

**MEASUREMENT OF INFORMATION SECURITY AND PRIVACY AWARENESS
USING THE MULTIPLE CRITERIA DECISION ANALYSIS (MCDA) METHOD
AT XYZ UNIVERSITY**

I Gede Agus Sukariana Yasa¹, I Made Edy Listartha², I Made Ardwi Pradnyana³

^{1,2,3}Informatics Engineering, Engineering and Vocational Faculty, Universitas Pendidikan Ganesha, Bali,
Indonesia

Email: sukariana.yasa@gmail.com, listartha@undiksha.ac.id, ardwi.pradnyana@undiksha.ac.id

(Article Received: October 12, 2022; Revision: Desember 12, 2022; Published: August 18, 2023)

Abstract

Information security is an asset that has value so it must be protected, along with increasing assets it is undeniable that many people wish to gain access and control it so that behind the convenience in the digital world there are many risks to information assets. There are several cases that occur related to information security such as data theft, illegal access, information leakage and vandalism where this becomes the privacy of the user. So it is necessary to do research from the user's perspective to measure the level of information security and privacy awareness of students and lecturers as well as recommendations that will be suggested based on the results of measuring information security and privacy awareness. The objects in this research are students and lecturers at the XYZ University. The method used is Multiple Criteria Decision Analysis (MCDA) by measuring the dimensions of knowledge, attitude, behavior in six areas of information security and three areas of privacy. Data were obtained by distributing questionnaires using a Likert scale of 5. Based on the questionnaire from the respondents, it can be seen students and lecturers have awareness that is at a "good" level of 85% in information security while privacy is at a "good" level with a result of 89% but in the behavior dimension there are several areas that are included in the "average" level including the area passwords by 62%, mobile equipment area by 77% incident area by 70% and on privacy security on the behavior dimension there is one area namely the login activity area by 78% so this needs to be given recommendations for improvement in order to reach a "good" level by providing socialization/ training for students and lecturers

Keywords: Information security, privacy, MCDA, AHP

**PENGUKURAN KESADARAN KEAMANAN INFORMASI DAN PRIVASI MENGGUNAKAN
METODE MULTIPLE CRITERIA DECISION ANALYSIS (MCDA) DI UNIVERSITAS XYZ**

Abstrak

Keamanan informasi merupakan sebuah aset yang memiliki nilai sehingga harus dilindungi, seiring dengan meningkatnya aset tidak dipungkiri banyak orang yang berkeinginan untuk mendapatkan akses dan mengendalikannya sehingga dibalik kemudahan dalam dunia digital terdapat banyak risiko terhadap aset informasi. Adapun beberapa kasus yang terjadi berkaitan dengan keamanan informasi seperti pencurian data, akses secara ilegal, kebocoran informasi serta vandalisme yang mana hal tersebut menjadi privasi dari pengguna. Sehingga perlu dilakukan penelitian dalam perspektif pengguna untuk mengukur tingkat kesadaran keamanan informasi dan privasi terhadap mahasiswa dan dosen serta rekomendasi yang akan disarankan berdasarkan hasil pengukuran kesadaran keamanan informasi dan privasi, yang menjadi objek dalam penelitian ini adalah mahasiswa dan dosen di Universitas XYZ. Adapun metode yang digunakan adalah *Multiple Criteria Decision Analysis* (MCDA) dengan mengukur pada dimensi *knowledge*, *attitude*, *behavior* pada enam area keamanan informasi dan tiga area pada privasi, data diperoleh dengan menyebarkan kuesioner dengan menggunakan skala likert 5. Berdasarkan kuesioner dari responden maka dapat dilihat mahasiswa dan dosen memiliki kesadaran yang berada pada level "Good" sebesar 85% pada keamanan informasi sedangkan pada privasi berada pada level "Good" dengan hasil sebesar 89% namun pada dimensi *behavior* terdapat beberapa area yang termasuk kedalam level "Average" diantaranya area *password* sebesar 62%, area *mobile equipment* sebesar 77% area *incident* sebesar 70% dan pada keamanan privasi pada dimensi *behavior* terdapat satu area yakni area *login activity* sebesar 78% sehingga hal ini perlu diberikan rekomendasi perbaikan agar mencapai level "Good" dengan memberikan sosialisasi/pelatihan terhadap mahasiswa dan dosen.

Kata kunci: keamanan informasi, privasi, MCDA, AHP

1. PENDAHULUAN

Pada era industri 4.0 teknologi informasi sudah menjadi bagian dari kehidupan, perkembangan teknologi informasi tersebut tentunya membawa banyak perubahan yang berdampak positif bagi penggunaannya seperti mempermudah dalam memperoleh informasi yang dibutuhkan setiap saat.[1] Teknologi informasi sudah menjadi bagian dari kehidupan manusia salah satunya dalam bidang Pendidikan yakni di kalangan mahasiswa dan dosen, dari banyaknya teknologi informasi yang masuk tentunya tidak akan bermanfaat banyak jika tidak digunakan secara maksimal, akan tetapi dibalik dari kemudahan teknologi informasi di waspadai dan menjadi perhatian lebih sehingga dapat mengurangi dampak negatif dalam proses Pendidikan. Universitas XYZ memiliki sistem informasi bagi mahasiswa dan dosen diantaranya adalah SIAK, aplikasi ini bertujuan untuk memberikan layanan akademik bagi mahasiswa dan dosen.

Adapun risiko yang perlu menjadi perhatian bagi mahasiswa dan dosen adalah mengenai layanan yang terdapat pada mahasiswa yakni Pangkalan Data Mahasiswa (PDM) yang berisikan Nomor Induk Keluarga (NIK) hal ini jika di akses oleh pihak yang tidak bertanggung jawab dapat memicu penyalahgunaan terhadap data pribadi yang dapat merugikan dari pemilik informasi sehingga perlu dilakukan pengukuran terhadap pengguna baik mahasiswa ataupun dosen guna mengetahui tingkat kesadaran keamanan informasi yang ada. Salah satu hal yang harus di waspadai adalah keamanan, terdapat beberapa kasus yang terjadi berkaitan dengan keamanan informasi seperti pencurian data, akses secara *illegal*, kebocoran informasi, serta vandalisme[2]. Berdasarkan data dari BSSN menerbitkan pada *website* resminya pada tanggal 30 Maret 2022 mengenai laporan tahunan hasil monitoring keamanan siber tahun 2021 yang menyatakan bahwa terdapat 1,6 miliar anomaly trafik yang masuk ke Indonesia dengan trafik tertinggi pada bulan Desember, adapun mayoritas dari *trafik* tersebut merupakan aktivitas *malware* dan *ransomware*, selain itu BSSN juga menerbitkan top 10 *vulnerabilities* yang diantaranya adalah: *Cross-Site Scripting (XSS)*, *Clickjacking*, *Possible Brutforce*, *Insecure Direct Object Reference (IDOR)*, *SQL Injection*, *Unencrypted Communication*, *ClearText Submission Password*, *Weak Password*, *Sensitive Data Exposure*, dan *Directory Listing* [3]

Berdasarkan latar belakang yang sudah di uraikan maka diperlukan sebuah penelitian untuk mengetahui tingkat kesadaran keamanan informasi di kalangan mahasiswa dan dosen sehingga penulis berinisiatif untuk melakukan penelitian dengan judul “pengukuran kesadaran keamanan informasi

dan privasi menggunakan metode *Multiple Criteria Decision Analysis (MCDA)* di Universitas XYZ”.

Penelitian mengenai pengukuran kesadaran keamanan informasi telah dilakukan oleh Muklis Amin pada tahun 2014 yang meneliti terkait kesadaran keamanan informasi pemerintah pemkot[4], selanjutnya penelitian mengenai pengukuran kesadaran keamanan informasi dan privasi pada pengguna *smartphone* oleh Akraman pada tahun 2018[5], penelitian mengenai pengukuran tingkat kesadaran keamanan informasi pada mahasiswa dengan metode MCDA yang dilakukan oleh Dafid pada tahun 2020[6] penelitian mengenai pengukuran kesadaran keamanan informasi dan privasi dalam media sosial oleh Hendro Gunawan pada tahun 2021[7] dan oleh Kusumaningrum pada tahun 2022 yang meneliti terkait pengukuran tingkat kesadaran keamanan siber di kalangan mahasiswa *study from home* dengan metode MCDA[8]

Penelitian ini bertujuan untuk melakukan pengukuran kesadaran keamanan informasi dan privasi terhadap mahasiswa dan dosen pada Universitas XYZ dengan menggunakan metode *Multiple Criteria Decision Analysis (MCDA)*. Penelitian ini diharapkan untuk dapat memberikan informasi terkait tingkat kesadaran keamanan informasi dan privasi terhadap mahasiswa dan dosen.

2. METODE PENELITIAN

Metode *Multiple Criteria Decision Analysis (MCDA)* biasanya digunakan dalam mengambil keputusan atas dasar beberapa alternatif yang memiliki kriteria tertentu[4]. Pendekatan ini didasari oleh perhitungan nilai total kriteria (area kesadaran keamanan informasi dan privasi)[9], nilai dari masing-masing alternatif dalam penelitian ini adalah dimensi yang merupakan nilai keseluruhan kriteria, krugger melakukan pengukuran pada tiga dimensi yakni dimensi *Knowledge*, *Attitude* dan *Behavior* adapun bobot yang diberikan oleh Krugger pada masing-masing dimensi adalah sebagai berikut:

Tabel 1. Bobot masing-masing dimensi

Dimensi	Bobot
<i>Knowledge</i>	30
<i>Attitude</i>	20
<i>Behavior</i>	50

serta enam area yang termasuk memiliki risiko yang kritis, yaitu:

- Selalu taat pada aturan perusahaan (*Policies*).
- Menjaga kerahasiaan *password* dan *personal identity number (Password)*.
- Menggunakan *e-mail* dan internet dengan bijaksana (*E-mail & Internet*).

- d. Berhati-hati menggunakan perangkat (*Mobile equipment*).
- e. Melaporkan insiden keamanan informasi (*Incident*).
- f. Menyadari konsekuensi setiap Tindakan (*Consequences*).

Serta dalam keamanan privasi diadopsi dari penelitian sebelumnya yang dilakukan oleh Akraman[5], yakni:

- a. *Login activity*
- b. *Perceived intrusion*
- c. *Secondary use of information*

Secara matematis pendekatan MCDA ditunjukkan pada persamaan yang di kemukakan oleh Krugger & Kearney pada tahun 2006[10].

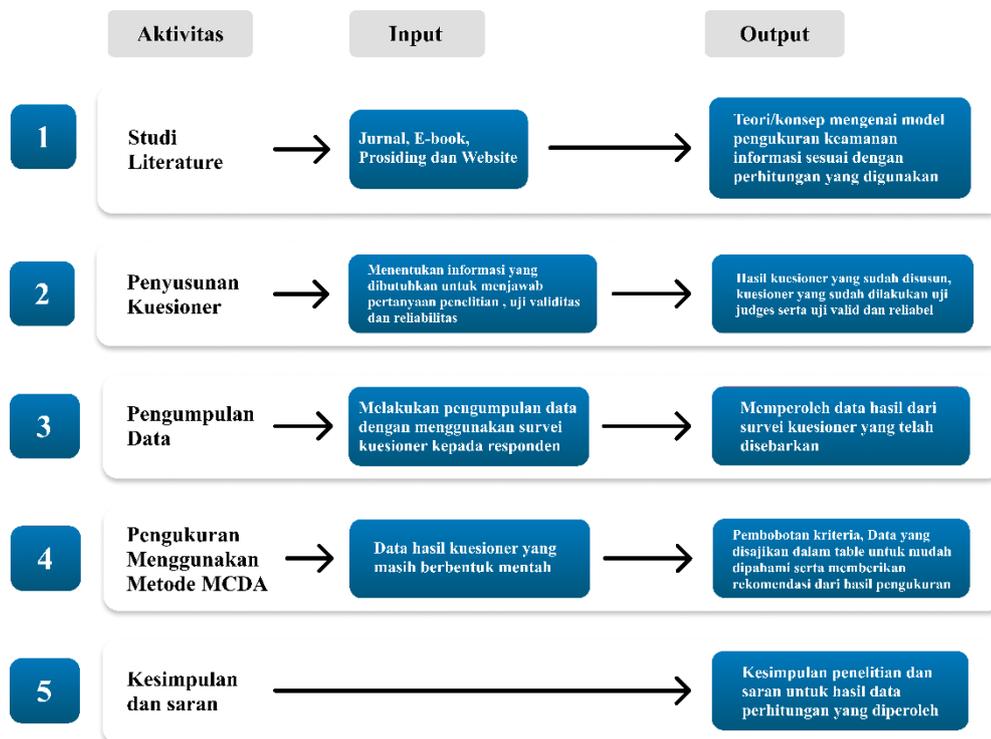
$$v(a) = \sum_{i=1}^n v_i(a)w_i \quad (1)$$

$V(a)$ merupakan nilai seluruh alternatif, $V_i(a)$ merupakan nilai skor yang mewakili dari setiap alternatif, $V_i(a)$ didapatkan dengan cara menggunakan pertanyaan berupa kuesioner dengan skala likert 5, dan W_i merupakan

bobot yang diberikan untuk menggambarkan tingkat kepentingan kriteria I yang didapat menggunakan metode AHP (*Analytic Hierarchy Process*) guna mencerminkan tingkat kepentingan setiap kriteria.

Nilai $V_i(a)$ ditentukan berdasarkan kuesioner yang disusun sebanyak 27 pertanyaan yang digunakan untuk menguji *knowledge*, *attitude* dan *behavior* responden yang berkaitan dengan enam area keamanan informasi dan tiga area keamanan privasi[11] dimana setiap jawaban dari responden terdiri atas lima skala[12]: Sangat Setuju (SS) = 5, Setuju (S) = 4, Netral (N) = 3, Tidak Setuju (TS) = 2, Sangat Tidak Setuju (STS) = 1. Dari 5 skala tersebut menunjukkan bahwa angka 1 merupakan pernyataan tidak persetujuan hingga angka 5 yang menyatakan setuju terhadap pernyataan yang terdapat pada kuesioner.

Penelitian ini terdapat beberapa tahapan yang dilakukan dimulai dari identifikasi masalah, perumusan masalah, studi literatur, penyusunan kuesioner, pengumpulan dan pengolahan data, hasil dan pembahasan, serta kesimpulan dan saran penelitian yang akan dijelaskan melalui bagan berikut:



Gambar 1. Alur Penelitian

2.1 Studi Literatur

Pada tahap ini dilakukan studi literatur dari berbagai sumber seperti jurnal nasional, jurnal internasional, *e-book*, *prosiding*, dan *website* yang dapat dijadikan pedoman penyelesaian masalah sehingga pada tahap ini *output* yang dihasilkan berupa teori atau konsep mengenai model atau metode pengukuran keamanan informasi dan keamanan privasi.

2.2 Penyusunan Kuesioner

Penyusunan kuesioner dilakukan untuk menentukan informasi apa saja yang dibutuhkan untuk menjawab pertanyaan penelitian dalam bentuk kuesioner yang berjumlah sebanyak 27 pertanyaan yang diadopsi dari penelitian sebelumnya[13] dengan mengacu pada 6 area yang dikemukakan oleh Krugger[10] serta 3 area privasi,

selain itu kuesioner yang sudah di susun selanjutnya dilakukan uji ahli instrumen yang bertujuan untuk apakah instrumen yang digunakan sudah layak dalam artian adalah mudah dimengerti oleh responden awam[14] serta melakukan uji validitas dan uji reliabilitas sehingga kuesioner yang sudah disusun sebelumnya dinyatakan valid dan reliabel untuk digunakan. Dalam melakukan uji validitas dan reliabilitas penulis menggunakan bantuan program SPSS[15]

Tabel 2. Contoh pernyataan masing-masing dimensi

Dimensi	Pertanyaan/ pernyataan
<i>Knowledge</i>	Internet merupakan sistem komunikasi secara global yang menghubungkan satu komputer dengan komputer lainnya melalui jaringan
<i>Attitude</i>	Saya sadar kata sandi merupakan kata kunci untuk memasuki sebuah sistem
<i>Behavior</i>	Saya terbiasa mengganti <i>password</i> pada sistem informasi yang saya gunakan secara berkala dalam 3 bulan

2.3 Pengumpulan Data

Setelah kuesioner memang benar-benar dinyatakan lolos pada uji ahli instrument dan valid maka kuesioner tersebut di sebarakan kepada responden dengan menggunakan skala 5 yang berpedoman pada [16]. Kuesioner ini ditujukan kepada dosen dan mahasiswa di masing-masing fakultas dengan jumlah setiap fakultas adalah 7 dosen dan 18 mahasiswa di 8 fakultas dimana sampel penelitian dipetakan menggunakan tabel Yount[17]. Pengumpulan data menggunakan bantuan *google form* yang nantinya penyebaran *linknya* melalui *online* baik menggunakan aplikasi *whatsapp* ataupun telegram.

2.4 Pengukuran Menggunakan Metode MCDA

Pada tahap ini data yang sudah di dapat dari responden yang masih berbentuk mentah diolah terlebih dahulu sehingga mendapatkan hasil yang akan disajikan dalam bentuk tabel guna mempermudah untuk memahami informasi di dalamnya. Adapun beberapa Langkah yang dilakukan adalah:

- Melakukan pembobotan kriteria yang sudah ditentukan dengan menggunakan pendekatan AHP langkah ini menggunakan konsep pendekatan AHP berupa matriks berpasangan yang perhitungannya menggunakan bantuan aplikasi Exel sehingga dalam pembobotan ini

menghasilkan area mana yang menjadi bobot prioritas. Adapun dalam menentukan pembobotan kriteria ini melibatkan dari salah satu pimpinan yang memang berada pada *scope* keamanan pada instansi UPT TIK. Yang perlu menjadi perhatian adalah jika tabel matriks nantinya yang di isi oleh pimpinan dilakukan *consisten relation* mendapatkan hasil $CR > 0,1$ maka dikatakan tidak konsisten sehingga perlu dilakukan pengisian ulang[18].

- Melakukan pengukuran secara keseluruhan kesadaran keamanan informasi dengan mengacu pada Average hasil perhitungan kuesioner setiap area dengan mengacu hasil pada Skala tingkat kesadaran keamanan informasi ditentukan dalam tiga tingkatan atau level yakni: *Good*, *Average*, *Poor*. Skala ini juga digunakan oleh Krugger[10] pada penelitiannya dalam mengukur kesadaran keamanan informasi serta mengutip dari penelitian [5] bahwasannya pada keterangan dari level mana saja yang diperlukan tindakan.

Tabel 3. Value measurement

Awareness	Measurement (%)	Tindakan
<i>Good</i>	80-100	Tidak Dibutuhkan
<i>Average</i>	60-79	Berpotensi Dibutuhkan
<i>Poor</i>	59 and less	Dibutuhkan

- Melakukan pengukuran terhadap mahasiswa dan dosen pada masing-masing area keamanan informasi dan privasi sehingga diketahui seberapa besar *presentase* dari masing-masing area, Ketika terdapat area yang mendapat level "*average*" dan "*poor*" maka nantinya akan diberikan Tindakan berupa rekomendasi terhadap area dan dimensi yang levelnya "*average*" dan "*poor*".
- Melakukan pemetaan dalam bentuk tabel baik dari hasil pengukuran terhadap mahasiswa atau dosen untuk mudah dimengerti setelah pemetaan dengan tabel dilakukan dapat diberikan rekomendasi sesuai hasil yang di dapat dari nilai Average dengan menggunakan persamaan MCDA

2.5 Kesimpulan dan Saran

Langkah terakhir dari seluruh proses ini adalah memberikan kesimpulan dari hasil pengolahan data serta memberikan saran untuk penelitian selanjutnya. Adapun kesimpulan yang dimaksud merupakan berisikan hasil dari pengolahan data mengenai:

- Seberapa tingkat kesadaran keamanan informasi mahasiswa dan dosen
- Memberikan penjelasan mengenai hasil dari proses pembobotan kriteria yang sudah

- dilakukan sehingga diketahui berapa bobot yang digunakan dalam penelitian ini
- c. Memberikan penjelasan terhadap hasil pengukuran kesadaran keamanan informasi secara keseluruhan.
- d. Memberikan penjelasan terhadap hasil pengukuran kesadaran dari mahasiswa dan dosen
- e. Memberikan penjelasan terhadap hasil pemetaan yang sudah disajikan dalam bentuk tabel, serta memberikan saran yang tepat sesuai dengan hasil perhitungan.

3. HASIL DAN PEMBAHASAN

Pada tahap ini akan menjelaskan terkait dari keseluruhan hasil dan pembahasan dari penelitian pengukuran kesadaran keamanan informasi dan privasi menggunakan metode *Multiple Criteria Decision Analysis* (MCDA). Adapun proses penelitian yang telah dilakukan yakni menggunakan beberapa metode atau model serta Teknik yang telah dijelaskan sebelumnya. Dalam penelitian ini Teknik yang digunakan adalah kuesioner yang disebarakan secara *online*, proses pengukuran melibatkan dosen serta mahasiswa sebanyak 56 dosen dan 144 mahasiswa sehingga keseluruhan sampel berjumlah sebesar 200 orang.

3.1. Uji ahli instrumen

Dari butir 1 sampai 27 bahwasanya ahli 1 dan ahli 2 menyatakan untuk keseluruhan butir pernyataan Sebagian besar relevan namun terdapat masukan serta rekomendasi perbaikan sehingga butir dari pernyataan semuanya dinyatakan relevan untuk *form* uji ahli instrumen.

3.2. Uji validitas

Berdasarkan hasil uji yang dilakukan dengan menggunakan bantuan program IBM SPSS Statistik 24 terhadap 40 mahasiswa yang menjadi responden dengan menggunakan taraf signifikansi 5% serta r tabel yang di tentukan berdasarkan tabel r *product moment* yang sebesar 0,312 dengan 27 pertanyaan dari variabel keamanan informasi dan privasi yang terdiri atas 9 indikator dengan masing-masing pertanyaan sebanyak 3 butir.

3.3. Uji reliabilitas

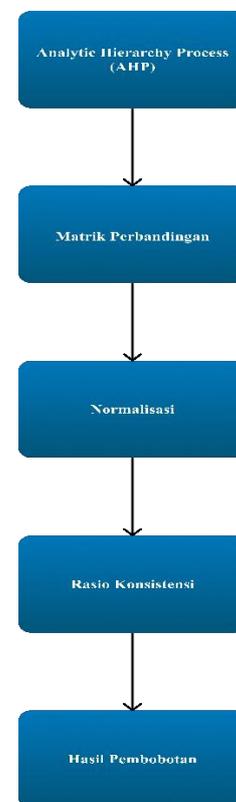
Melakukan uji reliabilitas, uji reliabilitas dilakukan guna mengukur konsistensi dari suatu jawaban atas pertanyaan atau pernyataan yang terdapat pada kuesioner. Pengujian ini dilakukan pada kuesioner yang akan di sebar kepada responden, uji reliabilitas dinyatakan konsisten dengan mengacu pada nilai *alpha Cronbach* apabila nilai *alpha Cronbach* > 0,6 maka *reliable* sebaliknya jika nilai *alpha Cronbach* < 0,6 maka dinyatakan tidak reliabel

Berdasarkan uji reliabel yang sudah dilakukan dengan menggunakan bantuan program IBM SPSS Statistik 24 didapatkan bahwa skor reliabilitas untuk kuesioner Kesadaran keamanan informasi dan privasi dengan banyak 27 butir pernyataan sebesar 0,950. Dengan skor 0,950 menunjukkan bahwa > 0,6 maka menunjukkan kuesioner dapat dikatakan reliabel atau konstan dapat dilihat pada tabel berikut:

Tabel 6. Uji Reliabilitas

Variabel	Reliabilitas	Keterangan
Kesadaran keamanan informasi dan privasi	0,950	Reliabel

3.4. Pembobotan menggunakan AHP



Gambar 2. Alur Proses *Analytic Hierarchy Process* (AHP)

Adapun hasil dari perhitungan menggunakan metode *Analytic Hierarchy Process* (AHP) untuk mendapatkan prioritas kepentingan setiap area baik keamanan informasi maupun privasi dapat dilihat pada tabel berikut:

Tabel 7. Matriks Perbandingan Keamanan Informasi

	consequences	incident	mobile equipment	email & internet	passwords	password
consequences	1	5	1	1	2	0,14
incident	0,2	1	0,14	0,2	1	0,14
mobile equipment	1	7	1	1	2	0,14
email & internet	1	5	1	1	1	0,14
policies	5	1	5	1	1	0,14
password	7	7	7	7	7	1
Total	15,2	26	15,14	11,2	10,4	1,7

Tabel 8. Normalisasi

Area	jumlah	prioritas
consequences	0,52	0,09
incident	0,26	0,04
mobile equipment	0,59	0,10
email & internet	0,59	0,10
policies	0,97	0,16
password	3,07	0,51
Total	6	1

Tabel 9. Rasio Konsistensi

Area	Jumlah Perbaris	Prioritas	Hasil
consequences	0,60	0,09	0,7
incident	0,33	0,04	0,4
mobile equipment	0,69	0,10	0,8
email & internet	0,73	0,10	0,8
policies	1,30	0,16	1,5
password	3,93	0,51	4,4
TOTAL			8,6

Tabel 10. Pembobotan keamanan informasi dengan AHP

Area	Hasil W_i
Password	0,51
Policies	0,16

Mobile equipment	0,10
Email & internet	0,10
Consequences	0,09
incident	0,04

Dari tabel yang sudah diperoleh berdasarkan pertimbangan dari Kepala Divisi Infrastruktur, Jaringan, dan Keamanan dipetakan berdasarkan prioritas yang paling tinggi hingga terendah. Hasil yang paling tertinggi diperoleh pada area *password* sebesar 0,51 kemudian di susul oleh area *policies* sebesar 0,16 selanjutnya di susul oleh area *mobile equipment* dan area *email & internet* yakni sebesar 0,10 kemudian di susul oleh area *consequences* sebesar 0,09 dan yang paling terendah adalah area *incident* sebesar 0,04. Selanjutnya adalah pembobotan pada privasi yang dapat dilihat pada tabel berikut:

Tabel 11. Matriks perbandingan Keamanan privasi

	login activity	perceived intrusion	secondary use of information
login activity	1	7	7
perceived intrusion	0,14	1	1
secondary use of information	0,14	1	1
Total	1,29	9	9

Tabel 12. Normalisasi

Area	Jumlah	Prioritas
login activity	2,33	0,78
perceived intrusion	0,33	0,11
secondary use of information	0,33	0,11
Total	3	1

Tabel 13. Rasio Konsistensi

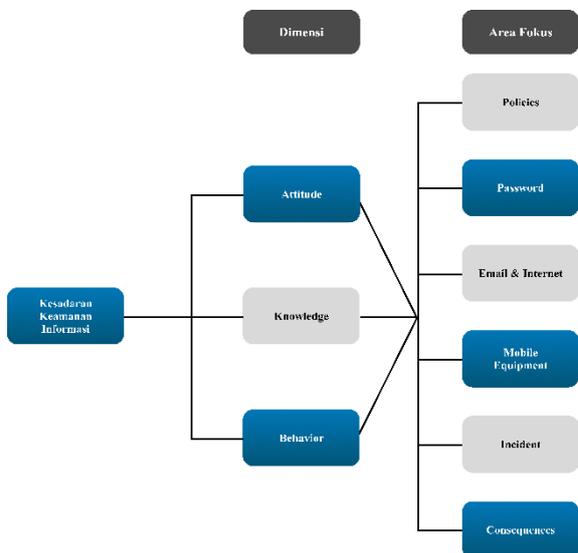
Area	jumlah perbaris	prioritas	hasil
login activity	2,33	0,78	3,11
perceived intrusion	0,33	0,11	0,44
secondary use of information	0,33	0,11	0,44
Total			4,00

Tabel 14. Pembobotan Privasi dengan AHP

Area	Hasil W_i
<i>Login activity</i>	0,78
<i>Perceived intrusion</i>	0,11
<i>Secondary use of information</i>	0,11

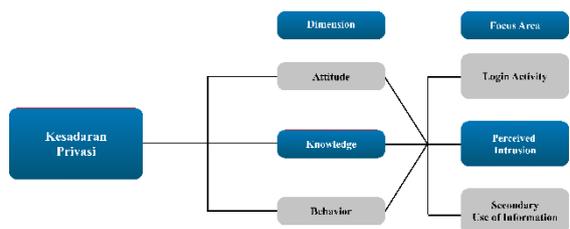
Dari tabel yang sudah diperoleh dipetakan juga berdasarkan prioritas yang paling tinggi hingga terendah, hasil yang paling tertinggi diperoleh dari area *login activity* sebesar 0,78 selanjutnya disusul dengan area *perceived intrusion* dan *secondary use of information* sama-sama sebesar 0,11.

3.5. Hasil pengukuran



Gambar 3. Diagram Alur Kesadaran Keamanan Informasi

Gambar diatas menjelaskan bahwa dalam pengukuran kesadaran keamanan informasi terdapat tiga dimensi yang digunakan sesuai dengan teori yang sudah dijelaskan dengan focus area sebanyak enam area. Atau untuk menguji knowledge, attitude dan behavior berkaitan dengan enam area kesadaran yang masing-masing area memiliki tiga pertanyaan sesuai dengan dimensi, adapun contohnya dapat dilihat pada Tabel 2. Contoh pernyataan masing-masing dimensi



Gambar 4. Diagram Alur Kesadaran Keamanan Privasi

Gambar diatas menjelaskan bahwa dalam pengukuran kesadaran keamanan privasi terdapat tiga dimensi yang digunakan sesuai dengan teori yang sudah dijelaskan dengan focus area sebanyak tiga area. Atau untuk menguji knowledge, attitude dan behavior berkaitan dengan tiga area kesadaran privasi yang masing-masing area memiliki tiga pertanyaan sesuai dengan dimensi, adapun contohnya dapat dilihat pada Tabel 2. Contoh pernyataan masing-masing dimensi.

Dimensi	Area						Total Nilai
	A1	A2	A3	A4	A5	A6	
Knowledge	A11	A21	A31	A41	A51	A61	$\sum_{j=1}^6 A_{1j}/6$
Attitude	A12	A22	A32	A42	A52	A62	$\sum_{j=1}^6 A_{2j}/6$
Behaviour	A13	A23	A33	A43	A53	A63	$\sum_{j=1}^6 A_{3j}/6$
Total Nilai	$\sum_{i=1}^3 A_{i1}/3$	$\sum_{i=1}^3 A_{i2}/3$	$\sum_{i=1}^3 A_{i3}/3$	$\sum_{i=1}^3 A_{i4}/3$	$\sum_{i=1}^3 A_{i5}/3$	$\sum_{i=1}^3 A_{i6}/3$	

Gambar 2. Perhitungan total nilai

Sebelum ditentukan tingkat kesadaran keamanan informasi dan privasi sebagai hasil akhir, untuk proses perhitungan total skor setiap dimensi dan area dapat dilihat pada Gambar 2.

Tabel 15. Total nilai keamanan informasi mahasiswa dan dosen

Dimensi	A1	A2	A3	A4	A6	A6	Total
K	96	90	85	87	83	87	88
A	87	95	95	86	88	82	89
B	91	62	93	77	70	80	79
Total	91	82	91	83	80	83	85

Keterangan :

AREA

A1 : *Policies*

A2 : *Password*

A3 : *Mobile equipment*

A4 : *Email & internet*

A5 : *Consequences*

A6 : *incident*

DIMENSI

K : Knowledge

A : Attitude

B : Behavior

Berdasarkan perhitungan yang sudah dilakukan didapatkan hasil total kesadaran keamanan informasi terhadap mahasiswa dan dosen adalah sebesar 85 yang dimana dapat dikatakan pada level “Good”, akan tetapi terdapat focus pada salah satu area yakni area *password* pada dimensi *behavior* dimana didapatkan hasil sebesar 62 yang berada pada level “Average” terendah sehingga dalam hal ini perlu dilakukan tindakan. Selanjutnya pada area *mobile equipment* pada bagian *behavior*

tergolong ke level “Average” dengan hasil sebesar 77, pada area *incident* dimensi *behavior* tergolong ke level “Average” dengan hasil yang diperoleh sebesar 70.

Tabel 16. Total nilai keamanan privasi terhadap mahasiswa dan dosen

Dimensi	A1	A2	A3	Total
K	85	93	92	90
A	94	82	94	90
B	78	91	94	87
Total	86	88	93	89

Keterangan :

AREA

A1 : *Login activity*

A2 : *Perceived intrusion*

A3 : *Secondary use of information*

DIMENSI

K : Knowledge

A : Attitude

B : Behavior

Adapun hasil dari perhitungan yang sudah dilakukan mendapatkan hasil sebesar 89 yang mana hasil tersebut termasuk ke level “Good”, akan tetapi terdapat salah satu area yang mendapat hasil “Average” dengan hasil 78 yang hampir mendekati level “Good” yakni pada area *login activity* dimensi *behavior*, hal ini perlu dilakukan tindakan guna meningkatkan keamanan privasi mahasiswa dan dosen ke level yang “Good”.

4. KESIMPULAN

Berdasarkan hasil yang sudah didapatkan maka dapat disimpulkan bahwa:

- mahasiswa dan dosen memiliki kesadaran yang berada pada level “Good” sebesar 85 pada keamanan informasi sedangkan pada privasi berada pada level “Good” dengan hasil sebesar 89.
- dimensi *behavior* terdapat beberapa area yang termasuk kedalam level “Average” diantaranya area *password* sebesar 62, area *mobile equipment* sebesar 77 area *incident* sebesar 70 dan pada keamanan privasi pada dimensi *behavior* terdapat satu area yakni area *login activity* sebesar 78.
- sehingga hal ini perlu diberikan rekomendasi perbaikan agar mencapai level “Good” dengan memberikan sosialisasi/pelatihan terhadap mahasiswa dan dosen

Sehingga Adapun beberapa rekomendasi yang dapat digunakan yang bersumber dari penelitian sebelumnya:

- Dimensi *behavior area password*** adapun rekomendasi yang dapat dilakukan adalah melakukan pembenahan berupa pelatihan terkait bagaimana cara mengamankan *password* serta memberikan fitur reminder dan penggantian *password* secara berkala [6]
- Dimensi *behavior area mobile equipment*** perlu dilakukan sosialisasi atau imbauan untuk selalu berhati-hati dalam menggunakan perangkat khususnya pada area-area yang bebas atau rentan terhadap keamanan informasi [6]
- Dimensi *behavior area incident*** mengutip dari [19] bahwa yang dapat dilakukan adalah program pelatihan terhadap kesadaran keamanan informasi karena mahasiswa dan dosen belum banyak mengetahui mengenai ciri-ciri serangan keamanan informasi sehingga menciptakan perilaku tidak peduli jika terjadi serangan-serangan.
- Dimensi *behavior area consequences*** perlu dilakukan sosialisasi terkait bahaya atau konsekuensi dalam menggunakan fasilitas publik ketika mengakses informasi yang terdapat pada akun pribadi.
- Dimensi *behavior area login activity*** perlu dipertahankan serta di tingkatkan guna mencapai hasil ke level “Good” dengan cara jangan pernah memberikan *password* kepada orang lain ataupun kepada teman serta membatasi hak akses terhadap akun milik pribadi.

DAFTAR PUSTAKA

- [1] F. H. Purwanto and M. Huda, “Pengukuran Tingkat Keamanan Informasi Perguruan Tinggi XYZ Menggunakan Indeks Keamanan Informasi (KAMI) Berbasis ISO,” *J. VOI*, vol. 8, no. 2, pp. 31–40, 2019, [Online]. Available: <https://voi.stmik-tasikmalaya.ac.id/index.php/voi/article/view/162>
- [2] J. R. Batmetan, “Tingkat Kesadaran Privasi Atas Masalah Keamanan Informasi (Lack Of Security Awareness),” 2018, doi: 10.31219/osf.io/cahzh.
- [3] BSSN, “Press release launching laporan tahunan hasil monitoring keamanan siber tahun 2021,” <https://bssn.go.id/LapTahMonitoring>, 2022.
- [4] M. Amin, “Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan Multiple Criteria Decision Analysis (McdA),” *J. Penelit. dan Pengemb. Komun. dan Inform.*, vol. 5, no. 1, pp. 15–24, 2014.

- [5] R. Akraman, C. Candiwan, and Y. Priyadi, "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia," *J. Sist. Inf. Bisnis*, vol. 8, no. 2, p. 115, 2018, doi: 10.21456/vol8iss2pp115-122.
- [6] et al Dafid, "Metode MCDA Untuk Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 7, no. 1, pp. 11–20, 2020, doi: 10.35957/jatisi.v7i1.296.
- [7] H. Gunawan, "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Dalam Sosial Media," *J. Muara Sains, Teknol. Kedokt. dan Ilmu Kesehatan*, vol. 5, no. 1, p. 1, 2021, doi: 10.24912/jmstkik.v5i1.3456.
- [8] A. Kusumaningrum, H. Wijayanto, and B. D. Raharja, "Pengukuran Tingkat Kesadaran Keamanan Siber di Kalangan Mahasiswa saat Study From Home dengan Multiple Criteria Decision Analysis (MCDA)," *J. Ilm. SINUS*, vol. 20, no. 1, p. 69, 2022, doi: 10.30646/sinus.v20i1.586.
- [9] S. Destya, "Pengukuran Tingkat Kesadaran Keamanan Informasi Berdasarkan Behavior Dan Offence Scale," *CESS (Journal Comput. Eng. Syst. Sci.)*, vol. 5, no. 2, p. 236, 2020, doi: 10.24114/cess.v5i2.18206.
- [10] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, 2006, doi: 10.1016/j.cose.2006.02.008.
- [11] M. R. Ramadhani and A. R. Pratama, "Analisis Kesadaran Cybersecurity Pada Pengguna Media Sosial Di Indonesia," *Journal.Uii.Ac.Id*, vol. 1, no. 2, pp. 1–8, 2020.
- [12] T. Torres, "Library Binus_ Skala Likert," http://library.binus.ac.id/eColls/eThesisdoc/Bab2/RS1_2017_2_1040_Bab2.pdf, 2017.
- [13] Patricia Kalis Jati Sekar Agri, "Evaluasi Tingkat Kesadaran Keamanan Informasi Mahasiswa Akuntansi Universitas Sanata Dharma," Universitas Sanata Dharma, 2019.
- [14] E. P. Widoyoko, *Teknik Penyusunan Instrumen Penelitian*. Yogyakarta: Pustaka Pelajar. PUSTAKA PELAJAR, 2015.
- [15] F. Yusup, "UJI VALIDITAS DAN RELIABILITAS INSTRUMEN PENELITIAN KUANTITATIF," *J. Tarb. J. Ilm. Kependidikan*, vol. 7, no. 1, pp. 17–23, 2018, doi: 10.21831/jorpres.v13i1.12884.
- [16] P. D. Sugiyono, "Metode Penelitian Pendidikan: Pendekatan Kuantitatif, Kualitatif, R&D (Cetakan Ke 26)," *Bandung CV Alf.*, pp. 1–334, 2019.
- [17] R. Yount, "Populations and Sampling Frames," *Eur. Univ. Inst.*, pp. 1–11, 2006, [Online]. Available: http://www.vrdc.cornell.edu/info7470/2005/Lecture_Notes/lecture4a-populations-and-sampling-frames.pdf
- [18] G. K. Dewi, "Analisis Keamanan Sistem Informasi Universitas X," *Account. Bus. Inf. Syst. J.*, 2021, [Online]. Available: <https://journal.ugm.ac.id/abis/article/view/64235>
- [19] M. Amin, "Information Security Awareness Level Measurement Using Multiple Criteria Decision Analysis (McdA)," *J. Penelit. dan Pengemb. Komun. dan Inform.*, vol. 5, no. 1, p. 122371, 2014.

