Journal of Golden Generation Multidisciplinary
Volume: 2, Nomor: 2, (2026), April: 767 – 775
Link Publish: https://ejournal.lppnusantara.com/index.php/jggmultidisciplinary/article/view/716
E-ISSN: 3123-6278

Implementasi Kebijakan Keamanan Siber pada Pemerintah Daerah: Studi Kasus Diskominfo Kota Bogor

Muhammad Alfonzo Aprilio Irawan [1], Muhammad Husein Maruapey [2], Rita Rahmawati [3]
Program Magister Administrasi Publik, Universitas Djuanda Bogor [1,2,3]
Corresponding Author: *irwanalfonzo@gmail.com[1*], m.husein.maruapey@unida.ac.id[2], Rita.rahmawati@unida.ac.id[3]*

Info Artikel
Submitted: *19 Maret 2026*
Revised : *31 Maret 2026*
Accepted: *19 April 2026*
Published: *23 April 2026*

Keywords: *Cybersecurity Policy, Local Government, Policy Implementation, Diskominfo, Digital Governance*

Abstract
Cybersecurity has become a strategic issue in local digital governance because public services increasingly rely on electronic systems. Yet studies on local government cybersecurity still focus more on national strategy, public trust, or service quality than on implementation inside regional institutions. This study analyzes the implementation of cybersecurity policy at the Communication and Informatics Agency of Bogor City, identifies implementation challenges, and explains the role of society and the private sector. Using a qualitative narrative case study, data were collected through interviews with six key informants, observation, and document review in 2025. The findings show that the policy has been operationalized through regulatory compliance, data governance, encryption, access control, multi-factor authentication, firewall, IDS/IPS, routine system updates, and staff training. However, implementation remains limited by infrastructure, budget, trained personnel, and uneven cross-agency coordination. The study contributes an empirical explanation that local cybersecurity policy effectiveness depends on the linkage between regulation, technical controls, institutional capacity, and structured multi-stakeholder collaboration.

Kata Kunci*:* Keamanan Siber, Pemerintah Daerah, Implementasi Kebijakan, Diskominfo, Tata Kelola Digital

Abstrak
Keamanan siber menjadi isu strategis dalam tata kelola digital pemerintah daerah karena pelayanan publik semakin bergantung pada sistem elektronik. Namun, kajian kebijakan keamanan siber di daerah masih lebih banyak menyoroti strategi nasional, kepercayaan publik, atau kualitas layanan, belum pada proses implementasi di institusi daerah. Penelitian ini menganalisis implementasi kebijakan keamanan siber di Dinas Komunikasi dan Informatika Kota Bogor, mengidentifikasi tantangan implementasi, serta menjelaskan peran masyarakat dan sektor swasta. Penelitian menggunakan pendekatan kualitatif dengan desain studi kasus naratif melalui wawancara terhadap enam informan kunci, observasi, dan telaah dokumen pada 2025. Hasil penelitian menunjukkan bahwa kebijakan telah dioperasionalkan melalui kepatuhan regulatif, tata kelola data, enkripsi, kontrol akses, autentikasi multifaktor, firewall, IDS/IPS, pembaruan sistem, dan pelatihan pegawai. Meski demikian, implementasinya masih dibatasi oleh infrastruktur, anggaran, tenaga ahli, dan koordinasi lintas instansi yang belum merata. Kontribusi utama penelitian ini adalah menunjukkan bahwa efektivitas kebijakan keamanan siber di tingkat daerah bergantung pada keterhubungan antara regulasi, kontrol teknis, kapasitas institusional, dan kolaborasi multipihak yang terstruktur.

Publisher: Lembaga Penerbit Penelitian Nusantara

Pendahuluan

Transformasi digital telah memperluas penggunaan sistem elektronik pada pelayanan publik dan pada saat yang sama meningkatkan kerentanan pemerintah terhadap serangan siber, kebocoran data, serta gangguan terhadap kontinuitas layanan. Dalam konteks ini, keamanan siber tidak lagi dapat diperlakukan sebagai isu teknis semata, melainkan sebagai isu tata kelola publik yang menentukan integritas data, keberlanjutan operasi, dan kepercayaan masyarakat terhadap layanan pemerintah digital (Prayudi, 2018; Ramayanti & Lubis, 2023).

Literatur menunjukkan bahwa kebijakan keamanan siber yang memadai berhubungan dengan meningkatnya kepercayaan publik pada layanan elektronik pemerintah, meningkatnya kualitas pelayanan, dan berkurangnya risiko gangguan sistem (Susanti & Santoso, 2021; Pramudita & Yani, 2022). Di sisi lain, studi tentang risiko transformasi digital di sektor publik juga menegaskan bahwa perlindungan data, peningkatan kesadaran pengguna, dan penguatan infrastruktur menjadi syarat penting bagi efektivitas layanan digital (Pritam et al., 2020; Santoso et al., 2024).

Walaupun demikian, sebagian besar kajian terdahulu masih menempatkan keamanan siber pada level strategi nasional, kepercayaan publik terhadap e-government, persepsi masyarakat, atau kualitas layanan secara umum. Kajian yang secara khusus menelaah bagaimana kebijakan keamanan siber dioperasionalkan di instansi pemerintah daerah, bagaimana tantangan implementasinya, dan bagaimana kolaborasi multipihak dibangun di level organisasi masih relatif terbatas. Bahkan pada konteks Kota Bogor, fokus kajian sebelumnya belum secara mendalam memetakan hubungan antara regulasi, tata kelola data, pengamanan teknologi, kapasitas sumber daya manusia, dan kerja sama lintas pemangku kepentingan (Nurhaliza & Kurniawan, 2023).

Kota Bogor merupakan contoh penting karena pelayanan publiknya makin terhubung dengan infrastruktur digital, sementara Diskominfo Kota Bogor memegang fungsi sentral pada pengelolaan komunikasi, informatika, persandian, dan keamanan informasi pemerintah daerah. Tesis yang menjadi basis artikel ini menunjukkan adanya empat gap utama. Pertama, peningkatan kapasitas sumber daya manusia belum berlangsung secara konsisten dan menyeluruh. Kedua, penguatan infrastruktur keamanan masih dihadapkan pada keterbatasan perangkat, pembaruan sistem, dan anggaran. Ketiga, kesadaran masyarakat mengenai perlindungan data pribadi dan ancaman siber belum merata. Keempat, kolaborasi antara pemerintah daerah, sektor swasta, dan unsur masyarakat masih berjalan terbatas dan belum sepenuhnya terstruktur.

Dari sudut pandang kebijakan publik, kondisi tersebut menegaskan bahwa keberhasilan

kebijakan tidak cukup ditentukan oleh adanya regulasi formal, tetapi juga oleh pilihan pemerintah dalam mengorganisasi sumber daya, menetapkan prioritas, dan mengarahkan tindakan implementasi (Dye, 1975; Madani, 2011). Dari perspektif keamanan informasi, perlindungan atas kerahasiaan, integritas, dan ketersediaan data menuntut pengendalian yang sistematis, penilaian risiko, serta penguatan prosedur operasional yang konsisten (Whitman & Mattord, 2010; ISO/IEC 27001, 2013). Sementara itu, pendekatan good governance menempatkan akuntabilitas, transparansi, dan kolaborasi lintas aktor sebagai prasyarat untuk membangun tata kelola digital yang responsif dan berkelanjutan (Grindle, 2007; Kooiman, 2003; UNESCAP, 2009).

Berdasarkan kerangka tersebut, artikel ini bertujuan untuk menganalisis implementasi kebijakan keamanan siber di Diskominfo Kota Bogor, mengidentifikasi tantangan yang dihadapi dalam implementasi, dan menjelaskan peran masyarakat serta sektor swasta dalam mendukung kebijakan tersebut. Kebaruan artikel terletak pada pemetaan empiris mengenai bagaimana efektivitas kebijakan keamanan siber pemerintah daerah dibentuk oleh keterhubungan antara regulasi, kontrol teknis, kapasitas institusional, dan kolaborasi multipihak. Dengan demikian, artikel ini tidak hanya menyajikan gambaran implementasi kebijakan, tetapi juga menawarkan penjelasan tentang mengapa kebijakan yang secara normatif sudah tersedia masih menghadapi hambatan ketika dijalankan pada level organisasi pemerintah daerah.

Metode Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan desain studi kasus naratif untuk memahami implementasi kebijakan keamanan siber pada satu institusi pemerintah daerah secara mendalam. Pilihan ini sejalan dengan karakter penelitian kualitatif yang menekankan pemaknaan atas proses, konteks, dan pengalaman aktor yang terlibat dalam objek penelitian (Creswell, 2014). Penelitian dilaksanakan di Dinas Komunikasi dan Informatika Kota Bogor pada 2025.

Subjek penelitian dipilih secara purposif dari unsur yang secara langsung terlibat dalam tata kelola keamanan siber, yaitu Kepala Diskominfo Kota Bogor, Sekretaris Diskominfo, Kepala Bidang Persandian dan Keamanan Informasi, Analis Kebijakan Ahli Muda selaku Ketua Tim Tata Kelola Persandian dan Keamanan Informasi, Penelaah Teknis Kebijakan pada bidang yang sama, serta Pranata Komputer Ahli Muda. Data primer diperoleh melalui wawancara mendalam, sedangkan data pendukung diperoleh melalui observasi dan studi dokumentasi terhadap kebijakan, prosedur, dan dokumen organisasi yang relevan.

Analisis data dilakukan secara induktif melalui tahapan reduksi data, penyajian data, dan

verifikasi untuk menemukan pola implementasi, kendala, dan hubungan antartemuan. Keabsahan data dijaga melalui member checking dan triangulasi sumber serta teknik. Melalui prosedur ini, hasil penelitian diarahkan untuk tetap konsisten dengan fokus masalah, yaitu implementasi kebijakan, tantangan pelaksanaan, dan dukungan masyarakat serta sektor swasta terhadap keamanan siber di Kota Bogor.

Hasil dan Pembahasan

Hasil

Temuan penelitian menunjukkan bahwa implementasi kebijakan keamanan siber di Diskominfo Kota Bogor telah berkembang dari level normatif menuju level operasional. Kebijakan tidak berhenti pada rujukan regulasi, tetapi mulai diterjemahkan ke dalam tata kelola data, kontrol teknis, prosedur respons insiden, dan peningkatan kapasitas aparatur. Meski demikian, derajat implementasi setiap komponen masih belum seimbang. Ringkasan temuan utama disajikan pada Tabel 1.

Tabel 1. Ringkasan temuan utama implementasi kebijakan keamanan siber di Diskominfo Kota Bogor

Dimensi	Temuan inti	Implikasi
Regulasi dan tata kelola	Berbasis UU ITE, PP 71/2019, arahan BSSN, perlindungan data pribadi, dan rujukan ISO/IEC 27001.	Ada dasar kebijakan yang jelas untuk perlindungan data dan sistem pemerintah.
Kontrol teknis	Enkripsi, kontrol akses berbasis peran, autentikasi multifaktor, firewall, IDS/IPS, backup, dan prosedur respons insiden.	Kebijakan mulai diterjemahkan ke pengamanan operasional yang berlapis.
Kapasitas organisasi	Pelatihan dan sosialisasi sudah dilakukan, tetapi belum menutup kebutuhan tenaga ahli dan pembaruan sistem.	Terdapat gap antara komitmen kebijakan dan kapasitas implementasi.
Tantangan utama	Infrastruktur terbatas, anggaran terbatas, kekurangan SDM terlatih, dan koordinasi lintas instansi belum optimal.	Efektivitas kebijakan belum merata dan respons terhadap ancaman bisa

		melambat.
Kolaborasi eksternal	Masyarakat dibutuhkan untuk literasi dan pelaporan dini; sektor swasta dibutuhkan untuk teknologi dan pelatihan.	Keamanan siber daerah membutuhkan ekosistem kolaboratif, bukan hanya intervensi internal pemerintah.

Pada dimensi regulasi dan tata kelola, Diskominfo Kota Bogor mendasarkan kebijakan keamanan sibernya pada Undang-Undang Informasi dan Transaksi Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, ketentuan dari Badan Siber dan Sandi Negara, serta prinsip perlindungan data pribadi. Orientasi kebijakan diarahkan pada perlindungan kerahasiaan, integritas, dan ketersediaan data publik. Di tingkat implementasi, organisasi juga merujuk pada ISO/IEC 27001 sebagai acuan manajemen keamanan informasi, terutama untuk kontrol akses, pengelolaan risiko, dan perlindungan data sensitif.

Pada dimensi operasional, Diskominfo telah mengembangkan sejumlah pengamanan yang bersifat teknis dan prosedural. Temuan lapangan menunjukkan adanya penggunaan enkripsi untuk data sensitif, pembatasan hak akses berbasis peran, autentikasi multifaktor, firewall, dan sistem deteksi serta pencegahan intrusi. Selain itu, terdapat audit berkala, pembaruan perangkat lunak dan patch keamanan, mekanisme pencadangan dan pemulihan data, serta prosedur tanggap darurat ketika terjadi pelanggaran atau kebocoran data. Keberadaan tim keamanan siber atau CSIRT memperlihatkan bahwa organisasi mulai membangun respons kelembagaan terhadap insiden siber.
Pada dimensi kapasitas organisasi, Diskominfo juga telah melakukan pelatihan dan sosialisasi bagi pegawai mengenai keamanan data pribadi, kepatuhan terhadap prosedur, dan ancaman siber yang terus berkembang. Namun, hasil penelitian menunjukkan bahwa penguatan kapasitas ini belum sepenuhnya mampu menutup kebutuhan organisasi. Tantangan yang paling menonjol adalah keterbatasan infrastruktur teknologi informasi yang aman dan mutakhir, keterbatasan anggaran untuk pembaruan perangkat, serta kekurangan tenaga yang memiliki keahlian spesifik di bidang keamanan siber. Keterbatasan ini membuat kebijakan yang secara formal sudah ada belum selalu dapat dijalankan secara optimal dan merata.

Pada dimensi kolaborasi, penelitian menunjukkan bahwa Diskominfo memandang masyarakat dan sektor swasta sebagai bagian penting dari ekosistem keamanan siber daerah. Masyarakat dibutuhkan sebagai pengguna layanan digital yang sadar terhadap perlindungan data pribadi dan mampu melaporkan insiden secara dini. Sektor swasta dinilai penting karena dapat

menyediakan teknologi yang lebih canggih, dukungan teknis, dan pelatihan bagi aparatur pemerintah. Di sisi lain, koordinasi lintas instansi masih menjadi pekerjaan rumah. Kolaborasi dengan lembaga nasional dan sektor swasta sudah ada, tetapi belum sepenuhnya terstruktur sebagai mekanisme kelembagaan yang rutin dan terintegrasi.

Pembahasan

Temuan penelitian menegaskan bahwa implementasi kebijakan keamanan siber pada pemerintah daerah perlu dipahami sebagai proses kebijakan publik, bukan sekadar adopsi perangkat teknologi. Sesuai pandangan Dye (1975) dan Madani (2011), kebijakan menjadi nyata ketika pilihan pemerintah diterjemahkan ke dalam tindakan organisasi, pengalokasian sumber daya, dan prosedur kerja yang dapat dijalankan. Dalam kasus Diskominfo Kota Bogor, komitmen kebijakan tampak pada penggunaan regulasi nasional sebagai dasar, pembentukan pengaturan internal, dan pengembangan mekanisme pengamanan data serta respons insiden. Artinya, kebijakan sudah bergerak dari level pernyataan normatif menuju level tindakan birokratis.

Dari perspektif keamanan informasi, praktik yang ditemukan memperlihatkan adanya upaya memenuhi prinsip kerahasiaan, integritas, dan ketersediaan data melalui enkripsi, kontrol akses, autentikasi multifaktor, firewall, IDS/IPS, backup, dan pemulihan data. Hal ini sejalan dengan Whitman dan Mattord (2010), Stallings (2017), serta kerangka ISO/IEC 27001 (2013) yang menekankan bahwa keamanan informasi mensyaratkan pengendalian yang sistematis dan berlapis. Namun demikian, hasil penelitian juga menunjukkan bahwa kepatuhan terhadap standar belum otomatis menjamin efektivitas implementasi. Kesenjangan antara komitmen regulatif dan kapasitas nyata organisasi masih terlihat pada keterbatasan perangkat, pembaruan sistem, dan jumlah personel terlatih. Dengan kata lain, standar dapat berfungsi sebagai arah, tetapi keberhasilan implementasi tetap ditentukan oleh kesiapan institusional.

Hasil ini menguatkan penelitian terdahulu yang menyatakan bahwa kebijakan keamanan siber berkontribusi pada kualitas layanan dan kepercayaan publik ketika perlindungan data dan stabilitas sistem dapat dijaga (Prayudi, 2018; Susanti & Santoso, 2021; Pramudita & Yani, 2022). Akan tetapi, artikel ini memperluas temuan tersebut dengan menunjukkan bahwa pada level pemerintah daerah, persoalan utama bukan hanya pada ada atau tidaknya kebijakan, melainkan pada kemampuan organisasi mengoperasionalkan kebijakan secara berkelanjutan. Di sinilah letak kontribusi empiris artikel ini: efektivitas kebijakan keamanan siber di daerah sangat bergantung pada hubungan antar empat unsur, yaitu regulasi, kontrol teknis, kapasitas sumber daya, dan koordinasi antarpemangku kepentingan.

Dari sudut good governance, temuan tentang pentingnya kolaborasi dengan masyarakat, sektor swasta, dan lembaga nasional sejalan dengan pandangan Grindle (2007), Kooiman (2003), dan UNESCAP (2009) bahwa tata kelola yang baik menuntut akuntabilitas, keterbukaan, dan kerja sama antaraktor. Dalam isu keamanan siber, kolaborasi bukan sekadar pelengkap, melainkan komponen inti. Ancaman siber berkembang terlalu cepat untuk ditangani oleh satu organisasi secara terisolasi. Karena itu, keterlibatan masyarakat melalui literasi digital, pelaporan insiden, dan penggunaan layanan yang lebih aman menjadi faktor pendukung implementasi. Demikian pula, sektor swasta dapat memperkuat kemampuan daerah melalui transfer teknologi, dukungan teknis, dan pelatihan. Temuan ini juga sejalan dengan kajian yang menempatkan kampanye kesadaran dan kemitraan lintas sektor sebagai bagian penting dari penguatan keamanan siber (Pritam et al., 2020; Wibowo & Setiawan, 2023).

Secara substantif, kebaruan artikel ini tidak terletak pada penemuan model teknis baru, melainkan pada penjelasan yang lebih terstruktur tentang logika implementasi kebijakan keamanan siber di level pemerintah daerah. Studi ini menunjukkan bahwa walaupun Diskominfo Kota Bogor telah mengadopsi berbagai instrumen pengamanan, hambatan kapasitas dapat memperlambat respons, membatasi ruang pembaruan teknologi, dan membuat kolaborasi eksternal belum berkembang menjadi mekanisme yang mapan. Dengan demikian, kebijakan keamanan siber daerah seharusnya dinilai tidak hanya dari kepatuhan terhadap regulasi, tetapi juga dari tingkat kesiapan kelembagaan dan kemampuannya membangun ekosistem keamanan yang kolaboratif.

Artikel ini tetap memiliki keterbatasan karena berfokus pada satu instansi dan menggunakan desain kualitatif, sehingga hasilnya tidak ditujukan untuk generalisasi statistik. Namun demikian, fokus tersebut justru memberi kedalaman analisis mengenai dinamika implementasi kebijakan yang sering tidak tertangkap dalam studi yang lebih luas. Penelitian selanjutnya dapat memperluas cakupan pada perbandingan antardaerah, mengintegrasikan indikator kuantitatif kesiapan keamanan siber, atau menilai keterkaitan antara tingkat maturitas keamanan siber dan kualitas pelayanan publik daerah.

SIMPULAN

Penelitian ini menunjukkan bahwa implementasi kebijakan keamanan siber di Diskominfo Kota Bogor telah berjalan melalui tiga jalur utama, yaitu penguatan regulasi dan tata kelola data, penerapan kontrol teknis keamanan, serta peningkatan kapasitas aparatur. Dalam praktiknya, organisasi telah menggunakan rujukan regulatif nasional, mengadopsi prinsip ISO/IEC 27001,

menerapkan enkripsi, kontrol akses, autentikasi multifaktor, firewall, IDS/IPS, audit sistem, pembaruan perangkat lunak, serta prosedur respons insiden. Temuan ini menegaskan bahwa keamanan siber mulai diposisikan sebagai bagian dari tata kelola pemerintahan digital, bukan sekadar isu teknis di level operasional.

Akan tetapi, efektivitas implementasi kebijakan masih dibatasi oleh keterbatasan infrastruktur teknologi, anggaran, dan tenaga ahli keamanan siber, serta koordinasi lintas instansi yang belum sepenuhnya terstruktur. Karena itu, keberhasilan kebijakan tidak cukup hanya bertumpu pada regulasi formal dan pengadaan teknologi, tetapi perlu ditopang oleh penguatan kapasitas kelembagaan dan kolaborasi multipihak yang berkelanjutan. Dalam konteks Kota Bogor, masyarakat dan sektor swasta perlu diposisikan sebagai mitra strategis untuk memperkuat literasi digital, pelaporan insiden, transfer teknologi, dan pelatihan. Dengan arah tersebut, penguatan keamanan siber dapat berkontribusi langsung pada ketahanan pemerintahan digital dan peningkatan kualitas layanan publik daerah.

DAFTAR PUSTAKA

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches. SAGE Publications.

Dye, T. R. (1975). Understanding public policy. Duxbury Press.

Grindle, M. S. (2007). Good enough governance: Poverty reduction and reform in developing countries. Governance, 20(4), 533-548.

ISO/IEC 27001. (2013). Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization.

Kooiman, J. (2003). Governing as governance. SAGE Publications.

Madani, M. (2011). Pengantar teori dan analisis kebijakan publik. Alfabeta.

Nurhaliza, S., & Kurniawan, A. (2023). Analisis kebijakan keamanan siber di pemerintahan daerah: Studi kasus Kota Bogor. [PERLU DILENGKAPI data publikasi].

Pramudita, D., & Yani, A. (2022). Kebijakan keamanan siber dan implikasinya terhadap kualitas pelayanan publik. [PERLU DILENGKAPI data publikasi].

Prayudi. (2018). Keamanan siber dan pembangunan demokrasi di Indonesia. [PERLU DILENGKAPI data publikasi].

Pritam, A., Almulla, M., & Cullen, A. (2020). A survey of cybersecurity awareness programs and campaigns. Computers & Security, 96, 101891.

Ramayanti, D., & Lubis, A. H. (2023). Tinjauan literatur: Keamanan siber pada sistem pemerintahan

berbasis elektronik. Jurnal Teknologi Informasi dan Ilmu Komputer, 10(6), 1345-1354.

Santoso, F. B., Pujianto, R., & Ramadhan, T. (2024). Strategi penanganan keamanan siber (cyber security) di Indonesia. [PERLU DILENGKAPI data publikasi].

Stallings, W. (2017). Cryptography and network security: Principles and practice. Pearson Education.

Susanti, N., & Santoso, B. (2021). Pengaruh kebijakan keamanan siber terhadap kepercayaan publik di layanan e-government. [PERLU DILENGKAPI data publikasi].

UNESCAP. (2009). What is good governance? United Nations Economic and Social Commission for Asia and the Pacific.

Whitman, M. E., & Mattord, H. J. (2010). Principles of information security. Course Technology.

Wibowo, A., & Setiawan, D. (2023). Peran kolaborasi sektor publik dan privat dalam keamanan siber. Jurnal Manajemen dan Bisnis, 16(4), 289-296.