



Document details

< Back to results | 1 of 1

↗ Export ↴ Download 🖨 Print ✉ E-mail 💾 Save to PDF ☆ Add to List More... >

View at Publisher

2019 1st International Conference of Intelligent Computing and Engineering: Toward Intelligent Solutions for Developing and Empowering our Societies, ICOICE 2019 December 2019, Article number 9035133
1st International Conference of Intelligent Computing and Engineering, ICOICE 2019; Hadhramout; Yemen; 15 December 2019 through 16 December 2019; Category numberCFP19V10-ART; Code 158565

Exploring Staff Perception of InfoSec Policy Compliance : Palestine Universities Empirical Study (Conference Paper)

Iriqat, Y.M.^a ✉, Ahlan, A.R.^a ✉, Abdul Molok, N.N.^a ✉, Abd Rahim, N.H.^b ✉

^aKulliyyah of Information Communication Technology, International Islamic University, Malaysia

^bKICT, International Islamic University, Malaysia

Abstract

↕ View references (66)

There is worldwide recognition of the problems associated with insider threats, intentional and unintentional; One of the significant issues in mitigating InfoSec risks is Staff compliance intention of InfoSec policies (ISP's). The study purpose seeks to understand and explore Staff compliance intention of ISP's based on how Staff perceive several factors adopted from multi-Theories from ISP's research. Such as Sanction from General Deterrence Theory, Rewards as extrinsic motivation, Coping Appraisal from Protection Motivation Theory, and, Information Reinforcement that constitute the theoretical model. In the context of Palestine universities, the research Model first part constitutes the understanding of Staff awareness of ISP's based on four selected Policy-Focused Areas (PFA) from SANS 2014. Moreover, to assess this knowledge to reflect on the multi-Theory perception factors effects on Staff compliance intention. Furthermore, to investigated Staff SETA to assess how universities value their Staff knowledge on ISP's. The research Methodology explores the problem empirically using descriptive analysis research design such as summaries and regression analysis. The study has 600 datasets collected from six universities by the developed research quantitative instrument. The findings show that Staff value the importance of the model factors in promoting Staff compliance intention. Staff have some awareness of PFA's and SETA needs extra attention. The Practical implications for creating ISP compliance among university Staff by drawing on their perception of factors adopted from multi-Theories. Consequently, as for the organisation, effective SETA programs to sustain the effort of Staff compliance intention of ISP's. Meanwhile, this study seeks to assert that ISP's compliance is the responsibility of all academic and administrative Staff from all department and as a paradigm for other employees. The research covers ISP perception among Palestine Staff, and the expected outcome includes-A novel theoretical contribution model with six significantly contributing factors. Also, PFA in the context of Palestine contributes as a methodological contribution and Staff SETA as practical research contribution. © 2019 IEEE.

SciVal Topic Prominence ⓘ

Topic: Information Security | Protocol Compliance | Breach

Prominence percentile: 98.799



Author keywords

Information Security Policies

InfoSec Policies Compliance

Policy-Focused Area

SETA

Indexed keywords

Metrics ⓘ View all metrics >



PlumX Metrics



Usage, Captures, Mentions, Social Media and Citations beyond Scopus.

Cited by 0 documents

Inform me when this document is cited in Scopus:

Set citation alert >

Set citation feed >

Related documents

Information security policy perceived compliance among staff in palestine universities: An empirical pilot study

Iriqat, Y.M. , Ahlan, A.R. , Molok, N.N.A.

(2019) 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology, JEEIT 2019 - Proceedings

A descriptive review and classification of organizational information security awareness research

Hutchinson, G. , Ophoff, J. (2020) Communications in Computer and Information Science

Information security behavior: Towards multistage models

Pahnila, S. , Karjalainen, M. , Siponen, M. (2013) Proceedings - Pacific Asia Conference on Information Systems, PACIS 2013

View all related documents based on references

Find more related documents in Scopus based on:

Engineering
controlled terms:

Computation theory

Motivation

Regression analysis

Engineering
uncontrolled terms

Administrative staff

Contributing factor

Descriptive analysis

Extrinsic motivation

Methodological contributions

Protection motivation theory

Research methodologies

Theoretical modeling

Engineering main
heading:

Intelligent computing

Authors > Keywords >

ISBN: 978-172814487-0

Source Type: Conference Proceeding

Original language: English




DOI: 10.1109/ICOICE48418.2019.9035133

Document Type: Conference Paper

Publisher: Institute of Electrical and Electronics Engineers Inc.

References (66)

[View in search results format >](#)

☐ All [Export](#)  [Print](#)  [E-mail](#)  [Save to PDF](#) [Create bibliography](#)

- ☐ 1 Sadowsky, G., Dempsey, J.X., Greenberg, A.
(2003) *Information Technology Security Handbook*. Cited 16 times.
Washington World Bank

- ☐ 2 Alotaibi, M., Furnell, S., Clarke, N.
A Novel Model for Monitoring Security Policy Compliance?
(2016) *Journal of Internet Technology and Secured Transactions*, 5 (3-4). Cited 2 times.

- ☐ 3 Al-Omari, A., El-Gayar, O., Deokar, A.
(2012) *Security Policy Compliance: User Acceptance Perspective*
Paper presented at the System Science (HICSS), 45th Hawaii International Conference

- ☐ 4 Yazdanmehr, A., Wang, J.
Employees' information security policy compliance: A norm activation perspective
([Open Access](#))

(2016) *Decision Support Systems*, 92, pp. 36-46. Cited 28 times.
doi: 10.1016/j.dss.2016.09.009

[View at Publisher](#)

- ☐ 5 Samantha, M.
Data Breaches in Higher Education Institutions
(2018) *Honors Theses and Capstones*, p. 400.
<https://scholars.unh.edu/honors/400>