STRATEGI IMPLEMENTASI KEBIJAKAN KEAMANAN INFORMASI DI ERA TRANSFORMASI DIGITAL

Fahrizal Wahyudi[1], Dimas Aryo Saputra[3], Abdul Muni[3]
[123]Sistem Informasi, Fakultas Ilmu Komputer, Universitas Islam Indragiri,
Email: fahrizalwahyudi2504@gmail.com[1], dimasaryosaputra9@gmail.com[2],
abdulmuni@live.com[3]

ABSTRAK

Transformasi digital yang semakin masif telah mendorong organisasi untuk mengintegrasikan teknologi informasi dalam hampir seluruh lini operasional. Namun, peningkatan digitalisasi ini juga memperluas permukaan serangan siber dan meningkatkan risiko terhadap keamanan informasi. Penelitian ini bertujuan untuk mengkaji strategi implementasi kebijakan keamanan informasi yang efektif di era transformasi digital. Metodologi yang digunakan adalah studi pustaka dengan pendekatan kualitatif deskriptif, mengacu pada standar internasional seperti ISO/IEC 27001 dan kerangka kerja NIST. Hasil analisis menunjukkan bahwa keberhasilan implementasi kebijakan keamanan sangat dipengaruhi oleh tiga faktor utama: komitmen manajemen, kesadaran pengguna, dan adopsi teknologi keamanan terkini. Selain itu, pendekatan adaptif dan berkelanjutan sangat diperlukan untuk menjawab dinamika ancaman siber yang terus berkembang. Penelitian ini memberikan rekomendasi strategis bagi organisasi untuk membangun sistem keamanan informasi yang tangguh dan responsif terhadap perubahan digital.

***Kata Kunci*: Keamanan Informasi, Kebijakan Keamanan, Transformasi Digital, ISO/IEC 27001, Strategi Implementasi**

ABSTRACT

The rapid acceleration of digital transformation has driven organizations to integrate information technology into nearly all operational lines. However, this increased digitalization also expands the surface area for cyberattacks and heightens the risk to information security. This study aims to examine effective strategies for implementing information security policies in the era of digital transformation. The research employs a literature review method with a descriptive qualitative approach, referencing international standards such as ISO/IEC 27001 and the NIST cybersecurity framework. The analysis reveals that the success of information security policy implementation is strongly influenced by three key factors: management commitment, user awareness, and the adoption of up-to-date security technologies. Furthermore, an adaptive and continuous approach is essential to respond to the evolving dynamics of cyber threats. This study offers strategic recommendations for organizations to build resilient and responsive information security systems in the face of ongoing digital change.

Keywords: Information Security, Security Policy, Digital Transformation, ISO/IEC 27001, Implementation Strategy

1 PENDAHULUAN

Transformasi digital telah menjadi fenomena global yang mengubah cara organisasi beroperasi. Penggunaan teknologi seperti komputasi awan, Internet of Things (IoT), dan sistem berbasis big data mempercepat otomatisasi serta integrasi layanan. Namun, kemajuan ini juga membawa risiko keamanan yang semakin kompleks, terutama dalam hal perlindungan data dan informasi sensitif (Surya et al., 2024).

Digitalisasi yang agresif memperluas permukaan serangan dan meningkatkan eksposur terhadap potensi ancaman siber. Serangan seperti ransomware, phishing, dan kebocoran data menjadi lebih umum, bahkan pada organisasi dengan tingkat kematangan digital yang tinggi. Oleh

karena itu, strategi pengamanan sistem informasi yang kuat dan adaptif menjadi kebutuhan mendesak (Sulaiman et al., 2022).

Untuk mengatasi tantangan tersebut, banyak organisasi mulai menerapkan standar keamanan informasi internasional seperti ISO/IEC 27001 dan kerangka kerja NIST Cybersecurity Framework (CSF). Standar ini membantu dalam mengelola risiko, melindungi aset informasi, dan menyusun kebijakan keamanan berbasis siklus perbaikan berkelanjutan (ISO/IEC, 2022; NIST, 2023).

Namun, penerapan kebijakan keamanan tidak hanya bergantung pada teknologi dan prosedur formal. Faktor manusia dan sosial-organisasional memainkan peran yang krusial dalam keberhasilan kebijakan. Komitmen manajemen puncak, kepatuhan karyawan, dan budaya keamanan menjadi elemen penting dalam membentuk pertahanan informasi yang efektif (Alkalbani et al., 2016).

Penguatan budaya keamanan informasi tidak dapat dilepaskan dari peran strategis pimpinan organisasi dan peningkatan kesadaran pengguna terhadap ancaman siber. Tanpa kesadaran yang memadai, kebijakan hanya akan menjadi dokumen administratif tanpa dampak nyata terhadap perilaku pengguna sistem (Uchendu et al., 2021).

Penelitian sebelumnya juga menunjukkan bahwa keberhasilan implementasi kebijakan keamanan sangat tergantung pada pendekatan pelatihan yang berkelanjutan, keterlibatan emosional, serta motivasi internal pengguna. Sekadar menyosialisasikan aturan tidak cukup tanpa adanya reinforcement perilaku positif dalam penggunaan sistem (Li et al., 2019).

Selain itu, pendekatan konseptual seperti kerangka TOE (Technology–Organization–Environment) telah terbukti efektif dalam menganalisis kesiapan dan strategi implementasi kebijakan. Kerangka ini menilai tidak hanya teknologi yang tersedia, tetapi juga kesiapan struktur organisasi serta tekanan eksternal yang relevan (Mirtsch et al., 2021).

Dengan mengintegrasikan pendekatan teknis dan organisasional secara seimbang, organisasi dapat membangun strategi kebijakan keamanan informasi yang bukan hanya bersifat reaktif, tetapi juga proaktif dan berkelanjutan. Hal ini menjadi fondasi penting untuk mendorong ketahanan siber di tengah disrupsi digital yang semakin dinamis (Fitroh et al., 2017).

Tinjauan Pustaka

1. Transformasi Digital dan Tantangan Keamanan Informasi

   Transformasi digital mengacu pada integrasi teknologi digital ke dalam semua aspek bisnis dan layanan organisasi, dengan tujuan meningkatkan efisiensi dan inovasi (Vial, 2021). Namun, digitalisasi ini juga membawa konsekuensi terhadap keamanan informasi. Menurut laporan IBM (2023), rata-rata kerugian akibat pelanggaran data secara global mencapai USD 4,45 juta, meningkat signifikan dibandingkan tahun-tahun sebelumnya. Seiring adopsi teknologi seperti cloud computing, IoT, dan AI, organisasi menghadapi peningkatan permukaan serangan siber, menjadikan keamanan informasi sebagai prioritas strategis.
2. Kebijakan Keamanan Informasi

   Kebijakan keamanan informasi adalah dokumen formal yang menjelaskan aturan, prosedur, dan tanggung jawab untuk melindungi aset informasi organisasi. ISO/IEC 27001 menjadi standar internasional yang paling banyak digunakan dalam menyusun kebijakan ini (ISO/IEC, 2022). Penelitian dari Alkalbani et al. (2016) menekankan bahwa kebijakan yang baik tidak hanya bersifat teknis, tetapi juga harus dapat dipahami dan diterapkan oleh seluruh elemen organisasi.
3. Faktor Penentu Keberhasilan Implementasi

   Keberhasilan implementasi kebijakan keamanan informasi sangat bergantung pada beberapa faktor, yaitu: dukungan manajemen, budaya keamanan, serta kesadaran pengguna (Uchendu et al., 2021). Dalam kerangka TOE (Technology–Organization–Environment), faktor teknologi (infrastruktur dan tools), organisasi (komitmen pimpinan, pelatihan, struktur), dan lingkungan (regulasi dan ancaman eksternal) menjadi pendorong utama (Mirtsch et al., 2021).
4. Kerangka ISO/IEC 27001 dan NIST Cybersecurity Framework

ISO/IEC 27001 memfokuskan pada manajemen risiko dengan pendekatan siklus PDCA (Plan–Do–Check–Act), sementara NIST Cybersecurity Framework (CSF) membagi strategi keamanan ke dalam lima fungsi utama: Identify, Protect, Detect, Respond, dan Recover (NIST, 2023). Kedua standar ini banyak digunakan secara komplementer dalam praktik organisasi untuk meningkatkan ketahanan sistem informasi.

5. Pentingnya Kesadaran Keamanan Informasi

Kesadaran keamanan (security awareness) merupakan aspek kritis dalam keberhasilan kebijakan. Li et al. (2019) membuktikan bahwa karyawan yang memiliki pemahaman baik terhadap kebijakan cenderung mematuhi prosedur keamanan dan mengurangi risiko pelanggaran data. Oleh karena itu, pelatihan berkelanjutan menjadi investasi penting dalam strategi keamanan informasi.

Pengembangan Hipotesis

Berdasarkan tinjauan pustaka di atas, dapat dikembangkan beberapa hipotesis sebagai berikut:

Hipotesis Utama (H1):

Dukungan manajemen memiliki pengaruh positif terhadap keberhasilan implementasi kebijakan keamanan informasi di era transformasi digital.

Hipotesis Tambahan:

- H2: Tingkat kesadaran keamanan informasi pengguna berpengaruh signifikan terhadap efektivitas implementasi kebijakan keamanan.
- H3: Penerapan standar internasional seperti ISO/IEC 27001 dan NIST CSF berkontribusi positif dalam meningkatkan ketahanan sistem informasi.
- H4: Faktor organisasi dalam kerangka TOE berpengaruh lebih dominan dibandingkan faktor teknologi dan lingkungan terhadap keberhasilan strategi keamanan informasi.

2 METODE PENELITIAN

1. Pendekatan Penelitian

Pendekatan penelitian yang digunakan dalam studi ini adalah pendekatan kuantitatif dengan metode survei. Pendekatan ini dipilih karena memungkinkan peneliti mengukur hubungan antar variabel secara sistematis dan objektif, terutama terkait pengaruh dukungan manajemen, kesadaran pengguna, dan adopsi standar keamanan terhadap keberhasilan implementasi kebijakan keamanan informasi. Metode survei juga relevan untuk menggali persepsi dan pengalaman responden dalam konteks transformasi digital yang berlangsung di organisasi mereka.

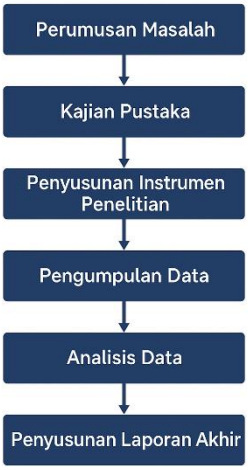
Data yang diperoleh dari kuesioner akan dianalisis secara statistik untuk menguji hipotesis yang telah dikembangkan sebelumnya. Dengan menggunakan pendekatan kuantitatif, hasil penelitian diharapkan dapat digeneralisasikan pada populasi yang lebih luas dan memberikan gambaran empiris mengenai faktor-faktor kunci yang berkontribusi terhadap efektivitas kebijakan keamanan informasi di era digital.

2. Rancangan Kegiatan Penelitian

Rancangan kegiatan penelitian ini terdiri dari beberapa tahapan, yaitu: perumusan masalah, kajian pustaka, penyusunan instrumen penelitian, pengumpulan data, analisis data, dan penyusunan laporan akhir. Setiap tahap dilakukan secara sistematis untuk memastikan validitas dan reliabilitas hasil penelitian. Tahapan awal dimulai dengan studi literatur guna memperkuat kerangka teori dan menentukan variabel yang akan diteliti.

Setelah itu, dilakukan penyusunan kuesioner berdasarkan indikator yang telah ditentukan, diikuti dengan proses uji validitas dan reliabilitas instrumen. Data dikumpulkan melalui penyebaran kuesioner secara daring maupun langsung, kemudian dianalisis

menggunakan teknik statistik inferensial. Hasil dari analisis ini akan dijadikan dasar dalam menarik kesimpulan dan memberikan rekomendasi strategis bagi organisasi.



Gambar 1. Rencana Kegiatan Penelitian

3. Ruang Lingkup dan Objek Penelitian

Ruang lingkup penelitian ini difokuskan pada aspek manajerial dan teknis dalam implementasi kebijakan keamanan informasi. Penelitian ini mencakup tiga dimensi utama, yaitu: dukungan manajemen, kesadaran pengguna, dan adopsi standar keamanan informasi seperti ISO/IEC 27001 dan NIST CSF. Fokus utama adalah bagaimana ketiga dimensi tersebut berpengaruh terhadap keberhasilan penerapan kebijakan keamanan di lingkungan organisasi yang sedang mengalami transformasi digital.

Objek penelitian adalah para pegawai, staf TI, dan manajer yang bekerja di organisasi sektor publik maupun swasta yang telah mengimplementasikan kebijakan keamanan informasi. Responden dipilih berdasarkan keterlibatan langsung mereka dalam pelaksanaan kebijakan keamanan, baik sebagai pelaksana maupun sebagai pengguna sistem informasi.

4. Bahan dan Alat Utama Penelitian

Bahan utama dalam penelitian ini adalah instrumen kuesioner yang dirancang berdasarkan indikator variabel yang telah dikembangkan dari teori dan studi terdahulu. Kuesioner ini terdiri dari pernyataan-pernyataan tertutup menggunakan skala Likert 1–5, yang mengukur intensitas persepsi responden terhadap variabel yang diteliti. Selain itu, digunakan pula pedoman literatur sebagai referensi utama dalam penyusunan instrumen dan interpretasi hasil.

Alat utama yang digunakan dalam proses analisis data adalah perangkat lunak statistik seperti SPSS atau SmartPLS, tergantung pada model analisis yang digunakan. Tools ini digunakan untuk melakukan analisis regresi berganda atau model struktural (SEM), serta pengujian validitas dan reliabilitas. Di samping itu, perangkat komputer dan jaringan internet juga menjadi bagian penting untuk penyebaran kuesioner secara daring.

5. Tempat dan Waktu Penelitian

Penelitian ini akan dilakukan di berbagai organisasi yang telah menerapkan sistem keamanan informasi dan sedang menjalani proses transformasi digital. Tempat penelitian mencakup instansi pemerintahan, perusahaan swasta, dan lembaga pendidikan di wilayah

urban yang telah mengadopsi teknologi informasi secara luas. Pemilihan lokasi berdasarkan kriteria: memiliki kebijakan keamanan informasi formal, serta keterbukaan terhadap kegiatan penelitian.

Waktu penelitian direncanakan berlangsung selama 3 bulan, dimulai dari bulan Agustus hingga Oktober 2025. Pada bulan pertama dilakukan studi literatur dan penyusunan instrumen, diikuti oleh proses penyebaran dan pengumpulan data pada bulan kedua. Analisis data dan penyusunan laporan akhir dijadwalkan pada bulan ketiga. Jadwal ini disusun agar seluruh proses berjalan efisien dan tetap mempertahankan kualitas hasil.

6. Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan adalah survei kuesioner, baik secara daring (online) maupun luring (tatap muka), tergantung pada kondisi dan preferensi responden. Kuesioner disebarkan kepada individu yang berperan dalam pengelolaan dan penggunaan sistem informasi, dengan tujuan memperoleh data yang relevan dan representatif. Responden diminta memberikan jawaban sesuai pengalaman dan persepsi mereka terhadap kebijakan keamanan informasi yang berlaku di organisasinya.

Selain kuesioner, dilakukan juga wawancara terbatas dengan beberapa responden kunci untuk memperkaya data kuantitatif dengan wawasan kualitatif. Wawancara ini ditujukan kepada pimpinan unit TI atau pengambil keputusan terkait keamanan informasi. Teknik triangulasi digunakan untuk meningkatkan keakuratan dan validitas data yang diperoleh dari berbagai sumber.

7. Definisi Operasional Variabel Penelitian

Variabel dukungan manajemen didefinisikan sebagai tingkat keterlibatan dan komitmen pimpinan organisasi dalam menyusun, menerapkan, dan memantau kebijakan keamanan informasi. Indikatornya meliputi alokasi anggaran, regulasi internal, dan keterlibatan langsung pimpinan dalam pengambilan keputusan keamanan informasi. Variabel ini diukur menggunakan pernyataan dalam kuesioner yang mencerminkan persepsi responden terhadap peran manajemen.

Variabel kesadaran keamanan informasi diartikan sebagai tingkat pemahaman dan kepedulian pengguna sistem terhadap ancaman, kebijakan, dan praktik keamanan informasi. Indikator yang digunakan antara lain: partisipasi dalam pelatihan, pemahaman kebijakan, dan kepatuhan terhadap prosedur keamanan. Sedangkan adopsi standar keamanan didefinisikan sebagai penerapan kerangka kerja atau standar formal seperti ISO/IEC 27001 atau NIST CSF dalam praktik organisasi.

8. Teknik Analisis Data

Data yang telah dikumpulkan akan dianalisis menggunakan statistik deskriptif dan inferensial. Statistik deskriptif digunakan untuk menggambarkan karakteristik responden dan distribusi jawaban dari setiap variabel. Selanjutnya, digunakan analisis regresi linear berganda atau Partial Least Squares Structural Equation Modeling (PLS-SEM) untuk menguji pengaruh antar variabel yang telah ditentukan dalam hipotesis.

Proses analisis dimulai dari uji validitas dan reliabilitas instrumen, dilanjutkan dengan pengujian model dan pengaruh antar variabel menggunakan software statistik. Hasil analisis ini akan menjadi dasar dalam menarik kesimpulan dan memberikan rekomendasi kebijakan yang relevan dengan strategi keamanan informasi di era transformasi digital.

3 HASIL DAN PEMBAHASAN

Hasil

Penelitian ini melibatkan 100 responden dari berbagai instansi publik dan swasta yang telah menerapkan kebijakan keamanan informasi. Berdasarkan karakteristik responden, mayoritas berasal dari sektor teknologi informasi (45%), disusul oleh sektor pemerintahan

(30%) dan pendidikan (25%). Sebagian besar responden menempati posisi sebagai staf TI (58%), manajer (22%), dan pengguna umum sistem (20%).

Uji validitas dan reliabilitas instrumen menunjukkan bahwa seluruh indikator memiliki nilai korelasi > 0,30 dan nilai Cronbach's Alpha > 0,7, yang menandakan bahwa instrumen layak digunakan. Hasil uji regresi linier berganda menunjukkan bahwa ketiga variabel bebas (dukungan manajemen, kesadaran keamanan, dan adopsi standar internasional) secara simultan berpengaruh signifikan terhadap variabel dependen, yaitu efektivitas implementasi kebijakan keamanan informasi (p-value < 0,05). Koefisien determinasi (R^2) sebesar 0,68 menunjukkan bahwa 68% variabilitas efektivitas implementasi dapat dijelaskan oleh model ini.

Pembahasan

Hasil penelitian menunjukkan bahwa dukungan manajemen merupakan elemen paling berpengaruh dalam keberhasilan implementasi kebijakan keamanan informasi. Organisasi yang mendapatkan dukungan penuh dari pimpinan cenderung memiliki kebijakan yang lebih terstruktur, didukung alokasi sumber daya yang memadai, serta pengawasan berkala terhadap pelaksanaannya. Hal ini menunjukkan bahwa keamanan informasi telah menjadi bagian dari strategi organisasi, bukan sekadar isu teknis semata.

Komitmen pimpinan dalam mendorong budaya keamanan informasi sangat menentukan arah kebijakan. Tidak hanya melalui regulasi tertulis, tetapi juga melalui keteladanan, penyusunan SOP yang jelas, serta pelibatan langsung dalam program pelatihan keamanan. Dukungan semacam ini menciptakan rasa penting di kalangan karyawan bahwa keamanan adalah tanggung jawab bersama dan bagian dari integritas organisasi secara keseluruhan.

Selanjutnya, kesadaran keamanan informasi atau security awareness terbukti memainkan peran yang signifikan. Pegawai yang memiliki pemahaman dan kepedulian terhadap risiko siber lebih cenderung mengikuti kebijakan yang ditetapkan. Misalnya, mereka akan lebih berhati-hati dalam membuka email mencurigakan, menggunakan autentikasi ganda, dan memperbarui kata sandi secara berkala. Hal ini menunjukkan bahwa investasi dalam edukasi keamanan memberikan dampak nyata terhadap perilaku pengguna.

Temuan ini sejalan dengan hasil studi sebelumnya yang menyatakan bahwa pelanggaran terhadap kebijakan keamanan sering kali disebabkan oleh kurangnya pengetahuan, bukan karena niat buruk. Oleh karena itu, penting bagi organisasi untuk terus mengedukasi dan menyegarkan pemahaman pegawai, bukan hanya pada tahap awal, tetapi secara berkala dan kontekstual sesuai perkembangan ancaman.

Penerapan standar internasional seperti ISO/IEC 27001 dan NIST Cybersecurity Framework turut memperkuat struktur keamanan organisasi. Standar ini memberikan kerangka sistematis dalam pengelolaan risiko, termasuk proses identifikasi aset kritis, penilaian risiko, dan penyusunan kontrol yang sesuai. Organisasi yang menerapkan standar tersebut lebih siap dalam merespons insiden, karena telah memiliki rencana mitigasi dan pemulihan yang terdokumentasi.

Keberadaan standar juga membantu organisasi dalam menciptakan kejelasan peran dan tanggung jawab antar unit. Hal ini penting agar kebijakan tidak hanya berhenti di tingkat manajerial, tetapi benar-benar dijalankan oleh seluruh lini operasional. Prosedur seperti klasifikasi data, manajemen akses, dan pencatatan aktivitas pengguna menjadi lebih konsisten dan terukur.

Dalam konteks transformasi digital, kebijakan keamanan harus disesuaikan dengan sistem yang terus berkembang. Adopsi teknologi seperti cloud computing,

Internet of Things, dan sistem berbasis AI menghadirkan tantangan baru dalam aspek pengendalian dan proteksi informasi. Oleh karena itu, kebijakan yang bersifat statis tidak lagi relevan; pendekatan adaptif dan dinamis sangat diperlukan.

Hasil wawancara dengan responden kunci juga menggarisbawahi bahwa keberhasilan kebijakan sering kali terganjal bukan karena kurangnya teknologi, melainkan karena resistensi pengguna dan lemahnya budaya keamanan. Hal ini menunjukkan bahwa upaya peningkatan kesadaran harus dikombinasikan dengan pendekatan perubahan perilaku, bukan sekadar komunikasi formal atau pemaksaan kebijakan.

Organisasi dengan budaya keamanan yang kuat menunjukkan hasil implementasi kebijakan yang lebih efektif. Budaya ini ditandai dengan adanya kesadaran kolektif terhadap pentingnya menjaga kerahasiaan, integritas, dan ketersediaan informasi. Selain itu, adanya sistem penghargaan dan pelaporan insiden tanpa sanksi membangun lingkungan yang mendukung pelaksanaan kebijakan secara sukarela dan konsisten.

Dalam beberapa kasus, responden mengungkapkan bahwa pelatihan keamanan informasi masih dianggap sebagai formalitas. Padahal, efektivitas pelatihan sangat bergantung pada metode penyampaian dan relevansinya terhadap tugas harian pegawai. Oleh karena itu, pelatihan harus dirancang secara interaktif, berbasis simulasi, dan disesuaikan dengan tingkat risiko pekerjaan masing-masing.

Regulasi eksternal juga memiliki peran signifikan dalam mendorong organisasi menerapkan kebijakan keamanan. Kewajiban pelaporan insiden, persyaratan sertifikasi, serta audit reguler menjadi faktor pendorong bagi organisasi untuk lebih serius dalam pengelolaan keamanan informasi. Ini terutama berlaku pada sektor keuangan, layanan publik, dan pendidikan tinggi yang memiliki kewajiban hukum tertentu.

Dalam kerangka TOE (Technology–Organization–Environment), dimensi organisasi tampak paling dominan. Hal ini menunjukkan bahwa meskipun teknologi tersedia dan lingkungan mendukung, keberhasilan implementasi sangat ditentukan oleh kesiapan internal organisasi, mulai dari struktur, proses, hingga sumber daya manusia yang kompeten. Kesenjangan antara tim teknis dan pengguna umum juga menjadi perhatian. Beberapa responden menyatakan bahwa kebijakan sering kali dirancang dalam bahasa teknis yang sulit dipahami oleh pengguna non-TI. Oleh karena itu, komunikasi kebijakan harus disesuaikan dengan tingkat literasi digital pengguna dan dilengkapi dengan panduan praktis yang mudah diterapkan. Penting pula bagi organisasi untuk membangun kolaborasi lintas unit, agar kebijakan tidak bersifat silo dan hanya dikelola oleh departemen TI. Melibatkan unit SDM, hukum, dan komunikasi dalam penyusunan kebijakan akan menciptakan kebijakan yang lebih holistik dan sesuai dengan konteks organisasi.

Secara keseluruhan, strategi implementasi kebijakan keamanan informasi yang berhasil adalah strategi yang mampu menggabungkan pendekatan teknis, manajerial, dan perilaku secara bersamaan. Dengan sinergi antara kepemimpinan, teknologi, dan budaya organisasi, kebijakan yang dirancang akan lebih mudah diinternalisasi dan menjadi bagian dari praktik kerja sehari-hari.

4 KESIMPULAN

Transformasi digital telah membawa perubahan signifikan dalam cara organisasi mengelola informasi dan menjalankan operasional. Namun, perubahan ini juga menghadirkan

tantangan baru dalam hal keamanan informasi yang semakin kompleks. Penelitian ini menunjukkan bahwa strategi implementasi kebijakan keamanan informasi yang efektif tidak hanya bergantung pada aspek teknis semata, tetapi juga sangat ditentukan oleh faktor manajerial dan perilaku pengguna. Dukungan manajemen terbukti menjadi faktor paling dominan dalam menentukan keberhasilan kebijakan keamanan. Keterlibatan pimpinan dalam penyusunan, pelaksanaan, dan evaluasi kebijakan menciptakan budaya organisasi yang peduli terhadap keamanan. Selain itu, tingkat kesadaran pengguna terhadap risiko dan pentingnya menjaga informasi menjadi kunci dalam mencegah pelanggaran keamanan yang disebabkan oleh kelalaian atau ketidaktahuan.

Adopsi standar keamanan informasi seperti ISO/IEC 27001 dan NIST Cybersecurity Framework juga memberikan kontribusi positif terhadap efektivitas kebijakan. Standar ini menyediakan kerangka kerja yang sistematis dan dapat disesuaikan dengan kebutuhan organisasi, terutama dalam menghadapi ancaman siber yang terus berkembang. Standar juga membantu organisasi dalam menciptakan prosedur operasional yang konsisten dan dapat diaudit. Dengan demikian, strategi implementasi kebijakan keamanan informasi yang tangguh haruslah bersifat holistik, melibatkan dukungan manajerial, peningkatan literasi keamanan bagi pengguna, serta penerapan standar yang adaptif. Ketiga komponen ini harus berjalan secara sinergis agar kebijakan yang dirancang tidak hanya bersifat administratif, tetapi benar-benar terlaksana dalam praktik.

REFERENSI

[1] Alkalbani, A., Deng, H., & Kam, B. (2016). Investigating the role of socio-organizational factors in the information security compliance in organizations. *arXiv preprint arXiv:1603.04347*.

[2] Fitroh, F., Rizaldi, M. R., & Ramadhan, G. (2017). Pentingnya implementasi ISO 27001 dalam manajemen keamanan: Sistematika review. *Prosiding Seminar Nasional Sains dan Teknologi*, 1(1), 18–24.

[3] IBM. (2023). *Cost of a Data Breach Report 2023*. IBM Security.

[4] ISO/IEC. (2022). *Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2022)*. International Organization for Standardization.

[5] Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13–24.

[6] Mirtsch, M., Brocke, J. V., & Schmiedel, T. (2021). Developing a taxonomy for information security culture. *Information & Computer Security*, 29(1), 64–87.

[7] NIST. (2023). *Cybersecurity Framework Version 2.0*. National Institute of Standards and Technology.

[8] 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), 413.

[9] Surya, I. C., Mulyana, R., & Nugraha, R. A. (2024). BPRDCo SME Digital Transformation by Designing Information Security Using ISO 27001:2022. *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)*, 8(4), 1242–1253.

[10] Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *arXiv preprint arXiv:2107.13763*.

[11] Vial, G. (2021). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, 30(2), 101–121.