JALIN RISTEK
Jurnal Ilmiah Inovasi Daerah Riset dan Teknologi
Vol. 2, Nomor 2, November 2025

ISSN 3063-878X

ANALISIS TINGKAT KESADARAN KEAMANAN INFORMASI PEGAWAI PEMERINTAH KABUPATEN GUNUNGKIDUL

ANALYSIS OF THE LEVEL OF INFORMATION SECURITY AWARENESS OF GOVERNMENT EMPLOYEES IN GUNUNGKIDUL DISTRICT

Didik Handoko, Via Aninda Sheva
Dinas Komunikasi dan Informatika Kabupaten Gunungkidul
Koresponding email : didikbermakna@gmail.com

ABSTRAK

Keamanan informasi menjadi bagian penting dalam perkembangan teknologi informasi saat ini dan transformasi digital pada pelaksanaan pemerintahan, termasuk di lingkungan Pemerintah Kabupaten Gunungkidul. Penelitian ini bertujuan menganalisis tingkat kesadaran keamanan informasi pegawai dengan pendekatan Pengetahuan, Sikap, dan Perilaku (*Knowledge, Attitude, Behavior*). Metode penelitian yang digunakan adalah penelitian kuantitatif deskriptif dengan instrumen kuesioner kepada 3.323 pegawai di 49 perangkat daerah pada periode 15–24 Januari 2025. Data dianalisis dengan *Microsoft Excel* 2019 dan SPSS versi 26 menggunakan skala *Likert* (1–4), dengan uji validitas *Pearson Correlation* yang menghasilkan seluruh item valid (*sig.*<0,05) dan uji reliabilitas *Cronbach's Alpha* dengan nilai 0,912 yang menunjukkan konsistensi instrumen sangat tinggi. Hasil penelitian menunjukkan tingkat kesadaran keamanan informasi pegawai berada pada kategori baik dengan rata-rata 87,13%. Kesadaran tertinggi terdapat pada aspek menjaga kerahasiaan password serta kepatuhan terhadap aturan, sedangkan pelaporan insiden keamanan informasi dan kebiasaan pencadangan data masih perlu ditingkatkan. Analisis berdasarkan demografi menunjukkan bahwa pegawai yang lebih muda dan dengan pengalaman kerja lebih singkat memiliki tingkat kesadaran lebih tinggi dibandingkan kelompok usia dan pengalaman kerja yang lebih lama. Temuan ini menegaskan pentingnya strategi peningkatan kesadaran keamanan informasi yang berfokus pada seluruh pegawai, terutama dalam memperkuat mekanisme pelaporan insiden dan mendorong kebiasaan pencadangan data secara berkala. Kesimpulannya, meskipun tingkat kesadaran keamanan informasi pegawai cukup baik, diperlukan kebijakan berkelanjutan berupa pelatihan terstruktur, integrasi kesadaran keamanan informasi dalam evaluasi kinerja, serta penanaman budaya keamanan informasi di seluruh perangkat daerah untuk mendukung tata kelola pemerintahan berbasis digital yang aman dan andal. Penelitian ini diharapkan memberikan kontribusi praktis dalam pengembangan kebijakan keamanan informasi Pemerintah Kabupaten Gunungkidul dan menjadi referensi bagi instansi pemerintah lainnya dalam meningkatkan kesadaran keamanan informasi di era transformasi digital.

Kata Kunci: Keamanan Informasi, Kesadaran, Pemerintah

ABSTRACT

Information security has become a vital part of current information technology developments and the digital transformation of government operations, including within the Gunungkidul Regency Government. This research aims to analyze the level of information security awareness among employees using the Knowledge, Attitude, Behavior approach. The research method used was a descriptive quantitative study with a questionnaire administered to 3,323 employees across 49 regional agencies from January 15 to 24, 2025. Data were analyzed

ISSN 3063-878X

using Microsoft Excel 2019 and SPSS version 26 with a Likert scale (1–4). A Pearson Correlation validity test showed that all items were valid (sig.<0.05), and a Cronbach's Alpha reliability test yielded a value of 0.912, indicating very high instrument consistency. The research results show that employees' information security awareness is in the good category, with an average of 87.13%. The highest level of awareness was found in the aspects of maintaining password confidentiality and compliance with regulations, while reporting information security incidents and the habit of data backup still need improvement. Demographic analysis revealed that younger employees with less work experience have higher awareness levels compared to older age groups and those with longer work experience. These findings underscore the importance of an information security awareness strategy that focuses on all employees, particularly in strengthening incident reporting mechanisms and encouraging the habit of regular data backups. In conclusion, although employees' information security awareness is reasonably good, continuous policies are needed, such as structured training, integrating information security awareness into performance evaluations, and fostering an information security culture across all regional agencies to support secure and reliable digital governance. This research is expected to make a practical contribution to the development of the Gunungkidul Regency Government's information security policies and serve as a reference for other government agencies in enhancing information security awareness in the era of digital transformation.

Keywords: Information Security, Awareness, Government

PENDAHULUAN

Penetrasi internet di Indonesia mengalami peningkatan yang signifikan. Pada tahun 2024, hasil survei menunjukkan penetrasi internet mencapai 79,5%, yang berarti 221.563.479 jiwa terkoneksi dari total populasi 278.696.000 jiwa (Asosiasi Penyelenggara Jasa Internet Indonesia, 2024). Ketersediaan internet yang tinggi dan adopsi teknologi dalam layanan publik memberikan berbagai dampak positif, termasuk peningkatan akses informasi, efisiensi proses bisnis, dan kemudahan dalam berkomunikasi (Kementerian Komunikasi dan Informatika, 2024a).

Pemerintah Kabupaten Gunungkidul saat ini telah mengimplementasikan *Smart City* dan Sistem Pemerintahan Berbasis Elektronik (SPBE) sebagai bagian dari transformasi digital, yang bertujuan meningkatkan efisiensi pelayanan publik berbasis digital. Pada tahun 2024, Indeks SPBE Kabupaten Gunungkidul mencapai 3,96 dengan kategori sangat baik, mencerminkan implementasi SPBE di Kabupaten Gunungkidul telah mendukung penguatan efektivitas tata kelola pemerintahan dan layanan kepada masyarakat (Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi, 2024). Selain itu, dalam implementasi *Smart City*, berdasarkan Laporan Hasil Evaluasi Tahap II Implementasi Kota Cerdas (*Smart City*) Tahun 2024 dari Kementerian Komunikasi dan Informatika, Kabupaten Gunungkidul memperoleh Indeks Pencapaian (*Performance*) urutan ke-3 secara nasional dan urutan pertama di Daerah Istimewa Yogyakarta dengan nilai 3,81 (Kementerian Komunikasi dan Informatika, 2024b).

Namun, seiring dengan kemajuan digitalisasi ini, keamanan informasi menjadi aspek yang krusial dalam keberlanjutan transformasi digital. Keamanan informasi adalah perlindungan aset informasi yang menggunakan, menyimpan, atau mengirimkan informasi melalui penerapan kebijakan, pendidikan, dan teknologi. Karakteristik penting informasi, termasuk (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*), harus dilindungi setiap saat (Whitman & Mattord, 2018).

ISSN 3063-878X

Laporan Evaluasi Pelaksanaan Persandian untuk Pengamanan Informasi Pemerintah Daerah Kabupaten Gunungkidul Tahun Anggaran 2024 yang dilakukan oleh Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa tingkat kepatuhan pelaksanaan persandian untuk pengamanan informasi telah mencapai kategori baik dengan nilai 89,301 (Badan Siber dan Sandi Negara, 2024b). Penilaian ini berdasarkan pada pemeriksaan dokumen, data dukung, serta konfirmasi kepada Dinas Komunikasi dan Informatika Kabupaten Gunungkidul. Meskipun hasil evaluasi tersebut menunjukkan tingkat kepatuhan yang baik, tantangan dalam pengamanan informasi tetap menjadi perhatian utama. Salah satu indikasi bahwa aspek ini masih perlu diperkuat adalah adanya notifikasi dari BSSN melalui surat Nomor T.20/BSSN/D2/DT.01.01/1/2025 tertanggal 5 Januari 2025, yang menginformasikan potensi insiden terkait keamanan data di lingkungan Pemerintah Kabupaten Gunungkidul (Badan Siber dan Sandi Negara, 2025). Dari tujuh rekomendasi tindak lanjut yang diberikan, salah satu yang ditekankan adalah pentingnya meningkatkan publikasi keamanan bagi pengguna akhir, agar mereka lebih memahami jenis kelemahan yang ditemukan serta secara aktif meningkatkan kesadaran terhadap keamanan informasi (*security awareness*).

Insiden tersebut mengindikasikan bahwa meskipun regulasi dan sistem keamanan telah diterapkan dengan baik, ancaman keamanan informasi masih dapat terjadi, terutama karena faktor kesalahan manusia. Kurangnya kesadaran akan kebijakan keamanan informasi organisasi, ketidaktahuan akan praktik keamanan informasi umum, atau kelalaian oleh karyawan adalah beberapa alasan pelanggaran data yang disebabkan oleh kesalahan manusia (Selvam, 2020).

Menurut Von Solms dan Van Niekerk (2013) terkait keamanan informasi, referensi pada faktor manusia biasanya berkaitan dengan peran manusia dalam proses keamanan. Dalam keamanan siber, faktor ini memiliki dimensi tambahan, yaitu manusia sebagai target potensial serangan siber atau bahkan tanpa sadar berpartisipasi dalam serangan siber. Whitman dan Mattord (2018) menekankan bahwa kesalahan karyawan adalah salah satu ancaman utama terhadap aset informasi, sehingga sangat berharga untuk mengembangkan program untuk memerangi ancaman.

Kesadaran keamanan informasi menjadi faktor utama dalam menjaga keberlangsungan sistem informasi pemerintah. Studi sebelumnya menunjukkan bahwa faktor manusia merupakan titik lemah utama dalam keamanan informasi. Salah satunya, penelitian yang dilakukan oleh Kruger dan Kearney (2006) mengungkapkan bahwa faktor individu, seperti pengetahuan, sikap, dan perilaku (*Knowledge, Attitude, and Behavior* (KAB)), sangat memengaruhi efektivitas kebijakan keamanan informasi dalam organisasi. Studi lainnya, penelitian yang dilakukan di Badan Meteorologi, Klimatologi, dan Geofisika (BMKG) menunjukkan bahwa penerapan ISO/IEC 27001:2013 meningkatkan kesadaran pegawai terhadap keamanan informasi (Dewi & Ruldeviyani, 2024). Studi tersebut menunjukkan bahwa kesadaran keamanan informasi memainkan peran penting dalam melindungi data dan sistem, terutama di lingkungan pemerintahan dan organisasi.

Penelitian di sektor swasta juga menunjukkan bahwa pengalaman kerja berpengaruh terhadap kesadaran keamanan informasi pegawai. Studi di PT Meshindo Jayatama menemukan bahwa pegawai dengan pengalaman lebih lama lebih waspada terhadap ancaman siber (Gofur & Kurniawan, 2024).

Pada lingkungan akademik, penelitian menunjukkan bahwa tingkat kesadaran keamanan informasi mahasiswa berada pada kategori sedang (66%). Mahasiswa memahami pentingnya keamanan informasi, tetapi praktik keamanan, terutama dalam pengelolaan *password* dan kewaspadaan terhadap phising, masih perlu ditingkatkan (Nurjanaha & Destyaa, 2022).

ISSN 3063-878X

Penelitian ini menggunakan pendekatan berbasis dimensi pengetahuan, sikap, dan perilaku yang dikembangkan oleh Kruger dan Kearney (2006). Penelitian ini bertujuan menganalisis tingkat kesadaran keamanan informasi pegawai dengan pendekatan Pengetahuan, Sikap, dan Perilaku (*Knowledge, Attitude, Behavior*). Dengan skala penelitian yang lebih luas dan variabel yang lebih beragam, hasil penelitian ini diharapkan dapat menghasilkan rekomendasi yang lebih akurat dalam meningkatkan tingkat kesadaran keamanan informasi pegawai di lingkungan pemerintah, khususnya Pemerintah Kabupaten Gunungkidul, serta mendukung kebijakan keamanan informasi yang lebih adaptif dan berkelanjutan.

METODE PENELITIAN

Penelitian ini menggunakan metode survei dengan instrumen kuesioner untuk menggali informasi terkait tingkat kesadaran keamanan informasi pegawai Pemerintah Kabupaten Gunungkidul. Kuesioner disebarkan kepada pegawai di 49 perangkat daerah/instansi. Pengumpulan data dilakukan dalam rentang waktu 15–24 Januari 2025, dengan jumlah responden akhir sebanyak 3.323 pegawai setelah dilakukan proses penyaringan data untuk menghilangkan pengisian ganda atau pengisian yang tidak valid.

Kuesioner terdiri atas 21 pertanyaan yang disusun berdasarkan tiga dimensi dan tujuh area pengukuran kesadaran keamanan informasi. Pembobotan masing-masing dimensi mengacu pada skala yang dikembangkan oleh Kruger dan Kearney (2006), tersaji pada tabel 1, sedangkan pembobotan masing-masing area dihitung dengan mempertimbangkan rekomendasi Badan Siber dan Sandi Negara (BSSN) melalui surat Nomor T.20/BSSN/D2/DT.01.01/1/2025 tertanggal 5 Januari 2025, tersaji pada Tabel 2.

Tabel 1. Pembobotan pada Dimensi

Dimensi	Bobot*
Pengetahuan (*Knowledge*)	30%
Sikap (*Attitude*)	20%
Perilaku (*Behavior*)	50%

Tabel 2. Pembobotan pada Area

Area	Bobot*
Selalu taat pada aturan perusahaan	20%
Menjaga kerahasiaan *password* dan *Personal Identity Number* (PIN)	25%
Menggunakan *e-mail* dan internet dengan bijaksana	15%
Berhati-hati dalam menggunakan perangkat seluler	10%
Melaporkan insiden keamanan informasi	15%
Menyadari konsekuensi dari setiap tindakan	10%
Selalu melakukan backup data	5%

Penelitian ini mengadopsi pendekatan konseptual yang dikembangkan oleh Kruger dan Kearney (2006) dalam mengukur kesadaran keamanan informasi. Pendekatan ini mengacu pada konsep dalam bidang psikologi yang menjelaskan bahwa kecenderungan individu dalam melakukan suatu tindakan yang menguntungkan atau merugikan berkaitan dengan tiga komponen utama, yaitu *affect, behavior*, dan *cognition*. Ketiga komponen ini kemudian diadaptasi ke dalam tiga dimensi kesadaran keamanan informasi.

ISSN 3063-878X

Kruger dan Kearney (2006) melakukan pengukuran terhadap tiga dimensi tersebut dalam enam area utama yang memiliki tingkat risiko kritis terhadap keamanan informasi, yaitu kepatuhan terhadap aturan perusahaan, penjagaan kerahasiaan kata sandi (*password*) dan *Personal Identity Number* (PIN), penggunaan *e-mail* dan internet secara bijaksana, kehati-hatian dalam menggunakan perangkat seluler, pelaporan insiden keamanan informasi, serta kesadaran terhadap konsekuensi dari setiap tindakan yang dilakukan. Dalam penelitian ini, pendekatan yang dikembangkan oleh Kruger dan Kearney (2006) dimodifikasi dengan menambahkan satu area tambahan, yaitu kebiasaan pencadangan (*backup*) data. Penambahan area ini disesuaikan dengan Indeks Keamanan Informasi (KAMI) versi 5.0 pada bagian Pengelolaan Aset Informasi, yang digunakan sebagai alat evaluasi tingkat kesiapan pengamanan informasi di instansi pemerintah (Badan Siber dan Sandi Negara, 2024a).

Data yang telah terkumpul, selanjutnya dianalisis menggunakan *Microsoft Excel* 2019 dan SPSS versi 26. Pengukuran tingkat kesadaran keamanan informasi dilakukan menggunakan skala Likert (1–4), dengan hasil yang dihitung berdasarkan nilai rata-rata (*mean*). Analisis dilakukan secara deskriptif dengan menghitung *mean* untuk mengukur kecenderungan umum tingkat kesadaran keamanan informasi pegawai, serta melakukan perbandingan *mean* berdasarkan karakteristik demografi responden (jenis kelamin, usia, pengalaman kerja, dan tingkat pendidikan), serta antar area kesadaran keamanan informasi.

Tingkat kesadaran keamanan informasi dikategorikan dalam tiga tingkatan, yaitu buruk, sedang, dan baik. Kriteria pembagian skala ini ditunjukkan pada Gambar 1 dan mengacu pada pendekatan yang digunakan oleh Kruger dan Kearney (2006).

0 – 59 %	Buruk	
60 – 79 %	Sedang	
80 – 100 %	Baik	

Gambar 1. Skala Tingkat Kesadaran Keamanan Informasi

Pengujian akurasi data menggunakan uji validitas dengan metode *Pearson Correlation* untuk memastikan bahwa setiap pertanyaan dalam kuesioner mengukur aspek yang dimaksud. Selain itu, dilakukan uji reliabilitas menggunakan *Cronbach's Alpha*.

HASIL PENELITIAN

Berdasarkan hasil uji validitas, diperoleh nilai korelasi (*pearson correlation*) positif, dan nilai probabilitas korelasi *sig.(2-tailed)* < 0,05 untuk seluruh item dalam kuesioner. Hal ini menunjukkan bahwa setiap item memenuhi kriteria validitas dan dapat digunakan dalam pengumpulan data. Menurut Ghozali (2021), uji validitas digunakan untuk mengukur sah atau valid tidaknya suatu kuesioner, dan reliabilitas adalah alat untuk mengukur konsistensi suatu kuesioner yang merupakan indikator dari variabel atau konstruk.

Tabel 3. Hasil uji reliabilitas

Reliability Statistics

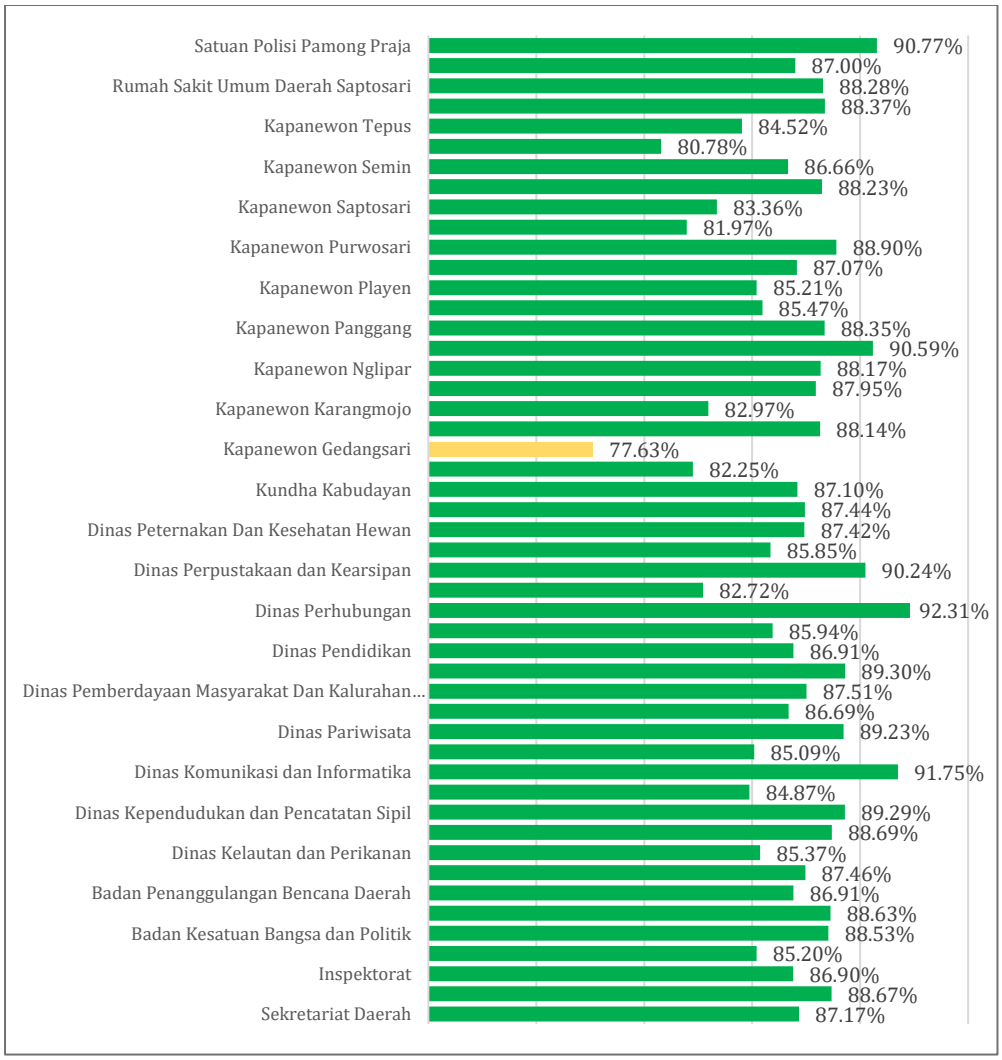
Cronbach's Alpha	*N of Items*
0,912	21

Sumber: Data diolah SPSS versi 26

JALIN RISTEK
Jurnal Ilmiah Inovasi Daerah Riset dan Teknologi
Vol. 2, Nomor 2, November 2025
ISSN 3063-878X

Selanjutnya, uji reliabilitas dilakukan menggunakan metode *Cronbach's Alpha* untuk menilai konsistensi internal antar pernyataan pada kuesioner. Hasil pengujian menunjukkan nilai *Cronbach's Alpha* sebesar 0,912, hasil ditunjukkan pada Tabel 3, yang dikategorikan reliabilitas tinggi. Menurut Ghozali (2021), instrumen penelitian dikatakan reliabel jika nilai *Cronbach's Alpha*-nya > 0,6. Nilai ini mengindikasikan bahwa instrumen memiliki keterkaitan antarpernyataan yang tinggi serta mampu mengukur konstruk penelitian secara konsisten.

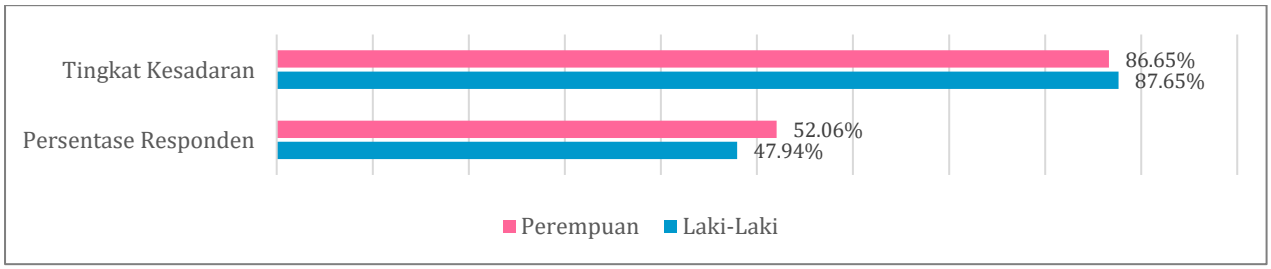
Berdasarkan hasil survei, nilai rata-rata tingkat kesadaran keamanan informasi pegawai Kabupaten Gunungkidul mencapai kategori baik, berada pada angka 87,13%. Beberapa perangkat daerah dengan nilai tingkat kesadaran keamanan informasi tertinggi diantaranya yaitu Dinas Perhubungan (92,31%) dan Dinas Komunikasi dan Informatika (91,75%). Sebaliknya, Kapanewon Gedangsari memiliki indeks terendah (77,63%), masuk dalam kategori sedang, seperti yang terlihat pada Gambar 2.



Gambar 2. Distribusi Berdasarkan Perangkat Daerah/Instansi

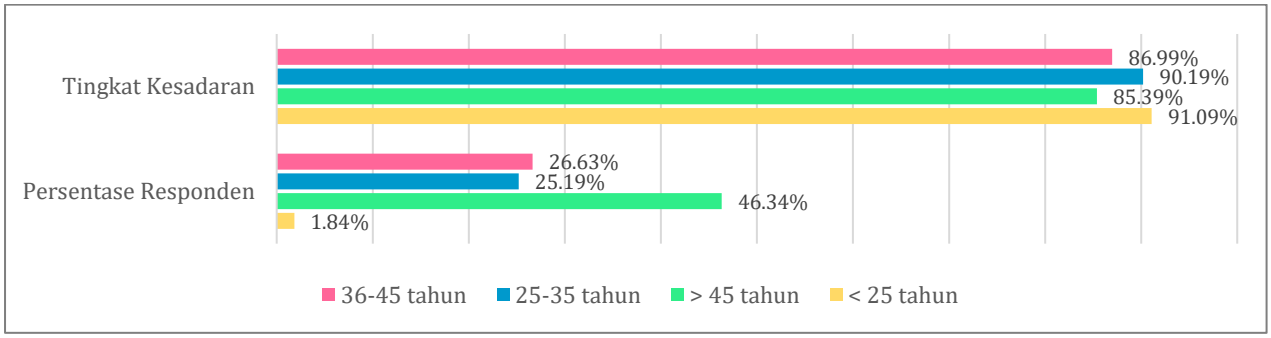
Hasil survei menunjukkan bahwa pegawai laki-laki memiliki tingkat kesadaran keamanan informasi yang sedikit lebih tinggi (87,65%) dibandingkan pegawai perempuan (86,65%). Perbedaan tingkat kesadaran keamanan informasi tersebut tidak terlalu signifikan dan masih dalam kategori baik seperti yang terlihat pada Gambar 3.

ISSN 3063-878X



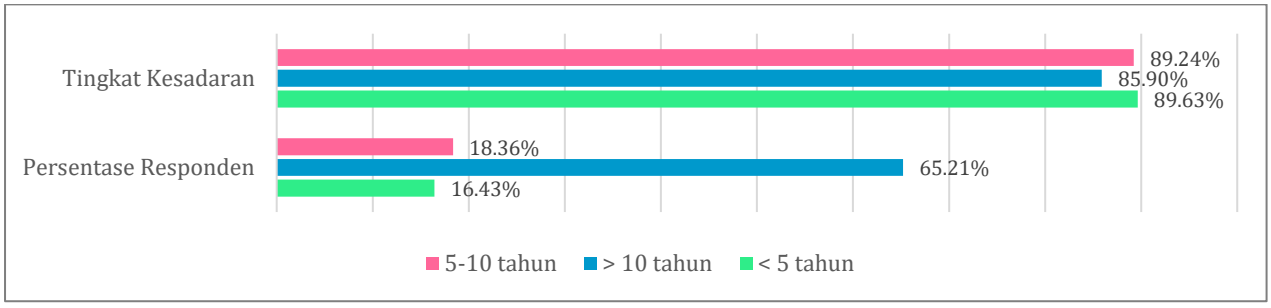
Gambar 3. Distribusi Berdasarkan Jenis Kelamin

Kelompok usia < 25 tahun memiliki tingkat kesadaran keamanan informasi tertinggi (91,09%). Sementara itu, kelompok usia > 45 tahun memiliki nilai terendah (85,39%). Hasil tersebut menunjukkan bahwa generasi muda cenderung lebih sadar akan keamanan informasi seperti yang terlihat pada Gambar 4.



Gambar 4. Distribusi Berdasarkan Usia

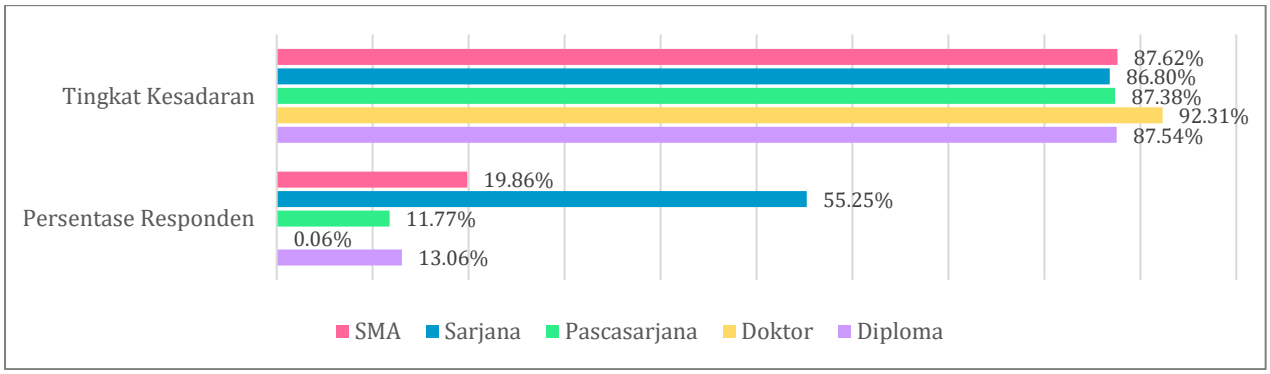
Pegawai dengan pengalaman kerja < 5 tahun memiliki tingkat kesadaran keamanan informasi tertinggi (89,63%) dibandingkan dengan pegawai yang memiliki pengalaman lebih dari 10 tahun memiliki tingkat kesadaran lebih rendah (85,90%) seperti yang terlihat pada Gambar 5.



Gambar 5. Distribusi Berdasarkan Pengalaman Kerja

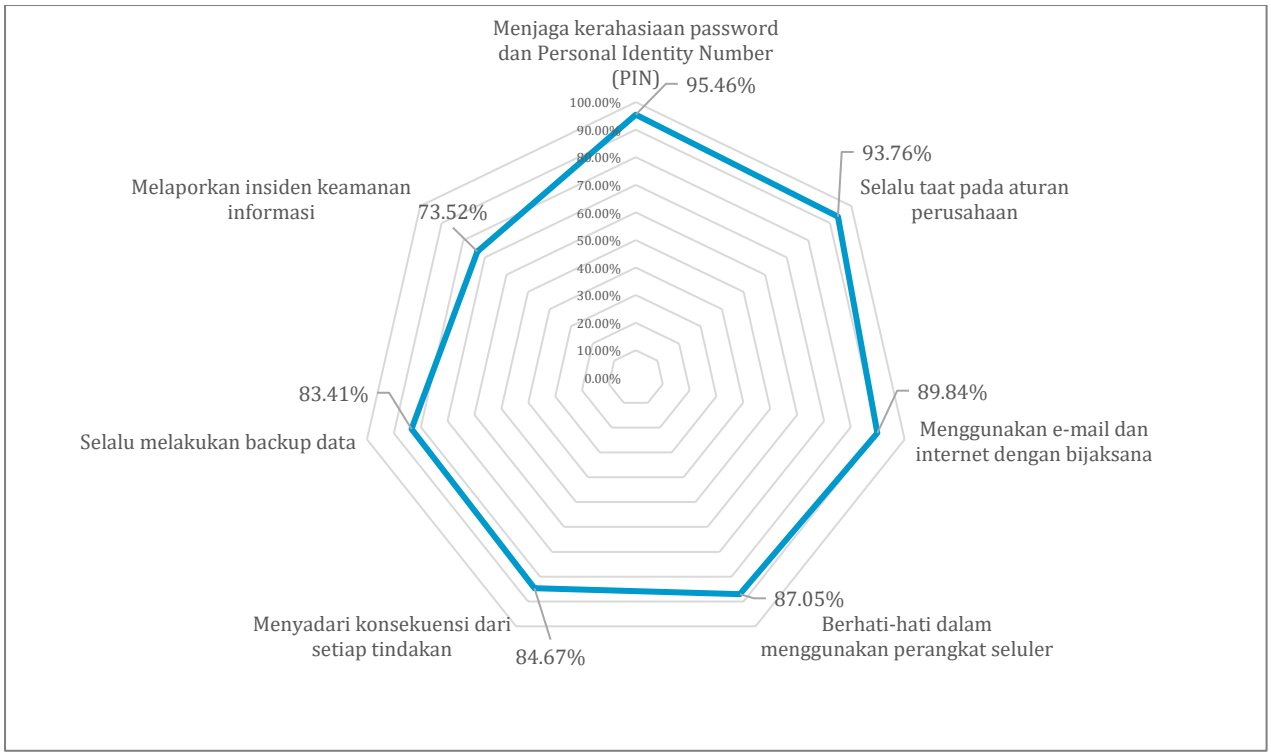
Pegawai dengan tingkat pendidikan Doktor memiliki tingkat kesadaran keamanan informasi tertinggi (92,31%), disusul oleh SMA (87,62%) dan Diploma (87,54%). Meskipun terdapat variasi tingkat kesadaran keamanan informasi berdasarkan tingkat pendidikan, seluruh kelompok masih masuk dalam kategori baik seperti yang terlihat pada Gambar 6.

ISSN 3063-878X



Gambar 6. Distribusi Berdasarkan Tingkat Pendidikan

Untuk memahami sejauh mana pegawai menyadari dan menerapkan prinsip-prinsip keamanan informasi, dilakukan pengukuran tingkat kesadaran pegawai dalam tujuh area pengukuran kesadaran keamanan informasi, dengan hasil ditunjukkan pada Gambar 7. Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan informasi tertinggi terdapat pada area menjaga kerahasiaan *password* dan PIN (95,46%) serta kepatuhan terhadap aturan yang ada pada perangkat daerah/instansinya (93,76%). Sebaliknya, pelaporan insiden keamanan informasi memiliki tingkat kesadaran terendah (73,52%). Selain itu, kebiasaan melakukan pencadangan data (83,41%) juga masih perlu ditingkatkan.



Gambar 7. Distribusi Berdasarkan Area

PEMBAHASAN

Hasil survei menunjukkan bahwa tingkat kesadaran keamanan informasi pegawai Pemerintah Kabupaten Gunungkidul berada pada kategori baik dengan nilai 87,13%. Temuan ini mengindikasikan bahwa secara umum, pegawai telah memiliki pemahaman dan penerapan yang cukup baik dalam keamanan informasi. Hal ini sejalan dengan teori Von

ISSN 3063-878X

Solms dan Van Niekerk (2013) bahwa peran manusia dalam keamanan informasi semakin menjadi bagian integral dari sistem pendukung keamanan.

Dari segi demografi pegawai, perbedaan kecil dalam tingkat kesadaran keamanan informasi antara pegawai laki-laki (87,65%) dan perempuan (86,65%) menunjukkan pemahaman yang relatif seimbang. Menurut Bello et al. (2021), terdapat risiko bahwa Revolusi Industri Keempat dapat melanggengkan ketidakseimbangan gender, karena perempuan masih menjadi minoritas dalam teknologi informasi digital, komputasi, fisika, matematika, dan teknik. Kelompok usia < 25 tahun memiliki tingkat kesadaran keamanan informasi tertinggi (91,09%), sementara kelompok usia > 45 tahun menunjukkan tingkat kesadaran keamanan informasi yang lebih rendah (85,39%). Hasil ini sejalan dengan penelitian Alhazmi dan Abu Alsheikh (2022) yang menunjukkan bahwa pengguna muda secara umum lebih peduli terhadap privasi digital dibandingkan dengan kelompok usia yang lebih tua. Hal ini mengindikasikan bahwa kelompok usia yang lebih muda memiliki tingkat adaptasi yang lebih tinggi terhadap kebijakan digital dibandingkan kelompok usia yang lebih tua.

Pegawai dengan pengalaman kerja < 5 tahun memiliki tingkat kesadaran keamanan informasi lebih tinggi (89,63%) dibandingkan pegawai dengan pengalaman kerja > 10 tahun (85,90%), hal ini sejalan dengan temuan pada kelompok usia, di mana pegawai yang lebih muda atau dengan pengalaman kerja lebih sedikit cenderung lebih peka terhadap praktik keamanan informasi. Hasil ini bertolak belakang dengan studi yang dilaksanakan di PT Meshindo Jayatama yang menemukan bahwa pegawai dengan pengalaman lebih lama lebih waspada terhadap ancaman siber (Gofur & Kurniawan, 2024). Pada kelompok pendidikan, pegawai berpendidikan Doktor memiliki kesadaran tertinggi (92,31%), disusul oleh SMA (87,62%) dan Diploma (87,54%). Meskipun terdapat variasi berdasarkan tingkat pendidikan, seluruh kelompok masih masuk dalam kategori baik, yang menunjukkan bahwa kesadaran keamanan informasi tidak hanya bergantung pada tingkat pendidikan formal tetapi juga pada pelatihan dan sosialisasi ataupun pelatihan yang diterima pegawai.

Area spesifik yang menunjukkan tingkat kesadaran keamanan informasi kesadaran tertinggi adalah menjaga kerahasiaan *password* dan PIN (95,46%) serta kepatuhan terhadap aturan keamanan informasi (93,76%), mencerminkan pemahaman yang baik terhadap perlindungan informasi pribadi dan kebijakan organisasi. Namun, pelaporan insiden keamanan informasi masih rendah (73,52%), yang menunjukkan perlunya peningkatan pemahaman dan kepatuhan dalam melaporkan insiden. Selain itu, kebiasaan melakukan pencadangan data (83,41%) juga masih perlu ditingkatkan guna mengurangi risiko kehilangan data. Hal ini sejalan dengan rekomendasi bahwa organisasi yang bertanggung jawab atas implementasi teknologi harus membuat, memelihara, dan menguji cadangan secara berkala, baik untuk sistem teknologi informasi maupun operasional manual pada jaringan yang terintegrasi (CISA, 2023). Dengan demikian, pencadangan terencana berperan penting dalam meningkatkan ketahanan sistem terhadap gangguan

KESIMPULAN DAN SARAN

Hasil penelitian menunjukkan bahwa tingkat kesadaran keamanan informasi pegawai Pemerintah Kabupaten Gunungkidul berada dalam kategori baik. Hal ini mencerminkan pemahaman dan penerapan yang cukup baik terhadap prinsip-prinsip keamanan informasi. Namun, terdapat variasi tingkat kesadaran keamanan informasi berdasarkan karakteristik demografi pegawai, di mana pegawai berusia lebih muda dan dengan pengalaman kerja lebih singkat cenderung memiliki tingkat kesadaran keamanan informasi yang lebih tinggi dibandingkan dengan kelompok usia yang lebih tua dan pegawai dengan pengalaman kerja

ISSN 3063-878X

lebih lama. Selain itu, kesadaran dalam menjaga kerahasiaan *password* dan kepatuhan terhadap kebijakan keamanan informasi memperoleh nilai tertinggi, sedangkan pelaporan insiden keamanan informasi dan pencadangan data masih menjadi area yang perlu ditingkatkan.

Berdasarkan temuan ini, terdapat beberapa saran bagi Pemerintah Kabupaten Gunungkidul dalam pengambilan kebijakan keamanan informasi. Pertama, peningkatan sosialisasi dan pelatihan keamanan informasi yang lebih terstruktur dan berkelanjutan, terutama bagi pegawai dengan pengalaman kerja lebih lama dan kelompok usia yang lebih tua. Kedua, memperkuat mekanisme pelaporan insiden keamanan informasi dengan membangun sistem yang lebih mudah diakses serta memastikan adanya umpan balik yang cepat dan efektif bagi pelapor. Ketiga, mendorong kebiasaan pencadangan data secara berkala melalui kebijakan internal dan penyediaan fasilitas teknologi yang mendukung. Keempat, menanamkan budaya kesadaran keamanan informasi di seluruh perangkat daerah dengan mengintegrasikan aspek kesadaran keamanan informasi dalam evaluasi kinerja pegawai.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada Sekretaris Daerah dan Kepala Dinas Komunikasi dan Informatika Kabupaten Gunungkidul yang telah memberikan dukungan penuh dalam pelaksanaan survei serta pemanfaatan data hasil survei untuk kepentingan penelitian ini. Ucapan terima kasih juga disampaikan kepada seluruh pegawai di lingkungan Pemerintah Kabupaten Gunungkidul yang telah berkenan menjadi responden dalam penelitian ini. Partisipasi dan kontribusi yang diberikan sangat berarti dalam memperoleh data yang valid dan relevan guna menganalisis tingkat kesadaran keamanan informasi pegawai di lingkungan Pemerintah Kabupaten Gunungkidul.

DAFTAR PUSTAKA

Alhazmi, H., Imran, A. and Abu Alsheikh, M., 2022. *How do socio-demographic patterns define digital privacy divide?*. *IEEE Access*, 10, pp.11296-11307.

APJII (Asosiasi Penyelenggara Jasa Internet Indonesia). 2024. *Survei Penetrasi Internet Indonesia 2024*. APJII. Jakarta.

Bello, A., Blowers, T., Schneegans, S., & Straza, T. (2021). *To be smart, the digital revolution will need to be inclusive*. *In UNESCO Science Report: The race against time for smarter development*. UNESCO Publishing

BSSN (Badan Siber dan Sandi Negara). 2024a. Indeks Keamanan Informasi (KAMI) Versi 5.0. https://www.bssn.go.id/indeks-kami. 1 Februari 2025 (09.30)

_____ 2024b. *Laporan Evaluasi Pelaksanaan Persandian untuk Pengamanan Informasi Pemerintah Daerah Kabupaten Gunungkidul*. BSSN. Jakarta.

_____ 2025. *Penyampaian Notifikasi Indikasi Dugaan Insiden Kebocoran Data Milik Pemerintah Kabupaten Gunungkidul*. BSSN. Jakarta.

CISA (Cybersecurity and Infrastructure Security Agency). 2023. *911 Cybersecurity Best Practices Package*. CISA

Dewi, K. M. R., Yudistira, R. D., & Ruldeviyani, Y. 2024. *Pengukuran tingkat kesadaran keamanan informasi pegawai pada instansi pemerintah. Indonesian Journal of Computer Science*, 13(2), 3274-3276.

Ghozali, I. 2021. *Aplikasi Analisis Multivariate Dengan Program IBM SPSS 26 Edisi 1*0. Badan Penerbit Universitas Diponegoro.

ISSN 3063-878X

Gofur, A., Aji, R. F., & Kurniawan, H. 2024. *Pengukuran kesadaran keamanan informasi pegawai: Studi kasus PT Meshindo Jayatama*. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 11(2), 315-320.

Kementerian Komunikasi dan Informatika. 2024a. *Satu Dekade Pembangunan Digital Indonesia 2014 – 2024*. Kementerian Komunikasi dan Informatika. Jakarta.

_____ 2024b. *Laporan Hasil Evaluasi Tahap II Implementasi Kota Cerdas (Smart City) Tahun 2024 Kab. Gunungkidul*. Kementerian Komunikasi dan Informatika. Jakarta.

Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. 2024. *Laporan Hasil Evaluasi SPBE 2024: Pemerintah Kab. Gunungkidul*. Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. Jakarta.

Kruger, H. A., & Kearney, W. D. 2006. *A prototype for assessing information security awareness. Computers & Security*, 25(4), 289–29

Nurjanah, D., & Destyaa, S. 2022. *Pengukuran tingkat kesadaran keamanan informasi mahasiswa pada pembelajaran online*. *Jurnal Sistem dan Teknologi Informasi*, 10(1), 81-83

Selvam, V.S.D. 2020. *Human Error in IT Security*. Edith Cowan University - PSB Academy. Singapore

Von Solms, R., & Van Niekerk, J. 2013. *From information security to cyber security. Computers & Security*, 3(1), 1-6

Whitman, M. E., & Mattord, H. J. 2018. *Principles of Information Security.* 6th edn. Cengage Learning. Boston.