KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Nusantara (JINU)
Vol.3, No.6 November 2026
e-ISSN: 3047-7603, p-ISSN :3047-9673, Hal 14-28
DOI : https://doi.org/10.61722/jinu.v3i6.11599

Dilema Etika BYOD antara Perlindungan Aset Digital Organisasi dan Privasi Karyawan

Evy Nurmiati[1], Muhammad Adha Darojat[2]
[1,2] Universitas Islam Negeri Syarif Hidayatullah
*Penulis Korespondensi: [1] evy.nurmiati@uinjkt.ac.id, [2] muhammad.adha24@mhs.uinjkt.ac.id

Abstract. *The Bring Your Own Device (BYOD) paradigm has become a global trend offering operational efficiency and flexibility for modern organizations. However, integrating personal devices into corporate networks raises serious information security challenges and ethical dilemmas regarding data privacy. This research employs a systematic literature review to analyze BYOD security challenges and ethical dilemmas within the context of data protection regulations. Findings indicate that while BYOD significantly enhances productivity, many organizations still lack comprehensive security policies. Furthermore, there exists an inherent tension between corporate demands for asset monitoring via Mobile Device Management (MDM) software and employee privacy rights. Results also highlight environmental aspects, where uncontrolled BYOD usage potentially increases the corporate carbon footprint. This research concludes that developing frameworks integrating technical controls with professional ethics and legal compliance is crucial. Transparent policy formulation and fostering a strong security culture are essential keys to balancing corporate asset protection with full respect for employee privacy rights in the era of digital transformation.*

Keywords: *Bring Your Own Device (BYOD), Data Breach, Data Privacy, IT Ethics Information Security, Security Policy.*

Abstrak. Paradigma kerja Bring Your Own Device (BYOD) telah menjadi tren global yang menawarkan efisiensi operasional serta fleksibilitas tinggi bagi organisasi modern. Namun, integrasi perangkat pribadi ke dalam jaringan perusahaan menimbulkan tantangan keamanan informasi yang serius serta dilema etika terkait privasi data. Penelitian ini menggunakan metode studi literatur untuk menganalisis tantangan keamanan BYOD dan dilema etika yang muncul dalam konteks kepatuhan terhadap regulasi pelindungan data pribadi. Hasil analisis menunjukkan bahwa meskipun BYOD terbukti meningkatkan produktivitas, banyak organisasi masih minim dalam menerapkan kebijakan keamanan yang komprehensif. Selain itu, terdapat ketegangan antara tuntutan perusahaan untuk memonitor aset data melalui perangkat lunak manajemen perangkat seluler dan hak privasi individu karyawan. Temuan juga menyoroti aspek lingkungan di mana penggunaan perangkat BYOD yang tidak terkontrol berpotensi meningkatkan jejak karbon secara signifikan. Penelitian ini menyimpulkan bahwa pengembangan kerangka kerja yang tidak hanya mengandalkan kontrol teknis, tetapi juga mengintegrasikan etika profesi serta kepatuhan hukum sangatlah penting. Perumusan kebijakan yang transparan serta pembangunan budaya keamanan siber yang kuat menjadi kunci utama dalam menyeimbangkan perlindungan aset korporat dengan penghormatan penuh terhadap hak privasi pekerja di era transformasi digital.

Kata kunci: Bring Your Own Device (BYOD), Etika Profesional TI, Kebocoran Data, Keamanan Informasi, Kebijakan Keamanan.

1. LATAR BELAKANG

Perkembangan teknologi informasi pada era digital saat ini telah membawa perubahan yang sangat fundamental dalam berbagai aspek kehidupan, termasuk dalam cara kerja dan operasional sebuah organisasi (Halim et al., 2024). Hal ini memunculkan sebuah tren yang dikenal dengan istilah konsumerisasi di bidang teknologi informasi, di

Naskah Masuk: 01 Juli 2026; Revisi: 02 Juli 2026; Diterima: 02 Juli 2026; Terbit: 04 Juli 2026

mana para pengguna secara aktif mengadopsi dan mengintegrasikan perangkat pribadi mereka ke dalam sektor bisnis maupun lingkungan institusi pendidikan (Mitra, 2013). Fenomena ini kemudian melahirkan sebuah paradigma kerja operasional yang dikenal secara luas dengan sebutan *Bring Your Own Device* (BYOD) (Mega Puspita & Hasanudin, 2022). Konsep yang pada awalnya diusulkan pada tahun 2009 oleh Malcolm Harkins dari Intel ini (Priyo Hadi Nugroho & Achmad Darajatun, 2021), secara fundamental mengizinkan karyawan untuk menggunakan perangkat komputasi bergerak milik pribadi guna mengakses jaringan dan menyelesaikan berbagai tugas harian perusahaan (Halim et al., 2024; Mega Puspita & Hasanudin, 2022). Seiring berjalannya waktu, adopsi BYOD terbukti memberikan keuntungan ganda; perusahaan dapat menekan biaya pengadaan dan pemeliharaan perangkat operasional secara drastic (Mitra, 2013; Priyo Hadi Nugroho & Achmad Darajatun, 2021), sementara karyawan menikmati tingkat kenyamanan dan produktivitas yang jauh lebih tinggi karena bekerja menggunakan antarmuka sistem operasi yang telah dikuasai secara personal. Fenomena ini mencapai puncaknya semenjak pandemi Covid-19 yang memaksa peralihan masif menuju sistem kerja dari rumah atau *Work From Home* (WFH) (Mega Puspita & Hasanudin, 2022).

Meskipun menawarkan efisiensi yang luar biasa, integrasi konsep BYOD ke dalam infrastruktur organisasi tidak luput dari ancaman serta risiko keamanan informasi yang sangat serius (Halim et al., 2024). Ketika sebuah perusahaan mengizinkan penggunaan perangkat pribadi, infrastruktur dan data yang sebelumnya terlindungi rapat di lingkungan tertutup berubah menjadi terekspos di lingkungan luar yang serba terbuka (Mitra, 2013). Dalam skenario ini, perusahaan kehilangan kendali penuh atas keamanan perangkat keras dan lunak, sehingga karyawan sering kali dianggap sebagai mata rantai keamanan yang paling rapuh (Halim et al., 2024). Kurangnya literasi keamanan membuat pekerja sangat rentan terhadap penipuan berkedok *phishing* maupun infeksi *malware* (Nurillah & Trihandoyo, 2024), yang juga dapat menyusup melalui instalasi aplikasi pihak ketiga yang tidak tepercaya (Mitra, 2013). Kerentanan jaringan akan semakin diperparah apabila pengguna memodifikasi sistem operasi melalui teknik *jailbreaking* atau *rooting* (Nurillah & Trihandoyo, 2024), serta konektivitas pada jaringan nirkabel publik yang tidak terenkripsi (Mitra, 2013), (Nurillah & Trihandoyo, 2024). Apabila serangkaian ancaman

siber ini tidak diantisipasi secara komprehensif, fenomena BYOD berpotensi berubah menjadi malapetaka bagi stabilitas organisasi (Mega Puspita & Hasanudin, 2022).

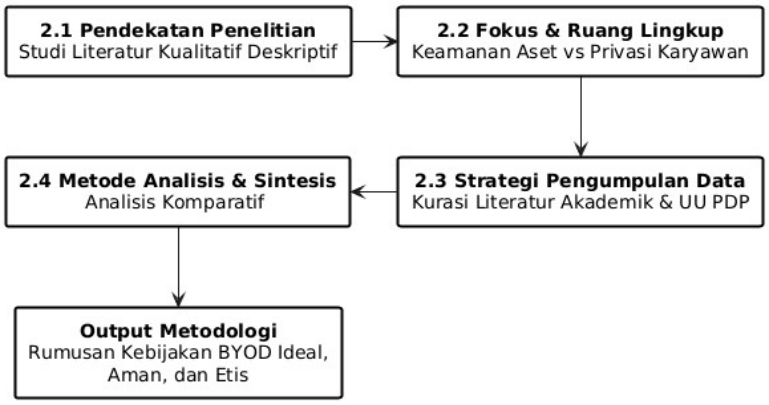
Dalam menghadapi ancaman teknis tersebut, perusahaan umumnya mengimplementasikan kontrol manajemen terpusat menggunakan *Mobile Device Management* (MDM) (Mega Puspita & Hasanudin, 2022). Namun, penerapan teknologi pengawasan ini memicu dilema etika yang kompleks antara menjaga keamanan aset perusahaan dan potensi pelanggaran privasi personal karyawan, mengingat adanya percampuran antara data korporat dengan data privasi seperti foto, kontak, dan surel personal di dalam satu perangkat (Mitra, 2013), (Nurillah & Trihandoyo, 2024). Dilema ini menjadi ujian krusial bagi praktisi keamanan siber dalam menjaga tiga pilar utama: kerahasiaan, integritas, dan ketersediaan data [1].

Guna mengurai kompleksitas tersebut, organisasi dituntut merumuskan kerangka kerja yang tidak hanya mengandalkan pendekatan teknologi, melainkan harus menyeimbangkannya dengan nilai-nilai etika profesi serta kepatuhan terhadap regulasi nasional, yaitu Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP) (Pemerintah Republik Indonesia, 2022). Implementasi BYOD yang ideal mewajibkan pemenuhan lima dimensi kontrol keamanan, yaitu kontrol data, akses, jaringan, manajemen perangkat, serta penyusunan kerangka regulasi non-teknis (Mitra, 2013), yang harus didukung oleh kebijakan transparan dan pembangunan budaya keamanan *(security culture)* melalui pelatihan karyawan (Halim et al., 2024). Berangkat dari problematika tersebut, artikel ini difokuskan guna membedah dilema etika kebijakan BYOD sekaligus merumuskan pedoman strategis yang mampu menyeimbangkan keamanan aset korporat dengan penghormatan penuh terhadap hak privasi individu.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode Studi Literatur (*Narrative Literature Review*). Metode studi literatur merupakan serangkaian proses mengumpulkan, meninjau, dan menyintesis literatur yang relevan untuk membangun landasan pemahaman yang mendalam mengenai topik tertentu tanpa

melakukan intervensi langsung ke lapangan (Snyder, 2019). Dalam konteks naskah ini, metode tersebut diterapkan untuk mengevaluasi secara kritis kebijakan keamanan dari penerapan *Bring Your Own Device* (BYOD) di berbagai organisasi, dan keselarasan implementasinya terhadap regulasi pelindungan data pribadi. Secara visual, tahapan metodologi dalam penelitian ini dapat dilihat pada Gambar 1.



Gambar 1 Metodologi Penelitian

Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi literatur. Fokus utama dari metode ini adalah melakukan eksplorasi, analisis, dan interpretasi mendalam terhadap berbagai referensi yang relevan dengan topik kebijakan *Bring Your Own Device*. Berbeda dengan metode kuantitatif yang mengandalkan data numerik, studi literatur ini memberikan ruang bagi peneliti untuk melakukan telaah kritis terhadap berbagai perspektif teoretis yang tersebar dalam literatur akademik. Pendekatan ini memungkinkan penulis untuk membedah kompleksitas fenomena BYOD yang dinamis serta melakukan sintesis antar konsep dari berbagai sumber yang berkaitan dengan dinamika hukum dan teknologi secara komprehensif.

Penentuan Fokus dan Ruang Lingkup Kajian

Langkah awal dalam penelitian ini adalah merumuskan batasan isu utama yang akan dianalisis. Fokus permasalahan ditekankan pada dialektika antara kebutuhan organisasi dalam melindungi aset informasi dan kewajiban hukum untuk menjaga hak privasi pemilik perangkat. Dalam tahap ini, penulis melakukan pemetaan spektrum permasalahan mulai dari aspek operasional, risiko keamanan, hingga implikasi etika

profesi yang sangat krusial dalam mencegah insiden kebocoran data di lingkungan organisasi(Suci Anugrah et al., 2025). Ruang lingkup kajian dibatasi pada tantangan implementasi BYOD di lingkungan organisasi modern yang dituntut untuk patuh terhadap regulasi privasi data yang berlaku, khususnya setelah diterbitkannya Undang-Undang Pelindungan Data Pribadi di Indonesia. Pembatasan fokus ini bertujuan agar analisis tetap tajam dan tidak melebar ke aspek teknis yang tidak relevan dengan esensi etika serta keamanan data yang diangkat.

Strategi Pengumpulan Data

Pengumpulan data dalam penelitian ini dilakukan sepenuhnya melalui metode studi kepustakaan dengan memanfaatkan berbagai literatur akademik yang kredibel sebagai sumber informasi utama. Strategi pemilihan referensi dilakukan secara selektif dengan mengutamakan literatur yang memberikan kontribusi fundamental terhadap topik kontrol akses, implementasi perangkat lunak Mobile Device Management, serta analisis mengenai dampak BYOD terhadap produktivitas dan psikologi pengguna. Selain artikel dari jurnal ilmiah, penelitian ini juga mengintegrasikan referensi dari prosiding konferensi teknologi informasi serta dokumen regulasi hukum terkait pelindungan data pribadi.

Pemilihan sumber data tersebut tidak dilakukan dengan teknik penapisan massal yang mekanis, melainkan melalui kurasi yang mendalam untuk memastikan bahwa setiap literatur yang digunakan memiliki keterkaitan kuat dengan fokus penelitian. Dengan mengkombinasikan berbagai perspektif dari banyak sumber, penelitian ini berupaya membangun argumen yang komprehensif dan tidak parsial. Dokumen regulasi resmi ditempatkan sebagai referensi dasar untuk memastikan setiap analisis mengenai etika privasi memiliki landasan normatif yang kuat dan sesuai dengan konteks hukum yang berlaku di Indonesia, mengingat kegagalan etis sering kali menjadi akar permasalahan dari insiden pelanggaran data privasi (Siti et al., 2026).

Metode Analisis dan Sintesis Literatur

Literatur yang telah terkumpul kemudian ditelaah secara mendalam melalui proses analisis deskriptif dan komparatif. Tahap ini dimulai dengan membedah argumen

mendasar dari masing-masing literatur utama untuk memahami pola pikir dan metodologi yang digunakan oleh peneliti sebelumnya. Setelah setiap literatur dipahami intisarinya, langkah selanjutnya adalah melakukan komparasi antar temuan guna mengidentifikasi persamaan, perbedaan, serta celah dalam strategi penanganan BYOD antar organisasi. Proses terakhir adalah sintesis konseptual, di mana hasil telaah dari berbagai sumber tersebut dirangkai kembali menjadi satu narasi yang utuh. Sintesis ini bertujuan untuk menghasilkan rumusan konseptual atau rekomendasi terkait kerangka kebijakan BYOD yang ideal, yang tidak hanya aman dari sisi arsitektur teknologi informasi, tetapi juga etis serta patuh terhadap regulasi privasi data yang berlaku saat ini.

3. HASIL DAN PEMBAHASAN

Berdasarkan tinjauan menyeluruh terhadap berbagai literatur, implementasi *Bring Your Own Device* (BYOD) telah berevolusi secara fundamental dari sekadar tren teknologi sesaat menjadi paradigma operasional standar yang tidak dapat dihindari di berbagai sektor industri maupun akademik. Dalam diskursus keilmuan Sistem Informasi, fenomena ini tidak lagi hanya dipandang sebagai perubahan fasilitas keras, melainkan sebuah disrupsi terhadap arsitektur perusahaan *(enterprise architecture)* secara keseluruhan. Meskipun menawarkan fleksibilitas yang sangat menggiurkan bagi peningkatan produktivitas dan kepuasan individu, penerapan kebijakan ini secara praktis membawa lapisan kompleksitas baru. Organisasi kini dituntut untuk menghadapi tantangan berlapis yang mencakup restrukturisasi manajemen infrastruktur jaringan, mitigasi risiko keamanan data tingkat lanjut, hingga pertimbangan implikasinya terhadap keberlanjutan lingkungan dan *Green Computing*.

Tren Adopsi dan Efisiensi Operasional BYOD

Penerapan ekosistem BYOD mendapatkan dukungan yang sangat masif dan hampir universal di berbagai struktur organisasi modern. Sebagai gambaran konkrit, sebanyak 97,5% organisasi dalam sebuah observasi empiris di wilayah Malaysia secara terbuka menyatakan dukungan penuh terhadap amalan operasional ini (Abdul et al., 2018). Jika ditelaah lebih jauh berdasarkan demografi sektoral, sektor pendidikan, khususnya institusi pendidikan tinggi, serta berbagai instansi pemerintah tercatat sebagai pengadopsi tertinggi dan paling progresif dibandingkan dengan sektor korporasi swasta (Abdul et al.,

2018). Tingginya tingkat adopsi pada sektor-sektor publik ini pada dasarnya didorong oleh kebutuhan mendesak untuk memfasilitasi karyawan maupun sivitas akademika agar mampu mengeksekusi tugas secara *mobile* dan asinkronus. Selain itu, kebijakan ini dipandang sebagai jalan keluar yang sangat pragmatis atas keterbatasan kapabilitas finansial dan anggaran organisasi dalam menyediakan perangkat keras mutakhir secara merata bagi seluruh penggunanya (Abdul et al., 2018).

Dari sudut pandang efisiensi operasional dan penyelarasan manajemen keuangan, BYOD secara fundamental mendisrupsi model pengadaan infrastruktur TI tradisional. Pendekatan ini memungkinkan organisasi untuk mengalihkan porsi terbesar dari beban kepemilikan aset perangkat keras *(Capital Expenditure)* secara langsung kepada pengguna akhir, sehingga secara berkesinambungan mampu memangkas biaya pemeliharaan, dukungan teknis, dan siklus pembaruan perangkat teknologi informasi (Bayu Taruno et al., 2014). Menariknya, peralihan beban finansial ini tidak serta merta memicu resistensi dari pihak pekerja. Sebaliknya, hal ini justru menciptakan ekuilibrium yang menguntungkan antara efisiensi ekonomi perusahaan dengan stabilitas mental dan operasional pekerja. Pengguna merasa lebih leluasa dan nyaman karena mereka mengoperasikan antarmuka perangkat yang telah dikustomisasi sesuai dengan preferensi dan kebiasaan pribadi mereka. Interaksi yang mulus dengan perangkat milik sendiri ini secara psikologis mampu menyeimbangkan kenyamanan emosional dengan beban kerja yang tinggi, yang pada gilirannya menstimulasi lonjakan produktivitas kerja secara signifikan (Marziana & Zulkefli, 2017).

Dari sudut pandang efisiensi operasional dan penyelarasan manajemen keuangan, BYOD secara fundamental mendisrupsi model pengadaan infrastruktur TI tradisional. Pendekatan ini memungkinkan organisasi untuk mengalihkan porsi terbesar dari beban kepemilikan aset perangkat keras *(Capital Expenditure)* secara langsung kepada pengguna akhir, sehingga secara berkesinambungan mampu memangkas biaya pemeliharaan, dukungan teknis, dan siklus pembaruan perangkat teknologi informasi (Bayu Taruno et al., 2014). Menariknya, peralihan beban finansial ini tidak serta merta memicu resistensi dari pihak pekerja. Sebaliknya, hal ini justru menciptakan ekuilibrium

yang menguntungkan antara efisiensi ekonomi perusahaan dengan stabilitas mental dan operasional pekerja. Pengguna merasa lebih leluasa dan nyaman karena mereka mengoperasikan antarmuka perangkat yang telah dikustomisasi sesuai dengan preferensi dan kebiasaan pribadi mereka. Interaksi yang mulus dengan perangkat milik sendiri ini secara psikologis mampu menyeimbangkan kenyamanan emosional dengan beban kerja yang tinggi, yang pada gilirannya menstimulasi lonjakan produktivitas kerja secara signifikan (Marziana & Zulkefli, 2017).

Kerentanan Keamanan Data dan Privasi

Terlepas dari berbagai keunggulan operasional yang ditawarkan, arsitektur BYOD secara inheren memunculkan ancaman yang sangat krusial terhadap integritas dan kerahasiaan data perusahaan. Ancaman ini muncul utamanya karena batasan isolasi antara kepentingan ranah pribadi dan kewajiban profesional menjadi semakin buram, tumpang tindih, dan sulit diawasi oleh administrator jaringan (Bayu Taruno et al., 2014), (Idris, 2019). Realitas di lapangan menunjukkan adanya paradoks kesadaran keamanan yang mengkhawatirkan; sebuah survei menemukan bahwa meskipun 65% pengguna perangkat bergerak mengaku khawatir akan isu keamanan siber secara umum, ironisnya 52% dari mereka terbukti tidak memiliki pemahaman teknis mengenai seberapa fatal risiko percampuran akses data pribadi dan aset perusahaan di dalam satu perangkat yang sama (Bayu Taruno et al., 2014). Rendahnya literasi keamanan ini terwujud secara nyata dalam perilaku pengguna yang berisiko tinggi. Temuan empiris menyoroti bahwa 60% partisipan BYOD secara aktif menggunakan aplikasi penyimpanan awan dan platform berbagi berkas pihak ketiga secara gratis tanpa kontrol pengamanan yang memadai, di mana 55% di antaranya menyembunyikan atau tidak melaporkan aktivitas *Shadow IT* tersebut kepada pihak manajemen organisasi (Marziana & Zulkefli, 2017).

Kerapuhan postur keamanan sistem informasi ini semakin diperparah oleh kelalaian struktural dari sisi manajemen tata kelola itu sendiri. Bukti observasi menunjukkan bahwa sebanyak 77,7% organisasi beroperasi tanpa memiliki landasan persyaratan atau kebijakan penggunaan perangkat BYOD yang terstandardisasi, dan lebih parahnya lagi, 69,5% tidak mengimplementasikan protokol otentikasi dasar seperti kewajiban penggunaan kata sandi pada gawai pribadi yang menumpang pada jaringan intranet

kantor (Marziana & Zulkefli, 2017). Kondisi tanpa regulasi ini sering kali menciptakan sebuah dilema etika bagi praktisi keamanan siber dalam menjaga privasi data pengguna di tengah tuntutan untuk melindungi aset digital korporat. Administrator dihadapkan pada kesulitan untuk memantau ancaman tanpa harus melanggar batas privasi di dalam perangkat keras yang secara hukum merupakan properti pribadi karyawan. Celah keamanan berlapis ini secara masif memfasilitasi vektor serangan yang destruktif, mulai dari insiden eksfiltrasi data akibat kehilangan media penyimpanan portabel, penyebaran infeksi *malware* lintas jaringan internal akibat absennya filter keamanan titik akhir *(endpoint)*, hingga kerentanan eksploitasi peretasan yang kerap menargetkan demografi pengguna usia muda yang sering abai terhadap pembaruan sistem operasi [10], (Idris, 2019), (Mahinderjit et al., 2017).

Strategi Implementasi dan Kebijakan Keamanan BYOD (BYOD-SP)

Untuk memitigasi spektrum ancaman yang luas tersebut tanpa mendegradasi manfaat fleksibilitas yang menjadi nilai jual utama BYOD, setiap entitas organisasi diwajibkan secara mutlak untuk merumuskan dan menegakkan Dokumen Kebijakan Keamanan BYOD (BYOD-SP) yang komprehensif. Kerangka kebijakan strategis ini harus dikonstruksi secara presisi agar mampu menciptakan keseimbangan yang harmonis antara hak akses pengguna, protokol keamanan berlapis, dan perlindungan privasi data pribadi (Mahinderjit et al., 2017). Dalam tahap pengembangannya, BYOD-SP membutuhkan integrasi beberapa komponen manajerial dan teknis; pihak manajemen harus membangun arsitektur model kepercayaan *(trust model)* bertingkat dan mendefinisikan dengan sangat spesifik klasifikasi sistem operasi serta tipe perangkat apa saja yang masuk ke dalam daftar putih *(whitelist)* untuk diizinkan mengakses jaringan perusahaan (Bayu Taruno et al., 2014).

Lebih lanjut, regulasi teknis di dalam kebijakan keamanan tersebut harus diwajibkan tanpa pengecualian. Hal ini mencakup penerapan enkripsi basis data *(data-at-rest encryption)*, keharusan instalasi perisian antivirus tingkat korporat, rotasi dan pengelolaan kata sandi berkala yang kompleks, serta penerapan teknik kontainerisasi untuk melakukan isolasi dan memisahkan kompartemen data bisnis dari aplikasi personal

secara logikal (Marziana & Zulkefli, 2017). Selain langkah preventif, infrastruktur respons insiden seperti *Mobile Device Management* (MDM) juga harus diaktifkan agar administrator memiliki kapabilitas melakukan fasilitas penghapusan data perusahaan secara jarak jauh *(remote wipe)* guna menetralisir risiko saat perangkat dilaporkan hilang atau dicuri (Bayu Taruno et al., 2014). Tentu saja, implementasi perangkat kebijakan ini tidak akan berjalan efektif apabila tidak diiringi dengan komunikasi kebijakan yang transparan serta program pelatihan kesadaran keamanan siber yang berkelanjutan agar pengguna benar-benar memahami tanggung jawab moral dan profesional mereka. Apabila hasil audit risiko menilai bahwa arsitektur BYOD terlalu rentan untuk diterapkan pada lanskap departemen dengan data yang sangat rahasia, organisasi dapat melakukan pivot strategis menuju model *Choose Your Own Device* (CYOD). Pendekatan alternatif ini memastikan departemen TI tetap memiliki kontrol otoritatif dalam menciptakan dan mengawasi lingkungan kerja virtual yang terpisah secara aman dari ranah data pribadi (Idris, 2019).

Perspektif Green IT dan Dampak Lingkungan

Dari sudut pandang ekologi dan inisiatif komputasi hijau *(Green IT)*, model BYOD pada fase awal kemunculannya disambut dengan optimisme tinggi sebagai solusi yang diklaim sangat ramah lingkungan. Asumsi dasar ini berakar pada kemampuan BYOD dalam menekan agregat volume pengadaan dan proses manufaktur perangkat komputasi oleh pihak korporasi, yang secara teori diasumsikan akan otomatis memotong rantai emisi dari pabrikasi, distribusi logistik, hingga penumpukan limbah elektronik *(e-waste)* di gudang organisasi (Idris, 2019). Namun, kajian literatur yang lebih mendalam dan komprehensif justru mengindikasi sebuah anomali. Penelitian menunjukkan bahwa BYOD justru menghadirkan paradoks *Green IT* yang memicu dampak tidak ramah lingkungan dengan meningkatkan jejak karbon perusahaan secara tersembunyi dan masif (Idris, 2019).

Lonjakan emisi karbon terselubung dalam ekosistem BYOD ini dikatalisasi secara langsung oleh eskalasi kebutuhan infrastruktur penyimpanan data yang tersebar luas serta konsumsi energi server komputasi awan yang terus meningkat akibat virtualisasi pusat data (Idris, 2019). Proses sinkronisasi data asinkronus tanpa henti yang terjadi antara

berbagai perangkat pintar milik karyawan dengan server pusat memaksa infrastruktur jaringan untuk terus menyala dan beroperasi pada kapasitas puncak. Selain itu, budaya "selalu terhubung" *(always-on)* membuat pengguna memiliki kecenderungan buruk untuk membiarkan banyak perangkat sekunder tetap aktif menganggur dalam kondisi siaga *(standby)*, yang secara akumulatif menyedot daya listrik dalam jumlah raksasa. Tidak berhenti di situ, energi listrik dan sumber daya perangkat keras ekstra yang terpaksa dibakar oleh tim keamanan jaringan dalam upaya pemantauan lalu lintas data, proses mengatasi rentetan insiden peretasan, hingga pemulihan pasca kebocoran data juga turut memberikan kontribusi pada jejak karbon yang sering kali diabaikan. Rangkaian variabel ini pada akhirnya menegaskan bahwa tanpa tata kelola energi yang ketat, ekosistem BYOD berpotensi menjadi kontributor polusi digital yang cukup membahayakan lingkungan (Idris, 2019).

4. KESIMPULAN

Implementasi kebijakan *Bring Your Own Device* (BYOD) dalam organisasi memberikan manfaat operasional yang signifikan melalui peningkatan fleksibilitas kerja, efisiensi biaya pengadaan perangkat keras, serta peningkatan produktivitas karyawan secara keseluruhan. Namun, efisiensi ini diiringi oleh risiko keamanan informasi yang kompleks akibat hilangnya kontrol fisik dan logis organisasi terhadap perangkat pribadi yang digunakan untuk mengakses aset data perusahaan. Ancaman siber seperti serangan *malware*, *phishing*, hingga kebocoran data akibat penggunaan jaringan yang tidak aman menjadi tantangan nyata yang harus dimitigasi secara sistematis oleh manajemen organisasi.

Temuan studi ini menegaskan bahwa solusi teknis seperti *Mobile Device Management* (MDM) tidak akan memadai jika tidak dibarengi dengan kerangka tata kelola yang transparan dan berbasis pada nilai etika profesi. Keberhasilan integrasi BYOD sangat bergantung pada keseimbangan antara kebutuhan perlindungan aset korporat yang kokoh dan penghormatan terhadap privasi individu sebagaimana yang diamanatkan dalam Undang-Undang Pelindungan Data Pribadi. Organisasi perlu menggeser pendekatan dari sekadar kontrol berbasis teknologi menuju strategi yang lebih

holistik, yang mencakup penetapan kebijakan yang spesifik, audit berkala terhadap kepatuhan pengguna, serta pembangunan budaya keamanan melalui edukasi karyawan secara berkelanjutan.

Sebagai rekomendasi strategis, organisasi disarankan untuk merumuskan kebijakan BYOD yang adaptif agar tetap berkelanjutan dalam jangka panjang. Setiap komponen kebijakan seperti prosedur enkripsi, pemisahan data antara ranah pribadi dan profesional, serta langkah remediasi saat terjadi kehilangan perangkat harus terdokumentasi dengan baik dan dipahami oleh seluruh pemangku kepentingan. Selain itu, organisasi perlu mempertimbangkan pendekatan alternatif seperti *Choose Your Own Device* bagi divisi dengan risiko data tinggi guna memastikan kontrol yang lebih presisi. Dengan mengintegrasikan aspek teknis yang tangguh, prinsip etika profesional yang tinggi, serta kepatuhan hukum yang ketat, BYOD dapat bertransformasi menjadi instrumen strategis yang mendukung tujuan organisasi tanpa harus mengorbankan hak privasi individu karyawan di tengah era transformasi digital.

5. SARAN

Berdasarkan analisis permasalahan dan hasil pembahasan yang telah diuraikan, terdapat beberapa rekomendasi strategis yang perlu dipertimbangkan oleh pihak manajemen organisasi maupun pembuat kebijakan dalam mengimplementasikan kebijakan *Bring Your Own Device* (BYOD) secara efektif dan etis.

Pertama, organisasi harus segera merumuskan dokumen kebijakan keamanan yang spesifik dan komprehensif, atau *BYOD Security Policy* (BYOD-SP), yang tidak hanya bersifat administratif tetapi juga teknis. Kebijakan ini tidak boleh disusun secara sepihak oleh departemen IT saja, melainkan harus melibatkan proses partisipasi aktif dari para karyawan dalam tahap perumusan untuk meningkatkan rasa memiliki dan kepatuhan pengguna terhadap aturan yang telah disepakati (Bayu Taruno et al., 2014). Dokumen kebijakan tersebut wajib mencakup komponen mendasar seperti ruang lingkup penggunaan, prosedur keamanan, kategori data yang diizinkan, serta konsekuensi logis atas setiap pelanggaran kebijakan (Marziana & Zulkefli, 2017).

Kedua, dari sisi teknis, organisasi disarankan untuk tidak hanya mengandalkan kebijakan tertulis melainkan harus mengintegrasikan kontrol keamanan yang tangguh

pada setiap perangkat. Langkah ini mencakup penerapan enkripsi data pada seluruh gawai yang mengakses jaringan perusahaan, kewajiban penggunaan kata sandi yang kuat bagi setiap pengguna, serta pemanfaatan solusi manajemen perangkat seluler atau *Mobile Device Management* (MDM) (Marziana & Zulkefli, 2017). Penggunaan MDM harus dilakukan secara terukur dengan tetap menjaga batasan privasi, terutama dalam hal pemantauan lokasi atau akses terhadap data personal karyawan yang tidak relevan dengan pekerjaan (Marziana & Zulkefli, 2017).

Ketiga, organisasi perlu memprioritaskan aspek edukasi dan pembangunan budaya keamanan siber di lingkungan kerja. Mengingat manusia sering dianggap sebagai mata rantai terlemah dalam rantai keamanan, pelatihan berkala mengenai kesadaran akan ancaman seperti *phishing*, bahaya instalasi aplikasi pihak ketiga yang tidak resmi, hingga risiko penggunaan jaringan Wi-Fi publik sangat krusial untuk dilaksanakan [7], (Bayu Taruno et al., 2014). Karyawan harus dibekali pengetahuan untuk mengenali potensi serangan dan memahami tanggung jawab mereka dalam menjaga integritas data organisasi di perangkat milik pribadi (Idris, 2019).

Keempat, terkait dengan aspek etika dan privasi, organisasi harus menerapkan kategorisasi data yang jelas untuk memisahkan antara data perusahaan dan data pribadi (Marziana & Zulkefli, 2017). Hal ini sangat penting untuk memastikan bahwa tindakan pengamanan yang dilakukan oleh perusahaan tidak melanggar hak privasi individu karyawan sebagaimana diatur dalam regulasi pelindungan data pribadi yang berlaku (Idris, 2019). Pemisahan logis ini akan memberikan rasa aman bagi karyawan bahwa aktivitas pribadi mereka di luar konteks pekerjaan tidak akan diawasi secara berlebihan oleh pihak organisasi (Marziana & Zulkefli, 2017).

Kelima, sebagai bentuk tanggung jawab terhadap isu *Green IT*, organisasi disarankan untuk memberikan edukasi kepada pengguna mengenai pentingnya efisiensi penggunaan perangka. Pengguna perlu disadarkan untuk tidak membiarkan perangkat dalam kondisi aktif terus menerus atau *idle* dalam durasi yang lama, serta mempertimbangkan jejak karbon dalam pemilihan perangkat keras yang ramah lingkungan (Idris, 2019). Dengan mengombinasikan langkah-langkah teknis yang presisi,

kebijakan yang etis, serta kepedulian terhadap lingkungan, organisasi dapat memastikan bahwa program BYOD tidak hanya memberikan manfaat ekonomi dan produktivitas, tetapi juga berjalan dengan standar keamanan yang kokoh dan berkelanjutan.

DAFTAR REFERENSI

Abdul, M., Mansor, Z., & Sulaiman, R. (2018). *Pemerhatian Awalan ke atas Amalan Membawa Peralatan Sendiri (BYOD) dalam Organisasi di Malaysia*. 1–7.

Bayu Taruno, R., Wahyu Winarno, W., & Adhipta, D. (2014). Strategi "Bring Your Own Devices" pada Perusahaan Sebagai Tantangan Penyelarasan Bisnis dan TI Untuk Memenuhi Sasaran Finansial. *STMIK AMIKOM Yogyakarta*, 77–82.

Halim, I. I. A., Buja, A. G., Idris, M. S. S., & Mahat, N. J. (2024). Implementation of BYOD Security Policy in Malaysia Institutions of Higher Learning (MIHL): An Overview. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *33*(2), 1–14. https://doi.org/10.37934/araset.33.2.114

Idris, Moh. (2019). Pemilihan Solusi Penerapan Bring Your Own Device (Byod) Berdasarkan Kontrol Keamanannya. *Jurnal Ilmiah Matrik*, *21*(3), 214–222. https://doi.org/10.33557/jurnalmatrik.v21i3.724

Mahinderjit, M., Wai, C., & Zulkefli, Z. (2017). Security and Privacy Risks Awareness for Bring Your Own Device (BYOD) Paradigm. *International Journal of Advanced Computer Science and Applications*, *8*(2), 53–62. https://doi.org/10.14569/ijacsa.2017.080208

Marziana, A. M., & Zulkefli, M. (2017). Pelaksanaan BYOD di Organisasi: Pemerhatian ke atas Penguatkuasaan Polisi BYOD. *3th International Conference on Information Technology & Society*, 1–5. http://fstm.kuis.edu.my/icits/2017/eproceeding/IC-ITS2017 IT04 pp1-5 Marziana.pdf

Mega Puspita, Y., & Hasanudin, M. (2022). Mobile Device Management for the Use of Bring Your Own Device (BYOD) as Company Data Security during the Covid-19 Pandemic. *International Journal of Information System & Technology Akreditasi*, *6*(158), 528–536.

Mitra, A. R. (2013). *Potensi Dampak Byod (Bring Your Own Device) Yang Tidak Ramah Lingkungan*. 46–60.

Nurillah, R. A., & Trihandoyo, A. (2024). Analisis Faktor-Faktor Keamanan Informasi Perusahaan Dalam Penerapan Bring Your Own Device (BYOD). *IKRA-ITH Informatika : Jurnal Komputer Dan Informatika*, *8*(2), 136–145. https://doi.org/10.37817/ikraith-informatika.v8i2.2973

Pemerintah Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Kementerian Sekretariat Negara.

Priyo Hadi Nugroho, & Achmad Darajatun, R. (2021). Perancangan Sistem Informasi Monitoring Pembangunan Desa Berbasis Bring Your Own Device. *Metik Jurnal*, *5*(2), 10–18. https://doi.org/10.47002/metik.v5i2.286

Siti, A., Andari, S., Nurmiati, E., Informasi, S., Sains, F., Hidayatullah, U. S., & Selatan, T. (2026). *Peran dan Tanggung Jawab Etis Profesional TI dalam Mencegah Kebocoran Data Privasi*. *2*(3), 3856–3863.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*(March), 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Suci Anugrah, Muhammad Zaky Himawan, Nabila Raihana Qalby, & Evy Nurmiati. (2025). Pengaruh Etika Profesi Terhadap Keamanan Informasi dalam Konteks Kebocoran Data BSI (Bank Syariah Indonesia): Studi Literatur Sistematis. *Jurnal Tata Kelola Dan Kerangka Kerja Teknologi Informasi*, *11*(2), 106–112. https://doi.org/10.34010/jtk3ti.v11i2.17033