SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I11P118

Volume 12 Issue 11, 216-227, November 2025
© 2025 Seventh Sense Research Group®

Original Article

Information Security Policy Compliance Model for the Federal Public Sector in Malaysia

Finlyson Anak Ludan[1], Zulaiha Ali Othman[1], Noridayu Adnan[1], Lokman Mohd Fadzil[2],
Muhammad Mustaqiim Roslan[2]

[1]*Center of Artificial Intelligence Technology, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Bangi, Malaysia.*
[2]*Cybersecurity Research Centre (CYRES), University Sains Malaysia (USM), Penang, Malaysia.*

[2]*Corresponding Author : lokman.mohd.fadzil@usm.my*

Received: 17 September 2025 Revised: 18 October 2025 Accepted: 17 November 2025 Published: 29 November 2025

Abstract *- An Information and Communication Technology (ICT) security policy is essentially an organization's protection against security risks. Nonetheless, these policies only demonstrate value when implemented with enforceability. Thus, a reference and a guide are needed as critical elements for the organization's security strategic implementation. Through key components' identification and measurement that incentivize employees' policy compliance, this article proposes an acceptable ICT security policy compliance model for Malaysia's federal public sector with fifteen variables developed based on relevant models. SPSS Pearson descriptive correlation analysis based on 204 Sarawak's federal government respondents indicates three most important factors: discerned usefulness, morality, and awareness; and three least important factors: punishment, maladaptive reward, and discerned severity, which stand out from the proposed model's 13 key base components. The proposed Malaysia federal sector ICT security policy will be subsequently implemented via the ICT security policy enforcement model.*

Keywords *- Information and Communication Technology, ICT Security Policy, Compliance Model.*

1. Introduction

Managing service delivery through information systems, including network infrastructure, is the responsibility of any organization's Information Technology Division. As ICT service delivery increased in 2000, the Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) ordered Malaysian government agencies to implement the Information and Communication Security Policy (DKICT), also known as the ICT Security Policy. For sensitive data to be available, confidential, and intact, an ICT security strategy is essential [1]. Since the security of ICT assets in every government agency is dependent on the three primary criteria of Information Security (IS)-confidentiality, integrity, and availability-enforcement is the primary goal of this policy [2]. Organizational security aims to protect organizations against cybercrime, while communal security focuses primarily on public ethics, laws, and privacy issues, encompassing both internal and external risks [3]. The service activities of each government agency serve as the foundation for its policies and programs. Nevertheless, they all have the same goal in mind: to guarantee that each government agency's operations are sustainable. ICT security policy failure or ignorance has resulted in security incidents, primarily information theft, which has damaged the organization's reputation and caused financial losses [4]. According to published data, there is an increasing danger in IS, especially from within organizations, and most breaches are brought on by users who do not follow information systems security [5].

As of October 2020, 9,042 cases in Malaysia pertaining to IS events had been reported by individuals and various businesses, according to the Malaysian Computer Emergency Response Team (MyCERT 2020) [6].

These incidents, including issues like fraud, spam, and human activity-based intrusion, characterized as the organization's information protection's weakest part [7], and staff members' ICT security policy requirements noncompliance, are acknowledged as prevalent issues in organizations [8]. This argument suggests that to create a compliance model that supports the ICT security rules, it is essential to distinguish the elements that impact an organization's ability to adhere to and comply with these rules.

The goal of an ICT security policy, according to ISO/IEC 27002 (2013), is to support management to ensure IS in compliance with service specifications and related legal provisions. Based on the service's objectives and the issue, management will determine the next course of action. It will uphold the policy to show dedication to and support for the organization's IS implementation. Furthermore, ISO 27002 also covers security policies that are essentially approved by the highest executives and communicated to all employees within the company or external stakeholders. According to the above definition, IS policy documents necessitate that all involved parties have a thorough comprehension of the objectives of the entities' services, their principal guidelines, and the means they are applied.

All interested parties must be able to retrieve and have the constant ability to scrutinize the application of IS policies to guarantee that ongoing implementation has been developed. Litigation, market value or investment loss, regulatory fines, extortion payments, discovery, regulatory notification, consumer redress and compensation, and lost business costs are some examples of economic expenses, depending on the type of breach [9]. Since employee noncompliance accounts for almost half of the establishment's security issues, IS regulations must be followed [10]. Additionally, either intentionally or unintentionally, users with system login access to an entity may harm the information system.

High reliance on Information Communication and Telecommunications (ICT) security is any company's largest challenge when it comes to processing information to provide services. Additionally, organizations must implement technical measures to reduce IS threats [11]. If a breach occurs, the organizations will face significant issues [12]. However, when organizational workers are not aware of potential safety issues, more than only technology interventions are needed [13].

The literature suggests putting IS rules into place [14] as a non-technical way to ensure the security of an organization's information technology and prevent security incidents caused by human nature. Because this research covers a wide range of sectors and domains, criminological, social, and psychological principles will be harnessed to identify acts against security enforcement throughout the IS literature study [15].

The key components of the basic model, as well as other elements pertaining to ICT Security Policy Compliance, are reviewed in the section that follows. Later in section three, the research's hypothesis includes a new list of variables for ICT Security Policy Compliance. The methodology of this work is covered in Section 4, and the questionnaires used to generate the model are presented in Section 5.

1.1. Research Gap

Despite the Malaysian government's ongoing enforcement of the Dasar Keselamatan ICT Sektor Awam (DKICT) through MAMPU, the efficacy of IS governance is still being threatened by federal public sector personnel's continual non-compliance. Prior studies primarily emphasize isolated behavioral constructs derived from theories such as the Technology Acceptance Model (TAM), Theory of Planned Behavior (TPB), and Protection Motivation Theory (PMT). However, there remains a lack of an integrated multi-theoretical model that contextualizes policy compliance within Malaysia's socio-cultural, moral, and organizational frameworks.

Moreover, most existing works focus on technical interventions and deterrent mechanisms (e.g., sanctions, system monitoring) rather than human-centric drivers, such as morality, awareness, and perceived usefulness - factors that the preliminary findings of this study reveal as significantly influencing compliance intention. Limited empirical exploration has been conducted on how these constructs interact synergistically across Malaysia's federal governance ecosystem, where hierarchical structures, bureaucratic culture, and moral obligations coexist.

Thus, there exists a research gap in understanding the holistic behavioral determinants of ICT policy compliance, specifically through an integrated framework combining PMT, TPB, TAM, General Deterrence Theory, and Practice Theory within Malaysia's federal public sector context.

1.2. Problem Statement

Malaysia's federal public sector still experiences frequent IS infractions despite established ICT security frameworks and national compliance standards, as many of these incidents are linked to staff non-compliance with security policies. Reports from MyCERT (2020) highlight that insider threats, negligence, and ignorance remain predominant causes of data breaches, signalling a disconnect between policy enforcement and human adherence.

Existing compliance models are unsuccessful in capturing the multi-dimensional characteristics of individual behaviors in organizational cybersecurity, often overlooking the interplay between individual cognition (e.g., discerned usefulness), moral conviction (e.g., ethical awareness), and institutional deterrence (e.g., punishment and sanctions). Consequently, while technical and procedural safeguards have matured, behavioral compliance remains inconsistent, fragmented, and weakly correlated with actual policy outcomes.

This gap in understanding the behavioral, cultural, and ethical underpinnings of compliance poses a serious challenge to national ICT governance. Without a comprehensive, empirically validated model tailored to Malaysia's federal administrative environment, ICT security policies risk remaining procedural formalities rather than enforceable behavioral standards. Therefore, this study addresses the critical question:

"What are the key behavioral, moral, and technological determinants influencing IS policy compliance among Malaysia's federal public sector employees, and how can these be modelled to improve enforceability and awareness?"

2. Literature Review

2.1. Dynamics of ICT Security Policy Fulfillment

The most recent comparative analysis studies were conducted using the basic model's factor with other factors. According to earlier studies, the Technology Acceptance Model (TAM), Theory of Planned Behavior (TPB), and

Protection Motivation Theory (PMT) are the theories that are most frequently used in literature analysis [16]. Additional elements that influence compliance intentions are also noted. These include the elements of the General Deterrence Theory and the initial elements that are also examined in conjunction with the fundamental model, specifically the awareness and morale components that fall under the Practice Theory category for the purposes of this investigation. There are still certain discrepancies in Table 1 that need to be tested on Malaysian businesses.

Punishment, Reward, Maladaptive Rewards, Discerned Ease of Use, and Discerned Usefulness are the five (5) elements that have been tested in Malaysia. Only a few of the fundamental models and other aspects were discovered to be involved in the 13 prior research works that were analyzed for this journal. Studies including all eleven (11) of the fundamental theoretical model's aspects, as well as four (4) more factors collectively, are still required in Malaysia and other nations.

For instance, the most recent research study conducted in Malaysia [17] only included the awareness element from the additional variables. It only included six (6) fundamental model factors, excluding the basic model from the Technology Acceptance Model. The most recent study only includes one (1) more aspect, awareness, and six (6) elements from the fundamental Protection Motivation Theory model [18]. Only [19] studied awareness, one of the extra aspects, and a few elements of all the main theories. The other thirteen (13) research studies in Table 1 do not incorporate all of the extra aspects and elements from the basic model. Regarding the moral component, it is the subject of only one study [8].

Table 1. Factors of the basic model

Theory Model															Journal	Country of Origin	Industry
Protection Motivation Theory						Theory of Planned Behaviour			Technology Acceptance Model		Additional Factors						
											General Deterrence Theory		Practice Theory				
Discerned Severity	Discerned Vulnerability	Maladaptive Rewards	Response Efficacy	Self-Efficacy	Response Cost	Attitude	Subjective Norm	Discerned Behavioral Control	Discerned Usefulness	Discerned Ease of Use	Rewards	Punishment	Awareness	Moral			
														✓	[8]	48 Countries	Company
✓	✓	✓	✓	✓	✓								✓		[18]	New Zealand	Higher Institutions
✓	✓		✓	✓		✓	✓						✓		[17]	Malaysia	Higher Institutions
✓	✓		✓	✓	✓										[20]	US & China	General Public
✓	✓		✓	✓	✓		✓								[21]	Saudi Arabia	General Public
						✓	✓	✓							[22]	Korea Selatan & USA	Instagram Users
✓	✓		✓	✓	✓										[23]	Australia	Real Estate Employees
✓	✓		✓	✓	✓	✓	✓	✓					✓		[24]	Malaysia	Industrial Workers
✓	✓		✓	✓	✓								✓		[25]	USA	Higher Institutions
✓	✓		✓	✓	✓	✓	✓								[26]	Canada	Management
✓	✓	✓	✓	✓	✓										[10]	Finland	Organization Employees
				✓			✓		✓	✓			✓		[19]	Jordan	Bank Employees
				✓		✓					✓	✓	✓		[14]	USA	Organization Employees

Table 2. Comparative analysis on existing research in literature

No	Authors	Paper Title	Methodology Used	Strengths	Research Gaps	Citations
1	B. Bulgurcu; H. Cavusoglu; I. Benbasat	IS policy compliance: An empirical study of rationality-based beliefs and IS awareness	Empirical study (as cited): examines rational beliefs and awareness influencing ISP compliance	Introduces rationality-based belief constructs; highlights the role of awareness	Limited contextualization for the Malaysian federal public sector; does not integrate moral/ethics explicitly	[14]
2	A. Vance; M. Siponen; S. Pahnila	Motivating IS security compliance: Insights from habit and protection motivation theory	Conceptual/empirical insights combining habit and PMT (as cited)	Bridges habit formation with PMT to explain compliance behavior	Emphasis on habit/PMT without integrating TAM and TPB in a single model; limited to non-Malaysian contexts	[10]
3	P. Ifinedo	Understanding information systems security policy compliance: Integrating the theory of planned behavior and the protection motivation theory	Integrated theoretical model (as cited)	Combines TPB and PMT to improve explanatory power for ISP compliance	Does not include TAM constructs (discerned utility/ease of use) or moral/awareness factors emphasized in the Malaysian context	[26]
4	N. S. Safa; M. Sookhak; R. Von Solms; S. Furnell; N. A. Ghani; T. Herawan	IS conscious care behavior formation in organizations	Organizational behavior study (as cited) focusing on conscious care behavior	Highlights organizational antecedents of secure behavior	Limited examination of punishment/reward efficacy; lacks federal public sector validation in Malaysia	[24]
5	B. Hanus; Y. A. Wu	Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective	PMT-based empirical analysis (as cited)	Quantifies the role of awareness within the PMT framework	Focuses on desktop behavior; lacks integration with TAM/TPB and moral determinants	[25]
6	P. Menard; G. J. Bott; R. E. Crossler	User motivations in protecting IS: Protection motivation theory versus self-determination theory.	Comparative theoretical/empirical assessment (as cited)	Compares PMT with self-determination to explain motivation	Does not evaluate Malaysian federal employees; limited treatment of policy usability (TAM)	[20]
7	S. Hina; D. D. D. P. Selvam; P. B. Lowry	Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world	PMT with institutional governance perspective (as cited)	Extends PMT with a governance lens for developing-world HEIs	Sector-specific to HEIs; lacks the moral/ethics construct emphasized in the Malaysian public sector	[17]

8	A. Almuqrin; I. Mutambik; A. Alomran; J. Z. Zhang	Enforcing information system security: Policies and procedures for employee compliance	Policy enforcement perspective (as cited)	Discusses policy and procedural levers for compliance	Deterrence emphasized; limited integration of discerned utility /ease of use and morality/awareness	[12]
9	M. N. Alraja; U. J. Butt; M. Abbod	IS policies compliance in a global setting: An employee's perspective	Global employee perspective (as cited)	Offers cross-context insights into policy compliance	Global lens may not capture Malaysian socio-cultural specifics, such as morality/awareness as top predictors	[5]
10	F. M. Alotaibi; A. Al-Dhaqm; W. M. S. Yafooz; Y. D. Al-Otaibi	A novel administration model for managing and organising the heterogeneous IS policy field	Model proposal (as cited)	Proposes administrative structuring for heterogeneous ISP domains	Focuses on administration rather than end-user behavioral compliance factors (morality, awareness, TAM)	[1]
11	S. Saeed	Digital workplaces and IS behavior of business employees: An empirical study of Saudi Arabia	Empirical study in digital workplaces (as cited)	Contextualizes security behavior in digital workplaces	Different national/sectoral context; limited portability to Malaysian federal governance structures	[3]
12	A. Vance; M. T. Siponen; D. W. Straub	Effects of sanctions, moral beliefs, and neutralization on IS policy violations across cultures	Cross-cultural empirical analysis (as cited)	Shows the importance of moral beliefs and sanctions across cultures	Does not provide a Malaysia-specific integrated model with TAM/TPB constructs or awareness as the top predictor	[8]
13	F. A. Shaikh, M. Siponen	IS risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity	Post-breach organizational analysis (as cited)	Highlights the role of top management attention after breaches	Focuses on risk assessment/management rather than employee ISP compliance intentions and integrated behavior models	[9]

2.2. Comparative Analysis on Existing Research in Literature

The comparative analysis reveals that the discourse surrounding IS Policy (ISP) compliance has evolved through a multidimensional theoretical foundation that integrates behavioral, cognitive, and organizational constructs (Table 2). Most existing studies draw heavily from theories such as the Technology Acceptance Model (TAM), Theory of Planned Behavior (TPB), and Protection Motivation Theory (PMT). For instance, Bulgurcu, Cavusoglu, and Benbasat (2010) pioneered the exploration of rationality-based beliefs and awareness as determinants of compliance intention, while Ifinedo (2012) advanced this understanding by integrating PMT and TPB into a unified model. Collectively, these works underscore that an interplay of personal cognition, discerned risk, and normative beliefs influences compliance behavior. However, a significant limitation persists in the lack of cross-cultural and sector-specific contextualization, particularly within Malaysia's federal public sector, where bureaucratic norms, hierarchical authority, and cultural morality may uniquely shape compliance behavior.

Across the reviewed literature, a predominant reliance on quantitative empirical designs emerges, with tools such as SPSS correlation analysis, regression modeling, and Structural Equation Modeling (SEM) being commonly employed. For instance, Vance, Siponen, and Pahnila (2012) utilized Protection Motivation Theory combined with habit formation to analyze behavioral compliance, while Hina, Selvam, and Lowry (2019) extended PMT to institutional governance within higher education settings. Although these methods provide statistical rigor, they often underrepresent moral and cultural variables, resulting in models that excel at prediction but lack human contextual sensitivity. In contrast, Safa et al. (2015) and Hanus & Wu

(2016) emphasized awareness and organizational antecedents but did not explore deterrence or ethical dimensions in depth. This methodological homogeneity suggests that while global models effectively quantify relationships, they inadequately capture the nuanced socio-ethical dynamics necessary to design policy frameworks for Malaysia's public sector.

One of the strongest aspects across these studies is the growing emphasis on theoretical integration to improve explanatory power. Ifinedo (2012) successfully merged TPB and PMT, highlighting intention as a central behavioral determinant, whereas Menard, Bott, and Crossler (2017) introduced Self-Determination Theory to explore intrinsic motivation. These studies collectively advanced the theoretical landscape by expanding the predictive factors influencing compliance intention, including discerned usefulness, discerned behavioral control, and self-efficacy. Moreover, Vance, Siponen, and Straub (2020) further enriched the domain by empirically confirming the influence of ethical faith and sanctions on compliance violations. However, most of these models remain theory-centric and technology-biased, overlooking moral education, awareness cultivation, and cultural upbringing as primary drivers—factors that have demonstrated statistical prominence in the current Malaysian study.

A key research gap evident from the comparative review is the absence of an integrated, context-specific model that combines technical, behavioral, and moral determinants of ISP compliance in Malaysia's federal governance environment. Most prior works—while methodologically robust—are drawn from Western or private-sector settings, where organizational culture, enforcement structures, and value systems differ substantially from those of Malaysian government institutions. The present study identifies morality (r = 0.735) and awareness (r = 0.628) as dominant predictors, suggesting that ethical conviction and continuous policy exposure are far more effective than punitive enforcement alone. This finding aligns with Malaysia's sociocultural emphasis on moral and religious education, indicating a distinct compliance behavior pattern that existing global models have not addressed. Consequently, integrating Practice Theory and General Deterrence Theory within a unified compliance model can better reflect Malaysia's federal realities-bridging the current gap between theoretical constructs and operational enforcement.

In synthesis, the comparative analysis demonstrates that while global literature provides a solid theoretical and empirical foundation, it falls short of offering culturally adaptive and human-centric compliance frameworks suitable for Malaysia's public sector. The proposed integrated model in this study contributes to the existing body of knowledge by harmonizing key constructs from PMT, TPB, TAM, GDT, and Practice Theory. This synthesis enables a more comprehensive understanding of compliance, acknowledging the coexistence of rational cognition (utilitarianism and ease of use), social norms (attitudes and behavioral control), and ethical imperatives (morality and awareness). By grounding the model in local governance and moral culture, this research bridges the global–local divide. It provides actionable insights for policymakers and ICT administrators to design sustainable, behaviorally anchored IS governance strategies.

2.3. Integrating Factors into Models

Based on earlier research projects carried out in various nations and kinds of companies, the suggested study model focuses on investigating and assessing the variables that influence compliance intentions. To establish a connection between all the elements involved, the findings of the theoretical model analysis are examined along with any other elements, conceptual models, or research frameworks that allude to the goal of adhering to the ICT Security Policy. Only a few of the models that were examined have been shown to offer a form of integrated factors that can be used as a guide for creating a model of ICT security enforcement, according to the results of the factors' assessment and the research model. Table 3 lists the current factors that have been used and researched in Malaysia, and all the factors explored are included in the theoretical model. The factors suggested in Malaysia are the most notable.

Table 3. Compliance intention conceptual model for malaysia

Model Basic	Categories	Factors
Protection Motivation Theory	Test Appraisal	Discerned Severity
		Discerned Vulnerability
		Maladaptive Rewards
	Coping Response	Response Efficacy
		Self-Efficacy
		Response Cost
Theory of Planned Behavior		Attitudes
		Subjective Norm
		Discerned Behavioral Control
Technology Acceptance Model		Discerned Usefulness
		Discerned Ease of Use
Additional Factors	General Deterrence Theory	Rewards
		Punishment
	Practice Theory	Awareness
		Moral/Ethical

3. Proposed Materials and Methods

The Information and Communication Security Policy (ICT) has been created and implemented within the Federal Department of the Public Sector's Information Technology Division in Kuching, Sarawak. Finding the elements influencing Sarawak Federal civil servants' inclination to obey the ICT Security Policy is the research objective. Therefore, the end goal of this research is to use a quantitative non-experimental design technique to propose a theoretical compliance model hypothesis, utilizing online surveys for employees subject to the ICT Security Policy.

Since it is simple to reach the respondents' intended audience—federal officials working in the Sarawak State Health Department—the online questionnaire approach using Google Form is employed in this study as the research instrument. The G*Power software is used to calculate the sample size. To assess the efficacy of statistical measures that are frequently employed in behavioral and social research, G* Power was developed as a stand-alone general application [27]. The number of expectations included in the questionnaire also influenced the effect of the sample size, which was assessed based on the statistical power [12] and the significance level [28]. Force of error 0.05, force (1-) = 0.8, the lowest allowable value, and effect calculation = 0.15, the middle level, are applied in this research.

In the meantime, the experiment has 15 Independent Variables (IVs), which aligns with the overall expectation. There are 139 responders in total when G*Power is used to make the measurements. This figure is the lowest that is sufficient to identify the effects of the sensitivity study [28]. Thirty respondents with at least ten years of ICT expertise who are aware that their businesses have an ICT Security Policy are given access to the revised questionnaire via an online survey once it has been reviewed by experts. A pilot test is a small-scale investigation conducted on a sample of at least 10 respondents [29] or 20-25 respondents with similar backgrounds [30] to identify issues with survey design and ensure the instruments' consistency and reliability [31].

4. Results and Discussion

The demographic distribution of data-collecting respondents is displayed in Table 4. 70 (33%) of the respondents are women, while 122 (67% of the respondents are men. Of the five age groups, 41% of respondents are between the ages of 30 and 39, 8% are under the age of 29, and over half are over 40. Most responders (64.6%) hold at least a tertiary degree, 17.9% hold a postgraduate degree, and 2.4% hold a doctorate. 10.4% of respondents held school certificates, while 23% had diplomas. Regarding work responsibilities, 90 respondents, or 42.5%, are involved in business operations, while 122 respondents, or 57.5%, occupy management positions. 144 respondents, or 67.9%, had more than ten years of work experience; forty (18.9%) respondents have worked for six to ten years, twenty-four (11.3%) have worked for one to five years, and four (1.9%) have worked for less than a year.

Table 4. Respondents' demography

Profile	Value	Frequency	Percentage (%)
Involved with ICT Security Policy	Yes	204	96.2
	No	8	3.8
Gender	Male	142	67
	Female	70	33
Age	20-29	17	8
	30-39	87	41
	40-49	96	45.3
	50 and above	12	5.7
Education levels	SPM/STPM/SIJIL	22	10.4
	Diploma	50	23.6
	Degree	94	44.3
	Masters	38	17.9
	PhD	5	2.4
	Others	40	18.9
Work Scope	Management	122	57.5
	Operation	90	42.5
Working experiences	< 1 year	4	1.9
	1 to 5 years	24	11.3
	6 to 10 years	40	18.9
	> 10 years	144	67.9

Using the Cronbach alpha value, coefficient values, relationship significance, and Pearson values, Table 4 displays the results for each variable. Cronbach's data validated its consistency. The Cronbach Alpha should be higher than 0.70, per [32]. Every Cronbach's alpha number in the table is greater than 0.823.

The Pearson analysis correlation value for 15 independent variables vs. one dependent variable is shown in Table 5. The correlation analysis results between each independent variable factor and the ICT Security Policy compliance model's dependent variable proposed at the start of the study are summarized in Table 5. Comparing two elements, two factors have a negative association with compliance intentions, whilst thirteen (13) aspects have a favorable correlation. 13 Intentions to comply are also significantly correlated with factors. In contrast, there was no discernible correlation between compliance intentions and Response Cost and Rewards. This is because, with values of 0.091 and 0.053, the significance level for the Response Cost and Rewards factors is higher than 0.05.

Table 5. Correlation value

Model	Factors		Cronbach Alpha Value	Coefficient value	Relationship	Pearson values
Protection Motivation Theory	Discerned Severity	F1	.869	Strong	Significant	.527
	Discerned Vulnerability	F2	.919	Strong	Significant	.515
	Maladaptive Rewards	*F3*	*.912*	*Very Weak*	*Significant*	*-.151*
	Response Efficacy	F4	.936	Strong	Significant	.555
	Self-Efficacy	F5	.868	Enough	Significant	.479
	Response Cost	*F6*	*.823*	*Very Weak*	*Not Significant*	*-.119*
Theory of Planned Behaviour	Attitude	F7	.903	Strong	Significant	.594
	Subjective Norm	F8		Enough	Significant	.327
	Discerned Behavioral Control	F9	.873	Strong	Significant	.592
Technology Acceptance Model	Discerned Usefulness	F10	.948	Strong	Significant	.525
	Discerned Ease of Use	F11	.849	Strong	Significant	.630
General Deterrence Theory	Rewards	F12	.825	Very Weak	Not Significant	.136
	Punishment	F13	.906	Enough	Significant	.333
Practice Theory	Awareness	F14	.896	Strong	Significant	.628
	Moral/Ethics	F15	.915	Strong	Significant	.735

The goals of General Deterrence Theory, Protection Motivation Theory, Theory of Planned Behavior, Technology Acceptance Model, and Practice Theory are used to categorize these Compliance Intention Factors (Table 6).

Table 6. Comparative analysis of selected theories/models

Theory	Overview	Strengths	Weaknesses	Citations
Practice Theory	Focuses on understanding actions based on cultural and social practices, emphasizing habitual activities and socially constructed norms.	- Captures the complexity of social contexts and habitual actions. - Focuses on the integration of behavior and social environment.	- Limited ability to predict individual behavior. - Hard to quantify or generalize due to its emphasis on qualitative data.	[33]
Technology Acceptance Model (TAM)	Explains why people accept technology, emphasizing the importance of discerned utility and ease of use.	- Simple and easy to apply across different technical contexts. - Highly adaptable to new and emerging technologies.	- Ignores external factors like social influence and environmental context. - Limited explanatory power beyond initial technology adoption.	[34-36]
Theory of Planned Behavior (TPB)	This implies that intentions, which are influenced by attitudes, subjective	- Strong predictive power for intention-driven behavior. - Can be applied across	- Overemphasizes rational decision-making. - Underplays the role of unconscious, habitual, or	[37-39]

	norms, and perceived behavioral control, are what motivate individual behavior.	diverse behavioral contexts (e.g., health, environment, technology).	automatic behaviors.	
Protection Motivation Theory (PMT)	Focuses on how people's assessments of threats (severity, vulnerability) and coping strategies (self-efficacy, reaction efficacy, and costs) influence their motivation to defend themselves.	- Incorporates both threat perception and coping strategies, making it comprehensive for health and security-related behaviors. - Well-supported in cybersecurity and health interventions.	- Can oversimplify the complexity of threat response in real-world settings. - Assumes rational cognitive processing of threats, which may not always be true.	[40, 41]
General Deterrence Theory (GDT)	Increases the discerned risk of punishment (e.g., certainty, severity, and swiftness of sanctions) in order to discourage unwanted conduct (e.g., crimes, security breaches).	- Effective for reducing harmful or non-compliant behaviors, particularly in security and legal frameworks. - Strong empirical support for its use in cybersecurity.	- Tends to focus too much on punishment and ignores factors like reward and reinforcement. - May be less effective in environments where compliance monitoring is low.	[42, 43]

The final ICT Security Policy Compliance model developed using the results is shown in Figure 1.

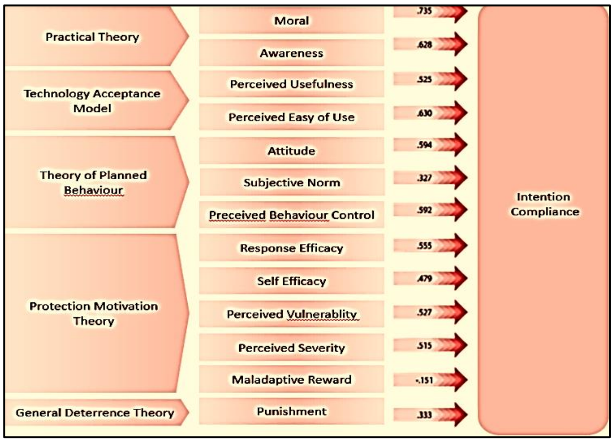

Fig. 1 ICT security policy intention compliance MODEL

Along with other elements that affect compliance intentions, this model suggests three (3) fundamental models. The following elements influence the desire to adhere to the ICT Security Policy and the comparison with earlier research:

The study discovered that, with a relationship strength value of 0.735, the moral element had the strongest correlation. These findings are consistent with a survey by [5], who discovered that these characteristics likewise yielded the strongest results out of all the criteria they looked at. At 0.628, the Awareness component, which is included in the same group, has the third-highest significance connection value. The idea that awareness affects intention compliance is supported by the strong connection strength value of the six (6) prior studies that have examined the awareness element. This clearly demonstrates the need to apply moral considerations and the consequences of violating or non-complying with established guidelines when raising awareness among employees, whether through speeches, briefings, or pamphlets. The rationale behind this is that moral education and Islamic education, which are subjects taught in Malaysian schools from an early age, are thought to improve adherence to the ICT Security Policy.

4.1. Technology Acceptance Model

The second-highest coefficient value component at 0.630 is discernible as ease of use. In the same fundamental model, discerned usefulness likewise gets a significant significance value of 0.525. These two elements have a high importance value for adherence to security regulations, according to earlier research in the literature review [14]. To apply Discerned Ease of Use aspects, ICT security policy development must eliminate jargon that makes security policy comprehension difficult. From the standpoint of discerned usefulness, employees should be consistently shown the benefits of adhering to the guidelines, such as productivity improvements and any other tangible values that could enhance employability.

4.2. Theory of Planned Behavior

The Attitude and Discerned Behavioral Control factors in this simple model have strong and nearly similar coefficient values of 0.594 and 0.592, respectively. The study [17] supports this value by demonstrating that all three of the model's components have a favorable effect on compliance intentions. Individual attitudes have been discovered to be influenced by knowledge in relation to the attitude component. As a model of alertness training that can modify the approach to obedience, the person in that situation needs to be constantly exposed to and monitored. The capacity to practice compliance within the framework of safety information and policies is another aspect of discerned behavioral control. Their capacity to exercise Discerned Behavioral Control is centered on their understanding of themselves and their ability to adhere to rules and regulations. In such a situation, if the nature of the threat or even the policy changes, notifications and briefings must be provided constantly. At 0.327, the coefficient of relationship for the third factor, the Subjective Norm, is sufficient. According to two Malaysian studies, [12] and [9], this component did not affect compliance intent and was significant. However, four other studies, primarily [16], found that this trait was the most important predictor of intention. Nevertheless, this study found that ICT security policies have an impact on the subjective norm, influencing people by informing them that, if top management adopts this as a work culture, employees have a duty to secure important corporate information assets.

4.3. Protection Motivation Theory

Five (5) of the six (6) components in the Protection Motivation Theory were found to have a substantial link with the desire to comply, or a coefficient value. Three factors have significant coefficient values: discerned vulnerability, discerned severity, and response effectiveness. Meanwhile, Maladaptive Rewards have weak and negative coefficient values, while Self-Efficacy has sufficient coefficient values. The Maladaptive Rewards component was left out of two earlier Malaysian studies [12, 19]. However, two global investigations [6, 13] have shown that the Maladaptive Rewards component has a similar negative intention value. According to the study [5, 13], these traits have no bearing on compliance intentions, and there is no meaningful correlation between compliance intentions and the Response Cost component. The components of this theory of protective motivation are separated into two (2) sections: threat assessment and coping response. People can enhance the threat assessment's components of maladaptive rewards, discerned vulnerability, and discerned severity if they have access to the most recent risk awareness and notification programs. It has components including the Self-Efficacy, Response Efficacy, and Coping Response. Self-efficacy is the capacity of an individual to follow the process. By limiting entry to adult websites and ensuring the efficacy of the reaction via guidelines on network firewall security, the person is guaranteed to respond to threats in this situation. These restraints should be clearly specified in the ICT Security Policy and any awareness-raising seminars or briefings.

4.4. General Deterrence Theory

Only the general deterrence theory's punishment component has a sufficient coefficient value of 0.333 regarding the intention to comply, out of the two components. This contrasts with earlier research that found both parameters had a positive intention value [9]. The ICT security policy implementer and top management should ensure that the suggested penalty for policy non-compliance is strong and can be executed immediately, for this study to have a satisfactory relationship value for the Punishment component. The objective is to ensure that people are committed to implementing the ICT security policy in practice.

5. Conclusion

This study included an analysis of the information gathered from 204 respondents via an online survey. According to SPSS statistical analysis, the conclusion that thirteen of the fifteen independent variable components had a substantial connection with the dependent variable is proven by a coefficient value of p less than 0.05. Exceptions are Response Cost and Rewards (2) independent variables due to their p-value being higher than 0.05. Therefore, the implementer of this policy must embrace Figure 2 characteristics listed in the ICT security policy compliance model to create a conducive environment that encourages ICT security policy compliance among Malaysian federal institutions.

The identified factors are Discerned Severity with Morals, Self-Efficacy, Response Efficacy, Maladaptive Rewards, Moral, Punishment, Awareness, Discerned Ease of Use, Discerned Utility, Discerned Behavioral Control, Subjective Norm, and Attitude, demonstrating the strongest correlation at 0.735. As the findings indicate, religious studies and moral education taught in elementary schools as potential influencing factors; ethical considerations ought to be given top priority when establishing an atmosphere that is consistent with the ICT security policy.

Funding Statement

This paper is the outcome of the Intelligent Connected Streetlights (ICS) research project work supported by the Renesas-Universiti Sains Malaysia (USM) external industry grant as per the MoA#A2021098 agreement with grant account no. [7304.PNAV.6501256.R128].

Acknowledgments

The authors would like to acknowledge staff and students from the Centre of Artificial Intelligence Technology, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), as well as the Cybersecurity Research Centre (CYRES), RCMO, and BJIM, Universiti Sains Malaysia (USM), for their full support, resulting in the publication of this paper.

References

[1] Fahad Mazaed Alotaibi et al., "A Novel Administration Model for Managing and Organising the Heterogeneous Information Security Policy Field," *Applied Sciences*, vol. 13, no. 17, pp. 1-18, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] Mampu, "General Circular Number 3 Year 200," *Pekeliling*, vol. 369, no. 1, pp. 1689-1699, 2000. [Publisher Link]

[3] Saqib Saeed, "Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia," *Sustainability*, vol. 15, no. 7, pp. 1-20, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Hussain Aldawood, and Geoffrey Skinner, "Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues," *Future Internet*, vol. 11, no. 3, pp. 1-16, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[5] Mansour Naser Alraja, Usman Javed Butt, and Maysam Abbod, "Information Security Policies Compliance in a Global Setting: An Employee's Perspective," *Computers & Security*, vol. 129, pp. 1-16, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Incidents Statistics, MyCert, Cybersecurity Malaysia, 2020. [Online]. Available: https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=3f99acd3-953d-463a-9018-bf5d85781124

[7] Efthymia Metalidou et al., "Human Factor and Information Security in Higher Education," *Journal of Systems and Information Technology*, vol. 16, no. 3, pp. 210-221, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[8] Anthony Vance, Mikko T. Siponen, and Detmar W. Straub, "Effects of Sanctions, Moral Beliefs, and Neutralization on Information Security Policy Violations across Cultures," *Information & Management*, vol. 57, no. 4, pp. 1-47, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[9] Faheem Ahmed Shaikh, and Mikko Siponen, "Information Security Risk Assessments Following Cybersecurity Breaches: The Mediating Role of Top Management Attention to Cybersecurity," *Computers & Security*, vol. 124, pp. 1-8, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Anthony Vance, Mikko Siponen, and Seppo Pahnila, "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," *Information & Management*, vol. 49, no. 3-4, pp. 190-198, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[11] Salvatore Aurigemma, and Raymond Panko, "A Composite Framework for Behavioral Compliance with Information Security Policies," *2012 45th Hawaii International Conference on System Sciences*, Maui, HI, USA, pp. 3248-3257, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[12] Abdullah Almuqrin et al., "Enforcing Information System Security: Policies and Procedures for Employee Compliance," *International Journal on Semantic Web and Information Systems*, vol. 19, no. 1, pp. 1-17, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Janine L. Spears, and Henri Barki, "User Participation in Information Systems Security Risk Management," *MIS Quarterly*, vol. 34, no. 3, pp. 503-522, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[14] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly*, vol. 34, no. 3, pp. 523-548, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[15] Sushma Mishra, and Gurpreet Dhillon, "Information Systems Security Governance Research: A Behavioral Perspective," *1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference*, New York, USA, pp. 18-26, 2006. [Google Scholar]

[16] Benedikt Lebek et al., "Employees' Information Security Awareness and Behavior: A Literature Review," *2013 46th Hawaii International Conference on System Sciences*, Wailea, HI, USA, pp. 2978-2987, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[17] Sadaf Hina, Dhanapal Durai Dominic Panneer Selvam, and Paul Benjamin Lowry, "Institutional Governance and Protection Motivation: Theoretical Insights into Shaping Employees' Security Compliance Behavior in Higher Education Institutions in the Developing world," *Computers & Security*, vol. 87, pp. 1-42, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] Farkhondeh Hassandoust, and Angsana A. Techatassanasoontorn, *Chapter 7 - Understanding Users' Information Security Awareness and Intentions: A Full Nomology of Protection Motivation Theory*, Cyber Influence and Cognitive Threats, Academic Press, pp. 129-143, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Ahmad Al-Omari, Omar El-Gayar, and Amit Deokar, "Security Policy Compliance: User Acceptance Perspective," *2012 45th Hawaii International Conference on System Sciences*, Maui, HI, USA, pp. 3317-3326, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[20] Philip Menard, Gregory J. Bott, and Robert E. Crossler, "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory," *Journal of Management Information Systems*, vol. 34, no. 4, pp. 1203-1230, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[21] Waleed Al-Ghaith, "Extending Protection Motivation Theory to Understand Security Determinants of Anti-virus Software Usage on Mobiles Devices," *International Journal of Computers*, vol. 10, pp. 125-138, 2016. [Google Scholar] [Publisher Link]

[22] Eunice Kim et al., "Predicting Selfie-Posting Behavior on Social Networking Sites: An Extension of Theory of Planned Behavior," *Computers in Human Behavior*, vol. 62, pp. 116-123, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[23] Kim-Kwang Raymond Choo et al., "Employees' Intended Information Security Behaviour in Real Estate Organisations: A Protection Motivation Perspective," *Americas' Conference on Information Systems (AMCIS)*, pp. 1-11, 2015. [Google Scholar] [Publisher Link]

[24] Nader Sohrabi Safa et al., "Information Security Conscious Care Behaviour Formation in Organizations," *Computers & Security*, vol. 53, pp. 65-78, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[25] Bartlomiej Hanus, and Yu "Andy" Wu, "Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective," *Information Systems Management*, vol. 33, no. 1, pp. 2-16, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[26] Princely Ifinedo, "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory," *Computers & Security*, vol. 31, no. 1, pp. 83-95, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[27] Edgar Erdfelder, Franz Faul, and Axel Buchner, “GPOWER: A General Power Analysis Program,” *Behavior Research Methods, Instruments, & Computers*, vol. 28, pp. 1-11, 1996. [CrossRef] [Google Scholar] [Publisher Link]

[28] Franz Faul et al., “G*Power 3: A Flexible Statistical Power Analysis Program for the Social, Behavioral, and Biomedical Sciences,” *Behavior Research Methods*, vol. 39, pp. 175-191, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[29] Mark N.K. Saunders, Philip Lewis, and Adrian Thornhill, *Research Methods for Business Students*, 7th ed., Pearson Education, pp. 1-768, 2016. [Google Scholar] [Publisher Link]

[30] George A. Johanson, and Gordon P. Brooks, “Initial Scale Development: Sample Size for Pilot Studies,” *Educational and Psychological Measurement*, vol. 70, no. 3, pp. 394-400, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[31] Kakali Bhattacharya, *Fundamentals of Qualitative Research: A Practical Guide*, 1st ed., Routledge, pp. 1-220, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[32] Darren George, and Paul Gallery, *IBM SPSS Statistics 23 Step by Step: A Simple Guide and Reference*, 14th ed., pp. 1-400, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[33] Amirali Faridi et al., “Adoption of Water and Soil Conservation Practices: Theoretical Frameworks and Attitudinal Components,” *AGROFOR International Journal*, vol. 5, no. 2, pp. 5-14, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[34] Dana Rad et al., “A Radial Basis Function Neural Network Approach to Predict Preschool Teachers’ Technology Acceptance Behavior,” *Frontiers in Psychology*, vol. 13, pp. 1-11, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[35] Insook Cho, “Frameworks for Evaluating the Impact of Safety Technology Use,” *Healthcare Informatics Research*, vol. 29, no. 2, pp. 89-92, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[36] Eiman Negm, “Internet of Things (IoT) Acceptance Model – Assessing Consumers' Behavior toward the Adoption Intention of IoT,” *Arab Gulf Journal of Scientific Research*, vol. 41, no. 4, pp. 539-556, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[37] Meggy Hayotte et al., “The French eHealth Acceptability Scale Using the Unified Theory of Acceptance and Use of Technology 2 Model: Instrument Validation Study,” *Journal of Medical Internet Research*, vol. 22, no. 4, pp. 1-11, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[38] Samar Rahi, “What Drives Citizens to get the COVID-19 Vaccine? The Integration of Protection Motivation Theory and Theory of Planned Behavior,” *Journal of Social Marketing*, vol. 13, no. 2, pp. 277-294, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[39] Reny Nadlifatin et al., “The Measurement of University Students’ Intention to Use Blended Learning System through Technology Acceptance Model (TAM) and Theory of Planned Behavior (TPB) at Developed and Developing Regions: Lessons Learned from Taiwan and Indonesia,” *International Journal of Emerging Technologies in Learning*, vol. 15, pp. 219-230, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[40] I. Al-Shanfari et al., “Determinants of Information Security Awareness and Behaviour Strategies in Public Sector Organizations among Employees,” *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 8, pp. 479-490, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[41] Hamidreza Shahbaznezhad, Farzan Kolini, and Mona Rashidirad, “Employees’ Behavior in Phishing Attacks: What Individual, Organizational and Technological Factors Matter?,” *Journal of Computer Information Systems*, vol. 61, no. 6, pp. 539-550, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[42] Nisreen Ameen et al., “Employees’ Behavioural Intention to Smartphone Security: A Gender-Based, Cross-National Study,” *Computers in Human Behavior*, vol. 104, pp. 1-35, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[43] Puspadevi Kuppusamy et al., “Systematic Literature Review of Information Security Compliance Behaviour Theories,” *Journal of Physics: Conference Series: 2nd International Conference on Recent Advancements in Science and Technology*, Putrajaya, Malaysia, vol. 1551, pp. 1-14, 2020. [CrossRef] [Google Scholar] [Publisher Link]