**JURNAL STARS**
DOI:

**VOL. 4. NO. 1 MEI 2025**

Diterbitkan Oleh: LPPM Universitas Pertiwi

# ANALISIS CYBERSECURITY DAN KEPATUHAN REGULASI PERLINDUNGAN DATA PADA PT IFORTE

**Dini Nurlita[1]; Luthfiyyah Labibah[2]; Nabila Septiyani Ruslia[3]; Wahyu Agung Prasetyo[4]**

Program Studi Sistem Informasi [1,2,3,4]
Universitas Pertiwi [1,2,3,4]
24530006@pertiwi.ac.id[1]; 24530009@pertiwi.ac.id[2]; 24530010@pertiwi.ac.id[3];
wahyu.agung@pertiwi.ac.id[4]

***Abstract***— *This study analyzes the implementation of cybersecurity at PT IForte Solusi Terbaik in the context of e-commerce and compliance with the Personal Data Protection Act (UU PDP) and ISO 27001. The research method used is descriptive qualitative with a case study approach through interviews and observations. The results show that the company has implemented technical measures such as closed network infrastructure and restricted access, but there are still shortcomings in policy documentation and data use transparency. This study provides recommendations to improve training, audit systems, and the adoption of international standards.*
***Keywords****: cybersecurity, data protection, ISO 27001, PDP*

**Abstrak**— Penelitian ini menganalisis penerapan cybersecurity di PT IForte Solusi Terbaik dalam konteks e-commerce serta kepatuhan terhadap UU Perlindungan Data Pribadi dan ISO 27001. Metode penelitian yang digunakan adalah kualitatif deskriptif melalui studi kasus dengan wawancara dan observasi. Hasil menunjukkan bahwa perusahaan telah menerapkan langkah teknis seperti jaringan tertutup dan pembatasan akses, namun masih ada kekurangan dalam dokumentasi kebijakan dan transparansi penggunaan data. Penelitian ini memberikan rekomendasi untuk meningkatkan pelatihan, sistem audit, dan adopsi standar internasional.
**Kata kunci**: cybersecurity, perlindungan data, ISO 27001, PDP

## PENDAHULUAN

Pertumbuhan e-commerce di Indonesia telah meningkatkan aktivitas digital dan pertukaran data pribadi. Namun, masih banyak perusahaan yang belum siap menghadapi ancaman siber. Keamanan data pribadi menjadi penting, terutama setelah disahkannya UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Menurut Yulianto dan Pratama (2023), masih banyak perusahaan di Indonesia yang belum memiliki struktur perlindungan data pribadi secara memadai, khususnya dalam konteks kepatuhan regulasi.

Selain itu, ISO 27001 memberikan pedoman tentang sistem manajemen keamanan informasi yang diperlukan dalam lingkungan digital yang kompleks dan terus berkembang (Putri & Sari, 2022). Oleh karena itu, penting untuk mengkaji kesiapan perusahaan dalam mengadopsi kebijakan dan sistem keamanan yang sesuai dengan standar internasional dan peraturan nasional.

## BAHAN DAN METODE

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode studi kasus. Penelitian dilakukan di kantor cabang PT IForte Solusi Terbaik, Jakarta. Teknik pengumpulan data yang digunakan adalah observasi langsung dan wawancara informal dengan satu karyawan yang bekerja di divisi sistem informasi dan keamanan data. Observasi dilakukan terhadap kondisi infrastruktur teknologi, prosedur akses data, dan sistem otentikasi yang digunakan perusahaan. Wawancara menggali sejauh mana kebijakan keamanan diterapkan, serta pemahaman karyawan terhadap regulasi yang berlaku. Wawancara ini dilakukan dengan Qhoirul Imam Karnaen, staf bagian sistem informasi PT IForte, pada tanggal 25

JURNAL STARS
DOI:
VOL. 4. NO. 1 MEI 2025
Diterbitkan Oleh: LPPM Universitas Pertiwi

Juni 2025, yang menjelaskan secara rinci proses pembatasan akses dan tantangan dalam dokumentasi kebijakan internal (Qhoirul Imam Karnaen, wawancara pribadi, 25 Juni 2025).

Alat bantu utama dalam pengumpulan data adalah lembar observasi dan panduan wawancara semi-terstruktur. Alat-alat umum seperti alat tulis, perekam audio, dan laptop tidak dijelaskan lebih lanjut karena merupakan alat bantu standar.

Proses analisis data dilakukan dengan metode analisis tematik melalui tiga tahap: reduksi data, penyajian data, dan penarikan kesimpulan. Validitas data diperkuat dengan melakukan triangulasi antara hasil observasi, wawancara, dan dokumen kebijakan yang diperoleh dari lokasi penelitian. Data hasil observasi dan wawancara dikodekan untuk diidentifikasi tema-tema kunci seperti manajemen risiko, kontrol akses, dan transparansi penggunaan data. Prosedur ini mengacu pada pendekatan Miles dan Huberman (1994) dalam analisis data kualitatif.

## HASIL DAN PEMBAHASAN

1. Penerapan Cybersecurity

Hasil observasi menunjukkan bahwa PT IForte telah menerapkan jaringan tertutup untuk membatasi akses terhadap data sensitif. Hal ini mencerminkan penerapan prinsip isolasi jaringan untuk mengurangi vektor serangan dari pihak luar (ISO, 2022). Namun, belum terdapat penggunaan multi-factor authentication (MFA) untuk pengguna internal maupun eksternal. Dalam wawancara, Qhoirul Imam Karnaen menyampaikan bahwa keterbatasan infrastruktur dan kurangnya pelatihan teknis menjadi kendala utama dalam mengimplementasikan sistem pencatatan akses dan pengamanan tambahan seperti MFA (wawancara pribadi, 25 Juni 2025). Ketidakhadiran fitur ini menyebabkan sistem lebih rentan terhadap penyusupan berbasis kredensial.

Temuan ini mengindikasikan bahwa meskipun perusahaan memahami pentingnya kontrol akses, pemenuhan terhadap praktik terbaik internasional belum terlaksana secara menyeluruh. Sebagaimana dijelaskan dalam penelitian oleh Oktaviani dan Yusuf (2021), penerapan autentikasi ganda secara signifikan menurunkan risiko pelanggaran data pada perusahaan digital di sektor e-commerce.

2. Evaluasi Kepatuhan terhadap UU PDP

Perusahaan telah menyadari keberadaan dan pentingnya UU No. 27 Tahun 2022, namun belum ada dokumentasi kebijakan perlindungan data yang dipublikasikan secara transparan. Belum tersedia formulir hak akses dan penghapusan data oleh pengguna sebagaimana diwajibkan oleh Pasal 6 dan Pasal 15 UU PDP. Firmansyah dan Wibowo (2023) menyebutkan bahwa tantangan umum di kalangan perusahaan Indonesia adalah lemahnya integrasi aspek hukum ke dalam sistem TI mereka.

Secara ilmiah, hal ini dapat dijelaskan sebagai akibat dari tidak adanya jabatan Data Protection Officer (DPO) yang bertugas memastikan pelaksanaan UU PDP secara strategis dan operasional. Ketiadaan DPO berimplikasi langsung terhadap lemahnya akuntabilitas pengelolaan data nasabah.

3. Evaluasi terhadap ISO 27001

Dari wawancara dan observasi, diketahui bahwa perusahaan belum memiliki sertifikasi ISO 27001 dan belum melaksanakan audit keamanan informasi secara berkala. Padahal, prinsip-prinsip seperti manajemen risiko dan pengendalian akses sebagian sudah diterapkan secara tidak formal. Menurut Putri dan Sari (2022), perusahaan yang telah tersertifikasi ISO 27001 menunjukkan peningkatan kepercayaan dari pengguna layanan digital.

Hal ini mengindikasikan bahwa PT IForte berada pada tahap awal implementasi sistem manajemen keamanan informasi (Information Security Management System) dan perlu roadmap formal menuju sertifikasi penuh.

4. Identifikasi Kelemahan

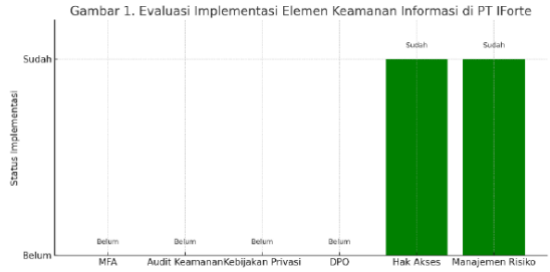
Gambar 1. Evaluasi Implementasi Elemen Keamanan Informasi di PT IForte

Temuan utama dari penelitian ini adalah bahwa kelemahan signifikan terletak pada aspek administratif dan regulatif, bukan teknis. Berdasarkan rangkuman dalam Tabel 1, celah

JURNAL STARS
DOI:
VOL. 4. NO. 1 MEI 2025
Diterbitkan Oleh: LPPM Universitas Pertiwi

terbesar mencakup: ketiadaan dokumentasi kebijakan, tidak adanya DPO, kurangnya pelatihan staf, dan ketiadaan sistem audit.

Secara ilmiah, kelemahan ini berakar pada rendahnya literasi hukum dan tata kelola TI dalam organisasi. Wahyuni (2021) menekankan bahwa perusahaan cenderung fokus pada pengamanan sistem tetapi mengabaikan faktor manusia dan kebijakan, yang justru menjadi titik rentan utama dalam serangan siber.




Gambar 1. Evaluasi Implementasi Elemen Keamanan Informasi di PT IForte

Dibandingkan dengan penelitian oleh Nugraha dan Lestari (2021), perusahaan e-commerce lokal memiliki pola serupa dalam hal minimnya kesesuaian kebijakan privasi dengan praktik aktual di lapangan.

## KESIMPULAN

Penelitian ini menunjukkan bahwa PT IForte telah mengambil langkah awal dalam menerapkan prinsip dasar keamanan informasi, terutama dari sisi teknis seperti penggunaan jaringan tertutup dan pembatasan akses data. Namun, penelitian ini juga mengungkap bahwa kesiapan administratif dan kepatuhan terhadap regulasi seperti UU PDP dan standar ISO 27001 masih tergolong rendah. Ketiadaan dokumentasi kebijakan, audit internal, serta peran Data Protection Officer menjadi hambatan utama dalam pencapaian keamanan informasi yang menyeluruh.

Temuan ini menegaskan bahwa keberhasilan perlindungan data nasabah bukan hanya bergantung pada teknologi, tetapi sangat ditentukan oleh tata kelola dan struktur kebijakan yang solid. Untuk tahap selanjutnya, penelitian ini merekomendasikan pengembangan roadmap penerapan ISO 27001 secara formal serta peningkatan literasi hukum dan keamanan siber bagi seluruh karyawan melalui pelatihan berkala. Studi lanjutan dapat difokuskan pada pengukuran indeks kesiapan kepatuhan data di sektor e-commerce nasional.

## REFERENSI

Adi, A., & Kurniawan, T. (2020). Cybersecurity dan perlindungan data di sektor e-commerce: Studi literatur global. Jurnal Internasional Teknologi Digital, 12(2), 18–29.

Departemen Komunikasi dan Informatika Republik Indonesia. (2022). Pedoman teknis penerapan UU Perlindungan Data Pribadi. Kementerian Komunikasi dan Informatika RI.

Firmansyah, H., & Wibowo, T. (2023). Evaluasi kesiapan perusahaan digital menghadapi UU PDP. Jurnal Hukum & Teknologi, 4(1), 33–44.

Handayani, L. (2020). Etika dan hukum siber dalam perlindungan konsumen digital. Literasi Global.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection. ISO.

Nisa, K., & Fauzan, R. (2022). Analisis risiko keamanan siber dalam infrastruktur teknologi informasi perusahaan. Jurnal Teknologi dan Keamanan, 6(1), 28–37.

Nugraha, A., & Lestari, V. (2021). Perlindungan data pribadi konsumen e-commerce: Studi kepatuhan platform lokal. Jurnal E-Bisnis, 7(3), 112–123.

Oktaviani, M., & Yusuf, A. (2021). Sistem autentikasi dan perlindungan data pelanggan pada aplikasi digital. Jurnal Teknologi Informasi dan Komunikasi, 10(2), 55–64.

Putri, A. R., & Sari, D. M. (2022). Implementasi ISO 27001 pada sistem manajemen keamanan informasi di perusahaan teknologi. Jurnal Sistem Informasi, 14(1), 17–26.

Rachman, Y. (2021). Manajemen risiko keamanan siber pada perusahaan digital. DeepTech Publishing.

Sembiring, B. (2020). Manajemen keamanan informasi dalam era digital: Pendekatan ISO dan best practice. Pustaka Mitra.

Susanto, A., & Fitriani, D. (2023). Tinjauan implementasi ISO 27001 di industri telekomunikasi Indonesia. Jurnal Telekomunikasi dan Sistem Keamanan, 5(4), 77–85.

Wahyuni, E. S. (2021). Pengaruh kebijakan keamanan informasi terhadap kepercayaan pelanggan digital. Jurnal Ilmu Komputer dan Bisnis, 9(3), 90–101.

Widodo, F., & Amelia, S. (2023). Prinsip-prinsip keamanan data dalam UU PDP dan implementasinya pada perusahaan startup. Jurnal Regulasi Teknologi, 3(1), 43–55.

Yulianto, D., & Pratama, R. (2023). Analisis kepatuhan perusahaan terhadap UU Perlindungan Data Pribadi di Indonesia. Jurnal Keamanan Siber Indonesia, 5(2), 91–102.*