Jurnal Pendidikan dan Teknologi Indonesia (JPTI)
Vol. 5, No. 12, Desember 2025, Hal. 3560-3573
DOI: https://doi.org/10.52436/1.jpti.1228
p-ISSN: 2775-4227
e-ISSN: 2775-4219

Penerapan HAIS-Q dalam Pengukuran Tingkat Kesadaran Keamanan Informasi Pegawai Disdukcapil Kota Malang

Bima Yusuf Dharmahita[*1], Mukhlis Prasetyo Aji[2], Ermadi Satriya Wijaya[3], Agung Purwo Wicaksono[4]

[1,2,3,4]Teknik Informatika, Fakultas Teknik dan Sains, Universitas Muhammadiyah Purwokerto, Indonesia
Email: [1]bimayusufdh@gmail.com, [2]prasetyo-aji@ump.ac.id, [3]ermadi_satriya@ump.ac.id, [4]wicaksono@ump.ac.id

Abstrak

Keamanan informasi merupakan aspek krusial dalam transformasi digital pelayanan publik, terutama bagi instansi pemerintah seperti Dinas Kependudukan dan Pencatatan Sipil (Disdukcapil) Kota Malang yang mengelola data pribadi masyarakat secara masif. Meskipun sistem informasi telah digunakan secara luas, hingga saat ini Disdukcapil belum pernah melakukan pengukuran formal terhadap tingkat kesadaran keamanan informasi pegawainya. Kondisi ini menjadi tantangan dalam merumuskan strategi mitigasi risiko berbasis data **(URGENSI)**. Penelitian ini mengukur tingkat kesadaran keamanan informasi pegawai Disdukcapil pada tiga peran strategis, yaitu Administrator Basis Data, Layanan Pelanggan, dan Operator. Data dikumpulkan melalui metode survei menggunakan instrumen *Human Aspects of Information Security Questionnaire* (HAIS-Q) yang menilai dimensi pengetahuan, sikap, dan perilaku. Hasil penelitian menunjukkan adanya variasi tingkat kesadaran antar peran, dengan aspek manajemen kata sandi, penggunaan surat elektronik, dan perangkat seluler masih berada pada tingkat yang memerlukan peningkatan. Temuan ini dapat menjadi dasar penyusunan program pelatihan yang lebih terarah dan mendukung kebijakan penganggaran guna memperkuat perlindungan data kependudukan di lingkungan Disdukcapil Kota Malang. Penelitian ini juga berkontribusi dalam memperluas pemahaman akademik mengenai pengukuran kesadaran keamanan informasi di sektor layanan publik, yang selama ini masih relatif terbatas dalam literatur **(Dampak penelitian pada ilmu pengetahuan).**

Kata kunci: *HAIS-Q, Keamanan Informasi, Kesadaran Keamanan Informasi, Perilaku Keamanan*

The Implementation of HAIS-Q in Measuring Information Security Awareness Levels Among Employees of the Malang City Department of Population and Civil Registration (Disdukcapil)

Abstract

Information security is a crucial aspect of the digital transformation of public services, especially for government agencies such as the Population and Civil Registration Office (Disdukcapil) of Malang City, which manages massive amounts of personal data. Despite the widespread use of information systems, the Disdukcapil has never formally measured the level of information security awareness of its employees. This poses a challenge in formulating a data-driven risk mitigation strategy. This study measured the level of information security awareness of Disdukcapil employees in three strategic roles, namely Database Administrator, Customer Service, and Operator. Data was collected through a survey method using the Human Aspects of Information Security Questionnaire (HAIS-Q) instrument that assesses knowledge, attitude, and behavior dimensions. The results showed variations in awareness levels between roles, with aspects of password management, electronic mail use, and mobile devices still at a level that requires improvement. These findings can serve as a basis for developing more targeted training programs and supporting budgeting policies to strengthen civil registration data protection within Disdukcapil Malang City. This research also contributes to expanding academic understanding of measuring information security awareness in the public service sector, which has been relatively limited in the literature.

Keywords: *HAIS-Q, Information Security, Information Security Awareness, Security Behavior*

p-ISSN: 2775-4227
e-ISSN: 2775-4219

1. PENDAHULUAN

Di era transformasi digital, instansi pemerintah seperti Dinas Kependudukan dan Pencatatan Sipil (Disdukcapil) dituntut untuk mengelola data kependudukan secara efektif dan aman. Digitalisasi layanan telah membawa peningkatan efisiensi dan aksesibilitas, namun juga memperbesar risiko kebocoran data pribadi yang dapat merusak kepercayaan publik dan menghambat pembangunan nasional [1], [2]. Ancaman keamanan informasi pun berkembang secara dinamis [3], dan dalam banyak kasus, faktor manusia menjadi titik lemah utama [4]-[6] dalam sistem pertahanan informasi. Rendahnya kesadaran pegawai terhadap praktik keamanan informasi membuka celah serangan siber, sehingga peningkatan kesadaran menjadi kebutuhan mendesak [7], termasuk bagi pegawai Disdukcapil Kota Malang.

Kesadaran keamanan informasi merujuk pada tingkat pemahaman dan perhatian individu terhadap potensi risiko serta tindakan yang dapat diambil untuk mencegah pelanggaran keamanan [8], [9]. Kesadaran ini tidak hanya menjadi tanggung jawab bagian teknologi informasi, tetapi harus menjadi bagian integral dari seluruh organisasi, termasuk karyawan operasional, manajerial, dan teknis. Ketika kesadaran ini tertanam kuat, pelaksanaan kebijakan keamanan akan lebih efektif dan tingkat kepatuhan terhadap aturan akan meningkat [10], [11]. Dalam konteks tersebut, penting untuk melakukan pengukuran kesadaran secara sistematis dan terstandar. Namun hingga saat ini, Disdukcapil Kota Malang belum pernah melakukan pengukuran formal terhadap tingkat kesadaran keamanan informasi pegawainya. Oleh karena itu, perlu dilakukan studi terstruktur yang dapat memberikan gambaran aktual kondisi kesadaran keamanan informasi di lingkungan kerja tersebut (**Belum Pernah dilakukan Pengukuran secara formal**).

Salah satu instrumen yang telah banyak digunakan untuk mengukur kesadaran keamanan informasi adalah *Human Aspects of Information Security Questionnaire* (HAIS-Q). Instrumen ini dikembangkan oleh Kathryn Parsons dan timnya yang dijelaskan dalam jurnal "*The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies*", instrumen ini terdiri dari 7 area fokus dan 21 sub-area serta dirancang berdasarkan dimensi KAB yang mencakup tiga aspek utama, yaitu *Knowledge* (pengetahuan), *Attitude* (sikap), dan *Behavior* (perilaku) [12], [13]. Pengetahuan mencakup pemahaman terhadap ancaman, praktik terbaik, dan sikap yang mencerminkan kesadaran serta rasa tanggung jawab terhadap keamanan, serta perilaku menilai tindakan nyata dalam menjaga keamanan informasi sehari-hari [14]. Ketiga komponen ini saling melengkapi dan menjadi fondasi pembentukan kesadaran yang utuh. Selain itu, instrumen HAIS-Q terbukti valid dan reliabel dalam menilai kesadaran keamanan informasi seseorang, serta memiliki korelasi yang kuat dengan perilaku keamanan individu [6].

Berbagai studi telah dilakukan untuk mengukur kesadaran keamanan informasi dalam beragam konteks. Ramadhan dan Purwandari (2023) menggunakan model KAB dan kuesioner HAIS-Q untuk menilai pengguna aplikasi perbankan digital di Indonesia. Hasilnya menunjukkan tingkat kesadaran yang baik secara umum, namun praktik perilaku masih perlu ditingkatkan [15]. Dewi et al. (2024) mengkaji pegawai Balai Wilayah BMKG dengan HAIS-Q yang dipadukan dengan Indeks KAMI, dan mencatat rata-rata kesadaran sebesar 81,67%, namun dengan kelemahan pada area password management, mobile computing, dan incident reporting [11]. Sementara itu, Kusnadi et al. (2024) mengamati mahasiswa dan menemukan bahwa meski pengetahuan dan sikap mereka tergolong baik, perilaku keamanan masih rendah, menekankan pentingnya praktik keamanan yang nyata. Ketiga penelitian ini menegaskan bahwa meskipun kesadaran keamanan informasi bisa tinggi secara teoritis, praktik di lapangan masih memerlukan penguatan[14]. Dengan demikian, studi terhadap pegawai Disdukcapil Kota Malang menggunakan instrumen HAIS-Q menjadi langkah penting untuk memahami dan memperkuat perlindungan data kependudukan yang bersifat sangat sensitif (**Perbandingan penelitian sebelumnya**).

Berbeda dari studi sebelumnya, penelitian ini secara spesifik menargetkan instansi pelayanan publik yang mengelola data sensitif, yakni Disdukcapil Kota Malang. Penelitian ini juga secara eksplisit membandingkan tingkat kesadaran pada tiga posisi strategis di Disdukcapil Kota Malang. Ketiga posisi tersebut terdiri dari *Administrator Database* (Administrator Basis Data), *Customer Service* (Layanan Pelanggan), dan Operator, yang berdasarkan observasi lapangan dan konsultasi internal memiliki tanggung jawab langsung dalam pengelolaan data kependudukan. Selain mengukur kesadaran, penelitian ini juga menyusun rekomendasi pelatihan dan kebijakan berdasarkan analisis hasil, menjadikannya lebih aplikatif dan kontekstual dalam mendukung penguatan sistem keamanan informasi sektor public (**Paragraf khusus kebaruan penelitian**).

Berangkat dari latar belakang tersebut, penelitian ini menggunakan pendekatan kuantitatif deskriptif melalui penyebaran kuesioner HAIS-Q pada responden terpilih. Instrumen HAIS-Q dipilih karena telah terbukti validitasnya pada penelitian sebelumnya yang dilakukan oleh Prenda [16]. Penelitian ini menyajikan hasil penerapan HAIS-Q di Disdukcapil Kota Malang untuk menganalisis tingkat kesadaran keamanan informasi pegawai, mengidentifikasi area kelemahan, dan memberikan rekomendasi pelatihan yang sesuai. Hasil penelitian

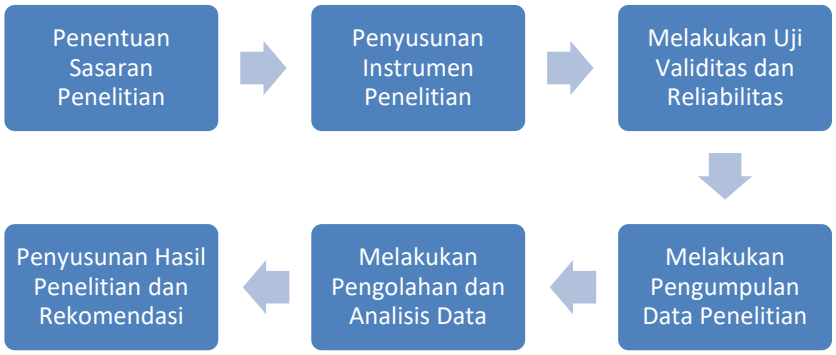
p-ISSN: 2775-4227
e-ISSN: 2775-4219

diharapkan dapat membantu memperkuat pertahanan keamanan informasi melalui peningkatan kualitas sumber daya manusia.

Tujuan dari penelitian ini adalah untuk mengukur dan menganalisis tingkat kesadaran keamanan informasi pegawai Disdukcapil Kota Malang berdasarkan dimensi pengetahuan, sikap, dan perilaku, serta untuk mengidentifikasi area kelemahan spesifik yang dapat dijadikan dasar dalam penyusunan strategi pelatihan dan penguatan kebijakan keamanan informasi (**Tujuan Penelitian**).

2. METODE PENELITIAN

Penelitian ini dilakukan melalui enam tahapan seperti pada Gambar 1. Alur Tahapan Penelitian , dimulai dari penentuan sasaran penelitian pada pegawai Disdukcapil Kota Malang dengan posisi Administrator Basis Data, Layanan Pelanggan, dan Operator. Setelah itu, tahapan dilanjutkan dengan penyusunan instrumen berupa kuesioner HAIS-Q. Tahap berikutnya dilakukan uji validitas dan reliabilitas menggunakan SPSS versi 30 (*Trial Mode*) dan dilanjutkan dengan pengumpulan data utama. Setelah itu, data diolah dan dianalisis untuk mengukur tingkat kesadaran keamanan informasi pegawai. Tahap akhir berupa penyusunan rekomendasi untuk peningkatan kesadaran keamanan informasi. Pelaksanaan seluruh tahapan penelitian ini berlangsung selama periode Januari hingga Mei 2025 **(Waktu Pelaksanaan)**.



Gambar 1. Alur Tahapan Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan jenis penelitian deskriptif survei. Pendekatan ini dipilih untuk mengukur dan mendeskripsikan tingkat kesadaran keamanan informasi pegawai Disdukcapil Kota Malang pada ketiga posisi yang telah ditentukan.

2.1. Penentuan Sasaran Penelitian

Sasaran dalam penelitian ini adalah pegawai Disdukcapil Kota Malang yang menduduki 3 posisi dengan jumlah populasi sebanyak 71 orang. Rincian populasi untuk Administrator Basis Data sebanyak 7 orang, Layanan Pelanggan sebanyak 55 orang, dan Operator sebanyak 9 orang. Penghitungan jumlah sampel keseluruhan dilakukan dengan menggunakan rumus *Slovin* [17] yang ditunjukkan pada persamaan (1).

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

Persamaan (1) menjelaskan bahwa n adalah total jumlah sampel, N adalah jumlah populasi, dan e adalah tingkat kesalahan sebesar 5%. Menggunakan persamaan ini [**penjelesan rumus slovin, rumus slovin ini digunakan untuk menentukan jumlah keseluruhan sampel pada ketiga posisi. Untuk penentuan jumlah sampel untuk tiap posisi, digunakan rumus 2 berdasarkan metode metode stratified random sampling**], jumlah sampel yang dibutuhkan dihitung sebagai berikut :

Tabel 1 Perhitungan Jumlah Sampel

Jumlah Populasi (N)	Perhitungan Sampel (n)	Jumlah Sampel
71	$n = \frac{71}{1+71(0{,}05)^2} = \frac{71}{1{,}18} = 60{,}29$	60

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Berdasarkan perhitungan pada **Error! Reference source not found.**, diperlukan total sampel sebanyak 60. Langkah selanjutnya adalah menentukan jumlah sampel untuk setiap posisi pegawai, yang dapat dilakukan menggunakan metode *stratified random sampling* berdasarkan persamaan (2).

$$ni = \frac{Ni}{N}\ x\ n \qquad (2)$$

Persamaan (2) digunakan untuk menentukan jumlah sampel yang diperlukan pada setiap posisi pegawai. Dalam formula ini, ni mewakili jumlah sampel untuk setiap posisi pegawai, Ni menunjukkan jumlah keseluruhan populasi dalam setiap posisi pegawai, N adalah jumlah populasi pegawai pada ketiga posisi yang telah ditentukan, serta n merupakan jumlah sampel keseluruhan. Berdasarkan persamaan tersebut, perhitungan detail jumlah sampel yang diperlukan untuk setiap posisi pegawai telah dilakukan dan hasilnya ditampilkan pada Tabel 2. Perhitungan Jumlah Sampel.

Tabel 2. Perhitungan Jumlah Sampel

Posisi Pegawai	Jumlah Populasi (Ni)	Perhitungan Sampel (ni)	Jumlah Sampel
Posisi Administrator Basis Data	7	$ni = \frac{7}{71}\ x\ 60 = 5{,}91$	6
Posisi Layanan Pelanggan	55	$ni = \frac{55}{71}\ x\ 60 = 46{,}47$	46
Posisi Operator	9	$ni = \frac{9}{71}\ x\ 60 = 7{,}60$	8
Total	71		60

Berdasarkan hasil pada Tabel 2. Perhitungan Jumlah Sampel, sampel dipilih secara acak sejumlah alokasi sampel yang dibutuhkan untuk setiap posisi pegawai. Proses pengambilan sampel dilakukan menggunakan fitur *randomizer* pada *Microsoft Excel*. Setiap responden dalam masing-masing posisi terlebih dahulu diberi nomor urut menggunakan fungsi RAND untuk menghasilkan nomort urut secara acak. Selanjutnya, nomor tersebut diurutkan berdasarkan nomor urut yang terkecil hingga terbesar, dan sejumlah sampel dipilih dari urutan tertas sesuai dengan kuota pada Tabel 2. Perhitungan Jumlah Sampel **(penjelasan bagaimana pengambilan sampel dilakukan secara stratified random sampling secara praktis)**.

2.2. Penyusunan Instrumen Penelitian

Instrumen pengumpulan data utama yang digunakan adalah kuesioner HAIS-Q. Kuesioner ini dirancang untuk mengukur Tingkat kesadaran kemanan informasi, termasuk pengetahuan, sikap, dan perilaku pegawai terkait keamanan informasi.

Hasil pengukuran Kesadaran Keamanan Informasi karyawan melalui HAIS-Q dapat dianggap sebagai dasar organisasi untuk melaksanakan program edukasi dan pelatihan keamanan informasi. Hal ini dikarenakan HAIS-Q mampu mengidentifikasi kekuatan dan kekurangan karyawan dalam setiap area fokus [18]. Area fokus dan sub-area fokus HAIS-Q dikelompokkan ke dalam kategori-kategori yang dapat dilihat pada Tabel 3. Area fokus dan Sub-area Fokus HAIS-Q. Hasil dari HAIS-Q dapat digunakan untuk merancang program pelatihan yang lebih efektif dan terarah, dengan fokus pada area-area di mana karyawan membutuhkan peningkatan pemahaman dan perilaku keamanan informasi.

Selain dikategorikan berdasarkan area fokus dan sub-area fokus, Tabel 3. Area fokus dan Sub-area Fokus HAIS-Q juga memetakan kuisioner ini ke dalam tiga dimensi utama kesadaran keamanan informasi, yaitu pengetahuan dengan simbol “a”, sikap dengan simbol “b”, dan perilaku dengan simbol “c”. Pemisahan ini bertujuan untuk memberikan pemahaman yang lebih terperinci mengenai aspek mana yang perlu ditingkatkan dalam diri karyawan, apakah dari sisi pengetahuan, sikap, atau perilaku nyata terkait kesadaran keamanan informasi. Pemetaan ini mengacu pada penelitian yang dilakukan oleh Dewi [11], dan digunakan sebagai dasar dalam menganalisis hasil pengisian kuesioner. Rincian pemetaan setiap item terhadap dimensi KAB juga disajikan pada Tabel 3. Area fokus dan Sub-area Fokus HAIS-Q.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Tabel 3. Area fokus dan Sub-area Fokus HAIS-Q

No	*Focus Area*	*Focus Sub-area*	*Dimensions*	*Statement*	*Statement Code*
1	*Password Management*	*Using the same password*	*Knowledge*	Saya tidak menggunakan kata sandi media sosial pribadi pada akun kerja karena saya paham risiko keamanan menggunakan kata sandi yang sama.	SA1a
		Sharing passwords	*Attitude*	Saya tidak pernah berbagi kata sandi akun kerja dengan orang lain karena saya menyadari potensi penyalahgunaannya.	SA2b
		Using a strong password	*Behavior*	Saya menggunakan kombinasi huruf, angka, dan simbol dalam kata sandi akun kerja, karena saya mengerti pentingnya keamanan kata sandi.	SA3c
2	*Email Use*	*Clicking on links in emails from known senders*	*Knowledge*	Saya selalu berhati-hati mengklik tautan di email, bahkan dari pengirim yang dikenal, karena saya tahu email bisa dipalsukan.	SA4a
		Clicking on links in emails from un-	*Attitude*	Saya tidak pernah mengklik tautan dari email pengirim yang tidak dikenal karena saya sadar risiko phishing dan malware.	SA5b
		known senders	*Behavior*	Saya tidak membuka lampiran email dari pengirim tidak dikenal karena saya paham bahaya malware yang mungkin terkandung di dalamnya.	SA6c
3	*Internet Use*	*Downloading files*	*Knowledge*	Saya hanya mengunduh file ke komputer kerja saya jika file tersebut membantu saya dalam melakukan pekerjaan saya.	SA7a
		Accessing dubious websites	*Attitude*	Saya menghindari mengakses situs web yang mencurigakan karena saya menyadari potensi ancaman keamanan siber.	SA8b
		Entering information online	*Behavior*	Saya selalu memastikan koneksi website aman (HTTPS) sebelum memasukkan informasi pribadi karena saya paham pentingnya keamanan data online.	SA9c
4	*Social Media Use*	*Social media privacy settings*	*Knowledge*	Saya secara aktif mengatur privasi akun media sosial saya karena saya peduli dengan keamanan informasi pribadi.	SA10a
		Considering the consequences	*Attitude*	Saya selalu mempertimbangkan dampak postingan media sosial sebelum mempublikasikannya karena saya memahami konsekuensi jangka panjangnya.	SA11b
		Posting about work	*Behavior*	Saya menghindari memposting hal terkait pekerjaan di media sosial pribadi karena saya sadar potensi risiko kebocoran informasi organisasi.	SA12c
5	*Mobile Device*	*Physically securing mobile devices*	*Knowledge*	Ketika bekerja di tempat umum, saya selalu memastikan laptop saya selalu bersama saya setiap saat.	SA13a

p-ISSN: 2775-4227
e-ISSN: 2775-4219

No	*Focus Area*	*Focus Sub-area*	*Dimensions*	*Statement*	*Statement Code*
		Sending sensitive information via Wi-Fi	*Attitude*	Saya tidak mengirim informasi sensitif melalui Wi-Fi publik yang tidak aman karena saya paham risiko intersepsi data.	SA14b
		Shoulder surfing	*Behavior*	Saya selalu menjaga privasi layar perangkat dari orang lain, terutama saat memasukkan informasi penting, karena saya tahu adanya risiko shoulder surfing.	SA15c
6	*Information Handling*	*Disposing of sensitive printouts*	*Knowledge*	Saya selalu menghancurkan dokumen kertas berisi informasi sensitif sebelum dibuang karena saya sadar pentingnya pembuangan dokumen yang aman.	SA16a
		Inserting removable media	*Attitude*	Saya hanya menggunakan removable media yang terpercaya dan sudah dipindai antivirus karena saya paham risiko malware dari media yang tidak aman.	SA17b
		Leaving sensitive material	*Behavior*	Saya tidak pernah meninggalkan dokumen atau perangkat berisi informasi sensitif di tempat terbuka karena saya mengerti risiko akses tidak sah.	SA18c
7	*Incident Reporting*	*Reporting suspicious behavior*	*Knowledge*	Saya akan melaporkan perilaku mencurigakan rekan kerja terkait keamanan informasi karena saya merasa bertanggung jawab terhadap keamanan lingkungan kerja.	SA19a
		Ignoring poor security behavior by colleagues	*Attitude*	Saya akan mengingatkan rekan kerja yang melakukan kesalahan keamanan karena saya peduli dengan keamanan informasi organisasi secara keseluruhan.	SA20b
		Reporting all incidents	*Behavior*	Saya selalu melaporkan setiap insiden keamanan informasi yang saya alami atau saksikan, sekecil apapun, karena saya memahami pentingnya pelaporan insiden.	SA21c

Sebelum instrumen digunakan dalam penelitian utama, kuesioner HAIS-Q terlebih dahulu dikonsultasikan kepada seorang dosen ahli di bidang keamanan informasi untuk memastikan kejelasan bahasa dan relevansi isi. Proses ini dilakukan sebagai bentuk validasi isi (*content validity*) melalui *expert judgement*. Selain itu, HAIS-Q juga telah tervalidasi secara empiris dalam penelitian yang dilakukan oleh Parsons pada tahun 2017 [12], yang menunjukkan bahwa instrumen ini memiliki reliabilitas dan validitas dalam mengukur kesadaran keamanan informasi individu [**Proses Validasi Instrumen**].

2.3. Pengujian Validitas dan Reliabilitas

Setelah instrument penelitian dibuat, dilakukan uji validitas dan reliabilitasnya menggunakan SPSS versi 30 (*Trial Mode*). Pengujian ini bertujuan untuk mengevaluasi keandalan dan keakuratan instrumen dalam mengukur apa yang seharusnya diukur, serta uji reliabilitas untuk menilai konsistensi jawaban responden terhadap pernyataan-pernyataan dalam kuesioner.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

2.4. Pengumpulan Data Utama

Penelitian ini menggunakan kuesioner berbasis *Google Form* sebagai instrumen utama dalam pengumpulan data yang dilakukan pada bulan april hingga mei 2025 **(periode pengumpulan data utama)**. Para responden diminta untuk memberikan tanggapan mereka pada setiap pernyataan dalam kuesioner menggunakan skala *Likert* 1 hingga 5, di mana penjelasan detail mengenai kategori skala tersebut disajikan pada Tabel 4 _ Skala Likert.

Tabel 4 _ Skala Likert

Skor	Pilihan Jawaban
5	Sangat Sesuai
4	Sesuai
3	Ragu-Ragu
2	Tidak Sesuai
1	Sangat Tidak Sesuai

2.5. Pengolahan dan Analisis Data

Tabel 5 _ Kategori Tingkat Kesadaran Keamanan Informasi

Tingkat Kesadaran	**Hasil Pengukuran (%)**
Baik	80-100
Rata-Rata	60-79
Buruk	Kurang dari sama dengan 59

Data yang diperoleh dari hasil penyebaran kuesioner selanjutnya diolah dan dianalisis untuk mengidentifikasi tingkat kesadaran keamanan informasi berdasarkan masing-masing posisi pegawai. Proses analisis ini mengacu pada kerangka teori yang dikembangkan oleh Kruger, sebagaimana digunakan dalam penelitian oleh Dewi [6], yang mengelompokkan tingkat kesadaran keamanan informasi ke dalam tiga kategori. Kategori tersebut disajikan dalam Tabel 5 _ Kategori Tingkat Kesadaran Keamanan Informasidan digunakan sebagai dasar dalam penarikan kesimpulan serta perumusan rekomendasi.

Teknik analisis data yang digunakan adalah analisis deskriptif. Data yang terkumpul dari kuesioner HAIS-Q diolah dan dianalisis untuk mendapatkan gambaran mengenai tingkat kesadaran kemanan informasi pegawai pada ketiga posisi dan pada masing-masing posisi. Analisis mencakup perhitungan skor rata-rata dan persentase jawaban pada setiap dimensi tingkat kesadaran keamanan informasi. Selain itu, dilakukan juga analisis komparatif untuk melihat perbedaan tingkat kesadaran keamanan informasi antar ketiga posisi pegawai yang menjadi fokus penelitian.

2.6. Penyusunan Rekomendasi

Penyusunan rekomendasi dilakukan sebagai tindak lanjut dari hasil analisis data kuisioner HAIS-Q yang mengukur tingkat kesadaran keamanan informasi pegawai di lingkungan Disdukcapil Kota Malang. Rekomendasi ini difokuskan pada area fokus yang menunjukkan nilai kurang baik pada dimensi pengetahuan, sikap, maupun perilaku. Tujuannya adalah untuk memberikan rekomendasi yang terukur dan aplikatif dalam meningkatkan kesadaran keamanan informasi secara menyeluruh. Rekomendasi yang disusun dapat menjadi dasar dalam perumusan program pelatihan, kebijakan internal, serta perbaikan prosedur kerja yang lebih aman dan responsif terhadap risiko keamanan informasi.

3. HASIL DAN PEMBAHASAN

3.1. Pengujian Validitas dan Reliabilitas

Pengujian validitas dan reliabilitas dalam penelitian ini dilakukan menggunakan data dari 10 responden yang berbeda dari responden utama. Hal ini bertujuan untuk menjaga objektivitas dan independensi hasil uji instrumen (**Penegasan ekspilist bahwa responden berbeda dari responden data utama**). Pengujian validitas dalam penelitian ini dilakukan dengan bantuan perangkat lunak SPSS versi 30 (*Trial Mode*) menggunakan analisis korelasi *Pearson*. Pengujian dilakukan dengan menghitung nilai R Tabel pada tingkat signifikansi 0,05 dan derajat kebebasan (dF) sebesar N-2, sesuai dengan uji dua arah, di mana N adalah jumlah responden. Dengan jumlah responden sebanyak 10, didapatkan nilai dF sebesar 8 dan nilai R Tabel sebesar 0,6319. Masing-masing responden memberikan jawaban atas tiga pernyataan pada setiap fokus area yang ditampilkan dalam Tabel 6 _ Hasil

p-ISSN: 2775-4227
e-ISSN: 2775-4219

Pengujian Validitas, seluruh pernyataan dinyatakan valid karena nilai korelasi *Pearson* lebih besar daripada nilai R Tabel.

Tabel 6 _ Hasil Pengujian Validitas

Area Fokus	Kode Pernyataan	Nilai Korelasi Pearson	Keterangan
Password Management	SA1a	0,739	Valid
	SA2b	0,731	Valid
	SA3c	0,831	Valid
Email Use	SA4a	0,910	Valid
	SA5b	0,780	Valid
	SA6c	0,813	Valid
Internet Use	SA7a	0,711	Valid
	SA8b	0,731	Valid
	SA9c	0,684	Valid
Social Media Use	SA10a	0,833	Valid
	SA11b	0,813	Valid
	SA12c	0,725	Valid
Mobile Device	SA13a	0,796	Valid
	SA14b	0,774	Valid
	SA15c	0,671	Valid
Information Handling	SA16a	0,706	Valid
	SA17b	0,766	Valid
	SA18c	0,758	Valid
Incident Reporting	SA19a	0,648	Valid
	SA20b	0,658	Valid
	SA21c	0,678	Valid

Pengujian reliabilitas dalam penelitian ini menggunakan SPSS versi 30 (*Trial Mode*) dengan mengacu pada nilai *Cronbach's Alpha* sebagai indikator. Hasil pengujian menunjukkan bahwa nilai *Cronbach's Alpha* sebesar 0,960 seperti pada Tabel 7 _ Hasil Pengujian Reliabilitas, yang menandakan bahwa pernyataan-pernyataan dalam kuesioner memiliki tingkat reliabilitas yang baik.

Tabel 7 _ Hasil Pengujian Reliabilitas

Cronbach Alpha Value	***Information***
0,960	*Reliable*

Hasil ini sejalan dengan penelitian sebelumnya yang menunjukkan bahwa nilai Cronbach's Alpha di atas 0,6 dianggap reliabel [11].

3.2. Pengumpulan Data Utama

Pengumpulan data dalam penelitian ini dilakukan melalui penyebaran kuesioner HAIS-Q menggunakan media *google form* kepada pegawai Disdukcapil Kota Malang. Instrumen ini menghasilkan data dalam bentuk angka pada skala 3 hingga 5, yang merepresentasikan tingkat persetujuan responden terhadap 21 pernyataan yang ada. Pengumpulan data utama ini dilaksanakan setelah instrumen dinyatakan valid dan reliabel melalui uji validitas dan reliabilitas sebelumnya. Untuk menjaga objektivitas dan menghindari bias, responden yang dilibatkan dalam pengumpulan data utama berbeda dari responden yang digunakan pada tahap uji validitas dan reliabilitas (**Penegasan ekspilist bahwa responden berbeda dari responden uji validitas dan reliabilitas**). Data yang diperoleh sebanyak 60 responden, yang terdiri dari pegawai dengan posisi strategis seperti Administrator Basis Data, Layanan Pelanggan, dan Operator dengan rincian karakteristik responden yang dapat dilihat pada Tabel 8 _ Demografi Responden. Dengan demikian, data yang diperoleh dapat untuk dianalisis lebih lanjut dalam menentukan tingkat kesadaran keamanan informasi pegawai.

Pengumpulan data utama dilakukan terhadap 60 responden yang berbeda dari responden uji validitas dan reliabilitas, untuk memastikan objektivitas hasil dan menghindari bias pengukuran.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

3.3. Demografi Responden

Penelitian ini melibatkan 60 pegawai Disdukcapil Kota Malang sebagai responden dengan karakteristik demografi seperti pada Tabel 8 _ Demografi Responden.

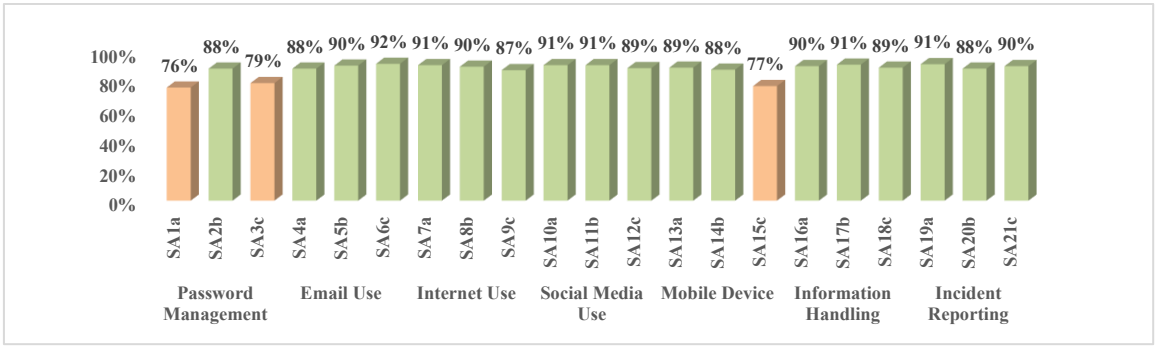
Tabel 8 _ Demografi Responden

No	Variabel	Item	Jumlah	Presentase
1	Jenis Kelamin	Pria	27	45 %
		Wanita	33	55 %
2	Usia	24 – 35	36	60 %
		36 – 45	21	35 %
		46 – 60	3	55 %
3	Bidang Pendidikan Terakhir	Teknologi Informasi	32	53 %
		Diluar Teknologi Informasi	28	47 %
4	Bidang Pekerjaan	Administrator Basis Data	6	10 %
		Layanan Pelanggan	46	77 %
		Operator	8	13 %

Berdasarkan Tabel 8 _ Demografi Responden, distribusi demografi dalam penelitian ini didominasi oleh wanita dengan presentase sebesar 55% dengan mayoritas usia responden berada pada rentang 24–35 tahun dengan presentase sebesar 60%. Selain itu, sebagian besar responden memiliki latar belakang pendidikan di bidang teknologi informasi dengan presentase sebesar 53% dan bekerja pada posisi layanan pelanggan dengan presentase sebesar 77%. Distribusi demografi ini menunjukkan bahwa mayoritas responden berada pada posisi yang berhubungan langsung dengan pemrosesan dan pengelolaan data kependudukan.

3.4. Hasil dan Anlisis Data Utama

Data yang diperoleh dari kuesioner HAIS-Q dianalisis untuk menentukan tingkat kesadaran keamanan informasi pada pegawai Disdukcapil Kota Malang. Berdasarkan Gambar 2. Grafik Hasil Pengukuran Tingkat Kesadaran pada Ketiga Posisi menunjukkan bahwa tingkat kesadaran keamanan informasi pegawai tergolng baik, dengan rata-rata skor berada diatas 85%.



Gambar 2. Grafik Hasil Pengukuran Tingkat Kesadaran pada Ketiga Posisi

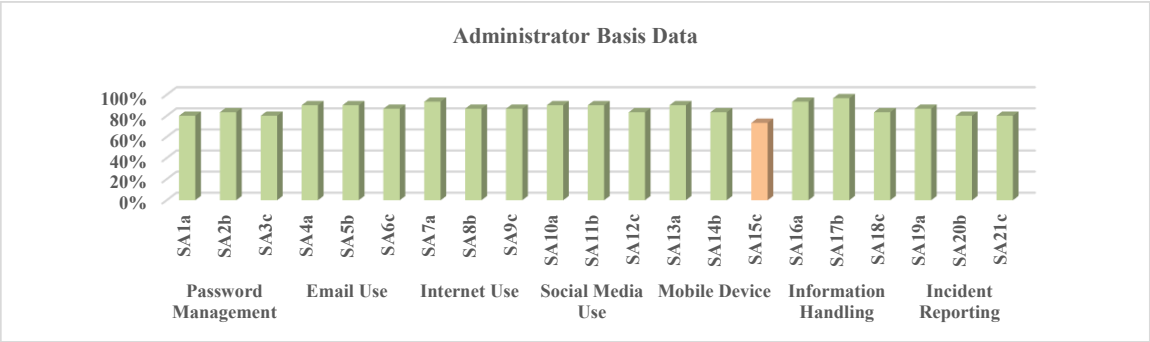
Namun, analisis lebih lanjut pada masing-masing posisi pegawai mengungkapkan adanya perbedaan kekuatan dan kelemahan yang spesifik. Terdapat beberapa fokus area yang hanya mencapai tingkat kesadaran "rata-rata" berdasarkan klasifikasi dalam Tabel 5 _ Kategori Tingkat Kesadaran Keamanan Informasi**Error! Reference source not found.**, yang disajikan menggunakan kode warna: hijau untuk "baik", jingga untuk "rata-rata", dan merah untuk "buruk". Oleh karena itu, meskipun hasil keseluruhan menunjukkan kondisi yang positif, penting untuk meninjau secara rinci temuan pada tiap posisi, guna mengidentifikasi area-area yang memerlukan perhatian dan perbaikan khusus.

3.4.1. Administrator Basis Data

Berdasarkan pada Gambar 3. Grafik Hasil Pengukuran pada Posisi Administrator Basis Data, data menunjukkan bahwa pegawai pada posisi administrator basis data secara umum menunjukkan tingkat kesadaran keamanan informasi yang baik, dengan rata-rata skor di atas 80%. Namun, terdapat satu aspek yang masih perlu perhatian, yaitu perilaku pada area perangkat selular (*mobile device*) yang hanya mendapatkan skor 73%. Skor ini

p-ISSN: 2775-4227
e-ISSN: 2775-4219

diperoleh dari hasil tanggapan responden terhadap pernyataan dengan kode "SA15c", di mana separuh dari responden masih memberikan jawaban pada skala 3 dari 5. Hal ini menunjukkan bahwa sebagian pegawai belum sepenuhnya menerapkan kebiasaan melindungi tampilan layar perangkat, sehingga diperlukan pelatihan tambahan terkait praktik perlindungan visual terhadap informasi sensitif.

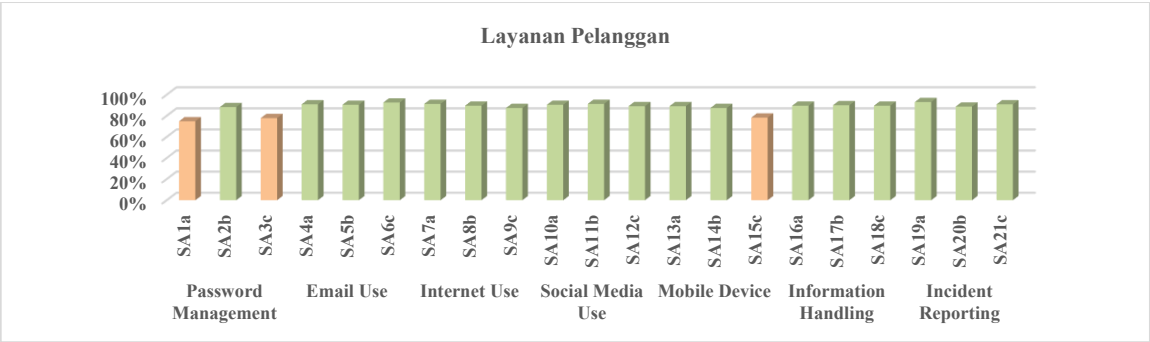


Gambar 3. Grafik Hasil Pengukuran pada Posisi Administrator Basis Data

3.4.2. Layanan Pelanggan

Berbeda dengan posisi administrator basis data, pegawai dengan posisi layanan pelanggan memiliki beberapa aspek yang masih perlu ditingkatkan. Berdasarkan Gambar 4. Grafik Hasil Pengukuran pada Posisi Layanan Pelanggan , pegawai pada layanan pelanggan menunjukkan tingkat kesadaran keamanan informasi yang baik, dengan sebagian besar skor berada di atas 85%. Namun, masih ditemukan beberapa aspek yang masih perlu ditingkatkan.

Pada area manajemen kata sandi (*password management*), skor aspek pengetahuan hanya mencapai 75%, yang mencerminkan pemahaman sebagian pegawai masih kurang terkait pentingnya menggunakan kata sandi yang berbeda untuk setiap akun yang berbeda (baik akun kerja ataupun akun media sosial). Skor ini didapat berdasarkan jawaban responden terhadap pernyataan dengan kode "SA1a", dimana sebanyak 17 dari 46 responden memberikan jawaban pada skala 3 dari 5. Hal ini diperkuat dengan temuan pada aspek perilaku yang hanya memperoleh skor 78% yang juga didapat berdasarkan jawaban responden terhadap pernyataan dengan kode "SA3c", aspek ini terkait dengan penggunaan kombinasi huruf, angka, dan simbol dalam pembuatan kata sandi akun kerja. Rendahnya skor ini menunjukkan bahwa masih terdapat risiko keamanan yang muncul dari penggunaan kata sandi yang lemah dan berulang, sehingga perlu ditingkatkan melalui edukasi dan kebijakan internal yang lebih tegas.



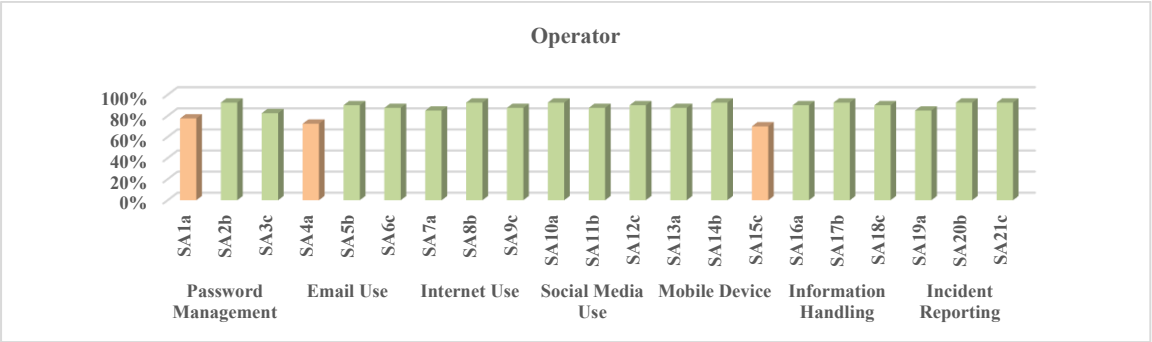
Gambar 4. Grafik Hasil Pengukuran pada Posisi Layanan Pelanggan

Sementara itu, pada area perangkat selular, aspek perilaku mendapatkan skor 78% yang didapat karena sebanyak 21 responden menjawab kuisioner pada skala 3 dari 5. Nilai ini didapat dari pernyataan dengan kode "SA15c" dan merujuk pada perilaku menjaga privasi layar perangkat dari pengintaian orang lain (shoulder surfing), terutama saat memasukkan informasi penting. Skor ini menunjukkan bahwa sebagian pegawai belum secara konsisten menerapkan kebiasaan tersebut dalam praktik sehari-hari, yang dapat menimbulkan potensi kebocoran data saat menggunakan perangkat di ruang publik atau area kerja bersama.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

3.4.3. Operator

Untuk pegawai pada posisi operator, hasil analisis pada Gambar 5. Grafik Hasil Pengukuran pada Posisi Operator menunjukkan aspek pengetahuan pada area manajemen kata sandi hanya mencapai skor 78%. Hal ini menunjukkan kurangnya pemahaman terkait pentingnya penggunaan kata sandi yang berbeda untuk setiap akun. Selanjutnya, pada area penggunaan surat elektronik (*email use*), aspek pengetahuan mencatat skor 73%. Hal ini menunjukkan bahwa masih ada pegawai yang belum sepenuhnya memahami risiko dari tautan berbahaya, meskipun dikirim oleh pengirim yang dikenal. Area perangkat selular juga memperlihatkan skor rendah pada aspek perilaku, yaitu sebesar 70%. Ketiga skor tersebut didapatkan dari jawaban responden terhadap pernyataan dengan kode ”SA1a”, ”SA4a”, dan ”SA15c”, dimana seluruh responden menjawab hanya pada skala 3 sampai 4 dari 5. Hal ini mengindikasikan bahwa kebiasaan menjaga privasi layar saat menggunakan perangkat belum sepenuhnya dilakukan secara konsisten. Secara umum, meskipun tingkat kesadaran pada posisi operator sudah baik, temuan ini menunjukkan perlunya peningkatan pemahaman dan pembiasaan perilaku aman, terutama melalui pelatihan dan penguatan kebijakan keamanan informasi.



Gambar 5. Grafik Hasil Pengukuran pada Posisi Operator

Dengan temuan ini, meskipun secara keseluruhan kesadaran sudah baik, organisasi tetap perlu memperkuat aspek-aspek yang lemah melalui edukasi rutin dan pembentukan budaya kerja yang lebih sadar terhadap keamanan informasi.

3.5. Penyusunan Rekomendasi

Berdasarkan hasil analisis, sebagian besar pegawai Disdukcapil Kota Malang telah menunjukkan tingkat kesadaran keamanan informasi yang baik, meskipun masih terdapat kelemahan pada beberapa fokus area. Untuk mengatasi hal tersebut, dinas perlu mengambil langkah strategis yang terintegrasi. Langkah pertama yang disarankan adalah penyelenggaraan pelatihan keamanan informasi yang relevan sesuai dengan kondisi kesadaran keamanan informasi pegawai. Materi pelatihan tersebut meliputi pelatihan terkait dengan manajemen kata sandi yang berfokus pada penerapan kata sandi yang berbeda untuk akun yang berbeda (bedakan kata sandi untuk akun pribadi dan akun kerja) dan pembuatan kata sandi yang kuat (penggunaan kombinasi huruf, angka, dan simbol) untuk akun kerja, selanjutnya ada pelatihan terkait dengan penggunaan perangkat selular yang berfokus dalam hal penjagaan privasi ketika menggunakan perangkat selular ditempat publik untuk kepentingan dinas, dan terakhit pelatihan terkait dengan penggunaan surat elektronik yang berfokus dalam hal kewaspadaan terhadap tautan yang terlampir dalam surat elektronik (sekalipun yang dikirim dari pihak yang tampak terpercaya). Untuk memperkuat pesan keamanan secara berkelanjutan, dinas juga perlu menjalankan kampanye visual melalui media seperti poster, infografik, dan pengingat digital di lingkungan kerja. Di samping itu, penguatan kebijakan internal menjadi hal yang krusial, misalnya dengan mewajibkan pembuatan kata sandi kuat untuk akun kerja, tidak diperbolehkannya penggunaan kata sandi akun pribadi untuk akun kerja, dan pembuatan SOP terkait dengan penggunaan perangkat selular untuk kepentingan dinas serta pemeriksaan tautan sebelum diakses. Evaluasi secara berkala juga penting dilakukan untuk memastikan efektivitas pengimplementasian kebijakan ini. Dengan strategi yang menyeluruh ini, diharapkan terbentuk budaya kerja yang lebih aman, peduli, dan siap menghadapi berbagai ancaman siber secara kolektif [4], [11], [18]-[20].

4. DISKUSI TEMUAN DAN IMPLIKASINYA (SUBBAB DISKUSI)

p-ISSN: 2775-4227
e-ISSN: 2775-4219

4.1. Perbandingan dengan Studi Sebelumnya

Hasil penelitian ini menunjukkan bahwa secara umum pegawai Disdukcapil Kota Malang telah memiliki tingkat kesadaran keamanan informasi yang baik, dengan rata-rata skor di atas 85%. Namun, kelemahan masih ditemukan pada beberapa area seperti manajemen kata sandi, penggunaan email, dan perangkat seluler. Temuan ini sejalan dengan penelitian Dewi pada tahun 2024 yang mengukur kesadaran keamanan informasi pegawai BMKG dan menemukan kelemahan serupa pada area password management dan mobile computing meskipun skor keseluruhan berada pada kategori "baik" sebesar 81,67% [11].

Selain itu, penelitian ini juga mendukung temuan Ramadhan dan Purwandari pada tahun 2023 yang menilai pengguna aplikasi perbankan digital. Mereka mendapati bahwa walaupun pemahaman dan sikap sudah cukup baik, praktik perilaku pengguna masih belum konsisten dan memerlukan peningkatan, khususnya pada kebiasaan digital sehari-hari seperti klik tautan yang tidak aman dan penggunaan sandi yang lemah [15]. Temuan serupa juga ditemukan oleh Kusnadi pada tahun 2024 terhadap kalangan mahasiswa, yang meskipun memiliki pemahaman teoretis cukup, tetap menunjukkan tingkat perilaku keamanan yang rendah [14].

4.2. Kontribusi Penelitian

Penelitian ini berkontribusi pada pengayaan literatur terkait pengukuran kesadaran keamanan informasi di sektor publik, khususnya di instansi pemerintah yang menangani data sensitif seperti Disdukcapil. Berbeda dari studi sebelumnya yang lebih banyak berfokus pada sektor perbankan atau pendidikan tinggi, penelitian ini secara spesifik menyoroti perbedaan tingkat kesadaran berdasarkan struktur posisi kerja, yaitu administrator basis data, layanan pelanggan, dan operator. Pendekatan ini memungkinkan analisis yang lebih mendalam dan kontekstual terhadap kebutuhan pelatihan dan kebijakan di masing-masing posisi strategis dalam organisasi.

Kontribusi praktis dari penelitian ini juga terletak pada penerapan instrumen HAIS-Q secara lokal dan adaptif, serta penyusunan rekomendasi pelatihan berbasis area fokus kelemahan pegawai, yang dapat langsung diterapkan oleh instansi terkait.

4.3. Implikasi terhadap Kebijakan dan Praktik Keamanan Informasi di Disdukcapil Kota Malang

Hasil penelitian ini memiliki implikasi langsung terhadap penguatan kebijakan keamanan informasi di lingkungan Disdukcapil Kota Malang. Pertama, identifikasi area-area kelemahan dapat menjadi landasan penyusunan program pelatihan keamanan informasi yang lebih terfokus dan tepat sasaran. Misalnya, pelatihan untuk meningkatkan kesadaran terhadap risiko shoulder surfing atau pengelolaan kata sandi yang aman.

Kedua, hasil ini dapat digunakan sebagai *evidence-based decision making* dalam penyusunan SOP baru serta revisi terhadap pedoman kerja yang berhubungan dengan keamanan informasi. Disdukcapil juga dapat menjadikan hasil pengukuran ini sebagai indikator kinerja tahunan dalam pengelolaan SDM.

Ketiga, hasil penelitian ini menunjukkan pentingnya menanamkan budaya keamanan informasi secara organisasi, bukan hanya pada level teknis. Hal ini dapat dilakukan dengan penyediaan media edukasi visual, pengingat berkala di sistem kerja, dan penyesuaian sistem informasi agar mendukung perilaku aman seperti keharusan mengganti sandi secara berkala dan pemeriksaan otomatis pada email masuk.

5. KESIMPULAN

Penelitian ini berhasil mengidentifikasi kondisi kesadaran keamanan informasi di lingkungan Disdukcapil Kota Malang berdasarkan analisis terhadap pegawai pada tiga posisi strategis, yakni Administrator Basis Data, Layanan Pelanggan, dan Operator. Hasil analisis menunjukkan bahwa secara umum tingkat kesadaran pegawai berada pada kategori baik, namun masih terdapat area fokus yang memerlukan perhatian lebih, khususnya pada manajemen kata sandi, penggunaan perangkat selular, dan surat elektronik **(Ringkasan hasil utama).** Temuan ini menegaskan bahwa aspek perilaku masih menjadi tantangan utama, meskipun aspek pengetahuan dan sikap tergolong cukup baik. Oleh karena itu, peningkatan kesadaran keamanan informasi perlu difokuskan pada pembentukan kebiasaan nyata yang konsisten dan sesuai dengan kebijakan organisasi **(Implikasi temuan – fokus pada praktik nyata).** Secara metodologis, penelitian ini menegaskan pentingnya penggunaan instrumen HAIS-Q dalam pemetaan kesadaran keamanan informasi secara terfokus berdasarkan posisi kerja, yang dapat memberikan dasar ilmiah dalam pengembangan strategi pelatihan dan kebijakan internal. Kontribusi utama dari penelitian ini adalah memperluas penerapan HAIS-Q dalam konteks instansi pemerintah, khususnya instansi pada sektor pelayanan publik yang menangani data kependudukan yang sangat sensitif **(Kontribusi ilmiah – penguatan metode dan konteks baru).** Dari sisi praktis, hasil penelitian ini memiliki implikasi langsung terhadap kebijakan dan praktik keamanan informasi, yaitu perlunya penyusunan program pelatihan berbasis data dan evaluasi rutin terhadap kebijakan internal. Intervensi yang disarankan mencakup pelatihan berbasis peran, kampanye keamanan

p-ISSN: 2775-4227
e-ISSN: 2775-4219

informasi, serta pembaruan standar operasional prosedur (SOP) untuk meningkatkan budaya kerja yang lebih aman dan responsif terhadap ancaman siber **(Implikasi praktis dan kebijakan – bukan harapan)**. Dengan memahami kondisi aktual di lapangan melalui hasil pengukuran yang terstandar, organisasi dapat melaksanakan peningkatan kesadaran secara lebih efektif dan berkelanjutan, serta menyesuaikan kebijakan kerja dan alokasi sumber daya secara strategis untuk memperkuat sistem pertahanan informasi di era digital **(Penekanan pada keberlanjutan strategi – bukan sekadar saran atau harapan).**

DAFTAR PUSTAKA

[1] A. A. Zaman, J. Anwar, dan A. Fadlian, "Pertanggung Jawaban Pidana Kebocoran Data BPJS Dalam Perspektif UU ITE," vol. 1, hlm. 146–157, Okt 2021, doi: https://doi.org/10.35706/djd.v1i2.5732.

[2] Z. Fadhli, S. W. Rahayu, dan I. A. Gani, "Perlindungan Data Pribadi Konsumen Pada Transaksi Paylater," *Compet Change*, Feb 2022.

[3] M. O. Hoshmand, S. Ratnawati, dan E. P. Korespondensi, "Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity," *Jurnal Sains dan Teknologi*, vol. 5, hlm. 679–686, 2023, doi: 10.55338/saintek.v5i2.2347.

[4] 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, hlm. 315–320, Apr 2024, doi: 10.25126/jtiik.20241128106.

[5] Faliandy, M Yonandio Lazuardi, dan Tata Sutabri, "Analisis Kesadaran Keamanan Siber pada Pengguna Aplikasi E-Court di Lingkungan Pengadilan," *Jurnal Ilmiah Binary STMIK Bina Nusantara Jaya Lubuklinggau*, vol. 5, no. 2, hlm. 101–107, Jul 2023, doi: 10.52303/jb.v5i2.106.

[6] K. Hore *dkk.*, "Cybersecurity and critical care staff: A mixed methods study," *Int J Med Inform*, vol. 185, Mei 2024, doi: 10.1016/j.ijmedinf.2024.105412.

[7] U. Ladayya, D. Prayitno, M. Syani, R. Hikmawan, dan N. W. Abdulmajid, "Kesadaran Keamanan Informasi atas Phising, Smishing, dan Vishing pada Warga Kota Cimahi," Jul 2024. [Daring]. Tersedia pada: https://journal.fkom.uniku.ac.id/ilkom

[8] 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," Universitas Telkom, Bandung, 2024. Diakses: 11 Juli 2025. [Daring]. Tersedia pada: 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

[9] A. Aprila Ipungkarti, "Penerapan IT Security Awareness Standar Keamanan ISO 27001 Di BPJS Ketenagakerjaan Kantor Cabang Purwakarta," *Jurnal Media Infotama*, vol. 19, hlm. 103, Apr 2023.

[10] S. Destya, "Pengukuran Tingkat Kesadaran Keamanan Informasi Berdasarkan Behavior Dan Offence Scale," *Journal of Computer Engineering System and Science*, vol. 5, no. 2, hlm. 236–240, Jul 2020, doi: https://doi.org/10.24114/cess.v5i2.18206.

[11] K. M. R. Dewi, R. D. Yudistira, dan Y. Ruldeviyani, "Pengukuran Tingkat Kesadaran Keamanan Informasi Pegawai Pada Instansi Pemerintah," *Indonesian Journal of Computer Science*, vol. 13, Apr 2024.

[12] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, dan T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Comput Secur*, vol. 66, hlm. 40–51, Jan 2017, doi: 10.1016/j.cose.2017.01.004.

[13] M. Ramadhani dan P. K. Sari, "Examining the Knowledge, Attitude, and Behavior of IT Division Staff on Information Security Issues: A Case Study in a Telecommunication Company," *International Research Journal of Economics and Management Studies*, vol. 3, no. 6, hlm. 354–361, Jun 2024, doi: 10.56472/25835238/IRJEMS-V3I6P139.

[14] K. Kirani Kusnadi, A. Hafizhah Brarida, I. Qinthara Heriswan, dan N. Aini Rakhmawati, "Pengukuran Tingkat Kesadaran Keamanan Informasi Dan Privasi Di Kalangan Mahasiswa Dengan HAIS-Q Instrument," 2024.

[15] Ramadhan Taufiq dan Purwandari Betty, "Analisis Tingkat Kesadaran Keamanan Informasi: Studi Kasus Pengguna Aplikasi Perbankan Digital Di Indonesia Guna Mencegah Social Engineering," *Syntax Idea*, vol. 5, Jan 2023.

p-ISSN: 2775-4227
e-ISSN: 2775-4219

[16] Prenđa Suzana, P. Mikac, dan S. Rački, "Human aspects of information security questionnaire (HAIS-Q) – Croatian translation and validation," Des 2024.

[17] G. P. Adhikari, "Calculating the Sample Size in Quantitative Studies," *Scholars' Journal*, vol. 4, Des 2021, [Daring]. Tersedia pada: https://www.nepjol.info/index.php/scholars

[18] 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," Jun 2023.

[19] B. E. Supriyanto, "Peningkatan Kesadaran Keamanan Informasi Kepada Pegawai KPPN Watampone," 2024. https://djpb.kemenkeu.go.id/kppn/watampone/id/data-publikasi/artikel/3726-peningkatan-kesadaran-keamanan-informasi-kepada-pegawai-kppn-watampone.html (accessed May. 27, 2025).

[20] C. Ridho, "7 Strategi Efektif untuk Mencegah Kebocoran Data," 2022. https://csirt.banjarmasinkota.go.id/posts/7-strategi-efektif-untuk-mencegah-kebocoran-data (accessed May. 27, 2022).