ISIHUMOR: Jurnal Ilmu Sosial dan Humaniora
Vol.4 No 4 Oktober 2026, Hlm. 1734-1755

PRAKTIK KEAMANAN INFORMASI ASN DALAM PENGGUNAAN PERANGKAT DAN PENGELOLAAN DATA DIGITAL DI PEMERINTAH PROVINSI DKI JAKARTA

Cakrawala Senja[1], Najma Nicky Ravae[2], Safa Khansa Farellya[3], Sammora Jogi Nasution[4], Lina Miftahul Jannah[5]

[1]Universitas Indonesia, Depok, Indonesia; cakrawala.senja@ui.ac.id
[2]Universitas Indonesia, Depok, Indonesia; najma.nicky@ui.ac.id
[3]Universitas Indonesia, Depok, Indonesia; safa.khansa@ui.ac.id
[4]Universitas Indonesia, Depok, Indonesia; sammora.jogi@ui.ac.id
[5]Universitas Indonesia, Depok, Indonesia; miftahul@ui.ac.id
* Corresponding Author: cakrawala.senja@ui.ac.id

INFO ARTIKEL

Diterima: 16 Juli 2026
Direvisi: 27 Juli 2026
Disetujui: 18 September 2026
Tersedia Daring: 30 Oktober 2026

Kata Kunci:
Aparatur Sipil Negara;
DigComp 3.0;
Keamanan Informasi;
Praktik Kerja Digital

ABSTRAK

Perkembangan praktik kerja digital dalam penyelenggaraan pemerintahan meningkatkan kebutuhan akan keamanan informasi, khususnya dalam penggunaan perangkat kerja dan pengelolaan data digital. Penelitian ini bertujuan untuk mendeskripsikan praktik keamanan informasi ASN di Pemerintah Provinsi DKI Jakarta dengan mengacu pada kompetensi 4.1 (*Protecting Devices*) dan 4.2 (*Protecting Personal Data and Privacy*) dalam kerangka DigComp 3.0. Penelitian menggunakan pendekatan kuantitatif dengan data primer yang diperoleh melalui kuesioner terhadap 370 responden, terdiri atas 221 PNS (59,7%), 90 PPPK (24,3%), dan 59 CPNS (15,9%). Data dianalisis menggunakan statistik deskriptif terhadap pertanyaan tertutup, sedangkan jawaban terbuka mengenai skenario risiko keamanan digital dikelompokkan berdasarkan kesamaan tindakan yang disebutkan responden. Hasil penelitian menunjukkan bahwa mayoritas responden melaporkan praktik keamanan informasi yang positif. Sebanyak 97,6% responden menyatakan menjaga keamanan perangkat kerja secara mandiri, 99,2% menggunakan kata sandi yang kuat, dan 97,3% memastikan perangkat lunak keamanan dalam versi terbaru. Selain itu, 99,7% menyatakan membatasi pembagian data pribadi masyarakat kepada pihak yang berkepentingan dan 99,2% menyatakan mampu mengenali upaya penipuan digital. Namun, jawaban terhadap skenario risiko menunjukkan bahwa tindakan pelaporan insiden belum banyak disebutkan secara eksplisit, khususnya pada skenario penerimaan pesan mencurigakan yang hanya disebutkan oleh 3,0% responden. Temuan ini menunjukkan bahwa tingginya praktik keamanan informasi yang dilaporkan belum sepenuhnya tercermin dalam penyebutan tindakan penanganan insiden. Oleh karena itu, diperlukan penguatan pelatihan berbasis skenario, kejelasan mekanisme pelaporan, dan dukungan sistem keamanan organisasi untuk mendukung praktik keamanan informasi ASN.

Keywords:
Civil Servants
DigComp 3.0
Information Security
Digital Work Practices

ABSTRACT

The development of digital work practices in government administration has increased the need for information security, particularly in the use of work devices and digital data management. This study aims to describe information security practices among civil servants in the Provincial Government of DKI Jakarta, referring to competencies 4.1 (Protecting Devices) and 4.2 (Protecting Personal Data and Privacy) in the DigComp 3.0 framework. This study employed a quantitative approach using primary data collected through a questionnaire involving 370 respondents, consisting of 221 civil servants (PNS) (59.7%), 90 government employees under employment agreements (PPPK) (24.3%),

and 59 prospective civil servants (CPNS) (15.9%). Closed-ended responses were analyzed using descriptive statistics, while open-ended responses concerning digital security risk scenarios were grouped based on similarities in the actions mentioned by respondents. The findings indicate that the majority of respondents reported positive information security practices. A total of 97.6% of respondents reported independently maintaining the security of their work devices, 99.2% reported using strong passwords, and 97.3% reported ensuring that security software was up to date. Furthermore, 99.7% reported restricting the sharing of citizens' personal data to authorized parties, while 99.2% stated that they could recognize digital fraud attempts. However, responses to the risk scenarios indicate that incident reporting was rarely mentioned explicitly, particularly in the scenario involving suspicious messages, where only 3.0% of respondents mentioned reporting such messages. This finding suggests that the high levels of reported information security practices are not fully reflected in the actions mentioned for incident handling. Therefore, scenario-based training, clear reporting mechanisms, and organizational security system support need to be strengthened to improve information security practices among civil servants.

© 2026
This is an open access article under CC-BY license

1. Pendahuluan

Kompetensi digital tidak hanya berkaitan dengan kemampuan seseorang dalam menggunakan teknologi, Digcomp 3.0 mendefinisikan kompetensi digital sebagai pengetahuan, keterampilan, dan sikap untuk menggunakan teknologi digital secara percaya diri, kritis, dan bertanggung jawab dalam belajar, bekerja, serta berpartisipasi di masyarakat (Cosgrove & Cachia, 2025). Cakupan kompetensi digital yang luas ini tercermin pada lima area kompetensi DigComp 3.0, yang salah satunya adalah Keamanan, Kesejahteraan, dan Penggunaan yang Bertanggung Jawab (*Safety, Wellbeing and Responsible Use*). Area ini juga memuat kompetensi 4.1 *Protecting Devices*, yaitu kemampuan menerapkan langkah keamanan siber untuk melindungi perangkat dan isinya, serta memuat kompetensi 4.2 *Protecting Personal Data and Privacy*, yaitu kemampuan melindungi data pribadi dan privasi serta menggunakan data milik sendiri maupun orang lain secara aman, etis, dan bertanggung jawab (Cosgrove & Cachia, 2025).

Pemahaman ini tentunya sangat penting bagi Aparatur Sipil Negara (ASN) karena pekerjaan ASN yang berhubungan langsung dengan informasi dan data masyarakat. Hal tersebut turut didorong dengan keluarnya Peraturan Presiden Nomor 95 Tahun 2018 terkait dengan Sistem Pemerintahan Berbasis Elektronik (SPBE) yang mendorong pemerintah utamanya ASN untuk menyelenggarakan layanan publik secara elektronik melalui Sistem Pemerintahan Berbasis Elektronik (Republik Indonesia, 2018), ASN harus mengelola data warga melalui perangkat dan sistem digital yang ada di instansinya. Karena data tersebut tersimpan dan diakses melalui perangkat dan akun kerja, maka ada kemungkinan dapat membuka jalan bagi pihak yang tidak berwenang untuk mengambil data warga (Mufid & Alkadry, 2026). Risiko ini tidak semata-mata berhenti pada

gangguan sistem, tetapi juga mengancam data pribadi warga yang dipercayakan kepada instansi pemerintah. Ancaman terhadap data warga inilah yang menjadi alasan utama agar pemerintah harus memastikan data tersebut terlindungi dalam setiap pemrosesannya.

Kewajiban melindungi data warga tersebut diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). UU PDP mengatur pemrosesan data pribadi dan menggolongkan badan publik sebagai pengendali data pribadi (Republik Indonesia, 2022), sehingga instansi pemerintah memikul kewajiban pengendali dan ASN berperan sebagai aktor yang menjalankannya dalam pekerjaan sehari-hari. Sebagai pelaksana kewajiban tersebut, ASN dituntut untuk memiliki dua kompetensi keamanan dalam DigComp 3.0, yang mana kompetensi 4.1 menuntut ASN menerapkan perlindungan dasar pada perangkat kerja, seperti antivirus, penguncian layar, dan kata sandi yang kuat (Cosgrove & Cachia, 2025), dan kompetensi 4.2 menuntut ASN menangani data pribadi, termasuk milik orang lain, secara hati-hati dan bertanggung jawab (Cosgrove & Cachia, 2025). Bagi ASN, kedua kompetensi ini berjalan beriringan, karena perangkat dan akun kerja menjadi jalur akses ke data warga yang harus dilindungi.

Meskipun kewajiban hukum dan rumusan mengenai kompetensi digital ASN telah ditetapkan, tetapi masih banyak kebocoran data yang terjadi di instansi pemerintah. Mulyadi et al. (2026) mencatat bahwa insiden kebocoran data naik dari 144 kasus pada 2023, 176 kasus pada 2024, dan mencapai 198 kasus hingga Oktober 2025. Namun, kenaikan jumlah kasus kebocoran data tersebut belum menunjukkan di mana titik lemahnya, karena kebocoran dapat bersumber dari banyak faktor sekaligus. Dari sisi sistem, Mulyadi et al. (2026) menguraikan kelemahan keamanan teknis, standar pengamanan yang tidak seragam antarinstansi, serta audit keamanan yang jarang dilakukan. Dari sisi pengguna, Khoironi (2020) juga menguraikan adanya penggunaan kata sandi yang lemah, penggunaan satu akun untuk banyak orang, dan banyaknya operator sistem yang tidak melakukan pembaruan perangkat lunak (*update patching*) secara berkala. Faktor pengguna ini menyumbang peran yang besar, sebab Izzuddin dan Yuswanto (2025), yang merujuk pada laporan Verizon, menyebutkan bahwa sekitar 60% insiden keamanan siber disebabkan oleh kelalaian dan rendahnya kesadaran dari pengguna. Kedua jenis faktor itu pun sulit dipisahkan karena instansi yang tidak menerapkan sistem pemantauan aktivitas (*logging monitoring*) akan kesulitan menentukan titik awal kebocoran (Mulyadi et al., 2026).

Dalam konteks ASN, Khoironi (2020) menyimpulkan bahwa dari hasil evaluasi dan monitoring SPBE yang belum optimal serta tingginya insiden siber pada domain pemerintah menunjukkan pentingnya kompetensi digital ASN dan pembentukan budaya keamanan siber, tetapi kajian tersebut berupa studi kepustakaan, sehingga praktik keamanan ASN sendiri belum diukur. Pengukuran terhadap hal itu penting karena mengetahui adanya ancaman belum tentu diikuti tindakan perlindungan. Mufid dan Alkadry (2026) melaporkan bahwa pengguna internet mungkin mengetahui pentingnya keamanan digital, tetapi tidak menerapkannya dalam praktik sehari-hari. Izzuddin dan Yuswanto (2025), yang merujuk pada kajian terdahulu juga menjelaskan bahwa

peningkatan pengetahuan tidak otomatis diikuti perubahan perilaku, dan pada kata sandi tantangannya sering terletak pada konsistensi pengguna dalam menerapkannya.

Penelitian ini tidak berhenti pada pertanyaan apakah ASN mengenali ancaman, tetapi juga melihat tindakan yang mereka laporkan dan nyatakan. Penelitian ini juga memetakan pada dua kelompok risiko. Pertama, keamanan perangkat kerja ASN (kompetensi 4.1), yang menjadi pintu akses ke data warga yang diukur melalui kebiasaan ASN mengganti kata sandi serta tindakan yang dilakukan ASN ketika akunnya diretas atau perangkat kerja hilang dan dicuri. Kedua, ancaman terhadap data pribadi masyarakat (kompetensi 4.2), yaitu dengan membatasi pembagian data warga hanya kepada pihak yang berkepentingan, mengenali upaya penipuan digital, serta tindakan yang dinyatakan ASN ketika menerima pesan yang mencurigakan. Kedua hal ini tentunya saling berkaitan, karena perangkat kerja yang hilang atau pesan penipuan yang ditanggapi dengan keliru akan membuka akses bagi pihak yang tidak berwenang ke data warga, sehingga perlu dikaji bagaimana ASN di Pemprov DKI Jakarta menjaga keamanan digitalnya dalam melindungi data masyarakat.

Keterkaitan antara keamanan akun dan perangkat kerja dengan perlindungan data warga pada penelitian ini juga berhubungan dan telah disinggung dalam sejumlah penelitian terdahulu, meskipun penelitian-penelitian tersebut memiliki fokus yang berbeda. Pada aspek keamanan perangkat dan sistem informasi, Destyana et al. (2026) pada 2024 menganalisis dugaan kebocoran 4.759.218 data ASN dari Satu Data ASN yang dikelola oleh Badan Kepegawaian Negara (BKN). Dengan memakai data sekunder, mereka mengaitkan dugaan kebocoran itu dengan lemahnya manajemen akses, dan belum diterapkannya *zero trust*, serta tidak adanya audit keamanan berkala. Mulyadi et al. (2026) juga menemukan praktik yang masih umum terjadi di lingkungan ASN, seperti kata sandi lemah, adanya satu akun yang digunakan oleh banyak pegawai, akses sistem melalui perangkat kerja pribadi, hingga pembaruan perangkat lunak yang tidak dilakukan secara berkala. Praktik-praktik tersebut menjadikan kebocoran data sebagai persoalan yang berulang di sektor publik. Mulyadi et al. (2026) menyebut pola kerentanan yang konsisten dan berulang pada berbagai instansi, sedangkan data yang bocor pada kasus BKN mencakup identitas pribadi, nomor induk pegawai, dan riwayat kepegawaian (Destyana et al., 2026). Penyebab kebocoran juga bertumpuk, sehingga instansi sulit menelusuri titik awalnya, terutama bila *logging monitoring* tidak dilakukan (Mulyadi et al., 2026). Dua praktik di atas memperberat kesulitan itu. Ketika satu akun dipakai banyak pegawai dan sistem diakses dari perangkat pribadi, catatan akses tidak dapat menunjukkan siapa yang membuka data warga dan dari perangkat mana. Kondisi ini memunculkan pertanyaan mengenai siapa saja yang secara faktual berwenang memegang dan mengakses data warga. Pada ranah kompetensi digital, Supit dan Pangalila (2025) menunjukkan bahwa kompetensi digital berpengaruh positif dan signifikan terhadap kinerja ASN dengan skor ($r = 0{,}642$; $R^2 = 0{,}412$), tetapi kesadaran keamanan digital memperoleh skor terendah, yaitu 3,56 di antara sepuluh indikator yang diukur. Pada aspek respons terhadap ancaman digital, Izzuddin dan Yuswanto (2025) mengukur kesadaran keamanan siber di lingkungan Pemerintah Kota Administrasi

Jakarta Barat. Skor kesadaran tercatat 2,48 pada pengukuran awal (77 pengelola TIK) dan 2,97 pada pengukuran lanjutan (419 pegawai ASN dan non-ASN) pada skala 1–4. Meskipun skor keseluruhan masuk ke kategori baik, indikator pelaporan insiden teknis (1,93) serta aspek hukum dan regulasi sosial (1,38) tetap rendah. Sementara itu, Salsabila et al. (2025) menegaskan bahwa organisasi di Indonesia cenderung reaktif dalam menangani krisis keamanan digital dan bahwa rekayasa sosial seperti *phishing* menyasar faktor manusia sebagai titik terlemah.

Meskipun sejumlah penelitian telah membahas keamanan digital dan perlindungan data di sektor publik, masih terdapat beberapa aspek yang belum banyak dikaji. Pertama, penelitian mengenai kebocoran data dan implementasi UU PDP (Destyana et al., 2026; Mulyadi et al., 2026) lebih banyak bertumpu pada analisis normatif, studi kasus, dan data sekunder pada tingkat kelembagaan. Dengan demikian, praktik ASN sebagai pelaksana dalam melindungi perangkat, sistem informasi, dan data masyarakat belum banyak diukur secara langsung. Praktik ASN yang diuraikan Mulyadi et al. (2026), misalnya, bersumber dari kajian terdahulu dan bukan hasil pengukuran langsung terhadap ASN. Kedua, penelitian Supit dan Pangalila (2025) mengkaji hubungan kompetensi digital dengan kinerja ASN pada satu instansi dengan jumlah 46 responden, tetapi belum secara khusus mengukur kompetensi perlindungan perangkat dan data sebagaimana dirumuskan dalam DigComp 3.0 (Cosgrove & Cachia, 2025). Ketiga, penelitian Izzuddin dan Yuswanto (2025) mengenai kesadaran keamanan siber di lingkungan Pemerintah Kota Administrasi Jakarta Barat menggunakan pendekatan *self-assessment* dengan kelompok responden yang berbeda pada pengukuran awal dan lanjutan, serta mencakup ASN dan non-ASN. Penelitian tersebut telah mengukur indikator kata sandi dan keamanan perangkat, tetapi belum secara khusus mengaitkannya dengan pembatasan pembagian data warga kepada pihak yang berkepentingan. Keempat, penelitian empiris mengenai tindakan yang dinyatakan ASN ketika menghadapi skenario risiko keamanan digital masih terbatas, khususnya pada situasi kehilangan atau pencurian perangkat kerja dan penerimaan pesan mencurigakan yang meminta data pribadi. Pelaporan insiden dalam penelitian Izzuddin dan Yuswanto (2025) lebih banyak ditempatkan sebagai salah satu indikator kesadaran keamanan digital, sedangkan tindakan yang dinyatakan ASN dalam menghadapi kedua skenario tersebut belum menjadi fokus kajian. Padahal, mekanisme respons insiden yang tidak terintegrasi dapat memperlambat proses deteksi dan penanganan kebocoran data (Destyana et al., 2026).

Berdasarkan kesenjangan tersebut, penelitian ini menawarkan kebaruan dalam tiga aspek. Pertama, penelitian ini menghubungkan kompetensi perlindungan perangkat dan sistem informasi (kompetensi 4.1) dengan perlindungan data pribadi dan privasi (kompetensi 4.2) dalam satu kerangka analisis berdasarkan DigComp 3.0. Kedua, penelitian ini tidak hanya mengkaji pengenalan ancaman digital, tetapi juga tindakan yang dinyatakan ASN ketika menghadapi dua skenario risiko, yaitu kehilangan atau pencurian perangkat kerja dan penerimaan pesan mencurigakan yang meminta data pribadi. Dengan demikian, penelitian ini dapat menggambarkan variasi tindakan yang disebutkan responden, termasuk penyebutan pelaporan insiden. Ketiga, penelitian ini dilakukan terhadap ASN di lingkungan Pemerintah Provinsi DKI Jakarta. Pemilihan lokasi

ini relevan karena ASN sebagai pelaksana pelayanan publik berhadapan dengan penggunaan perangkat dan sistem digital dalam pengelolaan data masyarakat. Selain itu, penelitian terdahulu mengenai kesadaran keamanan siber di wilayah Jakarta masih terbatas pada lingkungan Pemerintah Kota Administrasi Jakarta Barat (Izzuddin & Yuswanto, 2025), sehingga penelitian ini memberikan gambaran praktik keamanan informasi pada lingkup Pemerintah Provinsi DKI Jakarta berdasarkan data responden yang diteliti. Oleh karena itu, penelitian ini bertujuan mendeskripsikan praktik keamanan informasi ASN di Pemerintah Provinsi DKI Jakarta dengan mengacu pada kompetensi 4.1 dan 4.2 DigComp 3.0 (Cosgrove & Cachia, 2025), mencakup pengamanan perangkat dan akun kerja, pembatasan pembagian data warga, pengenalan penipuan digital, serta tindakan yang dinyatakan ASN dalam menghadapi skenario risiko. Secara teoritis, penelitian ini memperluas kajian kompetensi digital ASN yang selama ini berfokus pada hubungannya dengan kinerja (Supit & Pangalila, 2025) ke aspek keamanan informasi dengan membedakan pengenalan ancaman dari tindakan penanganan yang dinyatakan. Secara praktis, hasil penelitian diharapkan dapat menjadi masukan bagi pemerintah daerah dalam menyusun pelatihan berbasis skenario, memperjelas saluran dan prosedur pelaporan insiden, serta memperkuat praktik keamanan informasi dalam pelayanan publik berbasis SPBE.

2. Metode

2.1 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan jenis penelitian deskriptif dengan pendekatan kuantitatif. Penelitian deskriptif ini bertujuan untuk memberikan gambaran yang sistematis dan akurat terkait fenomena yang diteliti berdasarkan data empiris (Neuman, 2014). Dalam konteks penelitian ini, fokus kajian diarahkan pada praktik keamanan digital ASN dalam mendukung perlindungan data pribadi masyarakat dalam lingkup Pemerintah Provinsi DKI Jakarta. Pendekatan kuantitatif digunakan untuk menggambarkan distribusi jawaban responden terhadap pertanyaan tertutup.

2.2 Data dan Sumber Data

Data yang digunakan dalam penelitian ini merupakan data primer yang diperoleh melalui kuesioner mengenai kompetensi digital ASN. Analisis dibatasi pada 370 responden dengan data valid berdasarkan dokumen hasil pengolahan data penelitian. Pengambilan sampel dilakukan dengan menggunakan teknik *non-probability sampling* dengan *quota sampling.* Unit analisis penelitian berfokus pada jawaban responden pada pertanyaan di Dimensi 4, yaitu *Safety, Wellbeing and Responsible Use*. Dimensi ini mencakup rincian 5 pertanyaan tertutup dan 2 pertanyaan yang dianalisis dan disajikan pada Tabel 1.

Tabel 1. Indikator Penelitian pada Dimensi *Safety, Wellbeing, and Responsible Use*

Indikator	Jenis Pertanyaan	Pertanyaan
Keamanan perangkat kerja	Tertutup	Saya menjaga keamanan perangkat kerja saya sendiri, tidak hanya bergantung pada tim IT di Instansi
	Terbuka	Jika perangkat kerja Anda hilang atau dicuri, langkah apa yang akan Anda lakukan?
Penggunaan data sandi yang kuat	Tertutup	Saya menggunakan kata sandi yang kuat untuk melindungi perangkat kerja saya
Pembaruan perangkat lunak keamanan	Tertutup	Saya memastikan perangkat lunak (*software*) keamanan pada perangkat kerja saya ada dalam versi terbaru
Pembatasan pembagian data pribadi masyarakat	Tertutup	Saya memastikan data pribadi masyarakat (seperti KTP, KK, atau Nomor Telepon) hanya dibagikan kepada pihak yang berkepentingan menerimanya
Pengenalan upaya penipuan digital	Tertutup	Saya mengenali upaya penipuan digital yang berusaha memperoleh data pribadi masyarakat namun berisi tautan mencurigakan yang meminta data pribadi (seperti pesan yang mengaku dari Instansi resmi)
	Terbuka	Jika Anda menerima pesan yang mengaku dari instansi resmi namun meminta data pribadi melalui tautan mencurigakan, tindakan apa yang akan Anda lakukan?

Sumber: Hasil olah data primer PPAP Kelompok Negara 1 (2026)

2.3 Teknik Pengumpulan Data

Pengumpulan data dilakukan melalui kuesioner yang memuat pertanyaan tertutup dan terbuka. Metode kuantitatif ini mengumpulkan data melalui pertanyaan tertutup pada sebuah instrumen untuk menghasilkan data kuantitatif yang dapat diolah (Creswell & Creswell, 2018). Pertanyaan tertutup digunakan untuk mengidentifikasi kecenderungan jawaban responden mengenai praktik keamanan perangkat dan perlindungan data pribadi dalam penggunaan teknologi digital menggunakan skala jawaban yang digunakan dalam kuesioner. Pertanyaan terbuka berbasis skenario digunakan untuk memperoleh gambaran mengenai tindakan yang dinyatakan responden ketika menghadapi potensi risiko keamanan digital, seperti kehilangan atau pencurian perangkat kerja dan penerimaan pesan mencurigakan. Penggunaan pertanyaan tertutup memungkinkan jawaban responden dirangkum secara kuantitatif,

sedangkan pertanyaan terbuka memungkinkan responden mendapatkan ruang untuk menjelaskan tindakan yang akan mereka ambil pada situasi tertentu.

2.4 Teknik Analisis Data

Data empiris yang berhasil diperoleh, diolah dan dianalisis menggunakan SPSS. Selain itu, kami menggunakan statistik deskriptif dan analisis kualitatif deskriptif. Analisis statistik deskriptif dilakukan terhadap jawaban tertutup dengan menyajikan distribusi frekuensi dan persentase pada setiap kategori jawaban. Analisis ini digunakan untuk menggambarkan kecenderungan dari respons responden pada masing-masing aspek keamanan digital yang diteliti. Sementara itu, jawaban terbuka dianalisis dengan mengidentifikasi dan mengelompokkan tindakan yang disebutkan oleh responden berdasarkan kesamaan makna. Hasil analisis kedua jenis data kemudian digunakan untuk memberikan gambaran mengenai praktik keamanan digital yang dilaporkan responden dan respons yang mereka nyatakan terhadap skenario risiko. Interpretasi hasil dibatasi pada informasi yang diperoleh melalui kuesioner kemudian dikaitkan dengan aspek perlindungan perangkat serta perlindungan data pribadi dan privasi dalam kerangka DigComp 3.0.

3. Hasil dan Pembahasan

3.1 Praktik Keamanan Digital ASN

Praktik keamanan digital ASN dalam penelitian ini ditinjau melalui tiga pertanyaan, yaitu tanggung jawab menjaga keamanan perangkat kerja, penggunaan kata sandi yang kuat, dan pembaruan perangkat lunak keamanan. Distribusi jawaban responden pada masing-masing pertanyaan disajikan pada Tabel 2 di bawah ini.

Tabel 2. Distribusi Jawaban Responden mengenai Praktik Keamanan Digital ASN (n=370)

Pernyataan	Sangat Tidak Setuju (%)	Tidak Setuju (%)	Setuju (%)	Sangat Setuju (%)
Menjaga keamanan perangkat kerja secara mandiri	2 (0,5%)	7 (1,9%)	175 (47,3%)	186 (50,3%)
Menggunakan kata sandi yang kuat	0 (0,0%)	3 (0,8%)	150 (40,5%)	217 (58,6%)
Memastikan perangkat lunak keamanan dalam versi terbaru	0 (0,0%)	10 (2,7%)	190 (51,4%)	170 (45,9%)

Sumber: Hasil olah data primer PPAP Kelompok Negara 1 (2026)

Berdasarkan tabel tersebut, mayoritas responden menyatakan setuju atau sangat setuju terhadap ketiga pertanyaan mengenai praktik keamanan digital. Pada aspek menjaga keamanan perangkat kerja secara mandiri, sebanyak 361 responden (97,6%)

menyatakan sangat setuju atau setuju bahwa mereka menjaga keamanan perangkat kerja secara mandiri. Sedangkan, 9 responden (2,4%) menyatakan tidak setuju atau sangat tidak setuju. Sementara itu, penggunaan kata sandi yang kuat untuk melindungi perangkat kerja memperoleh persetujuan dari 367 responden (99,2%), dengan tiga responden (0,8%) menyatakan tidak setuju.

Hasil ini menunjukkan bahwa penggunaan kata sandi yang kuat memperoleh proporsi persetujuan tertinggi di antara ketiga pertanyaan dalam kelompok praktik keamanan perangkat. Adapun pada aspek pembaruan perangkat lunak keamanan, sebanyak 360 responden (97,3%) menyatakan setuju atau sangat setuju bahwa mereka memastikan perangkat lunak keamanan pada perangkat kerja berada dalam versi terbaru. Sebanyak sepuluh responden (2,7%) menyatakan tidak setuju. Dibandingkan dengan dua pertanyaan sebelumnya, pembaruan perangkat lunak keamanan memiliki proporsi persetujuan paling rendah, meskipun mayoritas responden tetap memberikan jawaban positif. Meskipun menunjukkan kecenderungan yang positif, tingginya persentase persetujuan tersebut perlu ditafsirkan secara hati-hati. Data penelitian diperoleh melalui kuesioner berdasarkan pernyataan responden mengenai praktik keamanan yang mereka lakukan, sehingga belum dapat memastikan apakah tindakan tersebut diterapkan secara konsisten dalam pekerjaan sehari-hari. Sebagai contoh, persetujuan terhadap penggunaan kata sandi yang kuat belum secara langsung menunjukkan bahwa responden selalu memperbarui kata sandi atau menerapkan pengamanan akun sesuai prosedur instansi. Dengan demikian, hasil ini lebih menggambarkan praktik keamanan perangkat yang dilaporkan responden daripada kemampuan aktual yang telah diverifikasi.

3.2 Perlindungan Data Pribadi dan Pengenalan Ancaman Digital

Perlindungan data pribadi dan pengenalan ancaman digital dalam penelitian ini diukur melalui dua pernyataan. Pertama, mengenai kecenderungan responden untuk memastikan bahwa data pribadi masyarakat, seperti KTP, KK, atau nomor telepon, hanya dibagikan kepada pihak yang berkepentingan menerimanya. Kedua, mengenai kemampuan responden dalam mengenali upaya penipuan digital yang berusaha memperoleh data pribadi melalui tautan mencurigakan, seperti pesan yang mengatasnamakan instansi resmi. Distribusi jawaban responden terhadap kedua pernyataan tersebut disajikan pada Tabel 3.

Tabel 3. Distribusi Jawaban Responden Mengenai Perlindungan Data Pribadi Dan Pengenalan Ancaman Digital (N=370)

Pernyataan	Sangat Tidak Setuju (%)	Tidak Setuju (%)	Setuju (%)	Sangat Setuju (%)
Memastikan data pribadi masyarakat hanya dibagikan kepada pihak yang berkepentingan	1 (0,3%)	0 (0,0%)	124 (33,5%)	245 (66,2%)
Mengenali upaya penipuan digital melalui pesan atau	0 (0,0%)	3 (0,8%)	167 (45,1%)	200 (54,1%)

tautan mencurigakan	

Sumber: Hasil olah data primer PPAP Kelompok Negara 1 (2026)

Hasil pada Tabel 3 menunjukkan bahwa kedua pernyataan memperoleh tingkat persetujuan yang tinggi. Pada pernyataan mengenai pembatasan pembagian data pribadi masyarakat kepada pihak yang berkepentingan, sebanyak 369 responden (99,7%) menyatakan setuju atau sangat setuju. Sebagian besar responden, yaitu 245 orang (66,2%), bahkan menyatakan sangat setuju, sedangkan satu responden (0,3%) menyatakan sangat tidak setuju. Sementara itu, pada pernyataan mengenai kemampuan mengenali upaya penipuan digital melalui pesan atau tautan mencurigakan, sebanyak 367 responden (99,2%) menyatakan setuju atau sangat setuju, sedangkan tiga responden (0,8%) menyatakan tidak setuju. Dengan demikian, kedua aspek menunjukkan proporsi persetujuan yang tinggi, dengan persetujuan tertinggi terdapat pada pernyataan mengenai pembatasan pembagian data pribadi masyarakat.

3.3 Respons yang Dinyatakan terhadap Skenario Risiko

Kuesioner penelitian juga memuat dua pertanyaan terbuka untuk mengetahui tindakan yang dinyatakan oleh responden ketika menghadapi situasi yang berpotensi menimbulkan risiko keamanan digital. Pertanyaan pertama berkaitan dengan kondisi ketika perangkat kerja hilang atau dicuri. Pertanyaan kedua berkaitan dengan penerimaan pesan yang mengatasnamakan instansi resmi dan meminta data pribadi melalui tautan (*link*) yang mencurigakan.

Tabel 4. Ringkasan Respons Responden terhadap Skenario Risiko Keamanan Digital

Skenario	Kategori Tindakan yang Muncul dalam Jawaban	Ringkasan Respons
Perangkat kerja hilang atau dicuri	Pencadangan data (*backup data)*	Responden menyebutkan penggunaan cadangan data sebagai salah satu langkah yang berkaitan dengan pengamanan data.
	Pelaporan kepada pihak berwajib	Responden menyebutkan pelaporan sebagai tindakan yang dapat dilakukan ketika perangkat hilang atau dicuri.
	Pengamanan dan pemblokiran akun	Responden menyebutkan pengamanan atau pemblokiran akun untuk mencegah penyalahgunaan data.
Menerima pesan yang mencurigakan yang meminta data pribadi	Mengabaikan atau tidak merespons pesan	Responden menyebutkan tidak menanggapi pesan yang mencurigakan.

	Verifikasi atau konfirmasi kepada instansi resmi	Responden menyebutkan perlunya memastikan kebenaran pesan melalui instansi resmi.
	Tidak mengklik tautan mencurigakan	Responden menyebutkan menghindari tautan yang berpotensi digunakan untuk memperoleh data pribadi.

Sumber: Hasil olah data primer PPAP Kelompok Negara 1 (2026)

Berdasarkan jawaban terbuka pada skenario kehilangan atau pencurian perangkat kerja, tindakan yang paling banyak disebutkan responden adalah pencadangan data (backup data), yaitu sebanyak 72 responden (19,5%). Selanjutnya, sebanyak 57 responden (15,4%) menyebutkan pelaporan kepada pihak berwajib dan 53 responden (14,3%) menyebutkan pengamanan atau pemblokiran akun. Selain itu, 48 responden (13,0%) menyatakan akan melaporkan kejadian tersebut kepada instansi atau kantor, 25 responden (6,8%) menyebutkan penggantian kata sandi, dan 15 responden (4,1%) menyebutkan penguncian perangkat dari jarak jauh. Sementara itu, pada skenario penerimaan pesan mencurigakan yang meminta data pribadi, tindakan yang paling banyak disebutkan adalah mengabaikan atau tidak merespons pesan, yaitu sebanyak 135 responden (36,5%). Sebanyak 85 responden (23,0%) menyebutkan akan melakukan verifikasi atau konfirmasi kepada instansi resmi, 47 responden (12,7%) menyatakan tidak akan mengeklik tautan mencurigakan, dan 43 responden (11,6%) menyebutkan tindakan memblokir pengirim. Adapun pelaporan pesan mencurigakan hanya disebutkan oleh 11 responden (3,0%).

Secara keseluruhan, jawaban terbuka menunjukkan bahwa responden menyebutkan beragam tindakan dalam menghadapi risiko keamanan digital, baik yang berkaitan dengan pengamanan perangkat dan akun maupun penanganan pesan mencurigakan. Pada skenario kehilangan perangkat, jawaban responden mencakup pencadangan data, pengamanan akun, dan pelaporan kepada pihak terkait. Sementara itu, pada skenario pesan mencurigakan, respons lebih banyak berupa tindakan pencegahan secara individual, seperti mengabaikan pesan, melakukan verifikasi, dan menghindari tautan mencurigakan. Hasil ini menggambarkan kecenderungan tindakan yang dinyatakan responden ketika dihadapkan pada situasi hipotetis, bukan bukti langsung bahwa tindakan tersebut selalu diterapkan dalam situasi nyata.

3.4 Praktik Keamanan Digital Sebagai Bagian dari Kompetensi ASN

Secara umum, pola jawaban responden menunjukkan bahwa praktik keamanan digital dasar banyak dilaporkan oleh ASN Pemprov DKI Jakarta dalam pekerjaan sehari-hari. Pola ini terlihat dari proporsi hasil responden yang menyatakan setuju atau sangat setuju terhadap perlunya menjaga keamanan perangkat kerjanya sendiri, tidak hanya menyerahkannya kepada tim IT instansi (97,6%); menggunakan kata sandi yang kuat (99,2%); serta memastikan perangkat kerjanya selalu memakai versi keamanan terbaru (97,3%). Dengan kata lain, dari setiap seratus ASN yang menjawab, hanya sekitar satu sampai tiga orang yang tidak sependapat. Kecenderungan tersebut juga tampak pada

jawaban lanjut responden mengenai tindakan yang dilakukan apabila perangkat kerja hilang atau dicuri, seperti mencadangkan data, melaporkan kejadian kepada pihak yang berwenang, serta mengamankan dan memblokir akun agar data tidak disalahgunakan. Namun, tingginya persentase perlu dianalisis lebih lanjut secara kritis karena seluruh temuan didasarkan pada pernyataan responden yang lebih mencerminkan sikap daripada kepatuhan aktual yang terverifikasi. Dengan kata lain, persetujuan yang tinggi menunjukan fondasi kesadaran namun belum membuktikan praktik keamanan digital diterapkan secara konsisten dalam situasi kerja nyata.

Pola jawaban tersebut dapat ditafsirkan menggunakan kerangka DigComp 3.0 sebagai indikasi kompetensi *protecting devices* dalam area *safety, wellbeing and responsible use* (Cosgrove & Cachia, 2025). Kompetensi ini tidak hanya mencakup kemampuan mengoperasikan perangkat, melainkan juga penerapan langkah pengamanan dan kesadaran terhadap risiko digital. Praktik yang dilaporkan responden, seperti penggunaan kata sandi kuat, pembaruan perangkat, serta pelibatan diri dalam pengamanan perangkat, selaras dengan indikator dasar kompetensi tersebut. Lebih dari itu, respons terhadap perangkat yang hilang atau dicuri menunjukkan kesadaran bahwa perangkat kerja merupakan media penyimpanan data yang berpotensi menimbulkan risiko apabila jatuh ke tangan pihak yang tidak berwenang. Dalam konteks ASN, kesadaran ini penting karena perangkat kerja dapat menjadi pintu akses terhadap data layanan publik dan data pribadi masyarakat

Meskipun demikian, DigComp 3.0 memandang kompetensi digital sebagai gabungan pengetahuan, keterampilan, dan sikap. Data penelitian ini cenderung menangkap sikap dan praktik yang dilaporkan responden, sehingga tingkat keterampilan aktual belum dapat dipastikan. Dengan begitu, persetujuan responden yang tinggi menunjukkan kecenderungan untuk menerapkan praktik keamanan digital dasar, tetapi belum otomatis membuktikan kepatuhan aktual, konsistensi penerapan, maupun efektivitas perlindungan data. Temuan ini lebih tepat dipahami sebagai fondasi kompetensi pengamanan perangkat, bukan sebagai bukti bahwa seluruh ASN telah mampu mengelola risiko keamanan secara menyeluruh. Tingginya persetujuan responden perlu ditafsirkan dengan mempertimbangkan adanya jurang antara pengetahuan atau kesadaran keamanan dengan perilaku kepatuhan aktual. Workman et al. (2008), sebagaimana dikutip dalam Delso-Vicente et al. (2025), mengidentifikasi adanya kesenjangan tersebut. Fenomena ini juga diperkuat oleh model *knowing-doing gap* yang dibangun Cox (2012) dan ditegaskan dalam penelitian Ali et al. (2021). Model ini menjelaskan bahwa seseorang dapat mengetahui cara menjaga keamanan informasi, tetapi belum tentu menerapkannya secara konsisten. Vilander (2021) menjelaskan bahwa model tersebut menghubungkan *knowing* sebagai pengetahuan dan kesadaran pengguna, *doing* sebagai perilaku keamanan aktual, serta faktor penghubung seperti sikap, pemahaman terhadap alasan kebijakan, dan penilaian ancaman. Oleh karena itu, tanpa adanya intervensi penguatan pada faktor-faktor penghubung tersebut, pengetahuan dan kesadaran belum tentu berbanding lurus dengan tindakan nyata di lapangan. Temuan ini juga sejalan dengan Chaudhary (2024), yang menegaskan bahwa

pengetahuan keamanan tanpa adanya pembentukan dan penguatan perilaku tidak memiliki nilai signifikan praktis bagi kepatuhan organisasi. Chaudhary (2024) mengidentifikasi adanya hambatan terhadap perubahan perilaku keamanan maupun dalam mengadopsi perilaku keamanan, seperti: prosedur keamanan yang dianggap membebani, rendahnya *perceived severity* atau penilaian terhadap tingkat keparahan risiko, komunikasi kebijakan yang kurang persuasif, serta minimnya keteladanan dan norma bersama di tempat kerja. Sebagaimana dapat dipahami, ASN DKI Jakarta berpotensi memiliki kesadaran bahwa perangkat kerja perlu diamankan. Namun, ASN belum tentu menerapkannya secara konsisten apabila risiko dianggap rendah, prosedur dianggap merepotkan, alasan kebijakan tidak dipahami, atau budaya kerja yang belum mendukung kepatuhan bersama. Oleh karena itu, penguatan kompetensi keamanan digital ASN tidak cukup berhenti pada peningkatan pengetahuan. Dukungan terhadap prosedur yang jelas, pelatihan respons insiden, serta budaya kerja yang menempatkan pengamanan perangkat sebagai bagian dari tanggung jawab perlindungan data masyarakat juga diperlukan sebagai esensi penting dalam penguatan kompetensi.

3.5 Praktik Perlindungan Data Pribadi Masyarakat dalam Pekerjaan ASN

Mayoritas responden menunjukkan sikap positif terhadap pembatasan pembagian data pribadi masyarakat, seperti Kartu Tanda Penduduk (KTP), Kartu Keluarga (KK), maupun Nomor Telepon. Sebanyak 124 responden (33,5%) menyatakan setuju dan 245 responden (66,2%) menyatakan sangat setuju bahwa data pribadi masyarakat hanya diberikan kepada pihak yang berkepentingan. Temuan ini mengindikasikan adanya kesadaran yang tinggi akan pentingnya menjaga kerahasiaan data warga, meskipun hasil masih sebatas persepsi dan sikap yang dilaporkan daripada praktik aktual di lapangan. Kesadaran ini menunjukkan fondasi sikap perlindungan data, namun belum membuktikan konsistensi penerapan pembatasan akses dalam situasi kerja nyata. Dengan begitu, tingginya persetujuan responden lebih tepat dipahami sebagai indikasi komitmen normatif terhadap perlindungan data pribadi.

Pihak berkepentingan dalam konteks pelayanan publik dapat dipahami secara terbatas, yaitu petugas atau instansi yang membutuhkan data untuk menjalankan fungsi layanan tertentu dan memiliki dasar kewenangan hukum. Pembatasan setidaknya harus mencerminkan prinsip *purpose limitation* dan *data minimization*, yaitu akses terhadap data pribadi hanya digunakan oleh pihak yang benar-benar membutuhkan untuk tujuan layanan yang sah. *Purpose limitation* menuntut agar data yang dikumpulkan hanya diproses untuk tujuan yang spesifik, eksplisit, dan sah. Sedangkan *data minimization* menuntut agar hanya data relevan dan diperlukan yang dapat diakses atau dibagikan. Dalam konteks birokrasi, prinsip ini berarti ASN tidak boleh mengakses dan menyebarkan data hanya karena data tersebut tersedia di dalam sistem instansi. Mikiver dan Tupay (2023) menekankan bahwa efisiensi berbagi data antarinstansi dalam *e-government* tetap harus dibatasi oleh tujuan awal agar tidak terjadi perluasan penggunaan yang tidak sah. Dengan demikian, sikap responden untuk membatasi pembagian data kepada pihak berkepentingan dapat dibaca sebagai kesadaran awal terhadap prinsip perlindungan data yang bukan hanya bersifat teknis, melainkan juga

bagian dari tata kelola data dan tanggung jawab organisasi publik. Finck & Biega (2021) menegaskan bahwa pengendalian data perlu diwujudkan melalui pembatasan hak akses, audit penggunaan data, dan prosedur persetujuan berbagi data. Artinya, kesadaran ASN perlu diterjemahkan menjadi mekanisme kerja yang terukur. Bukan sebatas komitmen individual tanpa adanya kontrol akses dan prosedur yang jelas.

Praktik dan batasan perilaku ASN memiliki landasan yuridis yang mengikat dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Secara umum, landasan ini menempatkan pemrosesan data pribadi harus dilakukan secara terbatas, spesifik, sah secara hukum, transparan, serta sesuai tujuannya. Proses ini wajib bersandar pada pelaksanaan tugas kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan berdasarkan peraturan perundang-undangan. Prinsip ini menegaskan bahwa pembatasan akses dan pembagian data oleh ASN bukan sekadar formalitas birokrasi, melainkan wujud kepatuhan terhadap standar hukum dan etika perlindungan hak asasi masyarakat. Dalam konteks ASN, kepatuhan hukum atas pembatasan akses bukan sebatas kewajiban moral, melainkan bagian dari pelaksanaan tanggung jawab organisasi publik atas data yang dipercayakan masyarakat.

Temuan ini sejalan dengan literatur perlindungan data publik. Marwenny et al. (2024) menegaskan bahwa perlindungan data pribadi merupakan hak asasi fundamental yang wajib dijamin dan dihormati oleh negara. Lebih dari sekadar kewajiban teknis, pembatasan akses ini merupakan bagian penting dari perwujudan tata kelola pelayanan publik yang transparan, sah, dan terbatas yang bertujuan untuk menjaga akuntabilitas instansi serta menjaga kepercayaan masyarakat. Namun, temuan perlu dibedakan dari kajian implementasi yang masih menghadapi beberapa hambatan. Mulyadi et al. (2026) menemukan adanya tantangan teknis dalam insiden kebocoran data di sektor publik. Kebocoran terus mengalami kenaikan berulang, yaitu 144 kasus pada 2023, 176 kasus pada 2024, dan mencapai 198 kasus hingga Oktober 2025 (Mulyadi et al., 2026). Literatur juga menemukan bahwa instansi pemerintah masih menggunakan sistem dan server lokal lama, di mana tantangan kelembagaan terlihat dari terbatasnya jumlah instansi yang memiliki staf TI dengan kompetensi keamanan tingkat lanjut. Padahal UU PDP mengharuskan adanya pengangkatan pejabat perlindungan data pribadi atau *Data Protection Officer* (DPO). Artinya, meskipun secara normatif kerangka regulasi perlindungan data pribadi telah tersedia, Mulyadi et al. (2026) menilai bahwa implementasinya di tingkat pelayanan publik masih terkesan formalitas. Hambatan cenderung bersumber dari ASN yang belum menginternalisasi keamanan data sebagai bagian dari budaya kerja dan etika pelayanan publik. Astrialita & Nafi'ah (2025) menyebutkan bahwa rendahnya literasi siber berisiko menyebabkan prosedur pengamanan dipersepsikan sebagai beban administratif dibandingkan sebagai kewajiban untuk melindungi hak warga negara. Sejalan dengan hal tersebut, Musdalipa et al. (2026) menekankan pentingnya peningkatan kapasitas sumber daya manusia melalui pendidikan dan pelatihan berkelanjutan dalam menghadapi tantangan transformasi digital, khususnya dalam konteks penegakan hukum. Kepatuhan terhadap hukum merupakan salah satu faktor penting dalam implementasi tata kelola digital dan

perlindungan data. Hal ini menunjukkan bahwa penguatan kapasitas aparatur perlu menjadi bagian dari upaya menghadapi risiko yang muncul dalam pemanfaatan teknologi digital.

Kesadaran terhadap pembatasan akses oleh ASN yang tinggi tidak bisa dipandang sebelah mata. Kesadaran dapat ditempatkan sebagai modal dasar atas terbentuknya perlindungan data yang konsisten. Hambatan di lapangan menandakan bahwa kesadaran individu ASN tidak dapat berdiri sendiri tanpa didukung oleh ekosistem kerja. Sebagaimana ekosistem kerja berfungsi sebagai wadah yang memfasilitasi penerapan kepatuhan tersebut. Oleh karena itu, kesadaran normatif ASN dapat ditransformasikan menjadi praktik kerja yang konsisten melalui dorongan oleh kebijakan dan panduan operasional spesifik yang mendukung; mekanisme pengamanan berbasis *Privacy-by-Design*; sistem kontrol akses otomatis yang membatasi hak akses, enkripsi, dan otentikasi yang terintegrasi dengan sistem kerja; serta internalisasi budaya organisasi (Martínez, 2025).

3.6 Respons ASN terhadap Risiko Keamanan Digital

Respons ASN terhadap risiko keamanan digital perlu dilihat bukan hanya dari kemampuan mengenali ancaman, tetapi juga dari tindakan yang dipilih ketika menghadapi situasi yang berpotensi membahayakan keamanan informasi. Dalam penelitian ini, sebanyak 367 dari 370 responden (99,2%) menyatakan setuju atau sangat setuju bahwa mereka mampu mengenali upaya penipuan digital yang meminta data pribadi melalui tautan mencurigakan. Hasil tersebut menunjukkan bahwa mayoritas responden memiliki persepsi positif terhadap kemampuan mereka dalam mengenali ancaman digital. Meskipun demikian, pengakuan atas kemampuan tersebut belum dapat secara langsung diartikan sebagai bukti bahwa responden selalu mampu menangani ancaman secara tepat dalam situasi nyata.

Gambaran yang lebih konkret terlihat dari jawaban responden ketika ditanyakan mengenai tindakan yang akan dilakukan apabila menerima pesan mencurigakan yang mengatasnamakan instansi resmi. Tindakan yang paling banyak disebut adalah mengabaikan atau tidak merespons pesan, yaitu sebanyak 135 responden (36,5%). Selanjutnya, 85 responden (23,0%) menyebutkan akan melakukan verifikasi atau konfirmasi kepada instansi resmi, sedangkan 47 responden (12,7%) menyatakan tidak akan mengeklik tautan mencurigakan. Terdapat pula responden yang memilih memblokir pengirim atau akun sebanyak 43 orang (11,6%). Sementara itu, tindakan yang secara eksplisit menyebut pelaporan kepada pihak berwenang, tim teknologi informasi (IT) atau atasan hanya ditemukan pada 11 responden (3,0%). Distribusi ini memperlihatkan bahwa respons yang dinyatakan responden lebih banyak berorientasi pada tindakan pencegahan secara individual, sementara pelaporan kepada pihak yang berwenang belum banyak disebutkan. Temuan tersebut tidak serta-merta menunjukkan bahwa responden yang tidak menyebutkan pelaporan memiliki perilaku yang tidak aman, tetapi mengindikasikan bahwa tindak lanjut melalui mekanisme organisasi belum menonjol dalam jawaban terbuka mereka. Padahal, pelaporan memiliki fungsi yang berbeda dari tindakan pencegahan individual karena memungkinkan organisasi mengetahui adanya ancaman dan mengambil langkah penanganan lebih lanjut.

Meskipun hampir seluruh responden menyatakan mampu mengenali upaya penipuan digital, pengenalan terhadap ancaman tersebut belum sepenuhnya tercermin dalam penyebutan tindakan penanganan yang melibatkan organisasi. Hal ini terlihat dari jawaban terbuka, ketika hanya 11 responden (3,0%) yang secara eksplisit menyebutkan pelaporan pesan mencurigakan kepada pihak berwenang, tim IT, atau atasan. Sebaliknya, respons yang lebih banyak disebutkan berkaitan dengan tindakan pencegahan secara individual, seperti mengabaikan pesan, melakukan verifikasi, dan tidak mengeklik tautan mencurigakan. Perbedaan ini menunjukkan bahwa kemampuan mengenali ancaman dan penyebutan tindakan pelaporan merupakan dua aspek yang perlu dibedakan dalam memahami respons keamanan digital ASN.

Jika ditinjau melalui kerangka DigComp 3.0, temuan ini berkaitan dengan kompetensi 4.2, yaitu *Protecting Personal Data and Privacy* yang mencakup kemampuan mengenali upaya manipulatif untuk memperoleh data pribadi serta mengenali dan merespons ancaman seperti *phishing* dan *social engineering* (Cosgrove & Cachia, 2025). Jawaban responden yang menyebutkan tindakan mengabaikan pesan, menghindari tautan mencurigakan, dan melakukan verifikasi menunjukkan adanya sejumlah bentuk respons preventif terhadap ancaman digital. Namun, kompetensi perlindungan data tidak hanya berkaitan dengan kemampuan individu mengenali dan menghindari ancaman, tetapi juga mencakup tindakan yang diperlukan untuk mengurangi risiko penyalahgunaan data. Dalam organisasi pemerintahan, tindakan tersebut perlu didukung oleh mekanisme penanganan insiden yang memungkinkan ancaman dilaporkan dan ditindaklanjuti oleh pihak yang bertanggung jawab. Rendahnya frekuensi jawaban yang secara eksplisit menyebutkan pelaporan memperlihatkan bahwa aspek tindak lanjut secara organisasional belum banyak tercermin dalam respons yang dinyatakan responden. Meskipun demikian, penelitian ini belum mengukur secara khusus pemahaman ASN terhadap prosedur pelaporan maupun ketersediaan mekanisme tersebut di instansi masing-masing. Oleh karena itu, temuan ini lebih tepat dipahami sebagai indikasi perlunya perhatian terhadap keterhubungan antara kemampuan individu dalam mengenali ancaman dan dukungan organisasi dalam menangani insiden keamanan digital.

Temuan ini dapat dibandingkan dengan penelitian Burda et al. (2026) yang mengkaji motivasi pegawai dalam melaporkan email *phishing*. Penelitian tersebut menemukan bahwa keinginan untuk melindungi organisasi dan rekan kerja merupakan pendorong utama pelaporan, diikuti oleh rasa tanggung jawab, kesadaran terhadap konsekuensi, dan perasaan tidak yakin terhadap keamanan pesan. Temuan tersebut memperlihatkan bahwa pelaporan ancaman tidak hanya berkaitan dengan kemampuan mengenali pesan mencurigakan, tetapi juga dengan kesadaran individu terhadap tanggung jawabnya dalam menjaga keamanan organisasi. Untuk konteks birokrasi, Sharon dan Sutanto (2026) juga menemukan bahwa literasi digital berpengaruh positif dan signifikan terhadap efektivitas reformasi birokrasi. Kedua penelitian tersebut memberikan perspektif bahwa kompetensi digital perlu didukung oleh penerapannya dalam pelaksanaan tugas dan tanggung jawab organisasi, termasuk ketika menghadapi

risiko keamanan informasi. Jika dikaitkan dengan penelitian ini, rendahnya frekuensi jawaban yang secara eksplisit menyebut pelaporan menunjukkan adanya aspek respons keamanan digital yang perlu mendapat perhatian lebih lanjut. Organisasi pemerintah tidak cukup hanya mendorong ASN agar mampu mengenali ancaman dan menghindarinya secara mandiri, tetapi juga perlu memastikan bahwa prosedur serta saluran pelaporan insiden dapat dipahami dan diakses dengan mudah. Dengan demikian, penguatan kompetensi keamanan digital ASN perlu mencakup pembiasaan tindakan pencegahan sekaligus pemahaman mengenai mekanisme penanganan insiden di lingkungan kerja. Namun, perbandingan ini perlu dilakukan secara hati-hati karena penelitian Burda et al. (2026) berfokus pada pegawai yang sebelumnya telah melaporkan email *phishing*, sedangkan penelitian ini menggunakan jawaban terbuka dari ASN mengenai tindakan yang akan mereka lakukan dalam suatu skenario hipotetis.

Penelitian Pourhashemi et al. (2026) juga relevan untuk memahami perbedaan antara pengetahuan mengenai ancaman dan kesiapan melakukan tindakan perlindungan. Dengan menggunakan *Protection Motivation Theory* (PMT), penelitian tersebut mengidentifikasi sejumlah faktor yang berkaitan dengan intensi pegawai untuk melindungi diri dari serangan *phishing*, termasuk persepsi terhadap tingkat keparahan dan kerentanan ancaman, efektivitas respons, hambatan, serta efikasi diri. Pengetahuan konseptual dan prosedural juga berhubungan dengan efikasi diri dalam melakukan tindakan perlindungan. Meskipun penelitian ini tidak mengukur konstruk PMT secara langsung, temuan Pourhashemi et al. (2026) membantu menjelaskan bahwa kemampuan mengenali penipuan digital perlu didukung oleh keyakinan dan pemahaman mengenai tindakan yang dapat dilakukan untuk menghadapi ancaman. Dalam lingkup ASN, tindakan tersebut dapat berupa tidak mengeklik tautan, memverifikasi identitas pengirim melalui kanal resmi, serta melaporkan pesan yang terindikasi sebagai upaya penipuan. Dengan demikian, pengenalan ancaman perlu ditempatkan sebagai tahap awal yang perlu diikuti dengan tindakan perlindungan yang sesuai.

Selain ancaman melalui pesan digital, penelitian ini juga menggali tindakan yang akan dilakukan responden apabila perangkat kerja hilang atau dicuri. Jawaban terbanyak adalah penggunaan cadangan data (*backup data*), sebanyak 72 responden (19,5%), diikuti pelaporan kepada pihak berwajib sebanyak 57 responden (15,4%), pengamanan dan pemblokiran akun sebanyak 53 responden (14,3%), serta pelaporan kepada instansi atau kantor sebanyak 48 responden (13,0%). Sebanyak 25 responden (6,8%) menyebutkan akan mengganti kata sandi, sementara 15 responden (4,1%) menyatakan akan melakukan penguncian perangkat dari jarak jauh. Variasi jawaban ini menunjukkan bahwa responden menyebutkan beberapa bentuk penanganan ketika menghadapi kehilangan perangkat kerja, baik yang berkaitan dengan pengamanan akses, pelaporan, maupun pemulihan data. Namun, setiap tindakan memiliki fungsi perlindungan yang berbeda. Misalnya penggunaan cadangan data lebih berkaitan dengan pemulihan informasi apabila data mengalami kehilangan, sedangkan pengamanan akun dan penguncian perangkat dari jarak jauh ditujukan untuk mengurangi kemungkinan akses oleh pihak yang tidak berwenang. Oleh karena itu, keberadaan tindakan pemulihan data saja belum cukup untuk memastikan bahwa informasi dalam perangkat yang hilang atau

dicuri telah terlindungi. Temuan ini memperlihatkan pentingnya pemahaman mengenai langkah penanganan yang mencakup pengamanan akses sekaligus pelaporan kepada pihak yang bertanggung jawab.

Hasil tersebut dapat dibaca bersama temuan Susanto dan Maulana (2024) serta Fadhil dan Yazid (2023) mengenai kesadaran keamanan informasi pegawai pemerintah. Kedua penelitian tersebut menyediakan pembanding untuk memahami bahwa keamanan informasi berkaitan dengan pengetahuan, sikap, dan perilaku pegawai, bukan hanya penguasaan pengetahuan teknis. Sementara itu, Sulaiman et al. (2022) membahas perilaku keamanan siber pegawai pemerintah melalui pendekatan PMT dan menyoroti pentingnya faktor-faktor yang berkaitan dengan perilaku protektif. Jika dikaitkan dengan penelitian ini, jawaban mengenai perangkat yang hilang atau dicuri menunjukkan bahwa responden telah menyebutkan beragam tindakan perlindungan, tetapi tindakan tersebut belum tentu mencerminkan pemahaman mengenai rangkaian penanganan insiden secara menyeluruh. Sebagai contoh, responden dapat menyebutkan pencadangan data sebagai langkah yang akan dilakukan, tetapi belum tentu memahami bahwa perangkat yang hilang juga perlu diamankan agar akses terhadap informasi di dalamnya tidak disalahgunakan. Meskipun demikian, karena data penelitian ini berupa jawaban atas skenario hipotetis, belum dapat dipastikan apakah responden benar-benar akan melakukan langkah-langkah tersebut secara berurutan atau sesuai prosedur ketika insiden terjadi. Dengan demikian, temuan ini lebih menggambarkan variasi tindakan yang diketahui atau dinyatakan responden daripada kemampuan aktual mereka dalam menangani insiden keamanan digital.

Dari sisi organisasi, Mwansa (2025) menekankan pentingnya dukungan kepemimpinan, pelatihan yang sesuai dengan kebutuhan pegawai, konsistensi kebijakan, serta prosedur penanganan dan pelaporan insiden dalam memperkuat kesadaran keamanan siber di instansi pemerintah. Perspektif tersebut relevan dengan temuan penelitian ini karena jawaban responden menunjukkan adanya variasi tindakan dalam menghadapi pesan mencurigakan maupun kehilangan perangkat kerja. Meskipun sebagian responden telah menyebutkan tindakan pengamanan akun dan pelaporan, jawaban terbuka belum menunjukkan apakah mereka memahami saluran pelaporan yang berlaku di instansinya atau mengetahui urutan penanganan insiden yang perlu dilakukan. Hal ini tidak serta-merta menunjukkan bahwa ASN tidak memahami prosedur atau bahwa instansi belum memiliki mekanisme penanganan insiden, sebab kedua aspek tersebut tidak diukur secara khusus dalam penelitian ini. Namun, temuan tersebut menunjukkan adanya ruang bagi organisasi untuk memastikan bahwa mekanisme penanganan insiden tidak hanya tersedia secara formal, tetapi juga dipahami dan dapat diterapkan oleh pegawai. Oleh karena itu, penguatan kompetensi keamanan digital ASN perlu diarahkan tidak hanya pada kemampuan mengenali ancaman, tetapi juga pada pembiasaan tindakan protektif dan pemahaman prosedur penanganan insiden. Upaya tersebut dapat dilakukan melalui pelatihan berbasis skenario, sosialisasi saluran pelaporan yang jelas, serta panduan penanganan insiden yang mudah diakses oleh pegawai. Upaya tersebut dapat mendukung penerapan kompetensi perlindungan data

dan privasi dalam DigComp 3.0, sekaligus memperkuat kesiapan organisasi dalam melindungi informasi yang dikelola dalam pelaksanaan pelayanan publik.

4. Kesimpulan

Penelitian ini menunjukkan bahwa keamanan informasi telah menjadi bagian dari praktik kerja digital yang secara positif dilaporkan oleh mayoritas ASN di lingkungan Pemerintah Provinsi DKI Jakarta. Kecenderungan tersebut terlihat dari tingginya persetujuan responden terhadap praktik pengamanan perangkat dan akun kerja, seperti menjaga keamanan perangkat secara mandiri, menggunakan kata sandi yang kuat, dan memastikan perangkat lunak keamanan berada dalam versi terbaru. Responden juga menunjukkan kecenderungan positif dalam membatasi pembagian data pribadi kepada pihak yang berkepentingan serta mengenali pesan atau tautan yang terindikasi sebagai upaya penipuan digital. Temuan ini memperlihatkan bahwa praktik keamanan informasi yang diteliti telah memperoleh perhatian dari sebagian besar responden dan relevan dengan kompetensi *Protecting Devices* serta *Protecting Personal Data and Privacy* dalam kerangka DigComp 3.0.

Meskipun demikian, jawaban responden terhadap skenario risiko menunjukkan bahwa pengenalan ancaman belum sepenuhnya diikuti oleh penyebutan tindakan penanganan yang menyeluruh. Pada skenario pesan mencurigakan, responden lebih banyak menyebutkan tindakan mengabaikan pesan, melakukan verifikasi, atau menghindari tautan, sedangkan pelaporan kepada pihak yang bertanggung jawab masih relatif jarang disebutkan. Sementara itu, pada skenario kehilangan atau pencurian perangkat, responden menyebutkan beragam tindakan, mulai dari pencadangan data hingga pengamanan akun dan pelaporan. Hal ini menunjukkan bahwa respons keamanan informasi tidak hanya berkaitan dengan kemampuan mengenali ancaman, tetapi juga pemahaman mengenai langkah penanganan yang tepat. Dengan demikian, tingginya persetujuan pada pertanyaan tertutup perlu dipahami sebagai praktik dan kemampuan yang dilaporkan responden, bukan sebagai bukti langsung atas keterampilan maupun perilaku aktual mereka dalam menghadapi insiden keamanan digital.

Berdasarkan temuan tersebut, pemerintah daerah perlu memperkuat keamanan informasi melalui pelatihan berbasis skenario yang tidak hanya meningkatkan kesadaran terhadap ancaman, tetapi juga membiasakan tindakan perlindungan dan penanganan insiden. Selain itu, instansi perlu menyediakan prosedur yang jelas dan mudah diakses mengenai pelaporan insiden, pengamanan akun, pembatasan akses, serta penanganan perangkat kerja yang hilang atau dicuri. Penguatan tersebut juga perlu didukung oleh kebijakan dan sistem keamanan organisasi agar tanggung jawab perlindungan informasi tidak hanya bergantung pada kesadaran individu ASN. Penelitian selanjutnya dapat melengkapi pendekatan kuesioner dengan wawancara, simulasi, atau pengamatan terhadap praktik keamanan informasi untuk memperoleh gambaran yang lebih mendalam mengenai kesesuaian antara tindakan yang dilaporkan dan penerapannya dalam pekerjaan sehari-hari.

5. Ucapan Terima Kasih

Penulis menyampaikan terima kasih kepada Kania Falahiatika, S.I.A. dan Fitria Ariyanti, S.I.A. selaku asisten dosen mata kuliah Praktik Penelitian Administrasi Publik Kelompok Negara 1 atas pendampingan dan dukungan yang diberikan selama proses penelitian berlangsung. Apresiasi juga disampaikan kepada seluruh mahasiswa mata kuliah Praktik Penelitian Administrasi Publik Kelompok Negara 1 yang telah berkontribusi dalam pelaksanaan penelitian, khususnya dalam proses pengumpulan data yang menjadi dasar penyusunan artikel ini. Artikel ini merupakan bagian dari pemanfaatan data penelitian bersama yang dikumpulkan melalui kegiatan mata kuliah Praktik Penelitian Administrasi Publik Kelompok Negara 1.

6. Daftar Pustaka

Ali, A., Faizan, R., Dominic, P. D., Azhar Ali, S. E., Rehman, M., & Sohail, A. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Kent Academic Repository, 11*(8). https://doi.org/10.3390/app11083383

Astrialita, P., & Nafi'ah, B. (2025). Tingkat Literasi Digital ASN Terhadap Aplikasi Kepegawaian Di Kabupaten Sidoarjo. *Jurnal Administrasi Publik dan Pemerintahan STISIP Imam Bonjol, 4*(1). https://doi.org/10.55850/simbol.v2i1

Burda, P., Allodi, L., Serebrenik, A., & Zannone, N. (2026). Phishing reporting in organizations: What motivates employees to take action?. *Information and Computer Security*, *34*(4), 562–589. https://doi.org/10.1108/ICS-02-2025-0037

Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. *Computers & Security, 142*. https://doi.org/10.1016/j.cose.2024.103858

Cosgrove, J., & Cachia, R. (2025). *DigComp 3.0: European Digital Competence Framework – Fifth Edition* (JRC Research Report No. JRC144121). Publications Office of the European Union. https://data.europa.eu/doi/10.2760/0001149

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior, 28*(5), 1849–1858. http://dx.doi.org/10.1016/j.chb.2012.05.003

Creswell, J.W. and Creswell, J.D. (2018) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage, Los Angeles.

Delso-Vicente, A., Diaz-Marcos, L., Aguado-Tevar, O., & Blanes-Sebastián, M. G. (2025). Factors influencing employee compliance with information security policies: a systematic literature review of behavioral and technological aspects in cybersecurity. *Future Business Journal, 11*(28), 1-16. https://doi.org/10.1186/s43093-025-00452-7

Destyana, D. P., Kurniawan, F. A., Azmiani, T. N., Putri, V. J., & Augustia, A. E. (2026). Analisis kebocoran data ASN oleh TopiAx: Etika, keamanan siber, dan perlindungan data pribadi. *JRIIN: Jurnal Riset Informatika dan Inovasi, 3*(8), 2288–2292. https://jurnalmahasiswa.com/index.php/jriin/article/view/3330

Fadhil, A., & Yazid, S. (2023). Measurement of employee information security awareness: A case study of National Civil Service Agency. *The Indonesian Journal of Computer Science*, *12*(6). https://doi.org/10.33022/ijcs.v12i6.3640

Finck, M., & Biega, A. J. (2021). Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems. *Technology and Regulation, 2021*, 44–61. https://doi.org/10.71265/z7r0t122

Izzuddin, N., & Yuswanto, A. (2025). Dashboard Security Awareness: Inovasi peningkatan kesadaran keamanan siber ASN di era digital. *Monas: Jurnal Inovasi Aparatur, 7*(2), 82–91. https://doi.org/10.54849/monas.v7i2.298

Khoironi, S. C. (2020). Pengaruh analisis kebutuhan pelatihan budaya keamanan siber sebagai upaya pengembangan kompetensi aparatur sipil negara di era digital. *Jurnal Studi Komunikasi dan Media, 24*(1), 37–56. https://doi.org/10.31445/jskm.2020.2945

Martinez, R. (2025). Digital Governance and Personal Data Protection: Proposals for an Ethical Public Transformation through the Privacy-by-Design Approach. *Salud, Ciencia y Tecnología - Serie de Conferencias, 4*. https://doi.org/10.56294/sctconf20251782

Marwenny, E., Syafwar, R., & Yani, P. (2024). Personal Data Protection in Public Services. Jurnal Ilmiah Ekotrans & Erudisi, 4(2), 74-85. https://doi.org/10.69989/yjew5p90

Mikiver, M., & Tupay, P. K. (2023). Has the GDPR killed e-government? The "once-only" principle vs the principle of purpose limitation. *International Data Privacy Law, 13*(3), 194–206. https://doi.org/10.1093/idpl/ipad010

Mufid, S. F., & Alkadry, A. U. (2026). Keamanan digital di era transformasi teknologi: Peran literasi dan perilaku dalam perlindungan diri. *Qolamuna: Keislaman, Pendidikan, Literasi dan Humaniora, 3*(1), 251–264. https://jurnal.qolamuna.id/index.php/JQ/article/view/406

Mulyadi, D., Mulyana, A., Carmenita, A., Utami, H. L., Aulia, K. A., Putri, M., & Alia, N. R. (2026). Implementasi Kebijakan Pemerintah terhadap Pencegahan Kebocoran Data Pribadi dalam Pelayanan Publik Berbasis Digital. *Jurnal Ilmu Sosial, Politik dan Humaniora, 11*(1), 1-15. https://doi.org/10.53697/iso.v6i1.3473

Musdalipa, R., Juangsah, & Jalil, B. (2026). Digital communication, artificial intelligence, and the transformation of law enforcement in Indonesia: Challenges and regulatory response. *ISIHUMOR: Jurnal Ilmu Sosial dan Humaniora, 4*(3), 480–495. https://doi.org/10.58540/isihumor.v4i3.1967

Mwansa, G. (2025). Cybersecurity awareness in government institutions: A systematic review of behavioral strategies and policy readiness. *Journal of Applied Informatics and Computing*, *9*(5), 2076–2088. https://doi.org/10.30871/jaic.v9i5.10041

Neuman, W. L. (2014). *Social research methods: Qualitative and quantitative approaches (7th ed.)*. Pearson Education Limited.

Pourhashemi, S. O., Naqvi, B., & Mehmandoost, M. A. (2026). Identifying factors influencing the employee's intention with self-protective behaviors against phishing attacks. *Information Technology & People*, *39*(8), 50–79. https://doi.org/10.1108/ITP-11-2024-1429

Republik Indonesia. (2018). *Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik*. Sekretariat Negara. https://peraturan.bpk.go.id/Details/96913/perpres-no-95-tahun-2018

Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. Kementerian Komunikasi dan Digital RI (JDIH Kemkomdigi). https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Salsabila, N., Fauzi, A., Ramadani, L., & Sari, A. N. (2025). Manajemen krisis dan respons insiden keamanan dalam era digital. *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen dan Keuangan, 2*(1). https://doi.org/10.63217/fibonacci.v2i1.253

Sharon, D., & Sutanto, B. (2026). Factors that influence the effectiveness of bureaucratic reform mediated by digital literacy. *ISIHUMOR: Jurnal Ilmu Sosial dan Humaniora*, *4*(2), 497–520. https://doi.org/10.58540/isihumor.v4i2.2117

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, *13*(9), Article 413. https://doi.org/10.3390/info13090413

Supit, B. F., & Pangalila, T. (2025). Kompetensi digital dan kinerja aparatur sipil negara di era birokrasi berbasis digital. *Konstruksi Sosial: Jurnal Penelitian Ilmu Sosial, 5*(3), 102–112. https://doi.org/10.56393/konstruksisosial.v5i3.3672

Susanto, T. D., & Maulana, M. D. (2024). Evaluating the influence of attitude versus knowledge and individual factor versus intervention factor on information security awareness in local government. *Procedia Computer Science*, *234*, 1428–1434. https://doi.org/10.1016/j.procs.2024.03.142

Vilander, J. (2021). *Bridging the knowing–doing gap: The role of attitude in information security awareness* [Master's thesis]. University of Jyväskylä. https://urn.fi/URN:NBN:fi:jyu-202105313312