

Pengukuran Kesadaran Keamanan Informasi Calon Tenaga Kerja Industri TPT Menggunakan HAIS-Q

Usaid Syawahidul Chaq^{1*)}, Nungky Amalia Imran²⁾

Teknik Pembuatan Kain Tenun, Akademi Komunitas Industri Tekstil dan Produk Tekstil Surakarta

¹⁾us@ak-tekstilsolo.ac.id, ²⁾nungky@ak-tekstilsolo.ac.id

Riwayat Artikel	Abstrak
Dikirim 26 Mei 2025 Diterima 29 Juli 2025 Diterbitkan 31 Agu 2025	Transformasi digital di industri Tekstil dan Produk Tekstil (TPT) memberikan dampak positif namun memberikan tantangan dan ancaman baru pada keamanan informasi. Penelitian ini bertujuan untuk mengukur tingkat kesadaran keamanan informasi calon tenaga kerja industri TPT menggunakan instrumen HAIS-Q (<i>Human Aspects of Information Security Questionnaire</i>) yang terdiri dari tiga dimensi: pengetahuan (<i>knowledge</i>), sikap (<i>attitude</i>), dan perilaku (<i>behavior</i>). Fokus penelitian pada sektor TPT dilakukan karena minimnya studi yang secara khusus membahas keamanan informasi pada bidang ini. Pengumpulan data dilakukan melalui penyebaran kuesioner yang diberikan kepada 112 responden di Kampus AKTEX. Analisis data menggunakan bobot dimensi berdasarkan model HAIS-Q serta metode <i>Analytical Hierarchy Process</i> (AHP) untuk menentukan prioritas fokus area. Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan informasi berada pada kategori sedang (<i>average</i>) dengan nilai 79,56%. Empat dari tujuh fokus area teridentifikasi sebagai prioritas peningkatan, yaitu manajemen kata sandi, penggunaan <i>email</i> , media sosial, dan penanganan informasi. Hasil temuan menunjukkan pentingnya integrasi edukasi keamanan informasi dalam kurikulum vokasi serta kolaborasi antara institusi pendidikan dan industri untuk membentuk SDM yang lebih siap menghadapi ancaman keamanan siber.
Kata kunci: Kesadaran Keamanan Informasi, HAIS-Q, Industri TPT, Keamanan Informasi, AHP, Pendidikan Vokasi	Abstract <i>Digital transformation in the Textile and Textile Products (TPT) industry has a positive impact but poses new challenges and threats to information security. This study aims to measure the level of information security awareness of prospective TPT industry workers using the HAIS-Q (Human Aspects of Information Security Questionnaire) instrument consisting of three dimensions: knowledge, attitude, and behavior. The research focus on the TPT sector was carried out due to the lack of studies that specifically discuss information security in this field. Data collection was carried out by distributing questionnaires given to 112 respondents at the AKTEX Campus. Data analysis used dimension weights based on the HAIS-Q model and the Analytical Hierarchy Process (AHP) method to determine priority focus areas. The results showed that the level of information security awareness was in the average category with a value of 79.56%. Four of the seven focus areas were identified as priorities for improvement, namely password management, email use, social media, and information handling. The findings show the importance of integrating information security education into the vocational curriculum and collaboration between educational institutions and industry to form human resources who are better prepared to face cybersecurity threats.</i>
Keywords: Information Security Awareness, HAIS-Q, TPT Industry, Information Security, AHP, Vocational Education	

1. PENDAHULUAN

Industri Tekstil dan Produk Tekstil (TPT) merupakan salah satu sektor strategis yang berperan penting dalam pertumbuhan ekonomi nasional. Industri TPT ini berkontribusi besar dalam meningkatkan ekspor nonmigas, meningkatkan devisa negara, dan penyerapan tenaga kerja [1,2]. Nilai PDB yang dihasilkan dari industri TPT mencapai Rp 218,2 Triliun pada kuartal ketiga tahun 2024 [3,4]. Seiring dengan perkembangan teknologi dan digitalisasi proses produksi maupun administrasi, industri TPT semakin bergantung pada sistem informasi dan data digital. Penggunaan teknologi IoT, sistem otomasi dan sistem ERP mendorong industri TPT untuk melakukan transformasi digital. Transformasi digital pada proses produksi di industri TPT memberikan manfaat dalam meningkatkan efisiensi operasional dan produktivitas perusahaan [5-7]. Dilain hal, ketergantungan ini membawa tantangan baru berupa perubahan budaya kerja, risiko keamanan data dan privasi [7]. Ketergantungan terhadap teknologi informasi dan data digital menuntut kesiapan sumber daya manusia dalam menjaga keamanan data perusahaan. Kelalaian dan kurangnya pengetahuan tentang keamanan dapat membuka celah bagi serangan siber, pencurian data, dan serangan *malware* berdampak pada gangguan operasional perusahaan [8-10].

Hasil studi menunjukkan faktor manusia menjadi penyebab utama kebocoran data dan insiden keamanan siber dibandingkan dengan faktor lainnya [9-11]. Menurut [terranovasecurity.com](https://www.terranovasecurity.com) pada tahun 2024, sekitar 95% insiden kebocoran data disebabkan oleh kesalahan manusia, yang mencakup kelalaian, kesalahan konfigurasi, dan kurangnya pelatihan keamanan siber. Hal ini menunjukkan bahwa faktor manusia merupakan titik rentan utama dalam keamanan informasi yang perlu mendapatkan perhatian serius dalam pengembangan kebijakan dan pelatihan keamanan [12]. Di Indonesia sendiri, pada tahun 2022 terjadi 290 juta kasus serangan siber yang berdampak pada kerugian sebesar US\$ 34,2 miliar [13].

Di perusahaan industri TPT, kepedulian keamanan data dan informasi menjadi tanggung jawab bersama bagi pihak manajemen dan tenaga kerjanya untuk keberlanjutan organisasi. Edukasi dan pembentukan perilaku tentang kesadaran keamanan informasi perlu dilakukan sejak perekrutan tenaga kerja. Pada tingkat individu, kesadaran keamanan informasi merupakan faktor penting yang mempengaruhi perlindungan aset informasi pada organisasi [14]. Kesadaran keamanan yang kurang seperti pengelolaan *password* yang buruk dan pengabaian kebijakan keamanan dapat berdampak kepada penurunan finansial perusahaan. Hal tersebut juga menimbulkan kehilangan klien, gangguan operasional, hingga ancaman keberlangsungan usaha [9,15].

Mahasiswa vokasi kampus AKTEX merupakan calon tenaga kerja yang dipersiapkan secara khusus untuk memenuhi kebutuhan industri TPT. Kampus AKTEX merupakan perguruan tinggi vokasi jenjang diploma dua, yang bekerja sama dengan berbagai perusahaan di sektor TPT dalam pengembangan kurikulum, pelatihan kerja praktik, hingga penyaluran lulusan ke dunia industri. Oleh karena itu, mahasiswa vokasi perlu dibekali pemahaman dan perilaku yang aman dalam penggunaan sistem informasi. Pengukuran tingkat kesadaran keamanan informasi sejak masa pendidikan vokasi menjadi langkah penting untuk memetakan kesiapan calon tenaga kerja ketika memasuki industri TPT. Apabila perusahaan dan perguruan tinggi dapat lebih cepat menyiapkan dan meningkatkan kompetensi SDM industri, maka dapat menciptakan keamanan yang kokoh dalam menghadapi bahaya serangan siber [16]. Penyiapan calon tenaga kerja dapat dilakukan dengan pelatihan maupun edukasi lainnya yang dirancang berdasarkan hasil pengukuran tersebut.

Beberapa penelitian terkait pengukuran kesadaran keamanan informasi yang pernah dilakukan menggunakan HAIS-Q (*Human Aspects of Information Security Questionnaire*) sebagai instrumen terstandar. Penelitian oleh Gofur, Fathoni Aji, dan Kurniawan (2024) melakukan pengukuran kesadaran keamanan pada pegawai PT Meshindo Jayatama. Perusahaan tersebut merupakan perusahaan penyedia komponen elektronik. Pada penelitian tersebut menggunakan instrumen HAIS-Q dengan kerangka *Knowledge, Attitude, Behavior* (KAB) untuk memberikan rekomendasi berdasarkan level kesadaran keamanan informasi. Penelitian tersebut juga menggunakan penskalaan prioritas fokus area untuk perbaikan menggunakan metode AHP [17]. Metode yang serupa juga dilakukan oleh Setiawan dan Rizal (2024) pada mahasiswa setelah periode pandemi Covid-19. Dalam penelitiannya juga menggunakan metode *Multi-Criteria Decision Analysis*

(MCDA) untuk menentukan bobot tiga dimensi dan tujuh area fokus yang telah ditentukan. Hasil penelitiannya dapat memberikan masukan berharga bagi institusi dalam meningkatkan kesadaran keamanan informasi mahasiswanya [18]. Styoutomo dan Ruldeviyani (2023) melakukan penelitian tentang strategi meningkatkan kesadaran keamanan informasi menggunakan HAIS-Q dengan ISO/IEC 27001:2013 untuk melakukan pengukuran kesadaran keamanan informasi. Penelitian tersebut mendapatkan lemahnya manajemen *password*, kebiasaan penggunaan *email* dan internet pada pegawai di lembaga finansial [16]. Penelitian lainnya oleh Alvito (2024) dengan menggunakan kerangka KAB menemukan rendahnya kesadaran keamanan informasi mahasiswa Fakultas Informatika Universitas Telkom, khususnya dalam penggunaan internet dan pelaporan insiden, yang dipengaruhi kekhawatiran merusak hubungan sosial di kampus [19].

Meskipun telah dilakukan berbagai penelitian terkait keamanan informasi dengan HAIS-Q pada sektor pendidikan, lembaga keuangan, maupun manufaktur [8,15–17], namun belum banyak penelitian yang secara khusus mengkaji calon tenaga kerja pada sektor industri strategis seperti TPT. Oleh karena itu, penelitian ini menggunakan instrumen HAIS-Q dengan tujuh fokus area pada dimensi KAB yang dikembangkan oleh Kruger dan Kearney (2006) untuk melakukan pengukuran tingkat kesadaran keamanan informasi pada calon tenaga kerja industri TPT [20]. Metode AHP juga digunakan untuk memeringkat fokus area yang akan dilakukan peningkatan terlebih dahulu. Metode AHP memiliki kelebihan dalam pemberian keputusan dan akomodasi terhadap atribut kualitatif maupun kuantitatif [21]. AHP dapat lebih sistematis dan objektif dalam mengevaluasi beberapa fokus area [22]. Penelitian ini memberikan kontribusi orisinal dengan menghadirkan perspektif baru terhadap kesiapan keamanan informasi pada calon tenaga kerja industri TPT, yang selama ini belum banyak dibahas. Hasil pengukuran tersebut diharapkan dapat memberikan rekomendasi kepada pihak kampus AKTEX dan industri TPT yang bekerja sama dalam merumuskan kurikulum dan metode dalam meningkatkan kesadaran keamanan informasi calon tenaga kerja industri TPT.

2. LANDASAN TEORI

2.1. Kesadaran Keamanan Informasi

Kesadaran keamanan informasi atau dikenal dengan istilah *Information Security Awareness* (ISA) berfungsi untuk melindungi organisasi dari ancaman siber. ISA cenderung berfokus pada dua aspek. Aspek pertama adalah sejauh mana karyawan memahami perilaku keamanan informasi yang aman, yang sering kali diuraikan dalam kebijakan, peraturan, dan panduan keamanan informasi organisasi. Kedua, adalah sejauh mana karyawan berkomitmen dan berperilaku sesuai dengan praktik terbaik yang sering diuraikan dalam kebijakan keamanan informasi, peraturan dan pedoman [17,23].

Pengertian lain tentang ISA adalah kewaspadaan dalam memahami berbagai ancaman keamanan informasi dan persepsi seseorang terkait dengan ancaman-ancaman keamanan informasi [14]. Dalam perspektif kondisi kognitif seseorang, ISA adalah proses peningkatan kesadaran dan reaksi perilaku terhadap ancaman keamanan informasi [14]. Secara khusus, ISA dikonseptualisasikan sebagai kesadaran individu tentang peran dan tanggung jawab mengenai keamanan informasi. ISA bertujuan untuk mengubah nilai, norma, persepsi, perilaku, sikap, kebiasaan, dan budaya organisasi seseorang terkait dengan praktik keamanan informasi [18].

2.2. *Human Aspects of the Information Security Questionnaire* (HAIS-Q)

HAIS-Q merupakan instrumen untuk mengukur ISA yang dikembangkan oleh Parsons. HAIS-Q memiliki tiga dimensi yaitu *Knowledge, Attitude, Behavior* (KAB) dengan setiap dimensi memiliki tujuh fokus area. Tujuh fokus area tersebut yaitu *password management* (PM), *email use* (EU), *internet use* (IU), *social media use* (SM), *mobile device* (MD), *information handling* (IH), dan *incident reporting* (IR). Masing-masing fokus area memiliki tiga sub-area [17,19,23]. Dengan adanya fokus area memungkinkan untuk mengidentifikasi kekuatan dan kekurangan ISA pada setiap individu [16].

2.3. *Awareness Training*

Integrasi antara institusi pendidikan vokasi dan dunia industri bukan hanya sebuah kolaborasi, melainkan pendekatan strategis untuk menyelaraskan kurikulum dengan kebutuhan dan tantangan

nyata di lapangan [24]. Salah satu aspek krusial yang perlu dimasukkan dalam penyelarasan tersebut adalah pelatihan kepedulian keamanan informasi melalui program *Security Education, Training, and Awareness* (SETA). SETA merupakan strategi yang banyak diterapkan dalam tata kelola keamanan organisasi dan bertujuan untuk mengurangi pelanggaran keamanan yang bersumber dari rendahnya kesadaran individu terhadap isu keamanan siber [25,26]. Program ini dirancang untuk mendidik karyawan agar mampu melindungi diri mereka sendiri, data, serta jaringan organisasi dari berbagai ancaman siber [26]. Namun, efektifitas SETA sangat bergantung pada kemampuannya dalam mengubah sikap dan perilaku individu terhadap insiden siber. Jika hanya berfokus pada transfer pengetahuan tanpa menyentuh aspek sikap, maka program ini berisiko gagal mencapai dampak positif bagi organisasi.

Oleh karena itu, program *awareness training* keamanan informasi harus dipandang sebagai investasi jangka panjang yang perlu dilakukan secara berkelanjutan [27]. Dengan pelatihan yang diberikan secara konsisten dan kontekstual, program ini tidak hanya meningkatkan kesadaran teknis, tetapi juga membantu membentuk budaya keamanan siber di lingkungan organisasi. Penggunaan teknologi memiliki peran dalam meningkatkan efektivitas *awareness training*. Teknologi terkini seperti *virtual reality* dan *augmented reality* telah terbukti meningkatkan efektivitas pemahaman teoritis dan keterampilan praktis peserta pelatihan [28,29]. Teknologi terkini lainnya adalah kecerdasan buatan atau *artificial intelligence* yang memiliki potensi besar menciptakan pembelajaran yang dipersonalisasi dan mengatasi kesenjangan antar disiplin ilmu [30], dalam hal ini adalah kesadaran keamanan informasi dan pendidikan vokasi. Dalam konteks pendidikan vokasi, *awareness training* ini juga akan sangat relevan untuk mempersiapkan lulusan yang tidak hanya kompeten secara teknis, tetapi juga memiliki kepekaan dan tanggung jawab terhadap keamanan informasi di tempat kerja [24].

3. METODE PENELITIAN

3.1. Instrumen Penelitian

Penelitian ini menggunakan merupakan penelitian kuantitatif dengan metode angket (kuesioner) berdasarkan HAIS-Q. Kuesioner digunakan untuk mendapatkan nilai tingkat kesadaran keamanan informasi pada calon tenaga kerja industri TPT. Kuesioner merupakan metode pengumpulan data yang dilakukan dengan memberikan sejumlah pertanyaan tertulis kepada responden untuk dijawab secara mandiri [31]. Pertanyaan pada kuesioner mencakup tujuh fokus area dan tiga sub-area. Tujuh fokus area dan tiga sub-area HAIS-Q pada masing-masing dimensi KAB disajikan pada Tabel 1.

Tabel 1. Fokus Area dan Sub-area HAIS-Q

Fokus Area (kode)	Sub-area (kode)
Password management (PM)	Using the same password (PM1)
	Sharing passwords (PM2)
	Using a strong password (PM3)
Email use (EU)	Clicking on links in emails from known senders (EU1)
	Clicking on links in emails from unknown senders (EU2)
	Opening attachments emails from unknown senders (EU3)
Internet use (IU)	Downloading files (IU1)
	Accessing dubious websites (IU2)
	Entering information online (IU3)
Social media use (SM)	Social media privacy settings (SM1)
	Considering the consequences (SM2)
	Posting about work (SM3)
Mobile device (MD)	Physically securing mobile devices (MD1)
	Sending sensitive information via Wi-Fi (MD2)
	Shoulder surfing (MD3)
Information handling (IH)	Disposing of sensitive printouts (IH1)
	Inserting removable media (IH2)
	Leaving sensitive material (IH3)
Incident reporting (IR)	Reporting suspicious behavior (IR1)
	Ignoring poor security behavior by colleagues (IR2)
	Reporting all incidents (IR3)

Terdapat satu pertanyaan pada setiap sub-area sehingga total pertanyaan yang dijawab responden adalah 63 pertanyaan. Sebagai contoh untuk sub-area SM3 (*Posting* tentang pekerjaan) pada fokus area penggunaan media sosial mempunyai tiga pertanyaan yang mencakup dimensi pengetahuan (*knowledge*), sikap (*attitude*), dan tindakan (*behavior*). Pertanyaan tersebut dapat dilihat pada Tabel 2. Pilihan jawaban menggunakan skala likert dengan nilai 1 apabila sangat tidak setuju dan nilai 5 untuk jawaban sangat setuju.

Tabel 2. Contoh pertanyaan di kuesioner

Dimensi	Pertanyaan
<i>Knowledge</i>	Saya tahu, berbahaya jika bercerita tentang pekerjaan di medsos
<i>Attitude</i>	Saya merasa tidak aman jika posting pekerjaan di medsos
<i>Behavior</i>	Saya tidak pernah upload foto dan bercerita tentang pekerjaan

Kuesioner yang disebarakan sebelumnya telah dilakukan uji validitas dan uji reliabilitas. Kuesioner dinyatakan valid jika *r*-hitung lebih besar dari *r*-tabel [16,19]. Sedangkan reliabilitas kuesioner dapat dikategorikan berdasarkan nilai cronbach alpha. Kategori tersebut *excellent* (>0.9), *good* (0.75-0.9), *moderate* (0.5-0.75), dan *poor* (<0.5) [16,32]. Pengujian tersebut bertujuan untuk memastikan instrumen penelitian benar pengukurannya sesuai fungsinya dan instrumen penelitian dapat dipercaya untuk pengumpulan data [33]. Tiga puluh (30) responden diambil untuk uji validitas dan uji reliabilitas sebelum kuesioner digunakan. Hasil pengambilan data dilakukan uji kembali untuk memastikan validitasnya dan reliabilitasnya.

Instrumen penelitian lainnya adalah matriks perbandingan berpasangan (*pairwise comparison matrix*) yang didapatkan dengan melakukan wawancara kepada pakar sebagaimana contoh pada Tabel 3. Terdapat dua pakar yang dihimpun pendapatnya, pakar yang pertama tergabung dalam tim IT di kampus AKTEX dengan pertimbangan pengetahuan dan pengalamannya dibidang IT dan keamanan informasi. Pakar yang kedua adalah ahli dibidang pertekstilan dengan pengalaman bekerja di industri TPT. Matriks tersebut digunakan untuk memberikan bobot prioritas pada masing-masing fokus area pada HAIS-Q dengan metode AHP. Skala perbandingan yang digunakan adalah 1-9. Skala 1 adalah *equal importance*, dimana kedua fokus area memiliki tingkat kepentingan yang sama. Skala 9 adalah *extreme importance*, dimana salah satu fokus area tingkat kepentinganya ekstrim sangat penting dibandingkan fokus area lainnya [34]. Hasil pembobotan selanjutnya dihitung rata-rata dari kedua pakar untuk digunakan dalam perhitungan menentukan tingkat ISA.

Tabel 3. Contoh *pairwise comparison* fokus area HAIS-Q

	9	8	7	6	5	4	3	2	1	2	3	4	5	6	7	8	9	
<i>Mobile device</i>												X						<i>Information Handling</i>
<i>Mobile device</i>								X										<i>Media social</i>

3.2. Pengambilan Data

Pengambilan data dilakukan dengan menyajikan kuesioner pada *Google Form* untuk memudahkan responden menjawab pertanyaan. Periode pengambilan data dilaksanakan pada 7 – 27 April 2025. Subjek penelitian ini adalah calon tenaga kerja industri TPT yang masih menempuh pendidikan di kampus AKTEX. Terdapat 112 responden dari 232 calon tenaga kerja industri TPT di kampus AKTEX yang melakukan pengisian kuesioner. Berdasarkan rumus Slovin seperti pada persamaan (1), diketahui tingkat eror penelitian di bawah 7%.

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

(1)

Pada persamaan (1) n adalah sampel atau responden yang mengisi, N adalah total populasi, e adalah tingkat eror (*error level*). Tingkat eror ditentukan oleh peneliti, biasanya 1%, 5%, 10%, dan lainnya [17].

3.3. Analisis Data

Analisis data dilakukan untuk mengetahui tingkat ISA pada calon tenaga kerja industri TPT. Untuk mengetahui nilai ISA, langkah pertama adalah menghitung nilai setiap fokus area. Nilai fokus area dapat diketahui dengan mengalikan nilai dimensi pada fokus area dengan bobot dimensi. Pada penelitian ini bobot dimensi menggunakan panduan yang telah ditetapkan oleh Kruger dan Kenney (2006) yang disajikan dalam Tabel 4 [17,20,21].

Tabel 4. Bobot dimensi KAB

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

Setelah didapatkan nilai setiap fokus area, langkah kedua adalah menghitung nilai ISA. Nilai ISA didapatkan dengan menjumlahkan perkalian setiap nilai fokus area dengan bobot fokus area. Bobot fokus area didapatkan dari penilaian pakar yang telah dilakukan sebelumnya. Nilai ISA dikategorikan menjadi tiga tingkatan, yaitu buruk (*poor*), menengah (*average*), dan baik (*good*) [20] seperti pada Gambar 1.



Gambar 1. Kategori *Information Security Awareness*

4. HASIL DAN PEMBAHASAN

Hasil pengambilan data didapatkan responden sejumlah 112 orang. Responden merupakan calon tenaga kerja industri TPT yang tersebar pada 27 perusahaan, dengan menempati di dua unit produksi utama yaitu tekstil (proses pemintalan benang hingga pertenenan menjadi kain) dan produk tekstil (bahan jadi seperti kemeja, celana, dsb) serta rentang usia dari 16 sampai 40 tahun. Responden didominasi oleh calon tenaga kerja industri perempuan, rentang usia terbanyak adalah 16 – 20 tahun diikuti rentang 21 – 25 tahun yang merupakan rentang usia produktif. Unit produksi terbanyak pada unit produksi produk tekstil. Detail demografi responden dan detail sebaran penempatan kerja responden disajikan pada Tabel 5 dan Tabel 6.

Tabel 5. Demografi responden

Kriteria	Variabel	Jumlah	%
Jenis Kelamin	Laki - laki	41	36,61%
	Perempuan	71	63,39%
Unit Produksi	Tekstil	48	42,86%
	Produk Tekstil	64	57,14%
Usia	16 - 20	70	62,50%
	21 - 25	33	29,46%
	26 - 30	4	3,57%
	31 - 35	4	3,57%
	36 - 40	1	0,89%

Tabel 6. Sebaran penempatan kerja responden

Kode PT	Unit Produksi	Jumlah
PC GMY	Tekstil	3
PT AMT	Tekstil	2
PT DNL	Tekstil	4
PT DNT	Tekstil	9
PT DSR	Tekstil	3
PT SLP	Tekstil	1
PT SWA	Tekstil	3
PT UMJ	Tekstil	1
PT EQY	Tekstil	2
PT HNL	Tekstil	4
PT IDS	Tekstil	4
PT KMS	Tekstil	1
PT KSM	Tekstil	2
PT LTS	Tekstil	2
PT PRM	Tekstil	1
PT SRI	Tekstil	3
PT TTI	Tekstil	3
INBIS	Produk Tekstil	3
PT AKG	Produk Tekstil	3
PT ALI	Produk Tekstil	3
PT AMT	Produk Tekstil	1
PT DNL	Produk Tekstil	16
PT EGU	Produk Tekstil	5
PT GBI	Produk Tekstil	3
PT HPL	Produk Tekstil	1
PT JAG	Produk Tekstil	5
PT LPW	Produk Tekstil	4
PT MAS	Produk Tekstil	4
PT PBT	Produk Tekstil	12
PT SWA	Produk Tekstil	4

4.1. Pembobotan Fokus Area

Pembobotan fokus area dihitung berdasarkan *pairwise comparison matrix* yang dilakukan oleh kedua pakar dengan metode AHP. Untuk mempermudah perhitungan, penulis menggunakan alat bantu AHP Priority Calculator yang dapat diakses secara daring [35]. Kedua pakar sependapat menetapkan fokus area penanganan informasi (IH) pada peringkat pertama. Untuk menghitung tingkat kesadaran keamanan informasi (ISA) maka diambil bobot rata-rata dari kedua pakar. Hasil pembobotan dan rata-rata pembobotan kedua pakar disajikan pada Tabel 7.

Tabel 7. Bobot Fokus Area

Fokus Area	Bobot P1	Bobot P2	Bobot Avg
PM	11,80%	9,60%	10,70%
EU	6,90%	5,70%	6,30%
IU	6,90%	17,80%	12,35%
SM	11,80%	17,80%	14,80%
MD	4,40%	9,60%	7,00%
IH	29,10%	29,90%	29,50%
IR	29,10%	9,60%	19,35%

4.2. Pemetaan Pengukuran ISA

Hasil kuesioner dari 112 responden dilakukan uji validitas dan reliabilitas untuk memastikan kuesioner valid dan dapat diandalkan. Nilai *r*-tabel adalah 0,1857 untuk derajat kebebasan (*degree of freedom*) 110. Nilai *r*-hitung dari setiap dimensi disajikan pada Tabel 8. Hasil perbandingan *r*-hitung dan *r*-tabel menunjukkan bahwa seluruh pertanyaan pada kuesioner sudah valid dikarenakan nilai *r*-hitung lebih besar daripada *r*-tabel. Nilai Cronbach Alpha kuesioner disajikan pada Tabel 9. Berdasarkan Tabel 9 maka dapat dipastikan kuesioner reliabel dengan kategori *excellent*.

Tabel 8. Nilai r-hitung kuesioner untuk uji validitas

Fokus Area	Sub-area	Knowledge	Attitude	Behavior
PM	PM1	0.673790	0.654779	0.461156
	PM2	0.702684	0.692543	0.376311
	PM3	0.524540	0.639235	0.662874
EU	EU1	0.660630	0.554022	0.422294
	EU2	0.669040	0.772968	0.649271
	EU3	0.760412	0.722987	0.670318
IU	IU1	0.733493	0.706307	0.818523
	IU2	0.689692	0.784353	0.790851
	IU3	0.770353	0.700832	0.787347
SM	SM1	0.718164	0.679757	0.705352
	SM2	0.573430	0.761826	0.444117
	SM3	0.672794	0.699002	0.502711
MD	MD1	0.745903	0.788876	0.716997
	MD2	0.523360	0.459284	0.708774
	MD3	0.597594	0.763271	0.735510
IH	IH1	0.476637	0.760440	0.656484
	IH2	0.629115	0.500111	0.686273
	IH3	0.654069	0.695403	0.593475
IR	IR1	0.545304	0.521098	0.763816
	IR2	0.694846	0.750160	0.782759
	IR3	0.626465	0.776361	0.800595

Tabel 9. Nilai cronbach untuk uji reliabilitas

Dimensi	Cronbach Alpha
<i>Knowledge</i>	0,9427
<i>Attitude</i>	0,9493
<i>Behavior</i>	0,9398

Hasil pengukuran ISA pada calon tenaga kerja industri TPT menunjukkan nilai 79,56%. Nilai tersebut menunjukkan berada pada kategori *average*. Kategori tingkat kesadaran keamanan informasi pada calon tenaga kerja industri TPT mengindikasikan bahwa perlu dilakukan pemantauan dan bila perlu dilakukan tindakan untuk meningkatkan kesadaran keamanan informasi. Hasil pengukuran ISA dan nilai setiap dimensi maupun fokus area disajikan pada Tabel 10.

Tabel 10. Hasil tingkat kesadaran keamanan informasi

Fokus Area	Knowledge	Attitude	Behavior	Total
PM	84,88%	78,69%	77,02%	79,71%
EU	83,04%	83,10%	74,94%	79,00%
IU	83,45%	83,63%	80,54%	82,03%
SM	79,64%	83,63%	75,65%	78,44%
MD	79,05%	78,04%	82,86%	80,75%
IH	74,05%	77,68%	80,36%	77,93%
IR	80,83%	82,32%	80,54%	80,98%
Total	79%	81%	79%	79,56%

Pada Tabel 10 diketahui tiga fokus area termasuk dalam kategori *Good*. Ketiga fokus area tersebut yaitu penggunaan internet (IU), penggunaan perangkat *mobile* (MD), dan pelaporan insiden (IR). Namun pada fokus area MD, dimensi *knowledge* dan *attitude* masih dalam kategori *average*. Hal tersebut dikarenakan responden belum mengetahui sepenuhnya tentang bahaya mengakses *wifi* publik dengan perangkat *mobile*, seperti berbagi file atau data menggunakan *wifi* gratis. Hal lainnya adalah kurangnya kewaspadaan dalam menjaga layar HP saat digunakan, utamanya saat menginput kata sandi.

Fokus area sisanya, yaitu manajemen *password* (PM), penggunaan *email* (EU), penggunaan media sosial (SM), dan penanganan informasi (IH) masuk dalam kategori *Average*. Fokus area IH menjadi fokus area dengan tingkat ISA terendah, yaitu 77,93%. Hal tersebut berkebalikan dengan peringkat fokus area yang ditentukan oleh pakar. Rendahnya nilai pada IH dikarenakan pada dimensi *knowledge*, responden memiliki pengetahuan yang cukup mengenai penanganan informasi, seperti cara memusnahkan data yang benar. Baik data pada dokumen fisik maupun data digital. Pada dimensi *attitude*, responden juga masih abai karena merasa aman ketika bertukar data informasi dengan *flashdisk*. Fokus area berikutnya SM dengan nilai 78,44%. Dimensi *knowledge* pada fokus area SM menunjukkan kurang pahamiannya responden terhadap konsekuensi saat *posting* di media sosial, termasuk *posting-an* tentang pekerjaan maupun kehidupan pribadi. Pada tindakan atau dimensi *behavior*, penyebab nilai kurang adalah responden merasa menyesal dengan apa yang pernah mereka *post*. Hal tersebut menunjukkan tindakan responden yang tidak memikirkan dulu dampak sebelum berbagi atau *posting* di media sosial. Pada fokus area EU, dimensi *knowledge* dan *attitude* sudah dalam kategori *Good*. Hanya dimensi *behavior* yang perlu dilakukan tindakan. Meskipun sudah ada pengetahuan tentang bahaya sembarangan klik *link* di *inbox email*, responden masih suka klik *link* tersebut karena rasa penasaran. Pada fokus area PM, nilai rendah yang didapatkan dikarenakan sikap dan tindakan responden yang masih menggunakan satu kata sandi untuk beberapa akun dan adanya tindakan berbagi kata sandi dengan orang lain.

Secara umum, kampus AKTEX dapat mengintegrasikan materi keamanan informasi dalam kurikulum dan praktik kerja industri. Sebagai contoh dalam mata kuliah, mahasiswa diberi studi kasus tentang kebocoran data produksi kain akibat mengirim file di jaringan publik serta dalam laporan praktik industri, mahasiswa diwajibkan memuat audit sederhana tentang keamanan informasi di tempat kerja. Di sisi lain, industri TPT dapat merancang pelatihan *onboarding* dan *security awareness training* yang mencakup simulasi ancaman siber seperti *phishing* dan praktik keamanan sehari-hari yang sesuai konteks operasional. Selain itu, penyusunan kebijakan keamanan informasi yang sederhana dan kontekstual seperti SOP penyimpanan, pertukaran dan pemusnahan dokumen di tempat kerja. Langkah-langkah ini diharapkan dapat menutup celah pada fokus area dengan skor rendah sehingga membentuk tenaga kerja industri TPT yang tidak hanya kompeten secara teknis, tetapi juga memiliki kesadaran yang kuat terhadap keamanan informasi.

5. KESIMPULAN

Pengukuran tingkat kesadaran keamanan informasi pada calon tenaga kerja industri TPT didapatkan nilai 79,56% dengan kategori *average*. Kategori tersebut mengindikasikan perlunya tindakan untuk meningkatkan tingkat kesadaran keamanan informasi. Secara umum perlu dilakukan sosialisasi secara berkala tentang keamanan informasi baik melalui seminar atau integrasi materi keamanan informasi dalam kurikulum pendidikan calon tenaga kerja industri TPT dan evaluasi berkala tentang tingkat kesadaran keamanan informasi. Pihak industri TPT juga perlu menerapkan kebijakan tentang area publik dan khusus untuk menjaga kebocoran informasi akibat kelalaian dari pegawainya. Selain itu, dari tujuh fokus area diketahui empat fokus area juga dalam kategori *average*. Empat fokus area tersebut yaitu manajemen *password* (PM), penggunaan *email* (EU), penggunaan media sosial (SM), dan penanganan informasi (IH). Beberapa rekomendasi dan saran untuk meningkatkan kesadaran keamanan informasi berdasarkan fokus area yaitu:

- Manajemen *password*: menerapkan ketentuan batas minimal panjang kata sandi, yaitu 8 karakter untuk kata sandi dengan perpaduan angka, huruf, dan simbol khusus. Pembaruan kata sandi setiap satu bulan pada aplikasi yang digunakan di lingkungan kerja, khususnya yang dikembangkan oleh instansi. Pengenalan *tools* manajemen *password* yang dapat membantu menyimpan dan mengelola banyak kata sandi dengan aman.
- Penggunaan *email*: menerapkan *Multi-factor Authentication* (MFA), yaitu mengharuskan pengguna memberikan lebih dari satu faktor otentikasi sebelum mengakses *email*. Melakukan *workshop* simulasi *phishing* untuk membiasakan mengenali *email* mencurigakan.

- Media sosial: melakukan edukasi mengenai privasi digital, termasuk pengaturan keamanan akun dan risiko *oversharing* informasi pribadi di media sosial. Mendorong etika berjejaring dan profesionalisme dalam membangun citra diri di media sosial menjelang masuk dunia kerja
- Penanganan informasi: pemberian edukasi secara langsung berupa *security awareness training* maupun poster tentang klasifikasi data (publik, internal, atau rahasia). Menerapkan prosedur tentang penyimpanan dan pemusnahan data fisik maupun digital.

REFERENSI

- [1] A. Anugrah, H. H. Mohamad, J. Otniel, M. R. Fahrezi, M. Radian, and F. Siswajanthi, "Analisis Industri Tekstil Di Jawa Barat Sebelum Dan Setelah Krisis Ekonomi," *Doktrin*, vol. 2, no. 2, pp. 118–135, Jan. 2024, doi: 10.59581/doktrin.v2i2.2579. Available: <https://ifrelresearch.org/index.php/Doktrin-widyakarya/article/view/2579>
- [2] M. R. Apriliyanto and R. Rusdarti, "Analisis Penyerapan Tenaga Kerja Industri Tekstil dan Produk Tekstil di Provinsi Jawa Tengah," *EDAJ*, vol. 7, no. 4, pp. 374–383, Dec. 2018, doi: 10.15294/edaj.v7i4.27718. Available: <https://journal.unnes.ac.id/sju/index.php/edaj/article/view/27718>
- [3] V. B. Kusnandar, "Kontribusi Industri Tekstil dan Pakaian terhadap PDB Menurun 2010-2024," *Databoks*, Mar. 03, 2025. Available: <https://databoks.katadata.co.id/ekonomi-makro/statistik/67c5476c13c85/kontribusi-industri-tekstil-dan-pakaian-terhadap-pdb-menurun-2010-2024> (accessed May 6, 2025)
- [4] A. R. Nurdifa, "Industri Tekstil Ditarget Jadi Mesin Pengerek Ekonomi, Bagaimana Prospek 2025?," *Bisnis.com*, Dec. 18, 2024. Available: <https://ekonomi.bisnis.com/read/20241218/257/1825180/industri-tekstil-ditarget-jadi-mesin-pengerek-ekonomi-bagaimana-prospek-2025> (accessed May 6, 2025)
- [5] T. L. Ahmad, I. P. Murni, and A. T. N. Adibah, "Pengaruh Mesin Cutting Otomatis Berbasis Internet of Thing (IoT) terhadap Efisiensi dan Produktivitas Pekerja Pada Mesin Building Tire di PT. ABC," *Jurnal Instrumentasi dan Teknologi Informasi (JITI)*, vol. 6, no. 1, pp. 121–128, Nov. 2024, Available: <https://jurnal.poltek-gt.ac.id/index.php/jiti/article/view/70>
- [6] S. Risqi, M. Farhan, R. Saputra, D. Defriansyah, and B. Wahyudi, "Kajian Literatur Masa Depan Manajemen Rantai Pasok dalam Perspektif Teknik Industri: Tantangan dan Strategi," *Journal of Industrial Engineering Innovation*, vol. 3, no. 01, pp. 1–10, Apr. 2025, Available: <https://ejournal.insightpublisher.com/index.php/jiei/article/view/196>
- [7] F. Harefa and D. H. Lase, "Pengaruh Teknologi Informasi Terhadap Transformasi Digital dan Inovasi dalam Organisasi," *IDENTIK*, vol. 2, no. 1, pp. 7–12, Jan. 2025, doi: 10.70134/identik.v2i1.156. Available: <https://sihojournal.com/index.php/identik/article/view/156>
- [8] K. Wang, X. Guo, and D. Yang, "Research on the Effectiveness of Cyber Security Awareness in ICS Risk Assessment Frameworks," *Electronics*, vol. 11, no. 10, p. 1659, May 2022, doi: 10.3390/electronics11101659. Available: <https://www.mdpi.com/2079-9292/11/10/1659>
- [9] L.-W. Wong, V.-H. Lee, G. W.-H. Tan, K.-B. Ooi, and A. Sohal, "The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities," *International Journal of Information Management*, vol. 66, p. 102520, Oct. 2022, doi: 10.1016/j.ijinfomgt.2022.102520. Available: <https://linkinghub.elsevier.com/retrieve/pii/S0268401222000548>
- [10] H. Taherdoost, "Towards an Innovative Model for Cybersecurity Awareness Training," *Information*, vol. 15, no. 9, p. 512, Aug. 2024, doi: 10.3390/info15090512. Available: <https://www.mdpi.com/2078-2489/15/9/512>
- [11] A. Astridefi, R. A. G. Gultom, and Y. D. W. Asnar, "Analisis Cyber Awareness terhadap Keamanan Data Pribadi dari Serangan Siber menggunakan Metode AHP," *Journal on Education*, vol. 6, no. 2, pp. 14227–14236, Feb. 2024, doi: 10.31004/joe.v6i2.5277. Available: <https://jonedu.org/index.php/joe/article/view/5277>
- [12] Fortra, "130 Cyber Security Statistics: 2024 Trends and Data," Aug. 12, 2024. Available: <https://www.terranovasecurity.com/blog/cyber-security-statistics> (accessed May 6, 2025)
- [13] A. W. O. K. Putri, A. R. M. Aditya, D. L. Musthofa, and P. Widodo, "Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator)," *GPS Journal*, vol. 6, no. 1, pp. 35–46, Jul. 2022, doi: 10.34010/gpsjournal.v6i1.6698. Available: <https://ojs.unikom.ac.id/index.php/gps/article/view/6698>
- [14] L. Jaeger, "Information Security Awareness: Literature Review and Integrative Framework," 2018. doi: 10.24251/HICSS.2018.593. Available: <http://hdl.handle.net/10125/50482>
- [15] T. Ncubekezit, "Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses," *iccws*, vol. 17, no. 1, pp. 395–403, Mar. 2022, doi: 10.34190/iccws.17.1.51. Available: <https://papers.academic-conferences.org/index.php/iccws/article/view/51>
- [16] Y. A. Styoutomo and 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. 2023, doi: 10.21512/commit.v17i2.8272. Available: <https://journal.binus.ac.id/index.php/commit/article/view/8272>
- [17] A. Gofur, R. Fathoni Aji, and H. Kurniawan, "Pengukuran Kesadaran Keamanan Informasi Pegawai: Studi Kasus PT

- Meshindo Jayatama," *JTIK*, vol. 11, no. 2, pp. 315–320, Apr. 2024, doi: 10.25126/jtiik.20241128106. Available: <http://jtiik.ub.ac.id/index.php/jtiik/article/view/8106>
- [18] B. Setiawan and M. A. Rizal, "Measurement of Information Security and Privacy Awareness in College Students after the Covid-19 Pandemic," *Procedia Computer Science*, vol. 234, pp. 1396–1403, 2024, doi: 10.1016/j.procs.2024.03.138. Available: <https://linkinghub.elsevier.com/retrieve/pii/S1877050924004964>
- [19] 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 - Dalam bentuk buku karya ilmiah," Skripsi, Universitas Telkom, S1 Teknologi Informasi, Bandung, 2024. Available: <https://repositori.telkomuniversity.ac.id/pustaka/217774/pengukuran-tingkat-kesadaran-keamanan-informasi-pada-mahasiswa-fakultas-informatika-menggunakan-human-aspect-of-information-security-questionnaire-hais-q-di-universitas-telkom-bandung-dalam-bentuk-buku-karya-ilmiah.html>
- [20] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Computers & Security*, vol. 25, no. 4, pp. 289–296, Jun. 2006, doi: 10.1016/j.cose.2006.02.008. Available: <https://linkinghub.elsevier.com/retrieve/pii/S0167404806000563>
- [21] M. S. Mahardika, A. N. Hidayanto, P. A. Paramartha, L. D. Ompusunggu, R. Mahdalina, and F. Affan, "Measurement of Employee Awareness Levels for Information Security at the Center of Analysis and Information Services Judicial Commission Republic of Indonesia," *Adv. sci. technol. eng. syst. j.*, vol. 5, no. 3, pp. 501–509, 2020, doi: 10.25046/aj050362. Available: <https://astesj.com/v05/i03/p62/>
- [22] A. Firmansyah, "IMPLEMENTASI METODE ANALYTICAL HIERARCHY PROCESS (AHP) UNTUK PEMILIHAN KOTA PENGHASIL KOPI DI JAWA TIMUR," *JITET*, vol. 12, no. 351, Oct. 2024, doi: 10.23960/jitet.v12i3S1.5066. Available: <https://journal.eng.unila.ac.id/index.php/jitet/article/view/5066>
- [23] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Computers & Security*, vol. 66, pp. 40–51, May 2017, doi: 10.1016/j.cose.2017.01.004. Available: <https://linkinghub.elsevier.com/retrieve/pii/S0167404817300081>
- [24] K. Yu and Hsueh Jen Tsao, "Research on the Challenges and Paths of Industry Education Integration in Vocational Colleges," *IJEH*, vol. 15, no. 3, pp. 303–307, Aug. 2024, doi: 10.54097/vs313783. Available: <https://drpress.org/ojs/index.php/ijeh/article/view/24957>
- [25] S. Hu, C. Hsu, and Z. Zhou, "Security Education, Training, and Awareness Programs: Literature Review," *Journal of Computer Information Systems*, vol. 62, no. 4, pp. 752–764, Jul. 2022, doi: 10.1080/08874417.2021.1913671. Available: <https://www.tandfonline.com/doi/full/10.1080/08874417.2021.1913671>
- [26] M. M. Al-Daeef, N. Basir, and M. M. Saudi, "Security Awareness Training: A Review," in *Proceedings of the World Congress on Engineering 2017*, London: World Congress on Engineering 2017, Jul. 2017, pp. 446–451. Available: https://www.iaeng.org/publication/WCE2017/WCE2017_pp446-451.pdf
- [27] R. Sabillon, "The Cybersecurity Awareness Training Model (CATRAM):," in *Research Anthology on Advancements in Cybersecurity Education*, I. R. Management Association, Ed., IGI Global, 2022, pp. 501–520. doi: 10.4018/978-1-6684-3554-0.ch025. Available: <http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-6684-3554-0.ch025>
- [28] U. S. Chaq and F. Samopa, "Teknologi Realitas Virtual pada Perangkat Bergerak untuk Media Pengenalan Lingkungan Haji," *JTIK*, vol. 11, no. 3, pp. 497–506, Jul. 2024, doi: 10.25126/jtiik.938271. Available: <https://jtiik.ub.ac.id/index.php/jtiik/article/view/8271>
- [29] Y. Long, X. Zhang, and X. Zeng, "Application and effect analysis of virtual reality technology in vocational education practical training," *Educ Inf Technol*, vol. 30, no. 7, pp. 9755–9786, May 2025, doi: 10.1007/s10639-024-13197-7. Available: <https://link.springer.com/10.1007/s10639-024-13197-7>
- [30] H. Zhang and W. Y. Leong, "Industry 5.0 and Education 5.0: Transforming Vocational Education through Intelligent Technology," *Journal of Innovation and Technology*, vol. 2024, Oct. 2024, Available: <https://iuojs.intimal.edu.my/index.php/joit/article/view/540>
- [31] Sugiyono, *Metode Penelitian Pendidikan Pendekatan Kualitatif, Kuantitatif dan R&D*. Bandung: Alfabeta, 2013.
- [32] A. Pack, A. Barrett, and J. Escalante, "Large language models and automated essay scoring of English language learner writing: Insights into validity and reliability," *Computers and Education: Artificial Intelligence*, vol. 6, p. 100234, Jun. 2024, doi: 10.1016/j.caeai.2024.100234. Available: <https://linkinghub.elsevier.com/retrieve/pii/S2666920X24000353>
- [33] L. Amanda, F. Yanuar, and D. Devianto, "Uji Validitas dan Reliabilitas Tingkat Partisipasi Politik Masyarakat Kota Padang," *Jurnal Matematika UNAND*, vol. 8, no. 1, pp. 179–188, Jul. 2019, doi: 10.25077/jmu.8.1.179-188.2019. Available: <https://jmua.fmipa.unand.ac.id/index.php/jmua/article/view/423>
- [34] R. D. F. S. M. Russo and R. Camanho, "Criteria in AHP: A Systematic Review of Literature," *Procedia Computer Science*, vol. 55, pp. 1123–1132, 2015, doi: 10.1016/j.procs.2015.07.081. Available: <https://linkinghub.elsevier.com/retrieve/pii/S1877050915015562>
- [35] Klaus D. Goepel, "AHP Priority Calculator." BPSMSG, Feb. 26, 2022. Available: <https://bpsmsg.com/ahp/ahp-calc.php> (accessed May 19, 2025)