# INFORMATION SECURITY POLICY PERCEIVED COMPLIANCE MODEL FOR STAFF IN PALESTINE UNIVERSITIES

BY

YOUSEF MOHAMMAD MOUSA IRIQAT

A thesis submitted in fulfilment of the requirement for the degree of Doctor of Philosophy in Information technology

Kulliyyah of Information and Communication Technology
International Islamic University Malaysia

NOVEMBER 2020

# ABSTRACT

Information security policies play a significant role in securing university information assets. There should be clear information security policies in place to ensure effective staff compliance—policy perceptibility has a positive impact on employee adherence. The focus of the research is staff compliance intention of information security policies in Palestine universities. There is a need for empirical analysis on staff perception of information security policies compliance based on the intersection and combination of factors adopted from research on multiple information security theories that could have a direct/ indirect effect on staff compliance intention. Therefore, this study seeks to understand and explore staff compliance intention of information security policies based on how they perceive several factors such as perceived sanction from general deterrence theory, perceived rewards as extrinsic motivation, perceived coping appraisal from protection motivation theory, and, information quality, information privacy and facilitating conditions perceived factors from information reinforcement. Therefore, we propose a theoretical novel model built around the perception core model and the Palestinian context. The core model constitutes the perception factors, that is, how "perceived" factors directly affect "perceived" intention to comply. Our model is suited for the Palestinian context, as it works to understand staff compliance of information security policies based on staff perception of policy focused areas and staff security education and training awareness. To significantly implement the theoretical research model, the population of the study covers a wide area of Palestine form several universities to validate and confirm the model empirically using structural equation modelling. The study research design is an empirical, quantitative, exploratory (and descriptive), in addition to the developed research instrument incorporated to achieve the research methods and objectives specifically. The study objective was achieved by carefully reviewing the most appropriate potential approaches to the problem. The researcher sought a model that could find and explain any gaps in staff perception of information security policies and model factors. Thus, a novel model was designed, validated and tested. This study made a theoretical contribution through its novel model. The use of policy focused areas made the model incorporate elements from the Palestinian context directly. This is important, as current staff perceptions of information security policies play a significant role in studying them and discussing potential future policies. In this sense, it provides a methodological contribution. Furthermore, the use of data on security education and training awareness enabled us to provide potential solutions to existing problems more effectively. Security education and training awareness programs demonstrably enhance compliance intention and unify efforts between universities and their employees to mitigate security threats from insiders, be they intentional or unintentional. This constitutes a practical contribution.

# خلاصة البحث

سياسات أمنية المعلومات لها دورًا كبيرًا في الحفاظ على أصول المعلومات الجامعية. لذلك ينبغي أن تكون هناك سياسات امنية واضحة في نظم المعلومات من اجل ضمان الإمتثال الفعال للموظفين – فإدراك السياسات له أثر إيجابي على التزام الموظفين. ركز هذا البحث على ادراك الموظفين في الامتثال لسياسات أمنية المعلومات في الجامعات الفلسطينية، بناءا على الحاجة إلى التحليل التجريبي على أساس التقاطع والمزج لعدد من العوامل النظرية من البحوث السابقة في أمنية المعلومات التي يمكن أن يكون لها أثر مباشر / غير مباشر على امتثال الموظفين. لذلك ، تسعى هذه الدراسة لفهم واستكشاف ادراك الموظفين في الامتثال لسياسات أمنية المعلومات، وذلك بالاعتماد على عوامل مثل ادراك العقوبة من نظرية الردع العام ، وادراك المكافآت كدافع خارجي ، وادراك تقييم المواجهة من نظرية الحماية الدافعية ، وعوامل نوعية المعلومات ، وخصوصية المعلومات وتسهيل الظروف من نظرية المعلومات التعزيزية. لذلك، يقترح هذا البحث نموذجاً نظرياً جديداً مبنياً على النموذج الأساسي للادراك مما سبق من النظريات آنفة الذكر وفي السياق الفلسطيني. ويشكل النموذج الأساسي عوامل الفهم والادراك، أي كيف تؤثر العوامل "المدركة / المفهومة" تأثيراً مباشراً على النية "المتصورة/المدركة" للإمتثال. أيضا النموذج مناسباً للسياق الفلسطيني، حيث أنه يعمل على فهم إمتثال الموظفين لسياسات أمنية المعلومات القائمة على تصور/ ادراك الموظفين للمجالات التي تركز على السياسات والتثقيف الأمني، التوعية والتدريبية للموظفين. تمتد الجامعات الفلسطينية على جميع مناطق فلسطين، ولتنفيذ نموذج البحث النظري وللتحقق من صحة النموذج وتأكيده تجريبياً باستخدام نمذجة المعادلات المهيكلة. ولتحقيق أساليب وأهداف البحث على وجه التحديد تم تصميم اداة بحث خاصة بالدراسة مبنية على عوامل الدراسة بالاضافة الى بعض من عوامل مجالات التركيز للسياسات الامنية، والتثقيف الأمني والتوعية التدريبية. وقد تحققت أهداف الدراسة عن طريق إجراء استعراض دقيق لأنسب النُهج الممكنة لمعالجة المشكلة. فوضع نموذج لاستكشاف وشرح أي ثغرات في ادراك الموظفين في الامتثال لسياسات أمنية المعلومات والعوامل النموذجية. وهكذا ، تم تصميم نموذج جديد وإقرارهِ واختباره. قدمت هذه الدراسة مساهمة نظرية من خلال نموذجها الجديد. وبما ان تصورات الموظفين الحالية لسياسات أمنية المعلومات تلعب دورا هاما في دراست ومناقشة السياسات المستقبلية المحتملة، بأستخدام عوامل التركيز الاساسية للحماية، لذللك قدم البحث مساهمة منهجية بدمج هذه العناصر في السياق الفلسطيني مباشرة. ايضا، فإن استخدام البيانات المتعلقة بالسياق الفلسطيني تمكننا من توفير حلول محتملة للمشاكل القائمة على نحو أكثر فعالية. تعزز بشكل واضح برامج التثقيف الأمني والتوعية التدريبية نية الامتثال وتوحيد الجهود بين الجامعات وموظفيها للتخفيف من التهديدات الأمنية ، سواء كانت مقصودة أو غير مقصودة. ويشكل ذلك مساهمة عملية.

# APPROVAL PAGE

The thesis of Yousef Mohammad Mousa Iriqat has been approved by the following:

_____

Abd. Rahman Bin Ahlan
Supervisor

_____

Nurul Nuha Binti Abdul Molok
Co-Supervisor

_____

Noor Hayani Binti Abd Rahim
Co-Supervisor

_____

Akram Zeki Khedher
Internal Examiner

_____

Ruzaini Abdullah Arshah
External Examiner

_____

Michael Eddie Kyobe
External Examiner

_____

Mohamed Naqib Eishan Jan
Chairman

# DECLARATION

I hereby declare that this thesis is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Yousef Mohammad Mousa Iriqat

Signature ....*Yousef Iriqat*..... Date .....6/11/2020.....

**INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA**

**DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH**

INFORMATION SECURITY POLICY PERCEIVED COMPLIANCE MODEL FOR STAFF IN PALESTINE UNIVERSITIES

I declare that the copyright holders of this thesis are jointly owned by the student and IIUM.





By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Yousef Mohammad Mousa Iriqat

| | |
|---|---|
| *Yousef Iriqat* | 6/11/2020 |
| ……..…….. | …….. |
| Signature | Date |

# ACKNOWLEDGEMENTS

All praise to Almighty **Allah** the most merciful most compassionate and most beneficial for giving me health, strength and patience for enabling me to pursue my studies at this stage of my life.

Gratitude is always given to the soul of my parents; peace be upon them. I wish to express my heartfelt love to my beloved family; my wife, sons and daughters, my sisters and brothers of whom have unfailingly given endless patience, love and support through the PhD journey. My utmost thanks to my brother Mahmoud for his encouragement, support and always ready to help being thousands of miles away. My appreciations for the continues support of my employer Al-Quds Open University.

Special thanks and appreciation for Dr. Nurul Nuha and Dr. Noor, my co-supervisors for their time, effort and guidance.

Of course, I would like to express my honest gratitude to my supervisor, the Deputy Dean of postgraduate studies at the Kulliyyah of Information & Communication (KICT) IIUM, **Dr. Abd. Rahman Ahlan** for providing me with a wealth of help and support during this fantastic learning journey, really this work would have never been completed without his vision and direction.

# TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

# LIST OF ABBREVIATIONS

| | |
|---|---|
| AC | Academic Staff |
| AD | Administrative Staff |
| ANOVA | Analysis of Variance |
| ASC | Staff Awareness of InfoSec Policies |
| AVE | Average Variance Extracted |
| CA | Cronbach's Alpha |
| CARE | Coping Appraisal Response Efficacy |
| CASE | Coping Appraisal Self-Efficacy |
| CB | Covariance-Based |
| CDP | Clean Desk Policy |
| CMB | Common Method Bias |
| CMV | Common-Method Variance |
| CR | Composite Reliability |
| EISP | Enterprise Information Security Policy |
| EM | Extrinsic Motivation |
| EUP | Email Usage Policy |
| GASSP | Generally Accepted Security System Principles |
| GCI | Global Cybersecurity Index |
| GDPR | General Data Protection Regulation |
| GDT | General Deterrence Theory |
| HEISC | Higher Education Information Security Council |
| HTMT | Heterotrait-Monotrait |
| IC | Intention to Comply |
| IM | Intrinsic Motivation |
| InfoSec | Information Security |
| IR | Information Reinforcement |
| IRFC | IR Facilitating Conditions |
| IRIP | IR Info Privacy |
| IRIQ | IR Info Quality |
| ISO | International Standards Organization |
| ISP | Information Security Policy |
| ISSP | Issue-Specific Security Policies |
| IT | Information Technology |
| IUP | Internet Usage Policy |
| KW | Kruskal- Wallis |
| NIST | National Institute of Standards and Technology |
| NSD | Non-Statistical Difference |
| PEP | Palestine Economy Portal |
| PFA | Policy Focused Areas |
| PLS | Partial Least Square |
| PMT | Protection Motivation Theory |
| PP | Password Policy |
| RO | Research Objective |
| RQ | Research Question |
| Rwds | Rewards |
| SC | Sanction Certainty |
| SCT | Social Cognitive Theory |
| SD | Statistical Difference |
| Std. | Standard Deviation |
| SEM | Structure Equation Modelling |
| SETA | Security Education and Training Awareness |
| Sig | Significance |
| SS | Sanction Severity |
| SysSP | System-Specific Security Policies |
| TAM | Technology Acceptance Model |
| TRA | Theory of Reasoned Action |
| TPB | Theory of Planned Behaviour |
| VIF | Variance Inflation Factor |

# CHAPTER ONE

# INTRODUCTION

## 1.1 INTRODUCTION

Universities have recently begun to recognise that, in today's interconnected world, they must actively protect their information assets from both internal and external threats. As they constitute potential insider threats to information security (InfoSec), employees are often seen as the weakest link. Both employees and organisations must be aware of this rising challenge. Understanding staff perception of InfoSec policy compliance is critical for universities that want to leverage staff capabilities to mitigate InfoSec risks, specifically in developing countries, such as Palestine.

Recent studies have addressed the increasing importance of modern computer systems and information management by universities in Palestine. The widespread availability of the internet, which now extends beyond its traditional boundaries, has resulted in a wide variety of undesirable activities. As such, InfoSec policy compliance has emerged as a significant issue (ISACA, 2006; Saheb, 2013; Abdelwahed et al., 2017; Flores & Sun, 2018; Tsohou et al., 2015).

The protection of information assets and resources is critical to the proper functioning of a university. Issues such as unauthorised grade changes and persistent problems with registration or financial systems can undermine institutional credibility and viability.

Thus, more effort must be directed toward motivating staff to be security compliant and in line with university InfoSec policies (Al-Alawi et al., 2016). Universities tend to suffer from staff members who do not fulfil their InfoSec

responsibilities (Siponen et al., 2014; Silvius et al., 2012). Universities view information as one of their most valuable assets. The university environment makes for a unique dynamic in which information is constantly being exchanged, generated and applied in ways that allow affiliated students and staff on and off the campus to work with it through e-learning and shared resources (Dahbur et al., 2012).

## 1.2 RESEARCH BACKGROUND

Information technology is distributed around the world, meaning threats can come from anywhere through connected networks or shared resources (Sadowsky et al., 2003). According to Sadowsky et al. (2003), "Developing countries should regard InfoSec as a top priority, for the opportunity costs of not doing so may be very high indeed and criminal activity will migrate to places where controls are poor, and InfoSec is weak".

The principles of InfoSec are the same in both developed and developing countries. However, the significance of InfoSec penetration in developing countries could be far more severe (Sadowsky et al., 2003). Developing countries often suffer from a lack of technical resources and awareness. Moreover, some developing countries may not view InfoSec as a high priority because they face many other challenges. Palestine, for instance, faces financial, political and security issues on top of the Israeli occupation.

Like other institutions, universities face both external and internal threats (Barzak et al., 2016). Internal threats can emerge from staff with direct or indirect access to information systems. Most research views internal threats as related to noncompliance behaviour and divides internal threats into *intentional* and *unintentional* (Greitzer et al., 2014; Aurigemma & Mattson, 2017; Al-Omari et al., 2012). Intentional behaviour includes actions such as information theft and deliberate ignorance of rules.

Greitzer et al. (2014) explain that unintentional behaviour is accidental, often through "inadequate system knowledge" or ignorance caused by a "lack of awareness and lack of training".

Insider behaviour is expected to continue to be the most significant InfoSec threat. Despite this, organisations still fail to focus on this area (Kleeman, 2018; Bartnes, Moe & Heegaard, 2016; Ong & Chong, 2014; Montesdioca & Maçada, 2015; Posey, Roberts & Lowry, 2015). Employee maliciousness, negligence and human error accounted for 54% of all InfoSec incidents in 2014 (Ponemon Institute, 2016).

Staff actions, be they intentional or unintentional, can jeopardise information systems and threaten university information assets (Siponen et al., 2014; Kruger & Kearney, 2006; Flores & Sun, 2018). Several critical InfoSec operations are still not able to be fully automated, even with highly advanced technology (Silvius et al., 2012; Lebek et al., 2014; Theoharidou et al., 2005). As a result, careless behaviour among staff members, such as opening spam email links or downloading attachments from unknown emails, continues to be a significant factor for InfoSec policy violations.

InfoSec policies play a significant role in securing university information assets. There should be clear InfoSec policies in place to ensure effective staff compliance—policy visibility has a positive impact on employee adherence (Siponen et al., 2009).

Emphasising these InfoSec policies is important, as it focuses attention on security and makes staff conscious about the skills they need to protect information assets (Pérez-González, 2019; Chan et al., 2005; Muhire, 2012; Herath & Rao, 2009). Of course, staff members must have good intentions for compliance encouragement to have much of an impact (Bulgurcu et al., 2010; D'Arcy & Herath, 2011; Herath & Rao, 2009; Alshare et al., 2018).

Therefore, this study seeks to analyse the perception of "intention to comply" with InfoSec policies among university staff.

### 1.2.1 Research Background in Palestine.

According to Symantec, a cybersecurity firm, more than two-thirds of the organisation in the Middle East were incapable of protecting themselves from sophisticated cyber-attacks. The state of InfoSec in Palestine does not stray from that of its region; it has been negatively affected by factors such as user base growth, low security awareness, lack of law enforcement training and lack of regulation (El-Guindy, 2014). Investment in information infrastructure has increased the value of e-business and created an enormous opportunity in the region. However, not all of this investment has considered the need for security solutions while developing this infrastructure (El-Guindy, 2014).

Using the Global Cybersecurity Index (2017), the researcher sees that the GCI index in Palestine is below the 33$^{rd}$ percentile; only three of 25 indicators are above the 65$^{th}$ percentile (cybercriminal legislation, government certification and international participation). A clear gap exists between developing countries in terms of awareness, understanding and knowledge on InfoSec practices.

The Palestine Economy Portal (2016) recommends extensive reforms to the rules and regulations surrounding government and institutional InfoSec policies. PEP (2016) argues for laws and legislation to facilitate the protection and security of information; it sees this as an urgent necessity to prevent the risks of cybercrime and InfoSec threats (PEP, 2016).

Recently, there has been a rising number of publications focused on cybercrime and InfoSec in Palestine (Abdelwahed et al., 2017; Amro, 2018; Al-Saheb, 2013). According to Amro (2018), the majority of people in Palestine are connected to the

internet and generally affected by technology. However, knowledge on cybercrime, including identity theft, financial fraud and defamation, does not match up with the high level of connection. In Palestine, for example, cybercrime laws and regulations are weak and must be reviewed (Amro, 2018).

Researchers have, in recent years, showing an increased interest in Palestinian university InfoSec policies (Abdelwahed et al., 2017; Al-Saheb, 2013). Al-Saheb (2013) recommends the establishment of university-level InfoSec units and the formalisation of InfoSec policy documents to avoid the risk of cybercrimes or penetration into the university information system.

According to a recent study on Palestinian universities in Gaza by Abdelwahed et al. (2017), universities should support the InfoSec policies from the process of risk assessment and creation of InfoSec policies to the process of continually reviewing and updating InfoSec policies.

### 1.3 RESEARCH PROBLEM

According to Abed et al. (2016), D'Arcy & Herath (2011), Alshare et al. (2018), Pahnila et al., (2007) and Aurigemma & Mattson (2017), human (staff) perception is crucial in an efficient InfoSec environment—technical solutions are insufficient. As knowledge accumulates on InfoSec policy compliance, it initiates changes in attitude, motivation and perception that gradually initiate positive changes in staff intention (Pérez-González, 2019; Alshaikh, et al., 2018; Kleeman, 2018).

According to Siponen and Vance (2010), Herath and Rao (2009), Siponen et al. (2014) and Safa et al. (2016), the mere implementation of InfoSec policies does not guarantee that employees will comply to its provisions. Correspondingly, employees may not perceive the effectiveness and importance of protecting information assets

through InfoSec policy compliance to be high; many employees may intentionally or unintentionally ignore, resist or abandon the policies, while some may perceive it as an obstruction to them completing their tasks.

Numerous research initiatives (da Veiga et al., 2020; Lebek et al., 2014; Aurigemma & Mattson, 2017; Siponen et al., 2010; Theoharidou et al., 2005; Tsohou et al., 2015) on InfoSec behaviour and awareness have focused on theory verification and validation or have simply been literature reviews of theory comparisons used in InfoSec or InfoSec policy compliance, and, as such, may present a biased viewpoint. Many researchers propose (Siponen et al., 2010; Lebek et al., 2014; D'Arcy & Herath, 2011; Alotaibi et al., 2016; Theoharidou et al., 2005) that a theoretical model without empirical evidence of employee InfoSec policy compliance does not offer any evidence to support their models.

Some research points to contradictions in the findings of other models or frameworks (Koohang et al., 2019; Rostami, Karlsson & Kolkowska, 2020; Lebek et al., 2014; Bulgurcu et al., 2010; Tsohou et al., 2015) based on the statistical results that confirm positive or negative relationships with InfoSec policy compliance. Each study sheds light on "staff intention to comply with InfoSec policy" through determinant and demographic differences. Correspondingly, the literature review reveals that perceived value of InfoSec policies and staff intention has yet to be sufficiently investigated (Bulgurcu et al., 2010; Parsons et al., 2013; Silvius et al., 2012; Chan & Mubarak, 2012).

While there is substantial research reviewing the factors that could influence InfoSec compliance intention (Tsohou et al., 2015; Siponen & Livari, 2006; Parsons et al., 2010; Harris & Furnell, 2012; Silvius et al., 2012; Yazdanmehr & Wang, 2016) that largely agrees on the importance of InfoSec policy compliance, significant issues must

still be explored. As suggested by Bulgurcu et al. (2010), an essential contribution to academic research is identifying the factors that lead to InfoSec policy compliance—several related studies indicate that there is a gap in this regard. New research could empirically test the hypothesised research models of different individuals and institutions.

Many studies (Trang & Brendel, 2019; Al-Alawi et al., 2016; Pahnila et al., 2007; Bulgurcu et al., 2010; Abdul Molok et al., 2010) confirm that the perception of social factors, such as sanctions, rewards and motivation, directly or indirectly shape staff compliance intention. Moreover, awareness of InfoSec policies can encourage compliance intention (Vance et al., 2012; Pahnila et al., 2007; Cheng et al., 2013; Barzak et al., 2016).

Therefore, combining factors from various theories could help with two issues related to the initial phenomenon of InfoSec policy compliance. First, it will help to study how staff perceive these theoretical factors as well as the differences among perception based on staff profiles. Second, it will provide an understanding of staff perceptions of the theory's factors based on its implications or effect on staff compliance intention.

Furthermore, to put this study in the context of Palestine universities, the researcher uses an investigation of several policy focused areas (PFA) adopted from SANS (2014), such as password policy, internet usage policy, email usage policy and clean desk policy (SANS, 2014) to shed more light on Palestinian staff perception of restrictive policies and ascertain the potential reaction to (or knowledge of) InfoSec policies in the future. Foremost to further study of staff security education and training awareness (SETA).

Therefore, this study adopts factors from well-known theories related to staff compliance intention, including general deterrence theory (GDT), the theory of planned behaviour (TPB), protection motivation theory (PMT) and information reinforcement (IR). These intentions are expected to eventually influence behaviour, making recognition of InfoSec policies a latent factor. Therefore, researcher seeks insight into "staff intention to comply with InfoSec policies in the context of Palestine" by targeting Palestinian university staff and combining several factors from theories that study the sanctions, rewards, coping appraisals and information reinforcement of staff perception. The researcher hopes to achieve an improved understanding of InfoSec policies in practice so the researcher can contribute to the improvement of InfoSec policies.

The proposed conceptual model integrates "perceived" factors among the staff (sanctions, rewards, coping appraisal and information reinforcement) with perceived "intention to comply" (D'Arcy & Herath, 2011; D'Arcy et al., 2009; Abed et al., 2016). The "expected" perceived practices/policies and "expected" perceived intention to comply is suitable in the context of Palestine (a non-oil-rich Gulf country) to understand staff "perception" intention and, to an extent, their perception of PFAs as tools to mitigate security threats, specifically from insiders. Most universities could have InfoSec practices implemented and distributed to their staff, as having documented and enforced InfoSec policies to govern staff intention to comply is cost-effective in terms of technical, financial and human resources. Hence, most information systems have InfoSec policies enforced through technical and practical measures.

This issue of practical measures points out that many staff members may not even realise that InfoSec policies exist or that they are experiencing fairly limited ones. Therefore, in the context of Palestinian universities, this study attempts to measure staff awareness of InfoSec policies based on staff perception of four selected PFAs. It also