Jurnal Bumigora Information Technology (BITe)
Vol. 7, No. 2, Desember 2025, Hal. 83∼94
E-ISSN: 2685-4066, DOI: 10.30812/bite.v7i2.5430

Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan HAIS-Q: Mengungkap Kesenjangan antara Sikap dan Pengetahuan Mahasiswa

Measuring Information Security Awareness Using HAIS-Q: Revealing the Gap between Students' Attitudes and Knowledge

Shelbila Fisabil Arum*, **Ariyan Zubaidi**, **Raphael Bianco Huwae**
Universitas Mataram, Mataram, Indonesia

Informasi Artikel:
Diterima: 1 Agustus 2025, Direvisi: 27 September 2025, Disetujui: 3 Desember 2025

Abstrak-
Latar Belakang: Keamanan informasi menjadi isu penting di era digital, terutama di kalangan mahasiswa yang aktif memanfaatkan teknologi dalam kegiatan akademik maupun non-akademik.
Tujuan: Penelitian ini bertujuan untuk mengetahui seberapa tinggi tingkat kesadaran mahasiswa Universitas Mataram terhadap keamanan informasi.
Metode: Penelitian ini menggunakan model *Human Aspects of Information Security Questionnaire* (HAIS-Q) yang mencakup tiga dimensi utama yaitu pengetahuan, sikap, dan perilaku, serta mencakup enam fokus area keamanan informasi. Data diperoleh melalui penyebaran kuesioner secara daring kepada mahasiswa aktif. Analisis dilakukan dengan menghitung persentase rata-rata pada masing-masing dimensi dan domain.
Hasil: Hasil menunjukkan bahwa tingkat kesadaran mahasiswa secara keseluruhan berada pada kategori "sedang". Dimensi sikap memperoleh skor tertinggi sebesar 80,01%, diikuti perilaku sebesar 79,52%, dan pengetahuan sebesar 79,49%. Area *Information Handling* dan *Password Management* menunjukkan kesadaran yang baik, sedangkan *Internet Use* merupakan domain dengan skor terendah, terutama pada aspek pengetahuan.
Kesimpulan: Temuan ini menunjukkan bahwa meskipun mahasiswa memiliki sikap positif, penerapannya dalam keseharian masih belum optimal.

Kata Kunci: *Human Aspects of Information Security Questionnaire*; Keamanan Informasi; Kesadaran Keamanan Informasi; Mahasiswa.

Abstract-
Background: *Information security is an important issue in the digital age, especially among students who actively use technology in both academic and non-academic activities.*
Objective: *This study aims to determine students' level of awareness of information security at Mataram University.*
Methods: *The study uses the Human Aspects of Information Security Questionnaire (HAIS-Q) model, which covers three main dimensions: knowledge, attitude, and behavior, as well as six focus areas of information security. Data was collected through an online questionnaire distributed to active students. Analysis was conducted by calculating the average percentage for each dimension and domain.*
Result: *The results indicate that the overall level of awareness among students falls into the "moderate" category. The attitude dimension achieved the highest score at 80.01%, followed by behavior at 79.52%, and knowledge at 79.49%. The Information Handling and Password Management areas demonstrated strong awareness, while Internet Use had the lowest score, particularly in the knowledge aspect.*
Conclusion: *These findings indicate that while students have positive attitudes, their application in daily life remains suboptimal.*

Keywords:*Human Aspects of Information Security Questionnaire; Information Security; Information Security Awareness; Student.*

How to Cite: S. F. Arum, A. Zubaidi, & R. B. Huwae, "Pengukuran Tingkat Kesadaran Keamanan Informasi Menggunakan HAIS-Q: Mengungkap Kesenjangan antara Sikap dan Pengetahuan Mahasiswa," *Jurnal Bumigora Information Technology (BITe)*, vol. 7, no. 2, pp. 83-94, Des 2025. DOI: 10.30812/bite.v7i2.5430.

Penulis Korespondensi:

Shelbila Fisabil Arum,
Program Studi Teknik Informatika, Universitas Mataram,
Email: shelbilafisabilarum@gmail.com

1. PENDAHULUAN

Keamanan informasi menjadi hal yang penting seiring dengan berkembangnya teknologi yang memudahkan berbagai aktivitas, baik di bidang pribadi, akademik, maupun profesional, juga membawa risiko besar terhadap keamanan data [1]. Keamanan informasi tidak hanya terkait perlindungan dari ancaman luar, tetapi juga menjaga kerahasiaan, integritas, dan ketersediaan data dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan yang tidak sah. Masyarakat yang semakin terhubung secara digital, diperlukan pemahaman yang baik mengenai pentingnya perlindungan informasi, baik di tingkat individu maupun organisasi [2]. Tantangan terkait keamanan informasi di perguruan tinggi sangat besar dan terus meningkat seiring dengan kemajuan teknologi. Universitas merupakan tempat dengan berbagai arus informasi yang tinggi, mulai dari data akademik hingga data pribadi mahasiswa. Dengan berbagai sistem informasi yang digunakan di kampus, data mahasiswa menjadi salah satu yang paling rentan terhadap ancaman kejahatan siber, seperti peretasan atau pencurian data. Jika tidak dikelola dengan baik, hal ini dapat merusak reputasi universitas dan menimbulkan kerugian besar. Hal ini menjadikan keamanan informasi sebagai aspek penting di lingkungan universitas [3]. Salah satu langkah yang dapat dilakukan adalah dengan mengukur tingkat kesadaran mahasiswa terhadap perlindungan data dan risiko terkait keamanan sistem. Penilaian ini penting agar mahasiswa menyadari potensi ancaman seperti serangan siber dan celah keamanan yang dapat mempengaruhi keamanan data pribadi maupun sistem akademik [4]. Mahasiswa, sebagai pengguna aktif teknologi digital seringkali tidak menyadari potensi ancaman di dunia maya, sementara kesadaran akan keamanan informasi sangat penting dalam pemanfaatan teknologi informasi di perguruan tinggi. Mereka sering menggunakan berbagai *platform* untuk kegiatan akademis, seperti mengunduh dan mengunggah materi, berkomunikasi dengan dosen dan teman, serta mengakses informasi lainnya [5]. Namun, rendahnya kesadaran akan pentingnya menjaga informasi pribadi dan institusional membuat mereka menjadi target empuk bagi ancaman siber [2]. Menurut [6] salah satu bentuk rendahnya kesadaran informasi terlihat bahwa hanya sekitar 40% mahasiswa yakin dapat mengenali serangan siber seperti *phishing* dan *malware*, banyak mahasiswa belum menyadari ancaman dari penggunaan teknologi informasi di kampus. Akibatnya, mahasiswa rentan terhadap serangan siber yang dapat menyebabkan kerugian finansial, pencurian data pribadi, dan kerusakan reputasi institusi. Oleh karena itu, penting untuk mengukur kesadaran mahasiswa mengenai keamanan informasi agar dapat merancang strategi yang tepat untuk meningkatkan pemahaman mereka [5]. Salah satu metode yang dapat digunakan untuk mengukur tingkat kesadaran keamanan informasi ini adalah *Human Aspects of Information Security Questionnaire* (HAIS-Q). Metode ini bertujuan untuk mengukur pengetahuan, sikap, dan perilaku individu terkait keamanan informasi [7]. Hasil pengukuran ini akan memberikan gambaran mengenai sejauh mana mahasiswa memahami ancaman serta menerapkan langkah-langkah yang tepat dalam menjaga data pribadi maupun data yang ada di kampus. Dengan menggunakan HAIS-Q, hasil yang diperoleh akan memberikan wawasan penting untuk merancang intervensi yang efektif guna meningkatkan kesadaran keamanan informasi [8]. Penelitian ini memilih Universitas Mataram sebagai lokasi penelitian karena karakteristik universitas negeri yang memiliki jumlah mahasiswa cukup besar dan sangat bergantung pada teknologi untuk mendukung kegiatan akademiknya. Selain itu, belum ada penelitian yang mengukur tingkat kesadaran informasi pada mahasiswa di universitas ini. Oleh sebab itu, penelitian ini penting dilakukan agar pihak universitas memiliki data yang akurat mengenai tingkat kesadaran mahasiswa dan dapat merancang program pendidikan yang lebih efektif. Menurut [9] pengembangan dan validasi instrumen HAIS-Q didasarkan pada model *Knowledge-Attitude-Behavior* (KAB), yang menunjukkan bahwa peningkatan pengetahuan tentang kebijakan keamanan informasi dapat mempengaruhi

sikap dan perilaku risiko-*averse* dalam penggunaan teknologi. Dengan menggunakan model ini, peneliti dapat memahami bagaimana pengetahuan dan sikap mahasiswa terkait keamanan informasi berkontribusi terhadap perilaku yang lebih aman. Pendekatan ini membantu dalam merancang strategi pelatihan dan kebijakan keamanan yang lebih efektif dengan menitikberatkan pada aspek manusia dalam menjaga keamanan informasi.

Adapun berbagai penelitian sebelumnya telah dilakukan untuk menilai sejauh mana kesadaran informasi yang dimiliki oleh individu di berbagai sektor. Salah satunya, penelitian oleh [5] menggunakan metode MCDA untuk mengevaluasi tingkat kesadaran informasi mahasiswa di STMIK XYZ, menunjukkan bahwa tingkat kesadaran mahasiswa secara umum berada pada level "sedang" dengan skor 71%. Hasil tersebut mengindikasikan perlunya perhatian khusus terhadap aspek perilaku, kepatuhan terhadap kebijakan, penggunaan perangkat *mobile*, dan konsekuensi yang masih berada di level "buruk". Selain itu, dimensi perilaku mahasiswa juga menunjukkan hasil yang kurang baik, terutama dalam hal ketaatan aturan, penggunaan perangkat seluler yang hati-hati, dan kesadaran akan konsekuensi tindakan. Selanjutnya, penelitian oleh [8], menggunakan metode HAIS-Q untuk menilai perilaku pengguna *mobile banking* dalam menjaga keamanan informasi di Indonesia. Hasilnya menunjukkan bahwa pemahaman terhadap aspek keamanan informasi (ISA) tergolong cukup baik. Namun, beberapa area seperti *password management*, terutama sub area "*Sharing Passwords*" (M=2,83), dan *mobile device* pada sub area "*Sending sensitive information via WI-FI*" (M=2,68) masih tergolong rendah, menunjukkan perlunya peningkatan kesadaran dan perilaku hati-hati dalam menjaga keamanan data pribadi pengguna *mobile banking*. Penelitian oleh [10], untuk menguji kesadaran keamanan informasi pengguna *smartphone*, menunjukkan bahwa tingkat kesadaran pengguna *smartphone* Android terhadap keamanan dan privasi cukup baik, dengan skor mencapai 76%. Penelitian ini menggunakan model gabungan teori psikologi sosial dan kerangka pemikiran dari Kruger dan Kearney, yang mengukur dimensi pengetahuan, sikap, dan perilaku dalam konteks keamanan dan privasi. Hasilnya adalah meskipun pengguna menunjukkan kesadaran yang cukup baik, terdapat area yang perlu ditingkatkan, seperti pelaporan insiden keamanan dan penggunaan data kedua, yang menunjukkan tingkat kesadaran yang masih rendah. Selian itu, penelitian [11] melakukan pengukuran kesadaran keamanan informasi pegawai PT Meshindo Jayatama dengan menggunakan metode HAIS-Q berdasarkan kerangka kerja KAB. Hasil pengukuran menunjukkan bahwa secara umum tingkat kesadaran pegawai berada pada level "baik" dengan persentase sebesar 84,43%. Hasil tersebut mengindikasikan bahwa aspek pengetahuan, sikap, dan perilaku pegawai dalam pengelolaan keamanan informasi sudah cukup baik, meskipun masih terdapat fokus area tertentu yang perlu ditingkatkan, seperti pengelolaan password yang berada pada level sedang dengan skor 75%. Namun demikian, sebagian besar penelitian tersebut masih terbatas karena hanya dilakukan pada kelompok tertentu, seperti pegawai dengan jumlah responden yang terbatas atau yang diteliti pada divisi tertentu saja, maupun mahasiswa yang hanya diteliti pada lingkup program studi tertentu, tanpa melibatkan mahasiswa secara keseluruhan di tingkat universitas. Selain itu, belum ada penelitian yang secara spesifik menerapkan HAIS-Q untuk mengukur tingkat kesadaran keamanan informasi pada seluruh mahasiswa dalam satu universitas.

Menurut [9] mengukur kesadaran keamanan informasi sangat penting. Peneliti lain juga menjelaskan bahwa keamanan informasi sangat penting karena kesadaran keamanan informasi dapat mempengaruhi tingkat kerentanan sistem terhadap ancaman yang disebabkan oleh perilaku manusia [12]–[15]. Berbagai studi menunjukkan bahwa pendekatan ini efektif dalam menggambarkan tingkat kesadaran pengguna terhadap keamanan informasi di berbagai institusi, namun penerapannya di lingkungan perguruan tinggi masih terbatas. Padahal, mahasiswa sebagai salah satu aktor penting di kampus rentan terhadap ancaman keamanan informasi karena tingginya penggunaan perangkat digital dan akses ke jaringan universitas. Meskipun ada penelitian yang melibatkan mahasiswa, cakupannya masih terbatas dan belum merepresentasikan populasi mahasiswa secara keseluruhan di tingkat universitas. Kondisi ini menunjukkan adanya **kesenjangan penelitian** terkait penerapan instrumen pengukuran kesadaran keamanan informasi, khususnya HAIS-Q, di kalangan mahasiswa. Selain itu, meskipun instrumen HAIS-Q telah digunakan dalam sejumlah penelitian, penerapannya umumnya masih terbatas pada lingkup sempit sehingga belum memberikan gambaran komprehensif mengenai kesadaran keamanan informasi mahasiswa. Oleh karena itu, **penelitian ini bertujuan** untuk mengevaluasi tingkat

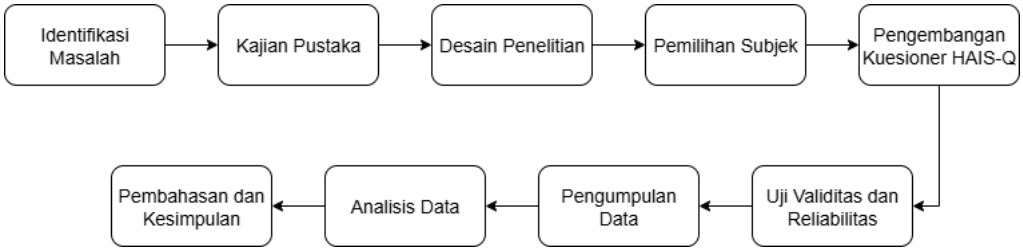
kesadaran keamanan informasi mahasiswa dengan cakupan lebih luas menggunakan HAIS-Q. Hasil penelitian diharapkan dapat memperoleh gambaran yang lebih representatif tentang bagaimana mahasiswa memahami, bersikap, dan bertindak terkait keamanan informasi, serta memberikan rekomendasi bagi universitas dalam meningkatkan kesadaran dan perlindungan data di lingkungan kampus [7].

Artikel ini disusun dalam beberapa bagian utama setelah pendahuluan. Bagian kedua membahas metode penelitian yang digunakan, dimulai dari identifikasi masalah, kajian pustaka, desain penelitian, pemilihan subjek, hingga pengembangan instrumen berupa kuesioner HAIS-Q. Selain itu, bagian ini juga menjelaskan proses uji validitas dan reliabilitas, pengumpulan data, serta teknik analisis data yang digunakan untuk memperoleh hasil penelitian yang akurat. Bagian ketiga memaparkan hasil penelitian dan pembahasan terkait tingkat pemahaman, sikap, dan perilaku mahasiswa dalam menjaga keamanan informasi. Bagian keempat menyajikan kesimpulan serta saran yang dapat dijadikan acuan untuk penelitian selanjutnya maupun implementasi di lingkungan perguruan tinggi. Tujuan utama penelitian ini adalah mengevaluasi tingkat kesadaran keamanan informasi mahasiswa menggunakan HAIS-Q pada lingkup universitas secara menyeluruh. Kontribusi penelitian ini terletak pada pemetaan kesadaran informasi berdasarkan dimensi pengetahuan, sikap, dan perilaku, yang dapat menjadi acuan dalam pengembangan program edukasi keamanan informasi di lingkungan universitas. Selain itu, hasil penelitian diharapkan dapat memberikan kontribusi bagi dunia penelitian melalui pengayaan literatur mengenai kesadaran keamanan informasi, strategi perguruan tinggi dalam meningkatkan kesadaran keamanan, serta pemahaman masyarakat mengenai pentingnya perilaku dalam penggunaan teknologi informasi.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kuantitatif deskriptif dengan HAIS-Q sebagai instrumen utama untuk mengukur kesadaran keamanan informasi pada mahasiswa Universitas Mataram. HAIS-Q merupakan metode dengan fokus pada tiga aspek utama yaitu pengetahuan (*Knowledge*), sikap (*Attitude*), dan perilaku (*Behavior*) mahasiswa terkait dengan keamanan informasi. Instrumen ini menggunakan skala Likert 1–5 untuk mengukur jawaban responden pada setiap item pertanyaan.

Studi kasus dalam penelitian ini dilakukan di lingkungan Universitas Mataram dengan subjek penelitian yaitu mahasiswa dari berbagai fakultas. Data diperoleh melalui penyebaran kuesioner HAIS-Q kepada responden secara daring maupun luring. Jumlah total pertanyaan dalam kuesioner adalah 54 item yang mencakup 6 domain terkait keamanan informasi. Data yang terkumpul selanjutnya dianalisis untuk menggambarkan tingkat kesadaran keamanan informasi mahasiswa. Langkah-langkah yang di lakukan pada penelitian ini dapat dilihat pada Gambar 1 [15]:



Gambar 1. Tahapan metode HAIS-Q

2.1. Identifikasi Masalah

Tahap pertama adalah identifikasi masalah yang bertujuan untuk merumuskan masalah yang akan dipecahkan. Pada penelitian ini permasalahan yang dihadapi adalah rendahnya kesadaran keamanan pada mahasiswa yang dapat menimbulkan resiko kebocoran data dan penyalahgunaan teknologi. Mahasiswa masih sering menggunakan kata sandi yang lemah hingga membagikan akun atau sandi kepada orang lain. Kondisi ini mencerminkan potensi rendahnya kesadaran terhadap keamanan informasi di lingkungan universitas, sehingga

penting untuk memahami sejauh mana perilaku tersebut terjadi.

2.2. Kajian Pustaka

Kajian pustaka merupakan tahapan penting dalam suatu penelitian yang bertujuan untuk mengkaji berbagai sumber informasi, seperti buku, jurnal ilmiah, dan karya akademik lainnya untuk memperoleh landasan teoritis yang relevan dengan masalah serta tujuan penelitian yang sedang dilakukan.

2.3. Desain Penelitian

Desain penelitian ditentukan untuk merencanakan metode dan strategi yang akan digunakan, seperti penyusunan kuesioner secara tertutup yang mencakup aspek-aspek penting dari kesadaran keamanan informasi, pemilihan responden, penyebaran kuesioner secara *online* kepada responden serta pengolahan data untuk menggambarkan hasil yang diperoleh dengan tujuan untuk memperoleh data yang valid dan dapat dipertanggungjawabkan.

2.4. Pemilihan Subjek

Pemilihan subjek pada penelitian ini dilakukan dengan memilih mahasiswa aktif dalam berbagai fakultas dan program studi di Universitas Mataram. Pemilihan subjek juga dilakukan dengan mempertimbangkan keragaman seperti jenjang semester, rentang usia dan jenis kelamin. Adapun untuk pengambilan sampel dari mahasiswa tersebut untuk menentukan jumlah sampel dari populasi yang diketahui, digunakan rumus *Yamane* dengan *margin of error* tertentu, sebagaimana ditunjukkan pada Persamaan (1) di bawah [16].

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

Dalam rumus tersebut, n merepresentasikan jumlah sampel yang harus digunakan dalam penelitian, sedangkan N menunjukkan jumlah populasi secara keseluruhan dan e merupakan *margin of error* atau tingkat kesalahan yang ditoleransi dalam pengambilan sampel, yang dalam penelitian ini ditetapkan sebesar 5% (0,05). Penggunaan *margin of error* ini bertujuan agar hasil penelitian tetap memiliki tingkat ketelitian yang dapat dipertanggungjawabkan meskipun tidak menggunakan seluruh populasi. Dalam penelitian ini, total populasi (N) pada mahasiswa aktif di Universitas Mataram sekitar 32.957, dengan tingkat kesalahan (e) yang ditetapkan sebesar 5% (0.05). Adapun untuk perhitungannya sebagai berikut:

$$n = \frac{32.957}{1 + 32.957\ (0.05)^2} = 395,2$$

Dengan demikian, jumlah sampel yang dibutuhkan dalam penelitian ini untuk mengukur tingkat kesadaran keamanan informasi pada mahasiswa di Universitas Mataram minimal sebanyak 395 sampel mahasiswa [11].

2.5. Pengembangan Kuesioner HAIS-Q

Selanjutnya pada tahap pengembangan kuesioner HAIS-Q, instrumen disusun berdasarkan pendekatan KAB yang bertujuan untuk mengukur tingkat pengetahuan, sikap, dan perilaku individu terkait keamanan informasi serta mengacu pada 6 domain yang telah ditetapkan pada HAIS-Q [9].

2.6. Uji Validitas dan Reliabilitas

Uji validitas dan reliabilitas dilakukan sebelum penyebaran kuesioner utama dengan tujuan untuk memastikan kuesioner yang digunakan memiliki keakuratan dan konsistensi yang tinggi. Uji validitas dilakukan menggunakan korelasi *Pearson Product Moment*, dimana item dinyatakan valid jika nilai r hitung > r tabel. Sedangkan untuk uji reliabilitas diukur dengan *Cronbach's Alpha*, dimana instrumen dianggap reliabel apabila nilai alpha > 0.7 [17].

2.7. Pengumpulan Data

Teknik pengumpulan data dilakukan dengan menyebarkan kuesioner HAIS-Q secara *online* kepada mahasiswa Universitas Mataram yang menjadi responden menggunakan *google form*. Kuesioner terdiri dari beberapa pernyataan yang terdiri dari 6 domain yaitu pengelolaan *password*, penggunaan internet, penggunaan email, penggunaan perangkat *mobile*, penggunaan media sosial dan pelaporan insiden. Setiap domain memiliki 3 pertanyaan yang mencakup 3 aspek yaitu aspek pengetahuan, sikap dan perilaku. Responden akan diminta untuk menjawab menggunakan skala likert 5 poin yang mengukur ketiga aspek tersebut dalam konteks keamanan informasi, dengan rentang jawaban 1 untuk sangat tidak setuju hingga 5 untuk sangat setuju [11].

2.8. Analisis Data

Setelah data terkumpul, dilakukan analisis data dengan menghitung skor rata-rata pada setiap aspek untuk melihat tingkat kesadaran keamanan informasi pada mahasiswa. Setiap aspek akan diberi bobot yang berbeda sesuai dengan pentingnya kontribusi terhadap kesadaran keamanan informasi, yaitu 30% untuk *Knowledge*, 20% untuk *Attitude* dan 50% untuk *Behaviour*. Menurut Kruger dan Kearney, aspek *behaviour* (perilaku) memiliki pengaruh yang besar karena mencerminkan langsung tindakan nyata pengguna sehingga diberi bobot tertinggi.

2.9. Pembahasan dan Kesimpulan

Pada tahap terakhir, hasil dari analisis data digunakan untuk mengkategorikan tingkat kesadaran keamanan informasi mahasiswa berdasarkan indikator pengetahuan, sikap, dan perilaku terhadap keamanan informasi. Kesimpulan dari analisis ini menjadi dasar untuk memberikan rekomendasi yang tepat dalam meningkatkan pemahaman dan penerapan perilaku yang aman dalam penggunaan teknologi informasi.

3. HASIL DAN PEMBAHASAN

3.1. Uji Validitas dan Reliabilitas

Sebelum mengumpulkan data utama, peneliti melakukan pengujian terhadap validitas dan reliabilitas terhadap instrumen penelitian dengan cara melakukan uji coba (*pilot testing*) yang melibatkan sekitar 50 mahasiswa dari Universitas Mataram. Tujuan dari uji validitas dan reliabilitas adalah untuk menentukan apakah instrumen penelitian dapat berfungsi dengan baik dan pertanyaan yang diajukan dapat dipahami. Dalam pengujian ini dilakukan terhadap 54 item pertanyaan dalam kuesioner dengan membandingkan nilai r hitung setiap item dengan nilai r tabel nya. Instrumen dapat dianggap valid jika nilai dari r hitung > r tabel, yang dimana pada penelitian ini nilai r tabel dengan derajat kebebasan (df) sebesar 48 adalah 0,2787. Nilai tersebut didapatkan dari tabel *Critical Values for Pearson's Correlation Coefficient* [18]. Untuk menentukan jumlah derajat kebebasan menggunakan Persamaan (2) berikut.

$$df = n - 2 \tag{2}$$

Derajat kebebasan (df) dihitung berdasarkan jumlah responden (n) yang digunakan dalam penelitian, di mana nilainya ditentukan dengan mengurangi jumlah responden tersebut sebanyak dua. Derajat kebebasan berfungsi untuk menentukan batas dalam pengujian statistik, khususnya saat melakukan uji validitas, sehingga hasil perhitungan dapat dibandingkan dengan nilai pada tabel distribusi r. Berdasarkan hasil uji validitas, terlihat bahwa semua item pada kuesioner memiliki nilai r hitung yang melebihi r tabel. Oleh karena itu, seluruh item dalam kuesioner ini dinyatakan valid dan layak digunakan untuk pengumpulan data. Hal ini diharapkan dapat memberikan hasil pengujian yang lebih akurat karena seluruh instrumen dapat digunakan untuk menilai kesadaran mahasiswa terhadap kemanan informasi di Universitas Mataram. Berikut merupakan hasil dari data yang telah diuji, sebagaimana yang terlihat pada Tabel 1.

Tabel 1. Hasil Uji Validitas

Item	r-Hitung (Total)	r-Tabel (5%)	Keterangan	Item	r-Hitung (Total)	r-Tabel (5%)	Keterangan
Q1	0.7519	0.2787	Valid	Q28	0.6469	0.2787	Valid
Q2	0.5187	0.2787	Valid	Q29	0.7974	0.2787	Valid
Q3	0.4178	0.2787	Valid	Q30	0.7124	0.2787	Valid
Q4	0.5194	0.2787	Valid	Q31	0.6475	0.2787	Valid
Q5	0.5631	0.2787	Valid	Q32	0.6903	0.2787	Valid
Q6	0.6494	0.2787	Valid	Q33	0.7216	0.2787	Valid
Q7	0.3319	0.2787	Valid	Q34	0.5303	0.2787	Valid
Q8	0.301	0.2787	Valid	Q35	0.5801	0.2787	Valid
Q9	0.3159	0.2787	Valid	Q36	0.7302	0.2787	Valid
Q10	0.7158	0.2787	Valid	Q37	0.5785	0.2787	Valid
Q11	0.2853	0.2787	Valid	Q38	0.6857	0.2787	Valid
Q12	0.5218	0.2787	Valid	Q39	0.6225	0.2787	Valid
Q13	0.664	0.2787	Valid	Q40	0.4396	0.2787	Valid
Q14	0.6624	0.2787	Valid	Q41	0.7008	0.2787	Valid
Q15	0.3991	0.2787	Valid	Q42	0.6126	0.2787	Valid
Q16	0.5334	0.2787	Valid	Q43	0.3765	0.2787	Valid
Q17	0.6259	0.2787	Valid	Q44	0.6764	0.2787	Valid
Q18	0.598	0.2787	Valid	Q45	0.4783	0.2787	Valid
Q19	0.7613	0.2787	Valid	Q46	0.7315	0.2787	Valid
Q20	0.5715	0.2787	Valid	Q47	0.4119	0.2787	Valid
Q21	0.6793	0.2787	Valid	Q48	0.6077	0.2787	Valid
Q22	0.6867	0.2787	Valid	Q49	0.606	0.2787	Valid
Q23	0.6281	0.2787	Valid	Q50	0.365	0.2787	Valid
Q24	0.7187	0.2787	Valid	Q51	0.5493	0.2787	Valid
Q25	0.7298	0.2787	Valid	Q52	0.4843	0.2787	Valid
Q26	0.624	0.2787	Valid	Q53	0.4695	0.2787	Valid
Q27	0.642	0.2787	Valid	Q54	0.4936	0.2787	Valid

Tabel 1 menunjukkan bahwa seluruh item dalam kuesioner terbukti valid karena nilai r-hitung lebih besar dari r-tabel. Hal ini menunjukkan setiap item pada kuesioner memiliki hubungan yang kuat dengan hasil jawaban responden secara keseluruhan sehingga mampu mengukur aspek yang ingin diteliti. Validitas yang baik memastikan bahwa tiap pertanyaan dalam kuesioner benar-benar mewakili kesadaran terhadap keamanan informasi. Setelah kuesioner dinyatakan valid, langkah selanjutnya melakukan uji reliabilitas untuk mengukur konsistensi instrumen secara keseluruhan ketika dilakukan pengukuran berulang. Uji ini dilakukan menggunakan metode *Cronbach's Alpha* yang dimana instrumen dinyatakan reliabel jika nilai alpha diatas 0.70. Dalam penelitian ini, nilai *Cronbach's Alpha* yang diperoleh sebesar 0.963 yang menunjukkan bahwa seluruh item pada kuesioner tersebut reliabel atau memiliki tingkat keandalan yang baik, dengan konsistensi tinggi dan hasil yang stabil ketika dilakukan pengukuran berulang [19]. Hasil ini selaras dengan penelitian yang dilakukan oleh [9] yang menyatakan bahwa instrumen berbasis domain KAB (*Knowledge*, *Attitude*, *Behaviour*) dapat menghasilkan validitas dan reliabilitas tinggi jika disusun dengan baik.

3.2. Hasil Uji dan Analisis Keseluruhan

Berasarkan hasil penyebaran kuesioner kepada mahasiswa di Universitas Mataram, jumlah responden yang berhasil mengisi kuesioner tersebut mencapai 400 orang. Jumlah tersebut telah melebihi batas minimum sampel yang dibutuhkan, yaitu sekitar 395 responden [11]. Adapun data karakteristik responden dalam penelitian ini ditunjukkan pada Tabel 2 berikut:

Tabel 2. Karakteristik Responden

Kriteria	Kategori	Frekuensi	Persentase
Fakultas	Fakultas Ekonomi dan Bisnis	78	19.5%
	Fakultas Hukum, Ilmu Sosial dan Ilmu Politik	87	21.7%
	Fakultas Keguruan dan Ilmu Pendidikan	51	12.8%
	Fakultas Pertanian	42	10.5%
	Fakultas Peternakan	15	3.7%
	Fakultas Teknik	76	19%
	Fakultas Matematika dan Ilmu Pengetahuan Alam	10	2.5%
	Fakultas Kedokteran	14	3.5%
	Fakultas Teknologi Pangan	27	6.8%
Jenis Kelamin	Laki-Laki	191	47.8%
	Perempuan	209	52.3%
	18 – 19 tahun	43	10.8%
Usia	20 – 21 tahun	131	32.8%
	22 – 23 tahun	213	53.3%
	24 – 25 tahun	13	3.2%
	Semester 2	45	11.3%
	Semester 4	35	8.8%
Semester	Semester 6	85	21.2%
	Semester 8	217	54.3%
	Semester >8	18	4.5%

Tabel 2 di atas menggambarkan karakteristik dari responden berdasarkan data mengenai fakultas, jenis kelamin, usia, serta semester. Dari tabel tersebut, dapat diketahui bahwa jumlah responden terbanyak berasal dari Fakultas Hukum dan mayoritas responden yang mengisi kuesioner adalah perempuan. Sebagian besar responden berada pada rentang usia 22 – 23 tahun dan berasal dari semester 8, yang menunjukkan bahwa kuesioner tersebut lebih banyak diisi oleh mahasiswa tingkat akhir.

Setelah dilakukan pengolahan data, diperoleh hasil tingkat kesadaran keamanan informasi pada mahasiswa berdasarkan 6 domain, yaitu *Password Management*, *Email Use*, *Internet Use*, *Social Media Use*, *Mobile Devices* dan *Information Handling*. Pengukuran dilakukan pada 3 aspek, yaitu Knowledge (30%), *Attitude* (20%), dan *Behaviour* (50%). Setiap domain dianalisis berdasarkan skor rata-rata dari masing-masing KAB, kemudian menghitung total *awareness* berdasarkan pembobotan yang dilakukan oleh Kruger & Kearney. Hasil perhitungan ditampilkan pada Tabel 3 berikut:

Tabel 3. Tingkat Kesadaran Keamanan Informasi

Fokus Area	***Knowledge***	***Attitude***	***Behaviour***	***Total Awareness***	**Rata – Rata**
Password Management	80.28	78.10	80.78	80.10	79.61%
Email Use	81.58	80.65	78.25	79.73	
Internet Use	72.82	78.32	76.87	75.94	
Social Media Use	79.15	78.38	79.38	79.31	
Mobile Devices	79.90	81.05	79.68	80.02	
Information Handling	83.18	82.58	82.15	82.55	

Tingkat penilaian kesadaran keamanan informasi dalam penelitian ini dibagi menjadi tiga kategori, yaitu "baik" apabila memperoleh skor ≥ 80, "sedang" apabila berada pada rentang skor 60 hingga 79, dan "buruk" apabila memperoleh skor kurang dari 60. Kategori ini digunakan untuk mempermudah interpretasi hasil serta melihat sejauh mana mahasiswa memahami penerapan keamanan informasi.

Berdasarkan hasil perhitungan tersebut, diperoleh total nilai rata-rata sebesar 79.61% yang menunjukkan kesadaran mahasiswa terhadap keamanan informasi di Universitas Mataram berada pada level "sedang". Meskipun tergolong sedang, skor ini cukup dekat dengan kategori "baik", yang berarti mahasiswa telah memiliki pemahaman dasar yang cukup mengenai keamanan informasi. Namun, masih terdapat celah antara pemahaman tersebut dan penerapan nyata dalam kebiasaan sehari-hari. Secara umum, aspek *Behaviour* cenderung memiliki

nilai lebih rendah dibandingkan aspek *Knowledge* dan *Attitude*, yang menunjukkan bahwa meskipun mahasiswa memiliki pengetahuan dan sikap yang cukup baik terhadap keamanan informasi, penerapannya dalam perilaku sehari-hari masih perlu ditingkatkan. Variasi skor ini juga terlihat di berbagai fokus area, yang mencerminkan adanya perbedaan tingkat pemahaman dan penerapan keamanan informasi pada mahasiswa.

Jika dilihat dari masing-masing domain, hasil tertinggi terdapat pada fokus area *Information Handling* (82.55%), dengan aspek *Knowledge* (83.18%), *Attitude* (82.58%), dan *Behaviour* (82.15%). Hal ini menunjukkan bahwa mahasiswa cukup menyadari pentingnya menjaga informasi pribadi serta menerapkannya dalam aktivitas akademik, seperti menyimpan dokumen penting secara aman dan tidak membagikan informasi sensitif kepada pihak tidak bertanggung jawab. Konsistensi skor tinggi di ketiga dimensi ini menandakan bahwa kesadaran mereka di area ini bersifat menyeluruh, baik dari sisi pemahaman, sikap, hingga perilaku nyata.

Fokus area *Password Management* dengan skor sebesar 80.10%, yang masuk dalam kategori "baik". Meskipun aspek *Attitude* menunjukkan nilai yang sedikit lebih rendah (78.10%) dibanding Knowledge (80.28%) dan *Behaviour* (80.78%), hasil ini menunjukkan bahwa sebagian mahasiswa mungkin belum memiliki sikap yang kuat untuk selalu mengganti *password* secara berkala atau membuat kombinasi yang kompleks. Namun secara keseluruhan, hasil ini tetap mencerminkan bahwa mahasiswa telah memiliki kesadaran yang cukup baik dalam mengelola dan menjaga kerahasiaan kata sandi mereka.

Fokus area *Mobile Devices* juga menunjukkan hasil yang baik dengan skor 80.02%, yang berarti mahasiswa cukup waspada terhadap keamanan informasi yang tersimpan dalam perangkat *mobile* mereka. Skor tertinggi berada pada dimensi *Attitude* (81.05%) yang menunjukkan bahwa mahasiswa cukup berhati-hati terhadap keamanan perangkat, seperti mengunci ponsel atau membatasi izin aplikasi. Namun, skor *Behaviour* (79.68%) menunjukkan bahwa praktik nyata penggunaan perangkat belum sepenuhnya optimal.

Berbeda dengan domain di atas, *Email Use* memperoleh skor 79.73%, yang meskipun masih dalam kategori "sedang", tetapi menunjukkan adanya kesenjangan antara pemahaman dan penerapan. Aspek *Behaviour* memperoleh nilai paling rendah (78.25%) dibanding *Knowledge* (81.58%) dan *Attitude* (80.65%). Hal ini menunjukkan bahwa mahasiswa belum sepenuhnya disiplin dalam menerapkan praktik keamanan saat menggunakan email, seperti mengenali email *phishing* atau menjaga privasi informasi yang dikirimkan melalui email.

Social Media Use menunjukkan skor 79.31%, juga dalam kategori "sedang". Hal ini menunjukkan bahwa kesadaran terhadap risiko berbagi informasi di media sosial masih perlu ditingkatkan. *Attitude* dan *Behaviour* berada di angka yang relatif serupa (78.38% dan 79.38%), namun skor *Knowledge* (79.15%) masih menunjukkan bahwa mahasiswa sudah memahami secara umum bahaya berbagi data pribadi di media sosial, hanya saja perlu didorong untuk lebih disiplin dalam menerapkan pengetahuan tersebut dalam praktik, terutama dalam pengaturan privasi dan konten yang dibagikan.

Skor terendah berasal dari domain *Internet Use*, yakni 75.94%, yang menunjukkan bahwa penggunaan internet mahasiswa belum didampingi oleh pemahaman dan kebiasaan aman yang optimal. Skor *Knowledge* (72.82%) menjadi yang paling rendah dari seluruh domain dan dimensi, menandakan bahwa banyak mahasiswa belum memiliki pemahaman menyeluruh tentang risiko yang berkaitan dengan aktivitas daring, seperti penggunaan jaringan publik tanpa perlindungan atau mengunjungi situs yang tidak aman. Kondisi ini juga berpengaruh pada rendahnya aspek *Behaviour* (76,87%), yang mencerminkan bahwa sebagian besar mahasiswa belum terbiasa menerapkan cara penggunaan internet yang lebih bijak dan waspada terhadap potensi ancaman digital dalam kegiatan sehari-hari mereka.

Jika dibandingkan dengan peneliti sebelumnya, temuan ini sejalan dengan penelitian [5] yang mengkategorikan skor tingkat kesadaran keamanan mahasiswa dalam level sedang yaitu 71%, namun skor pada penelitian ini lebih tinggi yaitu 79.61%. Hal ini bisa di sebabkan karena perbedaan instrumen yang digunakan. Meskipun keduanya mengukur dimensi dan bobot yang sama, perbedaan terlihat pada teknik penilaian yang digunakan. MCDA menilai kesadaran melalui enam area spesifik dengan pembobotan AHP sehingga skor akhir sangat dipengaruhi oleh aspek terlemah, sedangkan HAIS-Q menghitung skor berdasarkan rata-rata jawaban pada tiap indikator KAB. Selain itu, cakupan responden dalam penelitian ini lebih luas karena melibatkan mahasiswa

di tingkat universitas, sehingga hasil yang diperoleh lebih representatif dibandingkan penelitian sebelumnya. Pada penelitian [11] juga mengukur kesadaran keamanan informasi pada pegawai menggunakan metode HAIS-Q, dan hasilnya menunjukkan bahwa aspek yang paling rendah adalah penggunaan perangkat *mobile*. Hal ini terjadi karena pegawai masih cenderung mengirim file atau dokumen sensitif perusahaan menggunakan laptop sebagai perangkat *mobile* dan terkoneksi pada *Wi-Fi* umum, sehingga risiko keamanan meningkat. Sementara itu, penelitian ini mengukur tingkat kesadaran keamanan informasi pada mahasiswa di lingkungan universitas dengan metode yang sama, dan aspek yang paling rendah adalah penggunaan internet. Perbedaan ini menunjukkan pengaruh konteks dan kebiasaan pengguna, yaitu pegawai lebih berisiko pada perangkat *mobile* karena aktivitas pekerjaan, sedangkan mahasiswa lebih berisiko pada penggunaan internet karena aktivitas akademik dan non-akademik mereka. Dengan demikian, meskipun instrumen yang digunakan sama, area yang perlu mendapat perhatian berbeda tergantung karakteristik responden dan lingkungannya. Jika ditinjau dari rata-rata skor setiap dimensi, *Attitude* menjadi dimensi dengan skor tertinggi (80.01%), diikuti oleh *Behaviour* (79.52%) dan *Knowledge* (79.49%). Meskipun perbedaannya tidak signifikan, hal ini menunjukkan bahwa mahasiswa cenderung memiliki sikap positif terhadap pentingnya menjaga keamanan informasi dan mulai menerapkannya dalam tindakan nyata, meskipun belum sepenuhnya optimal. Urutan ini sedikit berbeda dari beberapa penelitian sebelumnya yang umumnya menemukan bahwa dimensi *Knowledge* cenderung lebih tinggi dibanding *Behaviour*. Namun, hasil penelitian ini justru memperlihatkan bahwa aspek *Attitude* paling menonjol, yang menjelaskan bahwa mahasiswa mulai menyadari pentingnya dan perlunya menjaga keamanan informasi, meskipun masih diperlukan pemahaman yang lebih baik dan praktik sehari-hari. Temuan ini tetap sejalan dengan pendapat [9], yang menekankan bahwa kesadaran keamanan informasi tidak hanya bergantung pada pengetahuan, tetapi perlu tercermin dalam tindakan nyata. Demikian pula, pendapat [2] juga mendukung bahwa meskipun mahasiswa memiliki tingkat sikap atau pengetahuan yang baik, penerapannya dalam kebiasaan sehari-hari seringkali belum konsisten.

Meskipun dimensi *Behaviour* bukan yang terendah, hasil penelitian tetap menunjukkan bahwa terdapat kesenjangan antara pengetahuan, sikap, dan tindakan nyata mahasiswa dalam menjaga keamanan informasi. Skor *Behaviour* yang berada di bawah *Attitude* menandakan bahwa meskipun mahasiswa memiliki sikap positif terhadap pentingnya menjaga keamanan data, hal tersebut belum sepenuhnya tercermin dalam perilaku sehari-hari. Kondisi ini dapat diartikan bahwa sebagian besar mahasiswa sudah memahami konsep dasar keamanan informasi dan memiliki sikap yang mendukung, tetapi belum menjadikannya sebagai kebiasaan yang konsisten. Hal ini memperkuat temuan bahwa kesadaran keamanan informasi tidak cukup hanya dilihat dari seberapa besar pengetahuan yang dimiliki, melainkan harus dibuktikan melalui tindakan nyata dalam penggunaan teknologi secara aman [20].

4. KESIMPULAN

Hasil penelitian menunjukkan bahwa tingkat kesadaran mahasiswa terhadap keamanan informasi berada pada kategori sedang dengan skor rata-rata keseluruhan sebesar 79.61%. Jika dilihat dari masing-masing dimensi, sikap mahasiswa terhadap keamanan informasi menempati posisi tertinggi, disusul oleh perilaku, dan yang terendah adalah pengetahuan. Ini menunjukkan bahwa mahasiswa pada umumnya memiliki sikap positif dan mulai berusaha menerapkan keamanan informasi dalam kehidupan sehari-hari, meskipun masih ada kekurangan dalam hal pemahaman dan konsistensi perilaku. Temuan ini juga menunjukkan adanya kesenjangan antara apa yang diketahui, diyakini, dan dilakukan oleh mahasiswa dalam menjaga keamanan informasi. Oleh karena itu, upaya peningkatan kesadaran perlu diarahkan tidak hanya pada pemberian informasi, tetapi juga pada penguatan sikap dan pembiasaan perilaku aman dalam aktivitas digital sehari-hari. Kontribusi penelitian ini terletak pada pemetaan kesadaran keamanan informasi mahasiswa secara lebih rinci berdasarkan dimensi pengetahuan, sikap, dan perilaku, sehingga dapat menjadi referensi bagi pengembangan program edukasi keamanan informasi yang lebih efektif di lingkungan universitas. Hasil penelitian juga sejalan dengan studi sebelumnya yang menunjukkan bahwa kesadaran keamanan informasi dipengaruhi oleh sikap dan perilaku, namun menambahkan wawasan baru

mengenai perbedaan skor antar-dimensi. Meski demikian, keterbatasan penelitian ini terletak pada fokusnya yang hanya pada mahasiswa saja di Universitas Mataram sehingga temuan hanya mencerminkan kondisi di universitas tersebut. Untuk penelitian berikutnya, disarankan melibatkan dosen dan staf universitas, menambah jumlah responden, serta menelaah faktor-faktor yang memengaruhi konsistensi penerapan keamanan informasi di seluruh civitas universitas.

DAFTAR PUSTAKA

[1] A. Putri et al., "Keamanan Online dalam Media Sosial: Pentingnya Perlindungan Data Pribadi di Era Digital (Studi Kasus Desa Pematang Jering)," *Jurnal Pengabdian Nasional (JPN) Indonesia*, vol. 6, no. 1, pp. 38–52, Nov. 28, 2024. DOI: 10.35870/jpni.v6i1.1097.

[2] D. Nurjanah dan S. Destya, "Pengukuran Tingkat Kesadaran Keamanan Informasi Mahasiswa pada Pembelajaran Online," *Jurnal Sistem dan Teknologi Informasi (JustIN)*, vol. 10, no. 1, p. 81, Jan. 31, 2022. DOI: 10.26418/justin.v10i1.44362.

[3] M. Alfian dan R. Rahman, "Keamanan Jaringan pada Perguruan Tinggi," en, *Jurnal Riset Sistem Informasi*, vol. 1, no. 3, pp. 59–64, Jul. 24, 2024. DOI: 10.69714/qgnbgv11.

[4] A. Jazuli, I. Salamah, dan S. Soim, "Deteksi Tingkat Kerentanan Keamanan Website dengan Metode Manual Pentest dan Tools Xspear," *Edumatic: Jurnal Pendidikan Informatika*, vol. 8, no. 2, pp. 418–427, Dec. 19, 2024. DOI: 10.29408/edumatic.v8i2.27109.

[5] D. Dafid dan D. P. Kesuma, "Metode MCDA Untuk Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 7, no. 1, pp. 11–20, Apr. 15, 2020. DOI: 10.35957/jatisi.v7i1.296.

[6] H. Humaira et al., "Membangun Kesadaran Mahasiswa Dalam Menghadapi Tantangan Cyber Security di Era Digital," en, *Iuris Studia: Jurnal Kajian Hukum*, vol. 5, no. 3, pp. 847–851, Dec. 17, 2024. DOI: 10.55357/is.v5i3.740.

[7] B. Alkhazi et al., "Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior," *IEEE Access*, vol. 10, pp. 132 132–132 143, 2022. DOI: 10.1109/ACCESS.2022.3230286.

[8] M. Anastasiah dan H. Pandia, "Analisis Perilaku Pengguna Mobile Banking Terhadap Keamanan Informasi Menggunakan Metode Human Aspects of Information Security Questionnaire (HAIS-Q)," *Innovative: Journal Of Social Science Research*, vol. 4, no. 2, pp. 4067–4078, Apr. 4, 2024. DOI: 10.31004/innovative.v4i2.9684.

[9] Y. A. Styoutomo dan Y. Ruldeviyani, "Information Security Awareness Raising Strategy Using Fuzzy AHP Method with HAIS-Q and ISO/IEC 27001:2013: A Case Study of XYZ Financial Institution," *CommIT (Communication and Information Technology) Journal*, vol. 17, no. 2, pp. 133–149, Sep. 6, 2023. DOI: 10.21512/commit.v17i2.8272.

[10] I. R. Munthe dan I. Purnama, "Uji Tingkat Kesadaran Keamanan Informasi Pengguna Smartphone (Studi Kasus: Amik Labuhan Batu)," *Jurnal Teknik Informasi dan Komputer (Tekinkom)*, vol. 2, no. 2, p. 156, Dec. 30, 2019. DOI: 10.37600/tekinkom.v2i2.113.

[11] A. Gofur, R. Fathoni Aji, dan H. Kurniawan, "Pengukuran Kesadaran Keamanan Informasi Pegawai: Studi Kasus PT Meshindo Jayatama," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 11, no. 2, pp. 315–320, Apr. 25, 2024. DOI: 10.25126/jtiik.20241128106.

[12] M. S. Mahardika et al., "Measurement of Employee Awareness Levels for Information Security at the Center of Analysis and Information Services Judicial Commission Republic of Indonesia," *Advances in Science, Technology and Engineering Systems Journal*, vol. 5, no. 3, pp. 501–509, 2020. DOI: 10.25046/aj050362.

[13] T. Ranas et al., "Measuring Information Security Awareness of Client's Information Security: Case Study at PT XYZ," *International Journal of Advances in Electronics and Computer Science (IJAECS)*, vol. 7, no. 7, pp. 1–6, 2020.

[14] A. Zulfia et al., "Measurement of Employee Information Security Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q): Case Study at PT. PQS," in *2019 5th International Conference on Computing Engineering and Design (ICCED)*, Singapore, Singapore: IEEE, Apr. 2019, pp. 1–5. DOI: 10.1109/ICCED46541.2019.9161120.

[15] F. N. Shakti dan A. N. Hidayanto, "Measurement of Employee Information Security Awareness: Case Study at Financial Institution," *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, vol. 9, no. 2, pp. 172–179, Feb. 1, 2024. DOI: 10.33480/jitk.v9i2.4163.

[16] S. K. Ahmed, "How to Choose a Sampling Technique and Determine Sample Size for Research: A Simplified Guide for Researchers," en, *Oral Oncology Reports*, vol. 12, p. 100 662, Dec. 2024. DOI: 10.1016/j.oor.2024.100662.

[17] R. N. Amalia, R. S. Dianingati, dan E. Annisaa', "Pengaruh Jumlah Responden terhadap Hasil Uji Validitas dan Reliabilitas Kuesioner Pengetahuan dan Perilaku Swamedikasi," *Generics: Journal of Research in Pharmacy*, vol. 2, no. 1, pp. 9–15, May 18, 2022. DOI: 10.14710/genres.v2i1.12271.

[18] G. B. N. Alvito, *Pengukuran Tingkat Kesadaran Keamanan Informasi Pada Mahasiswa Fakultas Informatika Menggunakan Human Aspect of Information Security Questionnaire (HAIS-Q) di Universitas Telkom Bandung*, id. Universitas Telkom, S1 Teknologi Informasi, Oct. 11, 2024.

[19] K. Kusnadi et al., "Pengukuran Tingkat Kesadaran Keamanan Informasi Dan Privasi Di Kalangan Mahasiswa Dengan HAIS-Q Instrument," *Etika Teknologi Informasi*, vol. 1, no. 1, pp. 1–9, Dec. 5, 2024.

[20] T. Tan et al., "Kesadaran Keamanan Siber pada Kalangan Mahasiswa Universitas di Kota Batam," *Jurnal Teknologi dan Informasi*, vol. 14, no. 2, pp. 163–173, Sep. 2, 2024. DOI: 10.34010/jati.v14i2.12518.