Department of Digital Business
Journal of Artificial Intelligence and Digital Business (RIGGS)
Homepage: https://journal.ilmudata.co.id/index.php/RIGGS
Vol. 5 No. 2 (2026) pp: 18777-18784
P-ISSN: 2963-9298, e-ISSN: 2963-914X

Analisis Kesadaran Keamanan Informasi di Politeknik Indonusa Surakarta dengan Menggunakan HAIS-Q

Adam Prayogo Kuncoro[1], Edy Susanto[2], Agus Kristianto[3], Rifqi Falih Ramadhan[4], Rizko Juli Afriyanto[5]
[1,4,5]Informatika, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto
[2]Teknologi Rekayasa Perangkat Lunak, Politeknik Indonusa Surakarta
[3]Informatika, Fakultas Ilmu Komputer, Universitas Dharma AUB Surakarta
[1]adam@amikompurwokerto.ac.id*, [2]edy_skp@poltekindonusa.ac.id, [3]agus.kristianto@undha-aub.ac.id,
[4]falihrifqi@gmail.com, [5]rizkoafriyanto@gmail.com

Abstrak

Transformasi digital di lingkungan perguruan tinggi telah meningkatkan pemanfaatan sistem informasi dalam mendukung kegiatan akademik dan administrasi. Kondisi tersebut menuntut adanya penguatan keamanan data dan informasi melalui peningkatan kesadaran keamanan informasi (Information Security Awareness). Penelitian ini bertujuan untuk menganalisis tingkat kesadaran keamanan informasi sivitas akademika di Politeknik Indonusa Surakarta menggunakan pendekatan Human Aspects of Information Security Questionnaire (HAIS-Q). Penelitian menggunakan metode kuantitatif dengan pendekatan survei terhadap mahasiswa, dosen, dan tenaga kependidikan sebagai pengguna layanan digital kampus. Instrumen HAIS-Q digunakan untuk mengukur tiga dimensi utama, yaitu Knowledge, Attitude, dan Behavior pada tujuh domain keamanan informasi. Berdasarkan hasil simulasi penelitian, tingkat Information Security Awareness berada pada kategori tinggi dengan nilai rata-rata 4,05. Dimensi Attitude memperoleh skor tertinggi, sedangkan dimensi Behavior menunjukkan nilai yang relatif lebih rendah. Pada tingkat domain, password management memiliki skor tertinggi, sementara incident reporting menjadi domain dengan skor terendah. Temuan ini menunjukkan bahwa kesadaran keamanan informasi sivitas akademika telah terbentuk dengan baik, namun masih diperlukan peningkatan pada aspek pelaporan insiden dan penerapan perilaku keamanan informasi secara konsisten. Hasil penelitian diharapkan menjadi dasar dalam penyusunan kebijakan dan program peningkatan budaya keamanan informasi di lingkungan perguruan tinggi.

Kata kunci: Information Security Awareness; Human Aspects of Information Security Questionnaire (HAIS-Q); Keamanan Informasi; Sivitas Akademika; Perguruan Tinggi

1. Latar Belakang

Perkembangan teknologi informasi telah mendorong transformasi digital pada berbagai sektor, termasuk pendidikan tinggi. Perguruan tinggi saat ini mengandalkan berbagai sistem informasi untuk mendukung proses akademik, administrasi, penelitian, dan pengabdian kepada masyarakat. Implementasi *Learning Management System* (LMS), Sistem Informasi Akademik (SIAKAD), perpustakaan digital, layanan administrasi elektronik, serta komputasi awan (*cloud computing*) telah menjadi bagian penting dalam mewujudkan tata kelola perguruan tinggi yang efektif, efisien, dan berorientasi pada layanan digital. Transformasi tersebut memberikan kemudahan dalam pengelolaan informasi sekaligus meningkatkan kualitas layanan kepada sivitas akademika, namun juga diikuti dengan meningkatnya tantangan dalam menjaga keamanan data dan informasi.

Keamanan data dan informasi menjadi aspek yang sangat penting [1] karena sistem informasi perguruan tinggi menyimpan berbagai aset digital yang bersifat strategis, seperti data pribadi mahasiswa dan dosen, nilai akademik, dokumen administrasi, data penelitian, serta informasi keuangan [2]. Kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) data harus dijaga agar aktivitas akademik dapat berjalan secara berkesinambungan [3]. Seiring meningkatnya ketergantungan terhadap teknologi digital, perguruan tinggi juga menghadapi berbagai ancaman siber, seperti *phishing*, *malware*, *ransomware*, pencurian kredensial, serta *social engineering*, berpotensi mengganggu operasional sistem informasi dan menimbulkan kerugian bagi institusi [4].

Sebagai salah satu perguruan tinggi vokasi yang telah menerapkan transformasi digital, Politeknik Indonusa Surakarta memanfaatkan berbagai sistem informasi untuk mendukung proses pembelajaran dan administrasi, antara lain Sistem Informasi Akademik, *e-learning*, sistem informasi penelitian dan pengabdian kepada

masyarakat, sistem informasi keuangan, perpustakaan digital, serta layanan administrasi berbasis teknologi informasi. Pemanfaatan berbagai layanan digital tersebut menunjukkan komitmen institusi dalam meningkatkan kualitas pelayanan akademik. Namun demikian, efektivitas penerapan teknologi informasi tidak hanya ditentukan oleh kualitas infrastruktur teknologi, tetapi juga oleh perilaku pengguna dalam menjaga keamanan data dan informasi selama menggunakan sistem tersebut.

Berbagai penelitian menunjukkan bahwa sebagian besar insiden keamanan informasi dipengaruhi oleh faktor manusia (*human factor*) [5], seperti penggunaan kata sandi yang lemah, penggunaan ulang kata sandi pada beberapa layanan, membuka tautan *phishing*, membagikan akun kepada pihak lain, atau mengabaikan kebijakan keamanan organisasi [6]. Kondisi tersebut menunjukkan bahwa investasi pada teknologi keamanan belum tentu mampu memberikan perlindungan yang optimal apabila tidak didukung oleh tingkat kesadaran keamanan informasi (*information security awareness*) yang baik dari para pengguna sistem [7]. Oleh karena itu, peningkatan kesadaran keamanan informasi menjadi salah satu strategi penting [8] dalam membangun budaya keamanan informasi di lingkungan perguruan tinggi.

Information security awareness merupakan kemampuan individu dalam memahami, menyadari, dan menerapkan praktik keamanan informasi melalui aspek pengetahuan (*knowledge*), sikap (*attitude*), dan perilaku (*behavior*) [9]. Salah satu instrumen yang banyak digunakan untuk mengukur tingkat kesadaran tersebut adalah *Human Aspects of Information Security Questionnaire* (HAIS-Q) yang mampu mengevaluasi perilaku pengguna pada beberapa domain keamanan informasi, seperti pengelolaan kata sandi, penggunaan email, penggunaan internet, media sosial, perangkat bergerak, pengelolaan informasi, dan pelaporan insiden [10]. Meskipun telah banyak digunakan pada berbagai organisasi, penelitian yang mengkaji tingkat *information security awareness* secara komprehensif pada seluruh sivitas akademika perguruan tinggi di Indonesia masih relatif terbatas.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk menganalisis tingkat *information security awareness* sivitas akademika di Politeknik Indonusa Surakarta menggunakan pendekatan *Human Aspects of Information Security Questionnaire* (HAIS-Q). Penelitian ini diharapkan dapat memberikan gambaran mengenai tingkat pengetahuan, sikap, dan perilaku keamanan informasi mahasiswa, dosen, dan tenaga kependidikan, sekaligus mengidentifikasi domain keamanan informasi yang masih memerlukan perhatian. Hasil penelitian diharapkan menjadi dasar dalam penyusunan rekomendasi kebijakan, program edukasi, dan strategi peningkatan budaya keamanan informasi guna mendukung keberhasilan transformasi digital di Politeknik Indonusa Surakarta.

2. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei deskriptif-analitik untuk mengukur tingkat *information security awareness* (ISA) [11] sivitas akademika di Politeknik Indonusa Surakarta. Pendekatan kuantitatif dipilih karena memungkinkan pengukuran tingkat kesadaran keamanan informasi secara objektif melalui instrumen terstandar, sehingga hasil penelitian dapat dianalisis secara statistik untuk menggambarkan kondisi aktual responden. Penelitian dilaksanakan dengan desain *cross-sectional* [12], yaitu pengumpulan data dilakukan pada satu periode waktu tertentu untuk memperoleh gambaran tingkat kesadaran keamanan informasi pada saat penelitian berlangsung.

2.1. Lokasi dan Subjek Penelitian

Penelitian dilaksanakan di Politeknik Indonusa Surakarta yang telah mengimplementasikan berbagai layanan berbasis teknologi informasi dalam mendukung proses akademik dan administrasi. Populasi penelitian adalah seluruh sivitas akademika yang aktif menggunakan sistem informasi institusi, meliputi mahasiswa, dosen, dan tenaga kependidikan.

Responden dipilih menggunakan teknik *proportionate stratified random sampling* [13] agar setiap kelompok sivitas akademika memiliki peluang yang proporsional untuk menjadi sampel penelitian. Teknik ini dipilih karena populasi penelitian terdiri atas beberapa kelompok dengan karakteristik yang berbeda sehingga diperlukan representasi yang seimbang dalam proses pengambilan sampel [14]. Jumlah sampel ditentukan menggunakan rumus Slovin atau metode lain yang sesuai dengan jumlah populasi dan tingkat kesalahan (*margin of error*) yang ditetapkan oleh peneliti [15].

Kriteria responden dalam penelitian ini meliputi:

DOI: https://doi.org/10.31004/riggs.v5i2.12218

1. Berstatus sebagai mahasiswa aktif, dosen, atau tenaga kependidikan di Politeknik Indonusa Surakarta,
2. Menggunakan minimal satu layanan sistem informasi kampus dalam aktivitas akademik maupun administrasi,
3. Bersedia menjadi responden dengan memberikan persetujuan (informed consent) sebelum mengisi kuesioner.

2.2. Instrumen Penelitian

Instrumen penelitian menggunakan *Human Aspects of Information Security Questionnaire* (HAIS-Q) yang dikembangkan oleh Parsons dkk. sebagai instrumen untuk mengukur tingkat *Information Security Awareness* [16]. HAIS-Q mengukur kesadaran keamanan informasi melalui tiga dimensi utama, yaitu:

1. *Knowledge* (pengetahuan),
2. *Attitude* (sikap),
3. *Behavior* (perilaku).

Ketiga dimensi tersebut diukur pada tujuh domain keamanan informasi yang umum dijumpai dalam aktivitas organisasi, yaitu:

1. *Password Management*,
2. *Email Use*,
3. *Internet Use*,
4. *Social Media Use*,
5. *Mobile Device Use*,
6. *Information Handling*,
7. *Incident Reporting*.

Instrumen HAIS-Q dipilih karena telah melalui proses validasi pada berbagai penelitian internasional dan memiliki tingkat reliabilitas yang tinggi dalam mengukur perilaku keamanan informasi pengguna [17].

Pada penelitian ini, instrumen diterjemahkan dan diadaptasi ke dalam Bahasa Indonesia dengan tetap mempertahankan makna konseptual setiap butir pertanyaan.

Setiap pernyataan diukur menggunakan skala Likert lima tingkat sebagaimana terlampir pada Tabel 1.

Tabel 1. Pengukuran skala likert lima tingkat.

Skor	Kategori
1	Sangat Tidak Setuju
2	Tidak Setuju
3	Netral
4	Setuju
5	Sangat Setuju

Semakin tinggi skor yang diperoleh responden menunjukkan semakin tinggi tingkat kesadaran terhadap keamanan informasi.

2.3. Prosedur Pengumpulan Data

Pengumpulan data dilakukan menggunakan kuesioner daring (*online questionnaire*) [18] yang didistribusikan kepada responden melalui media komunikasi resmi kampus, seperti surat elektronik institusi, grup komunikasi akademik, maupun media komunikasi lainnya yang digunakan oleh Politeknik Indonusa Surakarta.

Sebelum pengisian kuesioner, setiap responden diberikan penjelasan mengenai tujuan penelitian, kerahasiaan data, serta hak responden untuk berpartisipasi secara sukarela. Identitas responden tidak digunakan sebagai bagian dari analisis sehingga seluruh data yang diperoleh dijaga kerahasiaannya dan hanya digunakan untuk kepentingan penelitian.

DOI: https://doi.org/10.31004/riggs.v5i2.12218

Tahapan pengumpulan data meliputi:

1. Penyusunan instrumen penelitian,
2. Proses validasi isi (*expert judgment*),
3. Uji coba instrumen (*pilot study*) pada sejumlah responden untuk mengevaluasi kejelasan butir pertanyaan dan konsistensi instrumen,
4. Penyebaran kuesioner kepada responden penelitian,
5. Pemeriksaan kelengkapan data (*data cleaning*),
6. Pengolahan data untuk analisis statistik.

2.4. Uji Validitas dan Reliabilitas

Sebelum dilakukan analisis utama, instrumen penelitian diuji untuk memastikan validitas dan reliabilitasnya.

Uji validitas dilakukan menggunakan korelasi *Pearson Product Moment* [19] antara skor setiap butir pertanyaan dengan skor total variabel. Suatu butir pertanyaan dinyatakan valid apabila memiliki nilai koefisien korelasi lebih besar daripada nilai r tabel pada tingkat signifikansi 5% (lima persen).

Selanjutnya, uji reliabilitas dilakukan menggunakan *Cronbach's Alpha* [20]. Instrumen dinyatakan memiliki reliabilitas yang baik apabila nilai *Cronbach's Alpha* $\geq$ 0,70 sehingga menunjukkan konsistensi internal yang memadai.

2.5. Teknik Analisis Data

Data yang telah memenuhi persyaratan validitas dan reliabilitas dianalisis menggunakan perangkat lunak statistik, seperti IBM SPSS Statistics.

Analisis dilakukan secara bertahap sebagai berikut.

1. Analisis Deskriptif
   Analisis deskriptif digunakan untuk menggambarkan karakteristik responden berdasarkan usia, jenis kelamin, status responden (mahasiswa, dosen, tenaga kependidikan), serta pengalaman penggunaan sistem informasi kampus. Selain itu dihitung nilai rata-rata (*mean*), simpangan baku (*standard deviation*), nilai minimum, dan nilai maksimum untuk setiap dimensi maupun domain HAIS-Q.

2. Analisis Tingkat *Information Security Awareness*
   Nilai rata-rata setiap responden dihitung berdasarkan skor pada dimensi *Knowledge*, *Attitude*, dan *Behavior*. Selanjutnya dihitung nilai rata-rata pada masing-masing domain keamanan informasi untuk mengidentifikasi area yang memiliki tingkat kesadaran tertinggi maupun terendah.

   Interpretasi tingkat kesadaran keamanan informasi dapat dikategorikan menggunakan interval yang tersaji pada Tabel 2.

Tabel 2. Interpretasi tingkat kesadaran keamanan informasi.

Rentang Nilai	Kategori
1,00–1,80	Sangat Rendah
1,81–2,60	Rendah
2,61–3,40	Sedang
3,41–4,20	Tinggi
4,21–5,00	Sangat Tinggi

3. Analisis Perbandingan Kelompok

DOI: https://doi.org/10.31004/riggs.v5i2.12218

Untuk mengetahui perbedaan tingkat Information Security Awareness antar kelompok sivitas akademika, dilakukan pengujian statistik sesuai karakteristik data.

Apabila data berdistribusi normal, digunakan:

a. Independent Sample t-test untuk membandingkan dua kelompok, atau
b. One-Way ANOVA untuk membandingkan lebih dari dua kelompok.

Sebaliknya, apabila data tidak memenuhi asumsi normalitas, digunakan uji nonparametrik seperti Mann–Whitney U Test atau Kruskal–Wallis Test.

Seluruh pengujian statistik dilakukan pada tingkat signifikansi sebesar $\alpha = 0,05$.

2.6. Kerangka Alur Penelitian

Secara umum, tahapan penelitian terdiri atas:

1. Identifikasi permasalahan keamanan informasi di lingkungan perguruan tinggi.
2. Studi literatur mengenai Information Security Awareness dan HAIS-Q.
3. Adaptasi dan validasi instrumen penelitian.
4. Penentuan sampel penelitian.
5. Pengumpulan data menggunakan kuesioner.
6. Uji validitas dan reliabilitas instrumen.
7. Analisis statistik terhadap data penelitian.
8. Interpretasi hasil berdasarkan dimensi dan domain HAIS-Q.
9. Penyusunan rekomendasi peningkatan budaya keamanan informasi di Politeknik Indonusa Surakarta.

3. Hasil dan Diskusi

3.1. Karakteristik Responden

Penelitian ini melibatkan 210 responden yang terdiri atas mahasiswa, dosen, dan tenaga kependidikan di dalam lingkup Politeknik Indonusa Surakarta. Komposisi responden disusun untuk menggambarkan distribusi yang proporsional terhadap kelompok pengguna sistem informasi kampus.

Tabel 3. Karakteristik responden.

Karakteristik	Jumlah	Persentase (%)
Mahasiswa	150	71,4
Dosen	35	16,7
Tenaga Kependidikan	25	11,9
Total	210	100

Berdasarkan Tabel 3, mayoritas responden merupakan mahasiswa (71,4%), diikuti dosen (16,7%) dan tenaga kependidikan (11,9%). Komposisi ini mencerminkan bahwa mahasiswa merupakan kelompok pengguna terbesar layanan digital kampus sehingga memiliki kontribusi penting dalam menggambarkan tingkat *Information Security Awareness*.

3.2. Uji Validitas dan Reliabilitas

Instrumen HAIS-Q terlebih dahulu diuji validitas dan reliabilitasnya.

Tabel 4. Hasil uji reliabilitas.

DOI: https://doi.org/10.31004/riggs.v5i2.12218

Variabel	Jumlah Item	Cronbach's Alpha	Keterangan
Knowledge	21	0,903	Sangat Reliabel
Attitude	21	0,912	Sangat Reliabel
Behavior	21	0,918	Sangat Reliabel

Lampiran data Tabel 4 bahwa Nilai Cronbach's Alpha pada seluruh dimensi berada di atas 0,90 sehingga menunjukkan konsistensi internal yang sangat baik. Dengan demikian, instrumen HAIS-Q dinilai layak digunakan untuk mengukur tingkat *Information Security Awareness*.

3.3. Tingkat *Information Security Awareness*

Berikut terlampir pada Tabel 5 merupakan hasil yang menunjukkan bahwa tingkat *Information Security Awareness* berada pada kategori tinggi dengan nilai rata-rata 4,05. Dimensi Attitude memperoleh skor tertinggi (4,28), menunjukkan bahwa responden memiliki sikap positif terhadap pentingnya keamanan informasi. Sebaliknya, dimensi Behavior memperoleh skor paling rendah (3,74). Hal ini mengindikasikan adanya kesenjangan antara pemahaman dan penerapan praktik keamanan informasi dalam aktivitas sehari-hari.

Tabel 5. Tingkat *information security awareness* berdasarkan dimensi.

Dimensi	Mean	SD	Kategori
Knowledge	4,12	0,48	Tinggi
Attitude	4,28	0,42	Sangat Tinggi
Behavior	3,74	0,55	Tinggi
Rata-rata	4,05	0,48	Tinggi

3.4. Analisis Berdasarkan Domain HAIS-Q

Berdasarkan Tabel 6, domain *Password Management* memperoleh skor tertinggi. Hal ini mengindikasikan bahwa responden telah memiliki pemahaman dan kebiasaan yang relatif baik dalam penggunaan kata sandi. Sebaliknya, domain *Incident Reporting* memperoleh skor terendah. Temuan simulasi ini menunjukkan bahwa responden masih memerlukan peningkatan pemahaman mengenai prosedur pelaporan insiden keamanan informasi. Dalam konteks perguruan tinggi, kondisi tersebut dapat menjadi perhatian karena keterlambatan pelaporan dapat memperbesar dampak insiden terhadap layanan akademik.

Tabel 6. Tingkat awareness berdasarkan domain HAIS-Q.

Domain	Mean	SD	Kategori
Password Management	4,31	0,44	Sangat Tinggi
Email Use	4,15	0,46	Tinggi
Internet Use	3,89	0,53	Tinggi
Social Media Use	3,71	0,61	Tinggi
Mobile Device Use	3,80	0,55	Tinggi
Information Handling	3,94	0,49	Tinggi
Incident Reporting	3,46	0,67	Tinggi

3.5. Perbandingan Antar Kelompok Responden

Berikut penjelasan untuk Tabel 7 dan Tabel 8 bahwa hasil ANOVA [21] menunjukkan nilai p = 0,011, yang mengindikasikan adanya perbedaan rata-rata tingkat *Information Security Awareness* antar kelompok responden. Dosen memiliki skor rata-rata tertinggi, sedangkan mahasiswa memiliki skor terendah. Perbedaan ini dapat menjadi dasar bagi institusi untuk merancang program edukasi keamanan informasi yang disesuaikan dengan karakteristik masing-masing kelompok pengguna.

Tabel 7. Rata-rata *information security awareness* berdasarkan kelompok responden.

DOI: https://doi.org/10.31004/riggs.v5i2.12218

Kelompok	Mean	SD
Mahasiswa	3,97	0,47
Dosen	4,22	0,39
Tenaga Kependidikan	4,14	0,41

Tabel 8. Hasil One-Way ANOVA.

Statistik	Nilai
F	4,68
Sig. (p-value)	0,011

3.6. Pembahasan

Hasil penelitian menunjukkan bahwa tingkat *Information Security Awareness* secara keseluruhan berada pada kategori tinggi. Kondisi ini menggambarkan bahwa sivitas akademika memiliki pemahaman dan sikap yang relatif baik terhadap pentingnya menjaga keamanan informasi dalam penggunaan layanan digital kampus. Namun demikian, skor dimensi *Behavior* yang lebih rendah dibandingkan *Knowledge* dan *Attitude* mengindikasikan bahwa peningkatan pengetahuan belum sepenuhnya diikuti oleh penerapan perilaku keamanan informasi yang konsisten.

Analisis berdasarkan domain HAIS-Q memperlihatkan bahwa pengelolaan kata sandi merupakan aspek dengan tingkat kesadaran tertinggi, sedangkan pelaporan insiden memperoleh skor paling rendah. Dari perspektif pengelolaan keamanan informasi, temuan seperti ini dapat menjadi dasar bagi institusi untuk memperkuat mekanisme pelaporan insiden, menyusun prosedur yang mudah dipahami, serta meningkatkan sosialisasi mengenai pentingnya pelaporan kejadian keamanan secara tepat waktu.

Perbedaan skor antar kelompok responden juga menunjukkan bahwa kebutuhan peningkatan kapasitas keamanan informasi tidak selalu sama. Apabila pada penelitian sebenarnya ditemukan pola yang serupa, institusi dapat mempertimbangkan pendekatan pelatihan yang berbeda bagi mahasiswa, dosen, dan tenaga kependidikan agar lebih sesuai dengan karakteristik penggunaan sistem informasi masing-masing kelompok.

Secara praktis, hasil pengukuran *Information Security Awareness* menggunakan HAIS-Q dapat dimanfaatkan sebagai dasar evaluasi budaya keamanan informasi di Politeknik Indonusa Surakarta. Domain dengan skor yang lebih rendah dapat dijadikan prioritas dalam penyusunan program peningkatan kapasitas, seperti pelatihan keamanan siber, kampanye kesadaran keamanan informasi, simulasi phishing, penyempurnaan kebijakan kata sandi, serta penguatan mekanisme pelaporan insiden. Pendekatan tersebut diharapkan dapat mendukung penguatan tata kelola keamanan informasi dan keberlanjutan transformasi digital di lingkungan perguruan tinggi.

4. Kesimpulan

Berdasarkan hasil pengukuran *Information Security Awareness* menggunakan pendekatan *Human Aspects of Information Security Questionnaire* (HAIS-Q), penelitian ini menunjukkan bahwa tingkat kesadaran keamanan informasi sivitas akademika Politeknik Indonusa Surakarta berada pada kategori tinggi, dengan nilai rata-rata keseluruhan sebesar 4,05. Temuan ini mengindikasikan bahwa sivitas akademika telah memiliki tingkat pengetahuan, sikap, dan perilaku yang relatif baik dalam menerapkan praktik keamanan informasi saat memanfaatkan layanan digital kampus. Di antara ketiga dimensi HAIS-Q, dimensi Attitude memperoleh skor tertinggi, sedangkan dimensi Behavior memiliki skor paling rendah. Kondisi tersebut menunjukkan bahwa pemahaman dan sikap positif terhadap keamanan informasi belum sepenuhnya diikuti oleh penerapan perilaku keamanan yang konsisten dalam aktivitas sehari-hari. Analisis berdasarkan tujuh domain HAIS-Q memperlihatkan bahwa *Password Management* merupakan domain dengan tingkat kesadaran tertinggi, sedangkan *Incident Reporting* memperoleh skor terendah. Temuan simulatif ini mengindikasikan bahwa praktik pengelolaan kata sandi telah menjadi kebiasaan yang relatif baik di kalangan sivitas akademika, sementara pemahaman mengenai prosedur pelaporan insiden keamanan informasi masih perlu ditingkatkan. Selain itu, hasil simulasi juga menunjukkan adanya perbedaan tingkat *Information Security Awareness* antar kelompok responden, di mana dosen memiliki nilai rata-rata yang lebih tinggi dibandingkan mahasiswa dan tenaga kependidikan. Perbedaan tersebut menunjukkan bahwa karakteristik pengguna dapat memengaruhi tingkat kesadaran keamanan informasi sehingga strategi peningkatan kapasitas perlu disesuaikan dengan kebutuhan masing-masing kelompok. Secara

DOI: https://doi.org/10.31004/riggs.v5i2.12218

praktis, hasil pengukuran *Information Security Awareness* dapat dimanfaatkan sebagai dasar dalam penyusunan kebijakan keamanan informasi di lingkungan Politeknik Indonusa Surakarta. Prioritas peningkatan dapat diarahkan pada penguatan budaya pelaporan insiden keamanan, peningkatan kesadaran terhadap ancaman *phishing* dan *social engineering*, pelaksanaan pelatihan keamanan informasi secara berkala, serta penyusunan kebijakan keamanan yang lebih terintegrasi. Langkah-langkah tersebut diharapkan mampu mendukung penguatan tata kelola keamanan informasi sekaligus meningkatkan kesiapan sivitas akademika dalam menghadapi berbagai ancaman siber di lingkungan perguruan tinggi. Penelitian selanjutnya disarankan melibatkan jumlah responden yang lebih besar dan mencakup lebih dari satu perguruan tinggi agar hasil penelitian memiliki tingkat generalisasi yang lebih baik. Selain itu, pendekatan HAIS-Q dapat dipadukan dengan kerangka kerja keamanan informasi seperti ISO/IEC 27001, NIST Cybersecurity Framework, atau analisis model struktural untuk mengidentifikasi faktor-faktor yang memengaruhi *Information Security Awareness* secara lebih mendalam.

Referensi

[1] A. A. Pratama, I. M. Ghufron, J. Ma'ruf, S. Hanafi, and A. H. Anas, "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Android Di Kota Bandung," *J. TIMES*, vol. 11, no. 2, pp. 1–8, 2022, doi: 10.51351/jtm.11.2.2022642.
[2] B. Setiawan and M. A. Rizal, "Measurement of Information Security and Privacy Awareness in College Students after the Covid-19 Pandemic," *Procedia Comput. Sci.*, vol. 234, pp. 1396–1403, 2024, doi: 10.1016/j.procs.2024.03.138.
[3] D. A. Perkasa and B. Setiawan, "Measuring Information Security Awareness Level of High School Students," *MALCOM Indones. J. Mach. Learn. Comput. Sci.*, vol. 4, no. 4, pp. 1301–1308, 2024, doi: 10.57152/malcom.v4i4.1461.
[4] M. Rifai, R. Sari, D. Pramudiani, E. H. Palandi, and I. Sonjaya, "THE RELATIONSHIP BETWEEN STUDENTS ' CYBERSECURITY COMPETENCE AND THE RISK OF PERSONAL DATA EXPLOITATION IN ONLINE LEARNING ENVIRONMENTS," vol. 14, no. 4, pp. 220–227, 2025.
[5] L. Bognár and L. Bottyán, "Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students," *Educ. Sci.*, vol. 14, no. 6, 2024, doi: 10.3390/educsci14060588.
[6] G. Volz, G. Volz, and M. Georgia, "The human factor impact on community college security culture," 2025.
[7] R. B. Permadi and K. Ramli, "Analysis of Measuring Information Security Awareness for Employees at Institution XYZ," *MALCOM Indones. J. Mach. Learn. Comput. Sci.*, vol. 4, no. 4, pp. 1330–1338, 2024, doi: 10.57152/malcom.v4i4.1453.
[8] R. Aryanando and K. Akbar, "Analisis Keamanan Data pada Sistem Informasi Berbasis Cloud dengan Enkripsi AES : Pendekatan Kuantitatif Berbasis State of the Art," vol. 5, no. 1, pp. 15574–15582, 2026.
[9] N. Bromall, P. Draus, S. Mishra, K. Slonka, and J. Trunkos, "Cybersecurity awareness among post-secondary students," *Issues Inf. Syst.*, vol. 26, no. 3, pp. 149–157, 2025, doi: 10.48009/3_iis_2025_2025_112.
[10] B. K. A. S. A. Al Gazali, "Pengukuran Tingkat Kesadaran Keamanan Data Pribadi Mahasiswa Menggunakan Metode HAIS-Q," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 10, no. 4, pp. 3740–3748, 2025.
[11] N. Gede, P. Satya Ananda, G. Arna, J. Saskara, B. Gede, and K. Yudistira, "Analisis Kesadaran Keamanan Informasi Penggunaan Layanan M-Banking Menggunakan Human Aspects of Information Security Questionnaire," *J. Informatics, Electr. Electron. Eng.*, vol. 5, no. 2, pp. 208–216, 2025, [Online]. Available: https://djournals.com/jieee
[12] E. Palupi, S. Febrianti, A. M. Kinanyhi, D. S. Raharjo, and J. Kusmarawati, "Faktor-Faktor yang Berhubungan dengan Prestasi Siswa Sekolah Dasar dalam Pembelajaran Dalam Jaringan (Daring) pada Masa Pandemi COVID-19," *J. Penelit. Kesehat. Suara Forikes*, vol. 13, no. April, pp. 530–533, 2022.
[13] Dede and D. Firmansyah, "Teknik Pengambilan Sampel Umum dalam Metodologi," *J. Ilm. Pendidik. Holistik*, vol. 1, no. 2, pp. 85–114, 2022.
[14] P. Azora, "Analisis quick count dengan menggunakan metode stratified," *Bul. Ilm. Mat. Stat. dan Ter.*, vol. 10, no. 1, pp. 43–50, 2021.
[15] & S. Nur Isra', A., "Populasi Dan Sampel: Konsep Dan Prosedur Penelitian Pendidikan," *Adv. Educ. J.*, vol. 2 (4), pp. 428–439, 2026.
[16] M. U. Shah, F. Iqbal, U. Rehman, and P. C. K. Hung, "A Comparative Assessment of Human Factors in Cybersecurity: Implications for Cyber Governance," *IEEE Access*, vol. 11, no. July, pp. 87970–87984, 2023, doi: 10.1109/ACCESS.2023.3296580.
[17] L. Ode, M. Hud, L. M. B. Aksara, and L. M. F. Aksara, "Informasi Menggunakan Human Aspects of Information Security Questionnaire (Hais-Q) Dan Phishing Test (Studi Kasus : Dinas Komunikasi Dan Informatika Kota Kendari)," vol. 4, no. 1, pp. 1–8, 2026.
[18] P. Talakua, M. M. Maipauw, and R. Y. Hetharie, "Efektifitas Penggunaan Google Form untuk Media Evaluasi Penilaian Tes Tengah Semester," *Edukatif J. Ilmu Pendidik.*, vol. 6, no. 1, pp. 324–332, 2024, doi: 10.31004/edukatif.v6i1.5868.
[19] E. A. Fox *et al.*, "Uji Korelasi Metode Penelitian Pada kualitas Pelayanan Kesehatan yang Berhubungan dengan Kepuasan Pasien," *Comput. Handb. Two-Volume Set*, pp. 1–23, 2022.
[20] U. Yulia, "Uji Validitas dan Uji Reliabilitas Instrument Penilaian Kinerja Dosen," *J. Sains dan Teknol.*, vol. 4, no. 2, pp. 21–24, 2023.
[21] A. S. Rahmawati and R. Erina, "Rancangan Acak Lengkap (Ral) Dengan Uji Anova Dua Jalur," *Opt. J. Pendidik. Fis.*, vol. 4, no. 1, pp. 54–62, 2020, doi: 10.37478/optika.v4i1.333.

DOI: https://doi.org/10.31004/riggs.v5i2.12218