TUGAS AKHIR - IS184853

PENYUSUNAN REKOMENDASI UNTUK MENINGKATKAN KESADARAN KEAMANAN INFORMASI MAHASISWA BERDASARKAN NIST SP 800-50 (STUDI KASUS : INSTITUT TEKNOLOGI SEPULUH NOPEMBER)

RECOMMENDATIONS FOR IMPROVING INFORMATION SECURITY AWARENESS IN HIGHER EDUCATION BASED ON NIST SP 800-50 (CASE STUDY : SEPULUH NOPEMBER INSTITUTE OF TECHNOLOGY)

DYAH WIJI ASTUTI
NRP 052115 4000 0036

Dosen Pembimbing
Eko Wahyu Tyas Darmningrat S.Kom, M.BA
Hanim Maria Astuti, S.Kom, M.Sc., ITIL.

DEPARTEMEN SISTEM INFORMASI
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember
Surabaya 2019

TUGAS AKHIR – IS184853

PENYUSUNAN REKOMENDASI UNTUK MENINGKATKAN KESADARAN KEAMANAN INFORMASI MAHASISWA BERDASARKAN NIST SP 800-50 (STUDI KASUS : INSTITUT TEKNOLOGI SEPULUH NOPEMBER)

DYAH WIJI ASTUTI
NRP 052115 4000 0036

Dosen Pembimbing:
Eko Wahyu Tyas Darmningrat S.Kom, M.BA
Hanim Maria Astuti, S.Kom, M.Sc., ITIL.

DEPARTEMEN SISTEM INFORMASI
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember
Surabaya 2019

FINAL PROJECT - IS184853

RECOMMENDATIONS FOR IMPROVING INFORMATION SECURITY AWARENESS IN HIGHER EDUCATION BASED ON NIST SP 800-50 (CASE STUDY : SEPULUH NOPEMBER INSTITUTE OF TECHNOLOGY)

DYAH WIJI ASTUTI
NRP 052115 4000 0036

Supervisors:
Eko Wahyu Tyas Darmningrat S.Kom, M.BA
Hanim Maria Astuti, S.Kom, M.Sc., ITIL.

INFORMATION SYSTEM DEPARTEMENT
Faculty of Information Technology and Communication
Institut Teknologi Sepuluh Nopember
Surabaya 2019

LEMBAR PENGESAHAN

PENYUSUNAN REKOMENDASI UNTUK MENINGKATKAN KESADARAN KEAMANAN INFORMASI MAHASISWA BERDASARKAN NIST SP 800-50 (STUDI KASUS : INSTITUT TEKNOLOGI SEPULUH NOPEMBER)

TUGAS AKHIR
Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember

Oleh:

DYAH WIJI ASTUTI
05211540000036

Surabaya, 18 Juli 2019

KEPALA
DEPARTEMEN SISTEM INFORMASI

Mahendrawati ER, S.T., M.Sc., Ph.D
NIP 19761011 200604 2 001

LEMBAR PERSETUJUAN

PENYUSUNAN REKOMENDASI UNTUK MENINGKATKAN KESADARAN KEAMANAN INFORMASI MAHASISWA BERDASARKAN NIST SP 800-50 (STUDI KASUS : INSTITUT TEKNOLOGI SEPULUH NOPEMBER)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember

Oleh:

DYAH WIJI ASTUTI
05211540000036

Disetujui Tim Penguji
Tanggal Ujian : 10 Juli 2019
Periode Wisuda : September 2019

Eko Wahyu Tyas. D, S.Kom, M.BA	**(Pembimbing I)**
Hanim Maria Astuti, S.Kom., M.Sc., ITIL.	**(Pembimbing II)**
Sholiq, S.T., M.Kom., M.SA.	**(Penguji I)**
Anisah Herdiyanti, S.Kom, M.Sc	**(Penguji II)**

PENYUSUNAN REKOMENDASI UNTUK MENINGKATKAN KESADARAN KEAMANAN INFORMASI MAHASISWA BERDASARKAN NIST SP 800-50 (STUDI KASUS : INSTITUT TEKNOLOGI SEPULUH NOPEMBER)

Nama Mahasiswa	**:**	**Dyah Wiji Astuti**
NRP	**:**	**05211540000036**
Departemen	**:**	**Sistem Informasi FTIK-ITS**
Pembimbing 1	**:**	**Eko Wahyu Tyas Darmaningrat, S.Kom, M.BA**
Pembimbing 2	**:**	**Hanim Maria Astuti, S.Kom., M.Kom., ITIL**

ABSTRAK

Hasil riset yang dilakukan oleh Communucation and Information System Security Research Center (CISSReC) di sembilan kota besar di Indonesia menyatakan bahwa kesadaran keamanan informasi di masyarakat Indonesia pada tahun 2017 masih tergolong rendah. Survei Pelanggaran Keamanan Informasi yang dilakukan pada tahun 2017 menyatakan bahwa penyebab pelanggaran keamanan informasi adalah dari kelalaian pengguna. Kesenjangan tersebut merupakan titik awal dari penelitian yang bertujuan untuk merancang rekomendasi peningkatan kesadaran keamanan informasi yang berfokus pada ruang lingkup ITS. Dengan gelar sebagai kampus teknologi, ternyata ITS belum memiliki kebijakan yang mengatur tentang kesadaran keamanan informasi, sehingga tidak ada hal yang mendorong mahasiswa untuk sadar akan pentingnya keamanan informasi.

Pengukuran tingkat kesadaran keamanan informasi dibutuhkan untuk mengetahui kondisi dan kebutuhan organisasai. Dalam pengukuran kesadaran keamanan informasi digunakan dimensi kesadaran keamanan informasi dan area keamanan informasi. Dimensi kesadaran keamanan informasi mengacu pada Knowledge-Attitude -Behavior Model seperti penelitian yang

telah dilakukan oleh Kruger dan Kerney tahun 2006. Area keamanan informasi mengacu pada penelitian Arvie Gandhi dan Hazasanzadeh et al, yaitu manajemen password, penggunaan email, penggunaan internet, penggunaan media sosial, keamanan perangkat mobile dan desktop, penanganan informasi, pelaporan insiden, melakukan backup data, social engineering, dan malware.Pengukuran kesadaran keamanan informasi menggunakan metode analisis deskriptif presentase. Dalam penelitian ini digunakan framework NIST SP 800-50 sebagai acuan langkah-langkah menyusun rekomendasi peningkatan kesadaran keamanan informasi.

Berdasarkan hasil pengukuran kesadaran keamanan informasi didapatkan tingkat kesaaran keamanan informasi mahasiswa ITS secara keseluruhan sebesar 72% yang berarti dalam kategori cukup sadar, namun masih berpotensi membutuhkan tindakan. Dari sepuluh area, hanya area penggunaan email yang bernilai baik. Maka dari itu topik yang yang perlu diajukan dalam rekomendasi yaitu sembilan topik, selaian penggunaan email. Pengukuran keamanan informasi juga dimaksud untuk menentukan prioritas topik yang selanjutnya dapat digunakan untuk merancang rekomendasi. Penelitian ini menghasilkan enam rekomendasi kegiatan yang di dalamnya terdapat beberapa sub-kegiatan yang bersinambungan yang bertujuan untuk meningkatkan kesadaran keamanan informasi mahasiswa ITS.

Keyword: Kesadaran Keamanan informasi, , KAB Model. NIST SP 800-50, Rekomendasi Peningkatan Kesadaran Keamanan Informasi

RECOMMENDATIONS FOR IMPROVING INFORMATION SECURITY AWARENESS IN HIGHER EDUCATION BASED ON NIST SP 800-50 (CASE STUDY : SEPULUH NOPEMBER INSTITUTE OF TECHNOLOGY)

Student Name	:	**Dyah Wiji Astuti**
NRP	:	**05211540000036**
Department	:	**Sistem Informasi FTIK-ITS**
Supervisor 1	:	**Eko Wahyu Tyas Darmaningrat, S.Kom, M.BA**
Supervisor 2	:	**Hanim Maria Astuti, S.Kom., M.Kom., ITIL**

ABSTRACT

The results of research conducted by the Center for Research on Security and Information and Education Systems (CISSReC) in nine major cities in Indonesia, stated that information security issues in Indonesian society in 2017 are still relatively low. The Information Security Breaches Survey conducted in 2017 states that the cause of information security breaches comes from users negligence. The gap is the starting point of research that aims to design recommendations for increasing information security awareness that focus on the scope of ITS. With a degree as a technology campus, it turns out that ITS does not yet have a policy that regulates information security awareness, so there is nothing that encourages students to be aware of the importance of information security.

Measurement of the level of information security awareness is needed to determine the conditions and needs of the organization. In measuring information security awareness, information security awareness and information security areas are used. The dimensions of information security awareness refer to the Knowledge-Attitude-Behavior Model as research conducted by Kruger and Kerney in 2006. The information

security area refers to the research of Arvie Gandhi and Hazasanzadeh et al, namely password management, email use, internet use, social medi use, mobile devices security, information handling, incidents reporting, backup data, social engineering, and malware. Information security awareness measurement uses a percentage descriptive analysis method. n this study, the NIST SP 800-50 framework is used as a reference for the steps in compiling recommendations for improving information security awareness. Based on the results of the measurement of information security awareness, the overall level of information security of ITS students is 72%, which means that in the category is have enough awareness, but still has the potential to require action. From the ten of areas, only the email usee area is good value. So from that the topic that needs to be submitted in the recommendations is nine topics, along with the use of email. Measurement of information security is also intended to prioritize topics which can then be used to design recommendations. This study produced six recommendations for activities in which there were several continuous sub-activities aimed at improving ITS student information security awareness.

Keyword: information security awareness, NIST SP 800-50, recommendations for improving information security awareness

KATA PENGANTAR

Bismillahirrohmanirrohim. Puji syukur penulis panjatkan kepada Allah SWT yang telah melimpahkan rahmat, taufik, serta hidayah-Nya sehingga penulis dapat menyelesaikan Tugas Akhir dengan tepat waktu. Penulis tidak pernah berhenti untuk bersyukur dan berterimakasih atas segala Nikmat yang diberikan oleh Allah SWT.

Pada kesempatan kali ini, penulis ingin menyampaikan ucapan terimakasih kepada semua pihak yang telah mendukung, mengarahkan, membimbing, membantu, dan memberikan semangat kepada penulis, antara lain kepada :

1. Allah SWT yang telah melimpahkan rahmat dan karuniaNya kepada penulis , sehingga dapat menyelesaikan buku Tugas Akhir ini dengan tepat waktu.
2. Ibu Suharti dan Bapak Heru Setiyono yang selalu mendukung dan mendoakan penulis. Dan seluruh keluarga besar penulis yang selalu mendukung penulis.
3. Ibu Eko Wahyu Tyas Darmaningrat dan Ibu Hanim Maria Astuti selaku dosen pembimbing penulis yang selalu sabar dan telah meluangkan waktu dan pikiran untuk membimbing penulis untuk menuju hasil yang terbaik dan memuaskan dalam menyelesaikan buku Tugas Akhir ini.
4. Bapak Arif Wibisono dan Bapak Faizal Johan Atlethiko selaku dosen wali penulis yang telah mendukung dan mengarahkan penulis selama masa perkuliahan.
5. Seluruh bapak dan ibu dosen Departemen Sistem Informasi yang telah memberikan ilmu pengetahuan kepada penulis selama masa studi empat tahun ini.
6. Mahasiswa ITS selaku responden kuesioner yang telah meluangkan waktu untuk mengisi kuesioner dan membantu menyelesaikan Tugas Akhir .
7. Seluruh teman-teman yang sudah membantu menyebarkan link kuesioner selama penelitian Tugas Akhir.
8. Fadhila Alfi yang menjadi teman seperjuangan penulis selama perkuliahan, Keja Praktik dan pengerjaan Tugas Akhir.

9. Faiz Anggoro Mukti yang selalu memberikan semangat, masukan, bantuan dan menemani penulis saat mengerjakan Tugas Akhir.
10. Teman-teman "Terjebak Rindu" yaitu Dhila, Dina, Fani, Ervina, Finsa, dan Nasywa yang selalu memberikan semangat, bantuan dan masukan bagi penulis.
11. Teman-teman "Ruang Rindu" yaitu Rizky, Bella, Dewi, Weka, Ardian, Rina, dan Okti yang selalu memberikan semangat dan memberi dukungan untuk penulis.
12. Teman-teman LANNISTER yang menjadi teman seperjuangan mulai dari awal masuk perkuliahan hingga saat ini.
13. Pihak lainnya yang telah membantu dan mendukung penulis demi kelancaran dan kesuksesan penyelesaian buku Tugas Akhir ini.

Tidak ada sesuatu yang sempurna di dunia ini kecuali Allah SWT, tidak terkecuali dengan buku Tugas Akhir ini. Penyusunan Tugas Akhir ini masih banyak memiliki kekurangan dan jauh dari kata sempurna. Oleh karena itu penulis menerima segala kritik dan saran demi kesempurnaan untuk perbaikan di masa mendatang. Semoga Buku Tugas Akhir ini dapat memberikan manfaat bagi pembaca dan menjadi sebuah kontribusi bagi ilmu pengetahuan.

DAFTAR ISI

DAFTAR GAMBAR

*Halaman ini sengaja dikosongka**n***

DAFTAR DIAGRAM

Halaman ini sengaja dikosongkan

DAFTAR TABEL

BAB I PENDAHULUAN

Pada bab ini akan dibahas mengenai pendahuluan tugas akhir yang berisi latar belakang, perumusan masalah, batasan pengerjaan tugas akhir, tujuan dan manfaat dari pengerjaan tugas akhir serta sistematika penulisan buku tugas akhir.

1.1. Latar Belakang

Teknologi informasi dan komunikasi saat ini semakin berkembang pesat dan bukanlah hal yang sulit untuk didapatkan. Menurut data survei tahun 2017 yang dikeluarkan oleh Asosiasi Penyelenggaraan Jaringan Internet Indonesia (APJII), bahwa sebesar 50,08% penduduk Indonesia memiliki *smartphone* atau tablet dan 25,72% memiliki komputer atau laptop [1]. Hasil survei APJII juga menyatakan jika pengguna internet di Indonesia setiap tahunnya mengalami peningkatan, dan untuk tahun 2017 mencapai 143,26 juta dari total penduduk Indonesia pada tahun 2017 sebesar 261 juta jiwa. Dari hasil survey APJII tersebut dapat disimpulkan jika penggunaan teknologi informasi di Indonesia cukup tinggi.

Dalam pemanfaatan teknologi informasi, ada banyak manfaat atau dampak positif yang ditimbulkan, namun hal tersebut juga tidak terlepas dari adanya masalah atau aspek negatif dari adanya teknologi informasi, salah satu masalah yang penting adalah terkait keamanan informasi [2]. c, dimana serangan paling banyak adalah menerima email yang berisi penipuan. Dalam laman berita Kementerian Komunikasi dan Informasi (Kominfo) [4] menyatakan jika kesadaran keamanan informasi di masyarakat Indonesia pada tahun 2017 masih tergolong lemah. Hasil tersebut didukung oleh hasil riset yang dilakukan oleh *Communucation and Information System Security Research Center* (CISSReC) yang dilakukan di sembilan kota besar di Indonesia. Dalam penelitian lain pada tahun 2018 [5] juga menyatakan bahwa tingkat kesadaran keamanan informasi dan privasi pengguna smartphone di Indonesia berada pada kriteria rata-rata, sehingga diperlukan adanya tindakan untuk

meningkatkan kesadaran keamanan informasi bagi pengguna untuk mengurangi pelanggaran maupun kerugian akibat adanya serangan keamanan informasi.

Institut Teknologi Sepuluh Nopember (ITS) merupakan perguruan tinggi unggulan bidang sains dan teknologi di Indonesia yang berlokasi di Surabaya. Tantangan bagi banyak lembaga dan organisasi saat ini tidak hanya pada peningkatan perangkat lunak dan layanan keamanan, tetapi juga meningkatkan kesadaran keamanan informasi pada pengguna teknologi informasi dalam organisasi tersebut. Mahasiswa merupakan target dari penelitian ini, dikarenakan sudah dapat dipastikan jika sebagian besar bahkan seluruh mahasiswa telah memanfaatkan teknologi informasi dalam kehidupan sehari-hari dan dalam mendukung kegiatan belajar. Selain itu didapatkan pula fakta mengenai banyaknya mahasiswa yang belum sadar akan pentingnya keamanan informasi dari informasi yang mereka sebar. Hal tersebut didukung oleh fakta saat saya mengambil mata kuliah Keamanan Aset Informasi, dimana peneliti mendapatkan tugas untuk melakukan percobaan untuk mendapatkan *password*,dan hal tersebut berhasil dilakukan dengan cukup mudah. Dari percobaan tersebut dihasilkan bahwa banyak mahasiswa yang masih menggunakan *password* yang tidak sesuai standard, serta banyak mahasiswa yang tidak mengganti *password* Share ITS (menggunakan *password default*). Fakta lainnya juga didapatkan saat mengambil mata kuliah Manajemen Risiko TI, dimana saat itu mendapatkan tugas untuk melakukan *social engineering*, dan rata-rata mahasiswa masih sangat mudah untuk membagikan informasi yang sensitif. Selain itu, dengan gelar sebagai kampus teknologi didapatkan fakta bahwa ITS belum memiliki kebijakan yang mengatur mengenai keamanan informasi, sehingga tidak ada hal yang mendorong mahasiswa untuk sadar akan pentingnya keamanan informasi.

Berangkat dari masalah yang telah dijelaskan sebelumnya, tujuan dari penelitian ini adalah untuk mengetahui kondisi kesadaran keamanan informasi mahasiswa ITS dan kemudian

menyusun rekomendasi yang bertujuan untuk meningkatkan kesadaran keamanan informasi mahasiswa ITS. Dalam penyusunan rekomendai berpedoman pada framework NIST SP 800-50 dan melakukan analisis pengukuran kesadaran keamanan informasi berdasarkan dimensi kesadaran keamanan informasi dan area keamanan informasi.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka rumusan masalah yang menjadi fokus dan akan diselesaikan dalam tugas akhir ini sebagai berikut :

1. Seberapa besar tingkat kesadaran keamanan informasi mahasiswa ITS berdasarkan area dan dimensi kesadaran keamanan informasi dari skala 0-100 % ?
2. Apa saja topik keamanan informasi yang harus ditindak lanjuti agar mahasiswa lebih sadar mengenai keamanan informasi ?
3. Apa saja usulan kegiatan yang dapat dilakukan agar dapat mendorong kesadaran mahasiswa akan pentingnya keamanan informasi ?

1.3 Batasan Masalah

Batasan permasalahan yang menjadi ruang lingkup pengerjaan tugas akhir ini adalah :

1. Objek dari penelitian ini adalah mahasiswa S1 Institut Teknologi Sepuluh Nopember angkatan 2015 - 2018.
2. Penyusunan rekomendasi kesadaran keamanan informasi dirancang berdasarkan hasil pengukuran kesadaran keamanan informasi berdasarkan area keamanan informasi dan dimensi kesadaran keamanan informasi.

1.4 Tujuan Tugas Akhir

Dari perumusan masalah yang disebutkan sebelumnya, tujuan yang akan dicapai melalui tugas akhir ini adalah :

1. Membuat awareness map untuk memetakan tingkat

kesadaran keamanan informasi mahasiswa ITS.

2. Mengetahui apa saja topik keamanan informasi yang harus ditindak lanjuti agar mahasiswa semakin sadar akan pentingnya keamanan informasi.
3. Menyusun rekomendasi yang bertujuan untuk meningkatkan kesadaran keamanan informasi bagi mahasiswa ITS.

1.5 Manfaat Tugas Akhir

Melalui tugas akhir ini diharapkan dapat memberikan manfaat yaitu :

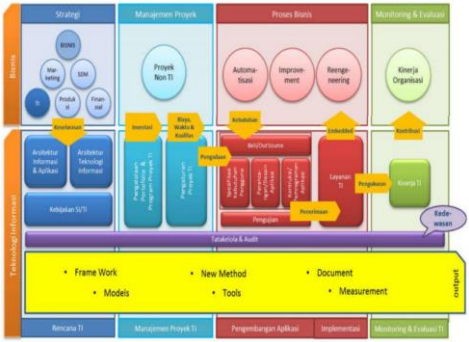
1. Membantu mengetahui tingkat kesadaran keamanan informasi pada mahasiswa ITS untuk berbagai topik dari keamanan informasi.
2. Menjadi alternatif sebagai langkah untuk meningkatkan kesadaran keamanan informasi pada mahasiswa ITS.

1.6 Relevansi Tugas Akhir

Tugas Akhir ini relevan untuk menjadi tugas akhir S1 dengan alasan berikut:

1. Perancangan rekomendasi kesadaran keamanan informasi merupakan bagian dari perencanaan dalam bidang teknologi informasi dan hal tersebut dibutuhkan oleh Manajer Sistem Informasi untuk meningkatkan pengetahuan, sikap, dan perilaku terkait keamanan informasi agar pengguna dalam organisasi dapat terhindar dari risiko yang diakibatkan dari ancaman terhadap keamanan informasi. Hasil penelitian ini nantinya dapat dijadikan rekomendasi sebagai langkah dalam meningkatkan kesadaran keamanan informasi pengguna teknologi informasi.
2. Tugas akhir ini berkaitan dengan mata kuliah Manajemen Risiko dan Evaluasi dan Audit Teknologi Informasi yang merupakan bagian dari bidang keilmuan yang ada pada Lab Manajemen Sistem Informasi (MSI). Sehingga dapat

dikatakan bahwa penelitian ini telah mempunyai relevansi sesuai dengan roadmap laboratorium MSI pada Jurusan Sistem Informasi.



Gambar 0.1 Roadmap Laboratorium Manajemen Sistem Informasi SI ITS

1.7 Sistematika Penulisan

Sistematika penulisan proposal tugas akhir ini dibagi menjadi tiga bab, di antaranya adalah sebagai berikut

BAB I PENDAHULUAN

Bab I merupakan bagian pendahuluan dari tugas akhir ini yang berisi latar belakang, rumusan masalah, batasan masalah, tujuan tugas akhir, manfaat tugas akhir, sistematika penulisan, serta relevansi tugas akhir.

BAB II TINJAUAN PUSTAKA

Bab II merupakan bagian yang berisi tinjauan pustaka, yaitu mengenai uraian dari istilah-istilah yang digunakan pada penulisan tugas akhir ini serta dasar teori yang digunakan pada tugas akhir ini.

BAB III METODOLOGI

Bab III merupakan bagian yang berisi penjelasan dari metode yang akan digunakan dalam penyelesaian tugas akhir. Metode dalam tugas akhir bertujuan sebagai pedoman dalam pengerjaan tugas akhir, sehingga proses pengerjaan lebih terarah dan sistematis. Tahapan dan proses dari metode ini dirangkum dalam sebuah diagram alur yang dapat memudahkan untuk memahami metode keseluruhan.

BAB II TINJAUAN PUSTAKA

Pada bab ini akan dibahan mengenai tinjauan pustaka dari tugas akhir. Bab ini berisi dasar teori yang mendukung tugas akhir. Adapun hal yang ada di dalam Tinjauan Pustaka adalah sebagai berikut.

2.1. Studi Sebelumnya

Dalam penelitian ini, digunakan beberapa penelitian terdahulu sebagai pedoman dan referensi dalam melaksanakan proses-proses dalam pengerjaan tugas akhir, informasi yang disampaikan dalam Tabel 2.1 sampai Tabel 2.5 berisi informasi penelitian sebelumnya, hasil penelitian dan hubungan terhadap tugas akhir.

Tabel 0.1 Penelitianl Sebelumnya Paper 1

Judul Penelitian	*A Framework for an Effective Information Security Awareness Program in Healthcare, A Case Study of Computer Game in Hospital Universiti Kebangsaan Malaysia* [6]
Penulis; Tahun	Arash Ghazvini, Zarina Shukur; 2017.
Deskripsi Umum Penelitian	Jurnal ini membahas tentang pengembangan program keamanan informasi pada Hospital University Kebangsaan Malaysia (HUKM). Untuk mendapatkan program yang efektif, telah dilakukan tiga penelitian sebelumnya yaitu : a. Pada tahun 2015 dilakukan penelitian terkait perancangan framework yang akan digunakan dalam merancang program kesadaran keamanan informasi [7]. Pemilihan topik keamanan informasi dilakukan dengan cara memilih topik keamanan informasi dari literatur yang ada kemudian

	melakukan wawancara dengan manager. *b.* Pada tahun 2016 dilakukan penelitian mengenai pemilihan metode penyampaian (transfer) program kesadaran keamanan berdasarkan Model yang diperkenalkan oleh Halton yaitu berfokus pada *Transfer Design* dengan melakukan penilaian berdasarkan *Training Success Factor* [8]. *c.* Pada tahun 2017 dilakukan penelitian terkait pengembangan konten program yang didasarkan pada beberapa faktor diantaranya kebijakan keamanan informasi internal organisasi, standard keamanan informasi, kesalahan keamanan informasi yang dilakukan karyawan, metode penyampaian yang dipilih, dan profil dari target program [9].
Keterkaitan Penelitian	Keterkaitan antara paper dengan penelitian saya adalah hasil yang diharapkan berupa program peningkatan kesadaran keamanan informasi. Untuk persamaannya adalah dalam merancang konten kesadaran keamanan informasi menggunakan standard keamanan informasi. Terdapat perbedaan dengan penelitian yang saya lakukan yaitu saya menggunakan *framework* NIST SP 800-50 sebagai pedoman dalam merancang program

	kesadaran keamanan informasi. Sebelum melakukan perancangan program, terlebih dahulu saya melakukan analisis tingkat kesadaran keamanan informasi berdasarkan tiga dimensi dan 9 area keamanan informasi. Dari hasil tersebut dapat diketahui apa saja topik keamanan informasi yang membutuhkan tindakan agar target lebih sadar akan pentingknya keamanan informasi.

Tabel 0.2 Penelitian Sebelumnya Paper 2

Judul Penelitian	Desain Program Kepedulian Keamanan Informasi Pada Perusahaan "X" [10]
Penulis; Tahun	Shafwan; 2008
Deskripsi Umum Penelitian	Penelitian ini membahas mengenai perancangan program yang bertujuan untuk meningkatkan kepedulian karyawan terhadaap keamanan informasi. Namun dalam penelitian ini tidak terlalu dijelaskan mengenai pedoman penyusunan program kesadaran keamanan informasi secara jelas. Hanya dalam memilih media penyampaian program bersumber pada ISACA 2005.
Keterkaitan Penelitian	Output yang dihasilkan sama yaitu program untuk meningkatkan kesadaran keamanan informasi. Namun terdapat perbedaan dari penelitian yang saya lakukan yaitu terkait identifikasi kebutuhan program dan *framework* penyusunan program.

Tabel 0.3 Penelitian Sebelumnya Paper 3

Judul Penelitian	*Analyzing The Role of Cognitive and Cultural Biases in Internalization of Information Security Policies: Recomendations for Information Security Awareness Programs* [11]
Penulis; Tahun	Anggeliki Tsohou, Maria Karyda, Spyros Kokolakis, 2015.
Deskripsi Umum Penelitian	Jurnal ini membahas mengenai rekomendasi dalam merancang dan membangun program kesadaran keamanan informasi berdasarkan analisis terhadap bias kognitif dan bias budaya dalam organisasi yang mempengaruhi niat pengguna untuk mematuhi kebijakan keamanan informasi. Dari hasil analisis tersebut kemudian peneliti memberikan usulan seperangkat pedoman untuk meningkatkan desain dan implementasi program kesadaran keamanan informasi. Standard yang digunakan dalam merancang usulan pedoman program kesadaran keamanan informasi adalah NIST SP 800-50 dan ENISA:2010 dengan berfokus pada program dalam meningkatkan kesadaran keamanan informasi.
Keterkaitan Penelitian	Keterkaitan antara paper dengan penelitian saya adalah hasil yang diharapkan berupa rekomendasi dalam perancangan program peningkatan kesadaran keamanan informasi. Namun, juga terdapat perbedaan dengan penelitian yang saya lakukan yaitu dalam melakukan analisis kebutuhan program, saya melakukan pengukuran kesadaran keamanan informasi melalui penyebaran kuesioner berdasarkan tiga dimensi dan sepuluh area keamanan informasi dikarenakan ITS belum

	memiliki kebijakan terkait keamanan informasi. Untuk merancang program saya beracuan pada *framework* NIST SP 800-50.

Tabel 0.4 Penelitian Sebelumnya Paper 4

Judul Penelitian	*Quantitative Assesment of Information Security Awareness on Informatics Students in a University* [12].
Penulis; Tahun	Arfive Gandhi. 2017
Deskripsi Umum Penelitian	Penelitian ini membahas mengenai pengukuran kesadaran keamanan informasi mahasiswa di sebuah universitas. Dalam penelitian ini berfokus pada tujuh bidang (fokus area) keamanan informasi yaitu adalah manajemen kata sandi, penggunaan email, penggunaan internet, penggunaan media sosial, perangkat seluler, penanganan informasi, dan pelaporan insiden. Penelitian ini juga didasarkan pada model Knowledge-Attitude-Behavior (KAB).
Keterkaitan Penelitian	Dalam penelitian yang saya lakukan, saya akan mrnggunakan KAB model dan fokus area keamanan informasi yang ada guna mendesain kuesioner yang digunakan untuk mengetahui kondisi organisasi. Fokus area yang saya gunakan juga beracuan pada penelitian tersebut dengan ditambahkan dua fokus area lain yang didapatkan dari penelitian lain yaitu *social engineering* dan *malware*.

11

Tabel 0.5 Penelitian Sebelumnya Paper 5

Judul Penelitian	*A Conceptual Framework for Information Security Awareness, Assessment, and Training* [13].
Penulis; Tahun	Mohammad Hazzanzadeg, Narges Jahangiri, and Ben Brewster, 2014.
Deskripsi Umum Penelitian	Penelitian ini membahas mengenai pengukuran kesadaran keamanan informasi dan prioritasi area yang perlu dilakukan tindakan yaitu berupa program kesadaran keamanan informasi. Dalam melakukan pengukuran kesadaran dilakukan dengan menggunakan model Knowledge-Attitude-Behavior (KAB) dan berdasarkan sembilan area keamanan informasi yaitu *email / spam, backup, password, social engineering, mobile security, malware, internet, reporting*, dan kepatuhan terhadap kebijakan. Berdasarkan analisa pengukuran kesadaran tersebut dapat diketahui mana saja area dan dimensi yang perlu dilakukan tindakan yaitu berupa adanya program peningkatan kesadaran keamanan informasi, serta berdasarkan prioritasi faktor dapat diketahui mana yang harus ditindaklanjuti terlebih dahulu.
Keterkaitan Penelitian	Dalam penelitian yang saya lakukan, saya menggunakan penelitian tersebut sebagai dasar dalam pengukuran kesadaran yang nantinya dapat digunakan sebagai topik dalam program kesadaran keamanan informasi, serta prioritasi faktor yang akan saya gunakan sebagai penentuan topik yang harus dirancang terlebih dahulu. Area keamanan informasi dalam penellitian ini juga akan saya gunakan sebagai acuan,

	kecuali kepatuhan terhadap kebijakan dikarenakan ITS belum memiliki kebijakan yang mengatur mengenai keamanan informasi.

2.2. Dasar Teori

Bagian ini akan membahas teori dan bahan penelitian lain yang menjadi dasar informasi untuk mengerjakan tugas akhir ini.

2.2.1. Keamanan Informasi

The Committee on National Security Systems (CNSS) mendefinisikan keamanan informasi sebagai perlindungan terhadap informasi dan elemen kritisnya termasuk sistem dan perangkat keras yang digunakan, penyimpanan, dan proses pengiriman informasi [14]. Keamanan informasi juga dapat diartikan sebagai upaya untuk melindungi informasi dan sistem informasi dari akses oleh pihak yang tidak berwewenang, dalam hal penggunaan, penyikapan, gangguan, modifikasi, maupun perusakan yang tidak sah untuk menjaga aspek keamanan informasi, seperti integritas, kerahasiaan, dan ketersediaan informasi [15].

2.2.2 Kesadaran Keamanan Informasi

Pengertian kesadaran keamanan informasi dijelaskan dalam Information Security Forum (ISF) [16], yaitu "Kesadaran terhadap keamanan teknologi informasi adalah tingkat atau jangkauan pemahaman dari setiap anggota dalam organisasi mengenai pentingnya keamanan teknologi informasi, level keamanan teknologi informasi yang sesuai dengan organisasi, dan tanggung jawab terhadap keamanan informasi secara individu". Shaw at al mengartikan kesadaran keamanan informasi sebagai tingkat pemahaman pengguna tentang pentingnya keamanan informasi dan memahami tanggung jawab mereka, serta mengetahui tindakan untuk mengkontrol keamanan informasi yang cukup untuk melindungi data dan jaringan dalam organisasi [17]. Tujuan dari meningkatkan

13

kesadaran akan keamanan informasi adalah membuat perubahan positif pada perilaku orang-orang yang terlibat dalam sebuah organisasi, sehingga pengetahuan mengenai keamanan informasi dalam hal ini merupakan hal penting guna menyadarkan orang-orang, baik secara individual maupun dalam organisasi akan risiko yang mereka hadapi dan merangsang mereka untuk mencegah risiko tersebut agar tidak terjadi [18].

2.2.3 Tingkat Kesadaran Keamanan Informasi

Tingkat kesadaran keamanan informasi akan dibagi menjadi 3 tingkatan yaitu: buruk, sedang dan baik. Penentuan skala ditunjukkan pada Tabel 2.2 yang dicetuskan oleh Hassanzadeh et al [13] dan Kruger et al [19] dalam mengukur kesadaran keamanan informasi, kemudian pada masing-masing tingkatan ditambaahkan tindakan yang harus diambil ketika tingkat kesadaran berada di tingkatan tertentu.

Tabel 0.6 Tingkat Kesadaran Keamanan Informasi

Tingkatan	Nilai (%)	Tindakan
Baik	80 – 100	Tidak dibutuhkan tindakan
Sedang	60 - 79	Berpotensi tindakan diperlukan
Buruk	0 - 59	Tindakan diperlukan

2.2.4 *Knowledge-Attitude-Behavior Model* (KAB Model)

Kruger dan Kearney (2006) mengembangkan model prototipe untuk mengukur kesadaran keamanan informasi di perusahaan pertambangan emas internasional berdasarkan *knowlodge* (pengetahuan), *attitude* (sikap), dan *Behavior* (perilaku). [19].

Model Knowledge-Attitude-Behavior (KAB) menjelaskan bahwa perilaku berubah secara bertahap. Ketika pengetahuan terakumulasi, kemudian perubahan sikap dimulai, selanjutnya

perubahan sikap menumpuk dan menghasilkan perubahan perilaku [20].

a. Knowledge (Pengetahuan)
   Berdasarkan *Oxford Dictionary* [21] , *knowledge (pengetahuan) adalah* sebuah fakta, informasi, dan keterampilan yang diperoleh melalui pengalaman atau pendidikan, pemahaman teoritis atau praktis dari suatu subjek. Dalam hal ini pengetahuan didasarkan pada pengetahuan pengguna tentang bagaimana menyikapi atau berperilaku dalam kondisi tertentu.

b. Attitude (Sikap)

   Berdasarkan *Oxford Dictionary* [21], attitude (sikap) adalah cara seseorang dalam berfikir atau berpendapat atau merasakan sesuatu hal. Dalam hal ini sikap mengacu pada sikap pengguna (bagaimana perasaan atau keyakinan pengguna) terhadap kemungkinan konsekuiensi dari perilaku yang mereka lakukan.

c. Behavior (Perilaku)

   Berdasarkan *Oxford Dictionary* [21], Behavior (perilaku) adalah cara seseorang bertindak atau memperlakukan atau memberi respon objek lain dalam situasi tertentu. Dalam dimensi perilaku dalam keamanan sistem informasi, ketika sesorang dapat mengembangkan perilaku dan kebiasaan yang baik, maka budaya keamanan informasi yang kuat akan terbentuk. Dalam hal ini perilaku didasarkan pada apa yang dilakukan pengguna terkait perilaku aktual mereka.

KAB Model ini tidak sepenuhnya baru dan peneliti lain telah melakukan penelitian di mana ilmu-ilmu sosial yang terkait dengan bidang kesadaran keamanan informasi.Tahun 2017 dilakukan pengukuran kesadaran keamanan informasi pada Kementerian Riset, Teknologi dan Pendidikan Tinggi di Indonesia berdasarkan KAB model dan fokus area keamanan informasi. Dalam institusi pendidikan juga terdapat penelitian yang menerapkan pengukuran kesadaran keamanan informasi

15

berdasarkan dimensi dari KAB Model serta fokus area keamanan informasi.

2.2.5 Knowledge, Attitude and Behavioral Change Strategy

Dalam dimensi kesadaran keamanan informasi dikenal istilah KAB model. Ada beberapa strategi yang dapat digunakan untuk meningkatkan masing-masing dimensi kesadaran keamanan informasi. Berikut penjelasan strategi untuk tiap dimensi kesadaran keamanan informasi :

a. Knowledge Sharing Strategy

Pengetahuan merupakan aset berharga ketika dibagikan dengan benar yang dapat digunakan untuk membantu pengambilan keputusan, meningkatkan efisiensi, mengurangi biaya pelatihan dan mengurangi risiko akibat adanya ancaman keamanan informasi [22]. Biasanya kampanye pendidikan menargetkan aspek pengetahuan manusia dan mengabaikan motif di balik perilaku manusia. Pengetahuan bukanlah motif untuk perilaku keamanan informasi manusia, namun kurangnya pengetahuan merupakan hambatan dalam mengembangkan perilaku yang diinginkan [23]. Dalam konteks keamanan informasi dalam organisasi,berbagi pengetahuan dapat dimanifestasikan melalui adanya kegiatan dengan menghadirkan spesialis guna meningkatkan pengetahuan, menyimpan dan memperbaharui pengetahuan ke dalam komputer dengan menggunakan situs intranet atau berbasis website agar dapat diakses oleh penggunanya, mengadakan lokakarya dan seminar atau pelatihan untuk mentransfer pengetahuan [24].

Berbagi pengetahuan adalah proses yang mengharuskan membimbing audiens dengan cara berpikir tertentu. Untuk melakukannya diperlukan beberapa strategi untuk mendukung keberhasilan proses berbagi pengetahuan. Tsui et al dalam *Knowledge Handbook Sharing* telah memberikan beberapa strategi dalam berbagi pengetahuan diantaranya sebagai berikut [25] :

1. Mempertimbangkan Kebutuhan Audiens
2. Merancang berbagai pengetahuan yang efektif membutuhkan pemahaman audiens, bukan hanya fokus pada konten yang akan disampaikan. Maka dari itu sangat penting mempertimbangkan konten yang memang sedang dibutuhkan oleh audiens. Sehingga sebelum merancang konten harus dilakukan penilaian kebutuhan.
3. Gunakan Bahasa Sesuai Audiens
4. Jika topik dalam materi merupakan topik yang belum banyak dimengerti oleh audiens, maka bahasa yang digunakan harus disesuaikan dengan audiens agar mudah dipahami. Jika ada istilah teknis harus terlebih dahulu dijelaskan.
5. Teknik bercerita dapat menjadi salah satu cara untuk menyajikan penelitian dan bentuk-bentuk pengetahuan lainnya dengan cara yang menarik bagi khalayak yang beragam. Naratif memungkinkan untuk berbagi pengalaman daripada informasi dan dapat membantu audiens dalam mempelajari konsep-konsep utama.
6. Menyoroti berbagai komponen dalam pengetahuan (*body of knowledge*) yang dibagikan untuk berfikir secara kolaboratif bukan hanya menyajikan informasi.
7. Mendorong audiens untuk terhubung satu sama lain untuk berbagi pengetahuan.
8. Meningatkan kemungkinan bahwa pengetahuan dapat diakses berulang kali dan dalam berbagai cara.

Selain itu penyampaian informasi yang efektif jika materi menarik, terkini dan cukup sederhana untuk diikuti. Setiap presentasi yang terasa terlalu umum akan dianggap oleh target hanya sebagai sesi wajib saja [17].

17

b. Attitude and Behavioral Change Strategy

Tujuan akhir dari program kesadaran keamanan yang efektif adalah membuat pengguna siap untuk bertindak untuk mencegah adanya ancaman keamanan informasi. Memiliki pengetahuan akan keamanan informasi tidak cukup dapat mengubah perilaku sadar akan keamanan informasi. Maka dari itu sangat penting untuk menanamkan perilaku keamanan informasi yang positif sehingga dapat mengakibatkan pemikiran menjadi kebiasaan dan bagian dari budaya keamanan organisasi [26].

Menurut Dolan et al [27] pada dasarnya ada dua cara berpikir tentang mengubah perilaku, yaitu :

1. Model Rasional (Kognitif) yang didasarkan pada pengaruh dari pemikiran. Model ini mrnunjukkan bahwa orang akan menganalisis berbagai informasi dan berbagai sumber, serta insentif yang ditawarkan dan mereka akan berfikir untuk bertindak sesuai dengan kepentingan terbaik mereka.
2. Model Konteks untuk membentuk perilau yang berfokus pada penilaian dan pengaruh yang otomatis. Model ini berfokus pada mengubah perilaku tanpa mengubah pikiran sehingga terkadang tampak tidak rasional dan tidak konsisten. Model ini kurang mendapat perhatian dari peneliti dan pembuat kebijakan.

Dalam mengubah sikap dan perilaku seseorang dikenal salah satu teknik yaitu dengan teknik persuasi (*persuasion technique*) yaitu upaya untuk mengubah sikap atau perilaku atau keduanya tanpa menggunakan pakasaan atau penipuan [26]. Terdapat beberapa teknik persuasi diantaranya [28]:

a. Basic Persuasion Techniques, meliputi :

1. Fear : memberikan rasa takut atas efek yang ditimbulkan dari perilaku yang salah.

2. Association : memberikan gambaran efek positif yang ditimbulkan dari adanya perubahan perilaku.

3. Penyampaian pesan oleh seseorang yang menarik atau

yang berpengaruh di lingkungan sosial.

4. Menghadirkan *expert*.
5. *Testimonials* : memberikan testimoni dari beberapa orang untuk meyakinkan target.
6. *Humour* : dikemas secara menarik, salah satunya dengan memberikan pesan yang dikemas dengan lelucon.
7. *Repetition* : Pengulangan kata atau gambar untuk memperkuat poin utama agar pesan tertanam dalam pikiran.

b. *Intermediate Persuasion Techniqu*es, meliputi :

1. *Rhetorical Question* : Merancang pertanyaan yang membuat target setuju dengan pembicara sehingga dapat meyakinkan target.
2. *Scintific Evidence* : memberikan bukti berupa fakta atau data yang ada.
3. *Symbols* : memberikan simbol berupa kata-kata atau gambar yang mengingatkan pada konsep yang lebih besar.

c. *Advance Persuasuion Techniques*, meliputi :

1. *Analogy :* memberikan analogi yang mirip untuk menggambarkan pesan yang disampaikan.
2. *Group Dynamic* : orang mudah terpengaruh oleh apa yang dipikirkan dan dilakukan oleh grup mayoritas.
3. *Majority Belief* :Memberikan hasil survei untuk mendukung argumen.
4. *Timing :* mencari waktu yang tepat.

Teknik lain yang dapat digunakan untuk mempengaruhi seseorang untu mengikuti perilau yang diinginkan adalah dengan teknik *Rewards and Punishments* [26]. *Rewards* (memberikan penghargaan) dapat diberikan untuk menghargai orang karena telah berperilaku dengan baik dan memberikan motivasi orang lain untuk melakukan hal tersebut. *Punishment*

19

(Hukuman) dapat diberikan untuk memberikan rasa takut akan perilaku yang buruk (dapat merugikan orang lain).

2.2.6 Program / Kegiatan Peningkatan Kesadaran Keamanan Informasi

Program atau dalam penelitian ini disebut sebagai usulan rekomendasi kesadaran keamanan informasi adalah sebuah kegiatan yang dirancang dengan tujuan melatih pengguna atau pihak yang bertanggung jawab terhadap informasi yang ada dalam organisasi sehingga dapat menghindari situasi yang membahayakan data dalam organisasi [17]. Tujuan utama dari program kesadaran keamanan informasi adalah untuk mendidik pengguna tentang tanggung jawab mereka dalam melindungi kerahasiaan, ketersediaan, dan integritas dari aset informasi dalam organisasi maupun secara individu, sehingga keamanan informasi dalam sebuah organisasi adalah tanggung jawab semua orang, bukan hanya departemen Teknologi Informasi [29]. Program atau kegiatan kesadaran keamanan informasi merupakan hal penting agar dapat memastikan seluruh pengguna menyadari akan pentingnya melindungi informasi sensitif, mengetahui tindakan yang harus dilakukan untuk menangani informasi dengan aman, dan meminimalisir risiko kesalahan penanganan informasi [30].

Wilson et al dalam NIST *Special Publication* 800-50 mengklaim jika usulan reomendasi yang paling efektif adalah kegiatan yang dirancang sesuai dengan misi atau tujuan dari organisasi ataupun secara individual, serta materi yang diberikan relevan dengan masalah yang ada pada peserta yang bersangkutan [16]. Kata "Efektif" yang telah disebutkan sebelumnya juga berarti berupa kegiatan yang mampu mempengaruhi tiga dimensi dalam kesadaran keamanan informasi [19], yaitu *knowledge* (pengetahuan) , *attitude* (sikap), dan *behavior* (perilaku) para peserta, serta membuat perubahan positif dalam kebiasaan menggunakan informasi terkait masalah keamanan informasi, sehingga perlu dipastikan bahwa kegiatan yang dirancang harus mencangkup topik yang sesuai, penting juga untuk memilih metode yang sesuai karena

keberhasilan dari suatu kegiatan peningkatan kesadaran keamanan informasi sangat bergantung dengan bagaimana metode atau cara membawakan sebuah program [31].

Berikut beberapa contoh program atau kegiatan yang bertujuan untuk meningkatkan kesadaran keamanan informasi yang telah berhasil dilaksanakan :

1. *European Cyber Security Month 2017*
   Kegiatan kampanye ini diselenggarakan melalui workshop pada April 2017 di Brussels dan menggundang koordinator Negara Anggota untuk berpartisipasi. Workshop tersebut dilaksanakan selama empat minggu dengan tema yang berbeda untuk setiap minggunya. Hasil evaluasi dari kegiatan tersebut menyatakan bahwa pelaksanaan kampanye tersebut di atas rata-rata, dimana hasil tersebut secara signifikan lebih baik dari pada tahun sebelumnya. Sebesar 60% koordinator setuju bahwa kegiatan tersebut memberikan nilai tambah dalam pekerjaan mereka. Selain itu sebesar 66% peserta meyakini atau merespon positif jika kegiatan seperti workshop perlu diselenggarakan kembali untuk tahun berikutnya [32].
2. *Make IT Secure Campaign*
   Departemen Komunikasi, Sumber Daya Kelautan dan Alam bersama-sama dengan BT, Dell, Eircom, Federasi Bankir Irlandia, IAB, Microsoft, Symantec, Pusat Nasional Teknologi dalam Pendidikan, Solusi Lingkungan dan Vodafone bekerja bersama untuk meningkatkan kesadaran akan kebutuhan mendesak bagi konsumen dan bisnis untuk membuat komputer mereka aman. Kampanye yang dilaksanakan pada periode 2005/2006 membahas masalah yang muncul, seperti 'Phishing; pencurian identitas; spyware dan keamanan anak online. Dengan adanya kampanye tersebut dihasilkan bahwa kesadaran pengguna meningkat menjadi 44% (dari sebelumnya adalah 33% pada tahun 2004). Pemahaman tentang istilah-istilah seperti 'pencurian identitas' dan 'spyware' meningkat secara drastis

21

dalam penelitian kampanye pasca-2005 dengan skor 55% (dari 24% sebelum kampanye) [33].

3. *Raising Information Security Awareness in Digital Ecosystem with Games – a Pilot Study in Thailand*
   Kegiatan ini dilakukan sebagi penelitian dan usaha untuk meningkatkan pengetahuan siswa pilot di Thailan mengenai keamanan informasi. Kegiatan yang dirancang dan dilaksanakan terdiri dari dua kegiatan pelatihan dan percobaan *mobile games* tentang keamanan informasi. Dari kegiatan tersebut 75% siswa menyatakan pelatihan dapat meningkatkan pengetahuan tentang keamanan informasi, sedangkan 100% siswa setuju bahwa adanya games tersebut dapat meningkatkan pengetahuan mereka terkait keamanan informasi[34].

Selain contoh di atas masih banyak terdapat contoh kegiatan untuk meningkatkan kesadaran keamanan informasi

2.2.7 NIST SP 800-50

National Institute of Standard and Technology Special Publication 800-50 atau biasa disingkat dengan NIST SP 800-50 merupakan sebuah pedoman untuk level strategis yang digunakan dalam merancang, membangun, dan melakukan suatu pembinaan mengenai kesadaran keamanan informasi [16]. Dalam dokumen NIST SP 800-16 dijelaskan terdapat tiga komponen utama dalam pembinaan kesadaran keamanan informasi yaitu dimulai dari adanya suatu kesadaran, yang dilanjutkan dengan pelatihan, dan berkembang menjadi sebuah pendidikan [17].

NIST SP 800-50 telah mendefinisikan empat langkah penting dalam siklus pembinaan kesadaran keamanan informasi, sebagai berikut :

a. Perancangan Kegiatan Kesadaran Keamanan Informasi.

   Pada langkah ini, organisasi harus melakukan penilaian kebutuhan dan strategi program dan pelatihan yang sesuai dengan kondisi organisasi dan dapat diaplikasikan pada

organisasi. Output dari langkah ini adalah *Awareness Training and Program Plan*. Dalam penelitian ini saya modifikasi menyesuaikan dengan penelitian yang saya lakukan menjadi *Information Security Awareness Plan.*

b. Pengembangan Kegiatan Kesadaran Keamanan Informasi.

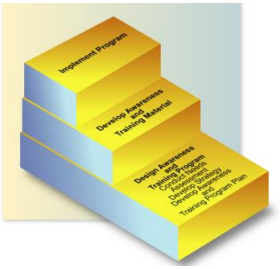
Pada langkah ini berfokus pada sumber – sumber kegiatan yang tersedia seperti pengembangan materi serta permohonan kerja sama kepada pihak ketiga jika diperlukan.

c. Pelaksanaan Kegiatan Kesadaran Keamanan Informasi.

Pada langkah ini organisasi harus mengetahui bagaimana komunikasi yang efektif dan metode yang tepat untuk melaksanakan kegiatan peningkatan kesadaran keamanan informasi. Output dari langkah (b) dan (c) merupakan sebuah kegiatan yang sudah dirancang secara detail yang disebut dengan *Information Security Awareness Materials.*

d. Pasca Pelaksanaan Kegiatan Kesadaran Keamanan Informasi.

Langkah ini memberikan petunjuk agar jalannya program serta proses monitoring dan evaluasi berjalan secara efektif.



Gambar 0.1 Step Penyusunan Program

NIST SP 800-50 telah memberikan 27 topik kesadaran keamanan informasi, sebagai berikut :

a. Penggunaan dan manajemen kata sandi – termasuk pembuatan, frekuensi perubahan, dan perlindungan.
b. Perlindungan dari *virus*, *worm*, *trojan horses*, dan pemindaian kode berbahaya lainnya.
c. Kebijakan – implikasi ketidakpatuhan.
d. Email / lampiran (*attachments*) yang tidak dikenal.
e. Penggunaan website – pemantauan aktivitas pengguna.
f. Spam
g. *Backup* dan penyimpanan data – pendekatan terpusat atau desentralisasi.
h. *Social engineering*.
i. Respon terhadap insiden.
j. *Shoulder Surfing*.
k. Perubahan dalam lingkungan sistem- peningkatan risiko pada data dan sistem (seperti air, api, debu atau kotoran, dan akses fisik).
l. *Inventory and property transfer* – identifikasi organisasi yang bertanggung jawab dan tanggung jawab dari pengguna.
m. Personal use and gain issues
n. Masalah keamanan perangkat genggam.
o. Penggunaan enkripsi dan transmisi informasi sensitif / rahasia melalui internet,
p. Keamanan laptop saat dalam perjalanan – menangani masalah keamanan fisik dan informasi.
q. Sistem dan perangkat lunak milik pribadi di tempat kerja - diizinkan atau tidak (misal hak cipta).

r. Penerapan *patch* sistem tepat waktu – bagian dari manajemen konfigurasi.

s. Masalah pembatasan lisensi perangkat lunak – alamat saat salinan diizinkan dan tidak diizinkan.

t. Perangkat lunak yang didukung / diizinkan pada sistem organisasi – bagian dari manajemen konfigurasi.

u. Masalah kontrol akses – membahas hak istimewa dan pemisahan tugas.

v. Akuntabilitas individu- menjelaskan apa artinya dalam organisasi.

w. Penggunaan pernyataan secara resmi – kata sandi, akses sistem dan data, penggunaan dan perolehan secara pribadi.

x. Kontrol pengunjung dan akses fisik – diskusikan kebijakan dan prosedur keamanan fisik yang berlaku

y. Keamanan desktop – mendiskusikan penggunaan screensaver, membatasi pandangan pengunjung tentang informasi pada layar (mencegah /membatasi shoulder surfing), perangkat *backup* baterai, dan memungkinkan akses pada sistem.

z. Melindungi informasi yang dirahasiakan.

aa. Tata cara file terlampir dan aturan lainnya.

Gambar 0.2 Contoh rekomendasi meningkatkan kesadaran keamanan informasi berdasarkan NIST SP 800-50

25

2.2.8 Media Komunikasi Penyampaian Program

Penyampaian informasi yang efektif kepada target membutuhkan suatu media penyampaian yang sesuai dengan target agar informasi yang diberikan dapat diterima dengan baik. Pemmberi informasi tidak dapat hanya bergantung pada metode ceramah atau menggunakan slide power point. Pemberi informasi seharusnya berinovasi agar target dapat menerima informasi dengan baik [34]. Ada banyak media yang dapat digunakan sebagai alat untuk menyampaikan kegiatan dalam meningkatkan kesadaran keamanan informasi. Berikut beberapa penjelasan terkait media penyampaian berdasarkan penelitian yang dilakukan oleh [23].

a. Presentasi
   Kampanye dalam bentuk presentasi biasanya menargetkan untuk aspek pengetahuan, dan mengabaikan bagaimana perilaku manusia. Pengetahuan bukanlah motif untuk perilaku keamanan informasi manusia. Namun, kurangnya pengetahuan merupakan hambatan dalam mengembangkan perilaku yang diinginkan. Karena itu kampanye dalam bentuk presentasi hanya sebagai sumber transfer informasi dan pengetahuan dari presenter kepada audiens.
b. Pesan Elektronik (E-mail)
   Salah satu jenis kampanye untuk kesadaran keamanan informasi adalah pesan email. . Metode ini efektif dalam memberikan informasi terkait keamanan dan karenanya dapat meningkatkan pengetahuan. Namun, membaca pesan email tidak berarti pesan tersebut telah dipahami oleh penerima. Oleh karena itu, metode ini tidak cukup untuk mengubah sikap dan perilaku penerima pesan karena hanya terjadi komunikasi satu arah.
c. Grup Diskusi
   Diskusi kelompok melibatkan peserta dalam percakapan yang meningkatkan perhatian dan niat terkait keamanan informasi dari peserta [35]. Diskusi dan pertemuan kelompok lebih bersifat tipe interaktif dan karenanya lebih efektif. Pendekatan ini bermanfaat dalam meningkatkan

tingkat kesadaran dengan menggunakan pengetahuan, perhatian, sikap, norma sosial, motivasi dan strategi perilaku. Pendekatan ini menggunakan norma-norma sosial dan interaksi yang memengaruhi pemahaman individu tentang keamanan informasi.

d. Artikel / *Newsletter*
   Artikel maupun newsletter bagus digunakan dalam mentransfer pengetahuan keamanan informasi. Dalam artikel dapat dimuat informasi yang informatif dan berpengetahuan, sehingga baik dalam menambah pengetahuan dan mengubah sikap terhadap kesadaran keamanan informasi. Artikel tidak memiliki komponen norma subyektif, karena itu tidak dapat mengubah niat pembaca dan kemudian mengubah perilaku.
e. *Video Game*s
   Dikatakan oleh para peneliti bahwa video game adalah teknik yang baik dalam memotivasi pemain untuk mengadaptasi perilaku yang diinginkan karena menarik perhatian pemain dan melibatkannya. Namun, metode ini tidak memiliki komponen transfer pengetahuan kecuali pemain telah memperoleh pengetahuan keamanan informasi sebelum memulai permainan. Video game lebih interaktif dan membuat pemain tetap terlibat. Mereka bermanfaat dalam mengubah sikap; Namun, mereka bukan sumber pengetahuan yang sangat baik.
f. *Computer Based Training*
   Pelatihan berbasis komputer memiliki beberapa keunggulan dibandingkan metode konvensional kesadaran keamanan informasi. CBT tersedia setiap saat untuk semua karyawan dalam organisasi dan ini merupakan metode pelatihan kesadaran keamanan informasi yang efektif. metode ini tidak memiliki manfaat interaksi antara instruktur dan audiens dan di antara kelompok audiens, sehingga tidak dapat mengubah niat dan perilaku audiens.
g. Poster
   Poster adalah pengingat keamanan informasi yang sederhana dan efektif yang menarik perhatian pengguna akhir dan mengingatkan aturan keamanan informasi dasar.

27

Poster membutuhkan lebih sedikit sumber daya. Slogan-slogan yang menarik dan desain yang menarik berkontribusi besar pada efektivitas poster. Selain desain dan isi poster, lokasi poster ditampilkan juga menarik perhatian. Poster yang ditampilkan di daerah lalu lintas tinggi cenderung menarik perhatian pemirsa. Namun, mengandalkan poster kesadaran keamanan informasi saja tidak praktis karena tidak mungkin untuk menjelaskan sesuatu pada poster. Selain itu, norma sosial yang memiliki kontribusi besar dalam meningkatkan kesadaran hilang di poster-poster keamanan informasi. Karena komponen norma sosial yang hilang, niat tidak dapat diubah dan oleh karena itu, perilaku terkait keamanan informasi tetap tidak berubah.

Dari penjelasan media penyampaian di atas maka dapat dibuat pengelompokan seperti tabel di bawah ini [23].

Tabel 0.7 Pengelompokan media penyampaian program menurut Khan et al

No	Media	Komponen dalam pengetahuan	Komponen dalam mengubah sikap	Komponen dalam mengubah perilaku
1	Presentasi	V	V	V
2	Pesan Email	V	V	X
3	Grup diskusi	V	V	V
4	Newsletters	V	V	X
5	Video Games	X	V	X
6	CBT	V	V	X
7.	Poster	V	V	X

Selain itu, ISACA (2005) menunjukkan berbagai macam metode yang dapat digunakan sebagai media penyampaian kegiatan peningkatan kesadaran keamanan informasi. Mrdia tersebut dapat dilihat pada tabel di bawah ini [36].

Tabel 0.8 Metode dan media penyampaian informasi ISACA 2005

Educational Interactive (Edukasi yang intetaktif)	*Informational* (Memberikan Informasi)
- Presentasi - Pelatihan - *Short targeted session* - *Online learning modules* - Demo - Video - Workshop	- *Leaflets* - Artikel pendek - Website keamanan informasi - Peringatan melalui e-mail - *Tips tiap bulan* - *Security flash cards (*risiko, ancaman*)* - *Newsletters*
Promotional (Promosi)	Enforcing (Pendorong / Pemaksaan)
- *Event (*acara*)* - *Screen savers* - *Banner* - Majalah - Poster - *Puzzle and games* - *Post-it* / catatan - *T-shirts* - *Mug* - *Mouse pads* - Stiker	- Prinsip jaminan keamanan - Panduan keamanan informasi. - Perjanjian kerahasiaan - Ujian - Memberikan tindakan jika terdapat pelanggaran - Permberian penghargaan

Media edukasi interaktif dapat menghasilkan pemahaman dan penerapan dasar-dasar keamanan dalam jangka panjang, sedangkan media informasi serta promosi merupakan yang terbaik untuk menghasilkan komunikasi dan perhatian terhadap masalah-masalah tertentu. Media pendorong atau pemaksaan berbeda dengan ketiga metode lainnya karena faktor komunikasi yang digunakan sangat sedikit. Metode ini

29

menggambarkan key success factor dalam perubahan perilaku aktual dari setiap target.

Dalam NIST SP 800-50 juga dijabarkan mengenai media yang dapat digunakan dalam menyampaikan program kesadaran keamanan informasi, sebagai berikut [17]:

a. Pesan pada *awareness tools* (seperti pulpen, catatan post-it, buku catatan, kotak P3K, kotak pembersih, disket dengan lampiran pesan, bookmark, frisbee, jam, dsb.

b. Poster

c. *Screensaver* dan spanduk / pesan peringatan.

d. Newslatters

e. Pesan email.

f. Video.

g. Metode berbasis web.

h. Metode berbasis komputer.

i. Metode telekonferensi.

j. Workshop.

k. Peringatan hari keamanan TI atau acara serupa.

l. Seminar

m. Permainan (contoh teka teki silang)

n. Program penghargaan.

2.2.9 DPTSI (Departemen Pengembangan Teknologi Sistem Informasi) ITS

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) bertugas untuk menyediakan dan mengelola layanan Teknologi Informasi di lingkungan ITS. Terkait peran, DPTSI berperan untuk mendukung aktivitas akademik, penelitian dan pengabdian masyarakat, serta manajerial di lingkungan ITS dalam rangka membantu ITS mencapai visi misinya. DPTSI

ITS adalah salah satu badan di ITS yang menangani urusan teknologi dan sistem informasi yang sebelumnya bernama Badan Teknologi Sistem informasi [37]. Sesuai dengan OTK ITS periode implementasi OTK transisi sesuai dengan SK Rektor No. 03 tahun 2012, Badan Teknologi Sistem Informasi dibentuk untuk mengelola, mengkoordinasikan, mengendalikan serta mengembangkan teknologi dan sistem informasi secara terpadu sesuai peraturan perundang-undangan. BTSI meleburkan fungsi unit sebelumnya yaitu UPT Pusat Komputer dan fungsi Sistem Informasi di Biro Administrasi Perencanaan dan Sistem Informasi (BAPSI), ditambah fungsifungsi baru yang terkoordinasi di Pusat-Pusat.
Dalam menjalankan fungsi Badan Teknologi dan Sistem Informasi mempunyai tugas:

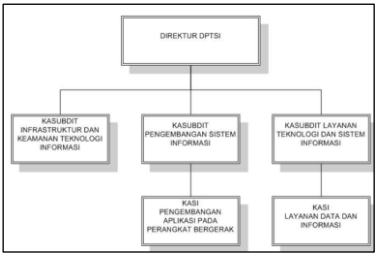
1. Menyusun dan melaksanakan Rencana Induk Pengembangan Teknologi dan Sistem Informasi;
2. Menyediakan dan mengelola infrastruktur;
3. Menyediakan dan mengelola situs dan portal ITS yang berkualitas;
4. Menyediakan dan mengelola aplikasi sistem informasi berbasis webuntuk mengoptimalkan e-layanan;
5. Menjamin keamanan sistem informasi;
6. Mendukung peningkatan kemampuan dan kompetensi tenaga kependidikan di bidang teknologi dan sistem informasi;
7. Menyediakan jasa di bidang teknologi dan sistem informasi dengan berbagai pihak;
8. Menetapkan standar teknologi dan sistem informasi yang dibutuhkan;
9. Menyediakan layanan komunikasi suara dan video berbasis teknologi dan sistem informasi;
10. Menyediakan dan mengelola *knowledge management system*;
11. Mengelola *database* ITS;

12. Mengelola ICT *Center*, *E-learning* dan pembelajaran jarak jauh;
13. Mengembangkan standar data dan informasi;
14. Menyediakan dan mengelola paket program lisensi tunggal;
15. Melakukan audit sistem informasi;
16. Mengkoordinasikan jaringan kerjasama antar institusi berbasis teknologi dan sistem informasi.

BTSI berubah nama menjadi LPTSI (Lembaga Pengembangan Teknologi Sistem Infromasi) berdasarkan Permendikbud No. 86, Tahun 2013 tentang OTK ITS. LPTSI mempunyai tugas melaksanakan, mengkoordinasi, memonitor dan mengevaluasi kegiatan penelitian dan pengembangan teknologi dan sistem informasi. Dalam melaksanakan tugasnya, LPTSI menyelenggarakan fungsi sebagai berikut :

1. Penyusunan rencana, program dan anggaran Lembaga;
2. Pelaksanaan penelitian dan pengembangan teknologi dan sistem informasi;
3. Pelaksanaan penjaminan keamanan sistem informasi;
4. Pelaksanaan peningkatan kemampuan dan kopetensi tenaga kependidikan di bidang teknologi dan sistem informasi;
5. Pengelolaan sistem informasi berbasis web;
6. Pelaksanaan pemberian layanan jasa dibidang teknologi dan sistem informasi;
7. Pelaksanaan koordinasi dan kerjasama antar institusi berbasis teknologi dan sistem informasi;
8. Pelaksanaan monitoring dan evaluasi pengembangan teknologi dan sistem informasi; dan
9. Pelaksanaan urusan administrasi Lembaga

Pada bulan Oktober 2016, LPTSI berubah nama menjadi DPTSI (Direktorat Pengembangan Teknologi dan Sistem Informasi)



Gambar 0.3 Struktur organisasi DPTSI

Direktorat Pengembangan Teknologi dan Sistem Informasi terdiri atas:

a. Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi, mempunyai tugas melaksanakan penyiapan bahan perumusan kebijakan, standar mutu, pelaksanaan pengembangan, pengawasan dan pemantauan, evaluasi, pemeliharaan, dan pelaporan untuk pengembangan dan pengkajian infrastruktur dan keamanan teknologi informasi.
b. Subdirektorat Pengembangan Sistem Informasi, mempunyai tugas melaksanakan penyiapan bahan perumusan kebijakan, standar mutu, pelaksanaan pengembangan, pengawasan dan pemantauan, evaluasi, pemeliharaan, dan pelaporan pengembangan sistem informasi. Dalam melaksanakan tugasnya dibantu oleh Seksi Pengembangan Aplikasi pada Perangkat Bergerak.
c. Subdirektorat Layanan Teknologi dan Sistem Informasi, mempunyai tugas melaksanakan penyiapan bahan perumusan kebijakan, standar mutu, operasional layanan, pengawasan dan pemantauan, evaluasi, dan pelaporan untuk layanan teknologi dan sistem informasi. Dalam melaksanakan tugasnya dibantu oleh Seksi Layanan Data dan Informasi.

33

Halaman ini sengaja dikosongkan

BAB III METODOLOGI PENELITIAN

Bagian ini menjelaskan mengenai metodologi atau alur pengerjaan tugas akhir dengan memberikan rincian di setiap tahapan yang dilakukan.

3.1. Tahapan Pelaksanaan Tugas Akhir

Berikut merupakan uraian langkah-langkah pengerjaan Tugas Akhir beserta gambar yang ditunjukkan pada Gambar 3.1.

3.1.1 Fase 1 : Persiapan

a. Identifikasi Permasalahan

Tahap ini dilakukan untuk mencari permasalahan yang ada, dan untuk selanjutnya dilakukan pencarian solusi yang dapat digunakan untuk menyelesaikan permasalahan yang telah ditemukan. Luaran dari tahap ini adalah topik tugas akhir yang diambil dari permasalahan dan solusi yang telah ditemukan.

b. Studi Literatur

Tahap ini dilakukan pengumpulan data dan informasi yang menunjang pengerjaan tugas akhir guna memperdalam pengetahuan tentang pengerjaan tugas akhir. Pencarian data dan informasi bersumber pada buku dan jurnal terkait kesadaran keamanan informasi dan menyusun rekomendasi untuk meningkatkan kesadaran keamanan informasi secara efektif, diantaranya bagaimana menentukan topik, konten, dan metode yang digunakan dalam kegiatan peningkatan kesadaran keamanan informasi. Selain itu, dilakukan pencarian mengenai *framework* yang dapat digunakan sebagai pedoman dalam menyusun rekomendasi kesadaran keamanan informasi. Dari beberapa framework yang ada, peulis memilih menggunakan *framework* NIST SP 800-50 segabai pedoman dalam membangun rekomendasi kesadaran keamanan informasi. Dari tahap ini, penulis juga mulai menyusun instrumen penelitian yang akan digunakan.

3.1.2 Fase 2 : Pengumpulan Data dan Informasi

a. Merancang Kuesioner

Kuesioner dirancang bertujuan untuk mengetahui tingkat kesadaran keamanan informasi. Kuesioner akan dirancang dalam bentuk pernyataan dan menggunakan skala likert dari angka 1 sampai dengan 5 dan berdasarkan area keamanan informasi dari yang telah digunakan oleh Arfive Gandhi [12] dan Hazasanzadeh et al [13] yang disesuaikan dengan kebutuhan organisasi, serta akan dibedakan berdasarkan tiga dimensi yaitu pengetahuan, sikap, dan perilaku. Tabel 3.2 merupakan area keamanan informasi yang telah dirancang oleh Arvie Ghani dan Hazasanzadeh et al.

Tabel 0.1 Area Keamanan Informasi yang digunakan

Area Keamanan Informasi	Arfive Gandhi	Hazasanzadeh et al
Password Management	v	v
Email Use	v	v
Internet Use	v	v
Social Media Use	v	
Mobile Devices Security	v	v
Information Handling	v	
Incident Reporting	v	v
Backup data		v
Social engineering		v
Malware		v
Adhare to policy		v

Dari 10 area keamanan informasi berdasarkan Tabel 3.2 , ada satu area yang tidak digunaakan yaitu *adhare to policy* (mematuhi kebijakan) dikarenakan belum adanya kebijakan keamanan informasi di ITS, sehingga area keamanan informasi yang akan digunakan adalah sebagai berikut :

1. *Password Management* (Pengelolaan Kata Sandi)
2. *Email Use* (Penggunaan Email)
3. *Internet Use* (Penggunaan Internet)
4. *Social Media Use* (Penggunaan Media Sosial)
5. *Mobile Device Security* (Keamanan Perangkat Mobile)
6. *Information Handling*
7. *Incident Reporting*
8. *Backup data* (Melakukan *backup data*)
9. *Social engineering*
10. *Malware*

b. Melakukan Uji Validitas Kuesioner

Uji validitas data dilakukan untuk mengukur sah atau valid tidaknya suatu kuesioner. Uji validitas dilakukan dengan menggunakan SPSS dengan membandingkan nilai r hitung dengan nilai r tabel. Jika r hitung > r tabel dan nilai positif maka indikator tersebut dinyatakan valid.

Dalam melakukan uji validaitas kuesioner akan digunakan sampel sebesar 10% dari total sampel penelitian. Dari rumus tersebut maka didapatkan sampel uji validitas dan reliabilitas kuesioner sebesar 39 orang.

c. Menyebarkan Kuesioner

Pada tahap ini dilakukan pembagian kuesioner kepada mahasiswa ITS. Jumlah minimal responden pada survei ini ditentukan berdasarkan metode slovin dengan rumus :

37

$$n = \frac{N}{N\alpha^2 + 1}$$

Keterangan : n = ukuran sampel

N = ukuran populasi

α = estimasi kesalahan

Pada pembagian kuesioner ditentukan $\alpha = 0{,}05$ (5%) dengan total mahasiswa S1 ITS sejumlah 14523 (data didapat dari dengan penyebaran tiap fakultas sebagai berikut :

Tabel 0.2 Tabel Jumlah Mahasiswa ITS

Fakultas	Jumlah Mahasiswa S1
Fakultas Sains (FS)	1189
Fakultas Teknologi Industri (FTI)	3518
Fakulas Teknologi Elektro (FTE)	1335
Fakultas Teknik Sipil, Lingkungan dan Kebumian (FTSLK)	1785
Fakultas Arsitektur, Desain, dan Perencanaan (FADP)	1780
Fakultas Teknologi Kelautan (FTK)	1782

Fakultas Matematika, Komputasu dan Sains Data (FMKSD)	986
Fakultas Teknologi Informasi dan Komunikasi (FTIK)	1458
Fakultas Bisnis dan Manajemen Teknologi (FBMT)	465
Fakultas Vokasi	2474

Dengan begitu dapat dilakukan perhitungan jumlah minimal responden yang harus didapatkan pada penelitian ini dengan menggunakan rumus slovin, sebagai berikut :

$$n = \frac{16997}{16997\ (0{,}05)^2+1} = \frac{16997}{43{,}50} = 390{,}80 \text{ atau } 391$$

Kemudian dari 389 responden tersebut didapatkan jumlah responden berdasarkan fakultas sebagai berikut :

FIA $= \frac{1189}{16997} \times 391 = 28$ responden

FTI $= \frac{3518}{16997} \times 391 = 81$ responden

FTE $= \frac{1335}{16997} \times 391 = 31$ responden

FTSLK $= \frac{1785}{16997} \times 391 = 41$ responden

FADP $= \frac{1780}{16997} \times 391 = 41$ responden

FTK $= \frac{1782}{16997} \times 391 = 41$ responden

FMKSD $= \frac{986}{16997} \times 391 = 23$ responden

39

FTIK $= \frac{1458}{16997} \times 391 = 37$ responden

FBMT $= \frac{465}{16997} \times 391 = 11$ responden

VOKASI $= \frac{2474}{16997} \times 391 = 57$

Penyebaran kuesioner dilakukan secara online dengan menggunakan fasilitas *google form* maupun secara offline dengan membagikan selebaran kuesioner kepada responden.

3.1.3 Fase 3 : Pengolahan dan Analisis Data

Pada fase ini dilakukan pengolahan dan analisis data yang selanjutnya akan digunakan sebagai acuan dalam penyusunan rekomendasi kesadaran keamanan informasi.Cara melakukan pengolahan data menggunakan metode analisis deskriptif persentase [38] dengan langkah-langkah sebagai berikut :

a. Membuat tabel jawaban angket.

b. Mengkuantitatifkan jawaban setiap pernyataan dengan mengalikan freuensi jawaban dari tiap alternatif jawaban dengan skor sesuai bobot yang telah ditentukan dalam skala likert yang dapat dilihat pada Tabel 3.4.

Tabel 0.3 Tabel Bobot Tiap Alternatif Jawaban

Alternatif Jawaban	Bobot Alternatif Jawaban	
	Pernyataan Positif (+)	Pernyataan Negatif (-)
Sangat Setuju (SS)	5	1
Setuju (S)	4	2
Ragu-ragu (RG)	3	3
Tidak Setuju (TS)	2	4
Sangat Tidak Setuju (STS)	1	5

Setelah masing-masing alternatif jawaban dikalikan, maka selanjutnya adalah menjumlahkan skor jawaban yang diperoleh. Untuk mempermudah, maka dapat ditulis dengan rumus berikut :

$$\mathbf{n=\sum(T\ x\ Pn)}$$

Keterangan :

n = jumlah skor tiap variable

T = Jumlah responden yang memilih untuk tiap skala likert

Pn = Bobot dari skala likert

c. Selanjutnya mengitung indeks skor tertinggi (Y) dengan rumus sebagai berikut :

$$\mathbf{N = SS\ x\ R}$$

Keterangan : SS = Bobot tertinggi dari skala likert.

R = Total responden.

d. Dari dua rumus di atas sehingga didapatkan hasil akhir dengan rumus yang telah dirumuskan oleh Muhammad Ali dalam thesis Ali Akbar Fahrani [38] :

$$\mathbf{Skor\ Akhir\ (\%)\ = \frac{n}{N}\ X\ 100\ \%}$$

Selanjutnya dapat dilakukan analisis data untuk mendukung kebutuhan dalam menyusun rekomendasi peningkatan kesadaran keamanan informasi berdasarkan tabel tingkat kesadaran keamanan informasi.

41

3.1.4 Fase 4 : Penyusunan Rekomendasi

Dalam menyusun rekomendasi peningkatan kesadaran keamanan informasi dalam penelitian yang saya lakukan akan mengacu pada *framework* NIST SP 800-50 dengan melakukan modifikasi sesuai dengan kebutuhan dari penelitian yang saya lakukan. Berikut merupakan langkah-langkah untuk membuat usulan rekomendasi peningkatan kesadaran keamanan informasi :

a. Merancang Usulan Rekomendasi Peningkatan Kesadaran Keamanan Informasi
   Dalam merancang rekomendasi peningkatan kesadaran keamanan informasi terdapat beberapa langkah yang dilakukan, yaitu :

   1. Menentukan Topik

      Sebelum merancang suatu rekomendasi atau kegiatan, sebelumnya sangat penting mengetahui daftar topik yang perlu dilakukan penindakan. Untuk menentuan topik tersebut dapat diketahui melalui hasil dari *security awareness maps*. Topik yang akan diambil adalah yang berada pada status sedang dan buruk karena perlu adanya penindakan.

   2. Mengembangkan Strategi dan Rancangan Kegiatan

      Berikut beberapa elemen penting yang harus diidentifikasi guna mengembangkan strategi dan rancangan kegiatan :

      - Media penyampaian
      - Grup target (jika terdapat perbedaan perlakuan)
      - Tujuan pembelajaran dari adanya kegiatan.
      - Peran dan tanggung jawab dalam merancang, mengembangkan, mengimplementasikan, memelihara, dan memastikan berjalannya kegiatan.
      - Frekuensi dari pelaksanaan kegiatan.

- Timeline pelaksanaan
- Deskripsi
- Indikator kesuksesan rekomendasi.

b. Mengembangkan Rancangan Usulan Kegiatan

1. Menyusun Materi

   Setelah mengetahui topik kesadaran keamanan informasi yang akan dibahas dalam usulan kegiatan, maka selanjutnya mengembangkan topik tersebut menjadi materi atau konten. Konten tersebut akan disusun berdasarkan studi literatur seperti buku, jurnal, standard keamanan informasi, dan sumber terpercaya lainnya.

2. Melakukan *Expert Judgement*

   Untuk memastikan kesesuaian kegiatan yang telah saya susun, maka selanjutnya saya akan melakukan validasi kepada *expert* , yaitu seorang psikolog yang mengerti mengenai cara mempengaruhi seseorang.

3. Mengembangkan Menjadi Sebuah Usulan Rekomendasi

   Setelah rancangan dan materi terah tervalidasi, selanjutnya adalah mengembangkan rancangan tersebut ke dalam usulan rekomendasi.

3.1.5 Fase 5 : Penyusunan Laporan Tugas Akhir

Tahapan ini merupakan tahapan terakhir dari metodologi. Pada tahap ini, seluruh hasil penelitian didokumentasikan dalam bentuk laporan tugas akhir. Selain itu, laporan tugas akhir juga berisi tentang hasil dari penelitian dan saran untuk penelitian selanjutnya.

43

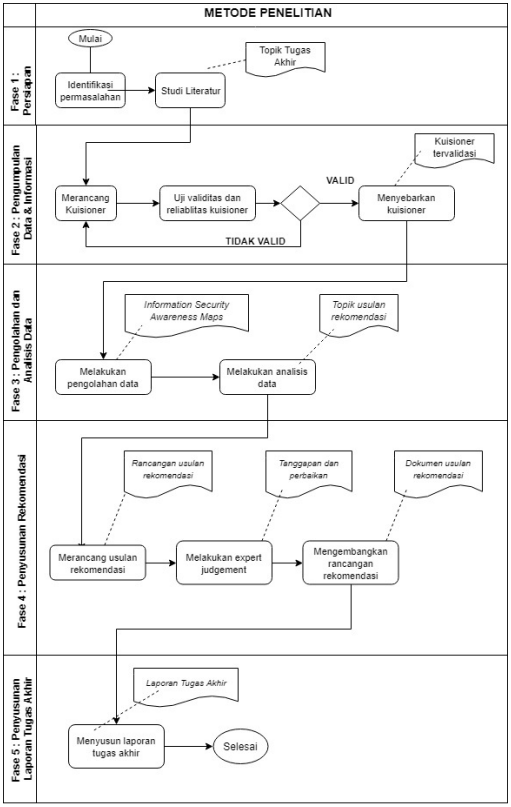


Diagram 0.1Metodologi Penelitian Tugas Akhir

BAB IV
PERANCANGAN

Bagian ini menjelaskan mengenai pembuatan kuesioner yang telah dilakukan pengujian validitas dan reliabilitas sehingga kuesioner dapat dipercaya sebagai alat ukur yang benar. Selain itu juga dijelaskan terkait pengelompokan berdasarkan studi literatur yang telah dilakukan oleh penulis.

4.1. Perancangan Studi Kasus

4.1.1 Tujuan Studi Kasus

Studi kasus merupakan alat yang dapat digunakan peneliti untuk mengambil keputusan. Studi kasus digunakan peneliti agar mendapatkan gambaran langsung mengenai kondisi yang terjadi pada fenomena tertentu. Dengan adanya studi kasus, peneliti dapat mempelajari berbagai aspek, menguji hubungan satu sama lain, dan menggunakan kapasitas peneliti dalam memahami suatu studi kasus tersebut.

4.1.2 Subjek dan Objek Penelitian

Subjek penelitian dalam Tugas Akhir ini merupakan mahasiswa Institut Teknologi Sepuluh Nopember (ITS) Surabaya dengan jenjang pendidikan tingkat Diploma (D1-D4) dan Sarjana (S1). Objek dalam penelitian ini adalah tingkat kesadaran keamanan informasi mahasiswa ITS dalam penggunaan teknologi informasi.

4.2 Perancangan Pengumpulan Data

Ada beberapa cara yang dapat digunakan dalam melakukan pengumpulan data, Osang et al [39] memberikan penjelasan terkait empat teknik dalam pengumpulan data yang dapat dilihat pada Tabel 4.1.

Tabel 0.1 Teknik Pengumpulan Data Menurut Oseng et al [39]

Wawancara	Kuesioner	Observasi	Eksperimen	Studi Kasus
Wawancara umumnya bersifat kualitatif yang dilakukan secara langsung atau melalui telepon dan membutuhkan banyak waktu untuk mendapatkan respon dari masing-masing responden.	Kuesioner dapat dianalisis menggunakan metode kuantitatif dengan menetapkan nilai numerik menggunakan skala likert. Hasilnya mudah untuk dilakukan analisis	Observasi dilakukan untuk mempelajari dinamika situasi, jumlah frekuensi, atau perilaku lain sesuai kebutuhan penelitian yang menghasilkan data berupa data kulitatif	Metode eksperimen digunakan dalam penelitian ilmiah untuk mengumpulkan data dalam perspektif sains dan teknik	Membantu peneliti dalam memahami atau menggambarkan pengalaman klien dalam suatu program, dan melakukan pemeriksaan kpmprehensif melalui perbandingan antar kasus.

Berdasarkan beberapa teknik yang telah dijelaskan sebelumnya, dalam penelitian ini akan menggunakan teknik kuesioner dalam mengumpulkan data. Teknik kuesioner dipilih karena dalam penelitian ini membutuhkan data dalam bentuk kuantitatif, serta penelitian ini membutuhkan responden yang cukup besar sehingga teknik kuesioner cocok digunakan karena dapat menyebar secara luas dengan mudah dan lebih cepat. Kuesioner akan disebar kepada responden, yaitu mahasiswa Institut Teknologi Sepuluh Nopember tingkat D1-S1dengan target minimal 391 responden.

4.2.1 Proses Penyusunan Kuesioner

Sebelum kuesioner disebarkan kepada target (responden), kuesioner perlu dipastikan validitasnya agar kuesioner dapat dianggap sebagai alat ukur yang sesuai dalam penelitian. Berikut merupakan langkah-langkah yang dilakukan dalam proses perancangan kuesioner sampai kuesioner dinyatakan valid.

a. Mencari Referensi
   Reverensi dibutuhkan agar penyusunan kuesioner lebih mudah dilakukan karena sudah ada penelitian sebelumnya yang dapat digunakan sebagai acuan.
b. Menyusun Pernyataan Kuesioner
   Setelah menemukan reveresnsi yang sesui, kemudian kuesioner dapat disusun berdasarkan acuan dan disesuaikan dengan kebutuhan target. Dalam penelitian ini kuesioner mengacu pada penelitian Parsons et al [40]
c. Melakukan Uji Pemahaman
   Uji pemahaman merupakan hal penting agar kuesioner yang telah disusun dipastikan dapat dipahami oleh responden. Uji pemahaman ini dilakukan kepada beberapa orang untuk mendapatkan feedback.
d. Melakukan Uji Validitas
   Setelah kuesioner dipastikan dapat dipahami, maka selanjutnya dilakukan uji validitas agar kuesioner benar-benkar dianggap dapat menjadi alat uur penelitian. Penyebaran kuesioner untuk uji validitas dilakukan kepada

47

40 orang yang memiliki latar belakang sama seperti responden sesungguhnya, yaitu seorang mahasiswa. Setelah kuesioner dianggap valid, maka kuesioner siap disebarkan ke responden yang sesungguhnya.

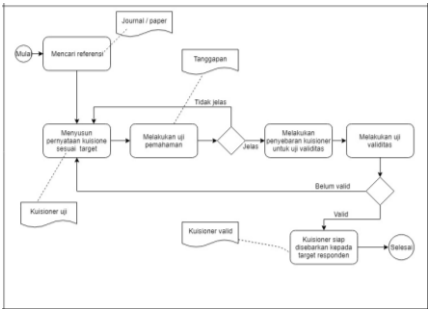
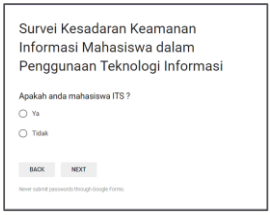


Diagram 0.1 Alur Penyusunan Kuesioner Hingga Valid

4.2.2 Perancangan Kuesioner

Dalam merancang kuesioner, kuesioner dibagi menjadi empat bagian, antara lain:

A. Bagian Pembuka



Gambar 0.1Bagian Pembuka Kuesioner

Bagian ini digunakan untuk memastikan apakah calon responden merupakan mahasiswa ITS. Jika responden menjawab “Tidak” maka pengisian kuesioner telah selesai.

B. Bagian Data Demografi

Gambar 0.2 Bagian Demografi Responden (1)

Gambar 0.3 Bagian Demografi Responden (2)

49

Pada bagian demografi responden dibutuhkan data-data sebagai berikut :

1. Nama : digunakan sebagai identitas dari responden.
2. Jenis kelamin : digunakan untuk mengetahui persebaran kuesioner berdasarkan jenis kelamin yang selanjutnya dapat digunakan untuk membandingkan kesadaran keamanan informasi.
3. Jenjang pendidikan :digunakan untuk menyeleksi responden karena responden dibatasi hanya untuk Diploma dan Sarjana 1, serta juga digunakan untuk mengatahui persebaran kuesioner.
4. Fakultas : digunakan untuk mengetahui asal fakultas dari responden sehingga menunjang bukti pencapaian target tiap fakultas yang telah ditentukan sebelumnya.
5. Departemen / Jurusan : digunakan untuk mengetahui asal departemen dari responden sehingga dapat digunakan sebagai bukti pendukung.
6. Kontak : merupakan informasi yang bersifat opsional karena hanya digunakan untuk pengundian hadiah sebagai ucapan terima kasih dari peneliti.
7. Durasi penggunaan komputer/internet : digunakan untuk mengetahui seberapa lama mahasiswa dalam menggunakan komputer/internet dan selanjutnya dapat diketahui tingkat penggunaan komputer/internet mahasiswa ITS.

C. List Pernyataan Mengenai Kesadaran Keamanan Informasi

Kuesioner dirancang berdasarkan adaptasi dari penelitian Persons et al [40]. Kuesioner ini dirancang berdasarkan dimensi kesadaran keamanan informasi dan area keamanan informasi yang masing-masing memiliki dua seb area. Area dan sub area keamanan, serta dimensi yang digunakan akan dijelaskan dalam Tabel 4.2.

Tabel 0.2 Area,Sub Area dan Dimensi dalam Penelitian

NO	Area	Sub Area	Dimensi	
1.	Manajemen *Password*	Penggunaan *password* untuk berbagai akun.	Knowledge	Pengetahuan terkait penggunaan *password* untuk media sosial dan akun perkuliahan penting untuk dibedakan.
			Attitude	Sikap atau perasaan aman seseorang terkait penggunaan *password* antara akun media sosial dan akun perkuliahan.
			Behavior	Perilaku seseorang dalam menggunakan *password* untuk akun media sosial dan akun perkuliahan.
		Kekuatan passwod.	Knowledge	Pengetahuan seseorang dalam kombinasi untuk membuat *password* yang aman.
			Attitude	Sikap atau rasa aman terhadap *password* dengan kombinasi yang tidak sesuai standard.
			Behavior	Perilaku seseorang dalam membuat *password*.
2.	Penggunaan Email	Mengklik link dalam email.	Knowledge	Pengetahuan sesorang terkait membuka link dari email seseorang yang tidak dikenal
			Attitude	Sikap atau rasa aman terhadap adanya link dalam email dari pengirim yang tidak dikenal.

NO	Area	Sub Area	Dimensi	
			Behavior	Respon seseorang dalam menaggapi jika ada email yang berisi link dari seseorang yang tidak dikenal.
		Mendownloa d lampiran dalam email	Knowledge	Pengetahuan sesorang terkait mendownlod lampiran dalam email dari seseorang yang tidak dikenal
			Attitude	Sikap atau rasa aman jika mendownload lampiran dalam email dari pengirim yang tidak dikenal.
			Behavior	Respon seseorang dalam menaggapi jika ada email berisi lampiran dari pengirim yang tidak dikenal
3.	Penggunaan Internet	Mendownloa d file dari internet.	Knowledge	Pengetahuan seseorang terkait mendownload file / software dari website yang tidak resmi.
			Attitude	Sikap atau rasa aman jika mendownload file dari website yang tidak resmi.
			Behavior	Perilaku seseorang dalam mendownload file/ software.
		Memasukkan informasi secara online.	Knowledge	Pengetahuan seseorang terkait bahaya menginputkan informasi pribadi pada suatu website.
			Attitude	Sikap atau rasa aman seseorang dalam menginputkan informasi pribadi pada suatu website.
			Behavior	Perilaku seseorang dalam mewaspadai website saat menginputkan informasi pribadi.

NO	Area	Sub Area	Dimensi	
4.	Penggunaan Media Sosial	Pengecekan pengaturan privasi secara berkala.	Knowledge	Pengetahuan seseorang terkait pentingnya pengecekan pengaturan privasi secara berkala.
			Attitude	Sikap seseorang terkait pentingnya pengecekan pengaturan privasi secara berkala.
			Behavior	Perilaku seseorang terkait pengecekan pengaturan privasi.
		Posting tentang informasi pribadi di Media Sosial.	Knowledge	Pengetahuan seseorang terkait informasi yang tergolong informasi pribadi.
			Attitude	Sikap atau rasa aman seseorang terkait informasi pribadi yang ditampilkan dalam profil media sosial.
			Behavior	Perilaku seseorang dalam menampilkan informasi pribadi.
5.	Keamanan Perangkat Mobile (Desktop dan Handphone)	Mengirim informasi sensitif melalui jaringan publik	Knowledge	Pengetahuan seseorang terkait risiko dalam mengirim atau mengakses informasi sensitif melalui jaringan publik.
			Attitude	Sikap atau rasa aman seseorang dalam mengirim atau mengakses informasi sensitif melalui jaringan publik.
			Behavior	Perilaku seseorang dalam mengirim atau mengakses informasi sensitif melalui jaringan publik.

NO	Area	Sub Area	Dimensi	
		Adanya *Shoulder Surfing*	Knowledge	Pengetahuan seseorang terkait adanya *shoulder surfing.*
			Attitude	Sikap atau rasa aman seseorang saat ada orang lain yang dapat melihat dokumen / pekerjaan sensitif yang sedang dikerjakan.
			Behavior	Perilaku seseorang dalam mewaspadai orang sekitar saat mengerjakan dokumen yang bersifat sensitif.
6.	Penanganan Informasi	Membuang kertas / dokumen dengan informasi sensitif	Knowledge	Pengetahuan seseorang terkait cara membuang kertas / dokumen yang bersifat sensitif.
			Attitude	Sikap atau rasa aman seseorang terkait cara membuang kertas / dokumen yang bersifat sensitif.
			Behavior	Perilaku seseorang dalam membuang kertas / dokumen yang bersifat sensitif.
		Memasukkan media yang ditemukan tanpa sengaja.	Knowledge	Pengetahuan seseorang terkait risiko menancapkan flaskdisk asing/temuan.
			Attitude	Sikap atau rasa aman seseorang jika menancapkan flashdisk asing/temuan.
			Behavior	Perilaku seseorang saat menemukan flashdisk.

NO	Area	Sub Area	Dimensi	
7.	Pelaporan Insiden	Melaporkan perilaku mencurigakan	Knowledge	Pengetahuan tentang tindakan yang harus dilakukan jika ada perilaku mencurigakan terkait masalah keamanan informasi di kampus.
			Attitude	Sikap yang ditunjukkan saat ada perilaku mencurigakan terkait masalah keamanan informasi di kampus.
			Behavior	Perilaku atau respon jika ada perilaku mencurigakan terkait masalah keamanan informasi di kampus.
		Melaporkan perilaku buruk teman.	Knowledge	Pengetahuan tentang adanya perilaku buruk/pelanggaran keamanan informasi yang dilakukan teman.
			Attitude	Sikap yang ditunjukkan jika ada perilaku buruk/pelanggaran keamanan informasi yang dilakukan teman.
			Behavior	Perilaku atau respon yanng dilakukaan saat ada perilaku buruk/pelanggaran keamanan informasi yang dilakukan teman.
8.	Melakukan *Backup data*	Melakukan *backup data*	Knowledge	Pengetahuan tentang perlunya melakukan *backup data* secara berkala.

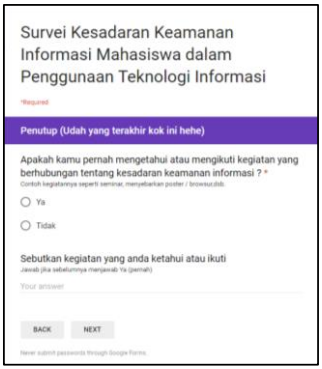
NO	Area	Sub Area	Dimensi	
		secara berkala	Attitude	Sikap atau rasa aman jika melakukan *backup data* secara berkala.
			Behavior	Perilaku dalam melaksanakan *backup data* secara berkala.
		Media *backup data*	Knowledge	Pengetahuan terkait media atau tempat yang aman digunakan dalam melakukan *backup data*
			Attitude	Sikap atau rasa aman dalam menyimpan file *backup*.
			Behavior	Perilaku dalam melakukan *backup data*.
9.	*Social engineering*	Phising	Knowledge	Pengetahuan tentang kejahatan memanipulasi halaman website.
			Attitude	Sikap atau rasa aman melakukan login media sosial yang terhubung dengan website.
			Behavior	Perilaku jika terdapat penawaran menarik dan diharuskan login dalam akun media sosial.
		Kepercayaan dengan orang lain	Knowledge	Pengetahuan seseorang terkait risiko memberi informasi pribadi kepada orang asing.
			Attitude	Sikap atau perasaan seseorang jika terdapat orang asing yang bertanya terkait informasi pribadi.
			Behavior	Perilaku seseorang jika terdapat orang asing yang bertanya terkait informasi pribadi.

NO	Area	Sub Area	Dimensi	
10.	Malware	Sumber Malware	Knowledge	Pengetahuan seseorang terkait indikasi adanya malware.
			Attitude	Sikap seseorang jika komputer berperilaku aneh (adanya malware).
			Behavior	Perilaku seseorang jika komputer berperilaku aneh (adanya malware).
		Pencegahan Malware	Knowledge	Pengetahuan seseorang terkait pencegahan adanya salah satu jenis malware (contohnya virus).
			Attitude	Sikap seseorang terkait adanya pencegahan adanya malware (contohnya virus).
			Behavior	Perilaku seseorang untuk mencegah adanya malware (contohnya virus).

Dalam kuesioner tersebut akan diberikan dua pernyataan negasi, yaitu pernyataan yang berkebalikan dengan pernyataan yang sudah ada. Pernyataan negasi digunakan untuk mengetahui apakah responden mengisi dengan sungguh-sungguh untuk mendukung validitas kuesioner.

D. Bagian Penutup

Dalam bagian penutup, peneliti ingin mengetahui apakah responden pernah mengetahui atau mengikuti kegiatan tentang kesadaran keamanan informasi. Untuk itu diberikan pertanyaan sebagai berikut :

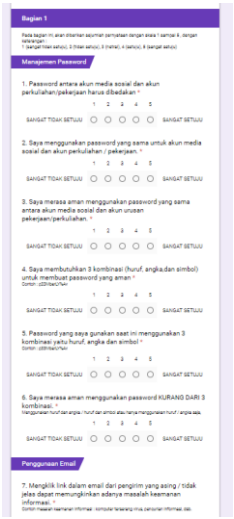


Gambar 0.4 Bagian Penutup Kuesioner

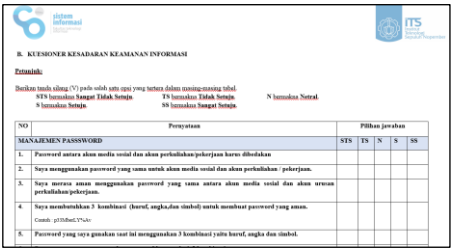
4.2.3 Penyebaran Kuesioner

Penyebaran kuesioner dilakukan dengan dua cara, yaitu *online dan offline* . Untuk kuesioner online dilakukan pembuatan dengan fitur yang ada pada *google*, yaitu *google form* dan dilakukan penyebaran informasi melalui media sosial, seperti LINE, *WhatsApp*, dan I*nstagram*, serta membagikan brosur kepada mahasiswa ITS di seluruh fakultas yang ada di ITS.

58



Gambar 0.5 Tampilan Bagian Pernyataan Kuesioner Online



B. KUESIONER KESADARAN KEAMANAN INFORMASI

Petunjuk:

Berikan tanda silang (V) pada salah satu opsi yang tertera dalam masing-masing tabel.
STS bermakna **Sangat Tidak Setuju**. **TS** bermakna **Tidak Setuju**. **N** bermakna **Netral**.
S bermakna **Setuju**. **SS** bermakna **Sangat Setuju**.

NO	Pernyataan	Pilihan jawaban				
MANAJEMEN PASSSWORD		**STS**	**TS**	**N**	**S**	**SS**
1.	**Password antara akun media sosial dan akun perkuliahan/pekerjaan harus dibedakan**					
2.	**Saya menggunakan password yang sama untuk akun media sosial dan akun perkuliahan / pekerjaan.**					
3.	**Saya merasa aman menggunakan password yang sama antara akun media sosial dan akun urusan perkuliahan/pekerjaan.**					
4.	**Saya membutuhkan 3 kombinasi (huruf, angka,dan simbol) untuk membuat password yang aman.** Contoh : p3Rtbe57A4					
5.	Password yang saya gunakan saat ini menggunakan 3 kombinasi yaitu huruf, angka dan simbol.					

Gambar 0.6 Tampilan Bagian Pernyataan Kuesioner Offline

Dari penyebaran kuesioner secara online maupun offline, diharapkan responden yang mengisi kuesioner dengan benar minimal berjumlah 389 orang.

4.3 Perancangan Pengolahan Data

Cara melakukan pengolahan data menggunakan metode analisis deskriptif persentase yang telah diperkenalkan oleh oleh Muhammad Ali yang dapat dilihat pada Tabel 3.4.

Setelah masing-masing alternatif jawaban dikalikan, maka selanjutnya adalah menjumlahkan skor jawaban yang diperoleh. Untuk mempermudah, maka dapat ditulis dengan rumus berikut :

$$n=\sum(T \; x \; Pn)$$

Keterangan :

n = jumlah skor tiap variable

T = Jumlah responden yang memilih untuk tiap skala likert

Pn = Bobot dari skala likert

a. Selanjutnya mengitung indeks skor tertinggi (Y) dengan rumus sebagai berikut :

$$N = SS \; x \; R$$

Keterangan : SS = Bobot tertinggi dari skala likert.

R = Total responden.

b. Dari dua rumus di atas sehingga didapatkan hasil akhir dengan rumus yang telah dirumuskan oleh Muhammad Ali dalam thesis Ali Akbar Fahrani [38] :

$$\text{Skor Akhir (\%)} = \frac{n}{N} \; X \; 100 \; \%$$

Selanjutnya dapat dilakukan analisis data untuk mendukung kebutuhan dalam menyusun rekomendasi peningkatan kesadaran keamanan informasi berdasarkan tabel tingkat kesadaran keamanan informasi.

4.4. Perancangan Analisis dan Pembuatan Usulan Rekomendasi

4.4.1 Analisis Data

Analisis data dilakukan berdasarkan dari hasil pengolahan data. Dari pegolahan data tersebut didapatkan nilai dari tiap area keamanan informasi dan dimensi kesadaran keamanan informasi. Dari nilai tersebut nantinya dapat diberikan status sesuai dengan tabel tingkat kesadaran keamanan informasi (Tabel 2.6).

4.4.2 Pembuatan Usulan Rekomendasi Kegiatan Peningkatan Kesadaran Keamanan Informasi

Usulan rekomendasi kegiatan untuk meningkatkan kesadaran keamanan informasi mahasiswa ITS akan dirancang berdasarkan framework NIST SP 800-50. Topik kesadaran keamanan informasi dirancang berdasarkan hasil dari analisis data yang menghasilkan status dari tiap area dan dimensi. Selanjutnya, topik tersebut akan dikembangkan menjadi materi dan dirancang mengikuti media penyampaian yang telah dipilih dengan mempertimbangkan studi literatur yang telah dilakukan peneliti. Untuk memastikan rekomendasi telah dirancang sesuai dengan kebutuhan target, maka selanjutnya dilakukan*expert* judgement, yaitu meminta pendapat dari beberapa ahli yang dalam hal ini adalah seorang psikolog yang ada di ITS.

61

Halaman ini sengaja dikosongkan

BAB V
IMPLEMENTASI

Bab ini menjelaskan hasil dari proses perancangan studi kasus yang didapatkan melalui penyebaran kuesioner

5.1. Pelaksanaan Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan menggunakan metode penyebaran kuesioner.Pengumpulan data dilakukan dengan dua tahap, yaitu tahap uji coba kuesioner dan tahap penyebaran kuesioner. Tahap uji coba bertujuan untuk memastikan kuesioner penelitian dapat dianggap valid atau mampu menjadi alat pengukuran yang benar. Setelah kuesioner dianggap valid maka selanjutnya dapat disebar secara luas kepada mahasiswa ITS yang telah ditargetkan. Rincian aktivitas pengumpulan data yang telah dilakukan peneliti adalah sebagai berikut:

Tabel 0.1 Timeline pelaksanaan pengumpulan data

Tanggal	Durasi	Aktivitas	Target	Jumlah	Hasil
25 Maret 2019	1 Hari	Uji pemahaman	Mahasiswa ITS	4	Beberapa item kurang jelas
27 Maret 2019	1 Hari	Uji pemahaman	Mahasiswa ITS	4	Jelas
9 April 2019 - 12 April 2019	3 Hari	Uji Validitas	Mahasiswa Umum	60	Beberapa item tidak valid
13 April 2019 – 15 April 2019	2 Hari	Uji Validitas	Mahasiswa Umum	60	Beberapa item tidak valid

Tanggal	Durasi	Aktivitas	Target	Jumlah	Hasil
16 April 2019 sampai 18 April 2019	2 Hari	Uji Validitas	Mahasis-wa Umum	40	Valid
20 April 2019 – 15 Mei 2019	25 Hari	Penyebaran kuesioner valid	Mahasis-wa ITS	479	Memenuhi target
17 Mei 2019	1 Hari	Filtering konsistensi responden	479 kuesioner yang telah terkumpul	425	Memenuhi Target
18 Mei 2019	1 Hari	Uji validitas kuesioner sesungguhnya	425 kuesioner yang telah konsisten (valid)	425	Valid

5.1.1. Tahap Uji Coba Kuesioner

Sebelum kuesioner disebarkan kepada target, kuesioner harus dipastikan valid agar kuesioner dapat dipercaya sebagai alat ukur yang benar. Maka dari itu kuesioner perlu dilakukan pengujian terlebih dahulu.Dalam pengujian kuesioner terdapat dua pengujian yang dilakukan, yaitu uji pemahaman item pernyataan dan uji validitas item pernyataan. Uji pemahan dilakukan kepada 8 orang mahasiswa ITS dengan memperlihatkan kuesioner dan meminta *feedback* untuk perbaikan kuesioner. Pengumpulan data untuk uji validitas kuesioner uji coba dilakukan dengan cara menyebarkan link kuesioner secara online menggunakan media sosial (LINE dan twitter) dengan kriteria responden adalah seorang mahasiswa. Link yang digunakan dalam pengumpulan data uji coba kuesioner adalah bi.ly/TAISA2019. Berikut hasil tahap uji coba kuesioner.

a. Hasil Uji Pemahaman Item Kuesioner

Uji pemahaman dilakukan agar kuesioner dipastikan dapat dipahami oleh responden yang akan mengisi. Penyebaran kuesioner untuk uji pemahaman dilakukan pada tanggal 25 Maret 2019 sampai 28 Maret 2019. Uji pemahaman ini dilakukan kepada 8 orang mahasiswa ITS dengan departemen yang berbeda. Dari 8 orang tersebut didapatkan tanggapan yang dapat dilihat pada Tabel 5.1.

Tabel 0.2 Tanggapan tentang pernyataan pada kuesioner

	Nama Reviewer	Tanggapan
Uji pemahaman Tahap 1	Nasywa Ibtisamah (Mahasiswa ITS, Sistem Informasi)	*8.* Lebih baik dikurangi sectionnya agar yang mengisi tidak terlalu banyak klik. *9.* Ada beberapa pernyataan yang mirip, jadi membingunkan. *10.* Tambahkan contoh, ada beberapa yang belum ada contohnya. *11.* Ada kata yang *typo*.
	Rizky Nurlaily (Mahasiswa ITS, Manajemen Bisnis)	*12.* Ada beberapa pernyataan yang perlu berfikir ulang, lebih baik diperjelas atau dipersingkat lagi. *13.* Tambahkan contoh untuk memperjelas pernyataan. *14.* Ada kata yang salah dalam penulisannya.
	Mega Septia Sarda Devi (Mahasiswa ITS, Teknik Sipil)	*15.* Terlalu banyak section, jadi terlihat banyak sekali pertanyaannya. *16.* Ada kata yang salah dalam penulisannya.

	Nama Reviewer	Tanggapan
		17. Ada pernyataan yang cenderung sama. *18.* Tambahkan penjelasan untuk kata-kata yang tidak umum diketahui banyak orang, seperti *backup data*, malware,dsb.
	Neneng Amel Hisniam (Mahasiswa ITS, Teknik Lingkungan)	*19.* Beberapa pernyataan hampir sama sehingga bingung dan harus berfikir ulang *20.* Ada kata yang salah penulisannya. *21.* Tambahkan contoh atau penjelasan terkait kata-kata yang tidak umum diketahui orang yang kurang paham TI.

Berdasarkan hasil tanggapan yang telah diberikan, kemudian peneliti melakukan perbaikan sebagai berikut :

1. Mengurangi *section* pada bagian pernyataan kuesioner online (dari 10 *section* menjadi 3 *section*).
2. Mengubah kata-kata yang salah dalam penulisan.
3. Mengubah beberapa pernyataan yang cennderung sama.
4. Mengubah beberapa pernyataan yang kata-katanya membingunkan.
5. Menambahkan penjelasan dan contoh untuk pernyataan yang tidak umum diketahui orang yang kurang paham TI.

Setelah kuesioner dilakukan perbaikan, maka kuesioner dibagikan lagi kepada mahasiswa yang berbeda dengan feedback yang dapat dilihat pada tabel berikut :

Tabel 0.3 Tanggapan uji pemahaman (revisi)

	Nama Reviewer	Tanggapan
Uji Pemahaman Tahap 2 (Sudah direvisi)	Faiz Anggoro Mukti (Mahasiswa ITS, Sistem Informasi)	Jelas
	Riva Dianita (Mahasiswa ITS, Teknik Geomatika)	Jelas
	Nurvitasari (Mahasiswa ITS, Teknik Sipil)	Jelas
	Dewi Purwaningrum (Mahasiswa ITS, Sistem Perkapalan)	Jelas

Hasil dari uji pemahaman kedua adalah semua responden menyatakan jelas, sehingga pengujian pemahaman telah dianggap selesai dan selanjutnya kuesioner dapat disebarkan untuk uji validitas kuesioner.

b. Uji Validitas Kuesioner

Sebelum kuesioner disebarkan kepada responden yang sesungguhnya, maka kuesioner perlu dilakukan pengujian terkait validitas dari item-item pernyataan. Uji validitas bertujuan untuk mengetahui apakah alat ukur (kuesioner) yang digunakan bersifat akurat. Berikut rincian aktivitas pengujian validitas kuesioner uji coba.

Tabel 0.4 Aktivitas pengumpulan data uji validitas kuesioner uji coba

Uji Coba ke-	Jumlah Responden	Jumlah item tidak valid	Solusi
1	60	8	Mengganti item pernyataan
2	40	2	Mengganti item pernyataan
3	40	0	-

Uji validitas kuesioner dilakukan penggunaka *tools* SPSS. Tingkat error yang digunakan dalam pengambilan data ini sebesar 0,05 (5%). Nilai r hitung untuk jumlah responden 40 dan tingkat error 0,05 adalah 0,3044. Item kuesioner dikatakan valid jika r tabel < r hitung. Berikut adalah hasil uji validitas dari item-item kuesioner yang telah valid.

Tabel 0.5 Hasil Uji Validitas Tahap Uji Coba

MANAJEMEN *PASSWORD*				
Sub Area	Kode	R Tabel	R hitung	Keterangan
Penggunaan *password* untuk berbagai akun..	MP1.01	0,3044	0,839	Valid
	MP1.02	0,3044	0,947	Valid
	MP1.03	0,3044	0,895	Valid
Kekuatan *password*	MP2.01	0,3044	0,928	Valid
	MP2.02	0,3044	0,945	Valid
	MP2.03	0,3044	0,881	Valid
PENGGUNAAN EMAIL				
Sub Area	Kode	R Tabel	R Hitung	Keterangan
Mengklik link dalam email.	PE1.01	0,3044	0,940	Valid
	PE1.02	0,3044	0,854	Valid
	PE1.03	0,3044	0,852	Valid
Mendownload lampiran dalam email	PE2.01	0,3044	0,940	Valid
	PE2.02	0,3044	0,853	Valid
	PE2.03	0,3044	0,852	Valid
PENGGUNAAN INTERNET				
Sub Area	Kode	R Tabel	R Hitung	Keterangan
Mendownload file dari internet.	PI1.01	0,3044	0,652	Valid
	PI1.02	0,3044	0,813	Valid
	PI1.03	0,3044	0,874	Valid
Memasukkan informasi secara online.	PI2.01	0,3044	0,714	Valid
	PI2.02	0,3044	0,759	Valid
	PI2.03	0,3044	0,752	Valid
PENGGUNAAN MEDIA SOSIAL				
Sub Area	Kode	R Tabel	R Hitung	Keterangan
	MS1.01	0,3044	0,927	Valid

Pengecekan pengaturan privasi secara berkala.	MS1.02	0,3044	0,896	Valid
	MS1.03	0,3044	0,924	Valid
Posting tentang informasi pribadi di Media Sosial.	MS2.01	0,3044	0,940	Valid
	MS2.02	0,3044	0,854	Valid
	MS2.03	0,3044	0,852	Valid
KEAMANAN PERANGKAT MOBILE				
Sub Area	Kode	R Tabel	R hitung	Keterangan
Mengirim informasi sensitif melalui jaringan publik	KPM1.01	0,3044	0,821	Valid
	KPM1.02	0,3044	0,862	Valid
	KPM1.03	0,3044	0,793	Valid
Adanya *Shoulder Surfing.*	KPM2.01	0,3044	0,826	Valid
	KPM2.02	0,3044	0,937	Valid
	KPM2.03	0,3044	0,922	Valid
PENANGANAN INFORMASI				
Sub Area	Kode	R Tabel	R Hitung	Keterangan
Membuang kertas / dokumen dengan informasi sensitif	PIF1.01	0,3044	0,799	Valid
	PIF1.02	0,3044	0,880	Valid
	PIF1.03	0,3044	0,859	Valid
PELAPORAN INSIDEN				
Sub Area	Kode	R Tabel	R Hitung	Keterangan
Melaporkan perilaku mencurigakan	PIN1.01	0,3044	0,768	Valid
	PIN1.02	0,3044	0,889	Valid
	PIN1.03	0,3044	0,828	Valid
Melaporkan perilaku buruk teman	PIN2.01	0,3044	0,704	Valid
	PIN2.02	0,3044	0,935	Valid
	PIN2.03	0,3044	0,874	Valid
MELAKUKAN *BACKUP DATA*				
Sub Area	Kode	R Tabel	R Hitung	Keterangan
Melakukan *backup data* secara berkala	BD1.01	0,3044	0,889	Valid
	BD1.02	0,3044	0,939	Valid
	BD1.03	0,3044	0,847	Valid
Media *backup data*	BD2.01	0,3044	0,784	Valid
	BD2.02	0,3044	0,814	Valid

Formatted: Left

Formatted: Left

	BD2.03	0,3044	0,782	Valid
SOCIAL ENGINEERING				
Sub Area	Kode	R Tabel	R Hitung	Keterangan
Phising	SE1.01	0,3044	0,512	Valid
	SE1.02	0,3044	0,511	Valid
	SE1.03	0,3044	0,491	Valid
Kepercayaan dengan orang lain	SE2.01	0,3044	0,485	Valid
	SE2.02	0,3044	0,525	Valid
	SE2.03	0,3044	0,402	Valid
MALWARE				
Sub Area	Kode	R Tabel	R Hitung	Keterangan
Sumber Malware	MW1.01	0,3044	0,870	Valid
	MW1.02	0,3044	0,918	Valid
	MW1.03	0,3044	0,791	Valid
Pencegahan Malware	MW2.01	0,3044	0,937	Valid
	MW2.02	0,3044	0,925	Valid
	MW2.03	0,3044	0,943	Valid

Formatted: Left

Formatted: Left

Formatted: Left

Formatted: Left

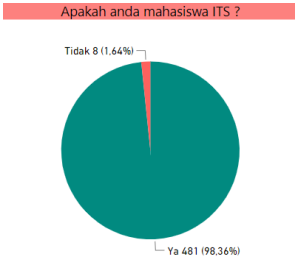
Jika kuesioner telah dinyatakan valid, maka kuesioner dapat disebarkan secara luas kepada target penelitian.

5.1.2 Tahap Penyebaran Kuesioner Sebenarnya

Setelah kuesioner dipastikan valid, maka kuesioner tersebut dapat disebarkan secara luas kepada mahasiswa ITS. Penyebaran kuesioner dilakukan secara online dan offline. Pengumpulan data secara *online* dilakukan dengan dengan menyebarkan link kuesioner online yang dapat diakses menggunakan link *bit.ly/surveyISA*. Link tersebut disebarkan melalui media sosial (LINE) dan dengan cara membagikan brosur yang berisi informasi tentang pengisian kuesioner di departemen-departemen ITS serta pasar jumat ITS. Pengumpulan data secara offline dilakukan dengan membagikan lembaran kuesioner yang dapat diisi oleh responden. Target responden keseluruhan dari penelitian ini adalah 391.

Hasil Pengumpulan Data

Penyebaran kuesioner dilakukan mulai tanggal 19 April 2019 sampai 15 Mei 2019. Total responden yang didapatkan adalah 487 orang, dengan rincian yang dapat dilihat pada gambar berikut :



Gambar 0.1 Presentase total responden yang didapatkan

Berdasarkan gambar bagan tersebut, dapat dilihat jika dari 489 responden, 8 orang bukan merupakan mahasiswa ITS, sehingga hanya 481 responden yang digunakan untuk tahap selanjutnya. Tahap selanjutnya adalah tahap pemilahan data yang valid yang didasarkan pada hasil konsistensi atau perbandingan antara pernyataan asli dengan pernyataan negasi yang telah dibuat. Hasil dari pemilahan data dapat dilihat pada tabel berikut :

Tabel 0.6 Hasil Penyebaran Kuesioner Tiap Fakultas

Fakultas	Total Responden	*Respon-den ~~yang~~ valid*	Target	*Respon rate*
Fakultas Sains (FS)	30	25	28	89,3%
Fakultas Teknologi Industri (FTI)	90	81	81	100%

Formatted Table
Formatted: Font: 10 pt
Formatted Table
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt

Fakultas	Total Responden	*Respon-den ~~yang~~ valid*	Target	*Respon rate*
Fakulas Teknologi Elektro (FTE)	34	30	31	96,8%
Fakultas Teknik Sipil, Lingkungan dan Kebumian (FTSLK)	56	47	41	100%
Fakultas Arsitektur, Desain, dan Perencanaan (FADP)	47	45	41	100%
Fakultas Teknologi Kelautan (FTK)	48	40	41	97,6%
Fakultas Matematika, Komputasu dan Sains Data (FMKSD)	32	30	23	100%
Fakultas Teknologi Informasi dan Komunikasi (FTIK)	61	56	37	100%
Fakultas Bisnis dan Manajemen Teknologi (FBMT)	18	15	11	100%
Fakultas Vokasi	64	58	57	100%

Formatted Table

Formatted: Font: 10 pt

Formatted Table

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted Table

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Formatted: Font: 10 pt

Fakultas	Total Responden	*Respon-den ~~yang~~ valid*	Target	*Respon rate*
TOTAL	481	427	391	100%

Keterangan : Respon rate = perbandingan antara responden yang dianggap valid dengan target responden

Berdasarkan hasil Tabel 5.13 dapat diketahui jika total responden yang telah valid berjumlah 427 atau 89% dari total responden yang didapatkan. Hasil responden yang telah valid tersebutlah yang dapat digunakan sebagai data untuk kebutuhan analisis data.

Hasil Uji Validitas Setelah Penyebaran Kuesioner

Uji validitas ini dilakukan untuk memastikan bahwa hasil kuesioner benar-benar dapat dipercaya sebagai alat ukur yang benar. Dalam pengujian ini diambil 100 sampel dari hasil penyebaran kuesioner. Hasil pengujian dikatakan valid apabila nilai r tabel < r hitung. Hasil pengujian dapat dilihat pada tabel-tabel berikut :

Tabel 0.7 Hasil Uji Validitas Tahap Penyebaran

MANAJEMEN *PASSWORD*				
Sub Area	Kode	R Tabel	R hitung	Keterangan
Penggunaan *password* yang media sosial dan akun perkuliahan.	MP1.01	0.1638	0,770	Valid
	MP1.02	0.1638	0,899	Valid
	MP1.03	0.1638	0,900	Valid
Membuat *password* yang aman.	MP2.01	0.1638	0,877	Valid
	MP2.02	0.1638	0,922	Valid
	MP2.03	0.1638	0,786	Valid
PENGGUNAAN EMAIL				

Formatted Table
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Font: 10 pt
Formatted: Indent: Left: 0 cm, Hanging: 2,25 cm, Space Before: 12 pt
Formatted: Normal, Left, No bullets or numbering

Sub Area	Kode	R Tabel	R Hitung	Keterangan
Mengklik link dari email yang tidak dikenal.	PE1.01	0.1638	0,753	Valid
	PE1.02	0.1638	0,815	Valid
	PE1.03	0.1638	0,819	Valid
Mendownload lampiran dari email yang tidak dikenal.	PE2.01	0.1638	0,707	Valid
	PE2.02	0.1638	0,813	Valid
	PE2.03	0.1638	0,869	Valid
PENGGUNAAN INTERNET				
Sub Area	Kode	R Tabel	R Hitung	Keterangan
Mendownload file dari internet.	PI1.01	0.1638	0,710	Valid
	PI1.02	0.1638	0,355	Valid
	PI1.03	0.1638	0,516	Valid
Memasukkan informasi secara online.	PI2.01	0.1638	0,715	Valid
	PI2.02	0.1638	0,786	Valid
	PI2.03	0.1638	0,766	Valid
PENGGUNAAN MEDIA SOSIAL				
Sub Area	Kode	R Tabel	R Hitung	Keterangan
Pengecekan pengaturan privasi secara berkala.	MS1.01	0.1638	0,873	Valid
	MS1.02	0.1638	0,877	Valid
	MS1.03	0.1638	0,849	Valid
Posting tentang informasi pribadi di Media Sosial.	MS2.01	0.1638	0,803	Valid
	MS2.02	0.1638	0,868	Valid
	MS2.03	0.1638	0,775	Valid
KEAMANAN PERANGKAT MOBILE				
Sub Area	Kode	R Tabel	R hitung	Keterangan
Mengirim informasi sensitif melalui jaringan publik	KPM1.01	0.1638	0,713	Valid
	KPM1.02	0.1638	0,792	Valid
	KPM1.03	0.1638	0,794	Valid
Adanya *Shoulder Surfing*.	KPM2.01	0.1638	0,777	Valid
	KPM2.02	0.1638	0,887	Valid
	KPM2.03	0.1638	0,881	Valid
PENANGANAN INFORMASI				
Sub Area	Kode	R Tabel	R Hitung	Keterangan

Membuang kertas / dokumen dengan informasi sensitif	PIF1.01	0.1638	0,776	Valid
	PIF1.02	0.1638	0,797	Valid
	PIF1.03	0.1638	0,756	Valid
Memasukkan media yang ditemukan tanpa sengaja.	PIF2.01	0.1638	0,566	Valid
	PIF2.02	0.1638	0,845	Valid
	PIF2.03	0.1638	0,88	Valid
PELAPORAN INSIDEN				
Sub Area	Kode	R Tabel	R Hitung	Keterangan
Melaporkan perilaku mencurigakan	PIN1.01	0.1638	0,870	Valid
	PIN1.02	0.1638	0,899	Valid
	PIN1.03	0.1638	0,847	Valid
Melaporkan perilaku buruk teman	PIN2.01	0.1638	0,715	Valid
	PIN2.02	0.1638	0,777	Valid
	PIN2.03	0.1638	0,828	Valid
MELAKUKAN *BACKUP DATA*				
Sub Area	Kode	R Tabel	R Hitung	Keterangan
Melakukan *backup data* secara berkala	BD1.01	0.1638	0,833	Valid
	BD1.02	0.1638	0,784	Valid
	BD1.03	0.1638	0,806	Valid
Media *backup data*	BD2.01	0.1638	0,758	Valid
	BD2.02	0.1638	0,798	Valid
	BD2.03	0.1638	0,700	Valid
SOCIAL ENGINEERING				
Sub Area	Kode	R Tabel	R Hitung	Keterangan
Phising	SE1.01	0.1638	0,420	Valid
	SE1.02	0.1638	0,909	Valid
	SE1.03	0.1638	0,907	Valid
Kepercayaan dengan orang lain	SE2.01	0.1638	0,848	Valid
	SE2.02	0.1638	0,840	Valid
	SE2.03	0.1638	0,829	Valid
MALWARE				
Sub Area	Kode	R Tabel	R Hitung	Keterangan
Sumber Malware	MW1.01	0.1638	0,531	Valid

Formatted: Left

Formatted: Left

Formatted: Left

Formatted: Left

Formatted Table

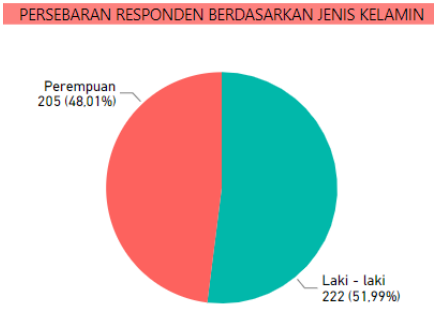
Formatted: Left

	MW1.02	0.1638	0,728	Valid
	MW1.03	0.1638	0,728	Valid
Pencegahan Malware	MW2.01	0.1638	0,722	Valid
	MW2.02	0.1638	0,812	Valid
	MW2.03	0.1638	0,813	Valid

Formatted: Left

5.3. Analisis Deskriptif Statistik

5.3.1. Persebaran Responden Berdasarkan Jenis Kelamin



Gambar 0.2 Persebaran responden berdasarkan jenis kelamin

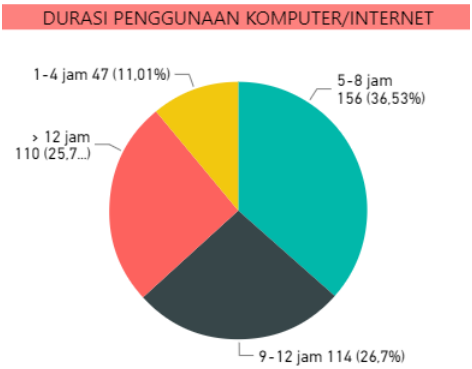
Berdasarkan data di atas, hasil dari penyebaran kuesioner kepada mahasiswa S1 ITS memperlihatkan jika responden laki-laki lebih besar daripada perempuan, dengan proporsi sebagai berikut :

Tabel 0.8 Jumlah responden berdasarkan jenis kelamin

Jenis Kelamin	Jumlah Responden	Rate
Laki-laki	222	52 %
Perempuan	205	48%

Hasil proporsi menunjukkan perbedaan yang sedikit, yaitu sekitar 4%. Hal tersebut dapat disimpulkan jika persebaran untuk jenis kelamin cukup merata karena selisih yang sedikit.

5.3.2 Persebaran Responden Berdasarkan Durasi Penggunaan Komputer atau Internet



Gambar 0.3 Persebaran responden berdasarkan durasi penggunaan komputer dan internet

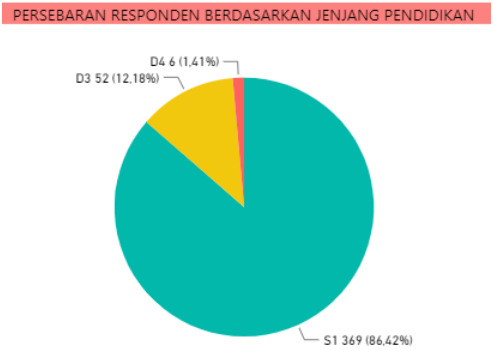
Berdasarkan gambar diatas, didapatkan bahwa mahasiswa ITS rata-rata menggunakan komputer atau internet di atas 4 jam dengan proporsi tertinggi pada penggunaan antara 5 sampai 8 jam. Proporsi lengkapnya dapat dilihat pada tabel berikut :

Tabel 0.9 Jumlah responden berdasarkan durasi penggunaan komputer/internet

Durasi	Jumlah Responden	Rate
1-4 jam	47	11%
5-8 jam	156	36,54%
9-12 jam	114	26,70%

>12 jam	110	25,76%

5.3.3 Persebaran Responden Berdasarkan Jenjang Pendidikan



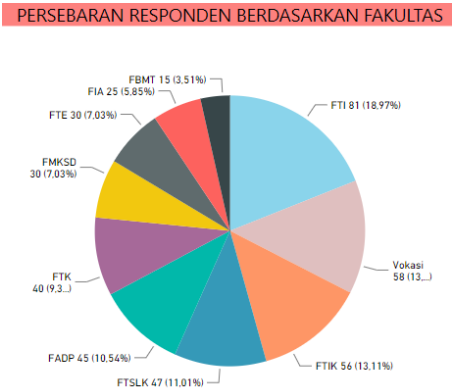
Gambar 0.4 Persebaran responden berdasarkan jenjang pendidikan

Berdasarkan bagan di atas, dapat dilihat jika responden terbanyak adalah mahasiswa S1 karena memang proporsi jumlah mahasiswa ITS yang terbanyak adalah mahasiswa S1. Berikut merupakan proporsi persebarannya :

Tabel 5. 1 Jumlah responden berdasarkan jenjang pendidikan.

Jenjang pendidikan	Jumlah Responden	Rate
D3	52	12,24%
D4	6	1,41%
S1	367	86,35%

5.3.4 Persebaran Responden Berdasarkan Fakultas



Gambar 0.5 Persebaran responden berdasarkan fakultas

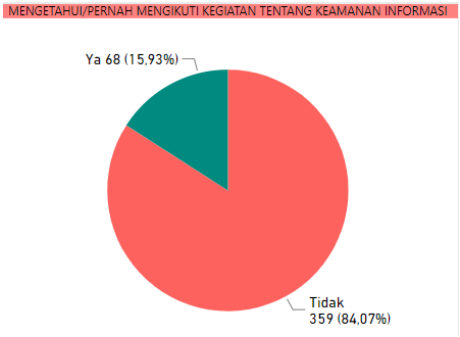
Berdasarkan bagan di atas dapat diketahui proporsi persebaran responden di setiap fakultas di ITS dan dihasilkan responden paling banyak ada pada Fakultas Teknologi Industri (FTI) sebesar 18,82% karena memang jumlah mahasiswa FTI adalah yang paling tinggi. Berikut rincian persebaran responden berdasarkan fakultas.

Tabel 0.10 Jumlah responden berdasarkan fakultas.

Fakultas	Jumlah Responden	*Rate*
Fakultas Sains / Fakultas Ilmu Alam (FIAS)	25	5,86%
Fakultas Teknologi Industri (FTI)	81	18,97 %
Fakulas Teknologi Elektro (FTE)	30	7,02%

Fakultas Teknik Sipil, Lingkungan dan Kebumian (FTSLK)	47	11,00%
Fakultas Arsitektur, Desain, dan Perencanaan (FADP)	45	10,54%
Fakultas Teknologi Kelautan (FTK)	40	9,37%
Fakultas Matematika, Komputasu dan Sains Data (FMKSD)	30	7,03%
Fakultas Teknologi Informasi dan Komunikasi (FTIK)	56	13,12%
Fakultas Bisnis dan Manajemen Teknologi (FBMT)	15	3,51%
Fakultas Vokasi	58	13,58%

5.3.5 Persebaran Responden yang Mengetahui atau Pernah Mengikuti Kegiatan Mengenai Keamanan Informasi



Gambar 0.6 Persebaran responden mengenai kegiatan kesadaran keamanan informasi

Berdasarkan bagan di atas, dapat dilihat jika mahasiswa ITS banyak yang belum pernah mengikuti atau mengetahui kegiatan mengenai keamanan informasi dengan presentase sebesar 16%. Rincian proporsi responden dapat dilihat pada tabel berikut :

Tabel 0.11 Jumlah responden berdasarkan pengetahuan tentang kegiatan mengenai keamanan informasi.

Pernah mengikuti/mengetahui	Jumlah Responden	Rate
Ya	68	16%
Tidak	359	84%

5.3.6 Analisis Statistik Deskriptif Berdasarkan Variabel Penelitian

Analisis statistik deskriptif berdasarkan variabel penelitian dilakukan untuk mengetahui distribusi jawaban responden dalam menjawab item pernyataan kuesioner. Sebelum dilakukan analisis statistik, terlebih dahulu menentukan interval kelas. Interval kelas bertujuan untuk memudahkan dalam menentukan kategori hasil data yang didapatkan. Berikut adalah rumus untuk menentukan interval kelas :

$$\text{Interval} = \frac{Nilai\ Tertinggi - Nilai\ Terendah}{Jumlah\ Kelas}$$

Berdasarkan rumus di atas, maka hasil perhitungannya adalah sebagai berikut :

$$\text{Interval} = \frac{5-1}{5} = 0{,}8$$

Selanjutnya menentukan kategori interval berdasarkan perhitungan interval, sebagai berikut :

Tabel 0.12 Range nilai (interval) skala linkert

Rata – rata interval kelas	Kategori
$1{,}0 \leq x \leq 1{,}8$	Sangat tidak setuju
$1{,}8 \leq x \leq 2{,}6$	Tidak setuju
$2{,}6 \leq x \leq 3{,}4$	Netral
$3{,}4 \leq x \leq 4{,}2$	Setuju
$4{,}2 \leq x \leq 5{,}0$	Sangat setuju

Tabel di atas berfungsi sebagai acuan dalam memberikan penilaian untuk distribusi jawaban responden dalam penelitian. Analisis ststistik deskriptif yang dipakai dalam penelitian ini adalah mean, median, modus, dan standar deviasi yang diolah menggunakan *software* SPSS . *Mean* adalah ukuran rata-rata yang merupakan hasil dari jumlah semua nilai pengukuran yang dibagi oleh banyaknya pengukuran. Median adalah salah satu teknik yang didasarkan atas nilai tengah dari suatu kelompok data. Standar deviasi berfungsi untuk mengukur seberapa baik mean mewakili data. Dari hasil analisis deskriptif digunakan untuk mengetahuai bagaimana hasil dari persebaran data kuesioner. Analisis dilakukan tiap area dari keamanan informasi. Berikut hasil analisis statistik deskriptif berdasarkan tiap variabel dan item-item pernyataan :

Tabel 0.13 Hasil analisis statistik deskriptif

Area	Sub Area	Kode	Mean	Skala Penilaian	Modus	Median	Standard Deviasi	Variance
Manajemen *Password*	Penggunaan *password* yang media sosial dan akun perkuliahan	MP1.01	3,15	Netral	3	3,00	1,248	1,557
		MP1.02	3,47	Setuju	4	4,00	1,340	1,794
		MP1.03	3,30	Netral	4	4,00	1,299	1,688
	Kekuatan *password*	MP2.01	3,33	Netral	5	3,00	1,382	1,909
		MP2.02	3,00	Netral	5	3,00	1,500	2,251
		MP2.03	3,16	Netral	4	3,00	1,284	1,649
Penggunaan E-mail	Mengklik link dari email yang tidak dikenal.	PE1.01	4,13	Setuju	5	4,00	0,963	0,926
		PE1.02	4,02	Setuju	5	4,00	1,075	1,115
		PE1.03	4,19	Setuju	5	4,00	0,865	0,749
	Mendownload lampiran dari email yang tidak dikenal.	PE2.01	3,93	Setuju	4	4,00	0,937	0,878
		PE2.02	4,02	Setuju	5	4,00	1,042	1,086
		PE2.03	4,11	Setuju	5	4,00	0,919	0,845
	Mendownload file dari internet.	PI1.01	3,78	Setuju	4	4,00	1,038	1,077
		PI1.02	3,98	Setuju	4	4,00	0,992	0,983

Area	Sub Area	Kode	Mean	Skala Penilaian	Modus	Median	Standard Deviasi	Variance
Penggunaan Internet		PI1.03	3,04	Netral	3	3,00	1,099	1,207
	Memasukkan informasi secara online.	PI2.01	2,15	Tidak Setuju	2	2,00	0,974	0,949
		PI2.02	3,72	Setuju	4	4,00	0,963	0,927
		PI2.03	4,04	Setuju	4	4,00	0,907	0,823
Penggunaan Media Sosial	Pengecekan pengaturan privasi secara berkala.	MS1.01	3,73	Setuju	4	4,00	1,075	1,155
		MS1.02	3,28	Netral	3	3,00	1,153	1,330
		MS1.03	3,06	Netral	4	4,00	0,949	0,901
	Posting tentang informasi pribadi di Media Sosial.	MS2.01	4,01	Setuju	5	4,00	0,949	0,901
		MS2.02	2,48	Tidak Setuju	2	2,00	1,051	1,105
		MS2.03	3,83	Setuju	4	4,00	0,985	0,970
Keamanan Perangkat Mobile	Mengirim informasi sensitif melalui jaringan publik.	KPM.1.01	2,67	Netral	2	3,00	1,074	1,153
		KPM1.02	2,94	Netral	3	3,00	1,161	1,348
		KPM.1.03	2,74	Netral	2	3,00	1,136	1,290
		KPM2.01	4,13	Setuju	4	4,00	0,860	0,740

Area	Sub Area	Kode	Mean	Skala Penilaian	Modus	Median	Standard Deviasi	Variance
	Adanya *Shoulder Surfing*.	KPM2.02	4,04	Setuju	5	4,00	0,973	0,947
		KPM2.03	4,13	Setuju	5	4,00	0,911	0,831
Penanganan Informasi	Membuang kertas / dokumen dengan informasi sensitif.	PIF1.01	4,07	Setuju	5	4,00	0,936	0,876
		PIF1.02	4,05	Setuju	5	4,00	0,981	0,962
		PIF1.03	2,37	Tidak Setuju	2	2,00	1,145	1,310
	Memasuk-kan media yang ditemukan tanpa sengaja.	PIF2.01	4,10	Setuju	4	4,00	0,876	0,768
		PIF2.02	2,85	Netral	2	3,00	1,208	1,459
		PIF2.03	2,62	Netral	2	3,00	1,110	1,231
Pelaporan Insiden	Melapor-kan perilaku mencurigakan.	PIN1.01	3,84	Setuju	4	4,00	0,907	0,823
		PIN1.02	3,79	Setuju	4	4,00	0,923	0,852
		PIN1.03	2,37	Tidak Setuju	2	2,00	1,029	1,059

Area	Sub Area	Kode	Mean	Skala Penilaian	Modus	Median	Standard Deviasi	Variance
	Melapor-kan perilaku buruk teman.	PIN2.01	3,92	Netral	4	4,00	0,807	0,651
		PIN2.02	2,40	Tidak Setuju	2	2,00	1,051	1,104
		PIN2.03	2,46	Tidak Setuju	2	2,00	1,016	1,033
Backup data	Melakukan *backup data* secara ~~regular~~berkala	BD1.01	3,87	Setuju	5	4,00	1,067	1,139
		BD1.02	3,68	Setuju	4	4,00	1,186	1,407
		BD1.03	3,77	Setuju	4	4,00	1,073	1,152
	Media *backup data*	BD2.01	3,37	Netral	4	3,00	1,125	1,267
		BD2.02	3,16	Netral	4	3,00	1,206	1,453
		BD2.03	3,09	Netral	3	3,00	1,157	1,339
Social engineering	*Phising*	SE1.01	3,89	Setuju	4	4,00	0,902	0,814
		SE1.02	2,74	Netral	3	3,00	1,148	1,317

Area	Sub Area	Kode	Mean	Skala Penilaian	Modus	Median	Standard Deviasi	Variance
		SE1.03	2,82	Netral	3	3,00	1,163	1,352
	Kepercayaan dengan orang lain	SE2.01	4,28	Sangat Setuju	5	4,00	0,834	0,695
		SE2.02	4,02	Setuju	4	4,00	0,911	0,830
		SE2.03	4,23	Sangat Setuju	5	4,00	0,806	0,649
Malware	Sumber Malware	MW1.01	3,79	Setuju	4	4,00	0,928	0,862
		MW1.02	2,48	Tidak Setuju	2	2,00	1,245	1,551
		MW1.03	2,35	Tidak Setuju	2	2,00	1,170	1,369
	Pencegahan Malware	MW2.01	4,04	Setuju	4	4,00	0,963	0,928
		MW2.02	3,37	Netral	3	3,00	1,131	1,280
		MW2.03	3,73	Setuju	5	4,00	1,166	1,360

5.2. Penghitungan Frekuensi Jawaban Tiap Item Pernyataan

Setelah data sudah dianggap valid, maka data tersebut dapat dilanjutkan pada pembuatan tabel frekuensi jawaban responden untuk tiap kategori jawaban di setiap item pernyataan. Tabel ini yang nantinya dapat digunakan untuk pengolahan data sehingga dapat diketahui nilai presentase untuk tiap area keamanan informasi dan dimensi kesadaran keamanan informasi. Berikut merupakan tabel frekuensi jawaban untuk tiap item pernyataan.

Tabel 0.14 Tabel frekuensi jawaban tiap item pernyataan

Area	Sub Area	Kode	Frekuensi	
Manajemen *Password*	Penggunaan *password* yang media sosial dan akun perkuliahan	MP1.01	1	39
			2	107
			3	111
			4	90
			5	80
		MP1.02	1	44
			2	78
			3	56
			4	130
			5	119
		MP1.03	1	47
			2	87
			3	72
			4	134
			5	87
	Kekuatan *password*	MP2.01	1	50
			2	89
			3	76
			4	92
			5	120
		MP2.02	1	94
			2	94
			3	59

Area	Sub Area	Kode	Frekuensi	
			4	77
			5	103
		MP2.03	1	55
			2	92
			3	77
			4	137
			5	66
Penggunaan E-mail	Mendownload file dari internet.	PI1.01	1	6
			2	50
			3	100
			4	146
			5	125
		PI1.02	1	14
			2	19
			3	73
			4	177
			5	144
		PI1.03	1	35
			2	105
			3	134
			4	114
			5	39
	Memasukkan informasi secara online.	PI2.01	1	115
			2	182
			3	92
			4	27
			5	11
		PI2.02	1	4
			2	30
			3	88
			4	173
			5	132
		PI2.03	1	3
			2	24
			3	78

Area	Sub Area	Kode	Frekuensi	
			4	172
			5	150
Keamanan Perangkat Mobile	Pengecekan pengaturan privasi secara berkala.	MS1.01	1	7
			2	57
			3	106
			4	131
			5	126
		MS1.02	1	22
			2	98
			3	120
			4	111
			5	76
		MS1.03	1	31
			2	106
			3	128
			4	129
			5	33
	Posting tentang informasi pribadi di Media Sosial.	MS2.01	1	3
			2	28
			3	88
			4	151
			5	157
		MS2.02	1	80
			2	152
			3	117
			4	66
			5	12
		MS2.03	1	4
			2	42
			3	100
			4	159
			5	122
Penanganan Informasi	Membuang kertas / dokumen dengan	PIF1.01	1	4
			2	23
			3	80

Area	Sub Area	Kode	Frekuensi	
	informasi sensitif.		4	153
			5	167
		PIF1.02	1	4
			2	35
			3	66
			4	153
			5	169
		PIF1.03	1	106
			2	156
			3	86
			4	57
			5	22
	Memasukkan media yang ditemukan tanpa sengaja.	PIF2.01	1	4
			2	19
			3	64
			4	185
			5	155
		PIF2.02	1	64
			2	116
			3	105
			4	103
			5	39
		PIF2.03	1	76
			2	128
			3	123
			4	82
			5	18
Pelaporan Insiden	Melaporkan perilaku mencurigakan.	PIN1.01	1	4
			2	27
			3	109
			4	179
			5	108
		PIN1.02	1	4
			2	27
			3	131

91

Area	Sub Area	Kode	Frekuensi	
			4	158
			5	107
		PIN1.03	1	88
			2	167
			3	116
			4	40
			5	16
	Melaporkan perilaku buruk teman.	PIN2.01	1	2
			2	16
			3	97
			4	211
			5	101
		PIN2.02	1	77
			2	186
			3	105
			4	35
			5	24
		PIN2.03	1	64
			2	186
			3	112
			4	46
			5	19
Backup data	Melaporkan perilaku mencurigakan.	BD1.01	1	8
			2	46
			3	89
			4	136
			5	148
		BD1.02	1	18
			2	70
			3	73
			4	137
			5	129
		BD1.03	1	10
			2	54
			3	85

Area	Sub Area	Kode	Frekuensi	
			4	155
			5	123
	Melaporkan perilaku buruk teman.	BD2.01	1	2
			2	16
			3	97
			4	211
			5	101
		BD2.02	1	77
			2	186
			3	105
			4	35
			5	24
		BD2.03	1	64
			2	186
			3	112
			4	46
			5	19
Social engineering	Melaporkan perilaku mencurigakan.	SE1.01	1	3
			2	22
			3	116
			4	165
			5	121
		SE1.02	1	73
			2	106
			3	129
			4	95
			5	24
		SE1.03	1	66
			2	109
			3	116
			4	109
			5	27
	Melaporkan perilaku buruk teman.	SE2.01	1	2
			2	15
			3	48

93

Area	Sub Area	Kode	Frekuensi	
			4	158
			5	204
		SE2.02	1	5
			2	16
			3	94
			4	161
			5	151
		SE2.03	1	2
			2	10
			3	58
			4	173
			5	184
Malware	Melaporkan perilaku mencurigakan.	MW1.01	1	5
			2	29
			3	121
			4	168
			5	104
		MW1.02	1	112
			2	136
			3	70
			4	81
			5	28
		MW1.03	1	124
			2	134
			3	78
			4	77
			5	14
	Melaporkan perilaku buruk teman.	MW2.01	1	10
			2	18
			3	76
			4	165
			5	158
		MW2.02	1	23
			2	73
			3	136

Area	Sub Area	Kode	Frekuensi	
			4	114
			5	81
		MW2.03	1	22
			2	41
			3	107
			4	116
			5	141

5.4. Pengelompokan Media Penyampaian

Pada bab 2 (2.2.5 dan 2.2.6) telah dilakukan studi literatur terkait media penyampaian yang akan digunakan sebagai media komunikasi pelaksanaan kegiatan peningkatan kesadaran keamanan informasi. Sebelumnya akan dilakukan kategorisasi antara metode penyampaian dan dimensi kesadaran keamanan informasi yang dapat dilihat pada tabel berikut:

Tabel 0.15 Kategorisasi metode penyampaian berdasarkan dimensi [36]

Metode penyamapaian	Dimensi Kesadaran Keamanan Informasi		
	Knowledge Strategy	Attitude Strategy	Behavioral Strategy
Educational Interactive (Edukasi Interaktif)	v	v	v
Informational (Media Informasi)	v	v	
Promotional (Promosi)	v	v	
Enforcing (Pendorong/ Pemaksaan)		v	v

Selanjutnya dapat dilakukan pengelompokan media penyampaian program menurut metode dan dimensi kesadaran

keamanan informasi. Media penyampaian program diambil berdasarkan NIST 800-50 dan ISACA 2005.Berikut merupakan *check list* pengelompokan media penyampaian berdasarkan studi literatur yang telah dilakukan oleh peneliti

Tabel 0.16 Checklist Media Penyampaian Kegiatan dengan Dimensi Pengukuran

No	Media Penyampaian (Berdasarkan NIST 800-50)	Kategori Metode	Dimensi		
			K	A	B
1	Awareness Tools (contoh : pulpen, post-it,buku catatan,dsb)	*Promotional*		V	
2	Poster / Infografis	*Promotional*	V	V	
3	Screensaver dan spanduk	*Promotional*	V	V	
4	Newsletters / E-Newsletters	*Informational*	V	V	
5	Email	*Informational*	V	V	
6	Video	*Educational Interactive*	V	V	V
7	Metode berbasis web	*Informational*	V	V	
8	Metode berbasis komputer	*Informational*	V	V	
9	Metode telekoferensi	*Educational Interactive*	V	V	
10	Workshop	*Educational Interactive*	V	V	V

11	Acara peringatan hari keamanan atau acara serupa lainnya.	*Promotional*	V	V	
12	Seminar	*Educational Interactive*	V		
13	Permaianan	*Educational Interactive*		V	
14	Program Penghargaan	*Enforcing*			V
15.	Artikel	*Informational*	V	V	
16.	Tips tiap bulan	*Informational*	V	V	
17.	*Security flash cards (*risiko, ancaman*)*	*Informational*	V	V	
18.	Memberikan tindakan jika terdapat pelanggaran	*Enforcing*			V
19.	Perjanjian/ Peraturan	*Enforcing*			V
20.	Ujian	*Enforcing*			V
21.	Panduan keamanan informasi.	*Enforcing*			V

Keterangan : K = *Knowledge*
A = *Attitude*
B = *Behavior*

5.5. Hambatan

Dalam melakukan implementasi perancangan terdapat beberapa hambatan yang dilalui peneliti, antara lain :

1. Instrumen kuesioner adalah hasil translasi yang menggunakan bahasa Inggris, maka dari itu peneliti melakukan translasi ke dalam bahasa Indonesia. Kesulitan pada saat melakukan translasi adalah memilih penggunaan kata yang tepat agar dapat dipahami oleh responden.
2. Saat melakukan uji validitas kuesioner membutuhkan waktu cukup lama karena dilakukan beberapa kali sampai kuesioner dinyatakan valid.
3. Jumlah pernyataan pada kuesioner yang tergolong banyak, sehingga memerlukan cara untuk membujuk responden agar mau mengisi kuesioner. Tak luput pula pada saat peneliti membagikan kuesioner para responden menolak dengan alasan ada kesibukan lain.
4. Saat pengisian kuesioner ditemukan responden yang menjawab tidak tepat (tidak konsisten) sehingga cukup banyak kuesioner yang tidak digunakan.

BAB VI.
HASIL DAN PEMBAHASAN

Pada bab VI ini akan dijelaskan mengenai hasil dan pembahasan terkait penelitian tugas akhir, yaitu keluaran dari setiap tahapan dalam metode penelitian yang telah dijelaskan dalam bab III.

6.1. Identifikasi Kebutuhan

6.1.1. Identifikasi Topik Usulan Rekomendasi

Sebelum usulan rekomendasi dirancang, hal pertama yang perlu diketahui adalah topik yang sesuai dengan kebutuhan target agar usulan rekomendasi yang dibuat nantinya sesuai dengan apa yang dibutuhkan target untuk meningkatkan kesadaran keamanan informasi. Untuk mendapatkan topik telah dibuat berdasarkan area keamanan informasi menurut Arfive Gandhie dan Hazasanzadeh et al. Dari sepuluh area keamanan informasi yang telah dipilih akan dikategorikan lagi berdasarkan tiga dimensi kesadaran keamanan informasi yaitu pengetahuan, sikap, dan perilaku target terhadap masing-masing area keamanan informasi.

Perhitungan untuk mendapatkan nilai kesadaran dilakukan berdasarkan metode deskriptif statistik presentase yang diperkenalkan oleh Muhammad Ali dalam thesis Ali Akbar Fahrani. Tiap item pernyataan akan dilakukan perhitungan berdasarkan bobot tiap jawaban seperti yang telah ditampilkan pada Tabel 3.3. Selanjutnya total skor untuk seluruh jawaban dari tiap item dijumlahkan dan kemudian dibandingkan dengan skor ideal, yaitu skor yang diharapkan yaitu total responden dikalikan dengan bobot tertinggi, yaitu 427 x 5 dan didapatkan sebesar 2135. Dari perbandingan total skor dan total iskor ideal tersebut maka didapatkan hasil presentase.

Berikut merupakan hasil penghitungan nilai presentase kesadaran keamanan informasi :

Tabel 0.1 Hasil tingkat kesadaran keamanan informasi area manajemen password

AREA : MANAJEMEN *PASSWORD*										
Dimensi	Kode	Kategori Pernyata-an	SS	S	N	TS	STS	Skor Total	Skor Ideal	Presen-tase
Knowledge (Pengetahuan)	MP1.01	Positif	80*5	90*4	111*3	107*2	39*1	1346	2135	63,04%
			400	360	333	214	39			
	MP2.01	Positif	120*5	92*4	76*3	89*2	50*1	1424	2135	67%
			600	368	228	178	50			
	Hasil Presentase Skor Total Dimensi *Knowledge*									65%
Behavior (Perilaku)	MP1.02	Negatif	119*1	130*2	56*3	78*4	44*5	1079	2135	51%
			119	260	168	312	220			
	MP2.02	Positif	103*5	77*4	59*3	94*2	94*1	1282	2135	60%
			515	308	177	188	94			
	Hasil Presentase Skor Total Dimensi *Behavior*									55%
Attitude (Sikap)	MP1.03	Negatif	87*1	134*2	72*3	87*4	47*5	1154	2135	54%
			87	268	216	348	235			
	MP2.03	Negatif	66*1	137*2	77*3	92*4	55*5	1214	2135	57%
			66	274	231	368	275			
HASIL PRESENTASE SKOR TOTAL AREA MANAJEMEN *PASSWORD*									59%	

Tabel 0.2 Hasil tingkat kesadaran keamanan informasi area penggunaan email.

AREA : PENGGUNAAN EMAIL										
Dimensi	Kode	Kategori Pernyata-an	SS	S	N	TS	STS	Skor Total	Skor Ideal (427*5)	Presen-tase
Knowledge (Pengeta-huan)	PE1.01	Positif	184*5	153*4	59*3	24*2	7*1	1764	2135	82,62%
			920	612	177	48	7			
	PE2.01	Positif	132*5	173*4	88*3	30*2	4*1	1680	2135	79%
			660	692	264	60	4			
	Hasil Presentase Skor Total Dimensi *Knowledge*									81%
Behavior (Perilaku)	PE1.02	Positif	186*5	120*4	71*3	43*2	7*1	1716	2135	80%
			930	480	213	86	7			
	PE2.02	Positif	132*5	173*4	88*3	30*2	4*1	1680	2135	79%
			660	692	264	60	4			
	Hasil Presentase Skor Total Dimensi *Behavior*									79,5%
Attitude (Sikap)	PE1.03	Positif	189*5	152*4	66*3	20*2	0*1	1791	2135	84%
			945	608	198	40	0			
	PE2.03	Positif	174*5	154*4	75*3	20*2	4*1	1755	2135	82%
			870	616	225	40	4			
	Hasil Presentase Skor Total Dimensi *Attitude*									83%
HASIL PRESENTASE SKOR TOTAL AREA PENGGUNAAN EMAIL									81%	

Tabel 0.3 Hasil tingkat kesadaran keamanan informasi area penggunaan internet

AREA : PENGGUNAAN INTERNET										
Dimensi	Kode	Kategori Pernyata-an	SS	S	N	TS	STS	Skor Total	Skor Ideal (427*5)	Presen-tase
Knowledge (Pengeta-huan)	PI1.01	Positif	125*5	146*4	100*3	50*2	6*1	1615	2135	75,64%
			625	584	300	100	6			
	PI2.01	Negatif	11*1	27*2	92*3	182*4	115*5	1644	2135	77%
			11	54	276	728	575			
	Hasil Presentase Skor Total Dimensi *Knowledge*									76%
Behavior (Perilaku)	PI1.02	Negatif	144*1	177*2	73*3	19*4	14*5	863	2135	40%
			144	354	219	76	70			
	PI2.02	Positif	93*5	175*4	110*3	43*2	6*1	1587	2135	74%
			465	700	330	86	6			
	Hasil Presentase Skor Total Dimensi *Behavior*									57%
Attitude (Sikap)	PI1.03	Negatif	39*1	114*2	134*3	105*4	35*5	1264	2135	59%
			39	228	402	420	175			
	PI2.03	Positif	150*5	172*4	78*3	24*2	3*1	1723	2135	81%
			750	688	234	48	3			
	Hasil Presentase Skor Total Dimensi *Attitude*									70%
HASIL PRESENTASE SKOR TOTAL AREA PENGGUNAAN INTERNET									68%	

Tabel 0.4 Hasil tingkat kesadaran keamanan informasi area penggunaan media sosial

AREA : PENGGUNAAN MEDIA SOSIAL										
Dimensi	Kode	Kategori Pernyata-an	SS	S	N	TS	STS	Skor Total	Skor Ideal (427*5)	Presentase
Knowledge (Pengeta-huan)	MS1.01	Positif	126*5	131*4	106*3	57*2	7*1	1593	2135	74,61%
			630	524	318	114	7			
	MS2.01	Positif	157*5	151*4	88*3	28*2	3*1	1712	2135	80%
			785	604	264	56	3			
	Hasil Presentase Skor Total Dimensi *Knowledge*									77%
Behavior (Perilaku)	MS1.02	Positif	76*5	111*4	120*3	98*2	22*1	1402	2135	66%
			380	444	360	196	22			
	MS2.02	Negatif	12*1	66*2	117*3	152*4	80*5	1503	2135	70%
			12	132	351	608	400			
	Hasil Presentase Skor Total Dimensi *Behavior*									68%
Attitude (Sikap)	MS1.03	Negatif	33*1	129*2	128*3	106*4	31*5	1254	2135	59%
			33	258	384	424	155			
	MS2.03	Positif	122*5	159*4	100*3	42*2	4*1	1634	2135	77%
			610	636	300	84	4			
	Hasil Presentase Skor Total Dimensi *Attitude*									68%
HASIL PRESENTASE SKOR TOTAL AREA PENGGUNAAN MEDIA SOSIAL									71%	

Tabel 0.5 Hasil tingkat kesadaran keamanan informasi area keamanan perangkat desktop

AREA : KEAMANAN PERANGKAT MOBILE (DESKTOP DAN HANDPHONE)										
Dimensi	Kode	Kategori Pernyata-an	SS	S	N	TS	STS	Skor Total	Skor Ideal (427*5)	Presen-tase
Knowledge (Pengeta-huan)	KPM1.01	Negatif	24*1	70*2	128*3	149*4	56*5	1424	2135	66,70%
			24	140	384	596	280			
	KPM2.01	Positif	165*5	176*4	67*3	16*2	3*1	1765	2135	83%
			825	704	201	32	3			
	Hasil Presentase Skor Total Dimensi *Knowledge*									75%
Behavior (Perilaku)	KPM1.02	Negatif	36*1	112*2	124*3	100*4	55*5	1307	2135	61%
			36	224	372	400	275			
	KPM2.02	Positif	163*5	154*4	83*3	17*2	10*1	1724	2135	81%
			815	616	249	34	10			
	Hasil Presentase Skor Total Dimensi *Behavior*									71%
Attitude (Sikap)	KPM1.03	Negatif	26*1	91*2	122*3	123*4	65*5	1391	2135	65%
			26	182	366	492	325			
	KPM2.03	Positif	177*5	155*4	72*3	19*2	4*1	1763	2135	83%
			885	620	216	38	4			
	Hasil Presentase Skor Total Dimensi *Attitude*									74%
HASIL PRESENTASE SKOR TOTAL AREA KEAMANAN PERANGKAT MOBILE									73%	

Tabel 0.6 Hasil tingkat kesadaran keamanan informasi area penanganan informasi

AREA : PENANGANAN INFORMASI										
Dimensi	Kode	Kategori Pernyata-an	SS	S	N	TS	STS	Skor Total	Skor Ideal (427*5)	Presentase
Knowledge (Pengeta-huan)	PIF1.01	Positif	167*5	153*4	80*3	23*2	4*1	1738	2135	81,41%
			835	612	240	46	5			
	PIF2.01	Positif	155*5	185*4	64*3	19*2	4*1	1752	2135	82%
			775	740	195	38	4			
	Hasil Presentase Skor Total Dimensi *Knowledge*									82%
Behavior (Perilaku)	PIF1.02	Positif	169*5	153*4	66*3	35*2	4*1	1729	2135	81%
			845	612	198	70	4			
	PIF2.02	Negatif	39*1	103*2	105*3	116*4	64*5	1340	2135	63%
			40	206	315	464	315			
	Hasil Presentase Skor Total Dimensi *Behavior*									72%
Attitude (Sikap)	PIF1.03	Negatif	22*1	57*2	86*3	156*4	106*5	1548	2135	73%
			22	114	258	624	530			
	PIF2.03	Negatif	18*1	82*2	123*3	128*4	76*5	1443	2135	68%
			18	164	369	512	380			
	Hasil Presentase Skor Total Dimensi *Attitude*									70%
HASIL PRESENTASE SKOR TOTAL AREA PENANGANAN INFORMASI									75%	

Tabel 0.7 Hasil tingkat kesadaran keamanan informasi area pelaporan insiden

AREA : PELAPORAN INSIDEN										
Dimensi	Kode	Kategori Pernyata-an	SS	S	N	TS	STS	Skor Total	Skor Ideal (427*5)	Presen-tase
Knowledge (Pengeta-huan)	PIN1.01	Positif	108*5 540	179*4 716	109*3 327	27*2 54	4*1 4	1641	2135	76,86%
	PIN2.01	Positif	101*5 505	211*4 844	97*3 291	16*2 32	2*1 2	1674	2135	78%
	Hasil Presentase Skor Total Dimensi *Knowledge*									78%
Behavior (Perilaku)	PIN1.02	Positif	107*5 535	158*4 632	131*3 393	27*2 54	4*1 4	1618	2135	76%
	PIN2.02	Negatif	24*1 24	35*2 70	105*3 315	186*4 744	77*5 385	1538	2135	72%
	Hasil Presentase Skor Total Dimensi *Behavior*									74%
Attitude (Sikap)	PIN1.03	Negatif	16*1 16	40*2 80	116*3 348	167*4 668	88*5 440	1552	2135	73%
	PIN2.03	Negatif	19*1 19	46*2 92	112*3 336	186*4 744	64*5 320	1511	2135	71%
	Hasil Presentase Skor Total Dimensi *Attitude*									72%
HASIL PRESENTASE SKOR TOTAL AREA PELAPORAN INSIDEN									74%	

Tabel 0.8 Hasil tingkat kesadaran keamanan informasi area backup data.

AREA : MELAKUKAN *BACKUP DATA*										
Dimensi	Kode	Kategori Pernyata-an	SS	S	N	TS	STS	Skor Total	Skor Ideal (427*5)	Presentase
Knowledge (Pengeta-huan)	BD1.01	Positif	148*5	136*4	89*3	46*2	8*1	1651	2135	77,33%
			740	544	267	92	8			
	BD2.01	Negatif	101*1	211*2	97*3	16*4	2*5	888	2135	42%
			101	422	291	64	10			
	Hasil Presentase Skor Total Dimensi *Knowledge*									59%
Behavior (Perilaku)	BD1.02	Positif	129*5	137*4	73*3	70*2	18*1	1570	2135	74%
			645	548	219	140	18			
	BD2.02	Negatif	24*1	35*2	105*3	186*4	77*5	1538	2135	72%
			24	70	315	744	385			
	Hasil Presentase Skor Total Dimensi *Behavior*									73%
Attitude (Sikap)	BD1.03	Positif	123*5	155*4	85*3	54*2	10*1	1608	2135	75%
			615	620	255	108	10			
	BD2.03	Negatif	19*1	46*2	112*3	186*4	64*5	1511	2135	71%
			19	92	336	744	320			
	Hasil Presentase Skor Total Dimensi *Attitude*									73%
HASIL PRESENTASE SKOR TOTAL AREA MELAKUKAN *BACKUP DATA*									68%	

Tabel 0.9 Hasil tingkat kesadaran keamanan informasi area social engineering

AREA : *SOCIAL ENGINEERING*										
Dimensi	Kode	Kategori Pernyata-an	SS	S	N	TS	STS	Skor Total	Skor Ideal (427*5)	Presen-tase
Knowledge (Pengetah-uan)	SE1.01	Positif	121*5	165*4	116*3	22*2	3*1	1660	2135	77,75%
			605	660	348	44	3			
	SE2.01	Positif	204*5	158*4	48*3	15*2	2*1	1828	2135	86%
			1020	632	144	30	2			
	Hasil Presentase Skor Total Dimensi *Knowledge*									82%
Behavior (Perilaku)	SE1.02	Negatif	24*1	95*2	129*3	106*4	73*5	1390	2135	65%
			24	190	387	424	365			
	SE2.02	Positif	151*5	161*4	94*3	16*2	5*1	1718	2135	80%
			755	644	282	32	5			
	Hasil Presentase Skor Total Dimensi *Behavior*									73%
Attitude (Sikap)	SE1.03	Negatif	27*1	109*2	116*3	109*4	66*5	1361	2135	64%
			27	220	348	436	330			
	SE2.03	Positif	184*5	173*4	58*3	10*2	2*1	1808	2135	85%
			920	692	174	20	2			
	Hasil Presentase Skor Total Dimensi *Attitude*									74%
HASIL PRESENTASE SKOR TOTAL AREA *SOCIAL ENGINEERING*									76%	

Tabel 0.10 Hasil tingkat kesadaran keamanan informasi area malware.

AREA : MALWARE										
Dimensi	Kode	Kategori Pernyata-an	SS	S	N	TS	STS	Skor Total	Skor Ideal (427*5)	Presenta-se
Knowledge (Pengeta-huan)	MW1.01	Positif	104*5	168*4	121*3	29*2	5*1	1618	2135	75,78%
			520	672	363	58	5			
	MW2.01	Positif	158*5	165*4	76*3	18*2	10*1	1724	2135	81%
			790	660	228	36	10			
	Hasil Presentase Skor Total Dimensi *Knowledge*									78%
Behavior (Perilaku)	MW1.02	Negatif	28*1	81*2	70*3	136*4	112*5	1504	2135	70%
			28	162	210	544	560			
	MW2.02	Positif	81*5	114*4	136*3	73*2	23*1	1438	2135	67%
			405	456	408	146	23			
	Hasil Presentase Skor Total Dimensi *Behavior*									69%
Attitude (Sikap)	MW1.03	Negatif	14*1	77*2	78*3	134*4	124*5	1558	2135	73%
			14	154	234	536	620			
	MW2.03	Positif	141*5	116*4	107*3	41*2	22*1	1584	2135	74%
			695	464	321	82	22			
	Hasil Presentase Skor Total Dimensi *Attitude*									74%
HASIL PRESENTASE SKOR TOTAL AREA MALWARE									74%	

Setelah dilakukan perhitungan data untuk tiap area keamanan informasi, selanjutnya dapat disimpulkan dalam bentuk map agar lebih mudah dalam melihat tingkat kesadaran keamanan informasi tiap area keamanan informasi dan dimensi kesadaran keamanan informasi. Berikut merupakan hasil *mapping* atau bisa disebut *Information Security Awareness Maps.*

Tabel 0.11 Information security awareness maps.

AREA	DIMENSI			TOTAL
	Knowledge	*Attitude*	*Behavior*	
Manajemen *Password*	65%	55%	55%	59%
Penggunaan Email	81%	83%	79,5%	81%
Penggunaan Internet	76%	70%	57%	68%
Penggunaan Media Sosial	77%	68%	68%	71%
Keamanan Perangkat Mobile	75%	74%	71%	73%
Penanganan Informasi	82%	70%	72%	75%
Pelaporan Insiden	78%	72%	74%	74%
Backup data	59%	73%	73%	66%
Social engineering	82%	74%	73%	76%
Malware	78%	74%	69%	74%
TOTAL KESADARAN	**75%**	**71%**	**69%**	**72%**

Keterangan :

: Sadar (tidak dibutuhkan tindakan)

: Cukup Sadar (berpotensi dibutuhkan tindakan).

: Kurang Sadar (dibutuhkan tindakan).

Berdasarkan *Information Security Awareness Maps*, maka dapat diketahui tingkat kesadaran keamanan informasi mahasiswa ITS. Untuk secara keseluruhan nilai kesadaran keamanan informasi mahasiswa ITS adalah sebesar 72%, yaitu berada pada kategori sedang atau berpotensi membutuhkan tindakan. Untuk status dari tiap area keamanan informasi, dari tabel tersebut didapatkan ada satu area keamanan informasi yang berada pada kategori buruk (membutuhkan tindakan) dan ada 8 area yang berada pada kategori sedang (berpotensi membutuhkan tindakan). Dari hasil tersebut, maka terdapat 9 area keamanan informasi yang dapat digunakan sebagai topik dalam menyusun rekomendasi untuk meningkatkan kesadaran keamanan informasi mahasiswa. Selanjutnya dilihat dari nilai presentase pada *Information Security Awareness Maps* dapat dilakukan prioritas sebagai topik acuan penyusunan rekomendasi kegiatan peningkatan kesadaran keamanan informasi. Berikut tabel prioritasi dari area keamanan informasi:

Tabel 0.12 Prioritasi topik kesadaran keamanan informasi.

No Prioritasi	Area / Topik
1	Manajemen *Password*
2	*Backup data*
3	Penggunaan Internet
4	Penggunaan Media Sosial
5	Keamanan Perangkat Mobile
6	Malware
7	Pelaporan Insiden
8	Penanganan Informasi
9	*Social engineering*

1. Manajemen *Password*

Berdasarkan penghitungan kesadaran keamanan informasi untuk tiap area keamanan informasi dan dimensi kesadaran keamanan informasi, didapatkan bahwa manajemen *password* adalah area yang memiliki nilai paling rendah (59%) dan masuk dalam status memerlukan tindakan. Untuk dimensi kesadaran keamanan informasi dari area manajaemen *password*, didapatkan bahwa nilai paling rendah adalah dimensi attitude dan Behavior yang memiliki nilai sama yaitu 55% dan selanjutnya adalah dimensi knowledge. Dari hasil tersebut dapat disimpulkan jika mahasiswa ITS sudah memiliki pengetahuan yang cukup tentang manajemen *password*, namun untuk sikap dan perilaku terkait manajemen *password* masih tergolong kurang. Sehingga rancangan usulan rekomendasi yang perlu diprioritaskan adalah untuk *dimensi Behavior, attitude, dan kemudian adalah knowledge*.

2. *Backup data*

Berdasarkan penghitungan kesadaran keamanan informasi untuk tiap area keamanan informasi dan dimensi kesadaran keamanan informasi, didapatkan bahwa *backup data* adalah area yang memiliki nilai yang cukup rendah (66%) dan masuk dalam status berpotensi memerlukan tindakan. Untuk dimensi kesadaran keamanan informasi dari area *backup data*, didapatkan bahwa nilai paling rendah adalah dimensi *knowledge* yaitu sebesar 59% dan selanjutnya adalah dimensi *attitude* dan *Behavior* yang memiliki nilai sama yaitu 73%. Dari hasil tersebut dapat disimpulkan jika mahasiswa ITS sudah memiliki sikap dan perilaku yang cukup tentang pentingnya dan cara melakukan *backup* yang benar, namun mereka tidak sadar bahwa hal tersebut merupakan cara untuk menjaga keamanan data dan hal tersebut memang seharusnya dilakukan. Sehingga rancangan usulan rekomendasi yang perlu diprioritaskan adalah untuk *dimensi knowledge, attitude, dan kemudian adalah Behavior*.

3. Penggunaan Internet

Berdasarkan penghitungan kesadaran keamanan informasi untuk tiap area keamanan informasi dan dimensi kesadaran keamanan informasi, didapatkan bahwa penggunaan internet adalah area yang memiliki nilai yang cukup rendah (68%) dan masuk dalam status berpotensi memerlukan tindakan. Untuk dimensi kesadaran keamanan informasi dari area penggunaan internet, didapatkan bahwa nilai paling rendah adalah dimensi *Behavior* yaitu sebesar 57% dan selanjutnya adalah dimensi *attitude* dengan presentase sebesar 70% dan dimensi *knowledge* yaitu sebesat 76%. Dari hasil tersebut dapat disimpulkan jika mahasiswa ITS sudah memiliki pengetahuan dan sikap yang baik dalam penggunaan internet, namun perilaku yang dilakukan masih tergolong buruk. Sehingga rancangan usulan rekomendasi yang perlu diprioritaskan adalah untuk *dimensi Behavior*, dan kemudian adalah dimensi *attitude* dan *knowledge*.

4. Penggunaan Media Sosial

Berdasarkan penghitungan kesadaran keamanan informasi untuk tiap area keamanan informasi dan dimensi kesadaran keamanan informasi, didapatkan bahwa penggunaan media sosial adalah area yang memiliki nilai yang sudah cukup baik yaitu sebesar 71% dan masuk dalam status berpotensi memerlukan tindakan. Untuk dimensi kesadaran keamanan informasi dari area penggunaan media sosial, didapatkan bahwa seluruh dimensi termasuk dalam kategori yang sudah cukup baik yaitu 68% untuk dimensi *attitude* dan *Behavior*, kemudian 77% untuk dimensi *knowledge*. Dari hasil tersebut dapat disimpulkan jika mahasiswa ITS sudah memiliki kesadaran yang sudah cukup baik dalam menggunakan media sosial, sehingga rancangan usulan rekomendasi disini berfungsi agar kesadaran keamanan informasi mahasiswa ITS terkait penggunaan media sosial tetap terjaga atau bisa menjadi lebih baik.

113

5. Keamanan Perangkat Mobile dan Desktop

Berdasarkan penghitungan kesadaran keamanan informasi untuk tiap area keamanan informasi dan dimensi kesadaran keamanan informasi, didapatkan bahwa keamanan perangkat mobile adalah area yang memiliki nilai yang sudah cukup baik yaitu sebesar 73% dan masuk dalam status berpotensi memerlukan tindakan. Untuk dimensi kesadaran keamanan informasi dari area keamanan perangkat mobile, didapatkan bahwa seluruh dimensi termasuk dalam kategori yang sudah cukup baik yaitu 71% untuk dimensi *Behavior*, 74% untuk dimensi *attitude*, kemudian 75% untuk dimensi *knowledge*. Dari hasil tersebut dapat disimpulkan jika mahasiswa ITS sudah memiliki kesadaran yang sudah cukup baik terkait adanya malware, sehingga rancangan usulan rekomendasi disini berfungsi agar kesadaran keamanan informasi mahasiswa ITS terkait menjaga keamanan perangkat mobile tetap terjaga atau bisa menjadi lebih baik.

6. Malware

Berdasarkan penghitungan kesadaran keamanan informasi untuk tiap area keamanan informasi dan dimensi kesadaran keamanan informasi, didapatkan bahwa malware adalah area yang memiliki nilai yang sudah cukup baik yaitu sebesar 74% dan masuk dalam status berpotensi memerlukan tindakan. Untuk dimensi kesadaran keamanan informasi dari area penggunaan media sosial, didapatkan bahwa seluruh dimensi termasuk dalam kategori yang sudah cukup baik yaitu 69% untuk dimensi *Behavior*, 74% untuk dimensi *attitude*, kemudian 78% untuk dimensi *knowledge*. Dari hasil tersebut dapat disimpulkan jika mahasiswa ITS sudah memiliki kesadaran yang sudah cukup baik terkait adanya malware, sehingga rancangan usulan rekomendasi disini berfungsi agar kesadaran keamanan informasi mahasiswa ITS terkait adanya malware tetap terjaga atau bisa menjadi lebih baik.

7. Pelaporan Insiden

Berdasarkan penghitungan kesadaran keamanan informasi untuk tiap area keamanan informasi dan dimensi kesadaran keamanan informasi, didapatkan bahwa pelaporan insiden adalah area yang memiliki nilai yang sudah cukup baik yaitu sebesar 74% dan masuk dalam status berpotensi memerlukan tindakan. Untuk dimensi kesadaran keamanan informasi dari area penggunaan media sosial, didapatkan bahwa seluruh dimensi termasuk dalam kategori yang sudah cukup baik yaitu 72% untuk dimensi *attitude*, 74% untuk dimensi *Behavior*, kemudian 78% untuk dimensi *knowledge*. Dari hasil tersebut dapat disimpulkan jika mahasiswa ITS sudah memiliki kesadaran yang sudah cukup baik dalam melaporkan adanya insiden keamanan informasi, sehingga rancangan usulan rekomendasi disini berfungsi agar kesadaran keamanan informasi mahasiswa ITS dalam melaporkan adanya insiden keamanan informasi tetap terjaga atau bisa menjadi lebih baik.

8. Penanganan Informasi

Berdasarkan penghitungan kesadaran keamanan informasi untuk tiap area keamanan informasi dan dimensi kesadaran keamanan informasi, didapatkan bahwa penanganan informasi adalah area yang memiliki nilai yang sudah cukup baik yaitu sebesar 75% dan masuk dalam status berpotensi memerlukan tindakan. Untuk dimensi kesadaran keamanan informasi dari area penggunaan media sosial, didapatkan bahwa seluruh dimensi termasuk dalam kategori yang sudah cukup baik yaitu 7% untuk dimensi *attitude*, 72% untuk dimensi *Behavior*, kemudian 82% untuk dimensi *knowledge*. Dari hasil tersebut dapat disimpulkan jika mahasiswa ITS sudah memiliki kesadaran yang sudah cukup baik dalam menangani informasi penting, sehingga rancangan usulan rekomendasi disini berfungsi agar kesadaran keamanan informasi mahasiswa ITS dalam menangani informasi penting tetap terjaga atau bisa menjadi lebih baik.

115

9. *Social engineering*

Berdasarkan penghitungan kesadaran keamanan informasi untuk tiap area keamanan informasi dan dimensi kesadaran keamanan informasi, didapatkan bahwa *social engineering* adalah area yang memiliki nilai yang sudah cukup baik yaitu sebesar 76% dan masuk dalam status berpotensi memerlukan tindakan. Untuk dimensi kesadaran keamanan informasi dari area *social engineering*, didapatkan bahwa seluruh dimensi termasuk dalam kategori yang sudah cukup baik yaitu 73% untuk dimensi *behavior*, 74% untuk dimensi *attitude*, kemudian 82% untuk dimensi *knowledge*. Dari hasil tersebut dapat disimpulkan jika mahasiswa ITS sudah memiliki kesadaran yang sudah cukup baik dengan adanya *social engineering*, sehingga rancangan usulan rekomendasi disini berfungsi agar kesadaran keamanan informasi mahasiswa ITS terkait adanya *social engineering* tetap tserjaga atau bisa menjadi lebih baik.

6.1.2. Identifikasi Metode Penyampaian Usulan Rekomendasi

Usulan rekomendasi dirancang berdasarkan dimensi yang membentuk kesadaran keamanan informasi. Sebelumnya peneliti telah melakukan studi literatur terkait media penyampaian kegiatan, dimana ada banyak metode yang dapat digunakan sebagai alat untuk menyampaikan informasi atau pesan tentang keamanan informasi kepada target. Dari berbagai media penyampaian tersebut perlu dipetakan berdasarkan dimensi kesadaran keamanan informasi untuk memudahkan dalam merancang rekomendasi. Untuk itu dari berbagai macam media penyampaian, maka dapat dilakukan kategorisasai dari media penyampaian usulan rekomendasi untuk setiap dimensi kesadaran keamanan informasi yang nantinya dapat digunakan dalam merancang usulan rekomendasi. Berikut merupakan media penyampaian usulan rekomendasi yang dapat digunakan untuk tiap dimensi:

Tabel 0.13 Tabel kategorisasai media penyampaian berdasarkan dimensi

Dimensi	Media Penyampaiana
Knowledgec (Pengetahauan)	✓ Poster / Infografis ✓ Screensaver dan spanduk ✓ Video ✓ Metode berbasis webs ✓ Metode berbasis komputer ✓ Seminar ✓ Metode telekonferensi ✓ Artikel ✓ Tips tiap bulan ✓ *Security flash card* (risiko, ancaman) ✓ *Newsletter* / Buletin ✓ Workshop ✓ Acara peringatan
Attitude (Sikap)	✓ Awareness Tools (Post-It, Buku Catatan) ✓ Poster / Infografis ✓ Screensaver dan spanduk ✓ Newsletter ✓ Video ✓ Metode berbasis web ✓ Metode berbasis komputer ✓ Metode telekonferensi ✓ Workshop / Pelatihan. ✓ Acara Peringatan ✓ Permaianan ✓ Artikel ✓ Tips Tiap Bulan ✓ *Security Flash Cards (*Risiko, Ancaman*)*
Behavior (Perilaku	✓ Video ✓ Permainan ✓ Workshop / Pelatihan ✓ Program Penghargaan ✓ Memberikan tindakan jika terdapat pelanggaran ✓ Perjanjian/ Peraturan ✓ Ujian ✓ Panduan keamanan informasi

117

6.1.3. Identifikasi Kondisi *Existing*

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) merupakan pihak yang berwewenang dan bertanggung jawab terkait teknologi dan sistem informasi di ITS. Hal tersebut berarti DPTSI juga bertanggung jawab mengenai keamanan informasi di lingkungan ITS.

DPTSI sebenarnya sudah memiliki keinginan untuk melakukan upaya dalam menjaga keamanan informasi dan upaya agar warga ITS sadar akan pentingnya keamanan informasi. Namun hal tersebut belum terlaksana dikarenakan saat ini DPTSI sedang fokus untuk mengembangkan sistem dan layanan pendukung ITS.

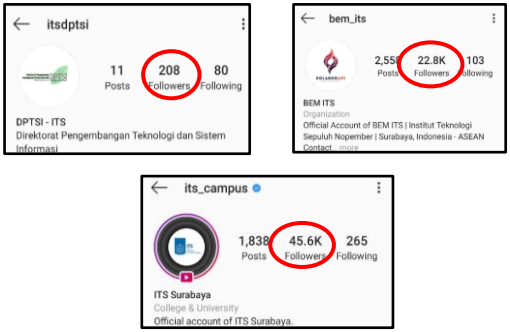
Untuk mendukung upaya peningkatan kesadaran keamanan informasi, perlu adanya dukungan media sebagai wadah dalam menyebarkan informasi. Untuk itu dilakukan identifikasi terkait media sosial yang dimiliki oleh DPTSI, selaku pihak yang akan menyelenggarakan kegiatan. Berikut beberapa media yang dimiliki oleh DPTSI :

a. Instagram

Sebenarnya pihak DPTSI sudah melakukan upaya untuk memberikan wawasan tentang keamanan informasi, yaitu menyebarkan informasi melalui media sosial (instagram) DPTSI ITS. Namun hal tersebut tidak berlangsung lama atau tidak berlanjut, hanya sedikit informasi yang dibagikan. Hal tersebut juga kurang didukung karena jumlah pengikut DPTSI yang masih sedikit, yaitu sekitar 1,2% dari total mahasiswa ITS, sehingga informasi tidak tersampaikan ke sebagian besar mahasiswa ITS

Gambar 6.1 dan 6.2 menunjukkan bahwa hanya 3x dilakukan penyebaran informasi keamanan informasi melalui instagram, dan dilakukan pada bulan Mei. Dapat dilihat juga perbandingan pengikut DPTSI sangat jauh jika dibandingakan dengan instagram milik ITS dan BEM ITS.

Gambar 0.1 Infografis tentang keamanan informasi yang diunggah DPTSI

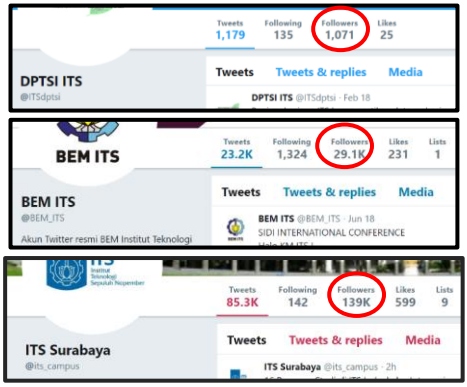


Gambar 0.2 Perbandingan jumlah pengikut instagram DPTSI, BEM ITS, dan ITS.

b. Twitter

Sama halnya dengan instagram, twitter milik DPTSI juga memiliki pengikut yang masih sedikit, yaitu sekitar 5% dari jumlah mahasiswa ITS. Perbandingan pengikut twitter milik DPTSI juga sangatjauh jika dibandingkan dengan BEM ITS dan ITS.

119



Gambar 0.3 Perbandingan jumlah pengikut twitter DPTSI, BEM ITS,dan ITS

c. Website DPTSI

Gambar 0.4 Tampilan website DPTSI

Website dan artikel merupakan salah satu media yang dapat digunakan untuk menyebarkan informasi. Dalam hal ini DPTSI sudah memiliki artikel yang dimuat pada website DPTSI. Namun, artikel tersebut kurang mendapat perhatian dari mahasiswa ITS, dilihat dari jumlah *viewers* untuk artikel yang rata-rata sekitar 100-250 *viewers*.

Gambar 0.5 Jumlah viewers artikel DPTSI

6.2 Penyusunan Usulan Rekomendasi

Setelah mengetahui topik keamanan informasi yang dibutuhkan oleh mahasiswa ITS, serta mengetahui media penyampaian yang cocok untuk tiga dimensi dalam meningkatkan kesadaran keamanan informasi, selanjutnya dapat dilakukan perancangan usulan rekomendasi berdasarkan topik keamanan informasi dan dimensi kesadaran keamanan informasi. Rancangan usulan rekomendasi dilakukan berdasarkan prioritasi topik keamanan informasi yang telah dilakukan (dapat dilihat pada Tabel 6.12). Berikut merupakan rancangan usulan rekomendasi yang dapat disebut sebagai *Information Security Awareness Plan* untuk setiap area keamanan informasi.

Perancangan usulan rekomendasi lebih fokus pada tiga topik keamanan informasi , dimana terdapat dimensi yang berada

121

pada level buruk (berstatus memerlukan tindakan), yaitu manajemen *password*, *backup data*, serta penggunaan internet. Untuk topik lainnya sudah dalam kategori sedang (berpotensi membutuhkan tindakan) sehingga topik tersebut tidak terlalu diprioritaskan, sehingga dapat digabung dengan topik lainnya dalam satu usulan rekomendasi. Dalam penyusunan rekomendasi terdapat tiga tahapan yaitu, perencangan usulan rekomendasi, penyusunan materi, melakukan validasi dengan *expert*, dan yang terakhir adalah mengembangkan usulan rekomendasi.

6.3.1. Perancangan Usulan Rekomendasi

Tahap rancangan usulan rekomendasi dibuat menggunakan media berdasarkan studi literatur yang telah dilakukan sebelumnya. Rancangan yang bertujuan untuk meningkatkan kesadaran keamanan informasi dibuat berdasarkan dimensi kesadarn keamanan informasi yaitu dibuat dengan tujuan meningkatkan pengetahuan, sikap, dan perilaku terkait keamanan informasi sesuai dengan hasil pengukuran kesadaran keamanan informasi. Dari hasil rancangan ini kemudian dilakukan tahapan *expert* judgement yaitu tahapan yang digunakan untuk menilai rekomendasi yang sesuai dengan karakter mahasiswa ITS.Tahapan *expert judgement* dilakukan dengan meminta pendapat kepada pakar yang dianggap memiliki keilmuan yang lebih daripada peneliti untuk memvalidasi apakah rekomendasi yang diusulkan merupakan langkah yang efektif untuk meningkatkan kesadaran keamanan informasi dalam aspek pengetahuan, sikap, dan perilaku. Berikut merupakan beberapa rancangan rekomendasi yang telah dirancang oleh peneliti untuk meningkatkan kesadaran keamanan mahasiswa ITS. Rekomendasi ini merupakan rekomendasi seblum melaukan *expert judgement.*

Tabel 0.14 Rancangan rekomendasi

Tujuan	Judul Rekomendasi	Media penyampaian	Media penyebaran	Deskripsi
Meningkatkan pengetahuan	Infografis Keamanan Informasi	Infografis / Poster Online	Media Sosial	Infografis yang berisi materi tentang keamanan informasi (sesuai topik keamanan informasi yang dipilih) dibuat dan disebarkan oleh Himpunan Mahasiswa ITS melalui media sosial, seperti instagram dan LINE.
	Artikel Keamanan Informasi	Artikel	ITS News	Artikel dibuat oleh DPTSI dan kemudian artikel disebarkan melalui ITS News.
	Perlombaan Keamanan Informasi	Artikel	ITS News Media Sosial	Perlombaan diadakan dengan membawa nama ITS untuk diikuti oleh seluruh mahasiswa ITS. Beberapa pemenang yang terpilih akan mendapatkan hadiah dan artikel akan *dipublish* ke dalam ITS News.

Tujuan	Judul Rekomendasi	Media penyampaian	Media penyebaran	Deskripsi
	Seminar / Kuliah Tamu	Seminar	Media sosial untuk menyebarkan informasi tentang seminar.	Seminar atau kuliah tamu dapat diikuti oleh mahasiswa ITS, namun dengan keterbatasan jumlah peserta. Agar peserta tidak terlalu banyak, maka seminar dapat dilakukan secara bertahap, yaitu dilakukan beberapa kali dengan target peserta yang berbeda. Agar mahasiswa tertarik untuk mengikuti seminar, maka seminar dialokasikan sebagai kuliah tamu, misal untuk mata kuliah wawasan teknologi. Narasumber yang mengisi adalah orang yang ahli dalam keamanan informasi dan korban (orang yang pernah mengalami masalah keamanan informasi).

Tujuan	Judul Rekomendasi	Media penyampaian	Media penyebaran	Deskripsi
	Video Keamanan Informasi	Video	Youtube, yang kemudian disebarkan ke media sosial	Video dibuat untuk memberikan pengetahuan (sesuai dengan topik keamanan informasi yang dipilih), video diunggah pada youtube agar mudah diakses, selanjutnya memanfaatkan media sosial untuk menyebar luaskan video.
Mempengaruhi Sikap	Video Ancaman dan Risiko Keamanan Informasi	Video	Youtube Media Sosial	Video berisi tentang gambaran atau contoh ancaman dan risiko yang ditimbulkan dari lemahnya keamanan informasi. Video diunggah di youtube dan selanjutnya disebarkan melalui media sosial
	Poster Keamanan Informasi	Poster	Dipasang di tiap departemen dan tempat umum di ITS.	Poster dibuat sebagai ajang perlombaan sebagai ajakan untuk menjaga keamanan informasi.

Tujuan	Judul Rekomendasi	Media penyampaian	Media penyebaran	Deskripsi
	Pesan peringatan keamanan informasi	Spanduk / Video Tron	Tempat umum di ITS	Pesan peringatan dibuat dengan tujuan sebagai pengingat tentang pentingnya waspada dan berhati-hati dalam menjaga keamanan informasi.
	Tips Menjaga Keamanan Informasi	Infografis / Poster online	Media sosial	Dengan diberikan tips tentang menjaga keamanan informasi, harapannya mahasiswa dapat lebih wasapada dan mengikuti tips yang diberikan. Tips disebar ke media sosial yang dimiliki organisasi mahasiswa ITS agar mudah dijangkau oleh mahasiswa.
	Workshop / Pelatihan Keamanan Informasi	Workshop	Penyebaran informasi tentang workshop melalui media sosial	Memberikan pelatihan terkait keamanan informasi untuk seluruh mahasiswa baru di tiap departemen yanga ada di ITS.

Tujuan	Judul Rekomendasi	Media penyampaian	Media penyebaran	Deskripsi
				Pelatihan dilaksanakan pada masa kegiatan mahasiswa baru, seperti OKKBK Pelatihan harus dilaksanakan oleh seluruh departemen yang ada di ITS. Pemateri dapat diambil dari dosen atau mahasiswa FTIK yang sudah mendapatkan mata kuliah terkait keamanan informasi.
Mengubah perilaku	Membuat Panduan Keamanan Informasi (Panduan membuat password)	Panduan Keamanan Informasi	Seluruh website dan aplikasi yang di bawah naungan ITS.	Pihak admin atau pihak pengembang aplikasi milik ITS diwajibkan untuk mencantumkan panduan pembuatan *password* yang aman pada halaman registrasi dan halaman pembuatan *password* baru. Dengan adanya panduan tersebut mahasiswa dapat

Tujuan	Judul Rekomendasi	Media penyampaian	Media penyebaran	Deskripsi
				mengikuti aturan pembuatan *password* yang aman sehingga saat membuat atau mengganti *password* akan menggunakan *password* yang sesuai standard keamanan.
	Notifikasi / Pengingat (Mengganti password secara berkala)	Panduan keamanan informasi.	Seluruh website dan aplikasi yang di bawah naungan ITS.	Menambahkan fitur notifikasi atau pengingat kepada mahasiswa untuk mengganti *password* secara berkala sesuai dengan waktu yang telah ditentukan. Waktu default diatur setiap 3 bulan sekali. Mahasiswa dapat memilih waktu dalam mengganti *password* secara berkala dengan diberikan pilihan mulai dari tiap 1 sampai 3 bulan sekali.

Tujuan	Judul Rekomendasi	Media penyampaian	Media penyebaran	Deskripsi
	Membuat Kebijakan (Pengumpulan tugas melalui *One Drive* ITS)	Perjanjian/ Peraturan		Sebelumnya dosen dan mahasiswa diberikan sosialisasi sebelum kebijakan dilakuakn. Setelah itu dosen memberikan aturan saat pengumpulan tugas harus dikumpulkan dalam *One Drive*. Hal tersebut merupakan langkah awal untuk membiasakan mahasiswa dalam menyalin file penting yang dimiliki, serta memperkenalkan dan memanfaatkan fasilitas yang telah dimiliki ITS, yaitu *One Drive* yang mungkin sebagian besar mahasiswa belum mengetahui atau belum menggunakannya.

Tujuan	Judul Rekomendasi	Media penyampaian	Media penyebaran	Deskripsi
	UU Kode Etik tentang Keamanan Informasi	Perjanjian/ Peraturan	Penyebaran informasi tentang kebijakan melalui media sosial dan spanduk.	Dirumuskan peraturan tentang keamanan informasi agar tidak ada tindakan yang kurang baik. Terdapat sanksi yang jelas jika peraturan tersebut dilanggar.
	Workshop / Pelatihan Keamanan Informasi	Workshop	Penyebaran informasi tentang workshop melalui media sosial	Memberikan pelatihan terkait keamanan informasi untuk seluruh mahasiswa baru di tiap departemen yanga ada di ITS. Pelatihan dilaksanakan pada masa kegiatan mahasiswa baru, seperti OKKBK Pelatihan harus dilaksanakan oleh seluruh departemen yang ada di ITS.

6.3.2 Penyusunan Materi

Setelah seluruh usuluan rekomendasi dirancang, langkah selanjutnya adalah menyusun materi keamanan informasi sesuai topik keamanan informasi.Tabel berikut merupakan sub materi dari tiap topik keamanan informasi. Untuk materi lengkapnya akan dijabarkan pada dokumen usulan rekomendasi.

Tabel 0.15 Materi keamanan informasi

Topik	Sub Topik	Sumber
Manajemen *Password*	Membuat *password* yang kuat.	[41] , [42] , [43], [39]
	Menjaga kerahasiaan *password*.	
	Penggunaan *password* untuk berbagai akun.	
	Mengganti *password* secara berkala	
Backup data	*Backup data* secara berkala	[44] , [45], [46]
	Memilih media *backup data*	
	Cara *backup data* (menggunakan *One Drive* ITS)	
Penggunaan Internet	Mewaspadai alamat URL	[39], [47] , [48] , [49], [50]
	Download file	
	Memasukkan informasi dalam internet	
Penggunaan Media Sosial	Tidak memposting informasi pribadi	[51]
	Memperhatikan privacy setting	

131

	Mengetahui dan mempertimbangkan konsekuensi	
	Mendownload lampiran dalam email	
	Berbagai ancaman email	
Keamanann Perangkat Mobile	Keamanan Fisik	[39], [52] , [53], [54]
	Shoulder surfing	
	Penggunaan Wireless	
	Authentication	
Malware	Jenis jenis malware	[55], [56], [57]
	Cara mengetahui malware	
	Cara mencegah malware	
Pelaporan Insiden	Mewaspadai tindak kejahatan keamanan informasi	[39]
	Melaporkan tindak kejahatan keamanan informasi	
Penanganan Informasi	Cara membuang dokumen/ kertas yang berisi informasi sensitif.	[40]
	Memasukkan USB/media pada komputer pribadi	
	Menjaga keberadaan dokumen dengan informasi sensitif / penting	

Social Engineering	Teknik Social Engineering	[57], [58]
	Cara Mengatasi Social Engineering	

6.3.2 Melakukan Validasi Kepada *Expert Judgement*

Setelah rancangan program untuk ketiga dimensi kesadaran keamanan informasi dibuat, selanjutnya dilakukan validasi kepada *expert* judgemet yang memiliki ilmu lebih mendalam. *Expert* judgemt terdiri atas tiga pakar, sebagai berikut :

1. Pakar 1, yaitu Ninda Hayyu, S.Psi bagian *Sub-directorate of Human Resources ITS*, yang mengerti tentang psikologis orang dalam mengubah pengetahuan sampai dengan perilaku.
2. Pakar 2, yaitu Rustini Hendra Wardani**,** S.Psi bagian dari Student Advisory Center (SAC) ITS, yang mengerti tentang psikologis mahasiswa ITS.
3. Pakar 3, yaitu Bekti Cahyo Hidayanto, S.Si, M.Kom, salah satu dosen Sistem Informasi yang memiliki ilmu tentang keamanan informasi.

6.3.2.1. Hasil *Expert Judgement* Rancangan Rekomendasi

Validasi tentang rancangan rekomendasi dilakukan kepada 2 pakar, yaitu pakar 1 dan pakar 2 yang memiliki latar belakang ilmu dalam bidang psikologi. Berikut merupakan hasil tanggapan untuk rancangan rekomendasi dari masing-masing *expert judgement*:

Tabel 0.16 Hasil expert judgement rancangan rekomendasi

Tujuan	Judul Rekomen-dasi	Media penyam-paian	Media penye-baran	Tanggapan	
				Pakar 1	Pakar 2
Meningkatkan pengetahuan	Infografis Keamanan Informasi	Infografis / Poster Online	Media Sosial	Setuju, karena memang benar saat ini media sosial berpengaruh besar.	Setuju, karena memang dengan media sosial informasi lebih cepat tersampaikan secara luas untuk mahasiswa.
	Artikel Keamanan Informasi	Artikel	ITS News	Setuju, artikel memang dapat digunakan sebagai salah satu media untuk memberikan informasi.	Setuju, dengan penambahan penyebaran link melalui media sosial karena memang tidak banyak mahasiswa yang

					sering mengakses ITS News.
	Perlombaan Keamanan Informasi	Artikel	ITS News Media Sosial	Setuju, dengan adanya reward akan menjadi daya tarik.	Setuju, dengan adanya hadiah dapat meningkatkan minat mahasiswa, selain itu juga harus sering diinformasikan mungkin bisa melalui Ketua Himpunan untuk menyebarkan informasi.
	Seminar / Kuliah Tamu	Seminar	Media sosial untuk menyebarkan informasi tentang seminar.	Setuju, jumlah peserta umumnya sekitar 100 orang.	Setuju, dengan memberikan daya tarik misal narasumber yang dibuat menarik.
	Telekoferensi Keamanan Informasi	Telekon-ferensi	Youtube Live.	Setuju, dengan sebelumnya melakukan	Setuju, asal dikemas dengan menarik sehingga

				pemberitahuan ke seluruh media sosial untuk memberikan daya tarik.	saat menonton mahasiswa tidak merasa bosan. Mungkin diberikan kuis berhadiah yang jawabany ada dalam video tersebut
Mempengaruhi Sikap	Video Ancaman dan Risiko Keamanan Informasi	Video	Youtube Media Sosial	Setuju, dengan ilustrasi yang nyata dan memberikan pesan singkat pada video.	Setuju, karena memang perlu diberikan ilustrasi nyata agar dapat mempengaruhi perasaan.
	Poster Keamanan Informasi	Poster	Dipasang di tiap departemen dan tempat umum di ITS.	Setuju, asalkan desain menarik dan dipasang pada tempat yang tepat atau tempat yang sering menjadi titik kumpul atau seringdilewati.	Setuju, asalkan unik dan menarik. Misal dari segi warna ataupun gambar dan pesan yang diberikan harus menarik.

	Pesan peringatan keamanan informasi	Spanduk / Video Tron	Tempat umum di ITS	Setuju. Gunakan kata yang tepat. Jangan gunakan kata "jangan", lebih baik gunakan kata perintah langsung, seperti "stop", "hindari", dsb.	Setuju, namun tambahkan media lain karena video tron letaknya kurang strategis dan hanya beberapa area yang diizinkan untuk pemasangan spanduk.
	Tips Menjaga Keamanan Informasi	Infografis / Poster online	Media sosial	Setuju Dengan tips berarti memberikan arahan atau panduan. Hal tersebut dapat memungkinkan mempengaruhi pemikiran.	Setuju Selain memberikan panduan, mungkin dapat ditambah dengan penjelasan mengenai pentingnya melakukan hal tersebut.

	Telekoferensi Keamanan Informasi	Telekonferensi	Youtube Live	Setuju, dengan ilustrasi yang nyata dan memberikan pesan singkat pada video.	Setuju, karena memang perlu diberikan ilustrasi nyata agar dapat mempengaruhi perasaan.
	Workshop / Pelatihan Keamanan Informasi	Workshop / Pelatiahn	Penyebaran informasi tentang workshop melalui media sosial	Kurang setuju, Jika pelatihan hanya dilakukan sekali hanya mempengaruhi seseorang dalam segi pengetahuan dan sikap saja. Lebih baik menggunakan coatching karena dibutuhkan beberapa kali pelatihan.	Setuju, tapi mungkin tidak untuk seluruh mahasiswa, karena pelatihan untuk mengubah perilaku itu susah jika pesertanya terlalu banyak. Akan lebih efektif jika pesertanya dengan jumlah sedikit. Mungkin dapat dilakukan secara bertahap.
Mengubah perilaku	Membuat Panduan	Panduan	Seluruh website dan aplikasi	Setuju, karena secara tidak	Setuju, namun juga diperlukan

	Keamanan Informasi (Panduan membuat password)		yang di bawah naungan ITS.	langsung menuntun untuk melakukan hal tersebut.	pengalaman secara langsung, seperti melakukan simulasi secara langsung.
	Notifikasi / Pengingat (Mengganti password secara berkala)	Pesan pengingat	Seluruh website dan aplikasi yang di bawah naungan ITS.	Setuju, dengan notifikasi dapat menjadi pengingat.	Setuju, dengan notifikasi dapat menjadi pengingat.
	Membuat Kebijakan (Pengumpulan tugas melalui *One Drive* ITS)	Peraturan		Setuju, dengan aturan lebih dapat mendorong perilaku karena adanya kewajiban yang harus dilakukan dan efek jika tidak melakukan hal tersebut.	Setuju, dengan aturan lebih dapat mendorong perilaku karena adanya kewajiban yang harus dilakukan dan efek jika tidak melakukan hal tersebut.
	UU Kode Etik tentang	Peraturan	Penyebaran informasi tentang	Setuju, dengan adanya sanksi dapat	Setuju, dengan adanya sanksi dapat

	Keamanan Informasi		kebijakan melalui media sosial dan spanduk.	memperngaruhi niat seseorang.	memperngaruhi niat seseorang.
	Workshop / Pelatihan Keamanan Informasi	Workshop / Pelatiahn	Penyebaran informasi tentang workshop melalui media sosial	Kurang setuju, Jika pelatihan hanya dilakukan sekali hanya mempengaruhi seseorang dalam segi pengetahuan dan sikap saja. Lebih baik menggunakan coatching karena dibutuhkan beberapa kali pelatihan.	Setuju, tapi mungkin tidak untuk seluruh mahasiswa, karena pelatihan untuk mengubah perilaku itu susah jika pesertanya terlalu banyak. Akan lebih efektif jika pesertanya dengan jumlah sedikit. Mungkin dapat dilakukan secara bertahap.

6.3.2.2 Hasil *Expert Judgement* Konten Keamanan Informasi
Dalam melakukan validasi terkait konten keamanan informasi dilakukan dengan pakar 3 yang memiliki keilmuan terkait keamanan informasi. Berikut merupakan hasil tanggapan mengenai konten keamanan informasi.

Tabel 0.17 Hasil expert judgement tentang konten keamanan informasi

Topik	Sub Topik	Pendapat Pakar 3	Keterangan Tambahan
Manajemen *Password*	Kekuatan *password*	V	– Akan lebih berpengaruh sebenarnya jika sistem yang dibuat harus memaksa atau mengharuskan mahasiswa melakukan hal tersebut. Contohnya seluruh website atau aplikasi di bawah naungan ITS harus membuat sistem yang mengharuskan mahasiswa membuat *password* sesuai standard, jika tidak memenuhinya maka tidak dapat
	Menjaga kerahasiaan *password*.	V	
	Penggunaan *password* untuk berbagai akun.	V	
	Mengganti *password*.	V	
Backup data	*Backup data* secara berkala	V	
	Memilih media *backup* yang tepat	V	
	Cara *backup data*	V	
Penggunaan Internet	Memperhatikan link website	V	
	Download file	V	
	Memasukkan informasi dalam internet	V	
Penggunaan Media Sosial	Tidak memposting informasi pribadi	V	

Topik	Sub Topik	Pendapat Pakar 3	Keterangan Tambahan
	Memperhatikan privacy setting	V	digunakan. Aturan lain misal diwajibkan menggunkan *One Drive* ITS saat menyimpan data. Aturan lainnya dengan membatasi akses internet dalam ITS, seperti memblok website yang terindikasi tidak aman. Hal lainnya yang dapat dilakukan yaitu dengan mendaftarkan setiap perangkat yang dimiliki mahasiswa dan No Hp yang terhubung, sehingga jika mahasiswa terindikasi melanggar, maka seluruh
	Mengetahui dan mempertimbangkan konsekuensi	V	
Penggunaan Email	Membuka link dalam email	V	
	Menjaga keamanan informasi saat mengirim email	V	
	Mendownload lampiran dalam email	V	
	Berbagai ancaman email	V	
Keamanann Perangkat Mobile dan Desktop	Keamanan Fisik	V	
	Shoulder surfing	V	
	Penggunaan Wireless	V	
	Ancaman terhadap keamanan perangkat mobile	V	
	Authentication	V	
Malware	Jenis jenis malware	V	

Topik	Sub Topik	Pendapat Pakar 3	Keterangan Tambahan
	Cara mengetahui malware	V	perangkat akan diblokir. – Membuat acara seminar untuk mahasiswa baru juga penting dilakukan untuk menumbuhkan kesadaran dari awal saat mahasiswa memasuki ITS. Buku saku juga perlu dibuat sebagai informasi atau panduan agar mahasiswa mengetahui bagaimana menjaga keamanan informasi. Seminar akan lebih mengenai target jika ditunjukan ilustrasi atau contoh permasalahan yang pernah terjadi. – Sebelum menerapkan
	Cara mencegah malware	V	
Pelaporan Insiden	Mewaspadai orang sekitar yang tidak dikenal	V	
	Melaporkan tindak kejahatan di sekitar	V	
Penanganan Informasi	Cara membuang kertas /dokumen yang berisi informasi sensitif	V	
	Memasukkan USB/media pada komputer pribadi	V	
	Menjaga keberadaan dokumen dengan informasi sensitif / penting	V	
Social engineering	Teknik *Social engineering*	V	
	Cara Mengatasi *Social engineering*	V	

143

Topik	Sub Topik	Pendapat Pakar 3	Keterangan Tambahan
			sistem atau aturan yang mengikat, lebih baik maelakukan sosialisasi atau kampanye tentang keamanan informasi sehingga mahasiswa memahami mengapa kebijakan tersebut penting .

6.3.3. Mengembangkan Usulan Rekomendasi

Berdasarkan hasil *expert judgement* yang telah dilakukan, maka rancangan rekomendasi dilakukan perbaikan seperti yang dijabarkan pada tabel berikut :

Tabel 0.18 Usulan Rekomendasi setelah tervalidasi

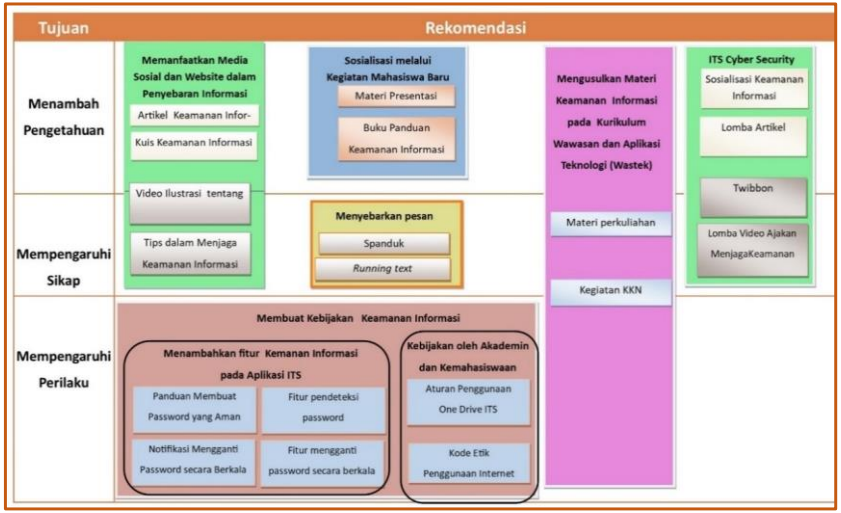
Tujuan	Judul Rekomendasi	Keterangan
Meningkatkan pengetahuan	Infografis Keamanan Informasi	Digunakan
	Artikel Keamanan Informasi	Digunakan

	Perlombaan Keamanan Informasi	Digunakan Tambahan : menyebarkan informasi perlombaan melalui himpunan mahasiswa tiap departemen, menargetkan terdapat perwakilan tiap departemen
	Seminar / Kuliah Tamu	Digunakan Tambahan : Bukan kuliah tamu akan tetapi memasukkan materi keamanan informasi pada mata kuliah wawasan teknologi.
Mempengaruhi Sikap	Video Ancaman dan Risiko Keamanan Informasi	Digunakan
	Poster Keamanan Informasi	Digunakan
	Pesan peringatan keamanan informasi	Digunakan Tambahan : tidak hanya pada tempat umum di ITS, namun juga memasang pesan peringatan di setiap departemen dengan memanfaatkan fasilitas seperti layar TV.
	Tips Menjaga Keamanan Informasi	Digunakan
Mengubah perilaku	Membuat Panduan Keamanan Informasi	Digunakan Tambahan : tidak hanya panduan, naum juga

145

	(Panduan membuat *password*)	ditambahkan sistem yang dapat mendeteksi keamanan *password*, sehingga mahasiswa tidak akan berhasil membuat *password* jika tidak memenuhi standard.
	Notifikasi / Pengingat (Mengganti *password* secara berkala)	Digunakan Tambahan : bukan hanya notifikasi yang dapat dilewati, namun notifikaso yang harus dilakukan. Jika tidak dilakukan maka risikonya tidak dapat mengakses akun dan harus melaporkan ke pihak DPTSI.
	Membuat Kebijakan (Pengumpulan tugas melalui *One Drive* ITS)	Digunakan
	UU Kode Etik tentang Keamanan Informasi	Digunakan Tambahan : menginformasikan UU pada halaman awal website dan aplikasi yang berada di bawah naungan ITS.
	Workshop / Pelatihan Keamanan Informasi	Tidak digunakan karena implementasi susah untuk pelatihan menyeluruh kepada mahasiswa ITS. Jika diganti dengan coatching pun susah juga.

Berdasarkan evaluasi di atas, selanjutnya dibuat dalam sebuah bentuk *roadmap* kegiatan untuk mengkategorikan rekomendasi agar memudahkan dalam pelaksanaan kegiatan.



Gambar 0.6 Roadmap Rekomendasi Kegiatan

Berdasarkan kategorisasi rekomendasi seperti yang telah digambarkan pada *roadmap* kegiatan, maka selanjutnya dibuat rincian dari tiap rekomendasi kegiatan yang telah dirancang.

1. Menyebarkan Informasi tentang Keamanan Informasi melalui Media Sosial dan Aplikasi Milik ITS.

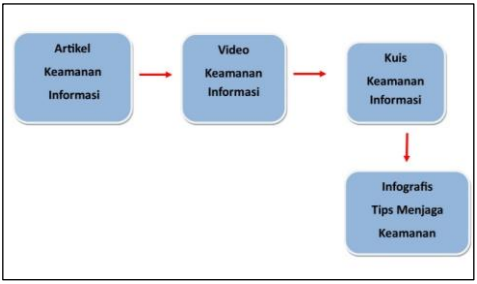
Dalam mendorong kesadaran akan keamanan informasi, terlebih dahulu dibutuhkan pengetahuan terkait pentingnya menjaga keamanan informasi. Dalam rekomendasi ini pengetahuan dapat diberikan melalui sebuah artikel. Dengan dukungan website yang telah dimiliki ITS (baik website DPTSI maupun ITS) maka artikel dapat disebarkan secara online melalui website tersebut. Dikarenakan fakta bahwa mahasiswa ITS sangat jarang mengakses website ITS, maka dibutuhkan media lain yaitu media sosial, seperti instagram, twitter dan LINE yang merupakan media sosial yang sering diakses oleh mahasiswa saat ini.

Video Keamanan Informasi yang berisi ilustrasi terkait ancaman dan risiko dari hilangnya keamanan informasi merupakan salah satu cara yang dapat dilakukan untuk membentuk sikap dikarenakan dalam studi literatur telah dijelaskan jika salah satu cara untuk mengubah persepsi adalah dengan teknik memberikan rasa takut atau menunjukkan dampak negatif dari tindakan yang salah.

Infografis yang berisi tips dalam menjaga keamanan informasi merupakan salah satu cara dalam membentuk perilaku seseorang karena dengan adanya tips tersebut dapat memberikan panduan terkait apa yang seharusnya dilakukan.

Kuis keamanan informasi diberikan hanya sebagai daya tarik untuk menarik minat mahasiswa dalam membaca artikel dan melihat video serta tips keamanan informasi.

Gambar berikut merupakan apelaksanaan kegiatan :



Gambar 0.7 urutan pelaksanaan rekomendasi 1

Tabel di bawah ini merupakan detail informasi terkait rekomendasi yang diusulkan terkait kegiatan menyebarkan informasi tentang keamanan informasi melalui aplikasi dan media sosial yang dimiliki ITS.

Tabel 0.19 Detail informasi rekomendasi 1

Menyebarkan Informasi tentang Keamanan Informasi melalui Media Sosial dan Aplikasi Milik ITS.
Catatan : - DPTSI membentuk tim pelaksana dan membagi PJ untuk setiap bentuk kegiatan (artikel, video, kuis, tips). - DPTSI memerlukan kerja sama dengan admin media sosial BEM ITS dan ITS untuk melakukan promosi dikarenakan jumlah pengikut website DPTSI yang masih sangat sedikit, sedangkan jumlah pengikut BEM ITS dan ITS dapat dibilang sudah banyak. - Rekomendasi dilakukan secara berurutan dan dalam satu minggu harus sesuai dengan topik yang dibahas. - Dapat beralih ke topik lainnya jika seluruh informasi tentang topik tersebut sudah tersampaikan.

149

- Topik yang disampaiakan harus sesuai dengan prioritasi topik yang telah dilakukan (Tabel 6.12)	
Artikel Keamanan Informasi	
Media Penyampaian	Artikel
Media penyebaran	Aplikasi (website DPTSI dan website ITS) Media sosial (instagram, twitter, LINE)
Tujuan	Meningkatkan pengetahuan mahasiswa terkait pentingnya menjaga keamanan informasi.
Topik	9 Topik keamanan informasi
Target/Penerima	Seluruh mahasiswa ITS
Deskripsi	Artikel keamanan informasi mencangkup seluruh topik keamanan informasi. Dalam satu artikel membahas satu topik dan berdasarkan prioritas dari topik keamanan informasi. Untuk manajemen *password* dikarenakan memiliki nilai buruk, maka lebih diperbanyak jumlah artikelnya dari pada topik lainnya.
Frekuensi	1 minggu 1x
Peran dan tanggung jawab	- PJ Kegiatan (DPTSI) : membuat materi artikel keamanan informasi. - Admin website : memasukkan artikel ke dalam website. - Admin Media Sosial : mengunggah informasi terkait artikel keamanan informasi.
Indikator keberhasialan	Jumlah *viewers* artikel meningkat dari artikel lain atau artikel sebelumnya.
Video Keamanan Informasi	
Media Penyampaian	*Video youtube*
Media penyebaran	Media sosial (instagram, twitter, LINE) Website DPTSI dan ITS
Tujuan	Mempengaruhi persepsi dan perasaan sesorang terkait pentingnya menjaga keamanan informasi
Topik	9 Topik keamanan informasi.
Target/Penerima	Seluruh mahasiswa ITS

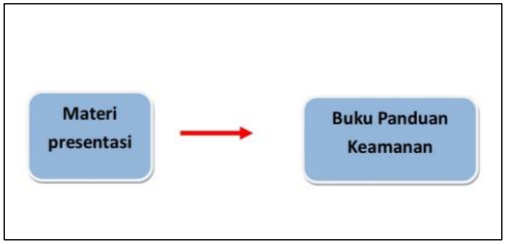
Deskripsi	- PJ Kegiatan (DPTSI) harus menghubungi admin website ITS untuk bekerja sama dalam menggunggah video ke dalam website ITS. - PJ Kegiatan (DPTSI) harus menyiapkan beberapa video keamanan informasi. - Video tersebut berisi ilustrasi terkait ancaman dan risiko jika tidak memperdulikan keamanan informasi - Video diunggah ke dlam youtube dan selanjutnya dapat disebarkan melalui media sosial.
Frekuensi	1 miggu 1x
Peran dan tanggung jawab	- PJ Kegiatan (DPTSI) : menyiapkan video dan mengunggah ke youtube - Admin media sosial : mengunggah informasi terkait video keamanan informasi. - Admin Website : memasukkan video tersebut ke dalam konten video dalam website ITS.
Indikator keberhasialan	Jumlah orang yang melihat video meningkat, dilihat dari video lain yang telah dipublikasikan.
Kuis Keamanan Informasi	
Media Penyampaian	Permaianan (kuis)
Media penyebaran	Media sosial (instagram)
Tujuan	Memberikan daya tarik agar mahasiswa tertarik untuk membaca dan melihat informasi tentang keamanan informasi yang telah diunggah.
Topik	9 Topik keamanan informasi
Target/Penerima	Seluruh mahasiswa ITS
Deskripsi	- Kuis akan diadakan seminggu sekali setelah artikel dan video diunggah. - Mahasiswa dapat menjawab kuis dengan mengisi jawaban dalam kolom komentar

151

	dan mengajak 3 temannya untuk menjawab. Hal ini dilakukan agar mahasiswa dapat mengajak mahasiswa lain untuk mengikuti kuis sehingga media sosial DPTSI lebih menyebar luas. - Dipilih beberapa pemenang, setiap orang yang mengikuti kuis tersebut wajib *follow* (mengikuti) media sosial DPTSI. Jika pemenang tidak *follow* akun media sosial DPTSI, maka dianggap tidak sah.
Frekuensi	1 minggu 1x
Peran dan tanggung jawab	- PJ Kegiatan (DPTSI) : menyusun ketentuan dan pertanyaan kuis. - Admin media sosial DPTSI : mengunggah informasi kuis.
Indikator keberhasialan	Jumlah komentar yang masuk dalam setiap kuis leboh dari 20.
Tips Menjaga Keamanan Informasi	
Media Penyampaian	Infografis
Media penyebaran	Media sosial (instagram, twitter, LINE)
Tujuan	Memberikan petunjuk
Topik	9 Topik keamanan informasi berdasarkan prioritas (Tabel 6.12)
Target/Penerima	Seluruh mahasiswa ITS
Deskripsi	Tips keamanan informasi mencangkup seluruh topik keamanan informasi yang membutuhkan tindakan. Untuk topik manajemen *password* lebih diperbanyak karena nilai yang masih buruk.
Frekuensi	1 minggu 1x
Peran dan tanggung jawab	- PJ Kegiatan (DPTSI) : menyusun materi dan membuat infografis. - Admin Media sosial : mengunggah infografis.
Indikator keberhasialan	Jumlah *reach* (jangkauan) minimal 50% dari jumlah pengikut media sosial tersebut.

2. Sosialisasi Melalui Kegiatan Mahasiswa Baru

Kegiatan mahasiswa baru merupakan kegiatan wajib yang harus diikuti oleh mahasiswa baru yang telah terdaftar menjadi mahasiswa ITS. Salah satu kegiatan yang wajib diikuti oleh mahasiswa baru adalah kegiatan IPITS (Informasi dan Pengenalan ITS), di mana kegiatan tersebut merupakan kegiatan untuk memberikan pengetahuan mahasiswa mengenai ITS. Kegiatan IPITS dapat dimanfaatkan sebagai sarana dalam mengenalkan pentingnya keamanan informasi bagi mahasiswa ITS. Dengan sosialiasi ini dapat menjangkau mahasiswa secara luas. Kegiatan ini bertujuan untuk memberikan pengetahuan kepada mahasiswa melalui materi presentasi, dan selanjutnya akan dibagikan buku panduan keamanan informasi agar mahasiswa dapat memahaminya lebih lanjut dikarenakan waktu yang terbatas, serta menerapkan seluruh panduan yang telah diberikan. Berikut merupakan gambar alur pelakasanaan kegiatan.



Gambar 0.8 Urutan pelaksanaan rekomendasi 2

Berikut merupakan detail informasi terkait kegiatan yang akan dilaksanakan :

Tabel 0.20 Detail informasi rekomendasi 2

Sosialisasi Melalui Kegiatan Mahasiswa Baru	
Catatan : - DPTSI membentuk tim pelaksana dan membagi PJ untuk setiap bentuk kegiatan. - Topik keamanan informasi dapat dirancang secara bebas dengan mempertimbangkan hasil pengukuran kesadaran keamanan informasi, termasuk penggunaan email. - Konten Buku Panduan mencangkup penjelasan umum, ancaman dan risiko, serta cara menghindari dan mengatasi masalah keamanan informasi.	
Materi Presentasi	
Media Penyampaian	Slide presentasi dan video
Media penyebaran	Seminar
Tujuan	Memberikan pengetahuan umum terkait keamanan informasi.
Topik	Seluruh topik keamanan informasi.
Target/Penerima	Mahasiswa baru ITS
Deskripsi	Sebelum dan sesudah materi presentasi, mahasiswa diberikan pertanyaan untuk mengetahui tingkat pengetahuan mahasiswa sebelum dan sesudah matrei. Materi presentasi harus diberikan secara interaktif agar mahasiswa tertarik untuk memperhatikannya, yaitu dengan bahasa yang mudah dipahami, serta menampilkan video yang menarik.
Frekuensi	1x
Peran dan tanggung jawab	- PJ Kegiatan (DPTSI) mengajukan proposal kepada Ketua Pelaksana IPITS. - Ketua Pelaksana mengalokasikan waktu dan lokasi kegiatan. - PJ Kegiatan (DPTSI) menentukan materi dan menyiapkan pembicara.

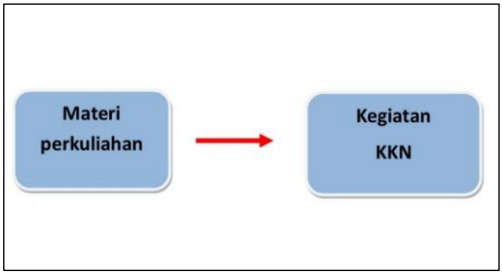
Indikator keberhasialan	Hasil *post test* > *pre test*
Buku Panduan Keamanan Informasi	
Media Penyampaian	Buku panduan
Media penyebaran	Seminar
Topik	Seluruh topik keamanan informasi.
Target/Penerima	Mahasiswa baru ITS
Deskripsi	Buku panduan diberikan agar mahasiswa dapat lebih memahami pentingnya menjaga keamanan informasi, serta mengetahui bagaimana cara agar terhindar dari masalah akibat hilangnya kemanan informasi. Buku panduan harus dibut menarik, dengan memberikan banyak gambar atau ilustrasi agar mahaisiswa lebih tertarik untuk membacanya.
Frekuensi	1x
Peran dan tanggung jawab	- PJ Kegiatan (DPTSI) membuat materi dan mendesain buku panduan keamanan informasi.
Indikator keberhasialan	Seluruh mahasiswa mendapatkan buku panduan.

3. Mengusulkan Materi Keamanan Informasi pada Kurikulum Mata Kuliah Umum Wawasan dan Aplikasi Teknologi (Wastek)

Mata kuliah Wawasan dan Aplikasi Teknologi merupakan salah satu mata kuliah umum yang ada di ITS, di mana kuliah ini wajib diambil oleh seluruh mahasiswa ITS. Dalam mata kuliah Wastek diperkenalkan mengenai wawasan teknologi yang berkembang secara umum, maka dari itu dapat diselipkan materi tentang keamanan informasi pada materi perkuliahan. Selain itu juga dapat diusulkan agar materi tentang keamanan informasi juga dapat disebarluaskan atau disosialisasikan kepada masyarakat melalui kegiatan Kerja Kuliah Nyata (KKN). Memberikan materi pada perkuliahan merupakan cara

155

yang cukup efektif untuk memberikan pengetahuan, bagaimana cara menyikapi, serta mulai mempengaruhi perilaku mahasiswa karena dalam kuliah mahasiswa dapat menyerap ilmu serta dapat melakukan praktik secara langsung dan dilaksanakan secara berkelanjutan (tidak hanya satu kali). Berikut merupakan gambar alur pelakasanaan kegiatan.



Gambar 0.9 Urutan pelaksanaan rekomendasi 3

Berikut merupakan detail informasi terkait kegiatan yang akan dilaksanakan :

Tabel 0.21 Detail informasi rekomendasi 3

Mengusulkan Materi Keamanan Informasi pada Kurikulum Mata Kuliah Umum Wawasan dan Aplikasi Teknologi (Wastek)
Catatan : - DPTSI membentuk tim pelaksana dan membagi PJ untuk setiap bentuk kegiatan. - Topik keamanan informasi dapat dipilih secara bebas dengan mempertimbangkan hasil pengukuran kesadaran keamanan informasi.

- Pihak DPTSI mengusulkan topik keamanan informasi, untuk materi dapat didiskusikan lebih lanjut oleh pihak yang berwenang.	
Materi Perkuliahan	
Media Penyampaian	Materi presentasi (silde presentasi dan video); Ujian (evaluasi, praktik, dan tugas); dan kebutuhan pendukung lainnya
Media penyebaran	Perkuliahan
Tujuan	Memberikan ilmu dan memberikan gambaran atau pengalaman langsung terkait keamanan informasi kepada mahasiswa ITS, sehingga dapat diharapkan mahasisiwa ITS akan lebih menyadari pentingnya menjaga keamanan informasi.
Topik	9 Topik Keamanan Informasi (dapat disesuaikan)
Target/Penerima	Mahasiswa ITS yang mengambil mata kuliah Wastek
Deskripsi	Materi tentang keamanan informasi diusulkan untuk disisipkan dalam salah satu materi pada mata kuliah Wastek. Kegiatan yang dapat dilaksanakan dalam perkuliahan Wastek, yaitu materi presentasi yang dapat memberikan pengetahuan mahasiswa, tugas dengan memberikan gambaran tentang ancaman dan risiko keamanan informasi melalui studi kasus dan bagaimana mahasiswa akan menanggapi hal tersebut yang dapat membentuk sikap mahasiswa, serta praktik dalam menjaga keamanan informasi yang dapat membentuk perubahan perilaku karena mahasiswa diberikan pengalaman secara langsung (praktik) terkait menjaga keamanan informasi.
Frekuensi	Minimal 3x pertemuan
Peran dan tanggung jawab	- Kasubdit Layanan Teknologi dan Informasi mengajukan proposal pengajuan materi keamanan informasi

157

	kepada Direktorat Akademik selaku pihak yang berwenang. - Bagian Direktorat akademik berdisikusi dengan pihak yang bertanggung jawab dalam menyusuN rancangan perkuliahan Wastek.
Indikator keberhasialan	Nilai Wastek mahasisiwa di atas rata-rata.
Kegiatan Kuliah Kerja Nyata (KKN)	
Tujuan	Mahasiswa dapat berbagi pengetahuan dan dapat mengajak untuk menjaga keamanan informasi kepada masyarakat umum.
Topik	9 Topik Keamanan Informasi (dapat disesuaikan)
Target/Penerima	Mahasiswa dan masyarakat
Deskripsi	Dengan berbagi pengetahuan dapat mendorong mahasisiwa untuk lebih mendalami tentang keamanan informasi, sehingga mahasiswa akan lebih tahu dan memahami tentang pentingnya keamanan informasi.
Frekuensi	Saat pelaksanaan KKN
Peran dan tanggung jawab	- Kasubdit Layanan Teknologi dan Informasi mengajukan proposal pengajuan materi keamanan informasi kepada Direktorat Akademik selaku pihak yang berwenang. - Bagian Direktorat akademik berdisikusi dengan pihak yang bertanggung jawab dalam menyusun rancangan perkuliahan Wastek.
Indikator keberhasialan	Nilai Wastek mahasisiwa di atas rata-rata.

4. Menyebarkan Pesan Peringatan

Setelah mahaisiswa sudah diberikan pengetahuan tentang pentingnya menjaga keamanan informasi, selanjutnya mahasiswa diberikan pengingat melalui pesan peringatan atau

pesan kutipan sebagai ajakan untuk melaksanakan hal tersebut. Memasang spanduk serta *running text* pada website milik DPTSI ITS merupakan media yang dapat digunakan untuk mendukung penyampaian pesan keamanan informasi.Berikut merupakan detail informasi terkait pelaksanaan kegiatan.

Tabel 0.22 Detail informasi rekomendasi 4

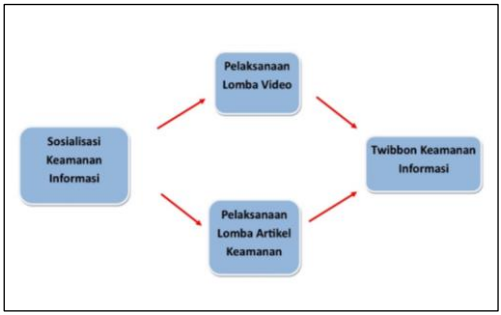
Menyebarkan Pesan Peringatan	
Catatan : - DPTSI membentuk tim pelaksana dan membagi PJ untuk setiap bentuk kegiatan. - Pesan peringatan dibuat dengan mempertimbangkan prioritasi topik keamanan informasi (Tabel 6.12), pesan terkait manajemen *password* sebagai topik yang bernilai buruk dapat lebih diperbanyak. - Pesan peringatan melalui spanduk dan website dapat dilaksanakan bersamaan.	
Pesan Peringatan melalui Spanduk	
Media Penyampaian	Spanduk
Media penyebaran	Dipasang pada tempat umum yang telah diizinkan.
Tujuan	Memberikan pesan agar mahasiswa lebih waspada terkait pentingnya keamanan informasi.
Topik	9 Topik Keamanan Informasi (dengan memperhatikan prioritasi topik)
Target/Penerima	Seluruh mahasiswa ITS.
Peran dan tanggung jawab	- PJ Kegiatan (DPTSI) : meminta izin pemasangan spanduk dan menyiapkan spanduk - Bagian Sarana prasarana : memberikan izin lokasi pemasangan spanduk.
Deskripsi	- PJ Kegiatan (DPTSI) meminta izik kepada pihak sarana dan prasarana untuk memasang spanduk.

159

	- PJ Kegiatan (DPTSI) mendesain dan menyetak spanduk. - Spanduk dipasang di tempat umum di sekitar ITS sesuai dengan lokasi yang diizinkan.
Frekuensi	1x
Indikator keberhasialan	Spanduk terpasang di seluruh tempat umum di ITS (yang telah diizinkan)
Pesan Peringatan melalui *Running text*	
Media Penyampaian	*Running text*
Media penyebaran	Website DPTSI, Website ITS, MyITS (integra).
Tujuan	Memberikan pesan agar mahasiswa lebih waspada terkait pentingnya keamanan informasi.
Topik	9 Topik Keamanan Informasi (dengan memperhatikan prioritasi topik)
Target/Penerima	Seluruh mahasiswa ITS
Peran dan tanggung jawab	- PJ Kegiatan : membuat pesan-pesan keamanan informasi, dan menghubungi tim pengembang website. - Tim pengembang website : menambahkan fitur pengisian *running text* pada website. - Admin website : memasukkan pesan secara berkala.
Deskripsi	Pesan yang ditampilkan dengan *running text* (tulisan berjalan) diletakkan pada posisi atas atau di bawah agar tidak mengganggu konten penting pada website. Perhatikan pemilihan warna yang tepat agar menarik dan tidak mengganggu penggunaan website.
Frekuensi	Pesan diganti secara berkala (misal setiap satu bulan sekali)
Indikator keberhasialan	Pesan ter-*update* secara berkala.

5. ITS *Cyber Security Month*

Kegiatan *Cyber Security Month* telah banyak dilaksanakan di berbagai negara untuk melakukan kampanye tentang keamanan informasi yang dilaksanakan selama kurang lebih dalam satu bulan. Kegiatan tersebut sudah banyak dilaksanakan, *seperti European Cyber Security Awareness Month 2017* [32], *National Cyber Security Month 2018* oleh *SANS Security* [59], *Cyber Security Awareness Month in University of Toronto* [60], dsb. Dari beberapa Cyber Security Month yang telah dilakukan, kegiatan tersebut dilaksanakan pada Bulan Oktober. Maka dari itu usulan rekomendasi ini akan dilaksanakan pada Bulan Oktober. Usulan rekomendasi ini berupa beragam kegiatan yang dilakukan selama satu bulan penuh untuk mengkampanyekan keamanan informasi yang bertujuan meningkatkan kesadaran mahasiswa ITS tentang pentingnya menjaga keamanan informasi. Berikut merupakan rangkaian kegiatan dalam ITS *Cyber Security Awareness Month.*



Gambar 0.10 Urutan pelaksanaan rekomendasi 5

161

Berikut merupakan detail informasi terkait kegiatan yang akan dilaksanakan.

Tabel 0.23 Detail informasi rekomendasi 5

ITS *Cyber Security Month*	
Catatan : - DPTSI membentuk tim pelaksana (panitia) dan membagi PJ untuk setiap bentuk kegiatan.	
Sosialisasi Keamanan Informasi	
Media Penyampaian	Seminar
Tujuan	Memberikan wawasan terkait keamanan informasi ke seluruh mahasiswa ITS
Topik	9 Topik Keamanan Informasi (dapat disesuaikan)
Target/Penerima	Mahasiswa ITS
Peran dan tanggung jawab	- PJ Kegiatan (DPTSI) mengajukan surat edaran kepada Kepala Departemen untuk meminta izin melakukan sosialisasi. - Kepala Departemen : mengintruksi Himpunan Mahasiswa Departemen (HMD) untuk menyebarkan surat edaran tersebut. - HMD : menyiapkan tempat dan perlengkapan sosialisasi dari departemen.
Deskripsi	Sosialisasi dilakukan secara bertahap di seluruh departemen yang ada di ITS.
Frekuensi	1x tiap departemen
Indikator keberhasialan	Peserta yang hadir lebih dari 50 orang.
Lomba Artikel Keamanan Informasi	
Media Penyampaian	Artikel pada website DPTSI

Media penyebaran	Media sosial
Tujuan	Meningkatkan pengetahuan mahasiswa terkait keamanan informasi
Topik	9 Topik Keamanan Infromasi (dapat disesuaikan)
Target/Penerima	Seluruh mahasisiwa ITS
Peran dan tanggung jawab	- PJ Kegiatan: memastikan kegiatan berjalan sesuai rencana. - Panitia Kegiatan : merancang dan melaksanakan perlombaan dan menyeleksi artikel yang masuk.
Deskripsi	- Artikel dibuat oleh mahasiswa ITS dalam bentuk perlombaan. Perlombaan ini bertujuan untuk mendorong mahasiswa untuk mencari informasi dan hal tersebut akan menambah pengetahuan mahasiswa. Informasi perlombaan disebarluaskan melalui media sosial. - Artikel tersebut juga sebagai ajang saling berbagi informasi antar mahasiswa - Peserta dapat memilih topik keamanan informasi (dapat memilih salah satu atau beberapa topik). - Terdapat kolom komentar sebagai wadah berpendapat atau berdiskusi antar mahasiswa - Beberapa artikel dengan topik yang berbeda akan dipilih yang terbaik dan akan mendapatkan hadiah serta dimasukkan ke dalam ITS Media.
Frekuensi	Selama bulan pelaksanaan
Indikator keberhasialan	Terdapat perwakilan dari tiap departemen yang mengikuti perlombaan.
Lomba Video Ajakan Menjaga Keamanan Informasi	
Media Penyampaian	Video youtube
Media penyebaran	Media sosial

163

Tujuan	Memberikan ajakan agar mahasiswa lebih menyadari akan pentingnya keamanan informasi.
Topik	9 Topik Keamanan Infromasi (dapat disesuaikan)
Target/Penerima	Seluruh mahasiswa ITS
Peran dan tanggung jawab	- PJ Kegiatan: memastikan kegiatan berjalan sesuai rencana. - Panitia Kegiatan : merancang dan melaksanakan perlombaan dan menyeleksi artikel yang masuk.
Deskripsi	- DPTSI atau panitia pelaksana selaku yang memahami konten keamanan informasi harus menyiapkan komponen penting dalam perlombaan, seperti materi, ketentuan, dsb. - Salah satu penilaian dari perlombaan adalah jumlah *viewers dan likes* agar video tersebut tidak hanya dilombakan namun juga informasi di dalamnya dapat dibagikan kepada mahasiswa lain. - Konten video berupa ajakan untuk memperhatikan keamanan informasi yang mencangkup seluruh topik keamanan informasi. - Beberapa pemenang mendapatkan hadiah dan dipublikasikan ke media sosial DPTSI.
Frekuensi	Selama bulan pelaksanaan
Indikator keberhasialan	Terdapat perwakilan dari tiap departemen yang mengikuti perlombaan.
***Twibbon* Keamanan Informasi**	
Media Penyampaian	Gerakan Keamanan Informasi
Media penyebaran	Media sosial
Tujuan	Meningkatkan *euforia* dalam gerakan meningkatkan kesadaran keamanan informasi.

Topik	9 Topik Keamanan Infromasi (dapat disesuaikan)
Target/Penerima	Seluruh mahasiswa ITS
Peran dan tanggung jawab	- PJ Kegiatan : menyiapkan keperluan seperti desain twibbon, caption, dsb, serta menghubungi direktorat kemahasiswaan untuk meminta bekerja sama dengan BEM ITS. - Direktorat kemahasiswaan : mengintruksikan BEM ITS untuk mendukung gerakan dan meminta seluruh himpunan dan BEM Fakultas untuk ikut mengunggahnya.
Deskripsi	Twibbon adalah bingkai foto yang dibuat dengan sedemikian rupa yang ditujukan untuk dukungan, promosi dan lainnya. Menurut pengalaman pribadi, Twibbon sangat berperan dalam hal promosi atau sebagai alat untuk mendukung sebuah acara. Untuk menarik minat mahasiswa dapat juga dipuat semacam undian berhadiah bagi yang beruntung.
Frekuensi	Selama bulan pelaksanaan
Indikator keberhasialan	Terdapat lebih dari 100 orang yang mengunggah twibbon, dilihat dari *hashtag.*

6. Membuat Kebijakan Keamanan Informasi

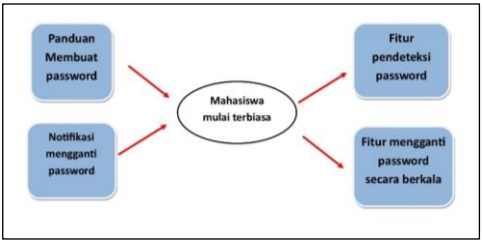
Kebijakan keamanan informasi merupakan aturan yang penting untuk ditegakkan dalam mendukung langkah untuk meningkatkan kesadaran akan pentingnya keamanan informasi. Sesuai dengan kondisi ITS, maka didapatkan tiga rekomendasi terkait kebijakan yang dapat diberlakukan oleh DPTSI, selaku pihak yang berwewenang terkait teknologi informasi. Terdapat 3 kebijakan yang dapat diterapkan, yaitu dengan memperbaiki sistem keamanan informasi pada seluruh aplikasi yang dimiliki ITS, aturan terkait pemanfaatan *One Drive* ITS sebagai media penyimpanan tugas, serta menambahkan kode etik penggunaan internet pada kode etik mahasiswa ITS. Kebijakan dibuat tidak

165

langsung secara keseluruhan, melainkan bertahap setelah dianggap kebijakan tersebut dapat diikuti oleh pihak yang bersangkutan.

a. Menambahkan Fitur Keamanan Informasi pada Aplikasi Milik ITS

Dalam mendukung kesadaran keamanan informasi mahasiswa ITS, diperlukan juga dorongan atau perbaharuan sistem yang baik dan aman agar mahasiswa dapat berperilaku sesuai dengan standard keamanan informasi. Cara untuk mendorong kemauan mahasiswa dapat diberikan dengan memberikan panduan, pengingat atau juga langkah pemaksaan (wajib) yang harus diikuti oleh mahasiswa. Berikut terdapat rekomendasi yang dapat digunakan sebagai langkah untuk mempengaruhi mahasiswa untuk mengikuti standard keamanan informasi. Berikut merupakan alur pelaksanaan rekomendasi.



Gambar 0.11 Urutan pelaksanaan rekomendasi 6 (1)

Untuk detail informasi rekomendasi dapat dilihat pada Tabel 6.24.

Tabel 0.24 Detail informasi rekomendasi 6 (1)

Menambahkan Fitur Keamanan Informasi pada Aplikasi Milik ITS	
Catatan : - DPTSI membentuk tim pelaksana dan membagi PJ untuk setiap bentuk kegiatan.	
Panduan Membuat *Password*	
Media Penyampaian	Kebijakan / Panduan Keamanan Informasi
Media penyebaran	Seluruh website dan aplikasi milik ITS
Tujuan	Agar mahasiswa mengetahui dan membiasakan diri untuk membuat *password* yang aman sehingga mencegah adanya risiko.
Topik	Manajemen *password*.
Target/Penerima	Pihak pengembang aplikasi dan website ITS
Peran dan tanggung jawab	- DPTSI : membuat kebijakan jika seluruh aplikasi dan website milik ITS harus mencantumkan panduan pembuatan *password* dengan persetujuan Warek III. - Pengembang Website / Aplikasi : menambahkan panduan pembuatan *password* ke setiap aplikasi atau website yang dikembangkan.
Deskripsi	- Pihak admin atau pihak pengembang aplikasi milik ITS diwajibkan untuk mencantumkan panduan pembuatan *password* yang aman pada halaman registrasi dan halaman pembuatan *password* baru. - Dengan adanya panduan tersebut mahasiswa dapat mengikuti aturan pembuatan *password* yang aman sehingga saat membuat atau mengganti

167

	password akan menggunakan *password* yang sesuai standard keamanan.
Frekuensi	Setiap ada pengembangan website atau aplikasi ITS yang membutuhkan penginputan *password*
Indikator keberhasialan	Seluruh aplikasi maupun website milik ITS menerapkan panduan tersebut.
Notifikasi Mengganti *Password* secara Berkala	
Media Penyampaian	Kebijakan
Media penyebaran	Seluruh website dan aplikasi milik ITS
Tujuan	Agar mahasiswa mengingat pentingnya mengganti *password* secara berkala
Topik	Manajemen *password*.
Target/Penerima	Pihak pengembang aplikasi dan website ITS
Peran dan tanggung jawab	- DPTSI : membuat kebijakan jika seluruh aplikasi dan website milik ITS harus menampilkan notifikasi sebagai pengingat untuk mengganti *password*. - Pengelola website atau aplikasi di bawah naungan ITS : mnambahkan fitur notifikasi sebagai pengingat mahasiswa untuk mengganti *password* secara berkala.
Deskripsi	- Menambahkan fitur notifikasi atau pengingat kepada mahasiswa untuk mengganti *password* secara berkala sesuai dengan waktu yang telah ditentukan. - Waktu default diatur misal setiap 3 bulan sekali. Notifikasi akan muncul sampai mahasisiwa mengganti *password*.
Frekuensi	Setiap ada pengembangan website atau aplikasi ITS yang membutuhkan penginputan *password*
Indikator keberhasialan	Seluruh aplikasi maupun website milik ITS menerapkan notifikasi tersebut.

Fitur Pendeteksi *Password*	
Media Penyampaian	Kebijakan
Media penyebaran	Seluruh website dan aplikasi milik ITS
Tujuan	Agar mahasiswa memiliki *password* yang aman untuk akun penting yang menunjang perkuliahan.
Topik	Manajemen *Password*
Target/Penerima	Pihak pengembang aplikasi dan website ITS
Peran dan tanggung jawab	- DPTSI : membuat kebijakan jika seluruh aplikasi dan website milik ITS harus menerapkan fitur pendeteksi kekuatan *password*, dengan persetujuan Warek III. - Pengelola Aplikasi / Website : menambahkan fitur pendeteksi kekuatan *password* .
Deskripsi	- Menambahkan fitur pendeteksi kekuatan *password* untuk menjamin *password* yang dibuat oleh mahasiswa merupakan kombinasi yang sesuai dengan standard pembuatan *password.* - Mahasiswa tidak akan sukses membuat akun jika *password* belum mencapai status *password* yang kuat.
Frekuensi	Setiap ada pengembangan website atau aplikasi ITS yang membutuhkan penginputan *password*
Indikator keberhasialan	Seluruh aplikasi maupun website milik ITS menerapkan fitur pendeteksi *password*..
Fitur Mengganti *Password* secara Berkala	
Media Penyampaian	Kebijakan
Media penyebaran	Seluruh website dan aplikasi milik ITS
Tujuan	Agar mahasiswa mengganti *password* secara berkala.
Topik	Manajemen *Password*
Target/Penerima	Pihak pengembang aplikasi dan website ITS

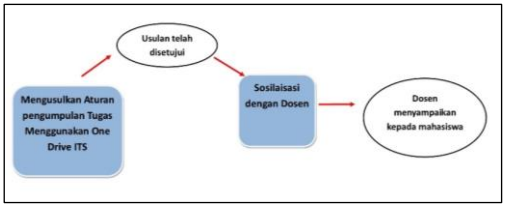
169

Peran dan tanggung jawab	- DPTSI : membuat kebijakan jika seluruh aplikasi dan website milik ITS harus menerapkan fitur fitur yang mengharuskan mahasiswa mengganti *password*., dengan persetujuan Warek III. - Pengelola Aplikasi / Website : menambahkan fitur fitur yang mengharuskan mahasiswa mengganti *password*.
Deskripsi	- Menambahkan fitur yang mengharuskan mahasiswa mengganti *password* secara berkala. - Waktu default diatur misal setiap 3 bulan sekali. - Jika *password* belum diganti, mahasiswa tidak dapat mengakses aplikasi tersebut. - Sebaiknya menerapkan sistem Single Sign-On terlebih dahulu untuk seluruh aplikasi atau website yang dibawah naungan institusi agar mahasiswa tidak memiliki banyak passwor untuk menghindari lupa *password* sehingga mahasiswa tidak sulit mengingat *password* yang dimiliki.
Frekuensi	Setiap ada pengembangan website atau aplikasi ITS yang membutuhkan penginputan *password*
Indikator keberhasialan	Seluruh aplikasi maupun website milik ITS menerapkan fitur yang mengharuskan mahasiswa mengganti *password*.

b. Aturan Penggunaan *One Drive* ITS

ITS telah berlangganan *One Drive* dari Microsoft yang disediakan untuk memfasilitasi mahasiswa. *Backup data* merupakan salah satu topik yang belum terlalu disadari oleh mahasiswa ITS, untuk itu sebagai upaya meningkatkan kesadaran keamanan informasi mahasiswa terkait melakukan *backup data*, maka dibuat aturan pengumpulan tugas dengan

memanfaatkan cloud storage yang telah difasilitasi oleh ITS. Selain mengubah perilaku mahasiswa dalam melakukan *backup data*, usulan ini juga dapat memperkenalkan *One Drive* ITS kepada seluruh mahasiswa ITS, dikarenakan pengetahuan terkait *One Drive* belum diketahui mahasiswa secara keseluruhan. Berikut merupakan alur pelaksanaan kegiatan terkait aturan pengumpulan tugas menggunakan *One Drive* ITS.



Gambar 0.12 Alur pelaksanaan rekomendasi 6 (2)

Untuk detail informasi rekomendasi sdapat dilihat pada tabel berikut.

Tabel 0.25 Detail informasi rekomendasi 6 (2)

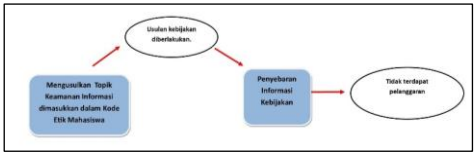
Aturan Penggunaan *One Drive* ITS	
Catatan : - DPTSI membentuk tim pelaksana dan membagi PJ untuk setiap bentuk kegiatan.	
Mengusulkan Aturan Pengumpulan Tugas menggunakan *One Drive* ITS	
Media Penyampaian	Kebijakan
Media penyebaran	*Cloud Storage (One Drive ITS)*
Tujuan	- Agar mahasiswa terbiasa menyimpan file atau dokumen di penyimpanan lain seperti (*cloud storage*).

	- Mensosialisasikan *One Drive* ITS kepada seluruh mahasiswa.
Topik	*Backup data*
Target/Penerima	Dosen dan Mahasiswa ITS
Deskripsi	DPTSI mengusulkan kebijakan terkait pengumpulan tugas menggunakan *One Drive* ITS. Kebijakan tersebut harus diterapkan oleh seluruh dosen yang ada di ITS. Setelah kebijakan disetujui selanjutnya dilakukan sosialisasi kepada seluruh dosen di ITS secara bertahap.
Frekuensi	1x
Peran dan tanggung jawab	- PJ kegiatan (DPTSI) : mengusulkan aturan tentang mewajibkan mahasiswa untuk mengumpulkan tugas menggunakan *One Drive* ITS dengan persetujuan Wakil Rektor 1 melalui Direktorat Akademik. - Kepala Program Studi : mengintruksi dosen untuk membuat aturan pengumpulan tugas menggunakan *One Drive ITS*. - Dosen ITS : memberikan instruksi kepada mahasiswa untuk mengumpulkan tugas pada *One Drive ITS*.
Indikator keberhasialan	Kebijakan disetujui.
Sosialisasi Dosen	
Media Penyampaian	Workshop
Tujuan	Untuk memberikan pemahaman kepada dosen terkait aturan pengumpulan tugas menggunakan *One Drive* ITS.
Topik	*Backup data*
Target/Penerima	Dosen ITS
Deskripsi	Kegiatan sosialisasi ini bertujuan untuk memberikan pemahaman dan tutorial secara langsung terkait penggunaan *One Drive* ITS, serta memberikan pengumuman terkait kebijakan aturan pengumpulan tugas menggunakan *One Drive* ITS.
Frekuensi	1x secara bertahap.

Peran dan tanggung jawab	- PJ Kegiatan (DPTSI) membuat surat edaran terkait sosialisasi kepada Kepala Departemen. - Kepala Departemen : menyebarkan surat edaran.
Indikator keberhasialan	Lebih dari 50% dosen dari tiap departemen mengikuti workshop.

c. Kode Etik Keamanan Informasi

Sebuah aturan yang mengikat dan adanya sanksi dapat digunakan sebagai langkah memperbaiki perilaku dikarenakan memberikan rasa takut sehingga mahasiswa tidak akan melakukan perilaku menyimpang. Kode Etik merupakan peraturan atau undang-undang yang mengikat, yang berarti terdapat konsekuensi dari adanya sebuah tindakan yang salah. Dengan adanya peraturan tersebut akan membuat mahasiswa bertindak dan mematuhi aturan terkait keamanan informasi, sehingga akan mengurangi masalah terkait keamanan informasi. Berikut merupakan alur pelaksanaan kegiatan terkait perumusan peraturan tentang keamanan informasi pada Kode Etik Mahasiswa ITS.



Gambar 0.13 Alur pelaksanaan rekomendasi 8

Untuk detail informasi rekomendasi sdapat dilihat pada tabel berikut.

Tabel 0.26Detail informasi rekomendasi 8

Kode Etik Keamanan Informasi	
Catatan : - DPTSI membentuk tim pelaksana dan membagi PJ untuk setiap bentuk kegiatan. - Topik yang diusulkan adalah penggunaan internet, namun dapat ditambah dengan topik keamanan informasi lainnya.	
Merumuskan Kode Etik Keamanan Informasi	
Media Penyampaian	Kebijakan / Aturan
Media penyebaran	UU Kode Etik Mahasiswa ITS Integra ITS
Tujuan	Meningkatkan perilaku terkait keamanan informasi bagi mahasiswa ITS, agar tidak ada lagi masalah keamanan informasi di lingkungan mahasiswa ITS
Topik	Penggunaan Internet (dapat menambah topik lain, sesuai dengan kebutuhan)
Target/Penerima	
Deskripsi	- Kode Etik tentang Penggunaan Internet dibuat agar mahasiswa berperilaku sesuai dengan yang seharusnya, agar tidak ada lagi kasus tentang penggunaan software bajakan, dan aktivitas menyimpang lainnya. - Aturan adalah salah satu cara yang dapat mengubah perilaku mahasiswa, dikarenakan jika tercantum dalam UU maka mahasiswa yang malanggar akan mendapatkan konsekuensi, sehingga akan memberikan efek jera pada mahasiswa. - Setelah kode etik ditetapkan, selanjutnya kode etik disebarluaskan melalui spanduk dan beranda integra saat akan menggunakan jaringan internet ITS.

Frekuensi	1x
Peran dan tanggung jawab	- PJ Kegiatan (DPTSI) : memberikan usulan untuk memasukkan keamanan informasi dalam UU Kode Etik Mahasiswa pada Direktorat Sumber Daya Manusia, Organisasi. - Direktorat Sumber Daya Manusia, Organisasi : merumuskan kebijakan dengan persetujuan Wakil Rektor Bidang Sumber Daya Manusia, Organisasi, dan Teknologi dan Sistem Informasi (Wakil Rektor III).
Indikator keberhasialan	Kebijakan diberlakukan.
Penyebaran Informasi Kebijkan	
Media Penyampaian	Spanduk, Integra ITS
Tujuan	Menyebarkan informasi terkait kebijakan agar mahasiswa mematuhinya.
Topik	Sesuai dengan UU Kode Etik Keamanan Informasi
Target/Penerima	Seluruh mahasiswa ITS
Deskripsi	Kegiatan ini dilakukan untuk mendukung adanya kebijkan terkait kode etik keamanan informasi agar tersebar luas kepada seluruh mahasiswa ITS. Penyebaran informasi dapat melalui spanduk dan dapat juga ditampilkan pada halaman saat setelah berhasil melakukan akses internet ITS agar mahasiswa tidak menggunakan internet untuk kegiatan yang melanggar atau negatif.
Frekuensi	1x
Peran dan tanggung jawab	- PJ Kegiatan : menyiapkan kebutuhan dan menghubungi pihak pengembang integra, serta bagian saranan prasarana.
Indikator keberhasialan	Spanduk berhasil dipasang, kode etik ditampilkan pada halaman hak akses internet ITS.

175

Beberapa rekomendasi yang telah dijelaskan bukan merupakan kegiatan yang harus dilaksanakan secara berurutan. Namun dalam satu kategori kegiatan, yang telah dijelakan alur pelaksanaannya harus dilakukan secara berurutan sesui dengan gambar dari alur yang telah ditunjukkan. Rekomendasi harus dilaksanakan mulai dari memberikan pengetahuan, mempengaruhi sikap, dan selanjutnya mempengaruhi perilaku.

BAB VII KESIMPULAN DAN SARAN

Bab ini menjelaskan kesimpulan dari penelitian, beserta saran yang dapat dimanfaatkan untuk perbaikan pada penelitian selanjutnya.

7.1. Kesimpulan

1. Seberapa besar tingkat kesadaran keamanan informasi mahasiswa ITS berdasarkan area dan dimensi kesadaran keamanan informasi dari skala 0-100 % ?
   Berdasarkan hasil rata-rata untuk presentase kesadaran keamanan informasi untuk tiap area keamanan informasi yang telah dipilih, menunjukkan bahwa tingat kesadaran mahasiswa ITS secara keseluruhan berada pada nilai 72% yang berarti mahasisiwa ITS cukup sadar akan keamanan informasi, namun masih berpotensi membutuhkan tindakan untuk meningkatkan kesadaran keamanan informasi.
2. Apa saja topik keamanan informasi yang harus ditindak lanjuti agar mahasiswa lebih sadar mengenai keamanan informasi ?
   Berdasarkan penilaian kesadaran keamanan informasi untuk tiap area keamanan informasi dan beserta dimensi yang membentuk kesadaran keamanan informasi didapatkan bahwa hanya ada satu area yang bernilai baik (tidak membutuhkan tindakan), yaitu penggunaan email. Untuk area yang bernilai buruk yaitu area manajemen *password*. Sedangkan untuk kedelapan area lainnya bernilai sedang yang berarti berpotensi membutuhkan tindakan. Dari kedelapan area yang bernilai sedang, terdapat dua area yang salah satu dimensi kesadaran nya bernilai buruk, yaitu area *backup data* untuk dimensi pengetahuan dan area penggunaan internet untuk dimensi perilaku.
   Dari hasil tersebut, maka area keamanan informasi yang dapat dijadikan sebagai topik usulan rekomendasi dalam meningkatkan kesadaran keamanan informasi adalah area manajemen *password*, *backup data*, penggunaan internet,

penggunaan media sosial, keamanan perangkat mobile, malware, pelaporan insiden, penanganan informasi, dan *social engineering*.

3. Apa saja usulan kegiatan yang dapat dilakukan agar dapat mendorong kesadaran mahasiswa akan pentingnya keamanan informasi ?
   Berdasarkan hasil pengukuran tingkat kesadaran keamanan informasi dan identifikasi kondisi *existing*, didapatkan enam kategori kegiatan yaitu menyebarkan informasi tentang keamanan informasi melalui media sosial dan aplikasi milik ITS, sosialisasi melalui kegiatan mahasiswa baru, mengusulkan materi keamanan informasi pada kurikulum mata kuliah umum Wawasan Dan Aplikasi Teknologi (Wastek), menyebarkan pesan peringatan, ITS *Cyber Security Month*, dan membuat kebijakan keamanan informasi. Dari ke-enam rekomendasi tersebut terdapat beberapa kegiatan di dalamnya.

7.2 Saran

Adapun saran yang dapat disampaikan penulis untuk penelitian selanjutnya :

a. Hasil dari penelitian ini hanya berupa usulan rekomendai yang dirancang peneliti , tidak sampai pada validasi untuk membuat program kerja yang harus dilakukan oleh pihak DPTSI. Untuk penelitian selanjutnya dapat dibuat program dengan mengidentifikasi leih dalam terkait program kerja DPTSI.
b. Penilaian efektifitas media sosial tidak dilakukan secara langsung dengan mahasiswa, tetapi menggunakan studi literatur dan berdasrkan pendapat *expert judgement*. Untuk penelitian selanjutnya dapat dilakukan analisis efektifitas media yang dilakukan langsung kepada mahasiswa.
c. Dapat dilakukan penilaian kesadaran keamanan informasi untuk warga ITS lainnya, seperti dosen, dan tenaga pendidik, sehingga dapat dilakukan tindakan untuk seluruh warga ITS

DAFTAR PUSTAKA

[1] APJII, "Penetrasi & Perilaku Pengguna Internet Indonesia," *APJII*, p. Hasil Survey, 2017.

[2] B. Rahardjo, "Keamanan Informasi," 2014.

[3] Government UK, "Cyber security breaches survey (technical report)," 2017.

[4] KOMINFO, "Kesadaran Keamanan Siber Di Masyarakat Masih Rendah," 2017.

[5] R. Akraman and Y. Priyadi, "Pengukuran Kesadaran Keamanan Informasi dan Privasi Pada Pengguna Smartphone Android di Indonesia," vol. 02, pp. 115–122, 2018.

[6] A. Ghazvini and Z. Shukur, "A Framework for an Effective Information Security Awareness Program in Healthcare," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 2, pp. 193–205, 2017.

[7] A. Ghazvini and Z. Shukur, "An Effective Awareness Training Program for Information Security in Hospital Universiti Kebangsaan Malaysia (HUKM)," *J. Next Gener. Inf. …*, vol. 6, no. 3, pp. 1–12, 2015.

[8] A. Ghazvini and Z. Shukur, "Awareness Training Transfer and Information Security Content Developmentfor Healthcare Industry," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 5, pp. 361–370, 2016.

[9] A. Ghazvini and Z. Shukur, "Information Security Content Development for Awareness Training Programs in Healthcare," *Int. J. Secur. Its Appl.*, vol. 11, no. 7, pp. 875–896, 2017.

[10] Shafwan, "Desain Program Kepedulian Keamanan Informasi pada Perusahaan X," 2008.

[11] A. Tsohou, M. Karyda, and S. Kokolakis, "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs," *Comput. Secur.*,

vol. 52, pp. 128–141, 2015.

[12] A. Gandhi, “Quantitative Assessment of Information Security Awareness on Informatics Students in a University,” pp. 346–350, 2018.

[13] M. Hassanzadeh, N. Jahangiri, and B. Brewster, *A Conceptual Framework for Information Security Awareness, Assessment, and Training*. Elsevier Inc., 2013.

[14] “National Security National Training Standard for Information Systems (NSNTSIS),” no. 4011, 1994.

[15] “Public Law 107 – 347 107th Congress An Act,” *Electron. Gov.*, pp. 2899–2970, 2003.

[16] Information Security Forum (ISF), “Effective Security Awareness,” no. April, 2002.

[17] M. Wilson and J. Hash, “Building an Information Technology Security Awareness and Training Program (National Institute of Standards and Technology),” *Organization*, vol. 2, no. 2, pp. 25–42, 2002.

[18] I. Veseli, “Measuring the effectiveness of information security awareness training,” 2007.

[19] K. Kruger, “A prototype for assessing information security awareness,” *Comput. Secur.*, vol. 25, no. 8, pp. 289–296, 2006.

[20] T. Baranowski *et al.*, “Are Current Health Behavioral Change Models Helpful in Guiding Prevention of Weight Gain Efforts ?,” 2003.

[21] Oxford, “Oxford Dictionaries.”

[22] A. Sarmento, “Knowledge management: at a cross-way of perspectives and approaches,” *Inf. Resour. Manag. J.*, vol. 18, no. 1, p. I, 2005.

[23] B. Khan, K. S. Alghathbar, S. I. Nabi, and M. K. Khan, “Effectiveness of information security awareness methods based on psychological theories,” vol. 5, no. 26, pp. 10862–10868, 2011.

[24] P. Belsis, S. Kokolakis, and E. A. Kiountouzis, “Information systems security from a knowledge management perspective,” *Inf. Manag. Comput. Secur.*, vol. 13, pp. 189–202, 2005.

[25] L. Tsui, S. A. Chapman, L. Schnirer, and S. Stewart, “A Handbook on Knowledge Sharing : Strategies and Recommendations for Researchers , Policymakers , and Service Providers,” *Community-University Partnersh. Study Child. Youth, Fam.*, pp. 1–43, 2006.

[26] M. Bada, “Cyber Security Awareness Campaigns - Why they fail to change behavior.pdf,” no. July, 2014.

[27] P. Dolan, D. Halpern, M. Hallsworth, D. King, and I. Vlaev, “Influencing behaviour through public policy,” *Inst. Gov. Cabinet Off.*, 2010.

[28] “MEDIA LITERACY TOOLBOX Media Literacy Concepts & Skills The Language of Persuasion,” 2007.

[29] M. King, “SANS Institute InfoSec Reading Room - Security Awareness - Implementing an Effective Strategy.”

[30] K. Lewis, “Information Supplement : Best Practices for Implementing a Security Awareness Program,” *Secur. Stand. Counc.*, no. October, 2014.

[31] C. M. F. Dominguez, M. Ramaswamy, E. M. Martinez, and M. G. Cleal, “A framework for information security awareness programs,” *Inf. Syst.*, vol. 11, no. 1, pp. 402–409, 2010.

[32] European Union Agency For Network and Information Security, *European Cyber Security Month 2017*, no. February. 2018.

[33] P. van D. Chris Connolly, Alana Maurushat, David Vaile, “An overview of international cyber-security awareness raising and educational initiatives Research report commissioned by the Australian Communications and Media Authority,” no. May, 2011.

[34] C. C. Fung, S. M. Ieee, V. Khera, M. Ieee, and A. Depickere,

181

"Raising Information Security Awareness in Digital Ecosystem with Games – a Pilot Study in Thailand," pp. 375–380, 2010.

[35] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue , participation and collective reflection . An intervention study," *Comput. Secur.*, vol. 29, no. 4, pp. 432–445, 2010.

[36] ISACA, "Security Awareness-Best Practices to Serve Your Enterprise," 2015.

[37] "Tentang DPTSI." [Online]. Available: https://www.its.ac.id/dptsi/id/tentang-dptsi/.

[38] A. A. Farhani, "Persepsi Bobotoh Persib Bandung Tentang Perilaku Kekerasan Penonton Pada Pertandingan Sepakbola Di Stadion Jalak Harupat Universitas Pendidikan Indonesia," 2014.

[39] U. Horizon, "HIPAA Privacy & Security Awareness Training for Students," no. February, 2010.

[40] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Comput. Secur.*, vol. 66, pp. 40–51, 2017.

[41] C. M. University, "Information Security Office Guidance - Password Managers." [Online]. Available: https://www.cmu.edu/iso/governance/guidance/password-managers.html.

[42] SANS Security, "Security Awareness Topik - Passwords." [Online]. Available: https://www.sans.org/security-awareness-training/blog/security-awareness-topic-6-passwords.

[43] ISO/IEC, "INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Code of practice for information security controls," vol. 2013, 2013.

[44] M. Luehr, "The Perfect Guide to Backup 5 Keys to Build a Better Backup Strategy for Imperfect Humans The biggest

data loss risk is right in front of you," pp. 1–7.

[45] P. Ruggiero and M. A. Heckathorn, "Data Backup Options," pp. 1–6, 2012.

[46] Yoga Ari Tofan, "Panduan Instalasi dan Penggunaan OneDrive For Business untuk Civitas ITS." [Online]. Available: https://www.its.ac.id/dptsi/id/2018/08/07/tutorial-instalasi-dan-penggunaan-onedrive-business-untuk-civitas/.

[47] Phoenix Group, "DOS AND DON ' TS ON THE INTERNET," no. July, 2017.

[48] The USSA Educational Foundation, "Internet Safety for Adults."

[49] Ruskwig, "Internet Acceptable Use Policy User Responsibilities," 1990.

[50] K. Siau and F. F. Nah, "Acceptable Internet use policy," no. January, 2002.

[51] N. Aldhafferi, C. Watson, and A. S. M. Sajeev, "P ERSONAL I NFORMATION P RIVACY S ETTINGS OF O NLINE S OCIAL N ETWORKS AND T HEIR," vol. 2, no. 2, pp. 1–17, 2013.

[52] National Computer Board, "Mobile Devices Security Guideline," no. 1, pp. 1–36, 2011.

[53] OCSF Information Security Office, "MAINTAINING THE PHYSICAL SECURITY OF INFORMATION," no. September, p. 2010, 2010.

[54] M. Sujithra, "Mobile Device Security : A Survey on Mobile Device Threats , Vulnerabilities and their Defensive Mechanism," vol. 56, no. 14, pp. 24–29, 2012.

[55] K. Scarfone, "NIST Special Publication 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops NIST Special Publication 800-83 Guide to Malware Incident Prevention and Handling for Desktops and Laptops."

[56] W. I. S. A. Cyberattack, "Cyber-attack Threat Methodologies," pp. 2–4.

183

[57] D. Salmon, *Foundations of Computer Security*. .

[58] F. Salahdine, “Social Engineering Attacks : A Survey as,” 2019.

[59] SANS Security, “National Cyber Security Awareness Month,” 2018.

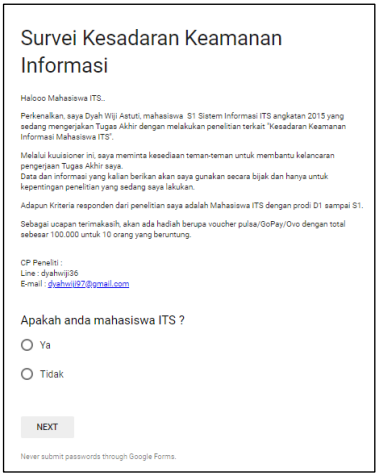
[60] U. of Toronto, “Cyber Security Awareness Month.” [Online]. Available: https://main.its.utoronto.ca/news/cyber-security-a.

BIODATA PENULIS

Penulis bernama Dyah Wiji Astuti yang biasa dikenal dengan Dyah dikalangan teman-temannya. Penulis lahir di Tulungagung pada tanggal 11 Juni 1997. Penulis merupakan anak pertama dari dua bersaudara. Penulis telah menempuh pendidikan formal di SDN 2 Wates, SMPN 1 Campurdarat, SMAN 1 Kedungwaru, dan saat ini sedang menempuh pendidikan di Departemen Sistem Informasi ITS Surabaya. Penulis masuk ITS menjadi angkatan 2015 melalui jalur SNMPTN dengan NRP 05211540000036. Selama perkuliahan penulis aktif di berbagai kegiatan organisasi dan kepanitiaan acara, diantaranya Himpunan Mahasiswa Sistem Informasi (HMSI), BEM FTIK,panitia ISE, panitia FTIF Festival, panitia Gemastik, dan sebagainya. Dan di akhir masa perkuliahan, penulis memilih topik Tugas Akhir pada bidang minat lab Manajemen Sistem Informasi (MSI). Jika terdapat pertanyaan mengenai Tugas Akhir ini, dapat menghubungi penulis pada email : dyahwiji97@gmail.com.

Halaman ini sengaja dikosongkan

LAMPIRAN A- BENTUK KUESIONER PENELITIAN



Survei Kesadaran Keamanan Informasi

Halooo Mahasiswa ITS..

Perkenalkan, saya Dyah Wiji Astuti, mahasiswa S1 Sistem Informasi ITS angkatan 2015 yang sedang mengerjakan Tugas Akhir dengan melakukan penelitian terkait "Kesadaran Keamanan Informasi Mahasiswa ITS".

Melalui kuuisioner ini, saya meminta kesediaan teman-teman untuk membantu kelancaran pengerjaan Tugas Akhir saya.
Data dan informasi yang kalian berikan akan saya gunakan secara bijak dan hanya untuk kepentingan penelitian yang sedang saya lakukan.

Adapun Kriteria responden dari penelitian saya adalah Mahasiswa ITS dengan prodi D1 sampai S1.

Sebagai ucapan terimakasih, akan ada hadiah berupa voucher pulsa/GoPay/Ovo dengan total sebesar 100.000 untuk 10 orang yang beruntung.

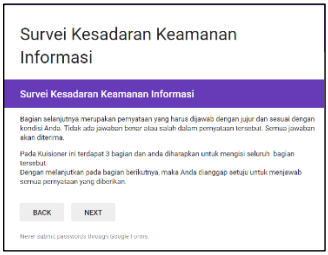
CP Penelti :
Line : dyahwiji36
E-mail : dyahwiji97@gmail.com

Apakah anda mahasiswa ITS ?

- Ya
- Tidak

NEXT

Never submit passwords through Google Forms.



Survei Kesadaran Keamanan Informasi

Survei Kesadaran Keamanan Informasi

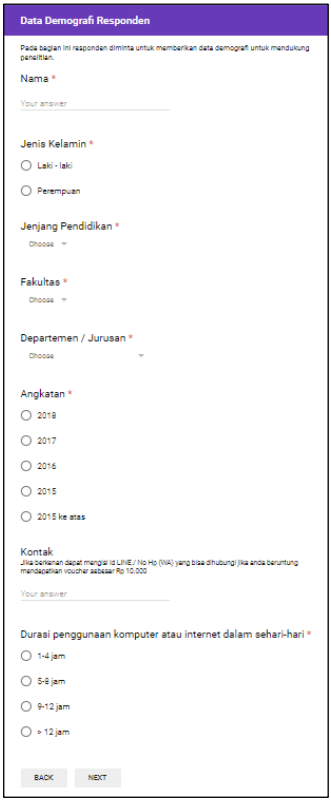
Bagian selanjutnya merupakan pernyataan yang harus dijawab dengan jujur dan sesuai dengan kondisi Anda. Tidak ada jawaban benar atau salah dalam pernyataan tersebut. Semua jawaban akan diterima.

Pada Kuisioner ini terdapat 3 bagian dan anda diharapkan untuk mengisi seluruh bagian tersebut.
Dengan melanjutkan pada bagian berikutnya, maka Anda dianggap setuju untuk menjawab semua pernyataan yang diberikan.

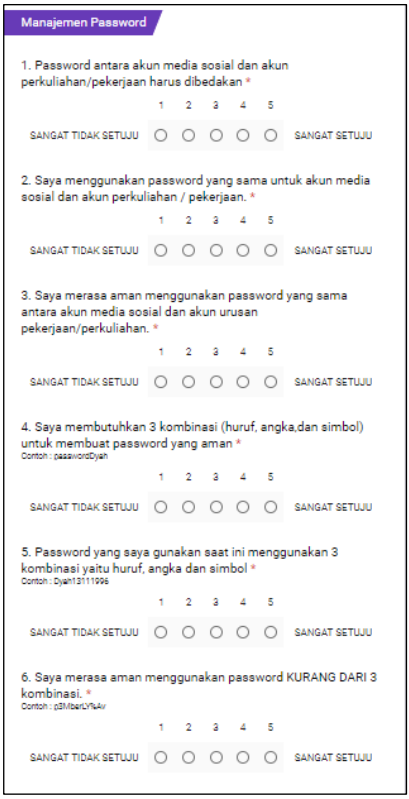
BACK NEXT

Never submit passwords through Google Forms.

Gambar. A.1Form Kuesioner (1)

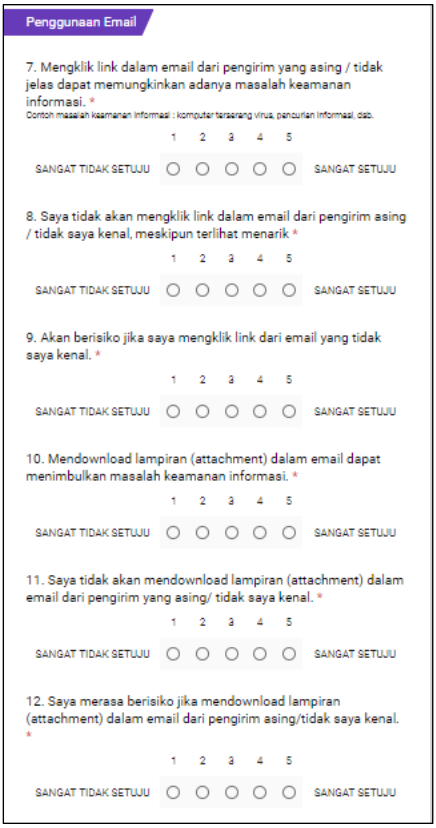


Gambar. A.2 Form Kuesioner (2)



Gambar. A.3 Form Kuesioner (3)

189



Penggunaan Email

7. Mengklik link dalam email dari pengirim yang asing / tidak jelas dapat memungkinkan adanya masalah keamanan informasi. *
Contoh masalah keamanan informasi : komputer terserang virus, pencurian informasi, dsb.

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

8. Saya tidak akan mengklik link dalam email dari pengirim asing / tidak saya kenal, meskipun terlihat menarik *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

9. Akan berisiko jika saya mengklik link dari email yang tidak saya kenal. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

10. Mendownload lampiran (attachment) dalam email dapat menimbulkan masalah keamanan informasi. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

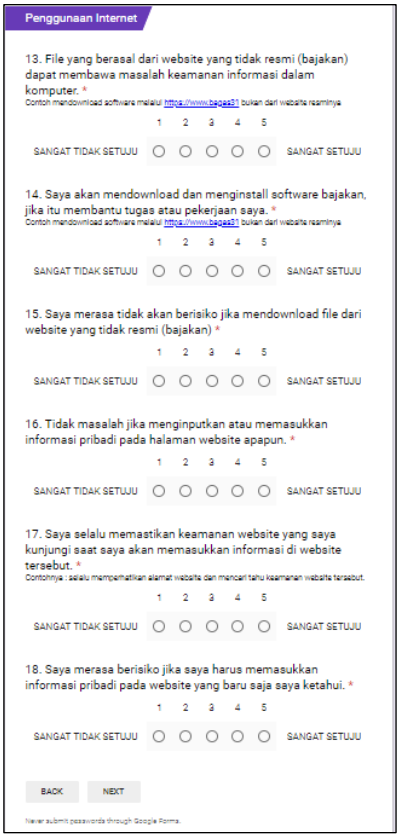
11. Saya tidak akan mendownload lampiran (attachment) dalam email dari pengirim yang asing/ tidak saya kenal. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

12. Saya merasa berisiko jika mendownload lampiran (attachment) dalam email dari pengirim asing/tidak saya kenal. *

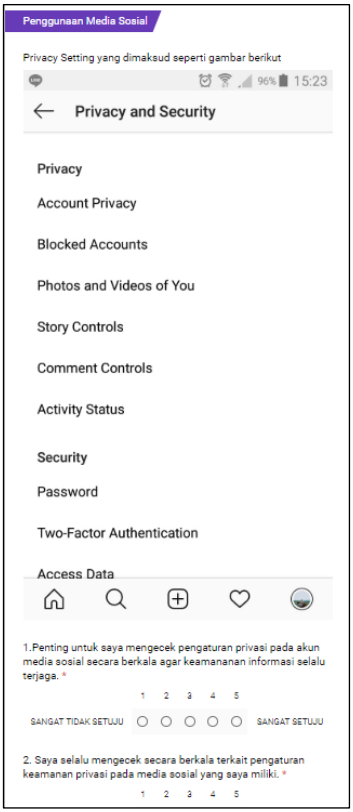
	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

Gambar. A.4 Form Kuesioner (4)

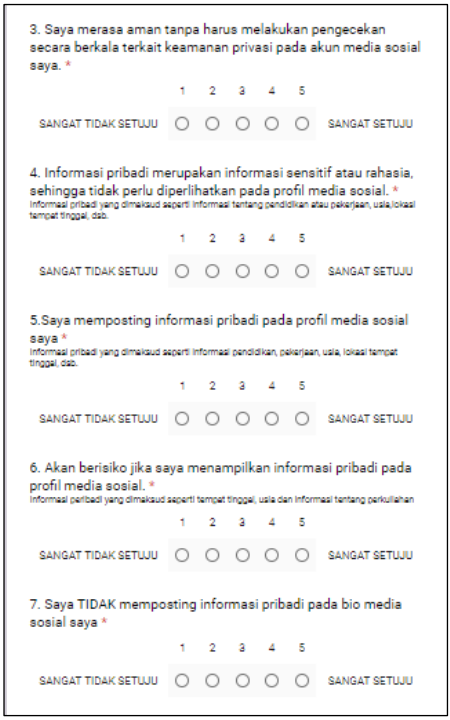


Gambar. A.5 Form Kuesioner (5)

191

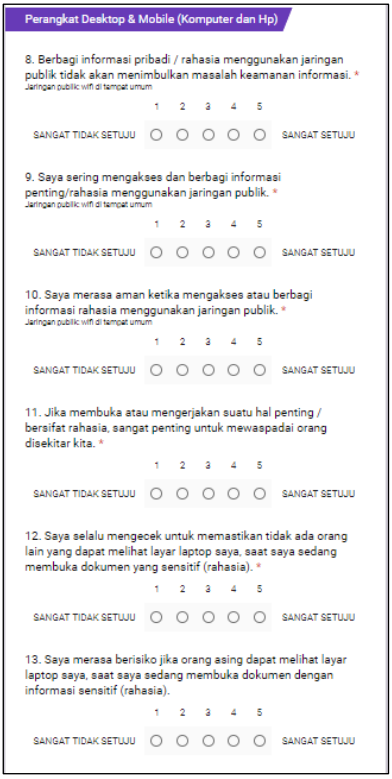


Gambar. A.6 Form Kuesioner (6)

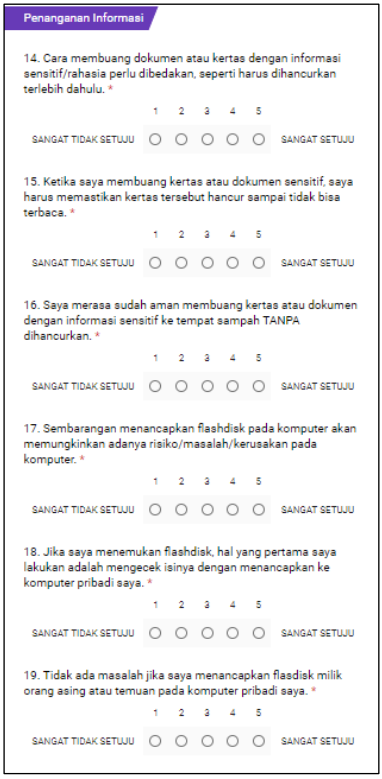


Gambar. A.7 Form Kuesioner *(7)*

193



Gambar. A.8 Form Kuesioner (8)



Penanganan Informasi

14. Cara membuang dokumen atau kertas dengan informasi sensitif/rahasia perlu dibedakan, seperti harus dihancurkan terlebih dahulu. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

15. Ketika saya membuang kertas atau dokumen sensitif, saya harus memastikan kertas tersebut hancur sampai tidak bisa terbaca. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

16. Saya merasa sudah aman membuang kertas atau dokumen dengan informasi sensitif ke tempat sampah TANPA dihancurkan. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

17. Sembarangan menancapkan flashdisk pada komputer akan memungkinkan adanya risiko/masalah/kerusakan pada komputer. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

18. Jika saya menemukan flashdisk, hal yang pertama saya lakukan adalah mengecek isinya dengan menancapkan ke komputer pribadi saya. *

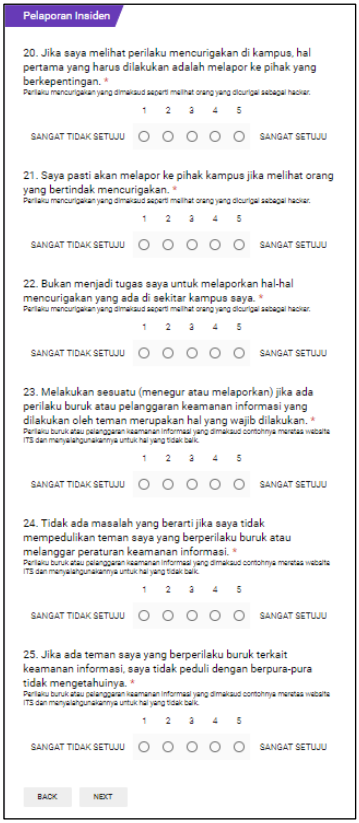
	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

19. Tidak ada masalah jika saya menancapkan flasdisk milik orang asing atau temuan pada komputer pribadi saya. *

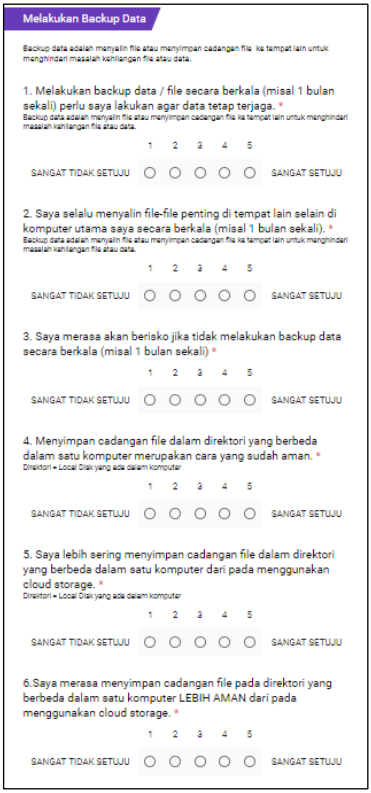
	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

Gambar. A.9 Form Kuesioner (9)

195



Gambar. A.10 Form Kuesioner (10)



Melakukan Backup Data

Backup data adalah menyalin file atau menyimpan cadangan file ke tempat lain untuk menghindari masalah kehilangan file atau data.

1. Melakukan backup data / file secara berkala (misal 1 bulan sekali) perlu saya lakukan agar data tetap terjaga. *
Backup data adalah menyalin file atau menyimpan cadangan file ke tempat lain untuk menghindari masalah kehilangan file atau data.

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

2. Saya selalu menyalin file-file penting di tempat lain selain di komputer utama saya secara berkala (misal 1 bulan sekali). *
Backup data adalah menyalin file atau menyimpan cadangan file ke tempat lain untuk menghindari masalah kehilangan file atau data.

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

3. Saya merasa akan berisko jika tidak melakukan backup data secara berkala (misal 1 bulan sekali) *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

4. Menyimpan cadangan file dalam direktori yang berbeda dalam satu komputer merupakan cara yang sudah aman. *
Direktori = Local Disk yang ada dalam komputer

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

5. Saya lebih sering menyimpan cadangan file dalam direktori yang berbeda dalam satu komputer dari pada menggunakan cloud storage. *
Direktori = Local Disk yang ada dalam komputer

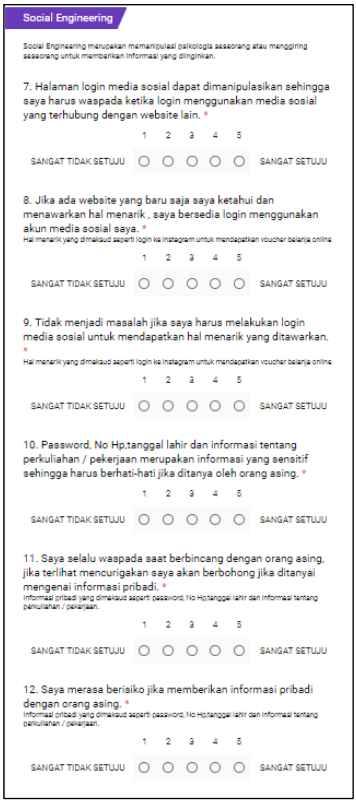
	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

6.Saya merasa menyimpan cadangan file pada direktori yang berbeda dalam satu komputer LEBIH AMAN dari pada menggunakan cloud storage. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

Gambar. A.11 Form Kuesioner (11)

197



Social Engineering

Social Engineering merupakan memanipulasi psikologis seseorang atau menggiring seseorang untuk memberikan informasi yang diinginkan.

7. Halaman login media sosial dapat dimanipulasikan sehingga saya harus waspada ketika login menggunakan media sosial yang terhubung dengan website lain. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

8. Jika ada website yang baru saja saya ketahui dan menawarkan hal menarik , saya bersedia login menggunakan akun media sosial saya. *

Hal menarik yang dimaksud seperti login ke Instagram untuk mendapatkan voucher belanja online

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

9. Tidak menjadi masalah jika saya harus melakukan login media sosial untuk mendapatkan hal menarik yang ditawarkan. *

Hal menarik yang dimaksud seperti login ke Instagram untuk mendapatkan voucher belanja online

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

10. Password, No Hp,tanggal lahir dan informasi tentang perkuliahan / pekerjaan merupakan informasi yang sensitif sehingga harus berhati-hati jika ditanya oleh orang asing. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

11. Saya selalu waspada saat berbincang dengan orang asing. jika terlihat mencurigakan saya akan berbohong jika ditanyai mengenai informasi pribadi. *

Informasi pribadi yang dimaksud seperti password, No Hp,tanggal lahir dan informasi tentang perkuliahan / pekerjaan.

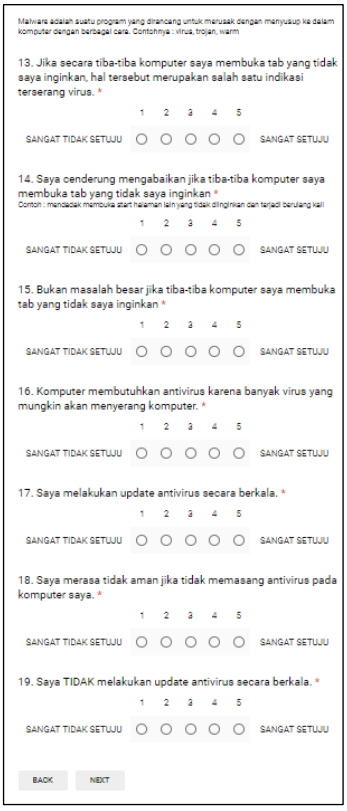
	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

12. Saya merasa berisiko jika memberikan informasi pribadi dengan orang asing. *

Informasi pribadi yang dimaksud seperti password, No Hp,tanggal lahir dan informasi tentang perkuliahan / pekerjaan.

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

Gambar. A.12 Form Kuesioner (12)



Malware adalah suatu program yang dirancang untuk merusak dengan menyusup ke dalam komputer dengan berbagai cara. Contohnya : virus, trojan, warm

13. Jika secara tiba-tiba komputer saya membuka tab yang tidak saya inginkan, hal tersebut merupakan salah satu indikasi terserang virus. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

14. Saya cenderung mengabaikan jika tiba-tiba komputer saya membuka tab yang tidak saya inginkan *
Contoh : mendadak membuka start halaman lain yang tidak diinginkan dan terjadi berulang kali

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

15. Bukan masalah besar jika tiba-tiba komputer saya membuka tab yang tidak saya inginkan *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

16. Komputer membutuhkan antivirus karena banyak virus yang mungkin akan menyerang komputer. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

17. Saya melakukan update antivirus secara berkala. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

18. Saya merasa tidak aman jika tidak memasang antivirus pada komputer saya. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

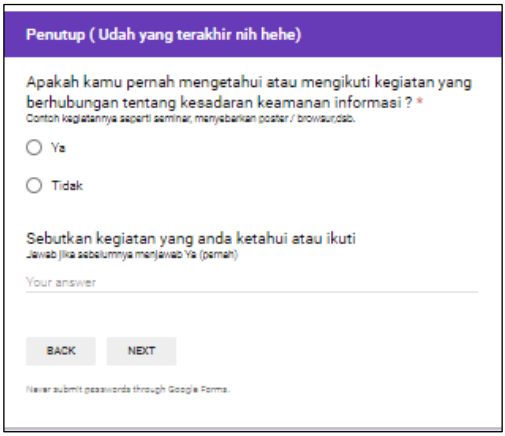
19. Saya TIDAK melakukan update antivirus secara berkala. *

	1	2	3	4	5	
SANGAT TIDAK SETUJU	○	○	○	○	○	SANGAT SETUJU

BACK NEXT

Gambar. A.13 Form Kuesioner (13)

199



Gambar. A.14 Form Kuesioner (14)

LAMPIRAN B-KATEGORI DAN KODE PERNYATAN KUESIONER PENELITIAN

Tabel. B.1 Kategori dan kode pernyataan kuesioner

NO	Sub Area	Dimensi	Kode	Pernyataan	Sumber
MANAJEMEN *PASSWORD*					
1.	Penggunaan *password* untuk berbagai akun.	Knowledge	MP1.01	*Password* antara akun media sosial dan akun perkuliahan/pekerjaan harus dibedakan	Parsons et al
		Behavior	MP1.02	Saya menggunakan *password* yang sama untuk akun media sosial dan akun perkuliahan / pekerjaan.	Parsons et al
		Attitude	MP1.03	Saya merasa aman menggunakan *password* yang sama antara akun media sosial dan akun urusan pekerjaan/perkuliahan.	Parsons et al
2.	Kekuatan *password*	Knowledge	MP2.01	Saya membutuhkan 3 kombinasi (huruf, angka,dan simbol) untuk membuat *password* yang aman.	Parsons et al
		Behavior	MP2.02	*Password* yang saya gunakan saat ini menggunakan 3 kombinasi yaitu huruf, angka dan simbol.	Parsons et al

NO	Sub Area	Dimensi	Kode	Pernyataan	Sumber
		Attitude	MP2.03	Saya merasa aman menggunakan *password* kurang dari 3 kombinasi.	Parsons et al
PENGGUNAAN EMAIL					
1.	Mengklik link dalam email.	Knowledge	PE1.01	Mengklik link dalam email dari pengirim yang asing / tidak jelas dapat memungkinkan adanya masalah keamanan informasi.	Parsons et al
		Behavior	PE1.02	Saya tidak akan mengklik link dalam email dari pengirim yang asing / tidak jelas, meskipun terlihat menarik.	Parsons et al
		Attitude	PE1.03	Akan berisiko jika saya mengklik link dari email yang tidak saya kenal.	Parsons et al
2.	Mendownload lampiran dalam email	Knowledge	PE2.01	Mendownload lampiran (attachment) dalam email yang tidak dikenal dapat memungkinkan timbulnya masalah keamanan informasi.	Parsons et al
		Behavior	PE2.02	Saya tidak akan mendownload lampiran (attachment) dalam email dari pengirim yang tidak jelas/ tidak saya kenal.	Parsons et al

NO	Sub Area	Dimensi	Kode	Pernyataan	Sumber
		Attitude	PE2.03	Saya merasa berisiko jika mendownload lampiran (attachment) dalam email dari pengirim yang tidak jelas.	Parsons et al
PENGGUNAAN INTERNET					
1.	Mendownload file dari internet.	Knowledge	PI1.01	File yang berasal dari website yang tidak resmi (bajakan) dapat membawa masalah keamanan informasi dalam komputer.	Parsons et al
		Behavior	PI1.02	Saya akan mendownload dan menginstall software bajakan, jika itu membantu tugas atau pekerjaan saya.	Parsons et al
		Attitude	PI1.03	Saya merasa akan berisiko jika mendownload file dari website tidak resmi (bajakan)	Parsons et al
2.	Memasukkan informasi secara online.	Knowledge	PI2.01	Tidak masalah jika menginputkan atau memasukkan informasi pribadi pada halaman website apapun.	Parsons et al
		Behavior	PI2.02	Saya selalu memastikan keamanan website yang saya kunjungi saat saya akan	Parsons et al

NO	Sub Area	Dimensi	Kode	Pernyataan	Sumber
				memasukkan informasi di website tersebut.	
		Attitude	PI2.03	Saya merasa aman mendownload file dari website yang tidak resmi (bajakan)	Parsons et al
PENGGUNAAN MEDIA SOSIAL					
1.	Pengecekan pengaturan privasi secara berkala.	Knowledge	MS1.01	Penting untuk saya mengecek pengaturan privasi pada akun media sosial secara berkala.	Parsons et al
		Behavior	MS1.02	Saya selalu mengecek secara berkala terkait pengaturan keamanan privasi pada media sosial yang saya miliki.	Parsons et al
		Attitude	MS1.03	Saya merasa aman tanpa harus melakukan pengecekan secara berkala terkait keamanan privasi pada akun media sosial saya. (bajakan), asalkan membantu pekerjaan saya.	Parsons et al

NO	Sub Area	Dimensi	Kode	Pernyataan	Sumber
2.	Posting tentang informasi pribadi di Media Sosial.	Knowledge	MS2.01	Informasi pribadi merupakan informasi sensitif atau rahasia, sehingga tidak perlu diperlihatkan pada profil media sosial.	Penulis
		Behavior	MS2.02	Saya memposting informasi pribadi pada profil media sosial saya	Penulis
		Attitude	MS2.03	Akan berisiko jika saya menampilkan informasi pribadi pada profil media sosial.	Penulis
KEAMANAN PERANGKAT MOBILE (DESKTOP DAN HANDPHONE)					
1.	Mengirim informasi sensitif melalui jaringan publik	Knowledge	KPM1.01	Berbagi informasi pribadi / rahasia menggunakan jaringan publik tidak akan menimbulkan masalah keamanan informasi.	Parsons et al
		Behavior	KPM1.02	Saya sering mengakses dan berbagi informasi penting/rahasia menggunakan jaringan publik.	Parsons et al
		Attitude	KPM1.03	Saya merasa aman ketika mengakses atau berbagi informasi rahasia menggunakan jaringan publik.	Parsons et al

NO	Sub Area	Dimensi	Kode	Pernyataan	Sumber
2.	Adanya *Shoulder Surfing*.	Knowledge	KPM2.01	Jika membuka atau mengerjakan suatu hal penting yang bersifat rahasia, sangat penting untuk mewaspadai orang disekitar kita.	Parsons et al
		Behavior	KPM2.02	Saya selalu mengecek untuk memastikan tidak ada orang lain yang dapat melihat layar laptop saya, saat saya sedang membuka dokumen yang sensitif (rahasia).	Parsons et al
		Attitude	KPM2.03	Saya merasa berisiko jika orang asing dapat melihat layar laptop saya, saat saya sedang membuka dokumen dengan informasi sensitif (rahasia).	Parsons et al
PENANGANAN INFORMASI					
1.	Membuang kertas / dokumen dengan informasi sensitif	Knowledge	PIF1.01	Cara membuang dokumen atau kertas dengan informasi sensitif/rahasia perlu dibedakan, seperti harus dihancurkan terlebih dahulu.	Parsons et al
		Behavior	PIF1.02	Ketika saya membuang kertas atau dokumen sensitif, saya harus memastikan kertas tersebut hancur sampai tidak bisa terbaca.	Parsons et al

NO	Sub Area	Dimensi	Kode	Pernyataan	Sumber
		Attitude	PIF1.03	Saya merasa sudah aman membuang kertas atau dokumen dengan informasi sensitif ke tempat sampah tanpa dihancurkan.	Parsons et al
2.	Memasukkan media yang ditemukan tanpa sengaja.	Knowledge	PIF2.01	Sembarangan menancapkan flashdisk pada komputer akan memungkinkan adanya risiko/masalah/kerusakan pada komputer.	Parsons et al
		Behavior	PIF2.02	Jika saya menemukan flashdisk, hal yang pertama saya lakukan adalah mengecek isinya dengan menancapkan ke komputer pribadi saya.	Parsons et al
		Attitude	PIF2.03	Tidak ada masalah jika saya menancapkan flasdisk milik orang asing atau temuan pada komputer pribadi saya.	Parsons et al
PELAPORAN INSIDEN					
1.	Melaporkan perilaku mencurigakan	Knowledge	PIN1.01	Jika saya melihat perilaku mencurigakan di kampus, hal pertama yang harus dilakukan adalah melapor ke pihak yang berkepentingan.	Parsons et al

NO	Sub Area	Dimensi	Kode	Pernyataan	Sumber
		Behavior	PIN1.02	Saya pasti akan melapor ke pihak kampus jika melihat orang yang bertindak mencurigakan.	Parsons et al
		Attitude	PIN1.03	Bukan menjadi tugas saya untuk melaporkan hal-hal mencurigakan yang ada di sekitar kampus saya.	Parsons et al
2.	Melaporkan perilaku buruk teman	Knowledge	PIN2.01	Melakukan sesuatu (menegur atau melaporkan) jika ada perilaku buruk atau pelanggaran keamanan informasi yang dilakukan oleh teman merupakan hal yang wajib dilakukan.	Parsons et al
		Behavior	PIN2.02	Tidak ada masalah yang berarti jika saya tidak mempedulikan teman saya yang berperilaku buruk atau melanggar peraturan keamanan informasi.	Parsons et al
		Attitude	PIN2.03	Jika ada teman saya yang berperilaku buruk terkait keamanan informasi, saya tidak peduli dengan berpura-pura tidak mengetahuinya.	Parsons et al
MELAKUKAN *BACKUP DATA*					

NO	Sub Area	Dimensi	Kode	Pernyataan	Sumber
1.	Melakukan *backup data* secara ~~regular~~berkala	Knowledge	BD1.01	Melakukan *backup data* / file secara berkala (misal 1 bulan sekali) perlu saya lakukan agar data tetap terjaga.	Penulis
		Behavior	BD1.02	Saya selalu menyalin file-file penting di tempat lain selain di komputer utama saya secara berkala (misal 1 bulan sekali).	Penulis
		Attitude	BD1.03	Saya merasa akan berisko jika tidak melakukan *backup data* secara berkala (misal 1 bulan sekali)	Penulis
2.	Media *backup data*	Knowledge	BD2.01	Menyimpan cadangan file dalam direktori yang berbeda dalam satu komputer merupakan cara yang sudah aman.	Penulis
		Behavior	BD2.02	Saya lebih sering menyimpan cadangan file dalam direktori yang berbeda dalam satu komputer dari pada menggunakan cloud storage.	Penulis
		Attitude	BD2.03	Saya merasa menyimpan cadangan file pada direktori yang berbeda dalam satu komputer lebih aman dari pada menggunakan cloud storage.	Penulis
SOCIAL ENGINEERING					

NO	Sub Area	Dimensi	Kode	Pernyataan	Sumber
1.	*Phising*	Knowledge	SE1.01	Halaman login media sosial dapat dimanipulasikan sehingga saya harus waspada ketika login menggunakan media sosial yang terhubung dengan website lain.	Penulis
		Behavior	SE1.02	Jika ada website yang baru saja saya ketahui dan menawarkan hal menarik , saya bersedia login menggunakan akun media sosial saya.	Penulis
		Attitude	SE1.03	Tidak menjadi masalah jika saya harus melakukan login media sosial untuk mendapatkan hal menarik yang ditawarkan.	Penulis
2.	Kepercayaan dengan orang lain	Knowledge	SE2.01	*Password*, No Hp,tanggal lahir dan informasi tentang perkuliahan / pekerjaan merupakan informasi yang sensitif sehingga harus berhati-hati jika ditanya oleh orang asing.	Penulis
		Behavior	SE2.02	Saya selalu waspada saat berbincang dengan orang asing, jika terlihat mencurigakan saya akan berbohong jika ditanyai mengenai informasi pribadi.	Penulis

NO	Sub Area	Dimensi	Kode	Pernyataan	Sumber
		Attitude	SE2.03	Saya merasa berisiko jika memberikan informasi pribadi dengan orang asing.	Penulis
MALWARE					
1.	Sumber Malware	Knowledge	MW1.01	Jika secara tiba-tiba komputer saya membuka tab yang tidak saya inginkan, hal tersebut merupakan salah satu indikasi terserang virus.	Penulis
		Behavior	MW1.02	Saya cenderung mengabaikan jika tiba-tiba komputer saya membuka tab yang tidak saya inginkan	Penulis
		Attitude	MW1.03	Bukan maslah besar jika tiba-tiba komputer saya membuka tab yang tidak saya inginkan	
2.	Pencegahan Malware	Knowledge	MW2.01	Saya membutuhkan Antivirus untuk menghindari atau menangani adanya serangan atau masalah keamanan dalam komputer.	Penulis
		Behavior	MW2.02	Saya memasang antivirus pada perangkan komputer saya.	Penulis
		Attitude	MW2.03	Saya merasa tidak aman jika tidang memasang antivirus pada komputer saya.	Penulis

Tabel. B.2 Pernyataan negasi sebagai filter responden

Sub Area	Dimensi	Kode	Pernyataan	Sumber
Posting tentang informasi pribadi di Media Sosial.	Behavior	MS2.04	Saya tidak memposting informasi pribadi pada profil media sosial saya	Penulis
Pencegahan Malware	Behavior	MW2.02	Saya memasang antivirus pada perangkan komputer saya.	Penulis

LAMPIRAN C- DOKUMENTASI

Berikut adalah dokumentasi saat melakukan penyebaran kuesioner kepada mahasiswa ITS.

Gambar. C.1 Media penyebaran link kuesioner

Gambar. C.2 Dokumentasi penyebaran kuesioner

LAMPIRAN D– HASIL *EXPERT* JUDGEMENT

Tabel. D.1 Hasil wawancara Pakar 1

Topik Wawancara	Media penyampaian yang efektif digunakan untuk membentuk pengetahuan, sikap dan perilaku mahasiswa ITS.
Narasumber	Ninda Hayyu, S.Psi
Jabatan	Sub-directorate of Human Resources ITS
Hari, Tanggal pelaksanaan	Jumat, 28 Juni 2019
Tempat	Perpustakaan Lantai 3
Tujuan Wawancara	Melakukan validasi terkait rancangan rekomendasi yang telah dirancang.
Pertanyaan	Apakah benar jika untuk mencapai kesadaran seseorang harus dimulai dari aspek pengetahuan, sikap dan perilaku ?
Jawaban	Perilaku adalah proses terakhir atau hasil luaran dari suatu proses menyadarkan seseorang akan suatu hal. Sebelum perilaku diubah, seseorang harus mengubah pemikiran, perasaan, sikap dan selanjutnya dapat merujuk pada aspek perilaku. Dalam bidang psikologi, tahapan untuk membentuk kesadaran seseorang dikenal dengan istilah kognitif (pemikiran), afektif (perasaan), konasi (sikap), dan psikomotorik (perilaku).
Pertanyaan	Apakah media seperti infografis yang disebarkan melalui media sosial dapat menambah pengetahuan ?
Jawaban	Bisa saja, infografis dengan desain yang menarik dapat menjadi daya tarik untuk orang. Informasi lebih detailnya dapat

	diletakkan di bagian lain, seperti mencantumkan link untuk menuju halaman lain.
Pertanyaan	Apakah artikel yang diletakkan dalam ITS News merupakan media yang cocoku untuk menambah pengetahuan mahasiswa ITS ?
Jawaban	Artikel bisa, akan tetapi saya rasa media seperti ITS News kurang cocok dikarenakan mahasiswa ITS cenderung kurang tertarik dalam mengakses ITS News.
Pertanyaan	Bagaimana jika dibuat kegiatan perlombaan seperti lomba artikel ?
Jawaban	Bisa saja, mahasiswa akan tertarik jika ada hadiah yang menarik.
Pertanyaan	Bagaimana jika dibuat acara seminar dengan target mahasiswa baru yang diwajibkan ?
Jawaban	Bisa, seminar adalah salah satu cara untuk memberikan materi atau isu-isu yang belum banyak diketahui. Untuk informasi lebih detail dapat dibuatkan buku saku yang dibagikan saat seminar. Dengan buku saku tersebut mahasiswa dapat mendalami pengetahuan yang telah disampaikan. Umumnya jumlah maksimal untuk seminar adalah 100 orang.
Pertanyaan	Apakah video yang menunjukkan ancaman dan risiko tentang perilaku yang salah dapat mempengaruhhi perasaan dan mengubah sikap seseorang ?
Jawaban	Video sebenarnya dapat digunakan untuk aspek kognitif (pengetahuan) sampai konasi (sikap) terganttung

215

	konten di dalamnya. Untuk aspek afektif (perasaan) biasanya dengan memberikan testimoni dari orang yang sudah pernah mengalaminya. Untuk aspek konasi biasanya diberikan pesan tersirat didalamnya. Dikarenakan video bukan media yang komunikastif sehingga lebih baik langsung diberikan sikap atau perilaku yang harus dilakukan seperti apa.
Pertanyaan	Apakah poster dapat menjadi media untuk mempengaruhi perasaan dan cara bersikap seseorang?
Jawaban	Poster juga dapat memberikan pengaruh dari segi pemikiran dan sikap seseorang tergantung pesan yang disampaikan. Agar poster dapat dilihat maka desain poster harus menarik dan diletakkan pada tempat yang strategis.
Pertanyaan	Apakah pesan singkat pada spanduk dan video tron dapat memberikan pengaruh sampai dengan aspek konasi (sikap) ?
Jawaban	Spanduk atau *running teks* dapat memberikan pengaruh meskipun tidak banyak. Cara ini sudah dibuktikan dalam penelitian tentang kampanye rokok. Dalam penelitian tersebut terbukti jika masyarakat yang merokok pada daerah yang dipasang spanduk mengalami penurunan. Pesan yang diberikan sebaiknya gunakan kata kerja, seperti " stop", "lakukan", "diam", jangan gunakan kata "jangan", misal "jangan buang sampah sembarangan", lebih baik "buang sampah pada tempat sampah".

Pertanyaan	Jika memberikan tips apakah dapat mempengaruhi seseorang dalam bersikap ?
Jawaban	Tips selain pada aspek konasi juga dapat berpengaruh langung ke aspek perilaku karena sudah diberikan saran untuk bisa dilakukan langsung.
Pertanyaan	Apakah dengan memberikan panduan dapat mempengaruhi perilaku seseorang?
Jawaban	Bisa, karena sudah dituntun untuk berperilaku seperti yang seharusnya.
Pertanyaan	Apakah dengan memberikan aturan yang mengikat dapat memberikan efek jera sehingga perilaku dapat berubah ?
Jawaban	Bisa, dengan aturan dan hukuman yang mengikat dapat memberikan efek jera untuk mahasiswa jika hukuman bener-benar dijalankan.
Pertanyaan	Apakah dengan memberikan pelatihan adalah cara yang efektif untuk mengubah perilaku seseorang?
Jawaban	Pelatihan sebenarnta tidak menjamin dapat mengubah perilaku seseorang apalagi jika pelatihan hanya dilakukan beberapa hari tanpa ada pantauan setelah kegiatan. Saat ini sedang banyak digunakan cara *coaching* atau bimbingan secara rutin dengan jangka waktu yang cukup lama, seperti beberapa bulan.

217

Tabel. D.2 Hasil wawancara Pakar 2

Topik Wawancara	Media penyampaian yang efektif digunakan untuk membentuk pengetahuan, sikap dan perilaku mahasiswa ITS.
Narasumber	Rustini Hendra Wardani, S.Psi
Jabatan	Student Advisory Center (SAC) ITS
Hari, Tanggal pelaksanaan	Selasa, 02 Juli 2019
Tempat	Gedung SAC
Tujuan Wawancara	Melakukan validasi terkait rancangan rekomendasi yang telah dirancang.
Pertanyaan	Apakah benar jika untuk mencapai kesadaran seseorang harus dimulai dari aspek pengetahuan, sikap dan perilaku ?
Jawaban	Benar, perubahan perilaku tidak dapat langsung tercipta tanpa memberikan pengetahuan dan mengubah pemikiran dan perasaan seseorang terhadap suatu hal.
Pertanyaan	Apakah media seperti infografis yang disebarkan melalui media sosial dapat menambah pengetahuan ?
Jawaban	Bisa, karena memang saat ini media sosial sangat mempengaruhi seseorang dan banyak diakses oleh kebanyakan mahasiswa.
Pertanyaan	Apakah artikel yang diletakkan dalam ITS News merupakan media yang cocoku untuk menambah pengetahuan mahasiswa ITS ?
Jawaban	Artikel dapat dijadikan media yang bagus untuk menambahkan pengetahuan. Tetapi sepertinya mahasiswa ITS sangat jarang membuka ITS News. Sebaiknya digunakan media

	lain untuk menyebarkan link artikel tersebut agar artikel tersebar luas.
Pertanyaan	Bagaimana jika dibuat kegiatan perlombaan seperti lomba artikel ?
Jawaban	Kalau lomba biasanya tergantung hadiahnya. Untuk menarik minat lomba lebih baik menargetkan setiap departemen harus memiliki perwakilan dengan menyebarkan informasi melalui Himpunan Mahasiswa tiap departemen.
Pertanyaan	Bagaimana jika dibuat acara seminar dengan target mahasiswa baru yang diwajibkan ?
Jawaban	Karakteristik mahasiswa ITS tidak akan tertarik dengan kegiatan seperti seminar jika belum merasa membutuhkan atau tidak mengalami secara langsung. Biasanya untuk menarik minat mahasiswa harus diberikan daya tarik seperti adanya sertifikat, makanan, atau diwajibkan untuk mengganti mata kuliah. Seminar juga akan lebih menarik jika narasumber yang dihadirkan menarik seperti mendatangkan orang yang berpengalaman, seperti orang yang pernah menjadi korban dan mantan *hacker* atau *hacker* yang baik, namun jangan gunakan sebutan mantan hacker, lebih baik menggunakan istilah pakar.
Pertanyaan	Apakah video yang menunjukkan ancaman dan risiko tentang perilaku yang salah dapat mempengaruhhi perasaan dan mengubah sikap seseorang ?
Jawaban	Bisa, asalkan kontennya sesuai, seperti memberikan gambaran atau ilustrasi

219

	tentang bahaya dan risikonya. Berikan fakta dan masalah-masalah yang pernah terjadi.
Pertanyaan	Apakah poster dapat menjadi media untuk mempengaruhi perasaan dan cara bersikap seseorang?
Jawaban	Bisa, tapi harus memiliki daya tarik misal dari segi warna dan gambar, atau menggunakan bentuk lain seperti karikatur. Dari segi pemasangan, pilih tempat yang sering menjadi tempat berkumpul mahasiswa.
Pertanyaan	Apakah pesan singkat pada spanduk dan video tron dapat memberikan pengaruh sampai dengan aspek konasi (sikap) ?
Jawaban	Bisa, asalkan pesan yang disampaian dapat memberi kesan. Penempatan video tron di ITS itu sebenarnya kurang tepat karena berada pada persimpangan. Untuk spanduk biasanya ada tempat tertentu yang diizinkan ITS.
Pertanyaan	Jika memberikan tips apakah dapat mempengaruhi seseorang dalam bersikap ?
Jawaban	Tips sebenarnya berguna untuk membentuk perilaku seseorang, tetapi tidak ada yang menjamin bahwa tips tersebut banyak dilakukan oleh target.
Pertanyaan	Apakah dengan memberikan panduan dapat mempengaruhi perilaku seseorang?
Jawaban	Dengan memberikan panduan berartikan mengarahkan untuk berbuat sesuai dengan aturan. Hal tersebut dapat mempengaruhi, tetapi susah dalam pengukuran keberhasilannya.

Pertanyaan	Apakah dengan memberikan aturan yang mengikat dapat memberikan efek jera sehingga perilaku dapat berubah ?
Jawaban	Iya, dari pada memberikan panduan akan lebih berpengaruh jika sibuat aturan yang harus dipatuhi. Bisa juga membuat sistem yang dapat mengharuskan mahasiswa melakukan hal itu.
Pertanyaan	Apakah dengan memberikan pelatihan adalah cara yang efektif untuk mengubah perilaku seseorang?
Jawaban	Pelatihan bisa membuat perilaku seseorang berubah karena diberikan pengalaman langsung (simulasi), tetapi hal tersebut juga tidak bisa terjamin jika tidak ada langkah pasca pelatihan

Tabel. D.3 Hasil wawancara Pakar 3

Topik Wawancara	Materi keamanan informasi
Narasumber	Bekti Cahyo Hidayanto, S.Si, M.Kom
Jabatan	Dosen Departemen Sistem Informasi (ahli bidang keamanan informasi)
Hari, Tanggal pelaksanaan	Senin, 01 Juli 2019
Tempat	Laboratorium IKTI
Tujuan Wawancara	Melakukan validasi terkait konten atau materi keamanan informasi
Pertanyaan	Apakah materi yang dibahas sudah sesuai ?
Jawaban	Semua materi sudah benar, sudah cukup mencangkup secara keseluruhan.
Pertanyaan	Bagaimana menurut Anda langkah yang dibutuhkan untuk meningkatkan

221

	kesadaran keamanan informasi untuk mahasiswa ITS?
Jawaban	– Membuat poster, spanduk, dan media sejenisnya kurang berarti jika tidak benar-benar menarik. Lebih baik menggunakan media sosial, tetpai bukan media sosial lembaga, sepeti media sosial DPTSI atau ITS. Lebih baik menggunakan media sosial Himpunan Mahasiswa tiap departemen. – Akan lebih berpengaruh sebenarnya jika sistem yang dibuat harus memaksa atau mengharuskan mahasiswa melakukan hal tersebut. Contohnya seluruh website atau aplikasi di bawah naungan ITS harus membuat sistem yang mengharuskan mahasiswa membuat *password* sesuai standard, jika tidak memenuhinya maka tidak dapat digunakan. Aturan lain misal diwajibkan menggunkan *One Drive* ITS saat menyimpan data. Aturan lainnya dengan membatasi akses internet dalam ITS, seperti memblok website yang terindikasi tidak aman. Hal lainnya yang dapat dilakukan yaitu dengan mendaftarkan setiap perangkat yang dimiliki mahasiswa dan No Hp yang terhubung, sehingga jika mahasiswa terindikasi melanggar, maka seluruh perangkat akan diblokir. – Membuat acara seminar untuk mahasiswa baru juga penting dilakukan untuk menumbuhkan

	kesadaran dari awal saat mahasiswa memasuki ITS. Buku saku juga perlu dibuat sebagai informasi atau panduan agar mahasiswa mengetahui bagaimana menjaga keamanan informasi. Seminar akan lebih mengenai target jika ditunjukan ilustrasi atau contoh permasalahan yang pernah terjadi. – Sebelum menerapkan sistem atau aturan yang mengikat, lebih baik maelakukan sosialisasi atau kampanye tentang keamanan informasi sehingga mahasiswa memahami mengapa kebijakan tersebut penting .

223

LAMPIRAN E – BUKTI VALIDITAS KUISIONER (SPSS)

Uji Validitas Tahap Uji Coba

Correlations

		MP1.01	MP1.02	MP1.03	TOTAL
MP1.01	Pearson Correlation	1	,526**	,677**	,839**
	Sig. (2-tailed)		,001	,000	,000
	N	39	39	39	39
MP1.02	Pearson Correlation	,526**	1	,632**	,847**
	Sig. (2-tailed)	,001		,000	,000
	N	39	39	39	39
MP1.03	Pearson Correlation	,677**	,632**	1	,895**
	Sig. (2-tailed)	,000	,000		,000
	N	39	39	39	39
TOTAL	Pearson Correlation	,839**	,847**	,895**	1
	Sig. (2-tailed)	,000	,000	,000	
	N	39	39	39	39

**. Correlation is significant at the 0.01 level (2-tailed).

Gambar. E.1 Bukti validitas kuesioner uji coba (1)

Correlations

		MP2.01	MP2.02	MP1203	TOTAL
MP2.01	Pearson Correlation	1	,860**	,697**	,928**
	Sig. (2-tailed)		,000	,000	,000
	N	39	39	39	39
MP2.02	Pearson Correlation	,860**	1	,735**	,945**
	Sig. (2-tailed)	,000		,000	,000
	N	39	39	39	39
MP1203	Pearson Correlation	,697**	,735**	1	,881**
	Sig. (2-tailed)	,000	,000		,000
	N	39	39	39	39
TOTAL	Pearson Correlation	,928**	,945**	,881**	1
	Sig. (2-tailed)	,000	,000	,000	
	N	39	39	39	39

**. Correlation is significant at the 0.01 level (2-tailed).

Gambar. E.2 Bukti validitas kuesioner uji coba (2)

224

Uji Validitas Tahap Penyebaran

Correlations

		MP1.01	MP1.02	MP1.03	TOTAL
MP1.01	Pearson Correlation	1	,499**	,513**	,770**
	Sig. (2-tailed)		,000	,000	,000
	N	100	100	100	100
MP1.02	Pearson Correlation	,499**	1	,788**	,899**
	Sig. (2-tailed)	,000		,000	,000
	N	100	100	100	100
MP1.03	Pearson Correlation	,513**	,788**	1	,900**
	Sig. (2-tailed)	,000	,000		,000
	N	100	100	100	100
TOTAL	Pearson Correlation	,770**	,899**	,900**	1
	Sig. (2-tailed)	,000	,000	,000	
	N	100	100	100	100

**. Correlation is significant at the 0.01 level (2-tailed).

Gambar. E.3 Bukti validitas kuesioner tahap penyebaran (1)

Correlations

		MP2.01	MP2.02	MP2.03	TOTAL
MP2.01	Pearson Correlation	1	,782**	,480**	,877**
	Sig. (2-tailed)		,000	,000	,000
	N	100	100	100	100
MP2.02	Pearson Correlation	,782**	1	,578**	,922**
	Sig. (2-tailed)	,000		,000	,000
	N	100	100	100	100
MP2.03	Pearson Correlation	,480**	,578**	1	,786**
	Sig. (2-tailed)	,000	,000		,000
	N	100	100	100	100
TOTAL	Pearson Correlation	,877**	,922**	,786**	1
	Sig. (2-tailed)	,000	,000	,000	
	N	100	100	100	100

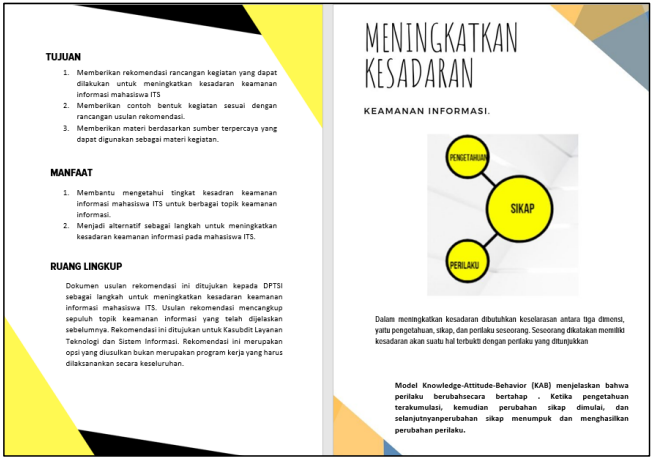
**. Correlation is significant at the 0.01 level (2-tailed).

Gambar. E.4 Bukti validitas kuesioner tahap penyebaran (2)

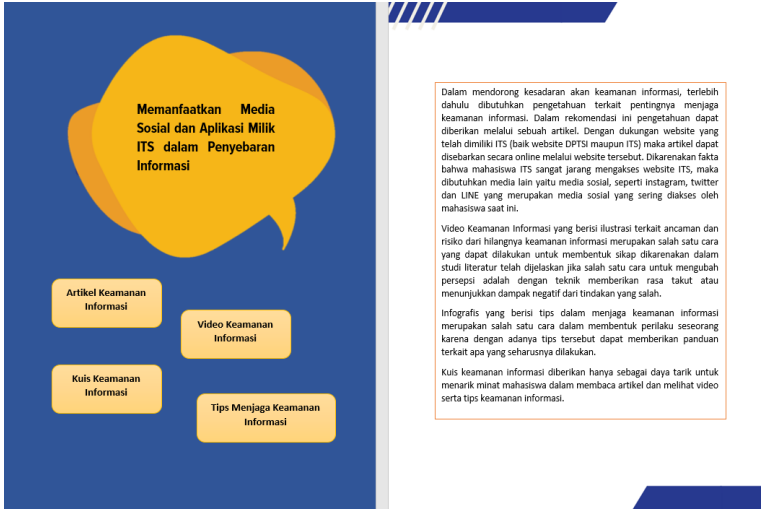
225

LAMPIRAN F- TAMPILAN DOKUMEN USULAN REKOMENDASI

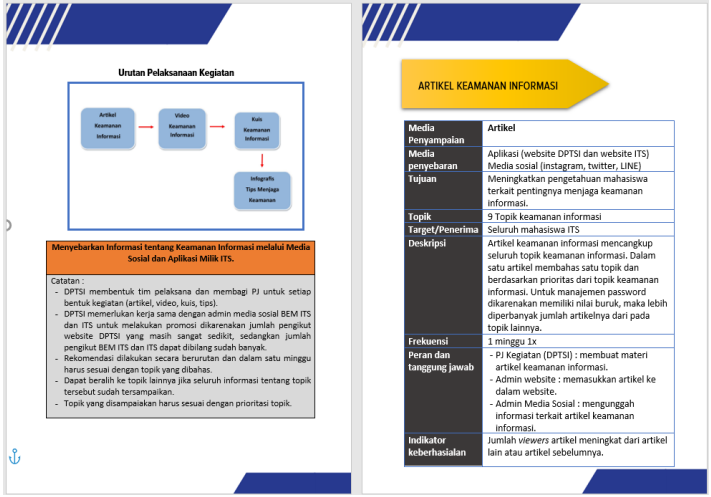
Gambar. F.1 Cover dokumen



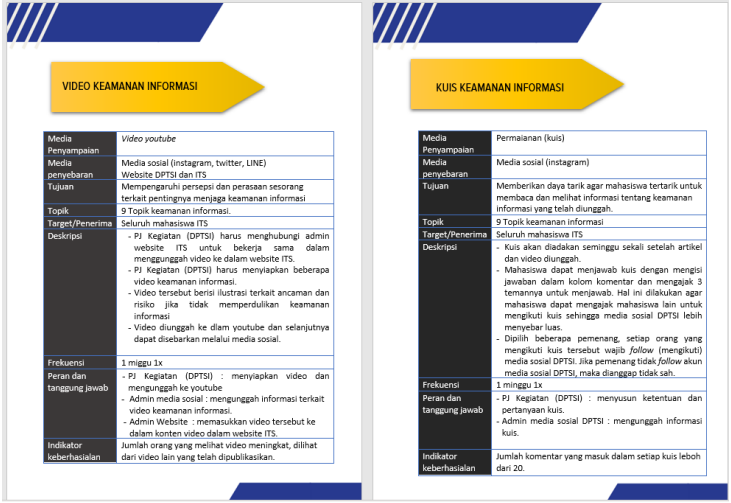
Gambar. F.2 Tampilan bagian pendahuluan



Gambar. F.3 Tampilan penjelasan rekomendasi kegiatan (1)



Gambar. F.4 Tampilan penjelasan rekomendasi kegiatan (2)



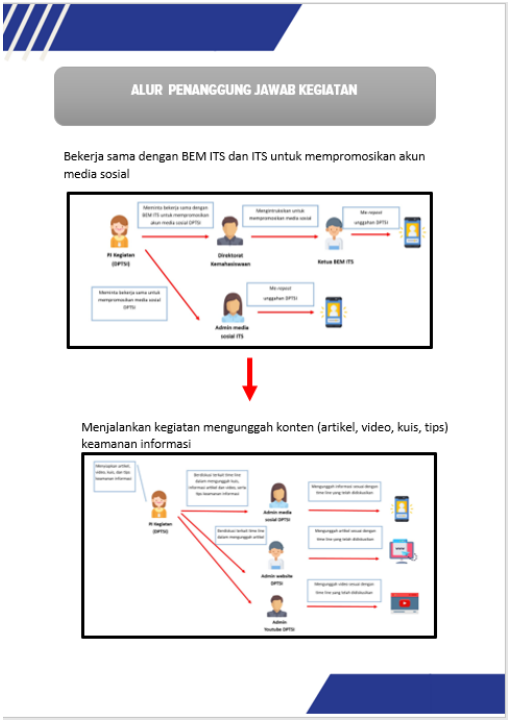
VIDEO KEAMANAN INFORMASI

Media Penyampaian	*Video youtube*
Media penyebaran	Media sosial (instagram, twitter, LINE) Website DPTSI dan ITS
Tujuan	Mempengaruhi persepsi dan perasaan sesorang terkait pentingnya menjaga keamanan informasi
Topik	9 Topik keamanan informasi.
Target/Penerima	Seluruh mahasiswa ITS
Deskripsi	- PJ Kegiatan (DPTSI) harus menghubungi admin website ITS untuk bekerja sama dalam menggunggah video ke dalam website ITS. - PJ Kegiatan (DPTSI) harus menyiapkan beberapa video keamanan informasi. - Video tersebut berisi ilustrasi terkait ancaman dan risiko jika tidak memperdulikan keamanan informasi - Video diunggah ke dlam youtube dan selanjutnya dapat disebarkan melalui media sosial.
Frekuensi	1 miggu 1x
Peran dan tanggung jawab	- PJ Kegiatan (DPTSI) : menyiapkan video dan mengunggah ke youtube - Admin media sosial : mengunggah informasi terkait video keamanan informasi. - Admin Website : memasukkan video tersebut ke dalam konten video dalam website ITS.
Indikator keberhasialan	Jumlah orang yang melihat video meningkat, dilihat dari video lain yang telah dipublikasikan.

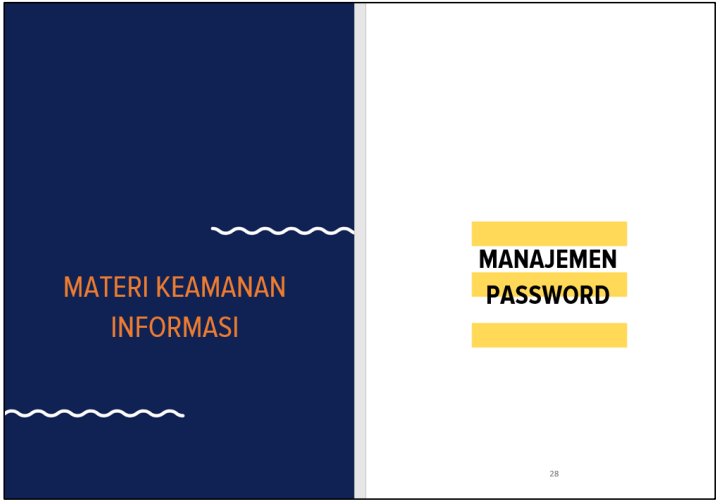
KUIS KEAMANAN INFORMASI

Media Penyampaian	Permaianan (kuis)
Media penyebaran	Media sosial (instagram)
Tujuan	Memberikan daya tarik agar mahasiswa tertarik untuk membaca dan melihat informasi tentang keamanan informasi yang telah diunggah.
Topik	9 Topik keamanan informasi
Target/Penerima	Seluruh mahasiswa ITS
Deskripsi	- Kuis akan diadakan seminggu sekali setelah artikel dan video diunggah. - Mahasiswa dapat menjawab kuis dengan mengisi jawaban dalam kolom komentar dan mengajak 3 temannya untuk menjawab. Hal ini dilakukan agar mahasiswa dapat mengajak mahasiswa lain untuk mengikuti kuis sehingga media sosial DPTSI lebih menyebar luas. - Dipilih beberapa pemenang, setiap orang yang mengikuti kuis tersebut wajib *follow* (mengikuti) media sosial DPTSI. Jika pemenang tidak *follow* akun media sosial DPTSI, maka dianggap tidak sah.
Frekuensi	1 minggu 1x
Peran dan tanggung jawab	- PJ Kegiatan (DPTSI) : menyusun ketentuan dan pertanyaan kuis. - Admin media sosial DPTSI : mengunggah informasi kuis.
Indikator keberhasialan	Jumlah komentar yang masuk dalam setiap kuis leboh dari 20.

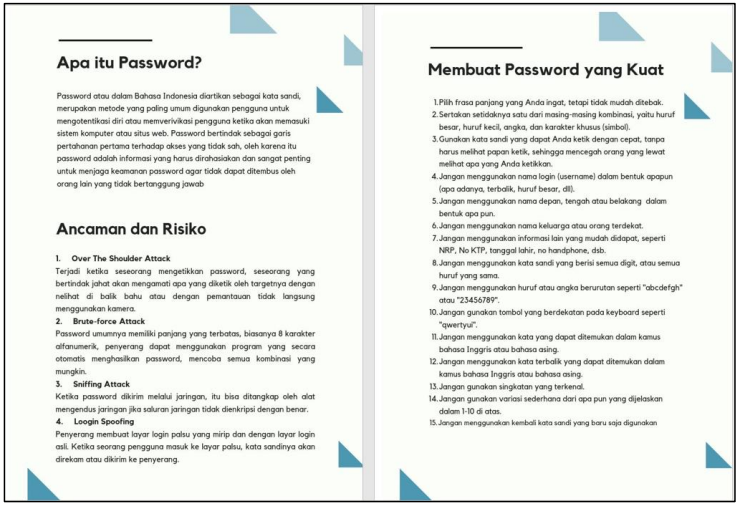
Gambar. F.5 Tampilan penjelasan rekomendasi kegiatan (3)



Gambar. F.6 Tampilan penjelasan rekomendasi kegiatan (4)



Gambar. F.7 Tampilan bagian materi keamanan informasi (1)



Apa itu Password?

Password atau dalam Bahasa Indonesia diartikan sebagai kata sandi, merupakan metode yang paling umum digunakan pengguna untuk mengotentikasi diri atau memverifikasi pengguna ketika akan memasuki sistem komputer atau situs web. Password bertindak sebagai garis pertahanan pertama terhadap akses yang tidak sah, oleh karena itu password adalah informasi yang harus dirahasiakan dan sangat penting untuk menjaga keamanan password agar tidak dapat ditembus oleh orang lain yang tidak bertanggung jawab

Ancaman dan Risiko

1. **Over The Shoulder Attack**

Terjadi ketika seseorang mengetikkan password, seseorang yang bertindak jahat akan mengamati apa yang diketik oleh targetnya dengan melihat di balik bahu atau dengan pemantauan tidak langsung menggunakan kamera.

2. **Brute-force Attack**

Password umumnya memiliki panjang yang terbatas, biasanya 8 karakter alfanumerik, penyerang dapat menggunakan program yang secara otomatis menghasilkan password, mencoba semua kombinasi yang mungkin.

3. **Sniffing Attack**

Ketika password dikirim melalui jaringan, itu bisa ditangkap oleh alat mengendus jaringan jika saluran jaringan tidak dienkripsi dengan benar.

4. **Loogin Spoofing**

Penyerang membuat layar login palsu yang mirip dan dengan layar login asli. Ketika seorang pengguna masuk ke layar palsu, kata sandinya akan direkam atau dikirim ke penyerang.

Membuat Password yang Kuat

1. Pilih frasa panjang yang Anda ingat, tetapi tidak mudah ditebak.
2. Sertakan setidaknya satu dari masing-masing kombinasi, yaitu huruf besar, huruf kecil, angka, dan karakter khusus (simbol).
3. Gunakan kata sandi yang dapat Anda ketik dengan cepat, tanpa harus melihat papan ketik, sehingga mencegah orang yang lewat melihat apa yang Anda ketikkan.
4. Jangan menggunakan nama login (username) dalam bentuk apapun (apa adanya, terbalik, huruf besar, dll).
5. Jangan menggunakan nama depan, tengah atau belakang dalam bentuk apa pun.
6. Jangan menggunakan nama keluarga atau orang terdekat.
7. Jangan menggunakan informasi lain yang mudah didapat, seperti NRP, No KTP, tanggal lahir, no handphone, dsb.
8. Jangan menggunakan kata sandi yang berisi semua digit, atau semua huruf yang sama.
9. Jangan menggunakan huruf atau angka berurutan seperti "abcdefgh" atau "23456789".
10. Jangan gunakan tombol yang berdekatan pada keyboard seperti "qwertyui".
11. Jangan menggunakan kata yang dapat ditemukan dalam kamus bahasa Inggris atau bahasa asing.
12. Jangan menggunakan kata terbalik yang dapat ditemukan dalam kamus bahasa Inggris atau bahasa asing.
13. Jangan gunakan singkatan yang terkenal.
14. Jangan gunakan variasi sederhana dari apa pun yang dijelaskan dalam 1-10 di atas.
15. Jangan menggunakan kembali kata sandi yang baru saja digunakan

Gambar. F.8 Tampilan bagian materi keamanan informasi (2)