habit will influence a user to comply with information security policies
hypothesis 2. organizational commitment, organizational culture, reward, and perceived cost user comply with information security policies
hypothesis 3. behavioral intentions moderating self-efficacy, attitude, and moral belief affect users to comply with information security policy

Variable habits explain by interview can influence user behavior always to manage information security by an understanding of the pattern. According to the theory of interpersonal behavior, habit is behavior has become automatic due to continuous activity, and they conduct it attentively without instruction [29]. The assumption that habits are related to the complexity of ISS actions causes research to be conducted to examine the processes that lead employees to become non-compiler habits and determine how bad habits and noncompliance behavior can be changed [30]. The habit of transferring behavior can increase explanatory power became a reason to conduct further research about the relationship between habits and intentions [20]. Compliance with information security can be implemented entirely with the commitment of the organization. Commitments will improve the efforts and energy of individuals to support organizational policies. Safa study show a significant relationship between commitment and individual attitudes towards compliance with information security policies [31]. Organizational responsibility and commitment pretend an essential role in protecting information assets. Consequently, employees will realize that compliance with security policies is part of their work [32].

An organizational commitment will inspire employees in the organization. Empirical studies have confirmed a positive relationship between employee commitment to the organization [33]. An understanding of security policy provides a new lens for learning noncompliance behavior. Employees sometimes sacrifice compliance with information security policies to complete their duties [34]. The research conducted by

Sharma, which states that organizational commitment influences behavioral intentions to comply with the Security Policy Information and employee status has an impact on organizational commitment [35]. This study argues that organizational commitment can improve compliance directly without influencing with user intention or employee status. Cultural factors influence modeling human behavior. Compliance culture should be within the organization and play an essential role in increasing individual compliance and behavior [36]. This statement is supported by Arage [37], which states that national culture has more influence on compliance behavior [37]. However, different results shown by Gerber, management culture does not provide any improvement at all [32]. In a company with a stable culture, the appropriate policies and procedures, including sanctions and education programs regarding the policy, will be well implemented. Employee non-compliance with information security policies (ISP) can be overcome by maintaining an ISP compliance culture through organizational culture [38]. Further studies are needed to find out factors such as organizational culture to find out the involvement of organizational culture can influence compliance with security policies. Reward factors mentioned by interviewee will increase employee compliance with information security policies.

Although the different results shown by [30] found that punishment and reward/cost no significant impact on the intention to comply with the information security policy, this opinion supports by [4], which mention awards to comply with the information security policy is not significant. However, [32] indicates reward will support achieve performance goals and improve security compliance. This study attempts to explore the importance of rewards with information security policies compliance. Non-compliance with policies will pose a higher risk of increasing costs. The organization will incur higher costs when an incident occurs due to non-compliance of its employees. Kajtazi [39] examines cost factors as a mediating mechanism to explain intentional violations by people in information security policies.

The results of the study also show that perceptions of employee sunk costs predicted by the effects of settlement and physical mismatches [39]. The same thing was explained by Han that fulfilling psychological contracts could reduce the adverse impact of costs on ISP compliance intentions in the supervisor group [2]. Different perceptions are conveyed by Sommestad that Prediction of intention to adhere to information security policies is improved if compliance costs [20]. In this study, the perceived costs are the costs that arise due to the risk of non-compliance. The organization would become aware of the importance of employee compliance with information security policies if organizations spent a higher cost to secure their information. Self-Efficacy is a variable that is widely used by previous research to determine compliance with information security policies. Previous research has consistently stated that self-efficacy significantly influences employees' intention to comply with information security policies [37, 40, 41]. Self-Efficacy can increase employee awareness in handling security threats [28].

However, different results were found by Sikolia [42] who researched at a mid-western university by combining variables from Protection Motivation Theory (PMT), the Theory of Reasoned Action, and Cognitive Evaluation Theory. The results found that response-efficacy had more influence on behavioral intentions than self-efficacy. This study will further test the user's behavioral intentions using the compliance of

information security policies using variable self-efficacy [42]. User attitudes and moral beliefs are also variables that are usually used by previous researchers to determine the user's intention to comply with information security policies. However, the empirical study conducted by Moody [30] the construct of moral beliefs does not significantly affect compliance. Moral cannot stand alone, so it needs to be united with self-concept, role, and influence, resulting in a new construct, namely the role value. Differences in moral definition affect by the culture of each organization. Therefore, in this study, it is still believed that moral constructs can affect user compliance.

## 4 Conclusion

This research has a contribution to theory with a proposed model that can be used by organizations to determine the level of compliance of their employees with information security policies. This model will develop using theories from a different field, combines several factors from several theories will provide additional knowledge in the field of information security behavior. This conceptual model uses organizational theory commitment, organizational culture, and cost with commitment organizational variables, culture organization, reward and perceived of cost. While for the theory of human behavior using planned behavior theory and additional habit variables.

The implementation model of information security policy compliance expected growth the effectiveness and efficiency of organizational performance. Moreover, changing user behavior will have a direct and indirect impact on an organization. Periodic assessment will be enhanced employee behavior and trigger organizational culture so that the organization can achieve its goal. This study will identify factors that influence compliance with information security policies. Formerly the variables found used to create models to evaluate employees the compliance of policy information security. The variables to be used are determined from the literature review and theories. Result of this study is a model that can be used by organizations to measure employee compliance with information security policies.

## References

1. Bélanger, F., Collignon, S., Enget, K., Negangard, E.: Information & management determinants of early conformance with information security policies. Inf. Manag. **54**, 887–901 (2017)
2. Han, J.Y., Kim, Y.J., Kim, H.: An integrative model of information security policy compliance with psychological contract: examining a bilateral perspective. Comput. Secur. **66**, 52–65 (2017)
3. Pahnila, S., Siponen, M., Mahmood, A.: Which factors explain employees' adherence to information security policies? An empirical study. In: Pacis 2007 Proceedings, pp. 438–439 (2007)
4. Siponen, M., Adam Mahmood, M., Pahnila, S.: Employees' adherence to information security policies: an exploratory field study. Inf. Manag. **51**, 217–224 (2014)
5. Nasir, A., Arshah, R.A., Ab Hamid, M.R.: Information security policy compliance behavior based on comprehensive dimensions of information security culture. In: Proceedings of 2017

International Conference on Information System and Data Mining. - ICISDM 2017, pp. 56–60 (2017)
6. Abed, J., Dhillon, G., Ozkan, S.: Investigating continuous security compliance behavior : insights from information systems continuance model. In: Twenty-second Americas Conference on Information Systems, San Diego, pp. 1–10 (2016)
7. Humaidi, N., Balakrishnan, V.: Leadership styles and information security compliance behavior: the mediator effect of information security awareness. Int. J. Inf. Educ. Technol. **5**, 311–318 (2015)
8. Doherty, N.F., Tajuddin, S.T.: Towards a user-centric theory of value-driven information security compliance. Inf. Technol. People **31**, 348–367 (2018)
9. Hwang, I., Kim, D., Kim, T., Kim, S.: Why not comply with information security? An empirical approach for the causes of non-compliance. Online Inf. Rev. **41**, 2–18 (2017)
10. Andress, J., Winterfeld, S.: Cyber Warfare Techniques, Tactics and Tools for Security Practitioners, vol. 2. Elsevier Inc., Waltham (2014)
11. Gikas, C.: A general comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS standards. Inf. Secur. J. Glob. Perspect. **19**, 132–141 (2010)
12. Katz, F.H.: The effect of a university information security survey on instruction methods in information security. In: Proceedings of 2nd Annual Conference on Information Security Curriculum Development, pp. 43–48 (2005)
13. Ayyagari, R., Tyks, J.: Disaster at a university: a case study in information security. J. Inf. Technol. Educ. Innov. Pract. **11**, 85–96 (2012)
14. BS ISO/IEC: ISO 27001 - Information Technology Security Techniques Information Security Management Systems, Requirements (2005)
15. Sommestad, T., Hallberg, J., Lundholm, K., Bengtsson, J.: Variables influencing information security policy compliance: a systematic review of quantitative studies. Inf. Manag. Comput. Secur. **22**, 42–75 (2014)
16. NIST: Glossary of Key Information Security Terms [NISTIR 7298 Rev 2] (2013)
17. Calder, A., Watkins, S.: It Governance an International Guide to Data Security and ISO 27001/ISO27002, vol. 6. Kopan Page, UK (2015)
18. Barry, L.: Information Security Policy Development for Compliance. CRC Press/Taylor & Francis Group, Boca Raton (2013)
19. Ross, R.S.: Assessing security and privacy controls in federal information systems and organizations: building effective assessment plans, pp. 1–487. NIST Special Publication (2014)
20. Sommestad, T., Karlzén, H., Hallberg, J.: The theory of planned behavior and information security policy compliance. J. Comput. Inf. Syst. **00**, 1–10 (2017)
21. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Comput. Secur. **32**, 90–101 (2013)
22. Vroom, C., Von Solms, R.: Towards information security behavioural compliance. Comput. Secur. **23**, 191–198 (2004)
23. Kankanhalli, A., Teo, H.H., Tan, B.C.Y., Wei, K.K.: An integrative study of information systems security effectiveness. Int. J. Inf. Manag. **23**, 139–154 (2003)
24. Chang, S.E.: Organizational factors to the effectiveness of implementing information security management (2006)
25. Lowry, P.B., Posey, C., Bennett, R.B.J., Roberts, T.L.: Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust. Inf. Syst. J. **25**(3), 193–273 (2015)
26. Alshare, K.A., Lane, P.L., Lane, M.R.: Information security policy compliance: a higher education case study. Inf. Comput. Secur. **26**, 91–108 (2018)

27. Doherty, N.F., Anastasakis, L., Fulford, H.: The information security policy unpacked: a critical study of the content of university policies. Int. J. Inf. Manag. **29**, 449–457 (2009)
28. Hina, S., Dominic, D.D.: Information security policies: investigation of compliance in universities. In: 2016 3rd International Conference on Computer and Information Sciences. In: Proceedings, ICCOINS 2016, pp 564–569 (2016)
29. Bamberg, S., Schmidt, P.: Incentives, morality, or habit? Predicting students' car use for University routes with the models of Ajzen, Schwartz, and Triandis. Environ. Behav. **35**, 264–285 (2003)
30. Moody, G.D., Siponen, M., Pahnila, S.: Toward a unified model of information security policy compliance. MIS Q. **42**, 285–311 (2018)
31. Sohrabi Safa, N., Von Solms, R., Furnell, S.: Information security policy compliance model in organizations. Comput. Secur. **56**, 1–13 (2016)
32. Gerber, N., McDermott, R., Volkamer, M., Vogt, J.: Understanding information security compliance - why goal setting and rewards might be a bad idea. In: International Symposium on Information Assurance and Security, HAISA 2016, vol. 10, pp. 145–155 (2016)
33. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. **34**, 523–548 (2010)
34. Kajtazi, M., Cavusoglu, H., Benbasat, I., Haftor, D.: Escalation of commitment as an antecedent to noncompliance with information security policy. Inf. Comput. Secur. **26**, 171–193 (2018)
35. Sharma, S., Warkentin, M.: Do I really belong? Impact of employment status on information security policy compliance. Comput. Secur. (2018)
36. Sommestad, T.: Social groupings and information security obedience within organizations. In: International Federation for Information Processing, pp. 325–338 (2015)
37. Arage, T., Belanger, F., Beshah, T.: Influence of national culture on employees' compliance with information systems security (ISS) policies: towards ISS culture in Ethiopian companies. In: AMCIS 2015 Proceedings, pp. 1–7 (2015)
38. Amankwa, E., Loock, M., Kritzinger, E.: Establishing information security policy compliance culture in organizations. Inf. Comput. Secur. **26**, 420–436 (2018)
39. Kajtazi, M., Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Assessing sunk cost effect on employees' intentions to violate information security policies in organizations. In: Proceedings of Annual Hawaii International Conference on System Sciences, pp. 3169–3177 (2014)
40. Sommestad, T., Karlzén, H., Hallberg, J.: The sufficiency of the theory of planned behavior for explaining information security policy compliance. Inf. Comput. Secur. **23**, 200–217 (2015)
41. Aurigemma, S., Mattson, T.: Privilege or procedure: evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls. Comput. Secur. **66**, 218–234 (2017)
42. Sikolia, D., Twitchell, D., Sagers, G.: Employees' adherence to information security policies: a partial replication. In: Proceedings of the Americas Conference on Information Systems, pp. 1–9 (2016). https://doi.org/10.1109/ICMTMA.2009.433