Review of Information Security Policy based on Content Coverage and Online Presentation in Higher Education

Arash Ghazvini, Zarina Shukur, Zaihosnita Hood
Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia,
43600 UKM, Bangi, Selangor, Malaysia

***Abstract*—Policies are high-level statements that are equal to organizational law and drive the decision-making process within the organization. Information security policy is not easy to develop unless organizations clearly identify the necessary steps required in the development process of an information security policy, particularly in institutions of higher education that largely utilize IT. An inappropriate development process or replication of security policy content from other organizations could fail in execution. The execution of a duplicated policy could fail to act in accordance with enforceable rules and regulations even though it is well developed. Hence, organizations need to develop appropriate policies in compliance with the organization regulatory requirements. This paper aims to reviews policies from selected universities with regards to ISO 27001:2013 minimum requirements as well as effective online presentation. The online presentation review covers the elements of aesthetics, navigation and content presentation. The information on the security policy document resides on the universities' website.**

Keywords—Information security policy; policy development; higher education

I. Introduction

The aim of information security is to protect the organization's information assets from any unauthorized access, disclosure or breaches. To enforce an effective information security, organizations need to develop good management practices comprising policies and controls [35]. Technical solutions provide support to protect information assets. However, technical solution alone cannot eliminate the risks of information leakage, modification or breaches. As this may cause significant loss, information security is critical to the business operation of most organizations, especially government and public bodies as the financial and non-financial costs are much greater compared to other organizations [37]. Similarly, information leakage or breaches may cause great losses for a higher education institution that store a large amount of student information within the management system, administrative systems and student portals [35], [38]. For example, a university credibility and integrity can be damaged due to illicit grade changes and constant difficulties with registration or financial systems [21].

The importance of information security and confidentiality in universities has been discussed since 1975 [36]. Universities and colleges are being targeted for cyber-attacks due to two main reasons. First, due to a large amount of computer power possess by universities and colleges. And second, due to the open access, they make available to the public. Universities' networking infrastructures are not only available to staff and students but are also available to other students, visitors, and researchers worldwide. While providing access to the public and promoting information sharing, there should be a balance to ensure the security of information assets [21].

Information security and protection against internal risks are focal concerns in many organizations. Technological solutions alone cannot guarantee data protection against various threats. Even though there are advanced technologies, human factor still remains as the major risk to the integrity of information systems security [17][24]. At this point, numerous security experts believe that implementation of security policy and enforcement are the most sensible approach to protect information systems security [15] and the key to an effective security control program [15][22]. 'Development process' [13][26] and 'contents' of the security policy are the two elements that mainly determine the effectiveness of security policy [8][19] [12].

Protection of organizations' information which is progressively stored, processed and disseminated is becoming more intricated and challenging. This is even more complex for knowledge-intensive organizations including universities as teaching and research activities are becoming more dependent on the availability, integrity, and accuracy of electronic information resources. This paper intends to study how to write general outlines and the structure of what a policy should contain, rather than the content of information security policies [7]. In addition, the online presentations of the policies are also reviewed based on a principle of good design.

II. Role And Scope of the Information Security Policy

The literature shows that the information security policy is gradually becoming a significant corporate document to protect the availability, confidentiality, and integrity of organization information resources. More specifically, it is argued that the policy document should establish the mechanism for an organization to proactively manage

information security [14]. Hence, an effective information security policy should define individual responsibilities, outline authorized and unauthorized use of the system, create room for users to report any suspected or identified threats to the system, clarify penalties in case of violations, and specify methods for updating a policy [7].

One of the most significant roles of information security policy is to precisely specify user's rights and responsibilities and to successfully communicate it to all users, to ensure there is a mutual and coherent understanding of information security that is embraced by the organization [11]. This eliminates excuses for employees who fail to follow and execute security practices aligned with the organization's policy [23]. As a result, policy document must act as a catalyst of employees' belief and behavior with respect to information security, and by doing so, it becomes the foundation of effective security management [7].

The objective of information security is to protect organizations' information assets from unauthorized uses, breaches, and disclosure. As defined by ISO/IEC 27001:2013, information security refers to the preservation of confidentiality, integrity, and availability of information. The goal is providing access to only those authorized personnel who need the access, keeping the information accurate and complete and making sure the information is available to the authorized user when they need it.

Proper management practices containing policies and controls should be established to ensure the effectiveness of implementation and enforcement of information security policy. According to ISO/IEC 27002:2013, information security policy aims to provide management with guidance and support in accordance with corporate requirements and regulations when dealing with information security. Undoubtedly, information security policy plays an important role to ensure the organization's well-being by protecting the information assets. However, the development and implementation process of an effective information security is unclear [9].

Due to lack of guidance, policy developers often refer to developed policies by other organizations, available commercial sources, or public templates from the Internet. Thus, the policy document created from such sources will not provide proper guidance for information security to protect that individual organization. Moreover, the developed policy may not be applicable to the threats and risks that they are supposed to mitigate, and thus they will not resolve the security issues that a particular organization is facing. "Sadly, many IT security experts do not recognize and comprehend the business risks, and eventually make lengthy security policies documents that attempt to protect everything" [9].

The development process and implementing of an effective information security policy is not a clear cut and is triggered by various issues including regulatory requirements, complications of advanced technologies, internal and external risks and threats. The literature underlines a number of information security policy development process and implementation methods [1], although these methods do not offer a comprehensive and integrated method that includes a step-by-step guideline [9].

III. Information Policy Structure vs. Policy Guideline

Even though there is a substantial body of literature underlying the importance of the policy document, there is a debate on the structure and key elements of the policies. The literature has mostly explored the structure of policy, generally from a conceptual perspective. For instant reference [3] argue if there should be a single policy or whether it should be divided into subdocuments with different types. The previous study [29] proposes two models namely 'computer-oriented and people/organizational' policies. However, literature [30] suggests a three-level model that are 'institutional policy, institutional ISP and technical ISP'. In [31] recommends a four-level model including 'system security policy, product security policy, community security policy and corporate information security policy'. Whilst there is increasing debate about the number of policies and how they are inter-related, reference [31] state that practically organizations are more likely to have a single policy document. Other scholars are focusing on the difference between high and low levels of policy practices [32], although it should provide guidelines on 'means' as well as 'ends' [33]. Over the years, more studies have been conducted on the effective configuration for information security documentation, but surely minimum effort to resolve the issue. In fact, the issue has become even more complex due to the manifestation of new forms of security documents such as 'Internet and email usage policies' [2]; 'copyright policies'' [18] that could complement the information security policy. As a result, there is a significant need for a focused, empirical study to examine the structural arrangements of information security policies, as they are currently being adapted and practiced by organizations [7].

The structure of information security policy has been largely discussed in the literature (although it lacks in empirical contributions and consensus). However, in academic, there is a fairly limited discussion about the particular issues that need to be addressed by the information security policy. The international standard 17799 ISO:2005 gives indications about the types of issues that can be addressed by information security policy, but the issues are less subjected to academic security. One of the very few attempts to precisely fill this gap was an empirical study by [7] about information security policies across large organizations in the UK, based on a framework where potential policy issues extracted from the literature. Even though the research offers useful insights, it lacks inconsistency of approach and terminology, because the study was drawn based on perceptions of IT decision makers about their own content of policy, rather than focusing on the actual content of policy [7].

In addition to concerns regarding the structure and content of policy, there are also concerns regarding policy effectiveness. Many organizations claim to have developed and implemented information security policy [20]. However, looking at the results, high degrees of information security

incidents and breaches suggest that there is a lack of effectiveness and/or communication of policy. In fact, the study by [34] revealed that there had been no significant changes in the number of security breached in organizations that had adopted an information security policy in comparison with those that had not. One possible reason for the ineffectiveness of information security policies is that organizations follow narrow policies that only focus on issues of information confidentiality, integrity, and availability. Unfortunately, infrastructure technology has failed to address increasingly important human and organizational aspects [6]. In fact, the most commonly adopted policy standard ISO 17799 (2005) @24) focus on the technically oriented conceptualization of information security (availability, confidentiality, and integrity), and ignores human factors such as trust, ethicality and the integrity of users [7].

A. Policy Writing Guidelines

Policies are high-level statements that correspond to corporate law that drives decision making in a university that is subject to a serious review process. The university's information security policies are accessible on their website. Standards are minimum requirements developed to address specific issues and requirements that ensure compliance with policies. Standards are used for verification purposes for audit and assessment. Every faculty and department are required to follow the standards and the adoption of local standards are encouraged to surpass the minimum requirements. A procedure is step-by-step instructions to accomplish certain tasks. Procedures can be also used to maintain compliance with regulations. Guidelines provide additional recommendations that provide a framework to help compliance with policies. They are more technical in nature compared to policies and standards. They are also updated more frequently to address changes in technology and university practices [28]. Fig. 1 presents the policy-making process.

Policy writing task should be done by reaching the intended audience with policies that are Clear, Easy to read and provide the right level of information to those affected by the content. If users understand a policy, they are more likely to follow it and incorporate it into their daily work. The key elements of a policy document are identified as 1) Policy Title, 2) Administrative Policy Statement Number and Functional Area, 3) Brief Description, 4) Applies To, 5) Reason for Policy, 6) Introduction, 7) Policy Statement, 8) Definitions, 9) Related Policies, Procedures, Forms, Guidelines, and Other Resources, 10) History, 11) Key Words [27].

- *Use Language That Reflects the Policy's Intent:*

Select the words carefully. Words like "should" and "may" imply a choice. For example, "Faculty and staff should not smoke in class." This means they shouldn't smoke but will be allowed if they do. The statement also does not address restrictions applicable to students. Examples of alternative phrasing would be: "Faculty, staff, and students are prohibited from smoking in class." this is much better, but only addresses a class setting. The best way to rewrite is "Smoking is not allowed inside University buildings".

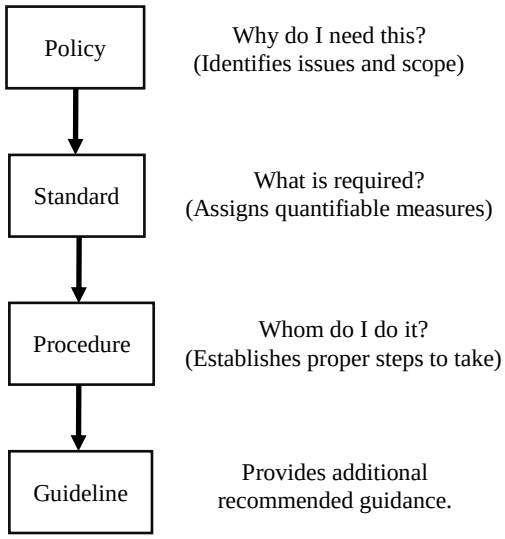

Fig. 1. Policymaking process

- *Use as Few Words as Possible to State a Case*

For instance, "All University faculty and staff, under the leadership of its officers, are obligated to ensure that University funds are used only for mission-related purposes." This statement implies that only those under the leadership are required to follow the policy. An alternative to the above statement is: "Employees must ensure that University funds are used only for mission-related purposes."

- *Ensure that Clarifying a Statement Did Not Alter Its Meaning:*

For example, "All faculty and staff must attend weekly meetings" The word "all" is redundant. Simply stating "Faculty and staff" implies all unless an exception is also written.

IV. Review of Information Security Policy Development Frameworks

A. A Generic Framework for Information Security Policy Development

Reference [12] proposed a general framework to enhance security policies development process of higher education, using content analysis and cross-case analysis methods (Fig. 2). The proposed framework could be used as a guide to developing more comprehensive and sustainable information security policies in the institution of higher education. The framework can be used as a guideline to improve or develop a policy management program. However, the framework is too general, and it is necessary to explore more specific development processes such as the Acceptable Use Policy or any specific system security policy.

In [12] identified risk assessment as the major part policy development process since it systematically identifies, analyzes and evaluates the information security threats related to information systems and services as well as required controls to manage them. The process of risk identification involves identifying information assets, threats, and vulnerabilities. These are the important elements in identifying

the origin of incidents that could potentially affect the university information assets. The findings indicate that comprehension of security policy's content could be determined by the risk assessment.

B. The Policy Development Framework Including the ISPDLC Components

The result of a study by [9] shows that the most important of constructs is Risk Assessment (Fig. 3). Therefore, Risk Assessment should be the prior step in developing an information security policy in order to identify the risks that need to be mitigated. Subsequently, Management Support is the second most important construct. Managers use policies to clarify their management intentions and direction. The result of the study also shows that Policy Monitoring was the least important construct. This suggests that the area of Policy Monitoring requires more attention. The content analysis implied similar results, with information security monitoring being the lowest frequency of tags among all categories.

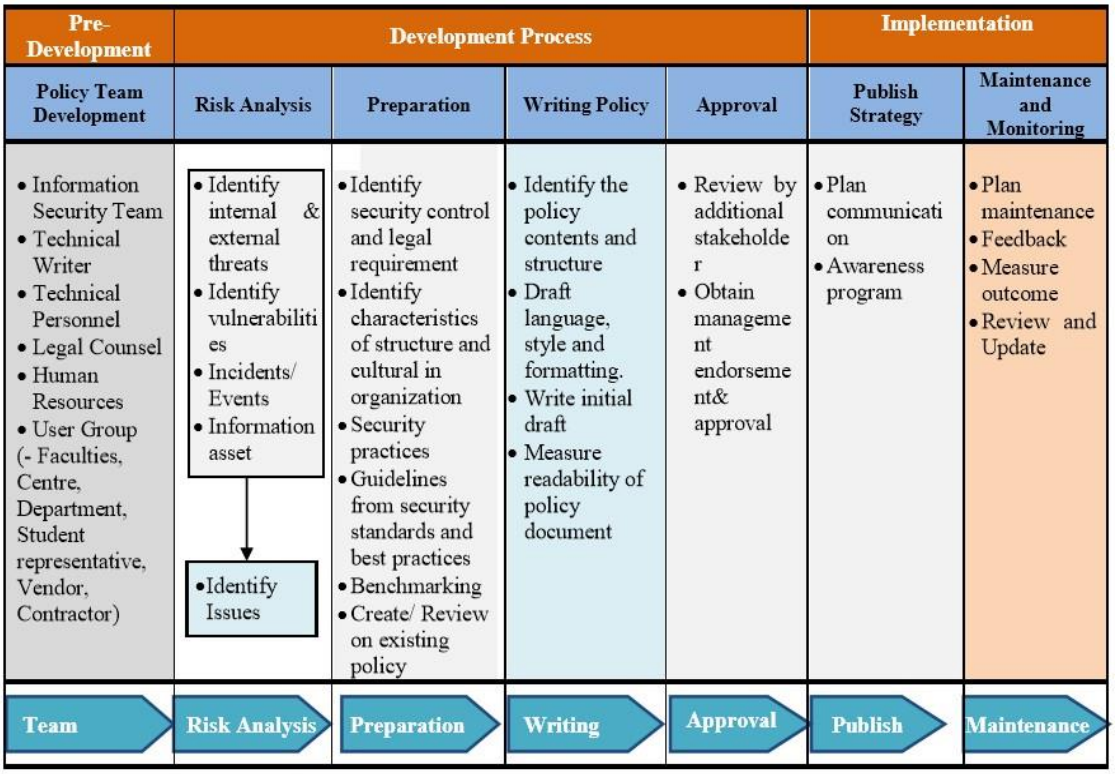

Fig. 2. A generic framework for information security policy development.

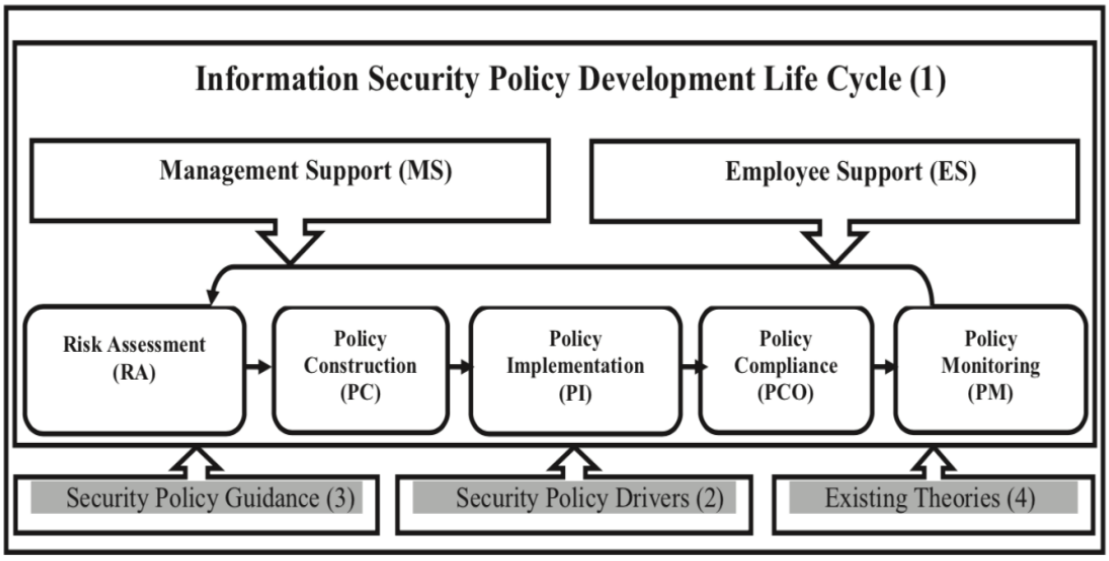

Fig. 3. The Policy development framework including the ISPDLC component.

The study by [9] has some limitations. The first one is the demographics of the respondents in the survey. The responded were only selected from the U.S. and the U.K. which makes it difficult to generalize the findings of the study, as the two countries are developed with advanced technology. Hence, while developing a framework, one should provide guidelines that can be adopted by both developed and underdeveloped countries to enhance their information security policy development process. In many developed countries, by law, senior managers or a board of directors are in charge of information security and risk management. Therefore, organizations have to spend resources to ensure the protection of an organization's information. However, this may not necessarily happen, especially in smaller organizations.

The second limitation is the time and cost involved in implementing the processes proposed in the framework. It requires organizations to have sufficient budget to cover all the costs such as the costs of conducting a risk assessment, constructing the information security policy, consulting with stakeholders, conducting training and education sessions and monitoring users' activities by, perhaps, using an automated monitoring system. Moreover, the costs are even higher for larger organizations as they require a significant amount of time and other resources. Lastly, the decision to develop and implement an information security policy should be based on organization security needs. Thus, a cost-benefit analysis should be carried on to understand whether it is worth for a particular organization to spend a large number of resources to do this exercise [9].

V. METHODOLOGY

As content analysis is helpful to identify trends and patterns in documents, this study focuses on two level of content analysis; first, to study information security policy development process for institutions of higher education, and second, to compare it to the common security information policy development adopted by organizations, which is discussed in the following sections. To fulfill this requirement, this study focused on the comparison of eleven universities' information security policy [12]. Information security policy is largely recognized as the most important information security mechanism to prevent, detect and respond to security breaches. Therefore, it plays important role in IT-enable organizations especially defining the scope and content of information security policies. Each university's website was reviewed to identify the available policy documents and the information security coverage. Furthermore, the policies were reviewed in terms of aesthetics, navigation, and content.

A. University Selection

To ensure the consistency and accuracy of data collection from the information security policies of each university, a pro forma was devised. This pro forma was used to review the policies of eleven universities. The pro forma data collection document comprised the following four broad components:

- *University Details (Table I):*

Name, abbreviation, country, position in worldwide university ranking, website address; eleven universities have been selected from North America, Europe, Australia and Asia. All the selected universities are ranked below 250 worldwide, based on QS 2018 rankings.

- *Policy Administration Details (Table I):*

Details about the responsible department for the creation, management, and maintenance of the policy which includes responsible unit, phone number, and email address. Only responsible units are added to Table I to avoid invasion of personal privacy.

- *Policy structure (Table II):*

Types of available policy on the university website, besides the information security policy (e.g. Acceptable Use of Information Technology Resources Policy, Data Security Classification Policy).

- *Policy Coverage (Table II):*

Information security coverage and policy titles are listed here from each university's website. This task was cross-checked during the investigation by sending out emails to the respective university to ensure the accuracy and consistency. The contents of the pro forma were then summarized in Tables I and II to enable comparisons to be made.

TABLE I. UNIVERSITY AND POLICY ADMINISTRATION DETAILS

University	Abbrev.	University details			Responsible Unit
		Country	Ranking	Website	
University of Arizona	Arizona	United States of America	230	http://www.arizona.edu	UA Information Security
University of Minnesota	UMN	United States of America	163	https://twin-cities.umn.edu	UMN Office of Information Technology
Durham University	DUR	United Kingdom	78	https://www.dur.ac.uk	DUR IT Service Desk
University of Oxford	OX	United Kingdom	6	http://www.ox.ac.uk	OX University Council
University of Wollongong	UOW	Australia	232	https://www.uow.edu.au	UOW Information Management & Technology Services (IMTS)
Monash University	Monash	Australia	60	https://www.monash.edu	Monash IT Service Desk
University of Malaya	UM	Malaysia	114	https://www.um.edu.my	UM Information Technology Center
Universiti Kebangsaan Malaysia	UKM	Malaysia	230	http://www.ukm.my	UKM Information Technology Center

City University of Hong Kong	Cityu	Hong Kong	49	http://www.cityu.edu.hk	Cityu Information Security Unit
The Chinese University of Hong Kong	CHUK	Hong Kong	46	http://www.cuhk.edu.hk	CHUK Information Technology Services Center
National University of Singapore	NUS	Singapore	15	http://www.nus.edu.sg	NUS IT Care

B. *Information Security Policies and Coverage*

The introduction part of every university' policy was helpful to understand its overall standpoint of information security. Some universities are concerned more about hardware protection or physical security, whereas other universities are more focused on confidentiality and integrity aspects of information assets and administrative data. There are some universities that emphasize the need for information for research. Therefore, they want to ensure security practices help to promote research activities while protecting against attack. Because there are various areas of focus by different universities, we are not surprised to have found out there are also various policy structural arrangements and coverage. As illustrated in Table II the selected universities have different policies and the information security content coverage varies among them. The differences are determined during the risk analysis when the policy development team identifies the internal and external threats, vulnerabilities, incidents and information security assets.

TABLE II. POLICY TILES AND INFORMATION SECURITY COVERAGE

University	Policy Title	Information Security Coverage
University of Arizona	• General Information Security Policy • Computer and Network Access Agreement Policy • Acceptable Use of Computers and Networks Policy • Electronic Privacy Statement Policy	• Information Security Policy • Asset Management • Human Resource Security • Physical and Environmental Security • Communications and Operations Management • Access Control • Information Systems Acquisition, Development, and Maintenance • Business Continuity Management • Compliance • Risk Assessment
University of Minnesota	• Acceptable Use of Information Technology Resources Policy • Data Security Classification Policy • Information Security Policy • Information Security Risk Management Policy • Internal Access to and Sharing University Information Policy • Reporting and Notifying Individuals of Information Security Breaches Policy • Including Privacy Statement on U Web Pages Policy	• Acceptable Use of Information Technology Resources • Data Security Classification • Information Security • Information Security Risk Management • Internal Access to and Sharing University Information • Reporting and Notifying Individuals of Information Security Breaches • Including a Privacy Statement on U Web Pages
University of Durham	• Overarching Information Security Policies 1. Information Security Policy • Data Protection and Information Management Policies 1. Data Protection Policy 2. Records Management Policy and Records Retention Schedule • IT Regulations and Policies	• Online Security • Data Handling • Responsibilities • Training and Advise
University of Oxford	• Data Protection: University Policy • Data Quality Policy • Freedom of Information Policy • Information Security Policy • Records Management Policy • Research Related Policy • Statement of Janet acceptable use policy	• Access to the Janet for non-members • Advertising material on University web pages • Compliance • Disclaimer of liability • Disposal of old computers • Guidelines for handling illegal material • IT Rules • Mobile wireless networking regulations • Peer-to-peer resource sharing • Rules on mass mailing
University of Wollongong	• Cyber Security Policy • IT Acceptable Use Policy • IT Server Security Policy • Telephone and Mobile Use Policy	• Computer Room Access • Cyber Security • IT Acceptable Use • IT User Account Management • Telephone and Mobile Use
Monash University	• Access to and Use of Electronic Resources Licensed by the Library Policy • Information Technology Acceptable Use Policy • Electronic Information Security Policy • Record-keeping Policy • Student Electronic Message Broadcast Policy • Web Accessibility Policy	• Access to and Use of Electronic Resources Licensed by Library • Information Technology Acceptable Use • Electronic Information Security • ICT Security and Risk Management • Record-keeping • Student Electronic Message Broadcast • Web Accessibility

University	Policy Title	Information Security Coverage
university of Malay	• General Information Security Policy • ICT Security Policy • Wireless Communication Policy • Email Usage Policy • Server Colocation at PTM Data Centre Policy • Web Hosting Policy • Server handling Centre of Responsibility Policy • Firewall Policy • Malware Policy • Removal and Disposal of Media Policy • Supplier Management Policy • Source Code Management Policy • System Planning and Acceptance Policy • Termination Policy • Wireless Communication Policy	• General • ICT Security • Network • Email • ICT Resources Management • Third Party / Vendor • Software • Website
Universiti Kebangsaan Malaysia	ICT Policies and Regulations	• Data Protection • Storage Security • Your Privacy • Information Collected • Policy Amendments
National University of Singapore	• IT Security Policy • Acceptable Use Policy	• Information Security • Protect Your Computer • Protect Your Data • Protect your Privacy
City University of Hong Kong	• Policy on Use of IT Services and Facilities • Information Security Policy and Standards • Domain Name System Policy and Guidelines • Password Management Policy for User and System Accounts • Software Copyright Declaration and Compliance Observation	• Use of IT Services and Facilities • Information Security and Standards • Domain Name System • Computer Account Retention for Leaving Staff • Retention for Deleted Email on MS Office 365 • Password Management for User and System Accounts
The Chinese University of Hong Kong	• University IT Policies • University IS Policies and Standards • Acceptable Use Policies and Guidelines	• ICT Facilities & Services • OnePass Password Expiry • WiFi • Sharing Large Computer Equipment • Information Security • Display Name for Office 365 • Email Address for Staff • Computer Network, Access, and Usage • Email and the Internet Services • Data Centre and Networks • Computing Systems, Software and Account Information • Computer Laboratory

C. Online Presentation and Content Coverage

In [39] define aesthetic as the study of emotions and mind in the related notions such as the beautiful, the ugly as applicable to the fine arts. The aesthetic issue can influence user perception of a website. User's emotion and attitude can play an important role to attract the user's attention and keeping website trustworthy. Factor influencing the perception of beauty are balance proportion, informational content and complexity, contrast and clarity, and symmetry. Factors for aesthetic design features are visual complexity, color, and balance and symmetry [39].

In the case of navigation, it should lead the user to an easy, convenient and efficient browsing experience. Pagination navigation should not be invisible for users, hard to understand and difficult to identify [41]. In order to reduce the risk of users feeling disoriented and to assist them in finding information, navigation link should be the same from page to page [40].

The focus for content strategy is on the planning, creation, delivery, and governance content which might represent by text, images and multimedia [43]. Best practice for creating content meaningful identified by [43] are:

- Reflect your organization's goals and the user's needs.
- Understand how the user's think and speak about a subject.
- Communicate to people in a way that they understand.
- Be useful.
- Stay up-to-date and remain factual.
- Be accessible to all people.
- Be consistent.
- Be able to be found.
- Help define the requirements for the overall site.

In this study, the policies of 11 HEI Information Security Policies have been reviewed based on the criteria suggested by [42] as follows:

Aesthetics:

- What feel does the website give orderly or messy? Sparse or crowded? Playful or formal?
- Is the style consistent throughout the website?
- Where are photos or decorative touches getting in the way of my message?

Navigation:

- How easy is it to find information?
- Is there a search button for visitors?
- Do all the links work?

Content:

- Does the design make content easy to find?
- Will this content be relevant to the reader?
- Is the content concise but still useful?

TABLE III. UNIVERSITY WEBSITE AND CONTENT REVIEW

University	Aesthetics	Navigation	Content
University of Arizona	• Attractive and simple design – Orderly, sparse, formal. • The style is inconsistent throughout the website • photos or decorative touches do not get in the way of the message	• Simple navigation without the need to guess • There is a search button • All links work	• Information is easy to find • Content is relevant • Content is concise but useful
University of Minnesota	• Appealing and simple design – Crowded but orderly, formal. • The style is consistent throughout the website • photos or decorative touches do not get in the way of the message	• Simple navigation without the need to guess • There is a search button • All links work	• Information is easy to find • Content is relevant • Content is comprehensive
University of Durham	• Simple design – Orderly, sparse, formal. • The style is consistent throughout the website • photos or decorative touches do not get in the way of the message	• Poor navigation - User can get lost in navigating between pages • There is a search button • All links work	• Information is not easy to find • Content is relevant but very brief in some cases • Content is presented in a form of: i. What do you know about this? ii. What do you need to do? (Do…, Don't…) iii. Where to next?
University of Oxford	• Attractive design – Orderly, sparse, playful. • The style is consistent throughout the website • photos or decorative touches do not get in the way of the message	• Simple navigation without the need to guess • There is a search button • All links work	• Information is easy to find • Content is relevant • Content is comprehensive
University of Wollongong	• Attractive design – Orderly, sparse, playful. • The style is consistent throughout the website • photos or decorative touches do not get in the way of the message	• Simple navigation without the need to guess • There is a search button • All links work	• Information is easy to find • Content is relevant • Content is concise but useful
Monash University	• Simple design – Orderly, Crowded, formal. • The style is inconsistent throughout the website • photos or decorative touches do	• Poor navigation - User can get lost in navigating between pages as most links open in PDF • There is a search button only	• Information is not easy to find – lack of good navigation and search button • Content is relevant • Content is concise but useful

University	Aesthetics	Navigation	Content
	not get in the way of the message	on the homepage • All links work	
University of Malay	• Appealing and simple design – Orderly, sparse, formal. • The style is consistent throughout the website • photos or decorative touches do not get in the way of the message	• Simple navigation without the need to guess • There is a search button on the main page only • All links work	• Information is not easy to find as the content is missing for some the policies and related documents • Content is relevant but not in single/default language. Some of the content is provided in English whereas the others in the Malay version. • Hyperlinks are not active for all PDF documents.
Universiti Kebangsaan Malaysia	• Appealing and simple design – Sparse and formal. • The style is consistent throughout the website • photos or decorative touches do not get in the way of the message	• Poor navigation as information is spread across multiple pages without direct links • There is a search button • No links to connect the relevant pages • Some of the links do not work • Some link load PDF in the browser whereas the others download the PDF without permission	• Information is not easy to find – Only covers UKM web security policy • Information security policies are presented as highlights and the content cannot be found • There is no default language as the English content is mixed with Malay version • Spelling mistakes – e.g. Guidelines • Does not state the objective and scope of UKM information security policy
National University of Singapore	• Appealing and simple design – Orderly, sparse, formal. • The style is consistent throughout the website • Photos or decorative touches can get in the way of the message	• Poor navigation – Redundant and confusing navigation Panes • There is a search button • All links work	• Information is not easy to find – Only registered users are allowed to access the most of policies and guidelines. • Content is relevant but very brief in some cases • Content is presented in a form of: i. Protect Your Computer ii. Protect Your Data iii. Protect Your Privacy
City University of Hong Kong	• Simple design – Orderly, crowded, formal. • The style is inconsistent throughout the website • photos or decorative touches do not get in the way of the message	• Simple navigation without the need to guess • There is a search button • All links work	• Information is easy to find • Content is relevant • Content is concise but useful
The Chinese University of Hong Kong	• Attractive design – Orderly, sparse, playful. • The style is consistent throughout the website • photos or decorative touches do not get in the way of the message	• Simple navigation without the need to guess • There is a search button • All links work	• Information is easy to find – Restricted access for some documents • Content is relevant • Content is comprehensive

Reviews from selected websites have been divided into three criteria aesthetics, navigation and content, as shown in Table III. Based on the table, we further highlight the existence of the respective criteria as shown in Table IV.

The strength of online presentation of this policies in terms of aesthetic elements are being attractive, orderly, sparse, simple, consistent, photos/decorative do not get in the way of the message, formal and appealing. However, some of the policies have issues in term of being inconsistent, crowded, playful and photos and decorative touches can get in the way of the message. Navigation strength of these policies are: simple navigation without the need to guess, search button available and link work.

Nonetheless, other identified issues are poor navigation where the user might get lost while searching for certain information, information is spread on multiple pages without a direct link, search functions are available on home page only, some link is not working and load pdf and download pdf without permission.

The strengths related to content are; easy to find, relevant content, concise but useful, and comprehensive. However, other identified issues are information not easy or cannot be found, brief and mixed, content is displayed in question and point form. Identified strengths from related websites can be a guide in order to design a good interface and avoiding some bad design issue of a website.

TABLE IV. ELEMENTS USED FOR AESTHETIC, NAVIGATION AND CONTENT CRITERIA

University	Aesthetic								Navigation			Content			
	Attractive	Orderly	Sparse	Simple	Consistent	Photos/ decorative do not get in the way of the message	Formal	Appealing	Simple Navigation	Search Button	Link Work	Easy to find	Relevant	Concise but useful	Comprehensive
University of Arizona	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	
University of Minnesota		✓		✓	✓	✓	✓	✓		✓	✓	✓	✓		✓
University of Durham		✓	✓	✓	✓	✓	✓		✓	✓	✓		✓		
University of Oxford	✓	✓	✓		✓	✓			✓	✓	✓	✓	✓		✓
University of Wollongong	✓	✓	✓		✓	✓				✓	✓	✓	✓	✓	
Monash University		✓		✓		✓	✓			✓	✓		✓	✓	
University of Malay		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		
Universiti Kebangsaan Malaysia			✓	✓	✓	✓	✓	✓		✓					
National University of Singapore		✓	✓	✓	✓		✓	✓		✓	✓		✓		
City University of Hong Kong		✓		✓		✓	✓		✓	✓	✓		✓	✓	
The Chinese University of Hong Kong	✓	✓	✓		✓	✓			✓	✓	✓	✓	✓		✓

Not all of 114 controls are mandatory as an organization can choose which controls are applicable and needs to be implemented and the rest could be declared as non-applicable. For example, the A.14.2.7 control, “Outsourced development” can be marked as non-applicable if the organization does not outsource any software development. The main criterion for selection of controls is the risk management as defined in clauses 6 and 8 of the ISO 27001.

ISO 27001:2013 Annex A is divided into three sections of mandatory documents, mandatory records and non-mandatory documents. Table V presents the structure of controls for the organization to be used to improve the security of information assets. (Please note that documents from Annex A are mandatory only if there are risks which would require their implementation).

TABLE V. ISO 27001:2013 ANNEX A MANDATORY AND NON-MANDATORY DOCUMENTS AND RECORDS

Mandatory documents required by ISO 27001:2013	Non-mandatory documents and records required by ISO 27001:2013	Mandatory records required by ISO 27001:2013
1. The scope of the ISMS (clause 4.3) 2. Information security policy and objectives (clauses 5.2 and 6.2) 3. Risk assessment and risk treatment methodology (clause 6.1.2) 4. Statement of Applicability (clause 6.1.3 d) 5. Risk treatment plan (clauses 6.1.3 e and 6.2) 6. Risk assessment report (clause 8.2) 7. Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4) 8. Inventory of assets (clause A.8.1.1) 9. Acceptable use of assets (clause A.8.1.3) 10. Access control policy (clause A.9.1.1) 11. Operating procedures for IT management (clause A.12.1.1) 12. Secure system engineering principles (clause A.14.2.5) 13. Supplier security policy (clause A.15.1.1) 14. Incident management procedure (clause A.16.1.5) 15. Business continuity procedures (clause A.17.1.2) 16. Statutory, regulatory, and contractual requirements (clause A.18.1.1)	1. Procedure for document control (clause 7.5) 2. Controls for managing records (clause 7.5) 3. Procedure for internal audit (clause 9.2) 4. Procedure for corrective action (clause 10.1) 5. Bring your own device (BYOD) policy (clause A.6.2.1) 6. Mobile device and teleworking policy (clause A.6.2.1) 7. Information classification policy (clauses A.8.2.1, A.8.2.2, and A.8.2.3) 8. Password policy (clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3) 9. Disposal and destruction policy (clauses A.8.3.2 and A.11.2.7) 10. Procedures for working in secure areas (clause A.11.1.5) 11. Clear desk and clear screen policy (clause A.11.2.9) 12. Change management policy (clauses A.12.1.2 and A.14.2.4) 13. Backup policy (clause A.12.3.1) 14. Information transfer policy (clauses A.13.2.1, A.13.2.2, and A.13.2.3) 15. Business impact analysis (clause A.17.1.1) 16. Exercising and testing plan (clause A.17.1.3) 17. Maintenance and review plan (clause A.17.1.3) 18. Business continuity strategy (clause A.17.2.1)	**1.** Records of training, skills, experience, and qualifications (clause 7.2) **2.** Monitoring and measurement results (clause 9.1) **3.** Internal audit program (clause 9.2) **4.** Results of internal audits (clause 9.2) **5.** Results of the management review (clause 9.3) **6.** Results of corrective actions (clause 10.1) **7.** Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3)

TABLE VI. MANDATORY DOCUMENTS REQUIRED BY ISO 27001:2013

Mandatory documents required by ISO 27001:2013	Arizona	UMN	DUR	OX	UOW	Monash	UM	UKM	NUS	Cityu	CHUK
The scope of the ISMS (clause 4.3)	X	X	X	X	X	X	X	X	X	X	X
Information security policy and objectives (clauses 5.2 and 6.2)	√	√	√	√	√	√	√	√	√	√	√
Risk assessment and risk treatment methodology (clause 6.1.2)	√	√	√	√	X	X	X	X	X	X	X
Statement of Applicability (clause 6.1.3 d)	√	X	X	X	X	X	X	X	X	X	X
Risk treatment plan (clauses 6.1.3 e and 6.2)	X	X	X	X	X	X	X	X	X	X	X
Risk assessment report (clause 8.2)	X	X	X	X	X	X	X	X	X	X	X
Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4)	X	X	X	√	X	√	X	X	X	X	X
Inventory of assets (clause A.8.1.1)	X	X	X	X	X	X	X	X	X	√	X
Acceptable use of assets (clause A.8.1.3)	√	√	X	X	√	√	X	X	√	√	X
Access control policy (clause A.9.1.1)	√	√	√	√	√	√	√	X	X	√	√
Operating procedures for IT management (clause A.12.1.1)	√	X	X	√	X	X	X	X	X	√	X
Secure system engineering principles (clause A.14.2.5)	X	X	X	X	X	X	X	X	X	X	X
Supplier security policy (clause A.15.1.1)	X	X	X	√	X	X	√	X	X	√	X
Incident management procedure (clause A.16.1.5)	√	X	X	√	X	X	X	X	X	√	X
Business continuity procedures (clause A.17.1.2)	√	X	X	X	X	X	X	X	X	√	X
Statutory, regulatory, and contractual requirements (clause A.18.1.1)	X	X	X	X	X	X	X	X	X	X	X
Total documents found out of 16 mandatory required documents	8	4	3	7	3	4	3	1	2	8	2

The selected universities' policies were reviewed in order to investigate the compliance with mandatory and non-mandatory documents and records by ISO 27001:2013. This task was cross-checked during the investigation by sending out emails to the respective university to ensure the accuracy and consistency. The findings were then summarised in Tables VI, VII and VIII to enable comparisons to be made. Table VI results show that none of the selected universities complied with all mandatory and no-mandatory documents and records from ISO 27001 Annex A.

This is again due to the policy development process, where the risk analysis task gives direction to policymakers to focus on certain information security issues. For instance, the University of Arizona made 8 out of 16 mandatory annex A documents available on the university's website, whereas the University Kebangsaan Malaysia has only 1 document available to be accessed by the visitors. Developing and dividing the information security content into standalone documents makes it easier to deliver the message to the intended audience and make the process more efficient.

TABLE VII. NON-MANDATORY DOCUMENTS AND RECORDS REQUIRED BY ISO 27001:2013

Non-mandatory documents and records required by ISO 27001:2013	Arizona	UMN	DUR	OX	UOW	Monash	UM	UKM	NUS	Cityu	CHUK
Procedure for document control (clause 7.5)	√	X	X	X	X	X	X	X	X	X	X
Controls for managing records (clause 7.5)	X	X	X	X	X	√	X	X	X	X	√
Procedure for internal audit (clause 9.2)	X	X	X	X	X	X	X	X	X	X	X
Procedure for corrective action (clause 10.1)	X	X	X	X	X	X	X	X	X	X	X
Bring your own device (BYOD) policy (clause A.6.2.1)	X	X	√	X	√	X	X	X	X	X	X
Mobile device and teleworking policy (clause A.6.2.1)	X	X	√	X	X	X	X	X	X	X	X
Information classification policy (clauses A.8.2.1, A.8.2.2, and A.8.2.3)	√	X	√	X	X	√	X	X	X	√	X
Password policy (clauses A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3)	√	X	√	X	X	X	X	X	X	√	√
Disposal and destruction policy (clauses A.8.3.2 and A.11.2.7)	X	X	X	X	X	X	X	X	X	X	X
Procedures for working in secure areas (clause A.11.1.5)	X	X	X	X	X	X	X	X	X	X	X
Clear desk and clear screen policy (clause A.11.2.9)	X	X	X	X	X	X	X	X	X	X	X
Change management policy (clauses A.12.1.2 and A.14.2.4)	X	X	X	X	X	X	X	X	X	√	X
Backup policy (clause A.12.3.1)	X	X	√	X	X	X	X	X	X	√	X
Information transfer policy (clauses A.13.2.1, A.13.2.2, and A.13.2.3)	√	√	√	X	X	X	X	X	X	X	X
Business impact analysis (clause A.17.1.1)	√	X	X	X	X	X	X	X	X	X	X
Exercising and testing plan (clause A.17.1.3)	X	X	X	X	X	X	X	X	X	X	X
Maintenance and review plan (clause A.17.1.3)	√	X	√	X	X	X	X	X	X	√	√
Business continuity strategy (clause A.17.2.1)	√	X	X	X	X	X	X	X	X	√	X
Total documents found out of 18 mandatory required documents	7	1	7	0	1	2	0	0	0	6	3

TABLE VIII. MANDATORY RECORDS REQUIRED BY ISO 27001:2013

Mandatory records required by ISO 27001:2013	Arizona	UMN	DUR	OX	UOW	Monash	UM	UKM	NUS	Cityu	CHUK
Records of training, skills, experience, and qualifications (clause 7.2)	√	X	√	√	X	X	X	X	X	X	X
Monitoring and measurement results (clause 9.1)	X	X	√	X	X	X	X	X	X	X	X
Internal audit program (clause 9.2)	X	X	X	X	X	X	X	X	X	√	X
Results of internal audits (clause 9.2)	X	X	X	X	X	X	X	X	X	X	X
Results of the management review (clause 9.3)	X	X	X	X	X	X	X	X	X	X	X
Results of corrective actions (clause 10.1)	X	X	X	X	X	X	X	X	X	X	X
Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3)	√	√	√	X	X	X	X	X	X	√	X
Total documents found out of 18 mandatory required records	2	1	3	1	0	0	0	0	0	2	0

VI. DISCUSSION

An effective information security policy should convert an organization's requirements into precise, measurable objectives that are readable and consistent [10]. Developing such information security policy that fulfills an organization's requirement is not easy an easy task. Duplicating a policy document from other organizations may not be sufficient to address issues such as compliance with regulatory requirements even though the replicated policy document is well-developed and properly referenced [16][3][4]. Thus, the security policy document must be developed based on the organization's culture, operations, environmental factors and policy requirement [25]. Therefore, the development process of information security policy should be tailored based on characteristics of the organizations, organizational culture, the potential technology changes in hardware and software, users and management support [5]. This applies to industries such as Higher Education where each university comprises diverse management structures, faculties, and departments, and practice different forms of behavior [21]. According to [13][9] studies often focus on the structure and content of policy but less on the development process, especially the step-by-step process. Hence, this paper exclusively focused on information security policy development in institutions of higher education [12].

If organizations seek to obtain ISO certification they must meet ISO 27001:2013 minimum requirement. These requirements are known as Annex A which includes mandatory and non-mandatory documents for organizations to create their policies based on. Many universities tend to develop a single document for all the policies and procedures (e.g. UKM), whereas other universities develop standalone policy documents based on ISO requirements. It is necessary to develop multiple policy documents because makes it possible to reach out to a targeted audience.

This paper conducted a comparative review of information security policy documents of eleven universities. The objective is to review policy documents based on i) ISO 27001: 2013 mandatory and unmannerly requirements and ii) available frameworks and guidelines for the development of policy for higher education. The findings show that none of the selected universities have produced documents for all required mandatory and unmannerly requirements. This is due to risk analysis that should be the initial stage of policy development where the universities must identify the organization-specific issues as well as the organization regulatory agreements. Thus, developing a policy document for all Annex A requirements may not be necessary for every organization.

The information security policies must be accessible from the university website. However, not all policies should be accessible by the public. The policies should be divided into two categories including public and privet. The policies intended for the public must be accessible by everyone whereas the privet policies should be restricted by user authentication or require to be accessed within the university internal network. The privet policies are made for university stakeholders and internal use only. Making these policies accessible makes the organization vulnerable by giving an edge to those with prying eyes.

VII. CONCLUSION

The process of developing and implementing an effective information security policy is not a clear cut. It is vital for universities to realize the significance of the development process of information security policy for the institutions of higher education. The challenge for higher education institutions is to understand how to develop and implement information security policy effectively based on risk analysis in accordance with the organization's requirements. Otherwise, in case of security breaches or violations, it is less likely to enforce regulations due to incomplete or incomprehensible security policies document. This paper selected 11 universities to review their information security policies in contrast with ISO 27001:2013 minimum requirements to reach a concise understanding of the policy-

making process and what is being practiced in higher education. This study can be used as a guide for other universities who are developing or improving their information security policy to comply with ISO 27k series.

ACKNOWLEDGMENT

This study is supported by University Kebangsaan Malaysia (UKM). Grant code: AP-2017-003/2.

REFERENCES

[1] V. Anand, J. Saniie, and E. Oruklu, "Security policy management process within six sigma framework," J. Inf. Secur., vol. 3, no. 1, p. 49, 2012.

[2] D. W. Arnesen and W. L. Weis, "Developing an effective company policy for employee internet and email use," J. Organ. Cult. Commun. Confl., vol. 11, no. 2, p. 53, 2007.

[3] R. Baskerville and M. Siponen, "An information security meta-policy for emergent organizations," Logist. Inf. Manag., vol. 15, no. 5/6, pp. 337–346, 2002.

[4] F. Bjorck, "Institutional theory: A new perspective for research into IS/IT security in organisations," in System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on, 2004, p. 5–pp.

[5] S. C. Clark, R. A. Griffin, and C. K. Martin, "Alleviating the policy paradox through improved institutional policy systems: A case study," Innov. High. Educ., vol. 37, no. 1, pp. 11–26, 2012.

[6] G. Dhillon and G. Torkzadeh, "Value-focused assessment of information system security in organizations," Inf. Syst. J., vol. 16, no. 3, pp. 293–314, 2006.

[7] N. F. Doherty, L. Anastasakis, and H. Fulford, "The information security policy unpacked: A critical study of the content of university policies," Int. J. Inf. Manage., vol. 29, no. 6, pp. 449–457, 2009.

[8] N. F. Doherty, L. Anastasakis, and H. Fulford, "Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy," Int. J. Inf. Manage., vol. 31, no. 3, pp. 201–209, 2011.

[9] S. V Flowerday and T. Tuyikeze, "Information security policy development and implementation: The what, how and who," Comput. Secur., vol. 61, pp. 169–183, 2016.

[10] S. Goel and I. N. Chengalur-Smith, "Metrics for characterizing the form of security policies," J. Strategy. Inf. Syst., vol. 19, no. 4, pp. 281–295, 2010.

[11] K.-S. Hong, Y.-P. Chi, L. R. Chao, and J.-H. Tang, "An empirical study of information security policy on information security elevation in Taiwan," Inf. Manag. Comput. Secur., vol. 14, no. 2, pp. 104–115, 2006.

[12] W. B. W. Ismail, S. Widyarto, R. A. T. R. Ahmad, and K. A. Ghani, "A generic framework for information security policy development," in Electrical Engineering, Computer Science and Informatics (EECSI), 2017 4th International Conference on, 2017, pp. 1–6.

[13] N. B. L. Jr, "Information Security Policy Development: A Literature Review," Int. J. Innov. Res. Inf. Secur., vol. 3, no. 04, pp. 1–7, 2016.

[14] R. Saint-Germain, "Information Security Management Best Practice Based on ISO/IEC 17799," Inf. Manag. J., vol. 39, no. 4, pp. 60–66, 2005.

[15] K. J. Knapp, R. F. Morris Jr, T. E. Marshall, and T. A. Byrd, "Information security policy: An organizational-level process model," Comput. Secur., vol. 28, no. 7, pp. 493–508, 2009.

[16] R. P. Kusserow, "Developing and Managing Compliance Policy Documents," J. Heal. Care Compliance—May–June, p. 28, 2014.

[17] B. Lebek, J. Uffen, M. Neumann, B. Hohler, and M. H. Breitner, "Information security awareness and behavior: a theory-based literature review," Manag. Res. Rev., vol. 37, no. 12, pp. 1049–1092, 2014.

[18] K. A. Loggie et al., "An analysis of copyright policies for distance learning materials at major research universities," J. Interact. Online Learn., vol. 5, no. 3, pp. 224–242, 2006.

[19] S. Maynard and A. B. Ruighaver, "What makes a good information security policy: a preliminary framework for evaluating security policy quality," in Proceedings of the fifth annual security conference, Las Vegas, Nevada USA, 2006, pp. 19–20.

[20] J. Merete Hagen, E. Albrechtsen, and J. Hovden, "Implementation and effectiveness of organizational information security measures," Inf. Manag. Comput. Secur., vol. 16, no. 4, pp. 377–397, 2008.

[21] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study," Comput. Secur., vol. 27, no. 7–8, pp. 241–253, 2008.

[22] N. S. Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," Comput. Secur., vol. 56, pp. 70–82, 2016.

[23] M. S. Saleh, A. Alrabiah, and S. H. Bakry, "Using ISO 17799: 2005 information security management: a STOPE view with six sigma approach," Int. J. Netw. Manag., vol. 17, no. 1, pp. 85–97, 2007.

[24] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," Comput. Secur., vol. 49, pp. 177–191, 2015.

[25] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," Inf. Manag., vol. 46, no. 5, pp. 267–270, 2009.

[26] T. Tuyikeze and S. Flowerday, "Information Security Policy Development and Implementation: A Content Analysis Approach.," in HAISA, 2014, pp. 11–20.

[27] University of Colorado, "User Guide to Writing Policies." [Online]. Available: https://www.cu.edu/sites/default/files/APSwritingguide.pdf.

[28] "Policy and Guidance," University of Arizona. [Online]. Available: https://security.arizona.edu/policy.

[29] M. T. Siponen, "Policies for construction of information systems' security guidelines," in IFIP International Information Security Conference, 2000, pp. 111–120.

[30] D. F. Sterne, "On the Buzzword?? Security Policy??," 1991, p. 219.

[31] K. R. Lindup, "A new model for information security policies," Comput. Secur., vol. 14, no. 8, pp. 691–695, 1995.

[32] B. Moule and L. Giavara, "Policies, procedures and standards: an approach for implementation," Inf. Manag. Comput. Secur., vol. 3, no. 3, pp. 7–16, 1995.

[33] J. Rees, S. Bandyopadhyay, and E. H. Spafford, "PFIRES: A Policy Framework for Information Security," Commun. ACM, vol. 46, no. 7, pp. 101–106, Jul. 2003.

[34] N. F. Doherty and H. Fulford, "Do information security policies reduce the incidence of security breaches: an exploratory analysis," Inf. Resour. Manag. J., vol. 18, no. 4, pp. 21–39, 2005.

[35] S. K. S. Cheung, "Information Security Management for Higher Education Institutions," in Intelligent Data analysis and its Applications, Volume I, Springer, 2014, pp. 11–19.

[36] B. Kerievsky, "Security and confidentiality in a university computer network," ACM SIGUCCS Newsl., vol. 6, no. 3, pp. 9–11, 1976.

[37] S. Singh and D. S. Karaulia, "E-governance: information security issues," in Proceedings of the International Conference on Computer Science and Information Technology, 2011, pp. 120–124.

[38] H.-J. Kam, P. Katerattanakul, G. Gogolin, and S. Hong, "Information Security Policy Compliance in Higher Education: A Neo-Institutional Perspective.," in PACIS, 2013, p. 106.

[39] J. Chen, "The Impact of Aesthetics on Attitudes Towards Websites," Sep-2013.

[40] D. R. Danielson, "Transitional volatility in web navigation," It Soc., vol. 1, no. 3, pp. 131–158, 2003.

[41] M. Hu and Y. Kuang, "Human-machine interface: Design principles of pagination navigation in web applications," in Computer Science & Education (ICCSE), 2014 9th International Conference on, 2014, pp. 1140–1143.

[42] S. Mallon, "5 Ways to Evaluate the Quality of Your Website Design.," straightnorth, 2018. [Online]. Available: https://www.straightnorth.com/insights/5-ways-evaluate-quality-your-website-design/.

[43] Usibility.gov, "Content Strategy Basics." [Online]. Available: https://www.usability.gov/what-and-why/content-strategy.html.