Penerbit
Akademia Baru

Journal of Advanced Research in Social and Behavioural Sciences
ISSN (online): 2462-1951 | Vol. 2, No. 1. Pages 49-74, 2016

Technology Ethics Attributes in Handling Confidential Information for the Armed Forces

N. A. Zakaria[*,a] *and Z. Ismail*[b]

Advanced Informatics School, Universiti Teknologi Malaysia, 54100 Kuala Lumpur, Malaysia

[a,*]*nazreen9@live.utm.my*, [b]*zurainiismail.kl@utm.my*

Abstract – *The scarcity of technology ethics awareness particularly in Armed Forces personnel practises in handling confidential information remain of utmost concerns. This research aims to identify technology ethics attributes in handling confidential information for the Armed Forces. This is executed by designing technology ethics model and evaluating the proposed model. 121 questionnaires were distributed to personnel in Royal Signal Regiment (RSR) Corp of the Malaysian Armed Forces (MAF) from Sergeant to Major in rank. Using SPSS version 20 analysis revealed that the correlation between the identified attributes namely security and privacy, autonomy, code of ethics, legal, accuracy and safety showed significant with moderate to strong positive. Accuracy reads the highest correlation with 76.9%, which may be due to personnel concerns on organisation's information sensitivity along with skills and knowledge equipped which portrayed their preciseness in decision making while handling confidential information. However, safety showed the lowest correlation of 31.4% while its regression reveals 9.9%. The overall regression analysis predicts 72.9% variations. This suggests personnel are excessive reliance with organisation's benefactor safety while ignoring the importance of individual safety in managing the information they encountered. This research may assist the Armed Forces in securing practises acquired in handling organisation's valuable assets which requires special guardianship towards its perseverance.*

Keywords: Confidential information, Technology ethics, Security and privacy, Autonomy, Code of ethics, Legal, Accuracy, Safety, Factor analysis, reliability, correlation, regression

1.0 INTRODUCTION

The rapid technology advancement has no doubt has been assisting people in many ways. Apart from that, the impact of the technology towards the Information and Communications Technology has transformed the working culture in the organisation. The existence of various technologies and operating systems platform have opened opportunities compromising security which demanded the paramount in storing and disseminating the confidential information limitation in order to provide an effective control [1]. Hence, the requirements are significance due to the role of Ministry of Defence itself which has given the responsibility and faith towards the safety and national defence. In addition, the technology being handled need to be safe from any mishandling that could invite invasion from any possible threats and contaminate the confidential information jeopardising organisation's reputation.

Organisations should identify the effective way of handling the different levels of organisations' documentations confidentiality which allotting the differences of "public", "confidential", "highly confidential", and "restricted" [2]. Accordingly, information needs to be organised delicately in terms of getting consent with proper guidelines to dispose and bring information outside the organisation. In response to this trend, organisations have generally employed various controls and employment measures. Likewise, Armed Forces' organisation believed that special concerned on all types of information they have desired an appropriate handling as to preserve its confidentiality. As the field success of modern military is depending on the reliability of communication, yet technology used is equally important in handling high data rates [3].

The shift in modern security is towards the human centred process [3] whereby social aspect of ethical affairs has played a major role since social and human discourse portrayed the root of the action assessment [4]. Therefore, the good judgement of ethical assessment along with the confidential information handling in the world of technologies should be aligned as the computer misemployment and corruption will continue to increase in the future [5]. The absence of those intended elements will increase the personnel chances to do the unethical work with the technology they possess. Simultaneously, personnel could face the degradation of interest, lose of power, and their positions placement in the society [6]. In other perspective, the view on the mischief of the confidential information handling has driven to threats emergence. Organisational threats as described by Samy *et al.* [7] is the acts of human failure in handling the storage of data or classified information in unprotected areas by staff. These findings are being strengthened by [4] in its annual security report on organisation's data protection. Undeniably, the current threat landscapes in security is the augmenting pressure to protect terabytes of information, as it is stated as the top concerns from the Chief Information Security Officers survey [4].

From the MAF aspects, there have been situations that have triggered to the development of technology ethics in handling confidential information. There were initially four main manifestations of threats to the MAF security which as allotted in Secretariat, A. [8] which are subversion where the personnel loyalty has diverted, espionage by performing clandestine and unlawful act of acquiring information, sabotage used by grudge against authority personnel and human failings that lead to security breaches to the unauthorised hands because of negligence to security instruction. At present, the rise of Islamist militant group, Islamic State in Iraq and Syria has struck a significance concern among leaders specifically in MAF which signified the subversion threats involving the MAF. It is seem as the deliberate threats in which the modus operandi used the cyber medium to spread the idealism among MAF personnel of the concept of jihad by spreading pictures and videos of Muslims' persecution and murders around the world [9]. The concern towards the MAF security threats is reflected in this kind of involvement whereby extremist always try to widen the chances of new recruitments and MAF personnel are of favour as they were equipped with skills required by the group to expedite its activities unlike civilian that need to be trained. Among them are skills in weapon handling, bomb experts, tactical experts, and doctrine disclosure experts. These subversive threats scenario of Islamic State could be further lead the MAF personnel to be tackled with sabotage threats by using cyber platform as the medium which might lead the espionage threats from the foreign intelligence organisations to further strengthen their surveillance over MAF security using the information exposure by the irresponsible personnel. On top of that, there is a pressing requirement for the MAF personnel to instil the technology ethics to assure a correct handling of the MAF confidential information.

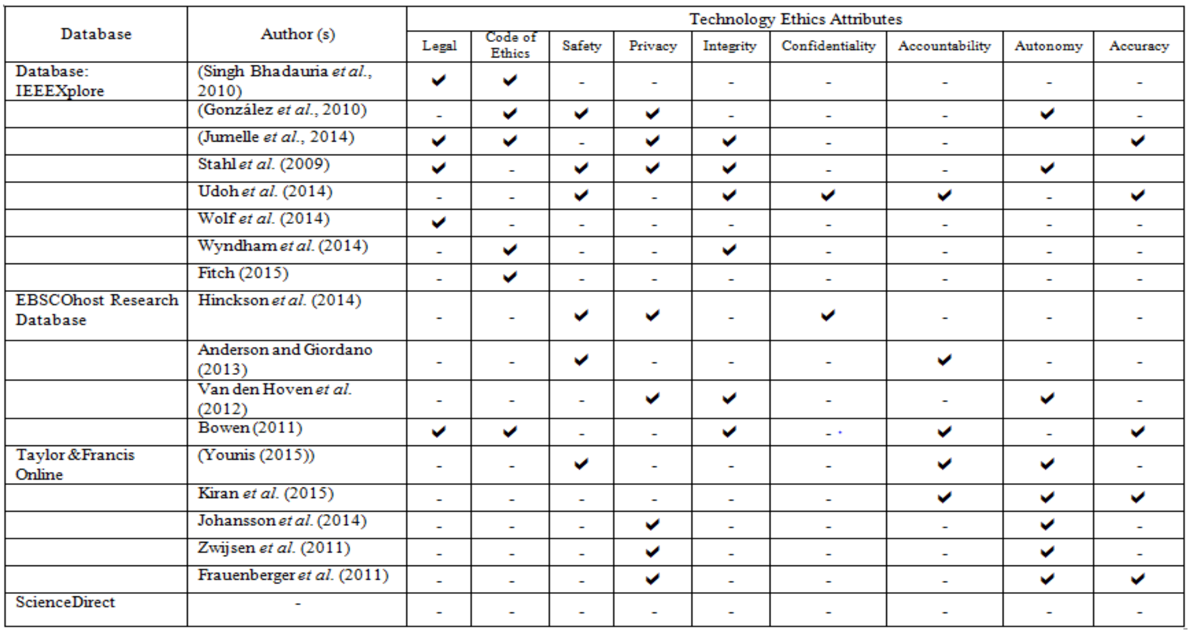
In MAF, the freedom of access in cyber platform which resulted from technologies proliferation through mobile network, internet or even static network for instance via smart phone, personal digital assistant, and laptop have subsequently contribute to the profound effect on the confidential information contamination and its security. The MAF is struggling to achieve information superiority title due to the technology advancement. This may be difficult to accomplish as the personnel disrespect the handling of confidential information by not taking serious compliances in its preservation. Instead of the effort in prohibiting the threats, exploitation and the outsider intervention, the internal elements of the insider threats is seem to be the largest contributor to the confidential information leakage to the outside world due to the personnel mishandling [10]. To date, the MAF sees the importance of ethics in using the technologies provided with the critical needs in conserving the confidential information. Therefore, the objectives of this research are to identify the technology ethics attributes in handling confidential information, to design and evaluate the technology ethics model in handling confidential information for the Armed Forces.

2.0 RELATED WORKS

2.1 Systematic Literature Review

The Systematic Literature Review (SLR) results to 9 attributes of the technology ethics derived from 17 studies derived as presented in Table 1. The identified attributes of technology ethics served as the attributes to be inserted in the proposed conceptual model.

Table 1: Systematic Literature Review Results



Database	Author (s)	Technology Ethics Attributes								
		Legal	Code of Ethics	Safety	Privacy	Integrity	Confidentiality	Accountability	Autonomy	Accuracy
Database: IEEEXplore	(Singh Bhadauria *et al.*, 2010)	✓	✓	-	-	-	-	-	-	-
	(González *et al.*, 2010)	-	✓	✓	✓	-	-	-	✓	-
	(Jumelle *et al.*, 2014)	✓	✓	-	✓	✓	-	-		✓
	Stahl *et al.* (2009)	✓	-	✓	✓	✓	-	-	✓	
	Udoh *et al.* (2014)	-	-	✓	-	✓	✓	✓	-	✓
	Wolf *et al.* (2014)	✓	-	-	-	-	-	-	-	-
	Wyndham *et al.* (2014)	-	✓	-	-	✓	-	-	-	-
	Fitch (2015)	-	✓	-	-	-	-	-	-	-
EBSCOhost Research Database	Hinckson *et al.* (2014)	-	-	✓	✓	-	✓	-	-	-
	Anderson and Giordano (2013)	-	-	✓	-	-	-	✓	-	-
	Van den Hoven *et al.* (2012)	-	-	-	✓	✓	-	-	✓	-
	Bowen (2011)	✓	✓	-	-	✓	-	✓	-	✓
Taylor &Francis Online	(Younis (2015))	-	-	✓	-	-	-	✓	✓	-
	Kiran *et al.* (2015)	-	-	-	-	-	-	✓	✓	✓
	Johansson *et al.* (2014)	-	-	-	✓	-	-	-	✓	-
	Zwijsen *et al.* (2011)	-	-	-	✓	-	-	-	✓	-
	Frauenberger *et al.* (2011)	-	-	-	✓	-	-	-	✓	✓
ScienceDirect	-	-	-	-	-	-	-	-	-	-

2.1.1 Legal Attribute

Legal is always referred to the adherence to the compliance with the predetermined standard and justice. Singh Bhadauria *et al.* [11] concerned on the benefits of global information technology processes such as e-Commerce and e-Business can be achieved with the presence of agreed level of legal certainty and uniformity that reflects the trust in the transaction. Jumelle *et al.* [12] addressed that cross boundary harmonisation in which legal challenges are stipulated with regards to a cross-cultural perspective which further supported by Wolf *et al.* [13]. He defined that the usage of the technology may raise ethical issues if the status in the boundary is not legal. However it varies over countries. Stahl *et al.* [14] viewed that the external governance on legal compliance is needed for the processes and procedures on the systems as well as procedures for dual use both military and terrorist application with the inclusion of social and political. Udoh *et al.* [15] mentioned that the implication of engineering activities should respect legal or state rules in order to keep high moral standard which established the common ground between ethics and legal that highlighted the interconnection of judicial standard acknowledgment, human life protection and environment preservation. Bowen [16] signifies that the expression in terms of law should be withstood as a long term result, in the sense that such respect underlay great protection since activities consequences varies and extensive in both place and time. Hence, it can be hypothesised that:

H1: Legal attribute has a positive relationship with Technology Ethics in Handling Confidential Information.

2.1.2 Code of Ethics Attribute

In the studies, Kanungo and Mendonca [17] stated that codes of ethics establish ethical principles that governs decisions and behaviour towards the accomplishment of the task while uplifting the moral climate. It was found that the usability of the codes of ethics are often seen as an engaging the ethical behaviour. Singh Bhadauria *et al.* [11] have seen that the codes of ethics allow some mutual trust in business transactions, thus the workgroup's ethical behaviour is likely to be influenced by the business organisation's formal and informal ethical practices with the perspective of regional political morality. Codes of ethics are viewed in leveraging towards safeguarding the right of human participants as stated in González *et al.* [18]. In a study by Jumelle *et al.* [12] stated that the presence of codes of ethics might help in standardising the reliability of health and medical information published on the sites which in this particular footing has employed the code certification that lays an ethical standard aimed at ensuring that health and medical information is correct, transparent, useful, and objectively supersede, while Wyndham *et al.* [19] indicated the need of the codes of ethics in reflecting the codes of procedures is strictly to be adhered in the major event of investigation operation which is scientifically vigorous and intact with the overlying code of conduct. While in other view such as by Fitch [20] which has incorporated the attributes of innovation of infrastructure and medical collaboration acquires the responsibility culture ventures which have been emphasised in the code of conduct which covers the sensitive main issue of privacy and life quality. Lee, M. and Lai, C. [21] asserted that strong identity and professional commitment characteristics are needed to be a quality professional. Bowen [16] further deliberated that any deliverable consequences demanded that it is justifiable and professional should harmonise the respect for life, for the law, and the public in accomplishing the desirable aftermath. Therefore, a hypothesis can be formulated as:

H2: Code of ethics attribute has a positive relationship with Technology Ethics in Handling Confidential Information.

2.1.3 Safety Attribute

The safety attribute generally means protection in any condition from any undesirable emanations. González *et al.* [18] highlighted the issue and demonstrated the sufficient transparency for the operative robustness indicator while Udoh *et al.* [15] have set forth the needs of competence level to be polished while resisting on the incompetence fields assigned to hinder any severe damages to the business and specifically to the society rather than to worry on jeopardising its reputation. Hinckson *et al.* [22] encouraged the storage of the data to be stored in predetermined period in the most secured way. Anderson and Giordano [23] on the other hand sees the self-equipped is needed in discovering problems generated by the use of the technology. Younis [24] associated the concerned on the ever increasing treacherous criteria over the number of development growth which has raised ethical reconsideration of the associated arguments as well as their short and long term impact of the activities. Consequently, a hypothesis can be codified as:

H3: Safety attribute has a positive relationship with Technology Ethics in Handling Confidential Information.

2.1.4 Privacy Attribute

Privacy is frequently seen as the state of not being disrupted by unintended parties. In a study by González *et al.*[18] stated that the violation of privacy may occurs because of the constant monitoring which could happened because of the unwillingness of sharing and providing the data to other entities of system or services. Stahl *et al.* [14] stressed on the governance of ethical reviews to be part of scientific review on privacy along with data protection on the employment of the new technologies which is also the case for sensitive trend operational validation. Stahl *et al.* [14] further extended the privacy in term of informed consent which also emphasised in Jumelle *et al.* [12], Hinckson *et al.* [22] as well as Frauenberger *et al.* [25], all in respective ways of presenting. Stahl *et al.* [14] have stressed on the governance of processes together with procedures to have an informed consent. Hinckson *et al.* [22] stressed the informed consent from the owner in terms of data collection activities. Frauenberger *et al.* [25] represented it in terms of the atonement of the ultimate objectives which should be fairly carried out and be informed to the concerned parties prior to the beheading intention while Jumelle *et al.* [12] informed their consent involved the owner's confidential data and to be adequately informed with the free choices of consent channel which are through paper or online form. Through online, people might be reluctant or give uninformed consent as they think that there might have some fraud risk. Extending from the studies, Jumelle *et al.* [12] followed the set of quality criteria by European Commission's (2002) action plan which is relevant to the technologies and applications that depicted the trust and privacy. Van den Hoven *et al.* [26] presented in his study that the deliverable designation would have to preserve the privacy in the adaptation accordance to value sensitive design. It differs from Johansson *et al.* [27] which emphasised the violation of privacy is allowed if the case would alleviate the suffers along with sound procedures practices. The opposed of privacy term also contradicted in Zwijsen *et al.* [28] which the study identifies varying terms with regard to privacy and implied that safety are much more desirable and people felt the privacy is not being opposed in the requirement-served basis. Henceforth, the formulated hypothesise can be proposed that:

H4: Privacy attribute has a positive relationship with Technology Ethics in Handling Confidential Information.

2.1.5 Integrity Attribute

Integrity is often described as being honest and trustworthy. It is further justified by Becker [29] through the synonyms of the words: integrity, honesty, and conscientiousness are often not differentiated and tend to be used as interchangeable terms without an introduction or further consideration. Jumelle *et al.* [12] identified the needs of ethics in virtualisation whereby users' interaction with computing resources in multiple operating systems that runs virtually cannot be determined and thus requires integrity. Stahl *et al.*[14] stated that the responsive trends of operational validation require data protection and trust. Udoh *et al.* [15] displayed the commitment of an engineer to perform duties with integrity and honesty which uphold the uprightness of the right platform in presenting the works.Wyndham *et al.* [19] encouraged integrity in the sense of honest investigation which is further relates in the real safety precautions from calamity.Van den Hoven *et al.* [26] assumed that the innovation is needed to be biased-free as it reflects the anticipation of moral values prior to the development. Bowen [16] stated that the professional needs to fertilise and stand firm with integrity and honesty albeit of varying business standards and cultures. As a deduction, it can be hypothesise that:

H5: Integrity attribute has a positive relationship with Technology Ethics in Handling Confidential Information.

2.1.6 Confidentiality Attribute

The confidentiality derivation can be described as a limitation or restriction. Confidential information must be kept confidential and rigorously almost in all prospects as the breach of confidentiality may cause a serious implication towards the business and self reputation and will bring down the built trust which is hard to tie again over scepticism as being urged by Udoh *et al.* [15]. The availability of sensitive data is required to be kept private and confidential and access is only given to limited and recognised parties only [22]. From here, the given hypothesis is that:

H6: Confidentiality attribute has a positive relationship with Technology Ethics in Handling Confidential Information.

2.1.7 Accountability Attribute

The responsibility is always associated with the accountability that is when Udoh *et al.* [15] identified accountability in his study, it should be inculcated as one of the engineers' commitment as the effect of the modern technology they are responsible for. The work operated is should be held responsible in every impact of circumstances initiated afterwards as stated in Anderson and Giordano [23]. The professionals' credibility kept getting acknowledgment from the society as the decision made upon each situation is to be encountered tremendously. As stated in Bowen [16] cited in Kiran *et al.* [30] depicted the sense of accountability would project one's imagination in conveying the technology in its desirable manner. Younis [24] stated that to have a centralised planning responsibility should be in accordance to the authority bodies, as they will have to conserve the issues at raise. On that account, it can be hypothesise that:

H7: Accountability attribute has a positive relationship with Technology Ethics in Handling Confidential Information.

2.1.8 Autonomy Attribute

Many of the studies describe the importance of autonomy as the freedom in self governance. The findings in González *et al.* [18] reflected that the technology employed should respect the user freedom of choice so that any inconvenience should be stated clearly, respire for justice and beneficence for life, and thus, the existence of unnoticeable technology placement would help to maintain dignity rather than to make the availability of the technology much more obvious. It is supported by Frankel and Siang [31] in which protecting human subjects rest on the principles of autonomy, that subjects should be treated with respect as autonomous agents and affirms that those persons with diminished autonomy are entitled to special protection that involves maximising possible benefits and good for the subject, while minimising the amount of possible harm, risks and justice which seeks a fair distribution of the burdens and benefits associated. Furthermore, Stahl *et al.* [14] stated that the respect towards autonomy is acquires for the intuitive trend of operational validation. Van den Hoven *et al.* [26] viewed the self governance is expected to be in practised correctly parallel with the values of moral in ethical perspective, whereas the development of the design is to be incorporated with moral values prior to ethical perspectives in the approach of value sensitive design as the primary objective among other major values. Thus the studies regarded ethics as an important element from the deliverable. Human centred-rights are moulded in the pertinent approach in protecting the human values resulted from moral values. Kiran *et al.* [30] further added that technology usability is not limited to its development but the sovereignty in technology handling itself needs to be reflected with the interrelation of ethics. Younis [24] valued that ethical decision in scrutinising the adherence of ethical leadership to preserve and protected the subject of interest while in this case the economy and citizens. Autonomy analogous in the Johansson *et al.* [27] as a specified features and situation will evoke the desirable, problematic, or neutral reflection of the ethics whereby Panatik,S. [32] emphasised that creativity output is driven by taking account on others' perceptions, measurement of creative potential and possible objective measures of creative output.. Zwijsen *et al.* [28] stated that as there are few debates in the advantage as well as the disadvantages of the autonomy rights following the technology usage as some said the technology itself would undermined the freedom of the users as the benefit that the technology brought rather than the remnants effect after all. These however should be based on direct or indirect affect of the technology on people and how one's reflected the independence or freed themselves. Frauenberger *et al.* [25] identified that improper installation guidelines would interfere the freedom of maltreatment parties. From these, the hypothesis can be expressed as:

H8: Autonomy attribute has a positive relationship with Technology Ethics in Handling Confidential Information.

2.1.9 Accuracy Attribute

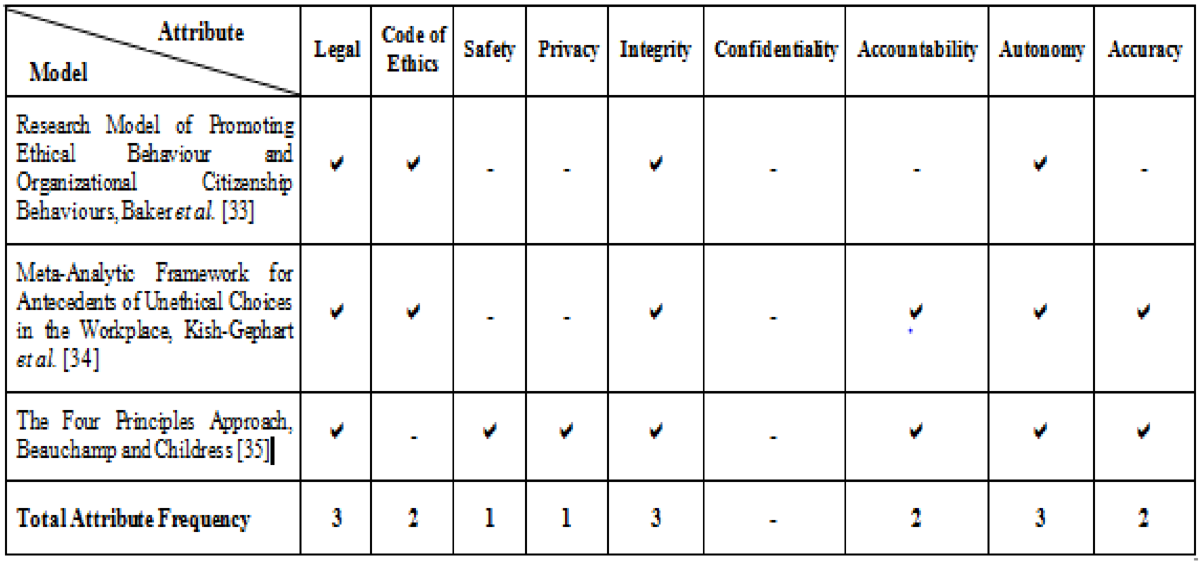
Accuracy brings the understanding of being precise. In Jumelle *et al.* [12] study on the accuracy, it can be defined in terms of equity and accessibility of socio demographic inequalities: computer and health literacy of quality and cost are addressed. Udoh *et al.* [15] and Bowen [16] desired the accuracy commitment of professionals in performing duties and the need of fully vital skills and knowledge in determining the accuracy and rigorousness of the acquired task to be accomplished respectively. Information channelling disseminated by the technologies would contribute to the great effects in building the confidence level due to its accuracy as stated in Kiran *et al.* [30] studies. Other than that, Frauenberger *et al.* [25] emphasised on the approach selection that should be meticulously considered which signifies the explicit need of the group. To that end, a hypothesis can be mapped as:

H9: Accuracy attribute has a positive relationship with Technology Ethics in Handling Confidential Information.

2.2 Summary of Related Attributes

Baker *et al.* [33] research model titled as 'Promoting Ethical Behaviour and Organisational Citizenship Behaviours' as well as, 'Meta-Analytic Framework for Antecedents of Unethical Choices in the Workplace' by Kish-Gephart *et al.* [34] together with, 'The Four Principles Approach' by Beauchamp and Childress [35], identified in literature review are mapped accordingly with the nine attributes gathered in the SLR outcomes. The summary of related variables derived is depicted in Table 2. It serves as the baseline to proceed with the development of the proposed conceptual model of technology ethics in handling confidential information.

Table 2: Summary of Related Variable

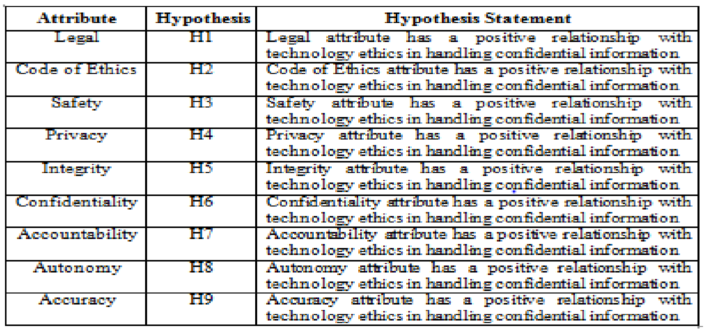


Attribute / Model	Legal	Code of Ethics	Safety	Privacy	Integrity	Confidentiality	Accountability	Autonomy	Accuracy
Research Model of Promoting Ethical Behaviour and Organizational Citizenship Behaviours, Baker *et al.* [33]	✓	✓	-	-	✓	-	-	✓	-
Meta-Analytic Framework for Antecedents of Unethical Choices in the Workplace, Kish-Gephart *et al.* [34]	✓	✓	-	-	✓	-	✓	✓	✓
The Four Principles Approach, Beauchamp and Childress [35]	✓	-	✓	✓	✓	-	✓	✓	✓
Total Attribute Frequency	**3**	**2**	**1**	**1**	**3**	**-**	**2**	**3**	**2**

2.3 Proposed Conceptual Model

All nine technology ethics attributes represented the pertinent hypothesises emerged in this chapter under the Attributes that Effect Technology Ethics' section are further highlighted in the proposed conceptual model in terms of H which denotes the hypothesis. The summary of the list of attribute and hypothesis is depicted in Table 3.

Table 3: Summary of Attributes and Hypothesises



Attribute	Hypothesis	Hypothesis Statement
Legal	H1	Legal attribute has a positive relationship with technology ethics in handling confidential information
Code of Ethics	H2	Code of Ethics attribute has a positive relationship with technology ethics in handling confidential information
Safety	H3	Safety attribute has a positive relationship with technology ethics in handling confidential information
Privacy	H4	Privacy attribute has a positive relationship with technology ethics in handling confidential information
Integrity	H5	Integrity attribute has a positive relationship with technology ethics in handling confidential information
Confidentiality	H6	Confidentiality attribute has a positive relationship with technology ethics in handling confidential information
Accountability	H7	Accountability attribute has a positive relationship with technology ethics in handling confidential information
Autonomy	H8	Autonomy attribute has a positive relationship with technology ethics in handling confidential information
Accuracy	H9	Accuracy attribute has a positive relationship with technology ethics in handling confidential information

The technology ethics attributes identified as well as the hypothesises as listed are then being projected to construct the proposed conceptual model of technology ethics in handling confidential information as presented in Figure 1 below.

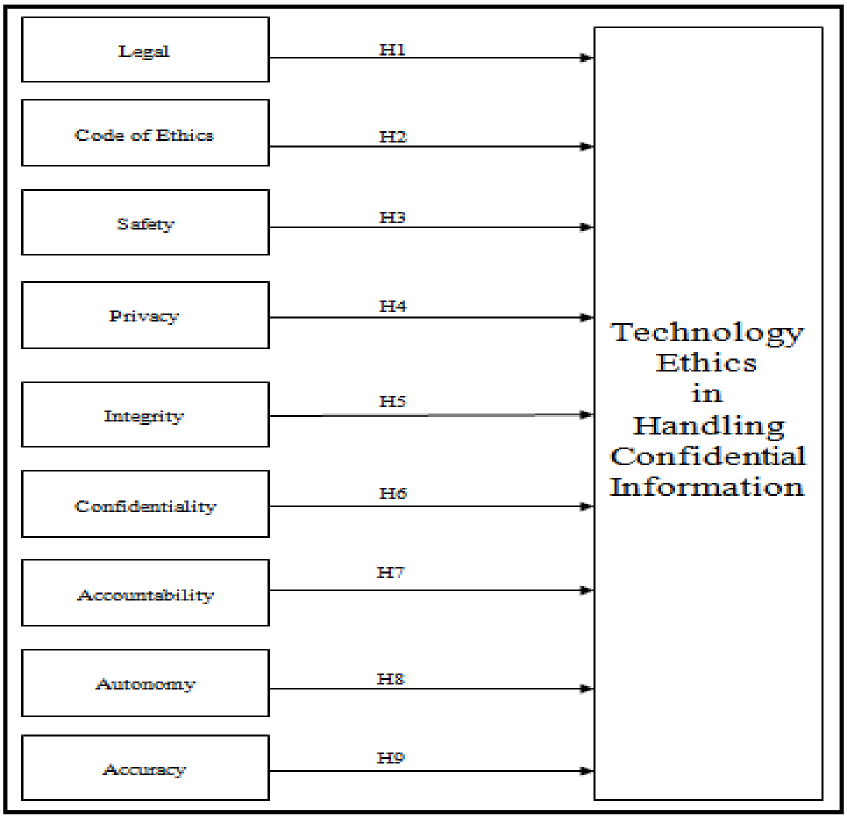


Figure 1: Proposed Conceptual Model for Technology Ethics in Handling Confidential Information for the Armed Forces

3.0 METHODOLOGY

The research operational framework comprises of 5 phases as shown in Figure 2. Each phase describe the activities involved.

3.1 Information Gathering and Project Planning

This phase comprises of two stages; i) performing the preliminary investigation by conducting the literature review from the related fields, and ii) preliminary interview conducted with selected personnel in gathering their experiences. This helps the researcher in finding the gap exists in the current researches field. It helps the derivation of the technology ethics attributes served as the input for the model designation on the next stage.

3.2 Design

There are two parts involved in this phase. The first part presented the development of the proposed conceptual model of technology ethics in handling confidential information which is constructed based on the results of the SLR. The second part continued with the questionnaire development. Questionnaire structure is to provide a self-determining and neutral evaluation of how the personnel grasp the practises of the technology ethics in their daily routine in handling confidential information. In pursuance, a set of questions are established that reflect the technology ethics attributes in handling confidential information in which the constructs are making use of the extracted attributes findings from the SLR's results related statement, the available questionnaires used by other researchers together with other researchers' statements to accommodate the development of the questionnaire.

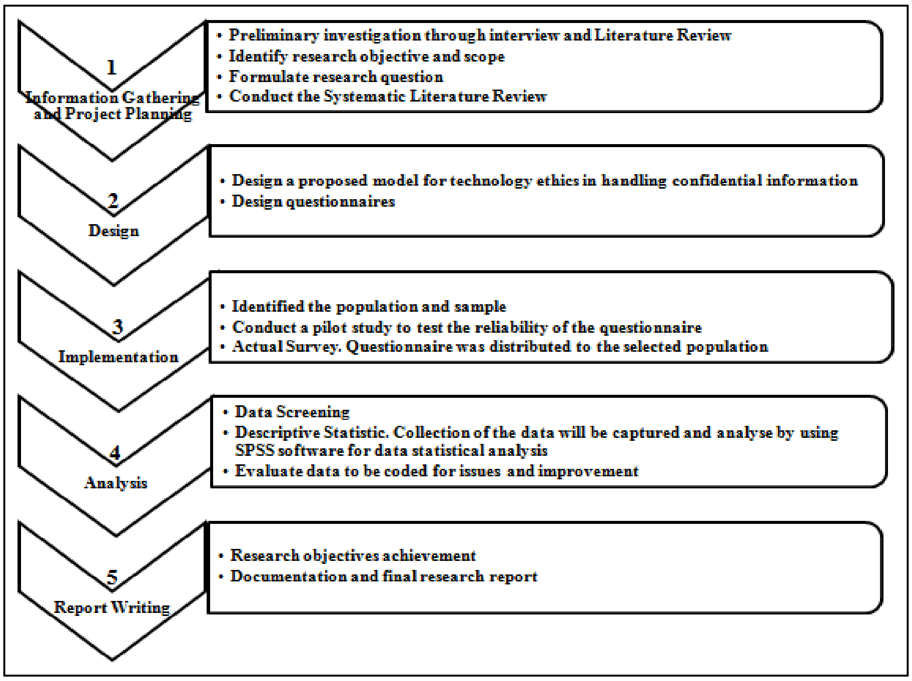

1
Information Gathering and Project Planning
• Preliminary investigation through interview and Literature Review
• Identify research objective and scope
• Formulate research question
• Conduct the Systematic Literature Review
2
Design
• Design a proposed model for technology ethics in handling confidential information
• Design questionnaires
3
Implementation
• Identified the population and sample
• Conduct a pilot study to test the reliability of the questionnaire
• Actual Survey. Questionnaire was distributed to the selected population
4
Analysis
• Data Screening
• Descriptive Statistic. Collection of the data will be captured and analyse by using SPSS software for data statistical analysis
• Evaluate data to be coded for issues and improvement
5
Report Writing
• Research objectives achievement
• Documentation and final research report

Figure 2: Research Operational Framework

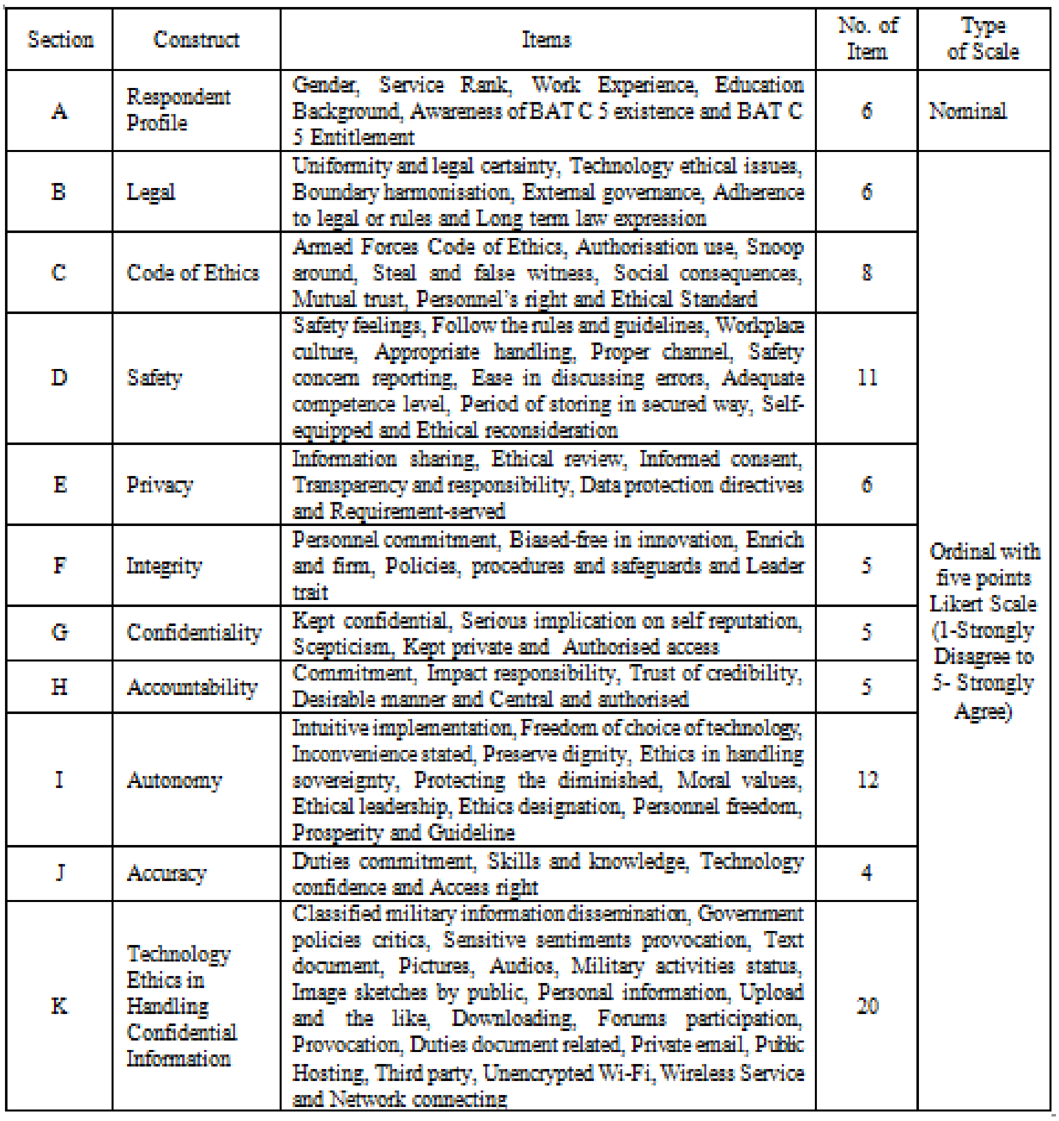
3.2.1 Variables and Measurements

The questionnaire design structure as in Table 4 consists of ten sections starting with section A on the respondents' profile where the questionnaire began, followed by section B on Legal, section C on Code of Ethics, section D on Safety, section E on Privacy, section F on Integrity, section G on Confidentiality, section H on Accountability, section I on Autonomy, section J on Accuracy, and Section K on Technology Ethics in Handling Confidential Information. Five point Likert Scale is used from section B until section K which denotes "strongly disagree" for scale 1, "disagree" for scale 2, "neutral" for scale 3, "agree" for scale 4, and "strongly agree" for scale 5.

3.3 Implementation

In this phase, there are several steps involving the population and sample design, formulating the questionnaires. Pilot study was conducted to revise the questionnaire and to distribute the corrected version of the questionnaire. The correct questionnaire will be distributed to the respondents identified at this stage.

Table 4: Questionnaire Design Structure



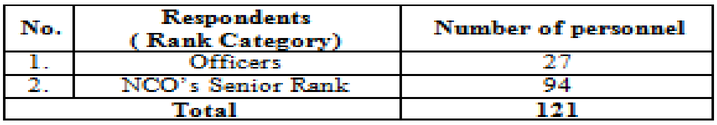
Section	Construct	Items	No. of Item	Type of Scale
A	Respondent Profile	Gender, Service Rank, Work Experience, Education Background, Awareness of BAT C 5 existence and BAT C 5 Entitlement	6	Nominal
B	Legal	Uniformity and legal certainty, Technology ethical issues, Boundary harmonisation, External governance, Adherence to legal or rules and Long term law expression	6	Ordinal with five points Likert Scale (1-Strongly Disagree to 5- Strongly Agree)
C	Code of Ethics	Armed Forces Code of Ethics, Authorisation use, Snoop around, Steal and false witness, Social consequences, Mutual trust, Personnel's right and Ethical Standard	8	
D	Safety	Safety feelings, Follow the rules and guidelines, Workplace culture, Appropriate handling, Proper channel, Safety concern reporting, Ease in discussing errors, Adequate competence level, Period of storing in secured way, Self-equipped and Ethical reconsideration	11	
E	Privacy	Information sharing, Ethical review, Informed consent, Transparency and responsibility, Data protection directives and Requirement-served	6	
F	Integrity	Personnel commitment, Biased-free in innovation, Enrich and firm, Policies, procedures and safeguards and Leader trait	5	
G	Confidentiality	Kept confidential, Serious implication on self reputation, Scepticism, Kept private and Authorised access	5	
H	Accountability	Commitment, Impact responsibility, Trust of credibility, Desirable manner and Central and authorised	5	
I	Autonomy	Intuitive implementation, Freedom of choice of technology, Inconvenience stated, Preserve dignity, Ethics in handling sovereignty, Protecting the diminished, Moral values, Ethical leadership, Ethics designation, Personnel freedom, Prosperity and Guideline	12	
J	Accuracy	Duties commitment, Skills and knowledge, Technology confidence and Access right	4	
K	Technology Ethics in Handling Confidential Information	Classified military information dissemination, Government policies critics, Sensitive sentiments provocation, Text document, Pictures, Audios, Military activities status, Image sketches by public, Personal information, Upload and the like, Downloading, Forums participation, Provocation, Duties document related, Private email, Public Hosting, Third party, Unencrypted Wi-Fi, Wireless Service and Network connecting	20	

3.3.1 Data and Procedure

In determining the design population and sample, a convenience sampling technique is used by dividing the entire population in the identified scope which is the selected RSR Corp of the MAF into three different subgroups. However, in this research only two subgroups are taken as the sample size as in Table 5. Convenience sampling is chosen because of the availability and easy approach [36] to the selected personnel in the selected environment in which data can be gathered in quickest period as possible. The population is gathered from Malaysian Armed Forces Pay Services Directorate of Malaysia Ministry of Defence that is responsible for keeping the record of the salary payment for each personnel in the MAF. The exact figure is gathered accordance to the September 2015 salary information retrieved from UGATNET system with assumption that the given personnel strength is right weighted with the omission of personnel posting in and out. The personnel identified are accordance to the selected population personnel in RSR Corp of the MAF which involved Non-Commissioned Officer

(NCO) personnel from Sergeant, Staff Sergeant, Warrant Officer Class II, and Warrant Officer Class I in rank which is categorised as NCO's Senior Rank and Officers of Second Lieutenant, Lieutenant, Captain and Major in rank.

Table 5: Population Size from Convenience Sampling

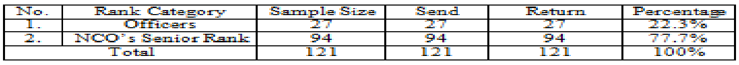


No.	Respondents (Rank Category)	Number of personnel
1.	Officers	27
2.	NCO's Senior Rank	94
Total		121

3.3.2 Sample

A total of 121 questionnaires were distributed with accordance to the rank identified in the selected sample. Table 6 shows the questionnaire distribution percentage. 22.3% questionnaire returned by Officers Rank while 77.7% questionnaire returned by NCO's Senior Rank.

Table 6: Percentage of Questionnaire Distributions



No.	Rank Category	Sample Size	Send	Return	Percentage
1.	Officers	27	27	27	22.3%
2.	NCO's Senior Rank	94	94	94	77.7%
Total		121	121	121	100%

3.4 Analysis

This phase involves the evaluation of the data collected. Statistical analysis tool of SPSS version 20 is used. The underlying analysis stages and its method used are depicted in Table 7.

3.5 Report Writing

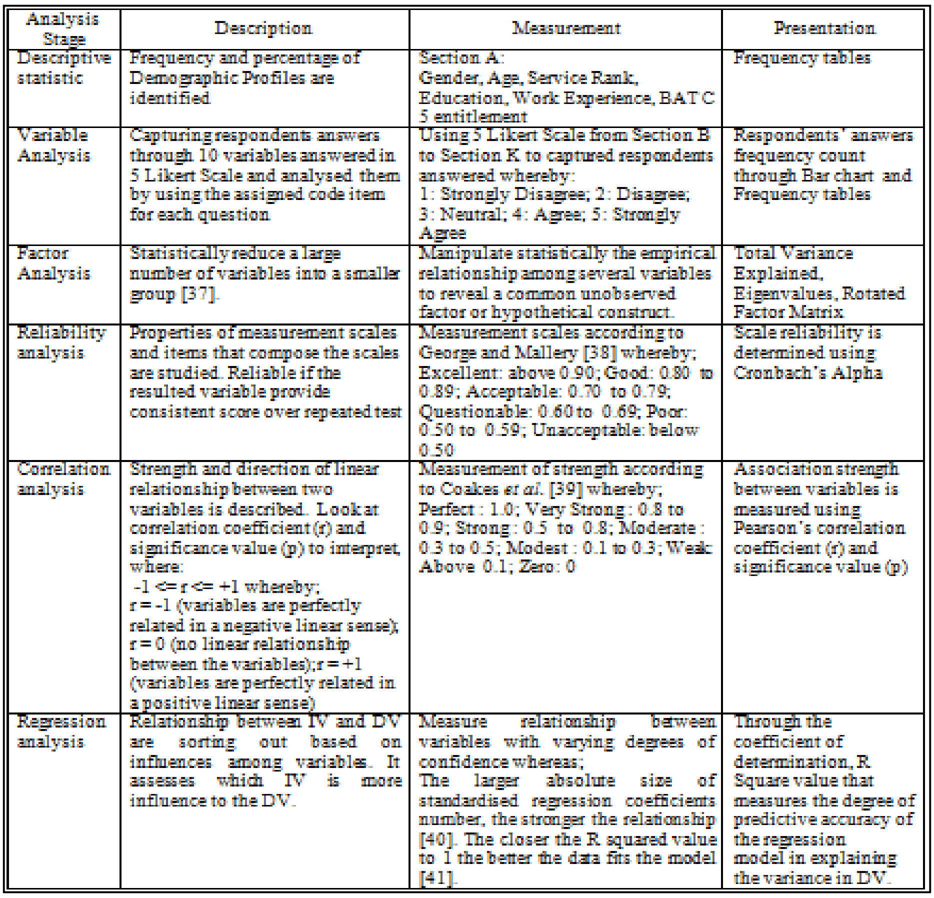
All findings and related discovery are documented. It served as a complete report that portrayed the research project fulfilment showing all deliverables.

4.0 RESULTS AND DISCUSSION

4.1 Respondents' Demographic Profile

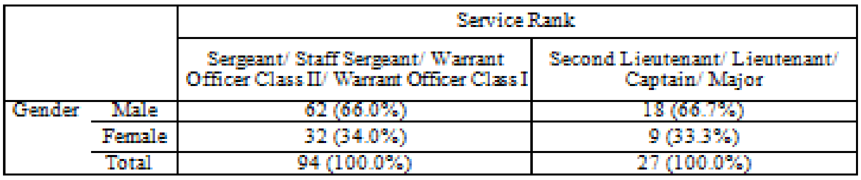
The demographic profile of the sample population findings is using the descriptive statistical analysis to determine the frequencies and percentages for each item. In this research, Section A depicts the demographic profile which comprises of six questions starting with the respondents' gender, service rank, working experience, education background, awareness of the BAT C 5 existence and BAT C 5 entitlement. A total of 121 personnel had participated in this questionnaire. It shows the sample population had more than half are males (N=80; 66.1%) than females (N-=41; 33.9%). The sample population also shown that there were more than half male than female for both categories where NCO's Senior Rank with (N=62; 66.0%) male than (N=32; 34.0%) female where as for the Officer's Rank there was (N=18; 66.7%) male than (N=9; 33.3%) female respectively as shown in Table 8.

Table 7: Analysis Stage and Method



Analysis Stage	Description	Measurement	Presentation
Descriptive statistic	Frequency and percentage of Demographic Profiles are identified	Section A: Gender, Age, Service Rank, Education, Work Experience, BAT C 5 entitlement	Frequency tables
Variable Analysis	Capturing respondents answers through 10 variables answered in 5 Likert Scale and analysed them by using the assigned code item for each question	Using 5 Likert Scale from Section B to Section K to captured respondents answered whereby: 1: Strongly Disagree; 2: Disagree; 3: Neutral; 4: Agree; 5: Strongly Agree	Respondents' answers frequency count through Bar chart and Frequency tables
Factor Analysis	Statistically reduce a large number of variables into a smaller group [37].	Manipulate statistically the empirical relationship among several variables to reveal a common unobserved factor or hypothetical construct.	Total Variance Explained, Eigenvalues, Rotated Factor Matrix
Reliability analysis	Properties of measurement scales and items that compose the scales are studied. Reliable if the resulted variable provide consistent score over repeated test	Measurement scales according to George and Mallery [38] whereby; Excellent: above 0.90; Good: 0.80 to 0.89; Acceptable: 0.70 to 0.79; Questionable: 0.60 to 0.69; Poor: 0.50 to 0.59; Unacceptable: below 0.50	Scale reliability is determined using Cronbach's Alpha
Correlation analysis	Strength and direction of linear relationship between two variables is described. Look at correlation coefficient (r) and significance value (p) to interpret, where: -1 <= r <= +1 whereby; r = -1 (variables are perfectly related in a negative linear sense); r = 0 (no linear relationship between the variables);r = +1 (variables are perfectly related in a positive linear sense)	Measurement of strength according to Coakes *et al.* [39] whereby; Perfect : 1.0; Very Strong : 0.8 to 0.9; Strong : 0.5 to 0.8; Moderate : 0.3 to 0.5; Modest : 0.1 to 0.3; Weak: Above 0.1; Zero: 0	Association strength between variables is measured using Pearson's correlation coefficient (r) and significance value (p)
Regression analysis	Relationship between IV and DV are sorting out based on influences among variables. It assesses which IV is more influence to the DV.	Measure relationship between variables with varying degrees of confidence whereas; The larger absolute size of standardised regression coefficients number, the stronger the relationship [40]. The closer the R squared value to 1 the better the data fits the model [41].	Through the coefficient of determination, R Square value that measures the degree of predictive accuracy of the regression model in explaining the variance in DV.

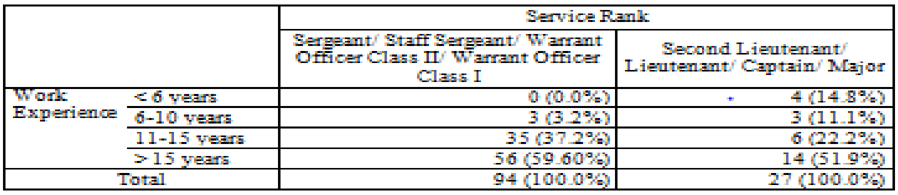
Table 8: Demographic Profile – Gender and Service Rank



		Service Rank	
		Sergeant/ Staff Sergeant/ Warrant Officer Class II/ Warrant Officer Class I	Second Lieutenant/ Lieutenant/ Captain/ Major
Gender	Male	62 (66.0%)	18 (66.7%)
	Female	32 (34.0%)	9 (33.3%)
	Total	94 (100.0%)	27 (100.0%)

The demographic profile of respondents work's experience with regards of the service rank is shown in Table 9. Slightly more than half respondents (N=56; 59.6%) and (N=14; 51.9%) from both service rank categories indicated work experience of more than 15 years for NCO's Senior Rank and Officer's Rank respectively. It followed by work experience from 11 to 15 years with slightly more than one third (N=35; 37.2%) for NCO's Senior Rank and nearly a quarter for the Officer's Rank (N=6; 22.2%)

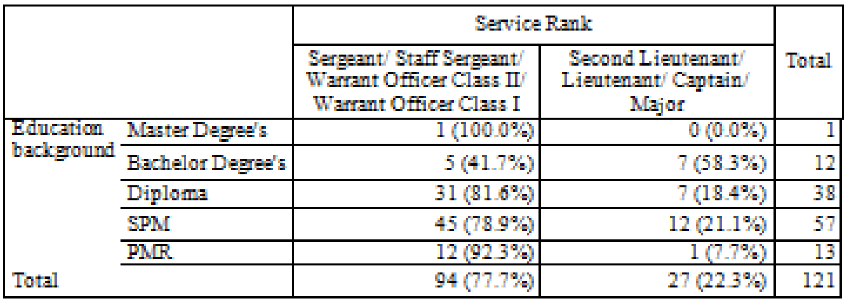
Table 9: Demographic Profile – Work Experience and Service Rank



		Service Rank	
		Sergeant/ Staff Sergeant/ Warrant Officer Class II/ Warrant Officer Class I	Second Lieutenant/ Lieutenant/ Captain/ Major
Work Experience	< 6 years	0 (0.0%)	4 (14.8%)
	6-10 years	3 (3.2%)	3 (11.1%)
	11-15 years	35 (37.2%)	6 (22.2%)
	> 15 years	56 (59.60%)	14 (51.9%)
Total		94 (100.0%)	27 (100.0%)

Table 10 depicts the demographic profile relationship between the education backgrounds with respect of the service rank. It shows that most of the respondent with those who had SPM with slightly more than three quarter (N=45; 78.9%) of the respondents were from NCO's Senior Rank background while nearly a quarter (N=12; 21.1%) were from the Officer's Rank. Diploma holder came second and followed by PMR and Bachelor Degree's holder.

Table 10: Demographic Profile – Education Background and Service Rank



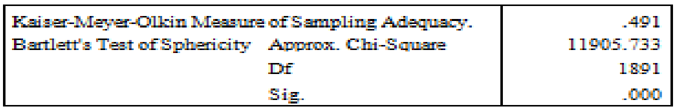
		Service Rank		Total
		Sergeant/ Staff Sergeant/ Warrant Officer Class II/ Warrant Officer Class I	Second Lieutenant/ Lieutenant/ Captain/ Major	
Education background	Master Degree's	1 (100.0%)	0 (0.0%)	1
	Bachelor Degree's	5 (41.7%)	7 (58.3%)	12
	Diploma	31 (81.6%)	7 (18.4%)	38
	SPM	45 (78.9%)	12 (21.1%)	57
	PMR	12 (92.3%)	1 (7.7%)	13
Total		94 (77.7%)	27 (22.3%)	121

Nearly all of the respondents (N=118; 97.52%) knew the existence of the BAT C 5 that enable one's to handle the confidential information with slightly more than three quarter of the respondents (N=92; 76.03%) represent the NCO's Senior Rank while nearly a quarter of respondents (N=26; 21.49%) represent the Officer's Rank. Nearly three quarter of the respondents (N=80; 66.1%) knew that they were entitled with BAT C 5 that recorded (N=53; 43.8%) represents the NCO's Senior Rank while (N=27; 22.3%) represents the Officer's Rank. Here, all of the officers realised with the BAT C 5 entitlement that enable them to handle the confidential information. More than a quarter (N=38; 31.4%) respondents are not entitled with the BAT C 5 and the remaining were not sure on the BAT C 5 entitlement.

4.2 Factor Analysis

Factor analysis is a group of sophisticated statistic techniques that require a computer to conduct [42]. In this research, Kaiser-Meyer-Oklin (KMO) measure of sampling adequacy and Bartlett's test of Sphericity is used prior to extract factors to assess the data appropriateness for further factor analysis. Table 11 indicates the KMO and Bartlett's Test of 0.491 which is considered suitable for factor analysis according to Tabachnick and Fidell [43] whereby the KMO greater than 0.5 is acceptable and the Bartlett's test is less than 0.05 which is considered significant for this test.

Table 11: KMO and Bartlett's Test

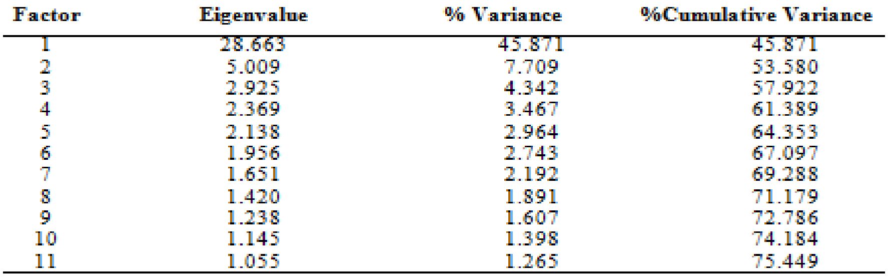


Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.491
Bartlett's Test of Sphericity	Approx. Chi-Square	11905.733
	Df	1891
	Sig.	.000

4.2.1 Factor Extraction Criteria and Rotational Method

The most commonly used methods are principal component analysis and principle axis factoring whereby decision to use either one of the techniques is debated as there is minor difference particularly when the reliability is high. In determining the factor extraction method, this research has applied the most popular Kaiser's eigenvalue greater than 1 criterion method to decide factors retention [44] along with suppressing a predetermined cumulative variance level to minimum value of 0.5 as suggested by Hair *et al*., [45]. This research used the Orthogonal varimax rotational method which is the common method used for factor analysis developed by Thompson [46]. Table 12 and Table 13 show the results of applying both suggested method to the data set which is the Total Variance and eigenvalues for pre-factor analysis items.

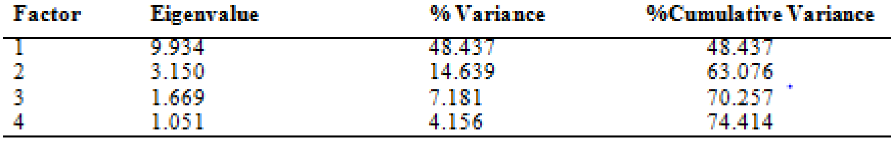
Table 12: Total Variance and Eigenvalues – Independent Variable



Factor	Eigenvalue	% Variance	%Cumulative Variance
1	28.663	45.871	45.871
2	5.009	7.709	53.580
3	2.925	4.342	57.922
4	2.369	3.467	61.389
5	2.138	2.964	64.353
6	1.956	2.743	67.097
7	1.651	2.192	69.288
8	1.420	1.891	71.179
9	1.238	1.607	72.786
10	1.145	1.398	74.184
11	1.055	1.265	75.449

From Table 12, it shows the extracted factors based on eigenvalues on all initially identified nine independent variables (IV) factor. They were, namely Legal that consists of 6 items, Code of Ethics with 8 items, Safety with 11 items, Privacy with 6 items, Integrity, Confidentiality and Accountability with 5 items respectively, followed by Autonomy with 12 items and Accuracy with 4 items which total to 62 items. Based on the result by using the extraction methods of eigenvalue greater than 1, principal axis factoring together with a cumulative variance above 50%, not all 62 items of IVs will be retained, only the first eleven factors were retained by using SPSS automated software.

Table 13: Total Variance and Eigenvalues – Dependent Variable

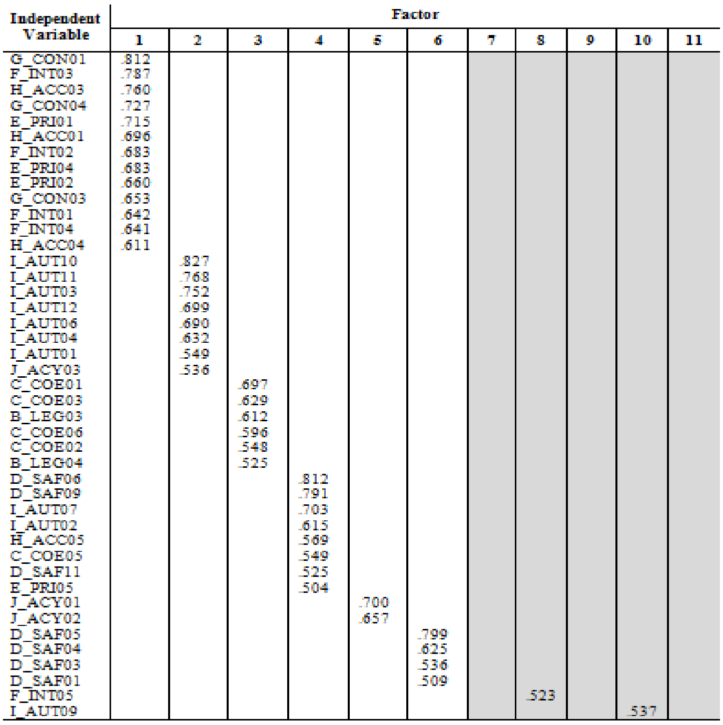


Factor	Eigenvalue	% Variance	%Cumulative Variance
1	9.934	48.437	48.437
2	3.150	14.639	63.076
3	1.669	7.181	70.257
4	1.051	4.156	74.414

4.2.2 Factor Extraction Criteria and Rotational Method

The emerged variables or items to a factor are examined whereby interpretation involved the process of determining and labelling on which items are attributable to which factors [47]. In addition, Henson and Roberts [48] stated that at least two or three items loading on a factor considered as giving a meaningful interpretation. The cut off value according to Tabachnick and Fidell [43] is labelled as the reading of values ranging from 0.32 indicates poor, fair of 0.45, good of 0.55, very good as 0.63 and excellent 0.71. This research applied the cut off values of 0.5 to be proceeded for further interpretation and all items loading less than 0.5 were removed. Items loading to more than one factor as suggested by Schonrock-Adema *et al.* [49] need to be removed for the item loading reading of 0.4 and above as well as factor which has no item loaded in it were eliminated for further analysis. Table 14 and Table 15 demonstrated the Item Loading on IV and DV respectively by the SPSS automated software that has generated the Rotated Factor Matrix with the suppressed value of 0.5.

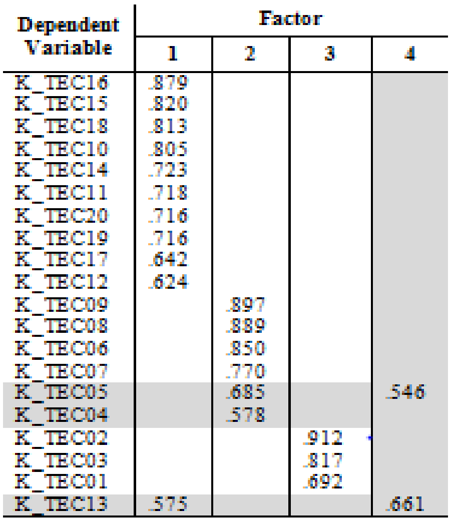
Table 14: Item Loading on Independent Variable – Rotated Factor Matrix[a]



Independent Variable	Factor										
	1	2	3	4	5	6	7	8	9	10	11
G_CON01	.812										
F_INT03	.787										
H_ACC03	.760										
G_CON04	.727										
E_PRI01	.715										
H_ACC01	.696										
F_INT02	.683										
E_PRI04	.683										
E_PRI02	.660										
G_CON03	.653										
F_INT01	.642										
F_INT04	.641										
H_ACC04	.611										
I_AUT10		.827									
I_AUT11		.768									
I_AUT03		.752									
I_AUT12		.699									
I_AUT06		.690									
I_AUT04		.632									
I_AUT01		.549									
J_ACY03		.536									
C_COE01			.697								
C_COE03			.629								
B_LEG03			.612								
C_COE06			.596								
C_COE02			.548								
B_LEG04			.525								
D_SAF06				.812							
D_SAF09				.791							
I_AUT07				.703							
I_AUT02				.615							
H_ACC05				.569							
C_COE05				.549							
D_SAF11				.525							
E_PRI05				.504							
J_ACY01					.700						
J_ACY02					.657						
D_SAF05						.799					
D_SAF04						.625					
D_SAF03						.536					
D_SAF01						.509					
F_INT05								.523			
I_AUT09										.537	

From Table 14, it depicts the IV readings after factor analysis showed 11 factors. The resulted item loading on IVs reflected on Factor 8 and Factor 10 (boldface) had indicated only 1 item loading reading while Factor 7, Factor 9 and Factor 11 (boldface) had no item loaded on it.

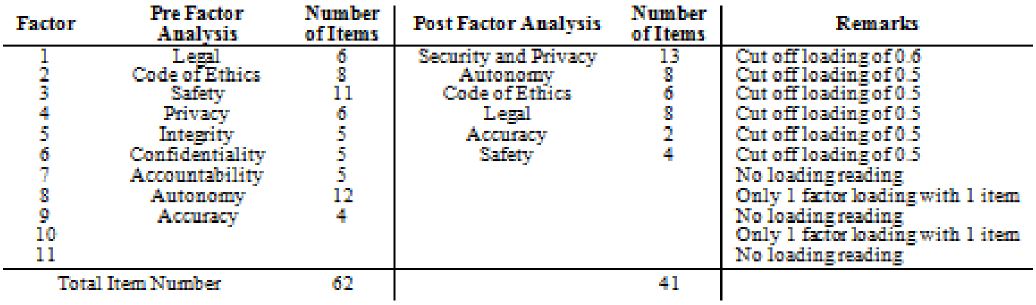
Table 15: Item Loading on Dependent Variable – Rotated Factor Matrix[a]



Dependent Variable	Factor			
	1	2	3	4
K_TEC16	.879			
K_TEC15	.820			
K_TEC18	.813			
K_TEC10	.805			
K_TEC14	.723			
K_TEC11	.718			
K_TEC20	.716			
K_TEC19	.716			
K_TEC17	.642			
K_TEC12	.624			
K_TEC09		.897		
K_TEC08		.889		
K_TEC06		.850		
K_TEC07		.770		
K_TEC05		.685		.546
K_TEC04		.578		
K_TEC02			.912	
K_TEC03			.817	
K_TEC01			.692	
K_TEC13	.575			.661

Based on Table 15, the cut off loading of 0.6 was applied which is found to be more reflective on the new emerged factor. It comprised of 4 factors for DV. Both reading from Factor 4 showed cross loading against Factor 1 (K_TEC13) and Factor2 (K_TEC05). Hence, factor 4 for DV is not considered for further analysis. Table 16 depicts factors that were renamed after Factor Analysis. Initially there were nine factors involved as the IV of this research. Among them are Legal, Code of Ethics, Safety, Privacy, Integrity, Confidentiality, Accountability, Autonomy and Accuracy with the number of items of 6, 8, 11, 6, 5, 5, 5, 12, and 4 respectively. After Factor Analysis whereby all items have been rotated, the initial factors named were then renamed to Security and Privacy with the 13 items. Autonomy are with 8 items, Code of Ethics with 6 items and Legal with 8 number of items, Accuracy with 2 items while Safety with 4 number of items.

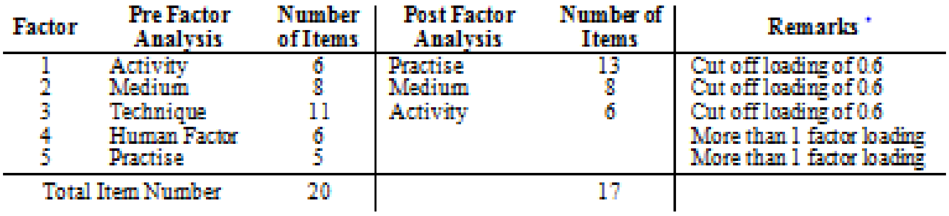
Table 16: Renaming of Factors for Independent Variable



Factor	Pre Factor Analysis	Number of Items	Post Factor Analysis	Number of Items	Remarks
1	Legal	6	Security and Privacy	13	Cut off loading of 0.6
2	Code of Ethics	8	Autonomy	8	Cut off loading of 0.5
3	Safety	11	Code of Ethics	6	Cut off loading of 0.5
4	Privacy	6	Legal	8	Cut off loading of 0.5
5	Integrity	5	Accuracy	2	Cut off loading of 0.5
6	Confidentiality	5	Safety	4	Cut off loading of 0.5
7	Accountability	5			No loading reading
8	Autonomy	12			Only 1 factor loading with 1 item
9	Accuracy	4			No loading reading
10					Only 1 factor loading with 1 item
11					No loading reading
Total Item Number		62		41	

Table 16 depicts the renaming of factors along with each of the related items after factor analysis. Cut off loading of 0.6 was applied to Factor 1 which leaves 13 items selected. This is found to be more reflective of the new factor called Security and Privacy. For Factor 2 to Factor 6 cut off loading of 0.5 was applied. Factor 2 was renamed as Autonomy with 8 items. It is followed by Factor 3 that was renamed as Code of Ethics indicated by 6 items and Factor 4 renamed as Legal with 8 items. Factor 5 which is Accuracy and Factor 6 named Safety comprised of 2 and 4 items respectively. Nevertheless, there were no loading reading indicated for Factor 7, Factor 9 and Factor 11. Factor 8 and Factor 10, both indicated by only 1 item loading with 1 item. This was discarded as one item would not be adequate for further analysis. As for the DV in Table 17, the factors names' were revised according to the rotated factor matrix identified. Factor 1 was renamed as Practise with 10 items, Factor 2 was renamed as Medium with 4 items and Factor 3 was renamed as Activity with 3 items loaded.

Table 17: Renaming of Factors for Dependent Variable

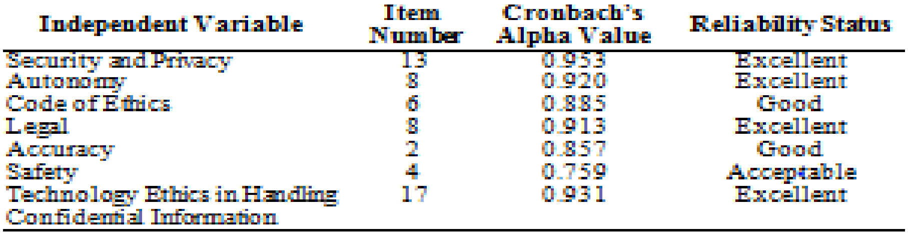


Factor	Pre Factor Analysis	Number of Items	Post Factor Analysis	Number of Items	Remarks
1	Activity	6	Practise	13	Cut off loading of 0.6
2	Medium	8	Medium	8	Cut off loading of 0.6
3	Technique	11	Activity	6	Cut off loading of 0.6
4	Human Factor	6			More than 1 factor loading
5	Practise	5			More than 1 factor loading
Total Item Number		20		17	

4.3 Reliability Analysis

The Cronbach's Alpha Value scales that was introduced by George and Mallery [38] is used. Table 18 summarised the Cronbach Alpha Value which has been tested for all six IVs of Security and Privacy, Autonomy, Code of Ethics, Legal, Accuracy and Safety together with the DV of Technology Ethics in Handling Confidential Information in this section.

Table 18: Cronbach's Alpha Value of Variables



Independent Variable	Item Number	Cronbach's Alpha Value	Reliability Status
Security and Privacy	13	0.953	Excellent
Autonomy	8	0.920	Excellent
Code of Ethics	6	0.885	Good
Legal	8	0.913	Excellent
Accuracy	2	0.857	Good
Safety	4	0.759	Acceptable
Technology Ethics in Handling Confidential Information	17	0.931	Excellent

Based on the reliability test in Table 18, all the variables denotes the Cronbach's Alpha value within the acceptable range and above were all in the range above the 0.90 which indicates "excellent" in terms of reliability whereas the variable of Code of Ethics and Accuracy has denotes "good" in terms of their returned reliability values where the Cronbach's Alpha values have laid in the range of 0.80 up to 0.89. However, the Safety variable depicts the "acceptable" reliability in which it has laid in within the range of 0.70 to 0.79. From the results, Security and Privacy has the highest Cronbach's Alpha values with the reading of 0.953. The findings show that the instrument is reliable for each variable. Figure 3 depicted the revised hypothesises of the proposed model resulted after Factor Analysis.

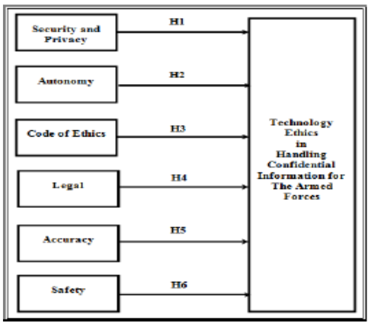
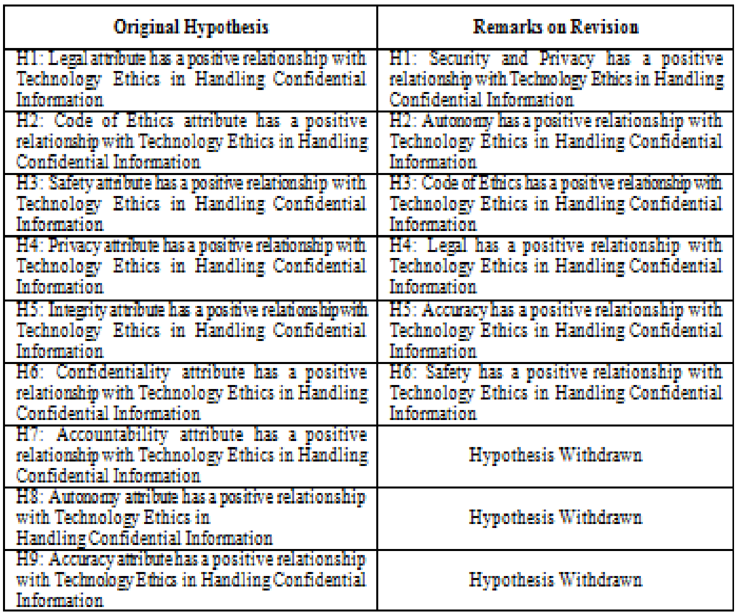

Security and Privacy
H1
Autonomy
H2
Code of Ethics
H3
Legal
H4
Accuracy
H5
Safety
H6
Technology Ethics in Handling Confidential Information for The Armed Forces

Figure 3: Post Factor Analysis Revised Hypothesis

Table 19 summarised the Revised Hypothesises involved in pre and post of Factor Analysis. Originally, there were nine hypothesises in the proposed conceptual model of Technology Ethics in Handling Confidential Information for the Armed Forces. However, after factor analysis was conducted, only six out of nine hypothesises have emerged against the variables being assigned as the new IV in this research. The said variables are Security and Privacy, Autonomy, Code of Ethics, Legal, Accuracy and Safety which have replaced the original IV of Legal, Code of Ethics, Safety, Privacy, Integrity, Confidentiality, Accountability, Autonomy and Accuracy.

Due to the modification on the research model, the questionnaire is revised accordingly. The revised questionnaire consists of eight sections which has started with section A on the respondents' profile where the questionnaire began, followed by section B on Security and Privacy, section C on Autonomy, section D on Code of Ethics, section E on Legal, section F on Accuracy, section G on Safety, and Section H on Technology Ethics in Handling Confidential Information.

Table 19: Revised hypothesis

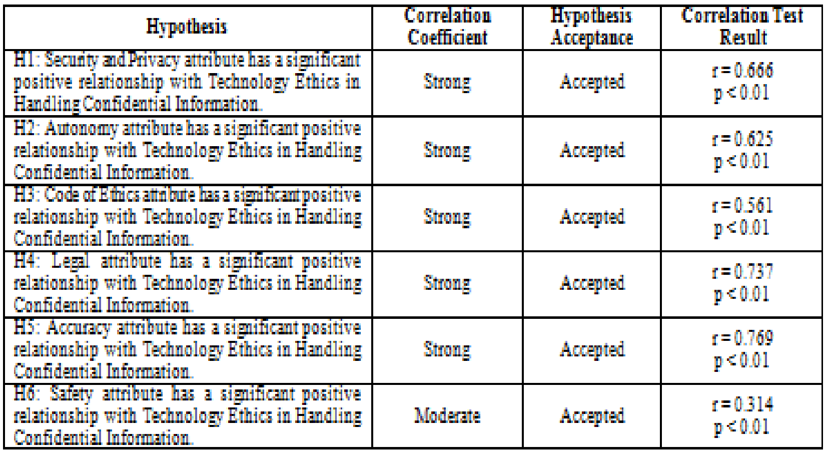


Original Hypothesis	Remarks on Revision
H1: Legal attribute has a positive relationship with Technology Ethics in Handling Confidential Information	H1: Security and Privacy has a positive relationship with Technology Ethics in Handling Confidential Information
H2: Code of Ethics attribute has a positive relationship with Technology Ethics in Handling Confidential Information	H2: Autonomy has a positive relationship with Technology Ethics in Handling Confidential Information
H3: Safety attribute has a positive relationship with Technology Ethics in Handling Confidential Information	H3: Code of Ethics has a positive relationship with Technology Ethics in Handling Confidential Information
H4: Privacy attribute has a positive relationship with Technology Ethics in Handling Confidential Information	H4: Legal has a positive relationship with Technology Ethics in Handling Confidential Information
H5: Integrity attribute has a positive relationship with Technology Ethics in Handling Confidential Information	H5: Accuracy has a positive relationship with Technology Ethics in Handling Confidential Information
H6: Confidentiality attribute has a positive relationship with Technology Ethics in Handling Confidential Information	H6: Safety has a positive relationship with Technology Ethics in Handling Confidential Information
H7: Accountability attribute has a positive relationship with Technology Ethics in Handling Confidential Information	Hypothesis Withdrawn
H8: Autonomy attribute has a positive relationship with Technology Ethics in Handling Confidential Information	Hypothesis Withdrawn
H9: Accuracy attribute has a positive relationship with Technology Ethics in Handling Confidential Information	Hypothesis Withdrawn

4.5 Correlation Analysis

This test described the strengths and direction of linear relationship between two variables. A bivariate correlation analysis is conducted to identify the association strength between the six IVs and a DV by using Pearson's correlation coefficient (r). The p-value also been looked at to measure the significance of the analysis in which the range are between 0 and 1 to represent the probability that the data would have arisen if the set null hypothesis were true [50]. According to the derived results, there are a significant (p-value < 0.01) and are positive with moderate to strong correlation coefficient (r) between the six IV of Security and Privacy, Autonomy, Code of Ethics, Legal, Accuracy and Confidentiality towards the DV of Technology Ethics in Handling Confidential Information as summarised in Table 20.

Table 20: Hypothesis Tested Result



Hypothesis	Correlation Coefficient	Hypothesis Acceptance	Correlation Test Result
H1: Security and Privacy attribute has a significant positive relationship with Technology Ethics in Handling Confidential Information.	Strong	Accepted	r = 0.666 p < 0.01
H2: Autonomy attribute has a significant positive relationship with Technology Ethics in Handling Confidential Information.	Strong	Accepted	r = 0.625 p < 0.01
H3: Code of Ethics attribute has a significant positive relationship with Technology Ethics in Handling Confidential Information.	Strong	Accepted	r = 0.561 p < 0.01
H4: Legal attribute has a significant positive relationship with Technology Ethics in Handling Confidential Information.	Strong	Accepted	r = 0.737 p < 0.01
H5: Accuracy attribute has a significant positive relationship with Technology Ethics in Handling Confidential Information.	Strong	Accepted	r = 0.769 p < 0.01
H6: Safety attribute has a significant positive relationship with Technology Ethics in Handling Confidential Information.	Moderate	Accepted	r = 0.314 p < 0.01

The evaluated model for Technology Ethics in Handling Confidential Information for the Armed Forces is depicted as in Figure 4. Accuracy has the highest correlation of 76.9% while Safety indicates the lowest correlation of 31.4%. However this value lies as having a moderate correlation (r of 0.3 to 0.5) and thus, this model is accepted.

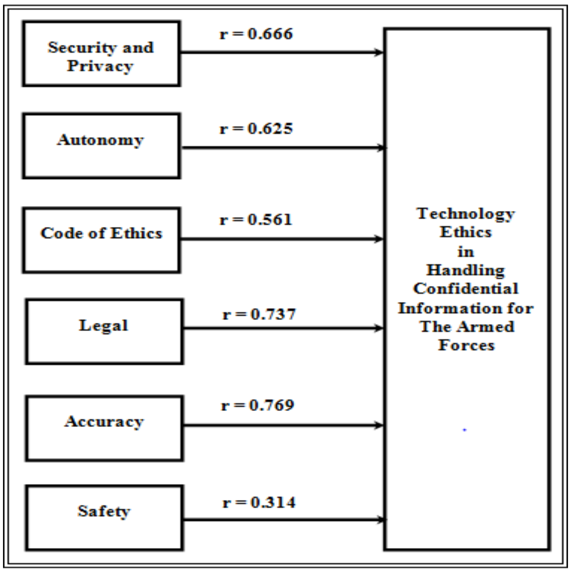
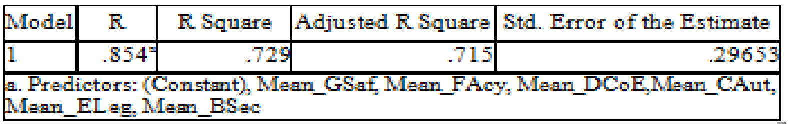


Figure 4: Evaluated Model based on Correlation of Independent and Dependent Variable

4.6 Regression Analysis

This section describes the analysis technique by using multiple regressions analysis to predict the value of a DV based on the value of IVs which sometimes being called as predictors. It is used to understand whether the DV can be predicted by the IVs which implied the overall fit of the model and relative contribution of each of the predictors to the total variance explained. Table 21 shows the model summary of regression information. The information contains in this table can be used to determine whether a regression model fits the data.

Table 21: Model Summary of Regression

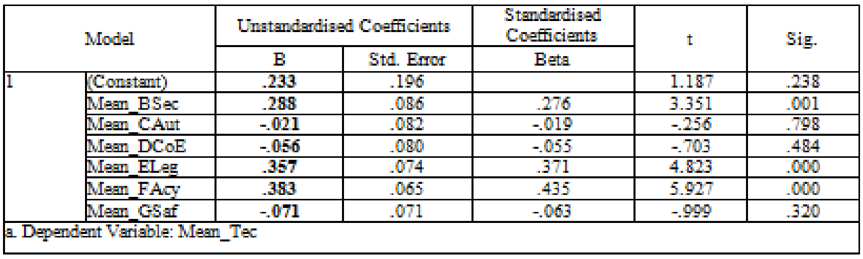


Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.854[a]	.729	.715	.29653

a. Predictors: (Constant), Mean_GSaf, Mean_FAcy, Mean_DCoE,Mean_CAut, Mean_ELeg, Mean_BSec

Based on Table 21, the central focuses is to look at the R square value which is also called as coefficient of determination. Hence, a total of 72.9% of the variations in the DV are explained by regression model using the IVs as predictors. This implies the acceptable values of R Square which depends on the field of study whereby an experimental study in a controlled environment ay expect values as high as 0.9, while for behavioural studies reflecting on human behaviour may accept lower values [51]. The remainder of 27.1% (100% - 72.9%) remains unexplained. There most probably could be other determinants for the residual percentages because this research has constraint up to only nine attributes during the SLR and six attributes left after Factor Analysis in which the attribute could be more during findings which can be proposed to conduct in future studies. Table 22 gives the information of coefficients. The information provided in the Unstandardised Coefficients column (boldface) is used to construct an estimated model coefficient.

Table 22: Coefficients[a]



Model		Unstandardised Coefficients		Standardised Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	**.233**	.196		1.187	.238
	Mean_BSec	**.288**	.086	.276	3.351	.001
	Mean_CAut	**-.021**	.082	-.019	-.256	.798
	Mean_DCoE	**-.056**	.080	-.055	-.703	.484
	Mean_ELeg	**.357**	.074	.371	4.823	.000
	Mean_FAcy	**.383**	.065	.435	5.927	.000
	Mean_GSaf	**-.071**	.071	-.063	-.999	.320

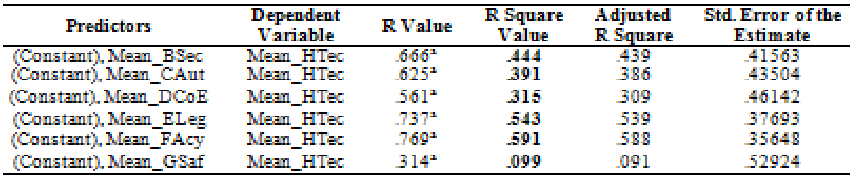
a. Dependent Variable: Mean_Tec

Thus, the general form of equation is derived as:

"Predicted **HTec** = 0.233 + (0.288 x **BSec**) - (0.021 x **CAut**) - (0.056 x **DCoE**) +
(0.357 x **ELeg**) + (0.383 x **FAcy**) - (0.071 x **GSaf**)"

This equation denotes that the variations in the HTec (DV) can be explained by regression model using the predictor of BSec, CAut, DCoE, ELeg, FAcy and GSaf (IVs). It also explained how much an increase of one unit in an IV could affect the DV with the assumption that other IVs are held constant. Table 23 summarised the R Square value (boldface) gotten from the Model Summary of Regression resulting from IVs towards the DV.

Table 23: Summary of Coefficient of Determination (R^2) for Independent towards Dependent Variable



Predictors	Dependent Variable	R Value	R Square Value	Adjusted R Square	Std. Error of the Estimate
(Constant), Mean_BSec	Mean_HTec	.666[a]	**.444**	.439	.41563
(Constant), Mean_CAut	Mean_HTec	.625[a]	**.391**	.386	.43504
(Constant), Mean_DCoE	Mean_HTec	.561[a]	**.315**	.309	.46142
(Constant), Mean_ELeg	Mean_HTec	.737[a]	**.543**	.539	.37693
(Constant), Mean_FAcy	Mean_HTec	.769[a]	**.591**	.588	.35648
(Constant), Mean_GSaf	Mean_HTec	.314[a]	**.099**	.091	.52924

From Table 23, the coefficient of determination (boldface) values used to evaluate the model as in Figure 5. It is based on Regression result of each IV towards the DV. According to the R Square value, the IV of Accuracy has the highest regression value while the IV of Safety has shown the lowest regression value of 59.1% and 9.9% respectively.

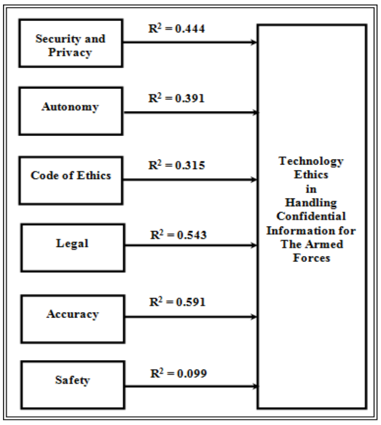


Figure 5: Evaluated model based on R^2 value between Independent and Dependent Variable

4.0 CONCLUSION

This research focuses on three main objectives which are: first, identifying the attributes of technology ethics that significantly influences the confidential information handling, followed by the second objective which is designing the technology ethics model in handling the confidential information and consecutively the third objective of evaluating the technology ethics model in handling confidential information that was designed in the selected environment of the Armed Forces.

The first objective of "to identify the technology ethics attributes in handling confidential information" was achieved through the SLR technique. This SLR was beneficiated from the exhaustive searches through 17 related journals. Hence, there were 9 attributes gathered. Among them are the Legal, Code of Ethics, Safety, Privacy, Integrity, Confidentiality, Accountability, Autonomy, and Accuracy.

The second objective of this research which is "to design the proposed technology ethics model in handling confidential information for the Armed Forces" remarks the right achievement when a total of 9 attributes found during the SLR (achieved in first objective) have consecutively mapped to the three models identified in Literature Review. The models involved are Research Model of Promoting Ethical Behaviour and Organisational Citizenship Behaviours by Baker, et al. [33], Meta-Analytic Framework for Antecedents of Unethical Choices in the Workplace by Kish-Gephart, et al. [34] along with The Four Principal Approach by Beauchamp and Childress [35]. These steps had produced the proposed conceptual model of technology ethics in handling confidential information which signifies the success of this second objective. Based on the proposed model that consist of 9 IVs and a DV, a set of questionnaires are developed, piloted and distributed to the selected population of RSR Corp.

The third objective of this research is "to evaluate the proposed technology ethics model in handling confidential information for the Armed Forces" has successfully implemented during the phase of Analysis. The proposed model identified in the second objective was tested and evaluated by using several techniques offer in SPSS version 20 software such as descriptive, factor, reliability, correlation as well as regression analysis. From the findings, it demonstrated that the initial 9 attributes in the proposed conceptual model was modified and that only 6 attributes remained which resulted the modification on the proposed conceptual model. The new emerged attributes are Security and Privacy, Autonomy, Code of Ethics, Legal, Accuracy and Safety that replaced the original found attributes of Legal, Code of Ethics, Safety, Privacy, Integrity, Confidentiality, Accountability, Autonomy, and Accuracy.

ACKNOWLEDGMENTS

The authors wish to thank the Public Service Department for the scholarship also to MAF personnel whom actively participated as respondents to fulfil the objectives of this research.

REFERENCES

[1] Department of Planning and Administration (2013). Dasar Keselamatan Teknologi Maklumat Dan Komunikasi (Ict) Kementerian Pertahanan versi 4.0. Malaysia: Department of Planning and Administration

[2] Cisco (2008). Data Leakage Worldwide: Common Risks and Mistakes Employees Make

[3] A. Umansky, High bandwidth portable transmission systems-use of ADSL technology in military and industrial applications, in EUROCOMM 2000. Information Systems for Enhanced Public Safety and Security. IEEE/AFCEA, 2000, pp. 364-368.

[4] Cisco (2014). Annual Security Report.

[5] Pinsent Masons (2008). Confidential Information. Retrieved 10 November 2015 http://www.out-law.com/page-389

[6] G. Bunker, Technology is not enough: Taking a holistic view for information assurance, Information Security Technical Report 17 (2012) 19-25.

[7] R. P. Reece and B. C. Stahl, The professionalisation of information security: Perspectives of UK practitioners, Computers & Security 48 (2015) 182-195.

[8] Secretariat (1985). Malaysian Armed Forces Security Instruction. Malaysia: Malaysian Armed Forces Secretariat.

[9] Directorate (2015). Parliament Trial Sheet. Malaysia: Security and Counter Intelligence Directorate.

[10] Secretariat (2013). Perintah Am Angkatan Tentera (PAAT) serial 1/ 2013. Malaysia: Malaysian Armed Forces Secretariat.

[11] S. Bhadauria, S. Sharma, R. Litoriya, Empirical analysis of Ethical issues in the era of future information technology, International Conference on Software Technology and Engineering (ICSTE) (2010) V2-31-V32-35.

[12] A.K.L. Jumelle, I. Ispas, C. Thuernmler, O. Mival, E. Kosta, P. Casla, Ethical assessment in e-Health, IEEE 16th International Conference on Paper presented at the e-Health Networking, Applications and Services (Healthcom) (2014) 262-268.

[13] K. Wolf, A. Schmidt, A. Bexheti, M. Langheinrich, Lifelogging: You're Wearing a Camera? Pervasive Computing, IEEE 13 (2014) 8-12.

[14] B.C. Stahl, S. Rogerson, K.J. Wakunuma, Future Technologies: The Matter of Emergent Ethical Issues in Their Development. Paper presented at the Future Computing, Service Computation, Cognitive, Adaptive, Content, Patterns, (2009) COMPUTATIONWORLD'09. Computation World:, 603-607.

[15] N.S. Udoh, O.T. Eluwole, A.O. Ologunde, Ethical responsibilities: The smart card engineer. IEEE International Symposium on Ethics in Science, Technology and Engineering (2014) 1-5.

[16] W.R. Bowen, Engineering innovation in healthcare: technology, ethics and persons, Human Reproduction And Genetic Ethics 17 (2011) 204-221.

[17] R. Kanungo, M. Mendonca, M. Ethical leadership in three dimensions. Journal of Human Values 4 (1998) 133-148.

[18] N. González, A. Kämäräinen, O. Kalla, Ethical aspects in ICT research an development: The case of the CONFIDENCE project. eChallenges (2010) 1-8.

[19] J.D. Wyndham, W.H. Coste, M.R. Smith, Ethics and the official reports about the destruction of the World Trade Center Twin Towers (WTC1 and WTC2) on 9/11: A case study. IEEE International Symposium on Ethics in Science, Technology and Engineering, (2014) 1-6.

[20] J. P. Fitch, Engineering a Global Response to Infectious Diseases. Proceedings of the IEEE 103 (2015) 263-272.

[21] M. F. Lee, and C. S. Lai, Rhetoric Value Based Model for Malaysian Special Vocational Education Secondary Schools' Teachers, Journal of Advanced Research in Social Sciences and Behavioural Sciences 2 (2016) 1-6.

[22] E. A. Hinckson, S. Duncan, M. Oliver, S. Mavoa, E. Cerin, H. Badland, Built environment and physical activity in New Zealand adolescents: a protocol for a cross-sectional study. BMJ Open 4 (2014) e004475-e004475.

[23] M. A. Anderson, J. Giordano, Aequilibrium prudentis: on the necessity for ethics and policy studies in the scientific and technological education of medical professionals. BMC medical education 13 (2013) 58.

[24] K. M. Younis, Views on potential methods for raising environmental awareness in developing countries: a study on social responsibility engagement in Liberia. Global Bioethics 26 (2015) 1-17.

[25] C. Frauenberger, J. Good, W. Keay-Bright, Designing technology for children with special needs: bridging perspectives through participatory design. CoDesign 7 (2011) 1-28.

[26] J. Van den Hoven, G.J. Lokhorst, I. Van de Poel, Engineering and the problem of moral overload. Science And Engineering Ethics 18 (2012) 143-155.

[27] V. Johansson, M. Garwicz, M. Kanje, L. Halldenius, J. Schouenborg, Thinking Ahead on Deep Brain Stimulation: An Analysis of the Ethical Implications of a Developing Technology. AJOB Neuroscience 5 (2014) 24-33.

[28] S. A. Zwijsen, A. R. Niemeijer, C.M.P.M. Hertogh, Ethics of using assistive technology in the care for community-dwelling elderly people: An overview of the literature. Aging & Mental Health 15 (2011) 419-427.

[29] T.E. Becker, Integrity in organizations: Beyond honesty and conscientiousness. Academy of Management Review 23 (1998) 154-161.

[30] A.H. Kiran, N. Oudshoorn, P.P. Verbeek, Beyond checklists: toward an ethical-constructive technology assessment. Journal of Responsible Innovation 2 (2015) 5-19.

[31] M.S. Frankel, S. Siang, Ethical and legal aspects of human subjects research on the Internet, AAAS online (1999) http://www.aaas.org/sites/default/files/migrate/uploads/report2.pdf.

[32] S. A. Panatik, M. F. Katimin and R. Shaari, The Effect of Personal Factors on Creativity among Research Officers in Malaysia, Journal of Advanced Research in Social Sciences and Behavioural Sciences 2 (2016) 33-49.

[33] T. L. Baker, T. G. Hunt, and M. C. Andrews, Promoting ethical behavior and organizational citizenship behaviors: The influence of corporate ethical values, Journal of Business Research 59 (2006) 849-857.

[34] J. J. Kish-Gephart, D. A. Harrison, and L. K. Treviño, Bad apples, bad cases, and bad barrels: meta-analytic evidence about sources of unethical decisions at work, Journal of Applied Psychology 95 (2010) 1.

[35] T. L. Beauchamp and J. F. Childress, Principles of biomedical ethics: Oxford university press, 2001.

[36] P. Sedgwick, Convenience sampling, BMJ 347 (2013) f6304.

[37] D.A. Newman, Longitudinal modeling with randomly and systematically missing data: A simulation of ad hoc, maximum likelihood, and multiple imputation techniques, Organizational Research Methods 6 (2003) 328-362.

[38] D. George and M. Mallery, Using SPSS for Windows step by step: a simple guide and reference, Boston, MA: Allyn y Bacon, 2003.

[39] S. Coakes, L. Steed, and C. Ong, Analysis without Anguish: SPSS version 16.0 for Windows, ed: John Wiley and Sons, Australia, Ltd, 2009.

[40] L. S. Aiken, S. G. West, and R. R. Reno, Multiple regression: Testing and interpreting interactions: Sage, 1991.

[41] D. Sharma, D. McGee, and B. G. Kibria, Measures of explained variation and the base-rate problem for logistic regression, American Journal of Biostatistics 2 (2011) 11.

[42] J. O. Kim and C. W. Mueller, Factor analysis: Statistical methods and practical issues Sage (1978).

[43] B. Tabachnick and L. Fidell, Multivariate analysis of variance and covariance, Using multivariate statistics, Pearson (2007).

[44] B. Williams, T. Brown, and A. Onsman, Exploratory factor analysis: A five-step guide for novices, Australasian Journal of Paramedicine 8 (2012) 1.

[45] J. F. Hair, W.C. Black, B.J. Babin, R.E. Anderson, Multivariate data analysis (7 ed.). Englewood Cliffs: Prentice Hall.

[46] B. Thompson, Exploratory and confirmatory factor analysis: understanding concepts and applications. Washington, DC: American Psychological Association; 2004.

[47] M. A. Pett, N. R. Lackey, J.J. Sullivan, Making sense of factor analysis: The use of factor analysis for instrument development in health care research: Sage (2003).

[48] R. K. Henson and J. K. Roberts, Use of exploratory factor analysis in published research common errors and some comment on improved practice, Educational and Psychological measurement 66 (2006) 393-416.

[49] J. Schönrock-Adema, M. Heijne-Penninga, E. A. van Hell, and J. Cohen-Schotanus, Necessary steps in factor analysis: Enhancing validation studies of educational instruments. The PHEEM applied to clerks as an example, Medical Teacher 31 (2009) e226-e232.

[50] N. Fenton and M. Neil, Risk assessment and decision analysis with Bayesian networks: CRC Press, 2012.

[51] M. Clerc and J. Kennedy, The particle swarm-explosion, stability, and convergence in a multidimensional complex space, Evolutionary Computation, IEEE Transactions, 6 (2002) 58-73.