Jurnal Ilmu Komputer dan Sistem Informasi
JIKSI, Vol. 02, No. 03, Oktober 2021: 121-125
Received: 5 Agustus 2021; Revised: 29 September 2021; Accepted: 26 Oktober 2021

Kebijakan dan Prosedur Keamanan Teknologi Informasi: Suatu Kajian Literatur

Desindra Deddy Kurniawan

Program Magister Teknik Informatika
Universitas Bina Darma
email : desindra.kurniawan@bmkg.go.id
Jl. Mr. H. St. Moh. Rasyid Nagari Ketaping,
Padang Pariaman 25586, Indonesia

Abstract

Advances in information technology (IT) have significantly enhanced effectiveness, efficiency, and innovation across various sectors. However, reliance on digital systems has also increased the potential for information security threats and cybercrime. This study aims to systematically examine the concept of IT security policies and procedures through a review of relevant literature. A qualitative literature study was conducted to analyze IT security theories, models, and frameworks implemented in various organizations. The findings indicate that IT security policies and procedures must be developed in an integrated manner, considering technical aspects, risk management, regulatory compliance, and human resource development. The application of the CIA Triad model, Zero Trust architecture, and the NIST Cybersecurity Framework has proven effective in strengthening organizational security systems. This study underscores the importance of integrating policies, procedures, and security culture to establish resilient and sustainable IT governance.

Kata kunci: *IT security, information policy, cyber risk management, security procedures, digital infrastructure.*

Abstrak

Kemajuan teknologi informasi (TI) membawa pengaruh besar terhadap efektivitas, efisiensi, dan inovasi di berbagai sektor. Namun, di sisi lain, ketergantungan terhadap sistem digital meningkatkan potensi ancaman keamanan informasi dan kejahatan siber. Penelitian ini bertujuan untuk menelaah secara sistematis konsep kebijakan dan prosedur keamanan TI berdasarkan kajian pustaka yang relevan. Pendekatan penelitian yang digunakan ialah studi literatur kualitatif yang meninjau teori, model, serta kerangka kerja keamanan TI yang telah diterapkan pada berbagai organisasi. Hasil kajian menunjukkan bahwa kebijakan dan prosedur keamanan TI harus disusun secara terpadu dengan memperhatikan aspek teknis, manajemen risiko, kebijakan regulatif, serta pengembangan sumber daya manusia. Penerapan model CIA Triad, Zero Trust, dan kerangka kerja NIST Cybersecurity Framework terbukti efektif dalam memperkuat sistem keamanan organisasi. Kajian ini menegaskan pentingnya integrasi antara kebijakan, prosedur, dan budaya keamanan untuk menciptakan tata kelola TI yang tangguh dan berkelanjutan.

Kata kunci: *keamanan TI, kebijakan informasi, manajemen risiko siber, prosedur keamanan, infrastruktur digital.*

1. PENDAHULUAN

Era transformasi digital telah mengubah paradigma pengelolaan organisasi di berbagai sektor, baik publik maupun privat. Teknologi informasi (TI) kini menjadi elemen krusial dalam mendukung proses bisnis, pengambilan keputusan, dan pelayanan publik. Pemanfaatan TI memungkinkan organisasi untuk meningkatkan efisiensi, mempercepat arus komunikasi, serta mengoptimalkan manajemen sumber daya. Namun, di balik manfaat tersebut, muncul pula risiko baru yang kompleks terkait keamanan data dan privasi informasi. Menurut Jumardi (2018), semakin luasnya penggunaan TI dalam aktivitas operasional organisasi berbanding lurus dengan meningkatnya potensi ancaman terhadap keamanan informasi. Pelanggaran keamanan (information security breach) tidak hanya menyebabkan kerugian material dan gangguan operasional, tetapi juga dapat merusak reputasi organisasi dan menurunkan kepercayaan publik.

Dalam konteks tata kelola teknologi informasi, keamanan informasi (information security) merupakan fondasi utama yang menjamin keberlangsungan sistem dan perlindungan terhadap data yang dikelola. Ferdiansyah et al. (2019) menjelaskan bahwa keamanan informasi mencakup tiga komponen strategis, yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability)—yang dikenal dengan istilah CIA triad. Kerahasiaan berfungsi menjaga agar data tidak diakses oleh pihak yang tidak berwenang, integritas memastikan data tetap akurat dan utuh, sedangkan ketersediaan menjamin bahwa informasi dapat diakses kapan pun dibutuhkan oleh pihak yang berhak. Penerapan prinsip-prinsip tersebut menjadi tolok ukur dalam membangun sistem informasi yang aman, andal, dan berdaya tahan terhadap ancaman siber.

Meski demikian, keamanan informasi tidak hanya bergantung pada kekuatan teknologi semata, tetapi juga pada kebijakan, prosedur, dan perilaku manusia dalam mengelola informasi. Nurul et al. (2022) menekankan bahwa faktor manusia sering kali menjadi titik lemah dalam sistem keamanan karena kelalaian, ketidaktahuan, atau kurangnya kesadaran terhadap risiko siber. Oleh karena itu, pendekatan keamanan yang efektif harus bersifat holistik, mencakup aspek teknis, kebijakan, dan budaya organisasi. Artinya, keberhasilan suatu sistem keamanan tidak hanya ditentukan oleh perangkat lunak dan infrastruktur jaringan, tetapi juga oleh perilaku etis dan kepatuhan seluruh anggota organisasi terhadap kebijakan yang telah ditetapkan.

Tantangan terbesar bagi organisasi modern adalah bagaimana menyusun dan mengimplementasikan kebijakan keamanan informasi yang selaras dengan perkembangan teknologi dan ancaman yang terus berevolusi. Wicaksana et al. (2016) mengemukakan bahwa dinamika ancaman siber bersifat adaptif—teknik serangan yang hari ini terdeteksi dapat muncul kembali dalam bentuk baru yang lebih kompleks di masa depan. Oleh karena itu, kebijakan keamanan informasi harus bersifat adaptif dan dinamis, dengan mekanisme evaluasi berkala untuk memastikan relevansinya terhadap kondisi terkini. Selain itu, kolaborasi antara unit TI, manajemen risiko, dan sumber daya manusia perlu diperkuat agar kebijakan keamanan dapat diterapkan secara konsisten dan efektif di seluruh level organisasi.

Dalam praktiknya, pengembangan kebijakan dan prosedur keamanan informasi sering kali menghadapi berbagai kendala, seperti keterbatasan sumber daya manusia yang kompeten, kurangnya dukungan manajemen puncak, serta minimnya pemahaman terhadap standar keamanan global seperti ISO/IEC 27001 atau NIST Cybersecurity Framework. Hal ini mengakibatkan banyak organisasi memiliki kebijakan keamanan yang bersifat reaktif dan fragmentaris, bukan proaktif dan terintegrasi. Akibatnya, potensi risiko kebocoran data dan serangan siber tetap tinggi meskipun organisasi telah berinvestasi dalam teknologi keamanan. Untuk itu, diperlukan kerangka konseptual dan strategi penerapan kebijakan keamanan yang tidak

hanya fokus pada pencegahan serangan, tetapi juga membangun ketahanan digital (cyber resilience) jangka panjang.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk mengidentifikasi konsep, kerangka, serta praktik terbaik (best practices) dalam penyusunan kebijakan dan prosedur keamanan informasi berdasarkan kajian literatur terkini. Fokus utama penelitian adalah pada aspek konseptual, strategi penerapan, dan relevansi kebijakan keamanan informasi terhadap kebutuhan organisasi modern. Melalui pendekatan ini diharapkan dapat diperoleh pemahaman menyeluruh tentang bagaimana organisasi dapat membangun kebijakan keamanan yang komprehensif, adaptif, dan berbasis mitigasi risiko, sekaligus menumbuhkan budaya kesadaran keamanan (security awareness culture) yang menjadi pondasi utama dalam menjaga integritas dan keberlanjutan sistem informasi di era transformasi digital.

2. METODOLOGI PENELITAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode studi pustaka (literature review). Metode ini dipilih karena mampu menyajikan analisis teoritis secara mendalam terhadap fenomena yang diteliti tanpa keterbatasan ruang dan waktu sebagaimana penelitian lapangan (Creswell & Plano Clark, 1993).

2.1 Tahapan Penelitian

1. Pengumpulan data sekunder, yakni literatur dari jurnal ilmiah, buku, dan laporan riset yang berkaitan dengan keamanan TI, kebijakan organisasi, dan manajemen risiko.
2. Klasifikasi literatur berdasarkan tema utama: teori keamanan, ancaman siber, serta kerangka kerja kebijakan.
3. Analisis tematik untuk menemukan keterkaitan antara teori dan praktik implementasi kebijakan.
4. Sintesis hasil kajian guna menghasilkan rekomendasi konseptual yang dapat diterapkan pada organisasi publik maupun swasta.

3. HASIL DAN PEMBAHASAN

3.1 Kerangka Teoritis Keamanan TI

a. Teori Tritunggal Keamanan (T3)

Teori ini berfokus pada tiga prinsip dasar keamanan informasi: kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) (Kusumaatmadja, 1990).

- Kerahasiaan menjamin data hanya diakses oleh pihak berwenang melalui mekanisme autentikasi dan enkripsi.
- Integritas memastikan data tetap utuh dan tidak dimodifikasi secara tidak sah dengan penerapan tanda tangan digital.
- Ketersediaan memastikan informasi dapat digunakan kapan pun dibutuhkan melalui perencanaan pemulihan bencana (disaster recovery plan).

b. Konsep Keamanan Berlapis (Layered Security)

Konsep ini dikenal sebagai Defense in Depth, yang mengombinasikan beberapa lapisan perlindungan seperti firewall, sistem deteksi intrusi, kebijakan akses, dan pelatihan pengguna (Schneier, 1999). Dengan demikian, kegagalan satu lapisan tidak serta-merta menimbulkan kebocoran data secara menyeluruh.

c. Pendekatan Mitigasi Risiko

Whitman dan Mattord (2018) menjelaskan bahwa mitigasi risiko dilakukan melalui lima tahap: identifikasi, penilaian, pengendalian, pemantauan, dan evaluasi. Setiap tahapan memerlukan dokumentasi formal agar organisasi memiliki dasar dalam pengambilan keputusan keamanan.

3.2 Ancaman Terhadap Infrastruktur TI

Ancaman terhadap sistem informasi dibedakan menjadi tiga kategori utama:

a. Ancaman Fisik – seperti pencurian perangkat keras, bencana alam, atau kerusakan listrik (Rahmawati, 2019).
b. Ancaman Logikal – meliputi malware, phishing, ransomware, dan serangan SQL injection yang menargetkan sistem digital (Farizy & Eriana, t.t.).
c. Ancaman Operasional – berkaitan dengan kelalaian manusia, kesalahan konfigurasi, serta ketidakpatuhan terhadap kebijakan keamanan (Budi, 2021).Pencegahan dilakukan melalui kombinasi teknologi proteksi dan kebijakan perilaku pengguna.

3.3 Pendekatan Strategis Keamanan TI

Beberapa kerangka dan model yang sering digunakan organisasi antara lain:

a. Model CIA Triad, menitikberatkan pada keseimbangan antara kerahasiaan, integritas, dan ketersediaan data (Turki et al., 2022).
b. NIST Cybersecurity Framework, menyediakan panduan Identify–Protect–Detect–Respond–Recover yang komprehensif untuk tata kelola keamanan (Mahendra, 2023).
c. Prinsip Zero Trust, menegaskan bahwa tidak ada entitas yang otomatis dipercaya tanpa verifikasi dan otorisasi berlapis (Tanque & Foxwell, 2023).
d. COBIT Framework, berfokus pada pengendalian risiko, kepatuhan regulasi, dan evaluasi kinerja keamanan TI (Haullussy, 2019).
e. Pelatihan dan Kebijakan SDM, yang memperkuat kesadaran serta tanggung jawab pengguna terhadap keamanan data (Ginanjar, 2022).

Pembahasan

Hasil kajian menunjukkan bahwa keberhasilan penerapan keamanan TI tidak hanya bergantung pada teknologi, tetapi juga pada budaya keamanan organisasi. Kebijakan dan prosedur yang baik berfungsi sebagai pedoman perilaku serta dasar hukum bagi pengelolaan keamanan informasi (Jumardi, 2018).

Penerapan Teori Tritunggal Keamanan dan Model Keamanan Berlapis terbukti efektif dalam menekan risiko serangan siber. Selain itu, integrasi kerangka NIST dan COBIT membantu organisasi melakukan evaluasi berkala terhadap efektivitas kebijakan yang diterapkan.Aspek manusia tetap menjadi titik lemah utama. Oleh karena itu, organisasi perlu menanamkan kesadaran keamanan melalui pelatihan berkelanjutan, pembaruan regulasi internal, serta audit berkala terhadap sistem dan proses kerja.

4. KESIMPULAN

Kebijakan dan prosedur keamanan TI harus disusun secara terpadu mencakup aspek teknis, manajerial, dan manusiawi. Penerapan kerangka kerja seperti CIA Triad, NIST Framework, Zero Trust, dan COBIT terbukti meningkatkan efektivitas keamanan. Pelatihan SDM dan budaya keamanan organisasi merupakan faktor penentu keberhasilan implementasi kebijakan. Evaluasi dan peninjauan berkala perlu dilakukan agar kebijakan tetap relevan terhadap dinamika ancaman siber.

Referensi

Budi, A. (2021). Evaluasi Manajemen Keamanan Informasi Berbasis ISO 27001 di Organisasi Publik. Jurnal Teknologi Informasi, 8(2), 45–54.

Creswell, J. W., & Plano Clark, V. L. (1993). Designing and Conducting Mixed Methods Research. SAGE Publications.

Ferdiansyah, R., et al. (2019). Strategi Peningkatan Keamanan Informasi di Lembaga Publik. Jurnal Sistem Informasi Nasional, 7(3), 221–229.

Ginanjar, H. (2022). Peran Kebijakan SDM dalam Meningkatkan Keamanan Data Perusahaan. Jurnal Manajemen Teknologi, 10(1), 55–66.

Haullussy, C. (2019). Evaluasi Penerapan COBIT Framework pada Institusi Pendidikan. Jurnal Teknologi dan Informasi, 9(4), 78–85.

Jumardi. (2018). Tata Kelola Keamanan Informasi di Era Digital. Jurnal Ilmu Komputer dan Sistem Informasi, 6(2), 103–114.

Kusumaatmadja, M. (1990). Dasar-Dasar Keamanan Informasi. Penerbit Tekno.

Mahendra, R. (2023). Implementasi NIST Cybersecurity Framework pada Organisasi Pemerintah. Jurnal Keamanan Digital, 5(1), 34–45.

Nurul, A., et al. (2022). Analisis Kebijakan Keamanan Informasi di Lembaga Keuangan. Jurnal Sistem Informasi, 12(2), 99–107.

Rahmawati, S. (2019). Perlindungan Fisik Aset Teknologi Informasi di Instansi Pemerintah. Jurnal Informatika Publik, 7(1), 11–18.

Schneier, B. (1999). Secrets and Lies: Digital Security in a Networked World. Wiley.Tanque, P., & Foxwell, M. (2023). Zero Trust Architecture in Government Information Systems. Cyber Defense Review, 12(2), 60–72.

Turki, F., et al. (2022). Integrating CIA Model in Modern Cybersecurity Policy. Information Security Journal, 9(3), 150–160.

Whitman, M., & Mattord, H. (2018). Principles of Information Security (6th ed.). Cengage Learning.

Wicaksana, D., et al. (2016). Manajemen Keamanan Informasi di Era Teknologi Digital. Jurnal Ilmiah Informatika, 5(1), 12–20.