202210050311086
Fila Dwi Agustin
Prodi Ilmu Pemerintahan

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi (TIK) di era digital saat ini sangat membuat perubahan besar dalam kehidupan, termasuk dalam pengelolaan pemerintahan (Gita Segara & Irwan Padli Nasution, 2025). Dengan adanya teknologi digital, instansi pemerintah dapat meningkatkan efisiensi operasional, mempercepat proses pelayanan kepada publik, serta memperluas akses komunikasi dengan masyarakat (Wiryany et al., 2022). Namun, selain peluang yang ada, kemajuan TIK juga menghadirkan tantangan serius berupa ancaman keamanan dunia maya yang semakin beragam, kompleks, dan sulit untuk diprediksi. Berbagai bentuk serangan siber seperti pencurian data serta penyalahgunaan media sosial sering kali menyebabkan kerugian baik secara materi maupun non-materi termasuk menurunkannya kepercayaan masyarakat terhadap pemerintah sebagai pengelola informasi (Amrina & Primandhana, 2022).

Dalam beberapa tahun terakhir, kebocoran data menjadi masalah serius yang mengancam keamanan informasi di berbagai instansi, termasuk lembaga pemerintah. Pada 20 Juni 2024 Pusat Data Nasional (PDN) mengalami serangan siber yang menyebabkan data nasional terkunci, serangan ini berdampak pada ratusan instansi pemerintah, memicu kekhawatiran publik terkait keamanan data pribadi, dan menyoroti efektivitas kebijakan keamanan siber nasional (Imanuel Toding Bua & Nur Isdah Idris, 2025). Kasus bocornya data pribadi masyarakat dan informasi instansi salah satunya terjadi karena adanya kelemahan dalam penerapan budaya keamanan siber dalam lingkungan kerja (Hisbulloh, 2021). Permasalahan ini juga terjadi karena rendahnya kesadaran dan kepatuhan pegawai terhadap kebijakan keamanan informasi yang berlaku. Kurangnya pemahaman tentang ancaman siber, penggunaan kata sandi yang mudah ditebak, serta kelalaian dalam

pengelolaan data rahasia menjadi penyebab utama insiden keamanan tersebut (Putri Nugroho et al., 2024).

Untuk mengatasi masalah kebocoran data tersebut, diperlukan pendekatan yang menyeluruh. Salah satu solusi yang dapat diterapkan adalah Salah satu upaya yang dilakukan Komdigi untuk meningkatkan pemahaman pegawai mengenai keamanan siber adalah melalui penyelenggaraan Program Security Awareness. Program ini merupakan kegiatan edukasi yang bertujuan untuk meningkatkan kesadaran dan pengetahuan pegawai mengenai berbagai ancaman keamanan siber, pentingnya perlindungan informasi, serta langkah-langkah yang harus dilakukan untuk mencegah terjadinya insiden keamanan siber. (Misni et al., 2025).

Program Security Awareness di lingkungan Komdigi dilaksanakan dalam bentuk workshop secara daring yang memungkinkan pegawai mengikuti kegiatan edukasi tanpa terbatas oleh lokasi kerja. Melalui workshop daring tersebut, pegawai memperoleh materi mengenai ancaman siber terkini, keamanan informasi, perlindungan data, pengelolaan kata sandi yang aman, pengenalan serangan phishing, serta prosedur pelaporan insiden keamanan siber. Pelaksanaan workshop secara daring juga menjadi alternatif yang efektif untuk menjangkau peserta dalam jumlah besar serta mendukung pelaksanaan pembelajaran yang fleksibel (Febrian Aska et al., 2024).

Berbagai penelitian sebelumnya menunjukkan bahwa program security awareness berperan penting dalam meningkatkan kesadaran dan perilaku aman saat menggunakan sistem informasi. Contohnya, studi dari Botagoz Khamzina dan rekan-rekannya (2020) membuktikan bahwa pelatihan daring dapat meningkatkan pemahaman mahasiswa mengenai ancaman siber serta langkah-langkah pencegahannya (Khamzina et al., 2022). Sejalan dengan hal tersebut, penelitian oleh Tiago Espinha Gasiba dan tim (2020) mengembangkan platform pembelajaran berbasis permainan (Sifu) yang efektif dalam meningkatkan keterampilan praktis peserta untuk menghadapi tantangan keamanan siber (Espinha Gasiba et al., 2020). Penelitian-penelitian ini menegaskan bahwa peningkatan literasi dan

keterampilan melalui program security awareness merupakan dasar utama dalam membangun budaya keamanan siber.

Pengetahuan keamanan siber menjadi faktor yang sangat penting bagi pegawai karena berkaitan langsung dengan kemampuan individu dalam menjaga keamanan informasi organisasi. Pegawai yang memiliki tingkat pengetahuan keamanan siber yang tinggi cenderung lebih mampu mengidentifikasi potensi ancaman, menghindari tindakan yang berisiko, dan mendukung terciptanya budaya keamanan informasi di lingkungan kerja. Sebaliknya, rendahnya pengetahuan keamanan siber dapat meningkatkan kerentanan organisasi terhadap berbagai bentuk serangan siber yang memanfaatkan kesalahan manusia.(Nandang Firmansyah et al., 2023).

Sejalan dengan upaya memperkuat pertahanan siber nasional, pemerintah telah mengeluarkan Peraturan Preiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber. Salah satu point utama dalam peraturan ini adalah kewajiban untuk meningkatkan kesadaran serta pelatihan keamanan siber (security awareness training) secara berkelanjutan dan terkoordinasi di seluruh instansi pemerintah serta sektor strategis lainnya. Perpres tersebut menegaskan bahwa peningkatan kesadaran dan kemampuan sumber daya manusia merupakan kunci untuk menciptakan ruang siber yang aman, selain penguatan aspek teknologi dan kebijakan. Oleh karena itu, pelaksanaan program security awareness di lingkungan Kementerian Komunikasi dan Digital Republik Indonesia tidak hanya menjadi kebutuhan internal, tetapi juga merupakan bentuk kepatuhan terhadap kebijakan strategis nasional.

Berdasarkan latar belakang tersebut, peneliti memutuskan untuk menentukan judul skripsi yaitu “Pengaruh Program Security Awareness terhadap Pengetahuan Keamanan Siber Pegawai Komdigi” dengan studi kasus pegawai Kementerian Komunikasi dan Digital Republik Indonesia.

1.2 Rumusan Masalah

Melihat dari latar belakang yang ada maka peneliti mengambil tiga rumusan masalah untuk penelitian ini yaitu :

1. Bagaimana tingkat pengetahuan keamanan siber pegawai Komdigi?

2. Seberapa besar pengaruh Program Security Awareness terhadap pengetahuan keamanan siber pegawai Komdigi?

1.3 Tujuan Penelitian

Tujuan dari penelitian ini yaitu :

1. Untuk mengetahui tingkat pengetahuan keamanan siber pegawai Komdigi.
2. Menganalisis besarnya pengaruh Program Security Awareness terhadap pengetahuan keamanan siber pegawai Komdigi.

1.4 Manfaat Penelitian

1.4.1 Manfaat Akademis

a. Menambah pengetahuan dan wawasan bagi peneliti maupun pembaca mengenai Keamanan Siber yang dilakukan oleh Kementrian Komunikasi dan Digital Republik Indonesia
b. Menjadi referensi dan bahan kajian ilmiah bagi pihak universitas dalam pengembangan penelitian serta pembelajaran di bidang keamanan informasi dan transformasi digital pemerintahan.

1.4.2 Manfaat Praktis

a. Hasil Penelitian ini diharapkan dapat menjadi bahan masukan bagi pemerintah dalam menyusun kebijakan atau memperbaiki sistem keamanan informasi
b. Hasil Penelitian ini diharapkan memberikan pemahaman yang mendalam terkait implementasi keamanan informasi di Kementrian Komunikasi dan Digital Republik Indonesia, dan dapat dijadikan referensi atau studi kasus dalam penelitian.
c. Penelitian ini diharapkan dapat meningkatkan pemahaman masyrakat luas mengenai pentingnya melindungi data pribadi dan informasi digital mereka, sehingga risiko menjadi korban kejahatan siber seperti pencurian identitas, penipuan online, atau peretasan akun media sosial dapat berkurang.

1.5 Definisi Konseptual

Menurut Najwa et dkk (2021) Definisi konseptual bertujuan untuk menjelaskan secara teoritis objek atau fenomena yang diteliti berdasarkan literatur dan sumber referensi yang relevan. Selain itu, definisi konseptual juga menjadi dasar untuk merumuskan definisi operasional, yang menyesuaikan dengan konteks penelitian spesifik yang dilakukan. Definisi operasional merupakan pendefinisian yang dilakukan oleh peneliti berdasarkan definisi konseptual tersebut dan kondisi nyata di lapangan agar fokus penelitian dapat diukur dan dianalisis secara sistematis. Dengan landasan konseptual yang jelas, penelitian dapat tersusun secara sistematis dan valid.

1.5.1 Program Security Awareness

Menurut penelitian Bader Alkhazi dkk. (2022) program security awareness merupakan komponen penting dalam strategi keamanan organisasi yang bertujuan untuk meningkatkan pengetahuan, sikap, dan perilaku karyawan terhadap keamanan informasi (Alkhazi et al., 2022). Dalam penelitian tersebut menekankan bahwa upaya menjaga keamanan tidak hanya ditentukan oleh teknologi, tetapi juga sangat bergantung pada peran manusia dan proses. Oleh karena itu, pelatihan security awareness menjadi salah satu langkah paling efektif dalam mencegah serangan siber yang disebabkan oleh kelalaian atau ketidaktahuan pengguna.

Program security awareness dirancang untuk tidak hanya meningkatkan pengetahuan teknis, tetapi juga membentuk kebiasaan dan perilaku aman dalam aktivitas sehari-hari di lingkungan kerja (Alkhazi et al., 2022). Dalam penelitian David Sikolia dkk (2023) program security awareness jelaskan sebagai inisiatif organisasi yang dirancang untuk meningkatkan pemahaman dan kesadaran karyawan terhadap ancaman keamanan siber serta mengurangi kesalahan manusia yang sering menjadi penyebab utama pelanggaran keamanan informasi. Program ini berperan penting dalam membekali pegawai dengan pengetahuan dasar mengenai keamanan siber (Sikolia et al., 2023). Pada penelitian Jody L. Jacobs dkk (2023) tujuan utama dari program security

awareness adalah membantu pegawai mengenali serta merespons isu-isu keamanan dengan tepat, sehingga dapat memperkuat postur keamanan organisasi secara keseluruhan (Jacobs et al., 2023).

1.5.2 Pengetahuan Keamanan Siber

Pengetahuan keamanan siber adalah tingkat pemahaman yang dimiliki seseorang mengenai berbagai konsep, prinsip, ancaman, risiko, kebijakan, serta praktik keamanan siber yang bertujuan untuk melindungi informasi, data, perangkat, jaringan, dan sistem informasi dari akses yang tidak sah, penyalahgunaan, kerusakan, maupun gangguan yang dapat mengancam keamanan organisasi. (Fahrizal Wahyudi et al, 2025). Dalam konteks pegawai Komdigi, pengetahuan keamanan siber tidak hanya mencakup pemahaman teoritis, tetapi juga kemampuan untuk mengenali, menghindari, dan merespons berbagai ancaman siber yang mungkin terjadi dalam pelaksanaan tugas sehari-hari. Semakin tinggi tingkat pengetahuan keamanan siber yang dimiliki pegawai, semakin besar kemampuannya dalam menerapkan praktik keamanan yang tepat dan meminimalkan risiko terjadinya insiden keamanan informasi (Fahrizal Wahyudi et al, 2025).

Pengetahuan keamanan siber merupakan tingkat pemahaman pegawai mengenai konsep, ancaman, risiko, kebijakan, dan praktik keamanan siber yang diperlukan untuk melindungi informasi dan sistem organisasi dari berbagai ancaman digital. Pengetahuan ini mencakup kemampuan pegawai dalam memahami jenis-jenis ancaman siber, menerapkan langkah-langkah perlindungan data dan akun, mematuhi kebijakan keamanan informasi, menggunakan perangkat dan jaringan secara aman, serta mengenali dan melaporkan insiden keamanan siber yang terjadi di lingkungan kerja. Pengetahuan keamanan siber menjadi faktor penting dalam mendukung terciptanya perilaku kerja yang aman dan memperkuat ketahanan keamanan informasi organisasi.

1.6 Definisi Operasional

Definisi operasional merupakan penjabaran dari variabel penelitian ke dalam dimensi dan indikator yang dapat diamati serta diukur. Definisi operasional digunakan untuk memberikan batasan yang jelas mengenai variabel yang diteliti sehingga memudahkan peneliti dalam menyusun instrumen penelitian dan melakukan pengukuran. Dalam penelitian ini terdapat dua variabel, yaitu Program Security Awareness sebagai variabel independen (X) dan Pengetahuan Keamanan Siber sebagai variabel dependen (Y) :

a. Program Security Awareness

Program Security Awareness merupakan serangkaian kegiatan edukasi, sosialisasi, dan pelatihan keamanan siber yang dilaksanakan oleh Kementerian Komunikasi dan Digital guna meningkatkan pemahaman pegawai mengenai keamanan informasi. Variabel ini diukur menggunakan teori implementasi kebijakan George C. Edward III yang terdiri atas empat dimensi sebagai berikut:

1. Komunikasi Program Security Awareness
    a. Sosialisasi program security awareness kepada pegawai
    b. Kejelasan tujuan program security awareness yang disampaikan oleh penyelenggara
    c. Konsistensi penyampaian informasi terkait keamanan siber kepada pegawai
    d. Kejelasan materi dan arahan yang diberikan selama kegiatan Security Awareness.
2. Sumber Daya
    a. Ketersediaan narasumber atau fasilitator yang kompeten dalam bidang keamanan siber.
    b. Ketersediaan fasilitas pelatihan bagi pegawai Komdigi
    c. Ketersediaan materi pelatihan yang sesuai dengan kebutuhan pegawai.
    d. Dukungan anggaran dan fasilitas dari instansi terhadap pelaksanaan program.
3. Disposisi
    a. Kesediaan pegawai Komdigi mengikuti kegiatan Security Awareness.
    b. Keseriusan pegawai dalam mengikuti seluruh rangkaian kegiatan

c. Komitmen pegawai untuk menerapkan hasil pelatihan dalam pekerjaan sehari-hari.
d. Dukungan pimpinan terhadap pelaksanaan Program Security Awareness.

4. Struktur Birokrasi
   a. Kejelasan SOP pelaksanaan Program Security Awareness di lingkungan Komdigi
   b. Koordinasi antarunit dalam pelaksanaan program Security Awareness.
   c. Keteraturan alur pelaksanaan kegiatan dari undangan hingga evaluasi
   d. Adanya mekanisme evaluasi terhadap pegawai peserta program.

b. Pengetahuan Keamanan Siber

Pengetahuan keamanan siber pegawai merupakan tingkat pemahaman pegawai mengenai ancaman siber, perlindungan data dan informasi, penggunaan sistem secara aman, serta penanganan insiden keamanan siber di lingkungan Kementerian Komunikasi dan Digital.

1. Pengetahuan tentang ancaman siber pada instansi pemerintah
2. Pengetahuan tentang perlindungan informasi dan data pemerintah
3. Pengetahuan tentang penggunaan sistem dan media digital pemerintah yang aman
4. Pengetahuan tentang penanganan dan pelaporan insiden siber

1.7 Metode Penelitian

1.7.1 Jenis Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan metode survei. Metode survei merupakan salah satu pendekatan penelitian yang memanfaatkan angket atau kuesioner sebagai alat utama dalam pengumpulan data lapangan dalam penelitian Syahrizal dkk (2023) Pendekatan ini bertujuan untuk memperoleh data yang bersifat empiris, objektif, dan terukur sehingga mampu menjelaskan hubungan antarvariabel yang diteliti secara sistematis. Metode ini bertujuan untuk mengumpulkan data bersifat empiris, onjektif, dan terukur agar hasilnya dapat menjelaskan hubungan antara variabel yang diteliti. Penelitian kuantitatif dengan metode survei dipilih karena sesuai dengan tujuan

penelitian yaitu untuk mengetahui pengaruh program security awareness dan kebijakan keamanan informasi terhadap budaya keamanan siber pada pegawai Kementerian Komunikasi dan Digital. Dengan metode ini, peneliti dapat mengukur secara statistik tingkat persepsi, sikap dan perilaku responden berdasarkan indikator yang tercantum.

1.7.2 Lokasi Penelitian

Berdasarkan judul penelitian yang diajukan, lokasi penelitian ditetapkan di Kementerian Komunikasi dan Digital Republik Indonesia yang dilakukan pada saat Magang MBKM dari tanggal 06 Agustus – 06 Desember 2025. Tujuannya untuk mendapatkan data yang berkaitan dengan pengaruh program security awareness dan kebijakan keamanan informasi terhadap budaya keamanan siber, sehingga dari hasil yang diperoleh akan membantu peneliti dalam menyusun uraian dan penjelasan secara sistematis dalam penulisan laporan penelitian yang telah dilakukan.

1.7.3 Variabel dan Definisi Operasional Pengukuran

1.7.3.1 Variabel

Menurut Sugiyono (2019:38) dalam penelitian tia setiani dkk (2022), Variabel penelitian dapat dipahami sebagai karakteristik, atribut, atau nilai yang melekat pada individu, objek, organisasi, maupun aktivitas tertentu yang memiliki variasi dan dipilih oleh peneliti untuk dianalisis sehingga dapat ditarik suatu kesimpulan. Dalam penelitian ini digunakan dua jenis variabel, yaitu variabel bebas dan variabel terikat yang dilambangkan dengan X dan Y. Variabel X terdiri atas X1 yang merepresentasikan program *security awareness* dan X2 yang menunjukkan kebijakan keamanan informasi, sedangkan variabel Y merujuk pada budaya keamanan siber.

a. Variabel bebas (*independent variable*) merupakan variabel yang berdiri sendiri dan tidak dipengaruhi oleh variabel lain. Dalam penelitian ini, variabel yang termasuk ke dalam variabel bebas adalah Program *Security Awareness*

b. Variabel terikat (*Dependent Variable*), yaitu suatu variabel yang memiliki ketergantungan dengan variabel yang satu dengan yang lain, sedangkan dalam penelitian ini variabel terikatnya adalah Pengetahuan Keamanan Siber (X)

Tabel 1.1 Definisi Opersional dan Pengukuran

Variabel	Definisi Operasional	Indikator	Pengukuran
Program *Security Awarenesss* (X)	Serangkaian kegiatan edukasi, sosialisasi, pelatihan, dan kampanye yang diselenggarakan oleh organisasi untuk meningkatkan kesadaran serta pemahaman pegawai mengenai keamanan siber dan keamanan informasi.	1. Komunikasi 2. Sumber Daya 3. Disposisi 4. Struktur Birokrasi	Skala Likert 1-5
Pengetahuan Keamanan Siber (Y)	Tingkat pemahaman pegawai mengenai ancaman siber, perlindungan data, kebijakan	1. Pengetahuan tentang ancaman siber pada instansi pemerintah 2. Pengetahuan tentang	Skala Likert 1-5

Variabel	Definisi Operasional	Indikator	Pengukuran
	keamanan informasi, penggunaan perangkat yang aman, serta penanganan insiden keamanan siber di lingkungan kerja.	perlindungan informasi dan data pemerintah 3. Pengetahuan tentang penggunaan sistem dan media digital pemerintah yang aman 4. Pengetahuan tentang penanganan dan pelaporan insiden siber	

Sumber: Data di Olah dari Hasil Wawancara Oleh Peneliti

1.7.4 Populasi dan Sampel penelitian

a. Populasi Penelitian

Populasi merupakan keseluruhan elemen, baik subjek maupun objek, yang menjadi fokus dalam suatu penelitian. Populasi juga kerap disebut sebagai *universe*, yaitu kumpulan individu, benda, atau fenomena yang memiliki karakteristik tertentu untuk diteliti. Anggota populasi dapat berupa makhluk hidup maupun benda mati, selama karakteristik yang dimilikinya dapat diukur, diamati, dan dianalisis sesuai dengan tujuan penelitian. Adapun populasi yang digunakan dalam penelitian ini adalah seluruh pegawai Kementerian Komunikasi dan Digital Republik Indonesia.

b. Sampel Penelitian

Setelah populasi penelitian ditetapkan, tahap selanjutnya adalah menentukan sampel yang dapat mewakili populasi tersebu. Menurut Penelitian Mushofa dkk (2024) sampel merupakan bagian dari populasi yang secara sengaja dipilih oleh peneliti untuk diamati, dengan ukuran yang lebih kecil dibandingkan populasi, namun tetap berfungsi sebagai representasi dari populasi secara keseluruhan. Dalam penelitian ini, teknik pengambilan sampel yang digunakan adalah *purposive sampling*. Sugiyono (2019:133) menyatakan bahwa *purposive sampling* merupakan teknik penentuan sampel berdasarkan pertimbangan tertentu. Pemilihan teknik ini didasarkan pada kesesuaiannya untuk penelitian kuantitatif atau penelitian yang tidak berorientasi pada generalisasi (Sugiyono, 2016:85). Adapun sampel dalam penelitian ini adalah pegawai Kementerian Komunikasi dan Digital Republik Indonesia yang mengikuti kegiatan *security awareness*. Karena jumlah populasi diketahui secara pasti, penentuan jumlah sampel dilakukan dengan menggunakan rumus Slovin:

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

Keterangan:

n : Jumlah Sampel

N: Ukuran Populasi

e : Persentase toleransi terhadap ketidaktepatan akibat kesalahan dalam pengambilan sampel, yang masih dapat diterima atau diharapkan, ditentukan oleh *margin of error* maksimal sebesar 10%. Maka, jumlah sampel minimum yang diperlukan untuk mencapai tingkat penelitian yang diinginkan adalah:

$$n = \frac{134}{1 + 134\ (0{,}1)^2}$$

n = 100,37 atau dibulatkan menjadi 100.

Jadi sampel yang digunakan dalam penelitin ini adalah sebanyak 100 pegawai yang mengikuti kegiatan security awarenes.

1.7.5 Sumber Data

Sumber data yang digunakan dalam penelitian ini adalah data primer dan data sekunder.

a. Data Primer

Muhammad Irfan (2022) menjelaskan bahwa data primer merupakan data yang diperoleh secara langsung dari sumber utamanya. Sejalan dengan hal tersebut, Nazir dalam buku *Analisis Data Penelitian* (2019) menyatakan bahwa data primer adalah data yang dikumpulkan langsung dari lapangan atau objek penelitian melalui teknik seperti pengukuran, observasi, maupun wawancara. Dalam penelitian ini, data primer diperoleh dari hasil pengisian kuesioner yang disampaikan secara tidak langsung melalui portal Kementerian Komunikasi dan Digital kepada para responden.

b. Data Sekunder

Muhammad Irfan (2022) menyatakan bahwa data sekunder merupakan data yang telah tersedia dan berasal dari hasil penelitian terdahulu. Dalam penelitian ini, data sekunder yang digunakan diperoleh dari berbagai sumber yang relevan, seperti buku, jurnal ilmiah, artikel, serta sumber lain yang sejenis.

1.7.6 Teknik Pengumpulan Data

Metode pengumpulan data yang diterapkan dalam penelitian ini adalah kuesioner. Kuesioner atau angket merupakan teknik pengumpulan data yang dilakukan dengan menyampaikan sejumlah pertanyaan atau pernyataan tertulis kepada responden untuk dijawab. Penggunaan metode kuesioner dalam penelitian ini bertujuan untuk mengidentifikasi pengaruh program *security awareness* dan kebijakan keamanan informasi terhadap budaya keamanan siber. Kuesioner yang digunakan

disusun dalam bentuk angket dengan skala Likert, di mana data yang diperoleh bersumber dari pendapat dan tanggapan responden.

1.7.7 Teknik Analisis Data

1.7.7.1 Pengolahan Data

Pengolahan data akan dilakukan dengan tahapan sebagai berikut:

a. Mengelola data hasil kuesioner mencakup proses pencatatan, pengumpulan, serta pengelompokan data yang diperoleh dari responden.
b. Pemberian bobot terhadap setiap jawaban responden dilakukan dengan menggunakan skala Likert, yaitu skala ordinal yang berfungsi untuk mengukur sikap atau persepsi individu terhadap suatu objek tertentu. Dalam penelitian ini, responden diberikan lima alternatif pilihan jawaban yang digunakan sebagai dasar penilaian, yaitu sebagai berikut:

Tabel 1.2 Kriteria Pemberian Skor

Jawaban Responden	Nilai Skor
Sangat Setuju (SS)	5
Setuju (S)	4
Netral (N)	3
Tidak Setuju (TS)	2
Sangat Tidak Setuju (STS)	1

Sumber: Data di Olah dari Hasil Wawancara Oleh Peneliti

Sugiyono (2001) menyatakan bahwa untuk menggambarkan tanggapan responden serta menjelaskan jawaban secara rinci dari setiap responden, data perlu diklasifikasikan ke dalam kategori skor tertentu dengan menggunakan rentang skala penilaian pada setiap item pernyataan sebagai berikut:

$$RS = \frac{n\,(m-1)}{m}$$

Keterangan : RS = Rentang skala

n = Jumlah sampel

m = Jumlah jawaban tiap item

1.7.7.2 Analisis Data

Pengujian dan pembuktian hipotesis dalam penelitian ini dilakukan melalui analisis deskriptif dengan pendekatan kuantitatif. Tahapan analisis meliputi uji validitas untuk menilai kelayakan setiap item pernyataan dalam instrumen penelitian, uji reliabilitas untuk mengukur tingkat konsistensi dan keandalan hasil pengukuran, serta uji asumsi klasik yang mencakup uji normalitas, multikolinearitas, dan heteroskedastisitas guna memastikan model regresi yang digunakan memenuhi persyaratan analisis. Selanjutnya, pengujian hipotesis dilakukan dengan menggunakan analisis regresi linier berganda untuk mengetahui arah dan besarnya pengaruh Program *Security Awareness* (X) terhadap Pengetahuan Keamanan Siber Pegawai Komdigi (Y). Uji t (parsial) digunakan untuk menguji pengaruh masing-masing variabel independen secara individual terhadap variabel dependen, sedangkan uji F (simultan) digunakan untuk menilai pengaruh kedua variabel independen secara bersama-sama. Selain itu, koefisien determinasi (R^2) dihitung untuk mengetahui tingkat kontribusi variabel independen dalam menjelaskan variasi pada variabel dependen.

a. Uji Validitas

UUji validitas dilakukan untuk menilai kelayakan setiap butir pernyataan dalam suatu konstruk yang digunakan untuk merepresentasikan variabel penelitian. Evaluasi terhadap masing-masing item dilakukan dengan melihat nilai *corrected item-total correlation*. Suatu butir pernyataan dinyatakan valid apabila nilai r-hitung (*corrected item-total correlation*) lebih besar dibandingkan dengan nilai r-tabel yang ditetapkan berdasarkan derajat kebebasan (*degree of freedom*). Proses pengujian validitas

ini dapat dilakukan dengan bantuan perangkat lunak analisis statistik, seperti Microsoft Excel, Statistical Analysis, maupun SPSS versi 27

b. Uji Reabilitas

Reliabilitas merupakan ukuran yang digunakan untuk menilai tingkat kestabilan dan konsistensi jawaban responden terhadap konstruk pertanyaan yang merepresentasikan dimensi suatu variabel dalam kuesioner.

Pengujian reliabilitas dilakukan dengan menggunakan *Cronbach's Alpha*, yang dapat dihitung melalui perangkat lunak seperti Microsoft Excel, *Statistical Analysis*, atau SPSS versi 27. . Suatu konstruk variabel dinyatakan memiliki reliabilitas yang baik apabila nilai *Cronbach's Alpha* lebih besar dari 0,60.

c. Uji Normalitas

Uji normalitas dilakukan untuk memastikan bahwa variabel independen dan variabel dependen dalam model regresi memiliki distribusi data yang normal. Model regresi yang baik ditandai dengan distribusi data yang normal atau mendekati normal, sehingga hasil analisis statistik yang dihasilkan dapat dinyatakan valid.

d. Uji Multikolinearitas

Uji multikolinearitas dilakukan untuk mengidentifikasi adanya hubungan atau korelasi antarvariabel independen dalam model regresi. Keberadaan multikolinearitas dapat meningkatkan nilai standar error, yang berdampak pada nilai t-hitung menjadi lebih kecil dibandingkan t-tabel. Oleh karena itu, model regresi yang baik seharusnya tidak mengandung gejala multikolinearitas. Pengujian multikolinearitas dilakukan dengan menggunakan nilai *Variance Inflation Factor* (VIF) dan *tolerance*

e. Uji Heteroskedastisitas

Uji Heteroskedastisitas adalah kondisi di mana varian residual tidak sama untuk semua pengamatan dalam model regresi. Uji heteroskedastisitas bertujuan untuk mendeteksi ketidaksamaan ini dengan menganalisis grafik *scatter plot* antara nilai prediksi variabel terikat (ZPRED) dan residual (SRESID).

f. Uji t

Uji t, yang juga disebut sebagai uji parsial, digunakan untuk menilai pengaruh masing-masing variabel independen secara individual terhadap variabel dependen. Pengujian dilakukan dengan membandingkan nilai t-hitung dengan nilai t-tabel.

g. Uji Koefisien Determinasi

Uji koefisien determinasi (R^2) digunakan untuk mengukur besarnya kontribusi atau kemampuan variabel independen dalam menjelaskan variasi pada variabel dependen. Dalam penelitian ini, pengujian koefisien determinasi bertujuan untuk mengetahui sejauh mana Program *Security Awareness* (X1) dan Kebijakan Keamanan Informasi (X2) mampu menjelaskan perubahan yang terjadi pada Budaya Keamanan Siber (Y). Nilai R^2 berada pada rentang 0 hingga 1, di mana nilai yang semakin mendekati 1 menunjukkan bahwa variabel independen memiliki pengaruh yang kuat terhadap variabel dependen, sedangkan nilai yang mendekati 0 mengindikasikan bahwa pengaruh tersebut relatif lemah.

Dengan demikian, uji determinasi menunjukkan sejauh mana peningkatan kesadaran keamanan dan penerapan kebijakan keamanan informasi dapat membentuk budaya keamanan siber di lingkungan Kementerian Komunikasi dan Digital Republik Indonesia.